เจาะลึกเวิร์กชอป PDPA: แนวทางปฏิบัติสำหรับมหาวิทยาลัยราชภัฏสกลนคร

สรุปกำหนดการอบรมเชิงปฏิบัติการ 2 วัน (30-31 มีนาคม 2569) ณ มหาวิทยาลัยราชภัฏสกลนคร โดยวิทยากร ดร.ณัฏฐ์ ธนวนทุล
เพื่อให้ผู้เข้าร่วมสามารถจัดทำเอกสารและวางระบบตามกฎหมาย PDPA ได้จริง

วันที่ 30 มีนาคม 2569: การวางรากฐานและเอกสารนโยบาย

การจัดตั้งคณะทำงานและบทบาท DPO
บรรยายสาระสำคัญของกฎหมายและกำหนดบทบาทหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

การจัดทำ Privacy Policy & Notice
ปฏิบัติการสร้างประกาศชี้แจงและนโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

การบันทึกรายการประมวลผล (RoP) และ Cookies
จัดทำข้อตกลงการประมวลผลข้อมูลและบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคล

วันที่ 31 มีนาคม 2569: การจัดการสิทธิ์และแผนเผชิญเหตุ

การจัดการสิทธิ์เจ้าของข้อมูลและความยินยอม
ปฏิบัติการทำ Data Subject Rights และระบบจัดการฐานความยินยอม (Consent Management)

แผนแจ้งเหตุข้อมูลรั่วไหลภายใน 72 ชั่วโมง
ฝึกจัดทำจดหมายแจ้งเหตุละเมิดและแผนการรายงานเหตุตามกฎหมายกำหนด

ณัฏฐ์ ธนวนกุล

บทบาท/ประสบการณ์/ผลงาน

ป.โท การตลาด
ป.เอก นวัตกรรมการจัดการเทคโนโลยี

เจ้าหน้าที่สอบประเมินสมรรถนะ
ของบุคคลตามมาตรฐานอาชีพ
(DPO ระดับ 5,6,7 และ ระดับ 7 ภาครัฐ)

สรุปย่อ
สาระสำคัญกฎหมาย PDPA

คณะทำงาน**แนวปฏิบัติ PDPA** กับ
- การคุ้มครองแรงงาน สำหรับสถานประกอบการ
- ธุรกิจโรงแรม และที่พัก

TPDPA
สมาคมผู้ตรวจสอบและให้คำปรึกษาการคุ้มครองข้อมูลส่วนบุคคลไทย
Thai Personal Data Protection Auditors and Consultants Association

นายณัฏฐ์ ธนวนกุล
กรรมการและประธานฝ่ายพัฒนามาตรฐานวิชาชีพ

กรรมการ และประธาน
สาขาพัฒนามาตรฐานวิชาชีพ
สมาคมผู้ตรวจสอบ และให้คำปรึกษา
การคุ้มครองข้อมูลส่วนบุคคลไทย (TPDPA)
Thai Personal Data Protection Auditors and Consultants Association

การวิเคราะห์การตรากฎหมาย และประเมินผลสัมฤทธิ์ของกฎหมาย ม.77

คณะทำงาน**บอร์ดเกม** PDPA

การตรวจประเมิน PDPA
เพื่อปฏิบัติตามกฎหมาย
PDPA สำหรับ DPO

Internal Audit

DPO Self-Audit Check list

10 หมวด Self-Audit check list

ที่ปรึกษา และวิทยากร
- PDPA Fundamental & Awareness
- PDPA Implementation

ที่ปรึกษา และวิทยากร
- ISO/IEC27001 , ISO/IEC27701
- ISO9001, ISO14001
- Cyber security awareness

DPO ระดับ 7
จาก TPQI สถาบันสอบคุณวุฒิวิชาชีพ

ผู้สอน DPO และ GDPO
ขึ้นทะเบียนกับ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

แจ้งการคุ้มครองข้อมูลส่วนบุคคลสำหรับ การเข้าร่วมกิจกรรมฝึกอบรม

มหาวิทยาลัยราชภัฏสกลนคร ในฐานะผู้จัดฝึกอบรม **ขอแจ้งให้ท่านผู้เข้าร่วมฝึกอบรมทราบ**ก่อนการเข้าร่วมกิจกรรมจะดำเนินการ

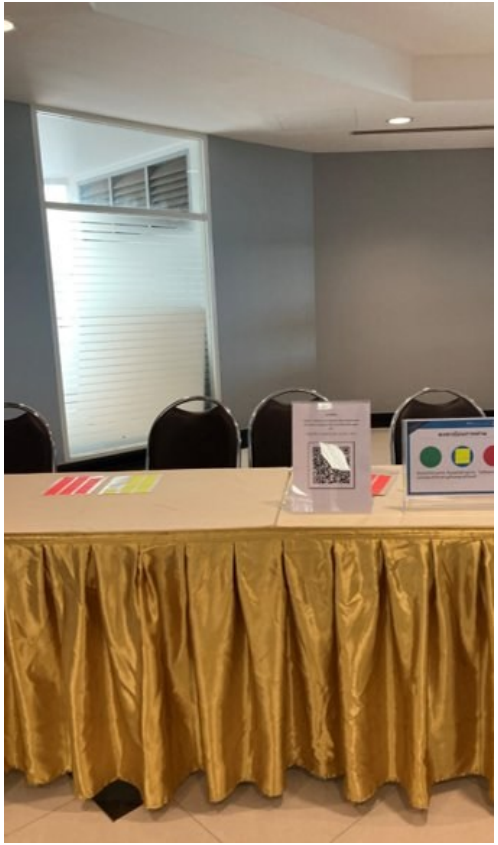
- **ลงทะเบียน**ผู้เข้าร่วมฝึกอบรม **เพื่อประโยชน์ในการยืนยันสิทธิของท่าน**
- ระหว่างการจัดฝึกอบรมจะมีการ**เก็บบรรยาการเป็นภาพนิ่งและภาพเคลื่อนไหว** ของผู้เข้าร่วมฝึกอบรม เพื่อ**นำไปประกอบเป็นสื่อประชาสัมพันธ์ผ่านช่องทางสื่อสารต่างๆ** ของผู้จัดฝึกอบรม
- **หากท่านไม่ประสงค์ให้มีการบันทึกภาพของท่าน** สามารถ**แจ้งให้ทีมงานของผู้จัดทราบ** ได้ที่จุดลงทะเบียน หรือแสดงเจตนาอย่างชัดเจนในการปฏิเสธการให้ถ่ายภาพของท่านได้

ทั้งนี้**ผู้จัดรับประกันจะไม่ดำเนินการในลักษณะที่จะกระทบสิทธิของท่าน**ในฐานะเจ้าของข้อมูลส่วนบุคคล และผู้จัด**รับประกันการรักษาความมั่นคงปลอดภัย**ของข้อมูลส่วนบุคคลของท่าน ที่เก็บรวบรวม ตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง โดย**จะไม่เปิดเผยข้อมูลส่วนบุคคลของท่านให้แก่บุคคลอื่น** เว้นแต่กรณีจำเป็นตามจุดประสงค์ที่ระบุไว้

ผู้จัดขอสงวนสิทธิในการ**เก็บข้อมูลส่วนบุคคลของท่านไว้ตลอดระยะเวลาการจัดกิจกรรมและภายหลังจากสิ้นสุดกิจกรรมตามวัตถุประสงค์ที่ระบุไว้** หากท่านมีข้อสงสัยหรือ**ต้องการใช้สิทธิ**ใดที่ท่านอาจมีเกี่ยวกับข้อมูลส่วนบุคคลของท่าน ภายใต้กฎหมายที่เกี่ยวข้อง ท่าน**สามารถติดต่อมายังผู้จัดได้ที่เจ้าหน้าจัดฝึกอบรม**

ประกาศ ณ วันที่ 30 มีนาคม 2569

ประกาศความเป็นส่วนตัวการฝึกอบรม



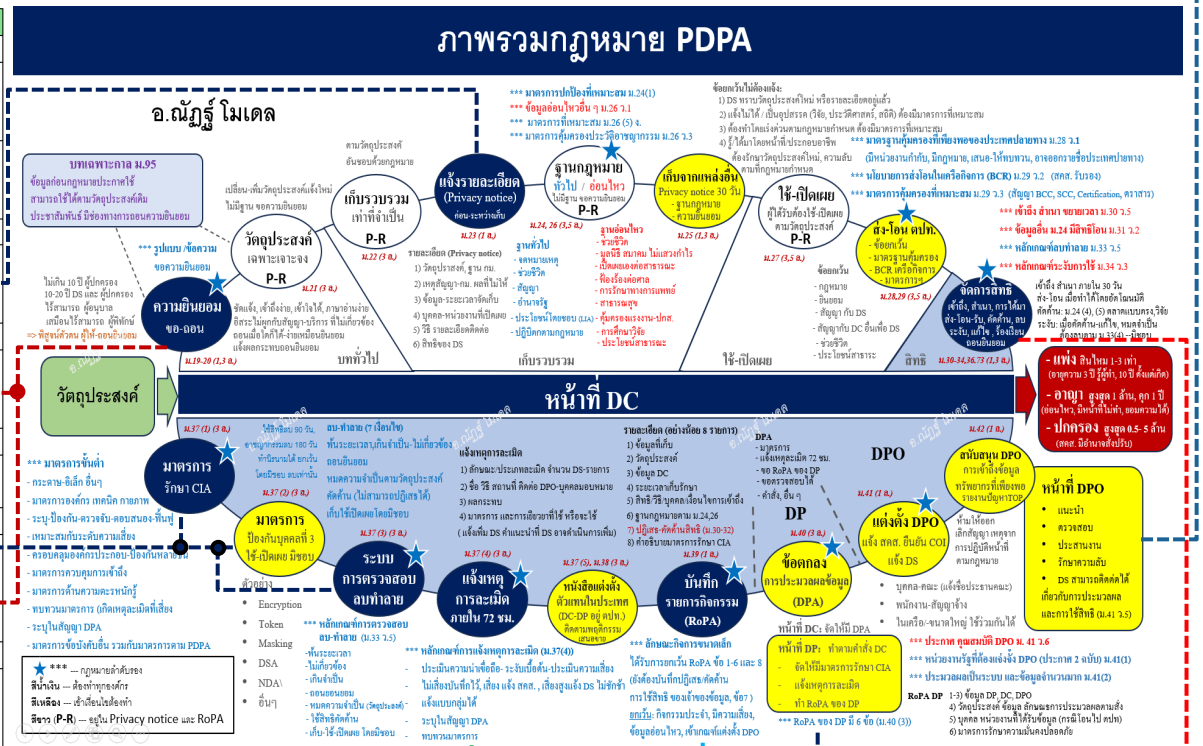
กำหนดการอบรมเชิงปฏิบัติการ

กำหนดการการอบรมเชิงปฏิบัติการ
การปฏิบัติตามกฎหมาย PDPA มหาวิทยาลัยราชภัฏสกลนคร
วันที่ 30-31 มีนาคม 2569

เวลา	กิจกรรม
วันที่ ๓๐ มีนาคม ๒๕๖๙	
๐๙:๐๐–๐๙:๓๐	- พิธีเปิดการอบรม โดยท่านอธิการบดี - บรรยายสาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล วิทยากร ดร.ณัฏฐ์ ธนวนกุล
๐๙:๓๐–๑๐:๓๐	- ปฏิบัติการจัดทำคณะทำงาน เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และบทบาทหน้าที่ตามกฎหมาย วิทยากร ดร.ณัฏฐ์ ธนวนกุล
๑๐:๓๐–๑๐:๔๕	พักรับประทานอาหารว่าง
๑๐.๔๕–๑๒:๐๐	- ปฏิบัติการจัดทำ Privacy Notice หรือ การสร้างประกาศชี้แจงการใช้ข้อมูลส่วนบุคคล - ปฏิบัติการจัดทำ Privacy Policy หรือ นโยบายการคุ้มครองข้อมูลส่วนบุคคล วิทยากร ดร.ณัฏฐ์ ธนวนกุล
๑๒:๐๐–๑๓:๐๐	พักรับประทานอาหารกลางวัน
๑๓:๐๐–๑๔:๓๐	- ปฏิบัติการจัดทำ Data Processing Agreement หรือข้อตกลงการประมวลข้อมูล - ปฏิบัติการจัดทำ Cookies หรือ Text Files ที่อยู่ประจำในคอมพิวเตอร์ ธนวนกุล
๑๔:๓๐–๑๔:๔๕	พักรับประทานอาหารว่าง
๑๔:๔๕–๑๖:๐๐	- ปฏิบัติการ Record Of Processing (RoP) หรือบันทึกการประมวลผลข้อมูลส่วนบุคคล วิทยากร ดร.ณัฏฐ์ ธนวนกุล
วันที่ ๓๑ มีนาคม ๒๕๖๙	
๐๙:๐๐–๑๐:๓๐	- ปฏิบัติการ มาตรการรักษาความมั่นคงปลอดภัย / การตรวจสอบลบทำลาย - ปฏิบัติการจัดทำ Data Subject Rights หรือ การทำสิทธิ์ของเจ้าของข้อมูล - ปฏิบัติการจัดทำ Consent Management หรือ การจัดการฐานความยินยอม วิทยากร ดร.ณัฏฐ์ ธนวนกุล
๑๐:๓๐–๑๐:๔๕	พักรับประทานอาหารว่าง
๑๐.๔๕–๑๒:๐๐	- ปฏิบัติการจัดทำแผนแจ้งเหตุข้อมูลรั่วไหลภายใน ๗๒ ชั่วโมง ตามกฎหมายกำหนด - พิธีปิดการอบรม วิทยากร ดร.ณัฏฐ์ ธนวนกุล

หมายเหตุ กำหนดการอาจเปลี่ยนแปลงตามความเหมาะสม

ภาพรวมกฎหมาย PDPA



"ข้อมูลส่วนบุคคล" คืออะไร?

ความหมายของ ข้อมูลส่วนบุคคล

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 6

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

ตามแนวทางของ GDPR

ยกตัวอย่างว่า กรณีดังต่อไปนี้เป็นข้อมูลส่วนบุคคล
< GDPR Article 4 (1) >

1. ชื่อ
2. หมายเลขประจำตัว
3. ข้อมูลสถานที่
4. สิ่งระบุอัตลักษณ์ออนไลน์
5. ปัจจัยอย่างหนึ่งหรือหลายอย่างรวมกันที่ระบุอัตลักษณ์ทางกายภาพ สรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรือสถานะทางสังคมของบุคคลธรรมดา

ข้อมูลใดเป็นข้อมูลส่วนบุคคลหรือไม่ จำต้องพิจารณาจากบริบทของการใช้ข้อมูลนั้น ๆ ประกอบด้วยว่าสามารถทำให้ระบุตัวบุคคลนั้น ๆ ได้หรือไม่ ซึ่งกฎหมายของไทยบัญญัติสอดคล้องกับกฎหมายในหลาย ๆ ประเทศที่กำหนดบทนิยามของข้อมูลส่วนบุคคลไว้แบบ "ปลายเปิด" เพื่อให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

ที่มา : มาตรา 6 แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ,
Article 4 General Data Protection Regulation (GDPR)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มือถือของเรา ทราบข้อมูลอะไรของเราบ้าง ?

รหัส

ชื่อ ที่อยู่

เบอร์โทร

การเข้าเว็บไซต์

ข้อความที่บันทึก

รูปถ่าย

บัตรเครดิต

เสียง

ไฟล์ที่ลบ

เพื่อน

ข้อมูลธนาคาร

ตัวอย่างข้อมูลส่วนบุคคลในชีวิตประจำวัน

สถานการณ์	ข้อมูลส่วนบุคคลที่ถูกเก็บ
สมัครเรียน/งาน	บัตรประชาชน, วุฒิการศึกษา, เบอร์ติดต่อ
ใช้แอปพลิเคชัน	ชื่อผู้ใช้งาน, ตำแหน่ง GPS, รูปโปรไฟล์
ลงทะเบียน WiFi มหาวิทยาลัย	เบอร์โทรศัพท์, อีเมล
ซื้อของออนไลน์	ชื่อ, ที่อยู่, เบอร์โทร, ประวัติการสั่งซื้อ
เดินเข้าอาคาร	ภาพเคลื่อนไหว, เสียง
สมัครสมาชิกห้องสมุด	ชื่อ, เลขที่ นักศึกษา, เบอร์ติดต่อ
เช่าหอพัก	ชื่อ, ที่อยู่, บัตรประชาชน, เบอร์ติดต่อ, เบอร์ญาติ
ซื้อของใน 7-11	ประวัติการซื้อสินค้า
สมัครงาน	ชื่อ, ที่อยู่, วุฒิการศึกษา, เบอร์ติดต่อ, เบอร์ญาติ

นิยามศัพท์ที่สำคัญ

ข้อมูลส่วนบุคคล

ข้อมูลเกี่ยวกับบุคคล
ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้
ไม่ว่าทางตรง หรือทางอ้อม
แต่ไม่รวมข้อมูลของผู้ถึงแก่กรรม
โดยเฉพาะ

บุคคล *หมายถึง บุคคลธรรมดา*

ทางตรง *หมายถึง ทราบทันที*

ทางอ้อม *หมายถึง ประกอบกันจึง*
ทราบ

ข้อมูลส่วนบุคคลทั่วไป

ชื่อ-สกุล
วันเดือนปีเกิด, อายุ
น้ำหนัก, ส่วนสูง
เลขที่บัตรประชาชน, หนังสือเดินทาง
เบอร์โทร, อีเมล, ที่อยู่
วุฒิ, การศึกษา. ประสบการณ์
เลขที่บัญชีธนาคาร, บัตรเครดิต
ตำแหน่ง, เงินเดือน
ทะเบียนรถ, ทะเบียนบ้าน
ตำแหน่ง GPS

ข้อมูลส่วนบุคคลอ่อนไหว

1. *เชื้อชาติ/เผ่าพันธุ์*
2. *ความคิดเห็นทางการเมือง*
3. *ความเชื่อในลัทธิ ศาสนา หรือปรัชญา*
4. *พฤติกรรมทางเพศ*
5. *ประวัติอาชญากรรม*
6. *ข้อมูลสุขภาพ*
7. *ความพิการ*
8. *ข้อมูลสหภาพแรงงาน*
9. *ข้อมูลพันธุกรรม*
10. *ข้อมูลชีวภาพ*
11. ***ข้อมูลอื่นใด ตามประกาศ***

การประมวลผลข้อมูล: การกระทำการใดๆ กับข้อมูล เช่น การเก็บ ใช้ เปิดเผย ส่งโอน เก็บรักษา ลบทำลาย

นิยามศัพท์ที่สำคัญ

ผู้ควบคุมข้อมูลส่วนบุคคล

(Data Controller, DC)

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคล

(Data Subject, DS)

บุคคลที่ข้อมูลบ่งชี้ไปถึง เป็นบุคคลธรรมดา ไม่ใช่นิติบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล

(Data Processor, DP)

บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคล ซึ่งดำเนินการดังกล่าว ไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(Data Protection Officer, DOP)

บุคคลที่ได้รับการแต่งตั้งตามกฎหมาย มาตรา 41 วรรค 1 ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ซึ่งมีหน้าที่ตามกฎหมาย มาตรา 42 วรรค 1 และติดต่อกับเจ้าของข้อมูลส่วนบุคคล ตาม มาตรา 41 วรรค 5

****** องค์กรที่ไม่อยู่ในเงื่อนไขตามกฎหมายก็สามารถแต่งตั้ง DPO ได้ เพื่อให้มีการกำกับดูแลที่ดีขึ้น***

ตัวละครใน PDPA

Data Subject (DS)

เจ้าของข้อมูลส่วนบุคคล

บุคคลธรรมดา (มีชีวิต) ที่ ข้อมูลบ่งชี้ไปถึง ได้รับสิทธิคุ้มครองข้อมูลฯ ตาม PDPA

สิทธิ

บุคคล
นิติบุคคลอื่น

Data Controller (DC)

ผู้ควบคุมข้อมูลส่วนบุคคล

บุคคล, นิติบุคคล ที่มีอำนาจตัดสินใจประมวลผลข้อมูลฯ มีหน้าที่ ปฏิบัติตาม PDPA

หน้าที่

ตัวแทน
ในประเทศ

Data Processor (DP)

ผู้ประมวลผลข้อมูลส่วนบุคคล

บุคคล, นิติบุคคล ทำตามคำสั่งของผู้ควบคุมข้อมูลฯ มีหน้าที่ ปฏิบัติตาม PDPA

หน้าที่

Data Protection Officer (DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

พนักงาน, ผู้รับจ้าง มีหน้าที่ ให้ความรู้, ตรวจสอบ,ประสานงาน รักษาความลับ

หน้าที่

Personal Data Protection Committee (PDPC)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

ควบคุม

หลักคุ้มครองข้อมูล 7 ประการ

7 Principles of Data protection

หมวด 2-3 และบทเฉพาะกาล

25 มาตรา, 75 วรรค

สาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล — บททั่วไป – การเก็บ – การใช้และเปิดเผย

หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล — สิทธิของ DS – หน้าที่ DC, DP, DPO

หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หมวด 5 การร้องเรียน — การร้องเรียน – กระบวนการพิจารณา – อำนาจของ สคส.

หมวด 6 ความรับผิดทางแพ่ง — โทษทางแพ่ง

หมวด 7 บทกำหนดโทษ — โทษทางอาญา – โทษทางปกครอง

บทเฉพาะกาล — ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมก่อนหน้าที่กฎหมายจะบังคับใช้

เจตนารมณ์ของกฎหมาย

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

ภาพรวมกฎหมาย PDPA

อ.ณัฏฐ์ ไมเดล

บทเฉพาะกาล ม.95
ข้อมูลก่อนกฎหมายประกาศใช้
สามารถใช้ได้ตามวัตถุประสงค์เดิม
ประชาสัมพันธ์ มีช่องทางการถอนความยินยอม

*** รูปแบบ /ข้อความขอความยินยอม

ไม่เกิน 10 ปี ผู้ปกครอง 10-20 ปี DS และ ผู้ปกครองไร้สามารถ ผู้อนุบาล เสมือนไร้สามารถ ผู้พิทักษ์
=> พิสูจน์ตัวตน ผู้ให้-ถอนยินยอม

ความยินยอม ขอ-ถอน — ม.19-20 (1,3 ส.)

วัตถุประสงค์ — ตามวัตถุประสงค์อันชอบด้วยกฎหมาย

วัตถุประสงค์ เฉพาะเจาะจง P-R — ม.21 (3 ส.)
เปลี่ยน-เพิ่มวัตถุประสงค์แจ้งใหม่ ไม่มีฐาน ขอความยินยอม
ชัดแจ้ง, เข้าถึงง่าย, เข้าใจได้, ภาษาอ่านง่าย
อิสระไม่ผูกกับสัญญา-บริการ ที่ไม่เกี่ยวข้อง
ถอนเมื่อใดก็ได้-ง่ายเหมือนยินยอม
แจ้งผลกระทบถอนยินยอม

เก็บรวบรวม เท่าที่จำเป็น P-R — ม.22 (3 ส.)

แจ้งรายละเอียด (Privacy notice) ก่อน-ระหว่างเก็บ — ม.23 (1 ส.)
รายละเอียด (Privacy notice)
1) วัตถุประสงค์, ฐาน กม.
2) เหตุสัญญา-กม. ผลที่ไม่ให้
3) ข้อมูล-ระยะเวลาจัดเก็บ
4) บุคคล-หน่วยงานที่เปิดเผย
5) วิธี รายละเอียดติดต่อ
6) สิทธิของ DS

ฐานกฎหมาย ทั่วไป / อ่อนไหว ไม่มีฐาน ขอความยินยอม P-R — ม.24, 26 (3,5 ส.)
*** มาตรการปกป้องที่เหมาะสม ม.24(1)
*** ข้อมูลอ่อนไหวอื่น ๆ ม.26 ว.1
*** มาตรการที่เหมาะสม ม.26 (5) จ.
*** มาตรการคุ้มครองประวัติอาชญากรรม ม.26 ว.3
ฐานทั่วไป
- จดหมายเหตุ
- ช่วยชีวิต
- สัญญา
- อำนาจรัฐ
- ประโยชน์โดยชอบ (LIA)
- ปฏิบัติตามกฎหมาย
ฐานอ่อนไหว
- ช่วยชีวิต
- มูลนิธิ สมาคม ไม่แสวงกำไร
- เปิดเผยเองต่อสาธารณะ
- ฟ้องร้องต่อศาล
- การรักษาทางการแพทย์
- สาธารณสุข
- คุ้มครองแรงงาน-ปกส.
- การศึกษาวิจัย
- ประโยชน์สาธารณะ

เก็บจากแหล่งอื่น Privacy notice 30 วัน - ฐานกฎหมาย - ความยินยอม — ม.25 (1,3 ส.)

ใช้-เปิดเผย ผู้ได้รับต้องใช้-เปิดเผยตามวัตถุประสงค์ P-R — ม.27 (3,5 ส.)
ข้อยกเว้นไม่ต้องแจ้ง:
1) DS ทราบวัตถุประสงค์ใหม่ หรือรายละเอียดอยู่แล้ว
2) แจ้งไม่ได้ / เป็นอุปสรรค (วิจัย, ประวัติศาสตร์, สถิติ) ต้องมีมาตรการที่เหมาะสม
3) ต้องทำโดยเร่งด่วนตามกฎหมายกำหนด ต้องมีมาตรการที่เหมาะสม
4) รู้/ได้มาโดยหน้าที่/ประกอบอาชีพ ต้องรักษาวัตถุประสงค์ใหม่, ความลับ ตามที่กฎหมายกำหนด

ส่ง-โอน ตปท.
- ข้อยกเว้น
- มาตรฐานคุ้มครอง
- BCR เครือกิจการ
- มาตรการฯ

ข้อยกเว้น
- กฎหมาย
- ยินยอม
- สัญญา กับ DS
- สัญญา DC อื่นเพื่อ DS
- ช่วยชีวิต
- ประโยชน์สาธาระ

ม.28,29 (3,5 ส.)
*** มาตรฐานคุ้มครองที่เพียงพอของประเทศปลายทาง ม.28 ว.1 (มีหน่วยงานกำกับ, มีกฎหมาย, เสนอ-ให้ทบทวน, อาจออกรายชื่อประเทศปลายทาง)
*** นโยบายการส่งโอนในเครือกิจการ (BCR) ม.29 ว.2 (สคส. รับรอง)
*** มาตรการคุ้มครองที่เหมาะสม ม.29 ว.3 (สัญญา BCC, SCC, Certification, ตราสาร)

จัดการสิทธิ เข้าถึง, สำเนา, การได้มา ส่ง-โอน-รับ, คัดค้าน, ลบ ระงับ, แก้ไข , ร้องเรียน ถอนยินยอม — ม.30-34,36,73 (1,3 ส.)
*** เข้าถึง สำเนา ขยายเวลา ม.30 ว.5
*** ข้อมูลอื่น ม.24 มีสิทธิโอน ม.31 ว.2
*** หลักเกณฑ์ลบทำลาย ม.33 ว.5
*** หลักเกณฑ์ระงับการใช้ ม.34 ว.3
เข้าถึง สำเนา ภายใน 30 วัน
ส่ง-โอน เมื่อทำได้โดยอัตโนมัติ
คัดค้าน: ม.24 (4), (5) ตลาดแบบตรง,วิจัย
ระงับ: เมื่อคัดค้าน-แก้ไข, หมดจำเป็น ต้องลบตาม ม.33(4) --มีชอบ

บททั่วไป | เก็บรวบรวม | ใช้-เปิดเผย | สิทธิ

หน้าที่ DC

มาตรการ รักษา CIA — ม.37 (1) (3 ส.)
*** มาตรการขั้นต่ำ
- กระดาษ-อิเล็ก อื่นๆ
- มาตรการองค์กร เทคนิค กายภาพ
- ระบุ-ป้องกัน-ตรวจจับ-ตอบสนอง-ฟื้นฟู
- เหมาะสมกับระดับความเสี่ยง
- ครอบคลุมองค์กรประกอบ-ป้องกันหลายชั้น
- มาตรการควบคุมการเข้าถึง
- มาตรการด้านความตะหนักรู้
- ทบทวนมาตรการ (เกิดเหตุละเมิดที่เสี่ยง
- ระบุในสัญญา DPA
- มาตรการข้อบังคับอื่น รวมกับมาตรการตาม PDPA

★ *** --- กฎหมายลำดับรอง

มาตรการ ป้องกันบุคคลที่ 3 ใช้-เปิดเผย มิชอบ — ม.37 (2) (3 ส.)
ใช้สิทธิลบ 90 วัน, อายุความรวมลบ 180 วัน ทำนิรนามได้ ยกเว้น โดยมิชอบ ลบเท่านั้น

ระบบ การตรวจสอบ ลบ-ทำลาย — ม.37 (3) (3 ส.)
ลบ-ทำลาย (7 เงื่อนไข)
พ้นระยะเวลา,เกินจำเป็น-ไม่เกี่ยวข้อง
ถอนยินยอม
หมดความจำเป็นตามวัตถุประสงค์
คัดค้าน (ไม่สามารถปฏิเสธได้)
เก็บใช้เปิดเผยโดยมิชอบ

ตัวอย่าง
- Encryption
- Token
- Masking
- DSA
- NDA\
- อื่นๆ

*** หลักเกณฑ์การตรวจสอบ ลบ-ทำลาย (ม.33 ว.5)
-พ้นระยะเวลา
-ไม่เกี่ยวข้อง
- เกินจำเป็น
- ถอนยอมยอม
- หมดความจำเป็น (วัตถุประสงค์)
- ใช้สิทธิคัดค้าน
- เก็บ-ใช้-เปิดเผย โดยมิชอบ

แจ้งเหตุ การละเมิด ภายใน 72 ชม. — ม.37 (4) (3 ส.)
แจ้งเหตุการละเมิด
1) ลักษณะ/ประเภทละเมิด จำนวน DS-รายการ
2) ชื่อ วิธี สถานที่ ติดต่อ DPO-บุคคลมอบหมาย
3) ผลกระทบ
4) มาตรการ และการเยียวยาที่ใช้ หรือจะใช้
(แจ้งเพิ่ม DS คำแนะนำที่ DS อาจดำเนินการเพิ่ม)

*** หลักเกณฑ์การแจ้งเหตุการละเมิด (ม.37(4))
- ประเมินความน่าเชื่อถือ- ระดับเบื้องต้น-ประเมินความเสี่ยง
- ไม่เสี่ยงบันทึกไว้, เสี่ยง แจ้ง สคส. , เสี่ยงสูงแจ้ง DS ไม่ชักช้า
- แจ้งแบบกลุ่มได้
- ระบุในสัญญา DPA
- ทบทวนมาตรการ

หนังสือแต่งตั้ง ตัวแทนในประเทศ (DC-DP อยู่ คปท.) ติดตามพฤติกรรม เสนอจาย — ม.37 (5), ม.38 (3 ส.)

บันทึก รายการกิจกรรม (RoPA) — ม.39 (1 ส.)
รายละเอียด (อย่างน้อย 8 รายการ)
1) ข้อมูลที่เก็บ
2) วัตถุประสงค์
3) ข้อมูล DC
4) ระยะเวลาเก็บรักษา
5) สิทธิ วิธี/บุคคล/เงื่อนไขการเข้าถึง
6) ฐานกฎหมายตาม ม.24,26
7) ปฏิเสธ-คัดค้านสิทธิ (ม.30-32)
8) คำอธิบายมาตรการรักษา CIA

*** ลักษณะกิจการขนาดเล็ก
ได้รับการยกเว้น RoPA ข้อ 1-6 และ 8
(ยังต้องบันทึกปฏิเสธ/คัดค้าน การใช้สิทธิ ของเจ้าของข้อมูล, ข้อ7)
ยกเว้น: กิจกรรมประจำ, มีความเสี่ยง, ข้อมูลอ่อนไหว, เข้าเกณฑ์แต่งตั้ง DPO

ข้อตกลง การประมวลผลข้อมูล (DPA) — ม.40 (3 ส.)
DPA
- มาตรการ
- แจ้งเหตุละเมิด 72 ชม.
- ขอ RoPA ของ DP
- ขอตรวจสอบได้
- คำสั่ง, อื่น ๆ

DP
- บุคคล-คณะ (แจ้งชื่อประธานคณะ)
- พนักงาน-สัญญาจ้าง
- ในเครือ/-ขนาดใหญ่ ใช้ร่วมกันได้

หน้าที่ DC: จัดให้มี DPA

หน้าที่ DP: ทำตามคำสั่ง DC
- จัดให้มีมาตรการรักษา CIA
- แจ้งเหตุการละเมิด
- ทำ RoPA ของ DP

*** RoPA ของ DP มี 6 ข้อ (ม.40 (3))

แต่งตั้ง DPO แจ้ง สคส. ยืนยัน COI แจ้ง DS — ม.41 (1 ส.)
ห้ามให้ออก เลิกสัญญา เหตุจาก การปฏิบัติหน้าที่ ตามกฎหมาย

สนับสนุน DPO การเข้าถึงข้อมูล ทรัพยากรที่เพียงพอ รายงานปัญหาTOP — ม.42 (1 ส.)

DPO

หน้าที่ DPO
- แนะนำ
- ตรวจสอบ
- ประสานงาน
- รักษาความลับ
- DS สามารถติดต่อได้ เกี่ยวกับการประมวลผล และการใช้สิทธิ (ม.41 ว.5)

*** ประกาศ คุณสมบัติ DPO ม. 41 ว.6
*** หน่วยงานรัฐที่ต้องแจ่งจั้ง DPO (ประกาศ 2 ฉบับ) ม.41(1)
*** ประมวลผลเป็นระบบ และข้อมูลจำนวนมาก ม.41(2)

RoPA DP 1-3) ข้อมูล DP, DC, DPO
4) วัตถุประสงค์ ข้อมูล ลักษณะการประมวลผลตามสั่ง
5) บุคคล หน่วยงานที่ได้รับข้อมูล (กรณีโอนไป ตปท)
6) มาตรการรักษาความมั่นคงปลอดภัย

- แพ่ง สินไหม 1-3 เท่า (อายุความ 3 ปี รู้ผู้ทำ, 10 ปี ตั้งแต่เกิด)
- อาญา สูงสุด 1 ล้าน, คุก 1 ปี (อ่อนไหว, มีหน้าที่ไม่ทำ, ยอมความได้)
- ปกครอง สูงสุด 0.5- 5 ล้าน (สคส. มีอำนาจสั่งปรับ)

ภาพรวมกฎหมาย PDPA

อ.ณัฏฐ์ โมเดล

บทเฉพาะกาล ม.95
ข้อมูลก่อนกฎหมายประกาศใช้
สามารถใช้ได้ตามวัตถุประสงค์เดิม
ประชาสัมพันธ์ มีช่องทางการถอนความยินยอม

วัตถุประสงค์

ความยินยอม ขอ-ถอน — ม.19-20 (1,3 ล.)
- *** รูปแบบ /ข้อความขอความยินยอม
- ไม่เกิน 10 ปี ผู้ปกครอง 10-20 ปี DS และ ผู้ปกครองไร้สามารถ ผู้อนุบาล เสมือนไร้สามารถ ผู้พิทักษ์
- => พิสูจน์ตัวตน ผู้ให้-ถอนยินยอม
- ชัดแจ้ง, เข้าถึงง่าย, เข้าใจได้, ภาษาอ่านง่าย อิสระไม่ผูกกับสัญญา-บริการ ที่ไม่เกี่ยวข้อง ถอนเมื่อใดก็ได้-ง่ายเหมือนยินยอม แจ้งผลกระทบถอนยินยอม

วัตถุประสงค์ เฉพาะเจาะจง P-R — ม.21 (3 ล.)
- เปลี่ยน-เพิ่มวัตถุประสงค์แจ้งใหม่ ไม่มีฐาน ขอความยินยอม

เก็บรวบรวม เท่าที่จำเป็น P-R — ม.22 (3 ล.)
- ตามวัตถุประสงค์ อันชอบด้วยกฎหมาย

แจ้งรายละเอียด (Privacy notice) ก่อน-ระหว่างเก็บ — ม.23 (1 ล.)
- รายละเอียด (Privacy notice)
  1) วัตถุประสงค์, ฐาน กม.
  2) เหตุสัญญา-กม. ผลที่ไม่ให้
  3) ข้อมูล-ระยะเวลาจัดเก็บ
  4) บุคคล-หน่วยงานที่เปิดเผย
  5) วิธี รายละเอียดติดต่อ
  6) สิทธิของ DS

ฐานกฎหมาย ทั่วไป / อ่อนไหว ไม่มีฐาน ขอความยินยอม P-R — ม.24, 26 (3,5 ล.)
- *** มาตรการปกป้องที่เหมาะสม ม.24(1)
- *** ข้อมูลอ่อนไหวอื่น ๆ ม.26 ว.1
- *** มาตรการที่เหมาะสม ม.26 (5) จ.
- *** มาตรการคุ้มครองประวัติอาชญากรรม ม.26 ว.3
- ฐานทั่วไป
  - จดหมายเหตุ
  - ช่วยชีวิต
  - สัญญา
  - อำนาจรัฐ
  - ประโยชน์โดยชอบ (LIA)
  - ปฏิบัติตามกฎหมาย
- ฐานอ่อนไหว
  - ช่วยชีวิต
  - มูลนิธิ สมาคม ไม่แสวงกำไร
  - เปิดเผยต่อสาธารณะ
  - ฟ้องร้องต่อศาล
  - การรักษาทางการแพทย์
  - สาธารณสุข
  - ประโยชน์สาธารณะ
  - คุ้มครองแรงงาน-ปกส.
  - การศึกษาวิจัย
  - ประโยชน์สาธารณะ

เก็บจากแหล่งอื่น Privacy notice 30 วัน
- ฐานกฎหมาย
- ความยินยอม
- ม.25 (1,3 ล.)

ใช้-เปิดเผย ผู้ได้รับต้องใช้-เปิดเผย ตามวัตถุประสงค์ P-R — ม.27 (3,5 ล.)
- ข้อยกเว้นไม่ต้องแจ้ง:
  1) DS ทราบวัตถุประสงค์ใหม่ หรือรายละเอียดอยู่แล้ว
  2) แจ้งไม่ได้ / เป็นภูมิสรรค (วิจัย, ประวัติศาสตร์, สถิติ) ต้องมีมาตรการที่เหมาะสม
  3) ต้องทำโดยเร่งด่วนตามกฎหมายกำหนด ต้องมีมาตรการที่เหมาะสม
  4) รู้/ได้มาโดยหน้าที่/ประกอบอาชีพ ต้องรักษาวัตถุประสงค์ใหม่, ความลับ ตามที่กฎหมายกำหนด
- *** มาตรฐานคุ้มครองที่เพียงพอของประเทศปลายทาง ม.28 ว.1 (มีหน่วยงานกำกับ, มีกฎหมาย, เสนอ-ให้ทบทวน, อาจออกรายชื่อประเทศปลายทาง)
- *** นโยบายการส่งโอนในเครือกิจการ (BCR) ม.29 ว.2 (สคส. รับรอง)
- *** มาตรการคุ้มครองที่เหมาะสม ม.29 ว.3 (สัญญา BCC, SCC, Certification, ตราสาร)

ส่ง-โอน ตปท.
- ข้อยกเว้น
- มาตรฐานคุ้มครอง
- BCR เครือกิจการ
- มาตรการฯ
- ม.28,29 (3,5 ล.)

จัดการสิทธิ เข้าถึง, สำเนา, การได้มา ส่ง-โอน-รับ, ลบ, ระงับ, แก้ไข , ร้องเรียน ถอนยินยอม — ม.30-34,36,73 (1,3 ล.)
- ข้อยกเว้น
  - กฎหมาย
  - ยินยอม
  - สัญญา กับ DS
  - สัญญา กับ DC อื่นเพื่อ DS
  - ช่วยชีวิต
  - ประโยชน์สาธาระ
- เข้าถึง สำเนา ภายใน 30 วัน ส่ง-โอน เมื่อทำได้โดยอัตโนมัติ
- คัดค้าน: ม.24 (4), (5) ตลาดแบบตรง,วิจัย
- ระงับ: เมื่อคัดค้าน-แก้ไข, หมดจำเป็น ต้องลบตาม ม.33(4) --มิชอบ

บททั่วไป | **เก็บรวบรวม** | **ใช้-เปิดเผย** | **สิทธิ**

หน้าที่ DC

มาตรการ รักษา CIA — ม.37 (1) (3 ล.)
- *** มาตรการขั้นต่ำ
- กระดาษ-อิเล็ก อื่นๆ
- มาตรการองค์กร เทคนิค กายภาพ
- ระบุ-ป้องกัน-ตรวจจับ-ตอบสนอง-ฟื้นฟู
- เหมาะสมกับระดับความเสี่ยง
- ครอบคลุมองค์กรประกอบ-ป้องกันหลายชั้น
- มาตรการควบคุมการเข้าถึง
- มาตรการด้านความตะหนักรู้
- ทบทวนมาตรการ (เกิดเหตุละเมิดที่เสี่ยง
- ระบุในสัญญา DPA
- มาตรการข้อบังคับอื่น รวมกับมาตรการตาม PDPA

มาตรการ ป้องกันบุคคลที่ 3 ใช้-เปิดเผย มิชอบ — ม.37 (2) (3 ล.)
- ใช้สิทธิลบ 90 วัน, อายุความ ลบ 180 วัน ทำปีนานได้ ยกเว้น โดยมิชอบ ลบเท่านั้น

ลบ-ทำลาย (7 เงื่อนไข) — ม.37 (3) (3 ล.)
- พื้นระยะเวลา,เกินจำเป็น-ไม่เกี่ยวข้อง
- ถอนยินยอม
- หมดความจำเป็นตามวัตถุประสงค์
- คัดค้าน (ไม่สามารถปฏิเสธได้)
- เก็บใช้เปิดเผยโดยมิชอบ

ตัวอย่าง
- Encryption
- Token
- Masking
- DSA
- NDA\
- อื่นๆ

*** หลักเกณฑ์การตรวจสอบลบ-ทำลาย (ม.33 ว.5)
- พื้นระยะเวลา
- ไม่เกี่ยวข้อง
- เกินจำเป็น
- ถอนยอมยอม
- หมดความจำเป็น (วัตถุประสงค์)
- ใช้สิทธิคัดค้าน
- เก็บ-ใช้-เปิดเผย โดยมิชอบ

ระบบการตรวจสอบลบทำลาย — ม.37 (4) (3 ล.)

แจ้งเหตุการละเมิด ภายใน 72 ชม. — ม.37 (5), ม.38 (3 ล.)
- แจ้งเหตุการละเมิดภายใน 72 ชม.
  1) ลักษณะ/ประเภทละเมิด จำนวน DS-รายการ
  2) ชื่อ วิธี สถานที่ ติดต่อ DPO-บุคคลมอบหมาย
  3) ผลกระทบ
  4) มาตรการ และการเยียวยาที่ใช้ หรือจะใช้
  (แจ้งเพิ่ม DS คำแนะนำที่ DS อาจดำเนินการเพิ่ม)
- *** หลักเกณฑ์การแจ้งเหตุการละเมิด (ม.37(4))
- ประเมินความน่าเชื่อถือ- ระบุเบื้องต้น-ประเมินความเสี่ยง
- ไม่เสี่ยงบันทึกไว้, เสี่ยง แจ้ง สคส. , เสี่ยงสูงแจ้ง DS ไม่ชักช้า
- แจ้งแบบกลุ่มได้
- ระบุในสัญญา DPA
- ทบทวนมาตรการ

หนังสือแต่งตั้งตัวแทนในประเทศ (DC-DP อยู่ ตปท.) ติดตามพฤติกรรมเสนอขาย — ม.37 (5), ม.38 (3 ล.)

บันทึกรายการกิจกรรม (RoPA) — ม.39 (1 ล.)
- รายละเอียด (อย่างน้อย 8 รายการ)
  1) ข้อมูลที่เก็บ
  2) วัตถุประสงค์
  3) ข้อมูล DC
  4) ระยะเวลาเก็บรักษา
  5) สิทธิ,วิธี/บุคคล/เงื่อนไขการเข้าถึง
  6) ฐานกฎหมายตาม ม.24,26
  7) ปฏิเสธ-คัดค้านสิทธิ (ม.30-32)
  8) คำอธิบายมาตรการรักษา CIA
- *** ลักษณะกิจการขนาดเล็ก ได้รับการยกเว้น RoPA ข้อ 1-6 และ 8 (ยังต้องบันทึกปฏิเสธ/คัดค้านการใช้สิทธิ ของเจ้าของข้อมูล, ข้อ7)
- ยกเว้น: กิจกรรมประจำ, มีความเสี่ยง, ข้อมูลอ่อนไหว, เข้าเกณฑ์แต่งตั้ง DPO

ข้อตกลง การประมวลผลข้อมูล (DPA) — ม.40 (3 ล.)
- DPA
  - มาตรการ
  - แจ้งเหตุละเมิด 72 ชม.
  - ขอ RoPA ของ DP
  - ขอตรวจสอบได้
  - คำสั่ง, อื่น ๆ
- DP
- หน้าที่ DC: จัดให้มี DPA
- หน้าที่ DP: ทำตามคำสั่ง DC
  - จัดให้มีมาตรการรักษา CIA
  - แจ้งเหตุการละเมิด
  - ทำ RoPA ของ DP
- *** RoPA ของ DP มี 6 ข้อ (ม.40 (3))

DPO — ม.41 (1 ล.)

แต่งตั้ง DPO แจ้ง สคส. ยืนยัน COI แจ้ง DS
- บุคคล-คณะ (แจ้งชื่อประธานคณะ)
- พนักงาน-สัญญาจ้าง
- ในเครือ/-ขนาดใหญ่ ใช้ร่วมกันได้

สนับสนุน DPO การเข้าถึงข้อมูล ทรัพยากรที่เพียงพอ รายงานบัญหาTOP
- ห้ามให้ออก เลิกสัญญา เหตุจากการปฏิบัติหน้าที่ตามกฎหมาย

หน้าที่ DPO
- แนะนำ
- ตรวจสอบ
- ประสานงาน
- รักษาความลับ
- DS สามารถติดต่อได้เกี่ยวกับการประมวลผล และการใช้สิทธิ (ม.41 ว.5)

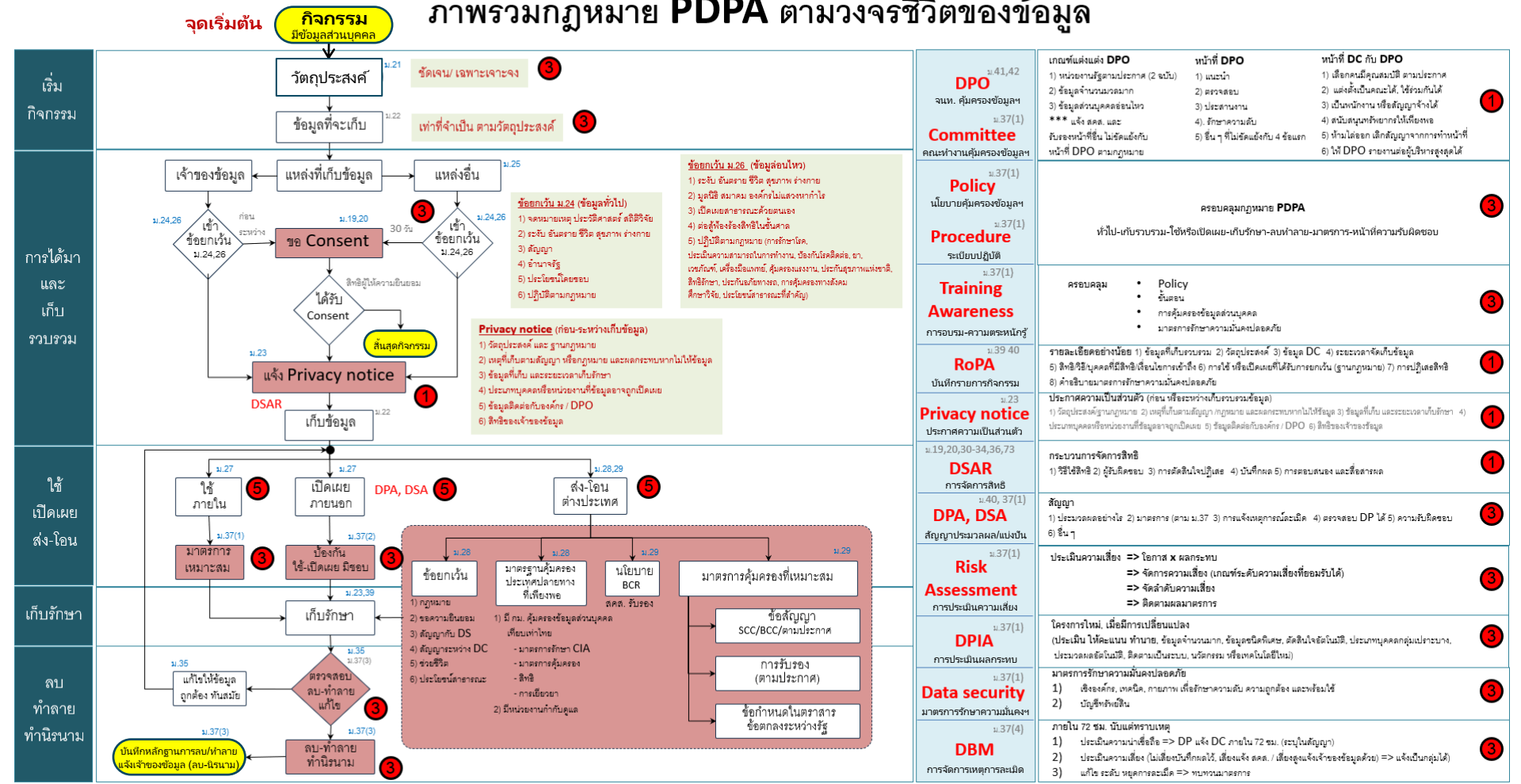
*** ประกาศ คุณสมบัติ DPO ม. 41 ว.6
*** หน่วยงานรัฐที่ต้องแจ่งตั้ง DPO (ประกาศ 2 ฉบับ) ม.41(1)
*** ประมวลผลเป็นระบบ และข้อมูลจำนวนมาก ม.41(2)

RoPA DP
1-3) ข้อมูล DP, DC, DPO
4) วัตถุประสงค์ ข้อมูล ลักษณะการประมวลผลตามสั่ง
5) บุคคล หน่วยงานที่ได้รับข้อมูล (กรณีโอนไป ตปท)
6) มาตรการรักษาความมั่นคงปลอดภัย

- แพ่ง สินไหม 1-3 เท่า (อายุความ 3 ปี รู้ผู้ทำ, 10 ปี ตั้งแต่เกิด)
- อาญา สูงสุด 1 ล้าน, คุก 1 ปี (อ่อนไหว, มีหน้าที่ไม่ทำ, ยอมความได้)
- ปกครอง สูงสุด 0.5- 5 ล้าน (สคส. มีอำนาจสั่งปรับ)

★ *** --- กฎหมายลำดับรอง
สีน้ำเงิน --- ต้องทำทุกองค์กร
สีเหลือง --- เข้าเงื่อนไขต้องทำ
สีขาว (P-R) --- อยู่ใน Privacy notice และ RoPA

ภาพรวมกฎหมาย PDPA ตามวงจรชีวิตของข้อมูล



โทษทางกฎหมาย

ปกครอง

ปรับไม่เกิน

0.5 – 5.0

ล้านบาท

สคส. มีอำนาจปรับได้เลย

pdpc สคส.

DC/DP/ตัวแทน/บุคคลใด

อาญา

ปรับไม่เกิน

0.5 – 1.0

ล้านบาท

หรือ/หรือทั้ง

จำคุกไม่เกิน

0.5 – 1.0

ปี

ยอมความได้

- DC
- ผู้ใดรู้ข้อมูลโดยหน้าที่ตาม PDPA นำไปเปิดเผยแก่ผู้อื่น
- กรรมการ ผู้จัดการ หรือบุคคลที่รับผิดชอบในการดำเนินงานของนิติบุคคล

แพ่ง

จ่ายค่าสินไหมทดแทน

1 – 3 เท่า

ของความเสียหาย
และค่าใช้จ่าย
ในการดำเนินการจริง

อายุความ 3 ปี รู้ผู้กระทำ

อายุความ 10 ปี
นับตั้งแต่เกิดเหตุ

DC/DP

โทษทางปกครอง

		ล้านบาท
ม.19-20	: ขอความยินยอมผิดจากกฎหมาย	1, 3 (หลอกลวงวัตถุประสงค์)
ม.21	: วัตถุประสงค์ไม่เฉพาะเจาะจง/ ไม่แจ้งวัตถุประสงค์ใหม่	3
ม.22	: เก็บข้อมูลส่วนบุคคลเกินจำเป็นจากวัตถุประสงค์	3
ม.23	: ไม่แจ้ง Privacy notice	1
ม.24,26	: ไม่มีฐานกฎหมายยกเว้นให้ประมวลผล	3
ม.25	: เก็บข้อมูลจากแหล่งอื่น ไม่ทำตามกฎหมาย	1, 3 (ไม่แจ้งใน 30 วัน)
ม.27	: ใช้หรือเปิดเผยนอกเหนือวัตถุประสงค์	3, 5 (เกี่ยวกับข้อมูลอ่อนไหว)
ม.28-29	: ส่งโอนไปต่างประเทศไม่ถูกต้องตามกฎหมาย	3, 5 (เกี่ยวกับข้อมูลอ่อนไหว)
ม.30-36	: ไม่ตอบสนองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย	1, 3 (คัดค้านแล้วไม่แยกส่วน)
ม.37	:ไม่ทำหน้าที่ของผู้ควบคุมตามกฎหมาย	3
ม.39	: ไม่จัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูล	1
ม.40	: ไม่ทำหน้าที่ของผู้ประมวลผลข้อมูลตามกฎหมาย	3
ม.41	: ไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบุคคล	1
ม.42	: ไม่สนับสนุน หรือให้ DPO ออกจากงานเพราะปฏิบัติหน้าที่ตามกำหมาย	1
	รวม	**28, 38**

สรุปการลงโทษการกระทำผิด PDPA ปี 2567 (7 ล้านลาท, จำนวน 1 คดี)

1. กรณีไม่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) – 1,000,000 บาท

บริษัทเข้าข่ายเป็นกิจการขนาดใหญ่ ที่เก็บรวบรวม ใช้ หรือประมวลผลข้อมูลส่วนบุคคล "เป็นกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล" ผ่านการจัดจำหน่ายสินค้าแก่ผู้บริโภคทั่วประเทศ และมีข้อมูลส่วนบุคคลของลูกค้าจำนวนมาก (จำนวนตั้งแต่ 100,000 รายขึ้นไป) จึงเข้าข่ายจำเป็นต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ตามกฎหมาย PDPA มาตรา 41 (2)

2. กรณีไม่มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม – 3,000,000 บาท

บริษัทไม่มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่มีมาตรฐานขั้นต่ำตามที่กฎหมายกำหนดหรือไม่มีประสิทธิภาพเพียงพอ ตามกฎหมาย PDPA มาตรา 37 (1) ทำให้เกิดเหตุการละเมิดข้อมูลส่วนบุคคลอย่างต่อเนื่อง โดยนอกจากนั้นในเชิงรายละเอียดยังขาด:

1) มาตรการการควบคุมการเข้าถึงข้อมูลส่วนบุคคล (Access Control) และ

2) การกำหนดสิทธิในการเข้าถึงหรือใช้งาน (Authorization)

3. กรณีไม่แจ้งเหตุละเมิดข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด – 3,000,000 บาท

เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลขึ้น จะต้องแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมงหลังทราบเหตุ และหากการละเมิดนั้นประเมินแล้วว่ามีผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลจะต้องดำเนินการแจ้งต่อเจ้าของข้อมูลด้วย ตามกฎหมาย PDPA มาตรา 37 (4) ซึ่งบริษัทไม่ได้ดำเนินการตามที่กฎหมายกำหนด

สรุปการลงโทษการกระทำผิด PDPA ปี 2568 (21.5 ล้านลาท, จำนวน 5 คดี)

หน่วยงาน	ประเภท	ลักษณะความผิด	ค่าปรับ (บาท)
หน่วยงานรัฐแห่งหนึ่งที่ให้บริการออนไลน์	รัฐ	ขาดมาตรการความปลอดภัย, ใช้พาสเวิร์ดอ่อนแอ, ไม่ประเมินความเสี่ยง, ละเลยข้อตกลงประมวลผลข้อมูล	153,120
บริษัทผู้พัฒนาและดูแลระบบของหน่วยงานรัฐ	เอกชน	ขาดมาตรการความปลอดภัย, ใช้พาสเวิร์ดอ่อนแอ, ไม่ประเมินความเสี่ยง, ละเลยข้อตกลงประมวลผลข้อมูล	153,120
โรงพยาบาลเอกชนขนาดใหญ่	เอกชน	ปล่อยเอกสารเวชระเบียนหลุด, ไม่ควบคุมกระบวนการทำลายเอกสาร	1,210,000
บุคคลธรรมดา (ผู้รับจ้างทำลายเอกสารโรงพยาบาล)	เอกชน	นำเอกสารไปเก็บที่บ้าน, ไม่แจ้งเหตุรั่วไหล, ไม่ทำตามข้อตกลงกับโรงพยาบาล	16,940
บริษัทขายคอมพิวเตอร์ขนาดใหญ่	เอกชน	ไม่มีมาตรการความปลอดภัย, ไม่แจ้งเหตุรั่วไหล, ไม่มี DPO	7,000,000
บริษัทขายเครื่องสำอาง	เอกชน	ไม่มีมาตรการความปลอดภัย, ไม่แจ้งเหตุรั่วไหล	2,500,000
บริษัทขายของเล่นสะสม	เอกชน	ไม่มีมาตรการรักษาความมั่นคงปลอดภัย แต่มีการเยียวยาผู้เสียหายซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลโดยเร็ว	500,000
บริษัทประมวลผลข้อมูล (ของเล่นสะสม)	เอกชน	ไม่มีมาตรการรักษาความมั่นคงปลอดภัย และไม่มีการตอบสนองที่รวดเร็ว และไม่มีการเยียวยาต่อผู้เสียหาย	3,000,000

ปฏิบัติการจัดทำคณะทำงาน เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และบทบาทหน้าที่ตามกฎหมาย

มาตรา 41-42

ระดับมหาวิทยาลัย แต่ทุกคนต้องทราบ

กฎหมายเกี่ยวกับ DPO

มาตรา ๔๑ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตน ในกรณีดังต่อไปนี้

(๑) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด

(๒) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอโดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด

(๓) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามที่คณะกรรมการประกาศกำหนดตามมาตรา ๒๙ วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวอาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันได้ ทั้งนี้ สถานที่ทำการแต่ละแห่งของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันดังกล่าวต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย

ความในวรรคสองให้นำมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นหน่วยงานของรัฐตาม (๑) ซึ่งมีขนาดใหญ่หรือมีสถานที่ทำการหลายแห่งโดยอนุโลม

ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องแต่งตั้งตัวแทนตามมาตรา ๓๗ (๕) ให้นำความในวรรคหนึ่งมาใช้บังคับแก่ตัวแทนโดยอนุโลม

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานทราบ ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ได้

คณะกรรมการอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยคำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลหรือเป็นผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้

มาตรา ๔๒ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

(๒) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(๓) ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามพระราชบัญญัตินี้

(๔) รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ไม่ได้ ทั้งนี้ ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับรองกับสำนักงานว่าหน้าที่หรือภารกิจดังกล่าวต้องไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

กฎหมายลำดับรอง ม.41 (1) : หน่วยงานรัฐที่ต้องแต่งตั้ง DPO

ฉบับที่ 1 ประกาศ วันที่ 27 มิ.ย.2566
มีผลบังคับใช้ 90 วัน นับจากวันที่ประกาศ

๑. สำนักนายกรัฐมนตรี
- ๑.๑ สำนักงานคณะกรรมการข้าราชการพลเรือน

๒. กระทรวงการคลัง
- ๒.๑ กรมบัญชีกลาง
- ๒.๒ สำนักงานเศรษฐกิจการคลัง

๓. กระทรวงการต่างประเทศ
- ๓.๑ กรมการกงสุล

๔. กระทรวงการท่องเที่ยวและกีฬา
- ๔.๑ กรมการท่องเที่ยว

๕. กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
- ๕.๑ สำนักงานปลัดกระทรวง
- ๕.๒ กรมกิจการเด็กและเยาวชน
- ๕.๓ กรมส่งเสริมและพัฒนาคุณภาพชีวิตคนพิการ

๖. กระทรวงเกษตรและสหกรณ์
- ๖.๑ กรมส่งเสริมการเกษตร
- ๖.๒ สำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม

๗. กระทรวงคมนาคม
- ๗.๑ กรมการขนส่งทางบก
- ๗.๒ กรมท่าอากาศยาน

๘. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
- ๘.๑ สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม
- ๘.๒ สำนักงานสถิติแห่งชาติ

๙. กระทรวงพาณิชย์
- ๙.๑ กรมทรัพย์สินทางปัญญา
- ๙.๒ กรมพัฒนาธุรกิจการค้า

๑๐. กระทรวงมหาดไทย
- ๑๐.๑ กรมการปกครอง
- ๑๐.๒ กรมการพัฒนาชุมชน
- ๑๐.๓ กรมที่ดิน

๑๑. กระทรวงแรงงาน
- ๑๑.๑ กรมการจัดหางาน
- ๑๑.๒ กรมพัฒนาฝีมือแรงงาน
- ๑๑.๓ สำนักงานประกันสังคม

๑๒. กระทรวงศึกษาธิการ
- ๑๒.๑ สำนักงานปลัดกระทรวง
- ๑๒.๒ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
- ๑๒.๓ สำนักงานคณะกรรมการการอาชีวศึกษา

๑๓. กระทรวงสาธารณสุข
- ๑๓.๑ สำนักงานปลัดกระทรวง
- ๑๓.๒ กรมการแพทย์
- ๑๓.๓ กรมควบคุมโรค
- ๑๓.๔ กรมวิทยาศาสตร์การแพทย์
- ๑๓.๕ กรมสุขภาพจิต
- ๑๓.๖ กรมอนามัย

๑๔. หน่วยงานอื่นของรัฐ
- ๑๔.๑ กรุงเทพมหานคร
- ๑๔.๒ กองทุนการออมแห่งชาติ
- ๑๔.๓ กองทุนเงินให้กู้ยืมเพื่อการศึกษา
- ๑๔.๔ กองทุนบำเหน็จบำนาญข้าราชการ
- ๑๔.๕ การทางพิเศษแห่งประเทศไทย
- ๑๔.๖ การประปานครหลวง
- ๑๔.๗ การประปาส่วนภูมิภาค
- ๑๔.๘ การไฟฟ้านครหลวง
- ๑๔.๙ การไฟฟ้าส่วนภูมิภาค
- ๑๔.๑๐ การรถไฟแห่งประเทศไทย
- ๑๔.๑๑ คุรุสภา
- ๑๔.๑๒ ธนาคารกรุงไทย จำกัด (มหาชน)
- ๑๔.๑๓ ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย
- ๑๔.๑๔ ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร

ฉบับที่ 2 ประกาศ วันที่ 9 ตุลาคม 2568
มีผลบังคับใช้ 60 วัน นับจากวันที่ประกาศ

- ๑๔.๑๕ ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย
- ๑๔.๑๖ ธนาคารแห่งประเทศไทย
- ๑๔.๑๗ ธนาคารออมสิน
- ๑๔.๑๘ ธนาคารอาคารสงเคราะห์
- ๑๔.๑๙ ธนาคารอิสลามแห่งประเทศไทย
- ๑๔.๒๐ บริษัท ขนส่ง จำกัด
- ๑๔.๒๑ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
- ๑๔.๒๒ บริษัท ไปรษณีย์ไทย จำกัด
- ๑๔.๒๓ มหาวิทยาลัยและสถาบันอุดมศึกษาของรัฐที่มีสถานพยาบาลในสังกัด
- ๑๔.๒๔ สถาบันการแพทย์ฉุกเฉินแห่งชาติ
- ๑๔.๒๕ สถาบันข้อมูลขนาดใหญ่ (องค์การมหาชน)
- ๑๔.๒๖ สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)
- ๑๔.๒๗ สถาบันคุ้มครองเงินฝาก
- ๑๔.๒๘ สถาบันทดสอบทางการศึกษาแห่งชาติ (องค์การมหาชน)
- ๑๔.๒๙ สำนักงานคณะกรรมการการเลือกตั้ง
- ๑๔.๓๐ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
- ๑๔.๓๑ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
- ๑๔.๓๒ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
- ๑๔.๓๓ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ๑๔.๓๔ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
- ๑๔.๓๕ สำนักงานหลักประกันสุขภาพแห่งชาติ

65 หน่วย + 1 กลุ่ม (รวม 88 หน่วย)

(๑) จังหวัด = 77
(๒) อบจ. = 76
(๓) เทศบาลนคร ≈ 30+
(๔) เมืองพัทยา = 1

กฎหมายลำดับรอง ม.41 (2) : ต้องตรวจสอบข้อมูล –ระบบอย่างสม่ำเสมอ โดยเหตุมีข้อมูลจำนวนมาก

ข้อ	เนื้อหา (โดยย่อ)
3	**"การดำเนินกิจกรรม"** หมายถึง การดำเนินการใด ๆ ของ DC/DP เกี่ยวกับการเก็บ-ใช้-เปิดเผยข้อมูลฯ ไม่ว่าจะเกี่ยวกับกิจกรรมหลักหรือกิจกรรมเสริมก็ตาม **"กิจกรรมหลัก"** หมายถึง การดำเนินการที่จำเป็น และสำคัญ เพื่อบรรลุวัตถุประสงค์ หรือเป้าหมายหลัก ในการดำเนินกิจการหรือภารกิจ เช่น ข้อมูลลูกค้า จำเป็นในการจัดส่งสินค้า, ข้อมูลกล้องวงจรปิด จำเป็นสำหรับการรับจ้างรักษาความปลอดภัย แต่ไม่รวมถึงกิจกรรมเสริม เช่น งานสนับสนุนด้านบุคลากร, เทคโนโลยีสารสนเทศ
4	ให้ DC/DP ที่การดำเนินกิจกรรมเก็บ-ใช้-เปิดเผยข้อมูลฯ ซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก จำเป็นต้องตรวจสอบข้อมูลฯ หรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลจำนวนมาก ตามข้อ5 และ 6 ต้องจัดให้มี DPO
5	การดำเนินกิจกรรมของ DC/DP ซึ่งเป็นกิจกรรมหลัก ที่มีการติดตาม เฝ้าสังเกต วิเคราะห์ ทำนายพฤติกรรม ทัศนคติ ลักษณะเฉพาะของบุคคล ซึ่งโดยทั่วไปจะมีการเก็บ-ใช้-เปิดเผย อย่างเป็นระบบ และเกิดขึ้นเป็นประจำ หรือเป็นปกติธุระ ให้ถือว่ามีความจำเป็นต้องตรวจสอบข้อมูลฯ หรือระบบสม่ำเสมอ การเก็บ-ใช้-เปิดเผยข้อมลฯดังนี้ ถือเป็นกรณีที่จำเป็นต้องตรวจสอบข้อมลฯ หรือระบบอย่างสม่ำเสมอด้วย 1) การเก็บ-ใช้-เปิดเผยข้อมูลฯ การใช้งานของผู้ถือบัตรสมาชิก บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์ หรือบัตรอื่นใด ซึ่งผู้ให้บริการบัตร หรือบุคคลอื่นใดสามารถตรวจสอบรายละเอียดข้อมูลการใช้บัตรได้ 2) การเก็บ-ใช้-เปิดเผยข้อมูลฯ ของลูกค้า หรือผู้รับบริการ ซึ่งเกิดขึ้นเป็นประจำ หรือเป็นปกติธุระ ที่มีการตรวจสอบสถานะ ประวัติ หรือคุณสมบัติ ก่อนเข้าทำสัญญา หรือให้บริการในลักษณะเดียวกัน เพื่อประเมินความเสี่ยงด้านต่าง ๆ เช่น การให้คะแนนเครดิต พิจารณาเบี้ยประกัน ป้องกันการโกง หรือฉ้อฉล (ไม่รวมการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตาม กม. ว่าด้วยการประกอบธุรกิจข้อมูลเครดิต) 3) การเก็บ-ใช้-เปิดเผยข้อมูลฯ เพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม 4) การเก็บ-ใช้-เปิดเผยข้อมูลฯ ของลูกค้าหรือผู้รับบริการ โดยผู้ให้บริการระบบเครือข่ายคอมพิวเตอร์ หรือผู้ประกอบกิจการโทรคมนาคม 5) การเก็บ-ใช้-เปิดเผยข้อมูลฯ เพื่อเฝ้าระวัง และรักษาความปลอดภัยตามสถานที่ต่าง ๆ 6) กรณีอื่น ตามที่คณะกรรมการกำหนด
6	การดำเนินกิจกรรมของ DC/DP ซึ่งเป็นกิจกรรมหลัก ที่มีข้อมูลจำนวนมาก ให้พิจารณาปัจจัยดังนี้ 1) จำนวน DS ที่เกี่ยวข้อง หรือสัดส่วนบุคคลที่มีการเก็บ-ใช้-เปิดเผย เมื่อเทียบกับจำนวนของ DS ทั้งหมดที่อาจเป็นไปได้ 2) ปริมาณ ประเภท หรือลักษณะของข้อมูลฯ ที่มีการเก็บ-ใช้-เปิดเผย 3) ระยะเวลา หรือความคงอยู่ ของการเก็บ-ใช้-เปิดเผยข้อมูลฯ เพื่อประโยชน์ในการดำเนินกิจกรรมหลัก 4) ขอบเขตการใช้ข้อมลฯ ขององค์กร หรือตามขนาดพื้นที่ หรือจำนวนประเทศที่เกี่ยวข้อง การเก็บ-ใช้-เปิดเผยข้อมลฯ ในกรณีดังต่อไปนี้ ให้ถือว่าเป็นข้อมลจำนวนมากด้วย 1) การเก็บ-ใช้-เปิดเผยข้อมูลฯ ซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก มีจำนวน DS ตั้งแต่ 100,000 ราย ขึ้นไป 2) การเก็บ-ใช้-เปิดเผยข้อมูลฯ เพื่อโฆษณาตามพฤติกรรม ผ่านโปรแกรมค้นหา หรือสื่อสังคมออนไลน์ ที่มีผู้ใช้งานอย่างกว้างขวาง 3) การเก็บ-ใช้-เปิดเผยข้อมูลฯ ลูกค้า หรือผู้รับบริการ ตามการดำเนินงานปกติโดยบริษัทตามกฎหมายว่าด้วยประกันชีวิต ประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงิน 4) การเก็บ-ใช้-เปิดเผยข้อมูลฯ ของลูกค้า หรือผู้รับบริการ โดยผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่ 3 ตาม กม. 5) กรณีอื่น ตามที่คณะกรรมการกำหนด
7	ในการพิจารณาเกณฑ์ตามข้อ 5 และ 6 ให้ศึกษึงถึงมาตรฐาน และแนวปฏิบัติของธุรกิจ หรือกิจการนั้น ๆ ตลอดจนความเสี่ยง และผลกระทบต่อ DS ด้วย
8	DPO อาจปฏิบัติหน้าที่ หรือภารกิจอื่นได้ แต่ DC/DP ต้องรับรองกับสำนักงาน ว่าหน้าที่ หรือภารกิจดังกล่าว ไม่ขัด หรือแย้งต่อการปฏิบัติหน้าที่ตาม กม. PDPA

บัตรสมาชิก, บัตรโดยสาร

คะแนนเครดิต, พิจารณาเบี้ยประกัน
ป้องกันฉ่อโกง, ฉ้อฉล

แพลตฟอร์มขายของออนไลน์

ค่ายมือถือ

บริษัท รปภ.

มากกว่า 1 แสนราย
โฆษณาตามพฤติกรรม สื่อที่นิยมใช้
ประกันชีวิต ประกันวินาศภัย สถาบันการเงิน

ค่ายมือถือ

ภาพรวม เรื่อง DPO ตามกฎหมาย

DC
DP
ตัวแทน

เงื่อนไขต้องแต่งตั้ง DPO

หน่วยงานรัฐตามประกาศ
ระยะ 1 **65+1 หน่วยงาน**
ระยะ 2 จว./อบจ/เทศบาลนคร/พัทยา

กิจกรรมหลัก
- **ตรวจสอบเป็นระบบ**
  - บัตรสมาชิก, บัตรโดยสารสาธารณะ บัตรอิเล็กทรอนิกส์
  - ให้คะแนนเครดิต พิจารณาเบี้ยประกัน การป้องกันการโกงหรืออ้อฉล
  - โฆษณาตามพฤติกรรม
  - เฝ้าระวังและรักษาความปลอดภัย ตามสถานที่ต่าง ๆ
  - อื่นๆ ตามประกาศกำหนด
- **มีข้อมูลจำนวนมาก**
  - จำนวน DS มากกว่า 100,000 ราย
  - การโฆษณาตามพฤติกรรม ผ่านโปรแกรมค้นหา สื่อสังคมออนไลน์
  - ประกันชีวิต วินาศภัย สถาบันการเงิน
  - กิจการโทรคมนาคม

(จำนวนสัดส่วน DS, ประเภทข้อมูล, ระยะการคงอยู่, ขอบเขตพื้นที่)

กิจกรรมหลัก
- **ประมวลผลข้อมูลอ่อนไหว**

แบบฟอร์มประเมินการแต่งตั้ง DPO

ลักษณะ DPO

พนักงาน/ผู้รับจ้าง

คนเดียว/คณะ

ใช้ DPO ร่วมกันได้
- สถานที่ทำการแต่ละแห่ง ต้องติดต่อ DPO ได้โดยง่าย
- หน่วยงานรัฐขนาดใหญ่ หรือ มีสถานที่ทำการหลายแห่ง

คุณสมบัติ DPO

- **ความรู้** หรือ
- **ความเชี่ยวชาญ** เกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคล

- สคส. **อาจประกาศ คุณสมบัติ DPO**

หน้าที่ DPO การสนับสนุน DPO

หน้าที่ DPO
- แนะนำ
- ตรวจสอบ
- ประสานงาน กับ สคส.
- รักษาความลับ
- หน้าที่อื่นๆ

การสนับสนุน DPO
- เครื่องมือ,อุปกรณ์
- อำนวยความสะดวก การเข้าถึงข้อมูล
- ห้ามให้ออก หรือ เลิกสัญญา เหตุจาก DPO ปฏิบัติหน้าที่ตาม PDPA
- มีปัญหาปฏิบัติหน้าที่ รายงานโดยตรงต่อ ผู้บริหารระดับสูงสุดได้

การแจ้งรายละเอียด DPO

แจ้ง สคส.
- อีเมล saraban@pdpc.or.th
- รับรองต่อ สคส. ว่า หน้าที่อื่น ไม่ขัดแย้ง กับหน้าที่ตาม PDPA

แจ้ง DS
- Privacy notice
- สามารถติดต่อกับ DPO เกี่ยวกับ การประมวลผลข้อมูล และการใช้สิทธิของ DS

แบบฟอร์มแจ้ง DPO ให้ สคส.

การรวบรวมข้อมูล DPO (สถิติ ณ 31 สิงหาคม 2567)

รวบรวมได้ทั้งหมด 2,214 หน่วยงาน

ภาครัฐ
125
หน่วยงาน

ภาครัฐที่ไม่เข้าข่าย มาตรา 41(1)
40หน่วยงาน

มาตรา 41(1)
85หน่วยงาน

ภาคเอกชน
2,089
หน่วยงาน

- ภาคเอกชนแต่งตั้งโดยสมัครใจ 1,037 หน่วยงาน
- มาตรา 41(2) 737 หน่วยงาน
- มาตรา 41(3) 96 หน่วยงาน
- มาตรา 41(2) และ มาตรา 41(3) 219 หน่วยงาน

การตรวจสอบความขัดแย้งต่อหน้าที่ของ DPO ตามกฎหมาย (ม.42)

ข้อ	หัวข้อการประเมิน	เรื่องที่ประเมิน	ใช่	ไม่ใช่	ผลลัพธ์ที่ควรจะเป็น (ตามมาตรฐานสากล)
1	การควบตำแหน่ง (Conflict of Interest)	- DPO ของท่านดำรงตำแหน่งผู้บริหารสูงสุด (CEO/MD) หรือไม่?			**ต้องไม่ใช่:** เพื่อป้องกันการตรวจตัวเอง
		- DPO ของท่านเป็นหัวหน้าฝ่าย IT, HR หรือ Marketing หรือไม่?			**ต้องไม่ใช่:** เพราะเป็นฝ่ายที่กำหนดวิธีการใช้ข้อมูลหลัก
2	สายการรายงาน (Reporting Line)	- DPO รายงานตรงต่อผู้บริหารระดับสูงสุด (Board/CEO) ใช่หรือไม่?			ต้องใช่: เพื่อให้มีอำนาจตัดสินใจและไม่ถูกบล็อกข้อมูล
		- DPO ต้องขออนุญาตหัวหน้าฝ่ายอื่นก่อนรายงานปัญหาใช่หรือไม่?			ต้องไม่ใช่: DPO ต้องมีสิทธิ์รายงานปัญหาได้ทันที
3	ทรัพยากรและการสนับสนุน (Resources)	- DPO มีงบประมาณและเวลาเพียงพอในการทำหน้าที่หรือไม่?			ต้องใช่: หากงานประจำล้นจนไม่ได้ทำหน้าที่ DPO องค์กรมีความผิด
		- DPO ได้รับเชิญเข้าประชุมระดับบริหารที่มีการคุยเรื่องข้อมูลหรือไม่?			ต้องใช่: DPO ต้องรับรู้โครงการใหม่ๆ ตั้งแต่ต้น (Privacy by Design)
4	การคุ้มครองการทำงาน (Protection)	- DPO เคยถูกตำหนิหรือทำโทษเพราะ "เตือน" เรื่องความเสี่ยงหรือไม่?			ต้องไม่ใช่: กฎหมายคุ้มครองไม่ให้ลงโทษ DPO จากการทำหน้าที่

ทางเลือกในการแต่งตั้ง DPO

ทางเลือก	วิธีการดำเนินการ	กลไกป้องกันความขัดแย้ง	ข้อดี	ข้อควรระวัง
1. ใช้คนภายในควบตำแหน่ง (Internal DPO with COI)	แต่งตั้งพนักงานที่มีอยู่ทำหน้าที่ DPO (เช่น IT, HR, Legal)	1) แยกบทบาทหน้าที่ (Role Separation) ชัดเจน 2) รายงานตรงต่อผู้บริหารสูงสุด (Board/CEO) ไม่ผ่านหัวหน้าแผนก	1) ประหยัดงบประมาณ 2) DPO เข้าใจวัฒนธรรมและระบบงานภายในได้ดี	ความเสี่ยง COI สูงสุด อาจขาดความเป็นอิสระในการตรวจสอบงานตัวเอง
2. ใช้ที่ปรึกษาภายนอกตรวจสอบ (Hybrid Model / External Audit)	ใช้ DPO ภายใน แต่จ้าง Audit ภายนอกมาตรวจประเมินรายปี	1) จ้าง Third-party Audit อย่างน้อยปีละ 1-2 ครั้ง 2) ใช้ผล Audit ภายนอกเป็นตัวยืนยันความถูกต้อง (Accountability)	1) สร้างความน่าเชื่อถือต่อหน่วยงานกำกับดูแล 2) ตรวจพบจุดบอดที่คนในมองไม่เห็น	มีค่าใช้จ่ายเพิ่มเติมสำหรับค่าธรรมเนียม Audit
3. ใช้ DPO ร่วมกัน (Shared DPO)	องค์กรในเครือ หรือสมาคมการค้าเดียวกัน ใช้ DPO คนเดียวกัน	1) ทำข้อตกลงการแบ่งปันทรัพยากร DPO 2) กำหนดเวลาการให้คำปรึกษาแก่แต่ละองค์กรชัดเจน	1) เฉลี่ยค่าใช้จ่ายระหว่างองค์กร 2) ลดปัญหา COI ภายในองค์กรเดียว	ต้องจัดการเรื่องความลับ (Confidentiality) ระหว่างองค์กรให้ดี
4. จ้าง DPO ภายนอกเต็มรูปแบบ (Outsourced / Virtual DPO)	จ้างบริษัทที่ปรึกษาทำหน้าที่ DPO ให้โดยตรงตามกฎหมาย	1) จัดสรรช่องทางการสื่อสารให้พนักงานเข้าถึงได้ง่าย 2) ให้สิทธิ DPO ภายนอกเข้าประชุมระดับบริหาร	1) เป็นอิสระ 100% (ไม่มี COI) 2) มีความเชี่ยวชาญสูง, Update กฎหมายตลอดเวลา	DPO อาจไม่คุ้นเคยกับรายละเอียดหน้างานจริงในเชิงลึก

กรณีศึกษาในต่างประเทศ

4 กรณีตัวอย่างที่ถูกลงโทษ เรื่อง DPO			
บทเรียนหลัก	**เคสตัวอย่าง /**	**รายละเอียดและความผิด**	**เหตุผล**
1. ห้าม DPO นั่งควบตำแหน่งบริหาร	เบลเยียม	บริษัทถูกปรับ 525,000 ยูโร เพราะให้ DPO ควบตำแหน่ง "กรรมการผู้จัดการ"	DPO ต้องไม่มีส่วนตัดสินใจ "วัตถุประสงค์และวิธีการ" ในการประมวลผลข้อมูล เพื่อป้องกันการ "ตรวจตัวเอง"
2. โครงสร้างสายการบังคับบัญชาต้องถูกต้อง	ลักเซมเบิร์ก	องค์กรถูกลงโทษเพราะให้ DPO รายงานตัวผ่านหัวหน้าแผนกบริหารความเสี่ยง หรือหัวหน้าฝ่าย Compliance	DPO ต้องรายงานตรงต่อผู้บริหารระดับสูงสุด เท่านั้น เพื่อป้องกันข้อมูลถูกบิดเบือนหรือสกัดกั้น
3. DPO สามารถถูกเลิกจ้างได้หากบกพร่อง	ฝรั่งเศส	มีเคสฟ้องร้องเรื่องการเลิกจ้าง DPO ที่ทำงานบกพร่อง	กฎหมายคุ้มครองการทำหน้าที่ตรวจสอบ แต่หาก ขาดคุณสมบัติวิชาชีพหรือบกพร่องร้ายแรง สามารถเลิกจ้างได้ตามกฎหมายแรงงาน
4. DPO ภายนอกไม่ใช่การปัดภาระ	บทบัญญัติทั่วไป	การจ้าง External DPO แต่ไม่สนับสนุนทรัพยากร หรือไม่ให้เข้าถึงข้อมูล/การประชุมสำคัญ	องค์กรยังมีความผิดฐาน ไม่สนับสนุนการทำงานของ DPO แม้จะเป็นคนนอกก็ตาม

ที่มา: The most iconic DPA decisions on DPOs and what you should take from them 2023 | IAPP

กฎหมายลำดับรอง: หน่วยงานรัฐที่ต้องแต่งตั้ง DPO ม. 41 (2)

แบบประเมินการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2)

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566 กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนในกรณีที่การดำเนินกิจกรรมหลักในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก

เพื่อส่งเสริมแนวทางการกำกับดูแลอย่างเหมาะสมและให้หน่วยงานทำการประเมินตนเองให้สอดคล้องกับหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และมีหลักฐานการประเมินหน้าที่ในการจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดังกล่าว องค์กร **พิจารณารายละเอียดหลักเกณฑ์และเงื่อนไขตามที่ประกาศฯ กำหนด ดังต่อไปนี้**

☐ **1.1 มีการดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities)**

กิจกรรมหลัก (core activities) คือ การดำเนินการที่จำเป็นและมีความสำคัญเพื่อบรรลุวัตถุประสงค์หรือเป้าหมายหลักในการดำเนินงานในกิจการหรือภารกิจของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล แต่ไม่รวมถึงกิจกรรมเสริม (ancillary activities) ที่เป็นเพียงงานสนับสนุนในการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งไม่ใช่การดำเนินการที่จำเป็นและมีความสำคัญเพื่อบรรลุวัตถุประสงค์หรือเป้าหมายหลักในการดำเนินงานในกิจการหรือภารกิจของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[1]

☐ **1.2 มีการดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ (regular and systematic monitoring)**

จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ (regular and systematic monitoring) คือการดำเนินการกิจกรรมหลักที่มีการมีการติดตาม (track) เฝ้าสังเกต (monitor) วิเคราะห์ หรือทำนายพฤติกรรม ทัศนคติ หรือลักษณะเฉพาะของบุคคล (profile) ซึ่งโดยทั่วไปจะมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอย่างเป็นระบบ (systematic) และเกิดขึ้นเป็นประจำหรือเป็นปกติธุระ (regular)[2]

☐ **1.3 มีการดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale)**

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในกรณีดังต่อไปนี้ ให้ถือเป็นกรณีที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale) [3]

(1) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities) โดยมีจำนวนเจ้าของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตั้งแต่ 100,000 รายขึ้นไป

(2) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม (behavioral advertising) ผ่านโปรแกรมค้นหา (search engine) หรือสื่อสังคมออนไลน์ (social media) ที่มีผู้ใช้งานอย่างกว้างขวาง

(3) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการตามการดำเนินงานปกติโดยบริษัทตามกฎหมายว่าด้วยประกันชีวิต บริษัทตามกฎหมายว่าด้วยประกันวินาศภัย ผู้ประกอบธุรกิจสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน ทั้งนี้ ไม่รวมถึงการดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

(4) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือผู้รับบริการโดยผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมแบบที่สามตามกฎหมายว่าด้วยการประกอบกิจการโทรคมนาคม

แบบฟอร์มประเมินการแต่งตั้ง DPO

กฎหมายลำดับรอง: หน่วยงานรัฐที่ต้องแต่งตั้ง DPO ม. 41 (2)

องค์กรในฐานะผู้ควบคุมข้อมูลส่วนบุคคล / ผู้ประมวลผลข้อมูลส่วนบุคคลได้ดำเนินการประเมินตามรายละเอียด ดังนี้

ลำดับ	หัวข้อ	เข้าเงื่อนไข	ไม่เข้าเงื่อนไข	เหตุผลประกอบ
1	การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ซึ่งเป็นส่วนหนึ่งของกิจกรรมหลัก (core activities)	☐	☐	
2	การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ (regular and systematic monitoring)	☐	☐	
3	การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก (on a large scale)	☐	☐	
สรุปผลการประเมิน		☐	☐	

ทั้งนี้ ให้คำนึงถึงมาตรฐานและแนวปฏิบัติของธุรกิจหรือกิจการนั้นๆ ตลอดจนความเสี่ยงและผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลด้วย

ดังนั้น องค์กรจึง

☐ ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ครบองค์ประกอบทั้งสามข้อข้างต้น)

☐ ไม่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามมาตรา 41 (2) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2566

ลงชื่อ .....

(.....)

ตำแหน่ง .....

ผู้มีอำนาจลงนาม

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล[4]

แบบฟอร์มแจ้ง DPO แก่ สคส.

แบบการแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

แบบฟอร์มแจ้ง
การแต่งตั้ง DPO

ส่วนที่ ๑ ข้อมูลทั่วไปของหน่วยงาน

๑.๑ หน่วยงาน .....

๑.๒ วันที่แจ้ง (วัน/เดือน/ปี) .....

๑.๓ ผู้แจ้ง .....

๑.๔ สถานที่ติดต่อและวิธีการติดต่อ

เลขที่.....หมู่ที่ .....ถนน.....ตำบล/เขต.....

อำเภอ/แขวง.....จังหวัด.....รหัสไปรษณีย์.....

หมายเลขโทรศัพท์.....หมายเลขโทรศัพท์เคลื่อนที่.....

อีเมล.....

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

(กรุณาทำเครื่องหมาย ✓หน้าช่องที่ถูกต้อง)

☐ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่คณะกรรมการประกาศกำหนด (ตามมาตรา ๔๑ (๑))

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

☐ กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖ (ตามมาตรา ๔๑ (๓))

☐ อื่นๆ

โปรดระบุ.....

ส่วนที่ ๒ ข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(กรุณาทำเครื่องหมาย ✓หน้าช่องข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อและวิธีการติดต่อ)

๒.๑ ☐ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (กรณีแต่งตั้งเป็นรายบุคคล)

ชื่อ – นามสกุล:.....

๒.๒ ☐ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (กรณีแต่งตั้งเป็นคณะทำงาน)

ชื่อ – นามสกุล (ประธานคณะทำงาน) :.....

๒.๓ สถานที่ติดต่อและวิธีการติดต่อ

เลขที่.....หมู่ที่ .....ถนน.....ตำบล/เขต.....

อำเภอ/แขวง.....จังหวัด .....รหัสไปรษณีย์.....

หมายเลขโทรศัพท์.....หมายเลขโทรศัพท์เคลื่อนที่.....

อีเมล.....

ส่วนที่ ๓ การรับรองการปฏิบัติหน้าที่หรือภารกิจอื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(กรุณาทำเครื่องหมาย ✓หน้าช่อง)

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลขอรับรองว่าการปฏิบัติหน้าที่หรือภารกิจอื่นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่ขัดหรือแย้งต่อการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ๒๕๖๒

☐ รับรอง

ส่วนที่ ๔ เอกสารหลักฐานประกอบการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

คำสั่งหรือหนังสือแต่งตั้งเจ้าหน้าที่คุ้มครองครองข้อมูลส่วนบุคคล

ลงชื่อ .....

(.....)

ตำแหน่ง .....

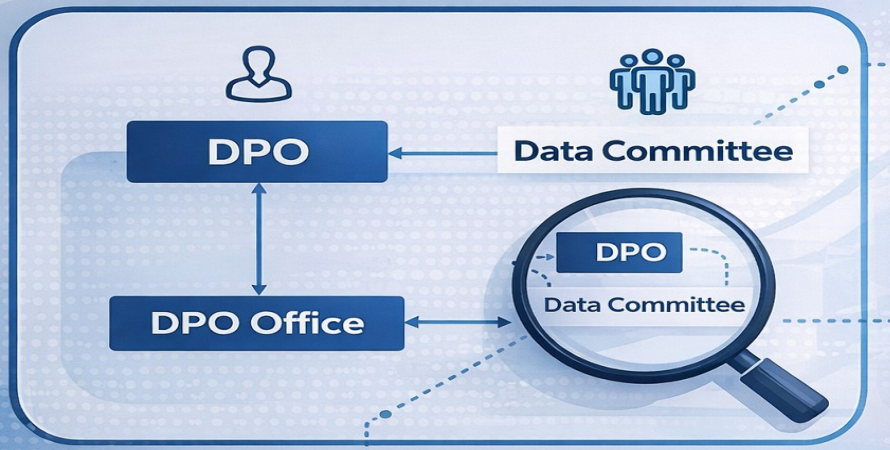
ผู้มีอำนาจลงนาม

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล


ANY QUESTIONS?

การแต่งตั้ง DPO และ คณะทำงาน

โครงสร้างที่แนะนำในการแต่งตั้ง DPO



1 DPO PDPA **ควรมีคณะกรรมการช่วย**

คณะกรรมการช่วยนี้ที่มีหน้าที่เหมาะสมตามที่กฎหมายกำหนด โดยประกอบการตัดสินใจของ DPO และประสานการดำเนินการด้าน PDPA ของแต่ละฝ่าย ซึ่งอาจประกอบด้วยตัวแทนจากหน่วยงานที่เกี่ยวข้อง

2 DPO ต้องมีสายสัมพันธ์กับผู้บริหารสูงสุด CEO

ต้องรายงานตรงต่อ CEO ได้

3 DPO ควรมีทีมงานของตนเอง

ภายใต้ DPO Office ควรประกอบด้วยพนักงานที่ดำเนินงานประจำเกี่ยวกับงานด้าน DPO โดยเฉพาะ เนื่องจากขอบเขตภาระงานของ DPO ค่อนข้างกว้าง เพื่อช่วยสนับสนุนงานในส่วนต่างๆ ของ DPO

ตัวอย่าง: การแต่งตั้งคณะทำงาน PDPA

คำสั่งมหาวิทยาลัยสวนดุสิต
ที่ ๑๒๙/๒๕๖๘
เรื่อง แต่งตั้งคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

เพื่อให้การดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต เป็นไปด้วยความเรียบร้อยและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบกับในปัจจุบันมหาวิทยาลัยมีการเปลี่ยนแปลงตำแหน่งคณะกรรมการและหน้าที่ความรับผิดชอบ จึงสมควรปรับปรุงคำสั่งให้เป็นปัจจุบัน โดยให้ยกเลิกคำสั่งมหาวิทยาลัยสวนดุสิตที่ ๓๗๑๗/๒๕๖๔ เรื่อง แต่งตั้งคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต สั่ง ณ วันที่ ๒๒ กันยายน พ.ศ. ๒๕๖๔ และคำสั่งมหาวิทยาลัยสวนดุสิตที่ ๑๓๗๘/๒๕๖๕ เรื่อง แก้ไขคำสั่ง สั่ง ณ วันที่ ๒๘ เมษายน พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๓๒ (๑) แห่งพระราชบัญญัติมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๕๘ มหาวิทยาลัยจึงแต่งตั้งคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต ดังนี้

๑. รองอธิการบดีฝ่ายบริหาร วิจัย และนวัตกรรม	ประธานกรรมการ
๒. รองอธิการบดีฝ่ายเทคโนโลยีสารสนเทศ	รองประธานกรรมการ
๓. คณบดีโรงเรียนกฎหมายและการเมือง	กรรมการ
๔. ผู้อำนวยการสำนักงานมหาวิทยาลัย	กรรมการ
๕. ผู้อำนวยการโรงเรียนสาธิตละอออุทิศ	กรรมการ
๖. ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ	กรรมการ
๗. ผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน	กรรมการ
๘. ผู้อำนวยการสถาบันภาษา ศิลปะและวัฒนธรรม	กรรมการ
๙. ผู้อำนวยการสถาบันวิจัยและพัฒนา	กรรมการ
๑๐. ผู้อำนวยการสำนักกิจการพิเศษ	กรรมการ
๑๑. ผู้อำนวยการกองกลาง	กรรมการ
๑๒. ผู้อำนวยการกองคลัง	กรรมการ
๑๓. ผู้อำนวยการกองพัฒนานักศึกษา	กรรมการ
๑๔. ผู้อำนวยการศูนย์สนเทศและแนะแนวอาชีพ	กรรมการ
๑๕. ผู้อำนวยการศูนย์พัฒนาทุนมนุษย์	กรรมการ
๑๖. ผู้อำนวยการศูนย์บริการทดสอบทางวิชาการสวนดุสิต	กรรมการ
๑๗. ผู้อำนวยการสำนักกฎหมาย	กรรมการ

-๒-/๑๘. ผู้อำนวยการ...

๑๘. ผู้อำนวยการกองบริหารงานบุคคล		กรรมการและเลขานุการ
๑๙. นายเอกรัฐ	เผ่าพงศ์ประเสริฐ	ผู้ช่วยเลขานุการ
๒๐. นางสาวรัตนา	บุญแสวง	ผู้ช่วยเลขานุการ
๒๑. นางสาวจิตรลดา	ผลนิล	ผู้ช่วยเลขานุการ

ให้คณะกรรมการมีอำนาจหน้าที่ ดังนี้

๑. ดำเนินงานด้านส่งเสริม และคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๒. พิจารณากำหนดหลักเกณฑ์นโยบายและแนวทางปฏิบัติการให้ความคุ้มครองข้อมูลส่วนบุคคล

๓. ส่งเสริมและสนับสนุนการคุ้มครองข้อมูลส่วนบุคคล มาตรการรักษาความปลอดภัย ความมั่นคงของข้อมูลส่วนบุคคลในมหาวิทยาลัยสวนดุสิต

๔. แต่งตั้งคณะอนุกรรมการ คณะทำงาน หรือบุคคล เพื่อปฏิบัติงานภายใต้หน้าที่และอำนาจของคณะกรรมการ

๕. ติดตาม ตีความ วินิจฉัยการดำเนินการด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๖. ปฏิบัติหน้าที่อื่นใดตามที่ได้รับมอบหมายจากมหาวิทยาลัย หรือตามที่กฎหมายกำหนด

ทั้งนี้ ตั้งแต่ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๗ ถึงวันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๘

สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๘

(ผู้ช่วยศาสตราจารย์ ดร.พิทักษ์ จันทร์เจริญ)
รักษาการแทนอธิการบดีมหาวิทยาลัยสวนดุสิต

ตัวอย่าง: การแต่งตั้งคณะทำงาน PDPA

คำสั่งมหาวิทยาลัยสวนดุสิต
ที่ ๓๖๖๘/๒๕๖๖
เรื่อง แต่งตั้งคณะกรรมการขับเคลื่อนนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

โดยเป็นการสมควรยกเลิกคำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๒๒๔๑/๒๕๖๕ เรื่อง แต่งตั้งคณะกรรมการขับเคลื่อนนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต สั่ง ณ วันที่ ๒๘ มิถุนายน พ.ศ. ๒๕๖๕ และคำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๔๘๒๙/๒๕๖๕ เรื่อง แต่งตั้งคณะกรรมการขับเคลื่อนนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต (เพิ่มเติม) สั่ง ณ วันที่ ๒๑ ธันวาคม พ.ศ. ๒๕๖๕ นั้น เนื่องจากมีการเปลี่ยนแปลงของกรรมการขับเคลื่อนนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

อาศัยอำนาจตามความในข้อ ๓๒(๑) แห่งประราชบัญญัติมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๕๘ และข้อ ๕ แห่งข้อบังคับมหาวิทยาลัยสวนดุสิต ว่าด้วย การบริหารงานบุคคล พ.ศ. ๒๕๖๔ ประกอบกับมติที่ประชุมคณะกรรมการขับเคลื่อนนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต ในการประชุมครั้งที่ ๕(๘)/๒๕๖๖ เมื่อวันที่ ๑๐ สิงหาคม พ.ศ. ๒๕๖๖ มหาวิทยาลัยจึงแต่งตั้งคณะกรรมการขับเคลื่อนนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต โดยมีรายนามดังนี้

๑. นายสวงค์	บุญปลูก	ประธานกรรมการ
๒. นายสุทัน	มุมแดง	กรรมการ
๓. นางจำนรรจา	พลอยมุกดา	กรรมการ
๔. นางสาววาสนา	จันทร์จ่าย	กรรมการ
๕. นายอธิพงศ์	อินโท	กรรมการ
๖. นายสนธยา	แย้มเดช	กรรมการ
๗. นางสาวธันยมัย	กลุ่นเขียว	กรรมการ
๘. นายจิรวัฒน์	สมิตสันต์	กรรมการ
๙. นายเอกรัฐ	เผ่าพงศ์ประเสริฐ	กรรมการ
๑๐. ผู้ช่วยศาสตราจารย์สร้อย	ไชยเดช	กรรมการ
๑๑. นางสาวรัตนา	บุญแสวง	กรรมการ
๑๒. นางสาวจิตรลดา	ผลนิล	กรรมการ
๑๓. นางสาวสุวิมล	แมตสอง	กรรมการและเลขานุการ
๑๔. นายชนาธิป	พยัคฆแพศ	ผู้ช่วยเลขานุการ

๒/คณะกรรมการ...

คณะกรรมการ มีอำนาจหน้าที่ ดังนี้

๑. ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่บุคลากรของมหาวิทยาลัยสวนดุสิต

๒. ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๓. กำหนดมาตรการหรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๔. ยกร่างระเบียบหรือประกาศและเสนอต่อมหาวิทยาลัยพิจารณา เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๕. ติดตามและตรวจสอบการจัดการข้อมูลส่วนบุคคลภายในมหาวิทยาลัยสวนดุสิต

๖. ประสานงานและให้ความร่วมมือกับผู้ปฏิบัติงานในมหาวิทยาลัย กรณีมีปัญหาเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๗. ปฏิบัติงานหรือภารกิจอื่นที่ได้รับมอบหมายหรือสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ทั้งนี้ ตั้งแต่วันที่ ๑๐ สิงหาคม พ.ศ. ๒๕๖๖ เป็นต้นไป หรือจนกว่าจะมีการเปลี่ยนแปลง

สั่ง ณ วันที่ ๓๐ สิงหาคม พ.ศ. ๒๕๖๖

(ดร.สุวมาลย์ ม่วงประเสริฐ)
รองอธิการบดี รักษาการแทนอธิการบดีมหาวิทยาลัยสวนดุสิต

30ส.ค.66 เวลา 13:31:56 Non-PKI Server Sign
Signature Code : MQBGA-DMARQ-AwAEU-ARqBD

ตัวอย่าง: การแต่งตั้งคณะทำงาน PDPA

คำสั่งมหาวิทยาลัยสวนดุสิต
ที่ ๑๓๐/๒๕๖๘
เรื่อง แต่งตั้งผู้ประสานงานเกี่ยวกับข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

เพื่อให้การดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต เป็นไปด้วยความเรียบร้อยและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบกับในปัจจุบันมหาวิทยาลัยมีการเปลี่ยนแปลงส่วนงาน หน่วยงาน ภายในมหาวิทยาลัย ส่งผลให้ตำแหน่งผู้ประสานงานและหน้าที่ความรับผิดชอบมีการเปลี่ยนแปลงไป จึงสมควรปรับปรุงคำสั่งให้เป็นปัจจุบัน โดยให้ยกเลิกคำสั่งมหาวิทยาลัยสวนดุสิตที่ ๑๖๖/๒๕๖๖ เรื่อง แต่งตั้งผู้ประสานงานเกี่ยวกับข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๖ คำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๘๗๑/๒๕๖๖ เรื่อง แก้ไขคำสั่ง สั่ง ณ วันที่ ๗ มีนาคม พ.ศ. ๒๕๖๖ และคำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๑๗๔๐/๒๕๖๖ เรื่อง แก้ไขคำสั่ง ลงวันที่ ๑๑ พฤษภาคม พ.ศ. ๒๕๖๖

อาศัยอำนาจตามความในมาตรา ๓๒ (๑) แห่งพระราชบัญญัติมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๕๘ มหาวิทยาลัยจึงแต่งตั้งผู้ประสานงานเกี่ยวกับข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต โดยมีหน้าที่และความรับผิดชอบ ดังนี้

๑. เป็นผู้ประสานงานกับส่วนงานหรือหน่วยงานที่รับผิดชอบฐานข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

๒. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาจากการปฏิบัติหน้าที่ตามกฎหมาย

๓. ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล นโยบายและมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

๔. จัดทำ และเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของส่วนงานหน่วยงาน ตามที่มหาวิทยาลัยกำหนด

๕. ปฏิบัติตามคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

๖. ติดตามข้อมูลและข่าวสารที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ

๗. ปฏิบัติหน้าที่อื่นหรือภารกิจอื่นด้านการคุ้มครองข้อมูลส่วนบุคคล ตามที่ได้รับมอบหมายจากมหาวิทยาลัย

ผู้ประสานงานเกี่ยวกับข้อมูลส่วนบุคคล มีรายชื่อแนบท้ายคำสั่งนี้

ทั้งนี้ ตั้งแต่ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๖๗ ถึงวันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๘

สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๘

(ผู้ช่วยศาสตราจารย์ ดร.พิทักษ์ จันทร์เจริญ)
รักษาการแทนอธิการบดีมหาวิทยาลัยสวนดุสิต

บัญชีรายชื่อแนบท้าย คำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๑๓๐/๒๕๖๘ สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๘
เรื่อง แต่งตั้งผู้ประสานงานด้านข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

ส่วนงาน/หน่วยงาน	ผู้ประสานงาน
๑. สำนักงานอธิการบดี (สำนักงานเลขานุการสภามหาวิทยาลัย)	(ก) หัวหน้าสำนักงานเลขานุการสภามหาวิทยาลัย (ข) นางสาวมาลุวดี พันธุ์คุ้มเย่า
๒. สำนักงานอธิการบดี (กองกลาง)	(ก) ผู้อำนวยการกองกลาง (ข) นางสาวสดินา วนสิทธิ์
๓. สำนักงานอธิการบดี (กองคลัง)	(ก) ผู้อำนวยการกองคลัง (ข) นางสาวสุชานัน ลังสุวรรณ
๔. สำนักงานอธิการบดี (กองบริหารงานบุคคล)	(ก) ผู้อำนวยการกองบริหารงานบุคคล (ข) นางสาวรัชญา รัตนบำรุง
๕. สำนักงานอธิการบดี (กองพัฒนานักศึกษา)	(ก) ผู้อำนวยการกองพัฒนานักศึกษา (ข) นางสาวมุทาพิน พรไชยะ
๖. สำนักงานอธิการบดี (กองอาคารและสถานที่)	(ก) ผู้อำนวยการกองอาคารและสถานที่ (ข) นางสาวพุทธาทิพย์ รัตนบำรุง
๗. สำนักงานอธิการบดี (กองประชาสัมพันธ์)	(ก) ผู้อำนวยการกองประชาสัมพันธ์ (ข) นางสาวอลิส พันธ์พรสม (ค) นายธีรพงษ์ จันคานสอ
๘. สำนักงานวิทยาเขตสุพรรณบุรี	(ก) ผู้อำนวยการสำนักงานวิทยาเขตสุพรรณบุรี (ข) นางสาวกัญธิกา บุญกิบาล
๙. สำนักงานวิทยาเขตสุพรรณบุรี (กองกลาง)	(ก) ผู้อำนวยการกองกลาง สำนักงานวิทยาเขตสุพรรณบุรี (ข) นางสาวลาวัลย์ ชาวบริสุทธิ์
๑๐. สำนักงานวิทยาเขตสุพรรณบุรี (กองอาคารและสิ่งแวดล้อม)	(ก) ผู้อำนวยการกองอาคารและสิ่งแวดล้อม สำนักงานวิทยาเขตสุพรรณบุรี (ข) นางสาวศศิวลา สุภสิงห์อง
๑๑. สำนักงานวิทยาเขตสุพรรณบุรี (กองบริการนักศึกษา)	(ก) ผู้อำนวยการกองบริการนักศึกษา สำนักงานวิทยาเขตสุพรรณบุรี (ข) นางณิยา วรรณพงษ์
๑๒. คณะครุศาสตร์	(ก) หัวหน้าสำนักงานคณะครุศาสตร์ (ข) นางสาวิภารี จงปู
๑๓. คณะมนุษยศาสตร์และสังคมศาสตร์	(ก) หัวหน้าสำนักงานคณะมนุษยศาสตร์และสังคมศาสตร์ (ข) นางสาวณัฐกัลยพร ไชสิงหรี่
๑๔. คณะวิทยาการจัดการ	(ก) หัวหน้าสำนักงานคณะวิทยาการจัดการ (ข) นางสาวอรุณรัศมี สุภากอ้วน
๑๕. คณะวิทยาศาสตร์และเทคโนโลยี	(ก) หัวหน้าสำนักงานคณะวิทยาศาสตร์และเทคโนโลยี (ข) นางสาวนราภรณ์ ศิริกิจวาน

บัญชีรายชื่อแนบท้าย คำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๑๓๐/๒๕๖๘ สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๘
เรื่อง แต่งตั้งผู้ประสานงานด้านข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

ส่วนงาน/หน่วยงาน	ผู้ประสานงาน
๑๖. คณะพยาบาลศาสตร์	(ก) หัวหน้าสำนักงานคณะพยาบาลศาสตร์ (ข) นางสาวสุกัญญา ศิลานนท์
๑๗. โรงเรียนการเรือน	(ก) หัวหน้าสำนักงานโรงเรียนการเรือน (ข) นายชนพล ภักดสังจานันท์
๑๘. โรงเรียนการท่องเที่ยวและการบริการ	(ก) หัวหน้าสำนักงานโรงเรียนการท่องเที่ยวและการบริการ (ข) นางสาพรสรวง เพ็งพริ้ง
๑๙. โรงเรียนสาธิตละอออุทิศ	(ก) หัวหน้าสำนักงานฝ่ายวิชาการโรงเรียนสาธิตละอออุทิศ (ข) นายโชคริทิน วิริยวรกุล
๒๐. บัณฑิตวิทยาลัย	(ก) หัวหน้าสำนักงานบัณฑิตวิทยาลัย (ข) นายกิตติพงศ์ อิ่มประคองศิลป์
๒๑. โรงเรียนกฎหมายและการเมือง	(ก) หัวหน้าสำนักงานโรงเรียนกฎหมายและการเมือง (ข) นายชยุต หาญชาญพานิชย์
๒๒. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	(ก) หัวหน้าสำนักงานฝ่ายการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ (ข) นายธีรบุญ เศรษฐคุณ
๒๓. สำนักส่งเสริมวิชาการและงานทหารนักเรียน	(ก) หัวหน้าสำนักงานฝ่ายการสำนักส่งเสริมวิชาการและงานทหารนักเรียน (ข) นางสาวสุดาลงค์ หงษ์กลาง
๒๔. สถาบันภาษา ศิลปะและวัฒนธรรม	(ก) หัวหน้าสำนักงานฝ่ายการสถาบันภาษา ศิลปะและวัฒนธรรม (ข) นางสาวรุ่งนภา ในวี
๒๕. สถาบันวิจัยและพัฒนา	(ก) หัวหน้าสำนักงานฝ่ายการสถาบันวิจัยและพัฒนา (ข) นางสาวพัชริดา สุวรรณนา
๒๖. สำนักกิจการพิเศษ	(ก) หัวหน้าสำนักงานฝ่ายการสำนักกิจการพิเศษ (ข) นางสาวสุนิสา ดนนงาม
๒๗. สวนดุสิตโพล	(ก) ประธานดำเนินงานสวนดุสิตโพล (ข) นางสาวปวมณี ไชวัง
๒๘. สวนดุสิตโอเปนเอาร์	(ก) ผู้จัดการสวนดุสิตโอเปนเอาร์ (ข) นางสาวอรุณี อัศวภูมิ
๒๙. ศูนย์การศึกษา ตรัง	(ก) ผู้อำนวยการศูนย์การศึกษา ตรัง (ข) นายธีรเดช รักไทย
๓๐. ศูนย์การศึกษา นครนายก	(ก) ผู้อำนวยการศูนย์การศึกษา นครนายก (ข) นางสาวพันธุ์ทิพย์ สิงห์ปาน

บัญชีรายชื่อแนบท้าย คำสั่งมหาวิทยาลัยสวนดุสิต ที่ ๑๓๐/๒๕๖๘ สั่ง ณ วันที่ ๑๓ มกราคม พ.ศ. ๒๕๖๘
เรื่อง แต่งตั้งผู้ประสานงานด้านข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

ส่วนงาน/หน่วยงาน	ผู้ประสานงาน
๓๑. ศูนย์การศึกษา ลำปาง	(ก) ผู้อำนวยการศูนย์การศึกษา ลำปาง (ข) นางสาวสุนทรี ศรีโกย
๓๒. ศูนย์การศึกษา หัวหิน	(ก) รองผู้อำนวยการศูนย์การศึกษา หัวหิน (ข) หม่อมหวงสุดิสิวัณย์ จักรพันธุ์
๓๓. ศูนย์บริการสื่อและสิ่งพิมพ์การพิพิคไทย์	(ก) ผู้อำนวยการศูนย์บริการสื่อและสิ่งพิมพ์การพิพิคไทย์ (ข) นางสาวศรีวรรณ พูนค่าย
๓๔. ศูนย์พัฒนาทุนมนุษย์	(ก) ผู้อำนวยการศูนย์พัฒนาทุนมนุษย์ (ข) นางสาวสุวรรณา แดงโด
๓๕. ศูนย์บริการทดสอบทางวิชาการสวนดุสิต	(ก) ผู้อำนวยการศูนย์บริการทดสอบทางวิชาการสวนดุสิต (ข) นายวิรวรานต์ ผลุงโยธิน
๓๖. โครงการปฏิบัติการอาหารแปรรูป	(ก) ผู้จัดการโครงการปฏิบัติการอาหารแปรรูป (ข) นางสาวภาณุจนา วรรณพงษ
๓๗. สำนักยุทธศาสตร์และแผน	(ก) รองผู้อำนวยการสำนักยุทธศาสตร์และแผน (ข) นางสาวฉลิรัตน์ บัวเอม
๓๘. สำนักกฎหมาย	(ก) ผู้อำนวยการสำนักกฎหมาย (ข) นายเอกรัฐ เผ่าพงศ์ประเสริฐ
๓๙. สำนักงานตรวจสอบภายใน	(ก) หัวหน้าสำนักงานตรวจสอบภายใน (ข) นางสาวเพ็ญพรัชฎ์ หิรัญสาย
๔๐. ศูนย์คนเทคและแนวการศึกษาและอาชีพ	(ก) ผู้อำนวยการศูนย์คนเทคและแนวการศึกษาและอาชีพ (ข) นางสาวณมร เพ็ชรทักษ์
๔๑. สำนักงานบริการอาคารวิทยาศาสตร์	(ก) ผู้จัดการสำนักงานบริการอาคารวิทยาศาสตร์ (ข) นางสาวพุทธสิณี โกมลสิงห์
๔๒. สำนักงานบริการอาคารบัณฑิตวิทยาลัย	(ก) ผู้จัดการสำนักงานบริการอาคารบัณฑิตวิทยาลัย (ข) นางสาวนิอัสรา เจ็ดสูงสิ่ง

ตัวอย่าง: การแต่งตั้งคณะทำงาน PDPA

คำสั่งมหาวิทยาลัยสวนดุสิต
ที่ ๒๒๔๐/๒๕๖๕
เรื่อง แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต

เพื่อให้การดำเนินการของมหาวิทยาลัยสวนดุสิตเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปด้วยความเรียบร้อย และสอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๓๒ (๑) แห่งพระราชบัญญัติมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๕๘ และมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการดำเนินการกำหนดนโยบายข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต ครั้งที่ ๔(๕)/๒๕๖๕ ในวันที่ ๒๗ มิถุนายน ๒๕๖๕ มหาวิทยาลัยจึงแต่งตั้ง ดร.สวงค์ บุญปลูก ตำแหน่ง รองอธิการบดีฝ่ายเทคโนโลยีสารสนเทศ เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยสวนดุสิต โดยให้มีอำนาจหน้าที่ ดังนี้

๑. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งส่วนงาน พนักงานมหาวิทยาลัย ลูกจ้างของมหาวิทยาลัยสวนดุสิต ผู้รับจ้างหรือผู้ที่ปฏิบัติงานให้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๒. ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งส่วนงาน พนักงานมหาวิทยาลัย ลูกจ้างของมหาวิทยาลัยสวนดุสิต ผู้รับจ้างหรือผู้ที่ปฏิบัติงานให้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๓. ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งส่วนงาน พนักงานมหาวิทยาลัย ลูกจ้างของมหาวิทยาลัยสวนดุสิต ผู้รับจ้างหรือผู้ที่ปฏิบัติงานให้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๔. รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และประกาศมหาวิทยาลัยสวนดุสิต เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

๕. รายงานปัญหาในการปฏิบัติหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยต่อผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรงได้

๖. ปฏิบัติหน้าที่หรือภารกิจอื่นที่สอดคล้องกับการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ทั้งนี้ ตั้งแต่วันที่ ๒๗ มิถุนายน พ.ศ. ๒๕๖๕ เป็นต้นไป

สั่ง ณ วันที่ ๒๘ มิถุนายน พ.ศ. ๒๕๖๕

(รองศาสตราจารย์ ดร.ศิโรจน์ ผลพันธิน)
อธิการบดีมหาวิทยาลัยสวนดุสิต

28มิ.ย.65 เวลา 15:39:00 Non-PKI Server Sign
Signature Code : QwA5A-DUAOA-BBADM-AQwBC

ตัวอย่าง: การแต่งตั้งคณะทำงาน PDPA

คำสั่งมหาวิทยาลัยราชภัฏจันทรเกษม
ที่ ๔๗๑/๒๕๖๕
เรื่อง แต่งตั้งคณะกรรมการดำเนินงาน และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
มหาวิทยาลัยราชภัฏจันทรเกษม

ด้วย มหาวิทยาลัยราชภัฏจันทรเกษม ได้ดำเนินงานเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย และสอดคล้องกับกฎหมายที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา ๓๑ แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ.๒๕๔๗ และมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ มหาวิทยาลัยจึงให้ยกเลิกคำสั่งมหาวิทยาลัยราชภัฏจันทรเกษม ที่ ๕๖๒/๒๕๖๕ เรื่อง แต่งตั้งคณะกรรมการดำเนินงานตามโครงการงานจ้างที่ปรึกษาโครงการการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และให้แต่งตั้งคณะกรรมการดำเนินงาน และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

๑. ผู้บริหารคุ้มครองข้อมูลส่วนบุคคล
รองอธิการบดี ฝ่ายบริหาร
อำนาจหน้าที่
๑. กำหนดทิศทางและเป็นที่ปรึกษาในการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคล
๒. กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล
๓. พิจารณากำหนดแนวทางและวิธีการประเมินความเสี่ยง เกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่สามารถยอมรับได้
๔. พิจารณาผลการประเมินความเสี่ยง
๕. พิจารณาและรับรองการดำเนินการตามมาตรการคุ้มครองข้อมูลส่วนบุคคล
๖. ให้การสนับสนุนการดำเนินงาน กำกับ ควบคุมและดูแลการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏจันทรเกษม

๒. คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

๑. รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ที่กำกับดูแลงานเทคโนโลยีสารสนเทศและงานเทคโนโลยีการศึกษา		ประธานกรรมการ
๒. รองผู้อำนวยการฝ่ายบริหาร สำนักส่งเสริมวิชาการและงานทะเบียน		กรรมการ
๓. นางสาวอาราตา	คู่เจริญถาวร	กรรมการ

อำนาจหน้าที่
๑. ให้คำแนะนำและความรู้ในการปฏิบัติตามข้อกำหนดสำคัญต่างๆ เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ แก่ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล และเจ้าหน้าที่เกี่ยวข้อง ตลอดจนกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับอื่น
๒. ตรวจสอบการดำเนินงานของมหาวิทยาลัยในการเข้าถึงและดูแลข้อมูลส่วนบุคคลต่างๆ ให้เป็นไปอย่างถูกต้องตามข้อกำหนดในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
๓. ประเมินผลและระบุถึงจุดประสงค์ของการนำข้อมูลส่วนบุคคลไปใช้หรือเผยแพร่ และชี้แจงถึงสิทธิของเจ้าของข้อมูลรวมถึงมาตรการนำมาใช้ในการปกป้องข้อมูลส่วนบุคคล
๔. ประสานงานกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในกรณีเกิดปัญหาการใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลในมหาวิทยาลัย
๕. ดูแลการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กรและบุคลากรที่เกี่ยวข้องสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และนโยบายคุ้มครองข้อมูลของมหาวิทยาลัย รวมถึงการจัดกิจกรรมคุ้มครองข้อมูลภายในมหาวิทยาลัย
๖. ประสานงานและร่วมมือกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล (หรือหน่วยงานที่เกี่ยวข้อง) ในกรณีที่มีปัญหาในการประมวลผลข้อมูล
๗. ไกล่เกลี่ยข้อพิพาทต่างๆ ในเบื้องต้นกับ เจ้าของข้อมูลส่วนบุคคล กรณีเกิดการร้องเรียนต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล
๘. รักษาความลับของข้อมูลส่วนบุคคลจากการปฏิบัติหน้าที่

๓. คณะกรรมการดำเนินงาน

๑. ผู้อำนวยการสำนักงานอธิการบดี		ประธานกรรมการ
๒. รองคณบดีคณะวิทยาศาสตร์ ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๓. รองคณบดีคณะเกษตรและชีวภาพ ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๔. รองคณบดีคณะวิทยาการจัดการ ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๕. รองคณบดีคณะมนุษยศาสตร์และสังคมศาสตร์ ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๖. รองคณบดีคณะศึกษาศาสตร์ ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๗. รองคณบดีวิทยาลัยการแพทย์ทางเลือก ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๘. รองผู้อำนวยการศูนย์การศึกษามหาวิทยาลัยราชภัฏจันทรเกษม-ชัยนาท ที่กำกับดูแลงานด้านวิชาการ		กรรมการ
๙. ผู้อำนวยการกองพัฒนานักศึกษา		กรรมการ
๑๐. ผู้อำนวยการกองคลัง		กรรมการ
๑๑. ผู้อำนวยการกองกลาง		กรรมการ
๑๒. หัวหน้าสำนักงานคณบดีคณะวิทยาศาสตร์		กรรมการ
๑๓. หัวหน้าสำนักงานคณบดีคณะเกษตรและชีวภาพ		กรรมการ
๑๔. หัวหน้าสำนักงานคณบดีคณะวิทยาการจัดการ		กรรมการ
๑๕. หัวหน้าสำนักงานคณบดีคณะมนุษยศาสตร์และสังคมศาสตร์		กรรมการ
๑๖. หัวหน้าสำนักงานคณบดีคณะศึกษาศาสตร์		กรรมการ
๑๗. หัวหน้าสำนักงานคณบดีวิทยาลัยการแพทย์ทางเลือก		กรรมการ
๑๘. หัวหน้าสำนักงานผู้อำนวยการศูนย์การศึกษา มหาวิทยาลัยราชภัฏจันทรเกษม-ชัยนาท		กรรมการ
๑๙. นายพัชร	ไวกสิกรรม	กรรมการ
๒๐. นายสมบูรณ์	ฟักอ่อน	กรรมการ
๒๑. นางสาววรรณเศรษฐ์	สวัสดิ์ถาวร	กรรมการ
๒๒. นางสาวดวงฤดี	พรมขวัญ	กรรมการ
๒๓. นายบุญช่วย	แก้วศรี	กรรมการ
๒๔. นายกฤษฎา	พูลยรัตน์	กรรมการ
๒๕. นางสาวปราณี	จิตรเย็น	กรรมการ
๒๖. นายจิรวุฒิ	เชยกลิ่น	กรรมการ
๒๗. นางสาวพัชรี	สำเภาทอง	กรรมการ
๒๘. ผู้อำนวยการกองบริหารงานบุคคล		กรรมการและเลขานุการ
๒๙. นางสาวรัตนาภรณ์	ผานิจ	ผู้ช่วยเลขานุการ
๓๐. นางสาวกุลพัชร	พูลเกษม	ผู้ช่วยเลขานุการ

อำนาจหน้าที่
๑. กำหนดมาตรการ แนวทางการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
๒. ให้คำแนะนำและความรู้ในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
๓. ตรวจสอบการดำเนินงานของมหาวิทยาลัย การดูแลรักษาข้อมูล จัดเก็บรวบรวม การใช้ข้อมูล หรือเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒
๔. รายงานผลและประเมินผลการดำเนินงานตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

สั่ง ณ วันที่ ๓๖ พฤษภาคม พ.ศ. ๒๕๖๕

(ผู้ช่วยศาสตราจารย์ราเชนทร์ เหมือนชอบ)
อธิการบดีมหาวิทยาลัยราชภัฏจันทรเกษม

.../ ๑๙. นายพัชร

แบบฟอร์มแต่งตั้งคณะทำงาน

(ร่างคำสั่งแต่งตั้งคณะกรรมการ)

คำสั่งมหาวิทยาลัยราชภัฏสกลนคร ที่ / 2569 เรื่อง แต่งตั้งคณะกรรมการดำเนินงาน และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏสกลนคร

ด้วย มหาวิทยาลัยราชภัฏสกลนคร ได้ดำเนินงานเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย และสอดคล้องกับกฎหมายที่เกี่ยวข้อง

อาศัยอำนาจตามความในมาตรา 31 แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. 2547 และมาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มหาวิทยาลัยจึงให้ยกเลิกคำสั่งเดิมที่เกี่ยวข้อง และแต่งตั้งคณะกรรมการดำเนินงาน และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. ผู้บริหารคุ้มครองข้อมูลส่วนบุคคล

- **รองอธิการบดี ฝ่ายบริหาร**
- **อำนาจหน้าที่:**
    - กำหนดทิศทางและเป็นที่ปรึกษาในการดำเนินงานการคุ้มครองข้อมูลส่วนบุคคล
    - กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล
    - พิจารณากำหนดแนวทางและวิธีการประเมินความเสี่ยง เกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่สามารถยอมรับได้
    - พิจารณาผลการประเมินความเสี่ยง
    - พิจารณาและรับรองการดำเนินการตามมาตรการคุ้มครองข้อมูลส่วนบุคคล
    - ให้การสนับสนุนการดำเนินงาน กำกับ ควบคุมและดูแลการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏสกลนคร

2. คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

1. **รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ** — ประธานกรรมการ
2. **รองผู้อำนวยการฝ่ายบริหาร สำนักส่งเสริมวิชาการและงานทะเบียน** — กรรมการ
3. **(ชื่อ-นามสกุล)** — กรรมการ

- **อำนาจหน้าที่:**
    - ให้คำแนะนำและความรู้ในการปฏิบัติตามข้อกำหนดสำคัญต่างๆ เกี่ยวกับ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แก่ผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูล และเจ้าหน้าที่ที่เกี่ยวข้อง
    - ตรวจสอบการดำเนินงานของมหาวิทยาลัยในการเข้าถึงและดูแลข้อมูลส่วนบุคคลต่างๆ ให้เป็นไปอย่างถูกต้องตามกฎหมาย
    - ประสานงานกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ในกรณีเกิดปัญหาการใช้ พรบ. คุ้มครองข้อมูลส่วนบุคคลในมหาวิทยาลัย
    - ดูแลการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลขององค์กรและบุคลากรให้สอดคล้องตามกฎหมาย
    - ไกล่เกลี่ยข้อพิพาทต่างๆ ในเบื้องต้นกับเจ้าของข้อมูลส่วนบุคคล กรณีเกิดการร้องเรียน
    - รักษาความลับของข้อมูลส่วนบุคคลจากการปฏิบัติหน้าที่

3. คณะกรรมการดำเนินงาน

1. **ผู้อำนวยการสำนักงานอธิการบดี** — ประธานกรรมการ
2. **รองคณบดีคณะต่าง ๆ (ระบุชื่อคณะ)** — กรรมการ
3. **ผู้อำนวยการกองพัฒนานักศึกษา / กองคลัง / กองกลาง** — กรรมการ
4. **หัวหน้าสำนักงานคณบดีทุกคณะ** — กรรมการ
5. **ผู้อำนวยการกองบริหารงานบุคคล** — กรรมการและเลขานุการ
6. **(ชื่อ-นามสกุล)** — ผู้ช่วยเลขานุการ

- **อำนาจหน้าที่:**

กิจกรรมที่ 1: เรื่อง การแต่งตั้งคณะทำงานการคุ้มครองข้อมูลส่วนบุคคล

แบ่งกลุ่ม
โจทย์: ให้คนในกลุ่มช่วยกันพิจารณาแต่งตั้ง
“คณะทำงานการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย”
จากคนในห้องนี้...

1. กำหนดโครงสร้างของคณะทำงาน (เริ่มตั้งแต่ประธานคณะ)
2. กำหนดชื่อตำแหน่ง (หรือพร้อมชื่อบุคคล) ลงในโครงสร้าง
3. อธิบายเหตุผลความเหมาะสมของแต่ละตำแหน่งในโครงสร้าง

โดยต้องอยู่บนหลักกฎหมาย คือ

1. DPO ต้องมีความรู้ หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 41 วรรค 6)
2. DPO หากมีหน้าที่อื่น ต้องไม่ขัดหรือแย้งกับหน้าที่ตามกฎหมาย (มาตรา 42 วรรค 4)
3. DPO ต้องมีเวลาทำงานตามหน้าที่ ที่กฎหมายกำหนด (มาตรา 41 วรรค 1)
4. สามารถแต่งตั้ง DPO สัญญาจ้างได้ (มาตรา 41 วรรค7)

ใช้เวลา 10 นาที อธิบายเหตุผล 2 นาที


ANY QUESTIONS?

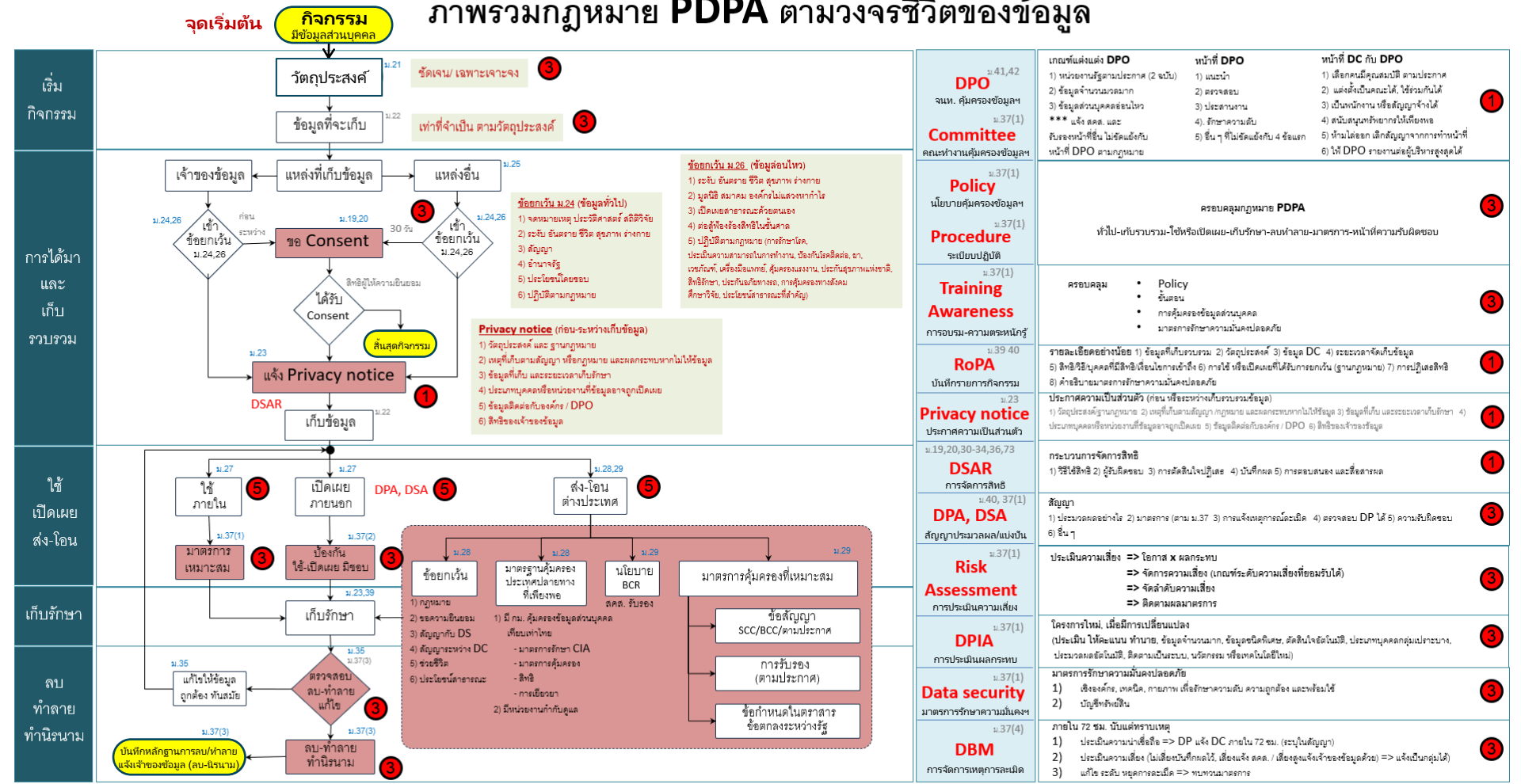
ประกาศความเป็นส่วนตัว

PRIVACY NOTICE

มาตรา 23,25

ทุกระดับ และผู้ปฏิบัติงานต้องทราบ

ภาพรวมกฎหมาย PDPA ตามวงจรชีวิตของข้อมูล



ภาพรวม Privacy Notice (ประกาศความเป็นส่วนตัว)

DC
ตัวแทน

คืออะไร?

- กฎหมายบังคับ (ม.23)
- แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ

รายละเอียดที่ต้องแจ้ง มี 6 ข้อ

1. วัตถุประสงค์ รวมถึงฐานกฎหมาย
2. เหตุที่ต้องเก็บตามกฎหมาย หรือสัญญา และผลกระทบหากไม่ให้ข้อมูล
3. ข้อมูลที่จะเก็บ และระยะเวลาเก็บรักษา
4. ประเภทของบุคคล หรือหน่วยงานที่อาจได้รับการเปิดเผย
5. วิธีการติดต่อ สถานที่ติดต่อ DC, ตัวแทนม DPO
6. สิทธิของเจ้าของข้อมูล (ดูตารางสิทธิ)

ตัวอย่าง ประกาศ

แจ้งเมื่อไร?

- **ก่อนเก็บข้อมูล**
- **ขณะเก็บข้อมูล**

เว้นแต่
ทราบรายละเอียดก่อนแล้ว

เก็บแหล่งอื่น
- **แจ้งใน 30 วัน**
- **แจ้งในครั้งแรก** ที่ติดต่อกับ DS
- **แจ้งก่อนเปิดเผย** ในครั้งแรก

แจ้งที่ไหน?

- **จุดที่เก็บข้อมูลจากเจ้าของข้อมูล หรือจุดที่เจ้าของ**

เช่น
- ทางเข้าพื้นที่
- เว็บไซต์
- แอปพลิเคชั่น
- จุดติดต่อสมัครงาน
- ห้องประชุม
- ห้องอบรม
- โทรศัพท์

แจ้งอย่างไร?

- กระดาษ
- QR Code
- หน้าเว็บไซต์
- หน้าแอปพลิเคชั่น
- โทรศัพท์

แจ้ง

- เจ้าของข้อมูล
- ผู้มีสิทธิตามกฎหมาย
- ผู้ปกครอง (ผีเยาว์)
- ผู้อนุบาล (ผีไร้คยามสามารถ)
- ผู้พิทักษ์ (ผู้เสมือนไร้ความสามารถ)

ใครแจ้ง?

ผู้ปฏิบัติงานหน้าที่เก็บข้อมูล
(จป., แผนกต้อนรับ, HR รับสมัครงาน รปภ., Sale, Marketing)

ทำไมต้องแจ้ง?

มีโทษทางปกครอง
ปรับไม่เกิน 1 ล้านบาท

เก็บจากแหล่งอื่น
ไม่แจ้งใน 30วัน
ปรับไม่เกิน 1 ล้านบาท

เก็บโดยไม่มีฐานกฎหมาย
และไม่ขอความยินยอม
ปรับไม่เกิน 3 ล้านบาท

ตัวอย่างประกาศ

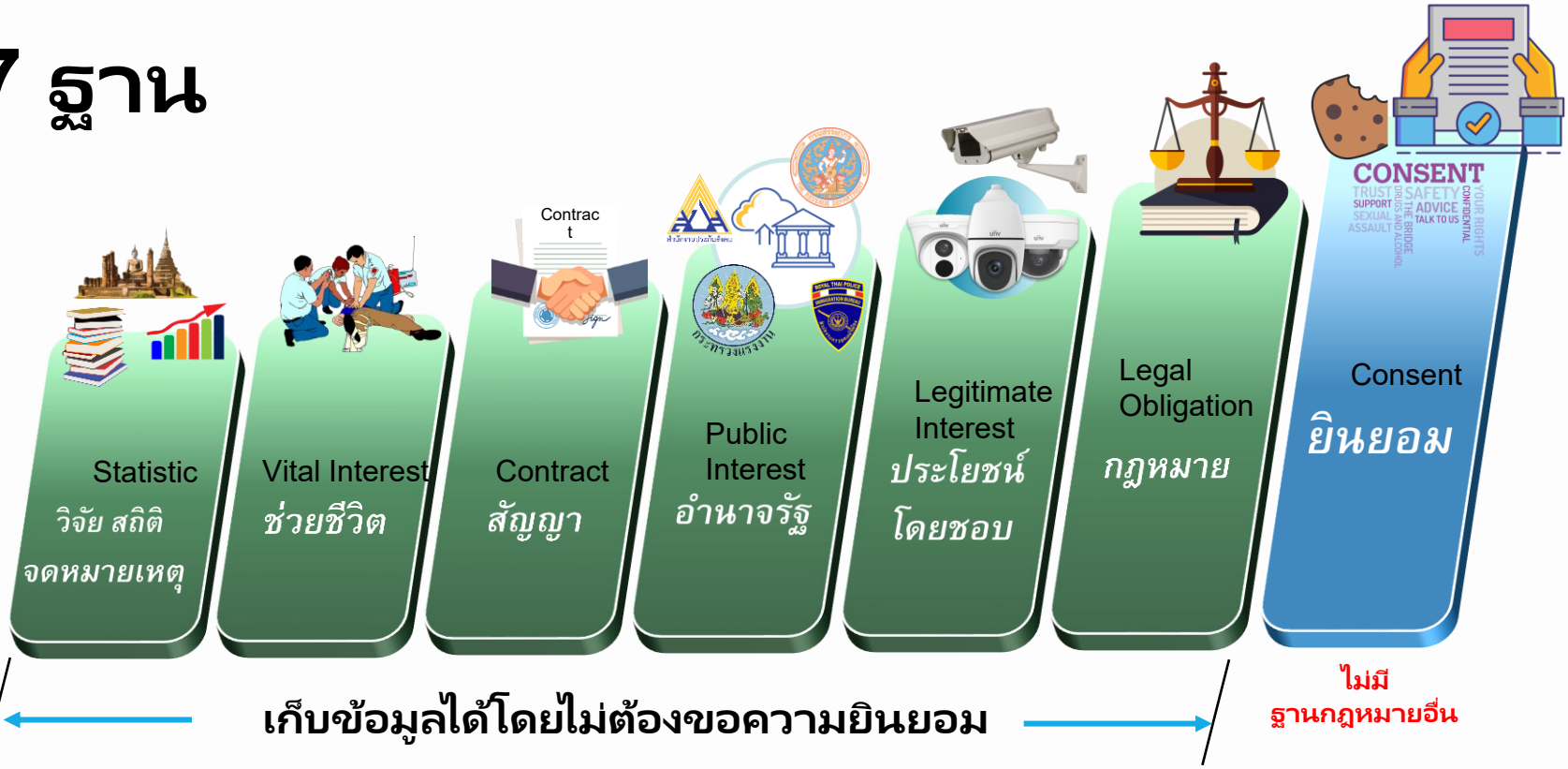
วัตถุประสงค์ต้องเฉพาะเจาะจง

ถูกต้อง (ชัดเจน เฉพาะเจาะจง)	ไม่ถูกต้อง (ไม่ชัดเจน ไม่เฉพาะเจาะจง)
1. ใช้ข้อมูลเพื่อยืนยันตัวตนในการสร้างบัญชีผู้ใช้งาน และจัดส่งข้อมูลเข้าสู่ระบบ	**1.** ใช้ข้อมูลของคุณสำหรับการยืนยันตัวตน และการให้บริการในอนาคต
2. ส่งอีเมลโปรโมชั่นและข้อเสนอพิเศษสำหรับผลิตภัณฑ์ที่เกี่ยวข้องกับความสนใจของผู้ใช้งาน	**2.** ใช้ข้อมูลเพื่อส่งอีเมลที่เกี่ยวข้องกับโปรโมชั่น หรือข้อมูลใดๆ ที่เราคิดว่าเหมาะสม
3. วิเคราะห์ข้อมูลการใช้งานเว็บไซต์เพื่อปรับปรุงประสบการณ์ของผู้ใช้งาน	**3.** รวบรวมข้อมูลทุกประเภทของคุณเพื่อพัฒนาบริการ
4. ใช้ข้อมูลเพื่อประเมินคุณสมบัติของผู้สมัครงาน และติดต่อกลับสำหรับการสัมภาษณ์	**4.** ใช้ข้อมูลของคุณเพื่อวัตถุประสงค์ในการจ้างงาน และกิจกรรมที่เกี่ยวข้องทั้งหมด
5. จัดเก็บข้อมูลเพื่อออกใบแจ้งหนี้และดำเนินการชำระเงินตามเงื่อนไขของสัญญา	**5.** เก็บข้อมูลสำหรับออกใบแจ้งหนี้ และอาจใช้เพื่อวัตถุประสงค์ทางธุรกิจในอนาคต

ฐานกฎหมายข้อมูลทั่วไป (มาตรา 24)

ไม่ใช่: เชื้อชาติ, ศาสนา, การเมือง, รสนิยมทางเพศ, ชีวภาพ, ประวัติอาชญากรรม, สุขภาพ, ความพิการ, พันธุกรรม, สหภาพแรงงาน

7 ฐาน



ฐานกฎหมายข้อมูลอ่อนไหว (มาตรา 26)

เชื้อชาติ, ศาสนา, การเมือง, รสนิยมทางเพศ, ชีวภาพ, ประวัติอาชญากรรม, สุขภาพ, ความพิการ, พันธุกรรม, สหภาพแรงงาน, อื่นๆ

ประโยชน์สาธารณะที่สำคัญ

การศึกษาวิจัย

วิทยาศาสตร์ ประวัติศาสตร์ สถิติ ประโยชน์สาธารณะอื่น
เพื่อบรรลุวัตถุประสงค์เท่าที่จำเป็น
จัดมาตรการที่เหมาะสม คุ้มครองสิทธิ, ประโยชน์

การคุ้มครองแรงงาน, ประกันสังคม

หลักประกันสุขภาพแห่งชาติ, สวัสดิการ
รักษาพยาบาลผู้มีสิทธิการรักษาตาม กม.
การคุ้มครองผู้ประกันภัยจากรถ
การคุ้มครองทางสังคม
จัดมาตรการที่เหมาะสม คุ้มครองสิทธิ, ประโยชน์

ประโยชน์สาธารณะด้านสาธารณสุข

การป้องกันโรคติดต่อ ควบคุมมาตรฐาน หรือ
คุณภาพยา เวชภัณฑ์ เครื่องมือแพทย์
จัดมาตรการที่เหมาะสม โดยเฉพาะการรักษาความลับ

เวชศาสตร์ป้องกัน อาชีวเวชศาสตร์

ประเมินความสามารถในการทำงาน
วินิจฉัยโรค รักษาโรค จัดการด้านสุขภาพ บริการสังคมสงเคราะห์
ปฏิบัติตามสัญญาระหว่าง DS กับผู้ประกอบวิชาชีพทางการแพทย์

ระงับหรือป้องกันอันตรายต่อชีวิต ร่างกาย สุขภาพ

DS ไม่สามารถให้ความยินยอมได้

มูลนิธิ, สมาคม, องค์กรไม่แสวงหากำไร

การเมือง,ศาสนา,ปรัชญา, สหภาพแรงงาน
มีการคุ้มครอง, ไม่เปิดเผยข้อมูลไปภายนอก
จัดมาตรการคุ้มครองเหมาะสม

เปิดเผยต่อสาธารณะ

ด้วยความยินยอมโดยชัดแจ้งของ DS

การก่อตั้ง ปฏิบัติ ใช้สิทธิเรียกร้อง ต่อสู้ในชั้นศาล

ตามกฎหมาย

ประกาศความเป็นส่วนตัว (Privacy notice) **คืออะไร?**

POLICY & NOTICE

Privacy *Policy* กับ Privacy *Notice* ต่างกันอย่างไร?

PART 2

ข้อแตกต่าง	PRIVACY POLICY นโยบายการคุ้มครองข้อมูลส่วนบุคคล	PRIVACY NOTICE ประกาศความเป็นส่วนตัว
สภาพบังคับทางกฎหมาย	กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)	กฎหมายกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้ง ตามมาตรา 23
ขอบเขต	เป็นเอกสารที่สื่อสารถึงบุคคลภายในองค์กร	เป็นประกาศที่มีผลเฉพาะเจ้าของข้อมูลส่วนบุคคลเท่านั้น
เนื้อหา	เป็นนโยบายและแนวปฏิบัติขององค์กรในการคุ้มครองข้อมูลส่วนบุคคล	เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเงื่อนไขเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

หมายเหตุ : Privacy policy อาจจะครอบคลุม Privacy notice ได้ โดยพิจารณาเนื้อหาภายใน หากครบถ้วนตามที่กฎหมายกำหนด ก็จะถือว่ามีการแจ้งวัตถุประสงค์ ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

No.10
V4

แจ้งรายละเอียด **อะไรบ้าง?**

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง

ประกาศความเป็นส่วนตัว สำหรับ...ลูกความ....

วัตถุประสงค์	ให้คำปรึกษาทางกฎหมาย	
ข้อมูลส่วนบุคคล	**ข้อมูลทั่วไป** - ชื่อ นามสกุล - หมายเลขโทรศัพท์ - เลขบัตร - อีเมล - ที่อยู่ - ข้อมูลเกี่ยวกับคดี บริษัทชน	**ข้อมูลอ่อนไหว** - ประวัติสุขภาพ
ฐานกฎหมาย (ตาม ม.24, 26)	การปฏิบัติตามสัญญา, การปฏิบัติตาม กฎหมาย	ขอความยินยอม
ระยะเวลาจัดเก็บ (หรือระยะเวลาที่คาดหมายได้ตามมาตรฐานการจัดเก็บ)	คลอดระยะเวลาการดำเนินคดี หรือระยะเวลาที่กฎหมายกำหนด หลังจากนั้นจะดำเนินการลบหรือทำลาย	
เหตุที่ต้องเก็บตามกฎหมาย หรือสัญญาใด (ตามกฎหมาย หรือสัญญา)	ข้อมูล การปฏิบัติตามกฎหมาย และสัญญา	
ผลกระทบ หากไม่ให้ข้อมูล	ไม่สามารถให้คำปรึกษาทางกฎหมายได้อย่าง	
ประเภทบุคคล หรือหน่วยงาน ที่ข้อมูลอาจถูกเปิดเผย	ครบถ้วน ศาล, ทนายความร่วมคดี, หน่วยงานรัฐ	

ตัวอย่าง

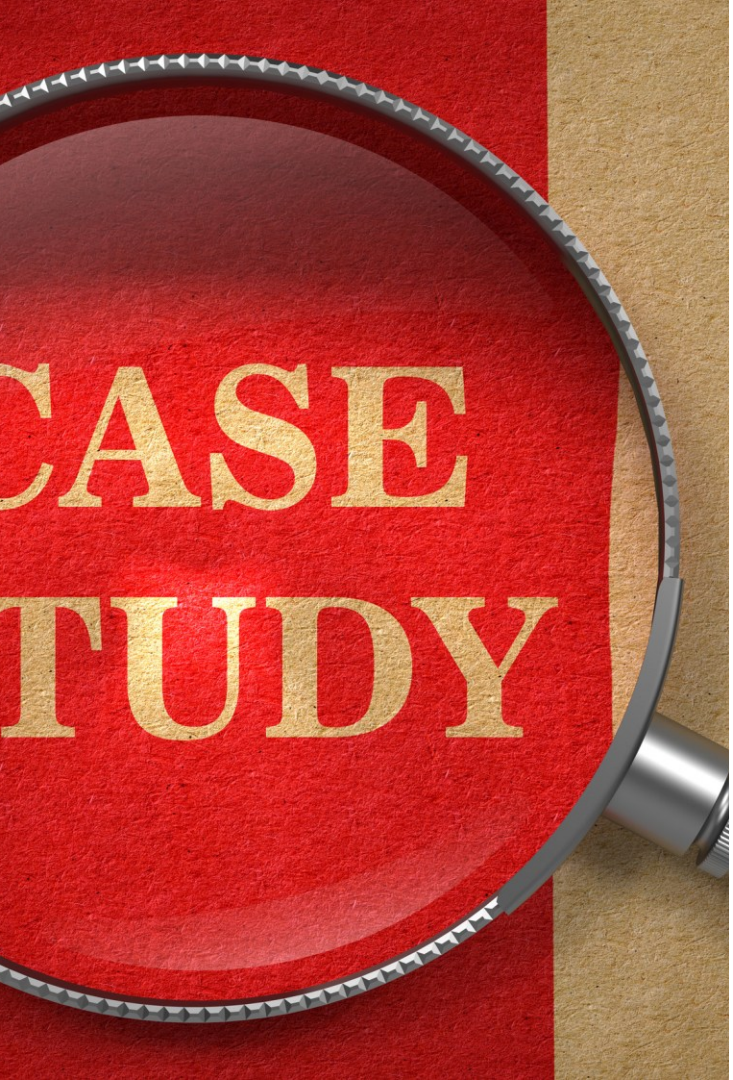
ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล	**สถานที่ติดต่อ**	**วิธีการติดต่อ**
ผู้ควบคุมข้อมูล (DC)	123/234 ม. 12 ต.....	Tel no. xxxxxxxxxx
ตัวแทนผู้ควบคุมข้อมูล (ตัวแทน DC)	-	-
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	-	-

	สิทธิ	**มี**	**ไม่มี**
สิทธิของเจ้าของข้อมูลส่วนบุคคล (ตามมาตรา 19, 30 34,36,73)	ถอนความยินยอม (เมื่อใดก็ได้)	มี	
	ขอเข้าถึง, รับสำเนา, ทราบการได้มา (แหล่งอื่น)	มี	
	โอนข้อมูล (กรณีทำได้โดยอัตโนมัติ)		ไม่มี
	คัดค้าน (เก็บ ใช้ หรือเปิดเผย)	มี	
	ขอลบ ทำลาย ทำให้เป็นข้อมูลนิรนาม	มี	
	ระงับการใช้ หรือเปิดเผย	มี	
	ขอแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน	มี	
	ร้องเรียนกับหน่วยงานกำกับดูแล (สคส.)	มี	

ช่องทางการสื่อสาร Privacy notice

- เหมาะสมกับเจ้าของข้อมูล
- สามารถเข้าถึงง่าย
- เข้าถึงได้ในทันที

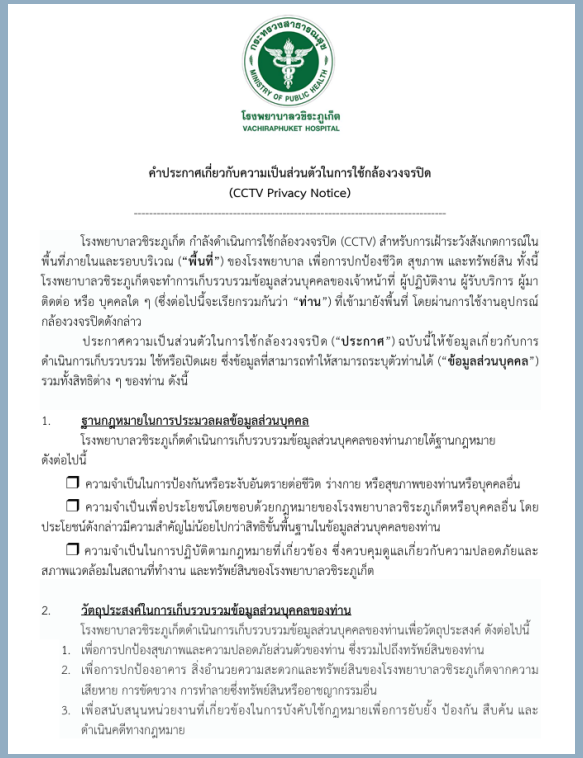
ถูกคน-ถูกที่-ถูกเวลา



ตัวอย่าง การประยุกต์ใช้ Privacy Notice

ตัวอย่างการแจ้ง Privacy notice แบบกระดาษ

กระดาษ



โรงพยาบาลวชิระภูเก็ต
VACHIRAPHUKET HOSPITAL

คำประกาศเกี่ยวกับความเป็นส่วนตัวในการใช้กล้องวงจรปิด
(CCTV Privacy Notice)

โรงพยาบาลวชิระภูเก็ต กำลังดำเนินการใช้กล้องวงจรปิด (CCTV) สำหรับการเฝ้าระวังสังเกตการณ์ในพื้นที่ภายในและรอบบริเวณ (**"พื้นที่"**) ของโรงพยาบาล เพื่อการปกป้องชีวิต สุขภาพ และทรัพย์สิน ทั้งนี้ โรงพยาบาลวชิระภูเก็ตจะทำการเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าหน้าที่ ผู้ปฏิบัติงาน ผู้รับบริการ ผู้มาติดต่อ หรือ บุคคลใด ๆ (ซึ่งต่อไปนี้จะเรียกรวมกันว่า **"ท่าน"**) ที่เข้ามายังพื้นที่ โดยผ่านการใช้งานอุปกรณ์กล้องวงจรปิดดังกล่าว

ประกาศความเป็นส่วนตัวในการใช้กล้องวงจรปิด (**"ประกาศ"**) ฉบับนี้ให้ข้อมูลเกี่ยวกับการดำเนินการเก็บรวบรวม ใช้หรือเปิดเผย ซึ่งข้อมูลที่สามารถทำให้สามารถระบุตัวท่านได้ (**"ข้อมูลส่วนบุคคล"**) รวมทั้งสิทธิต่าง ๆ ของท่าน ดังนี้

1. **ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล**
โรงพยาบาลวชิระภูเก็ตดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านภายใต้ฐานกฎหมายดังต่อไปนี้
   - ❒ ความจำเป็นในการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของท่านหรือบุคคลอื่น
   - ❒ ความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของโรงพยาบาลวชิระภูเก็ตหรือบุคคลอื่น โดยประโยชน์ดังกล่าวมีความสำคัญไม่น้อยไปกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของท่าน
   - ❒ ความจำเป็นในการปฏิบัติตามกฎหมายที่เกี่ยวข้อง ซึ่งควบคุมดูแลเกี่ยวกับความปลอดภัยและสภาพแวดล้อมในสถานที่ทำงาน และทรัพย์สินของโรงพยาบาลวชิระภูเก็ต

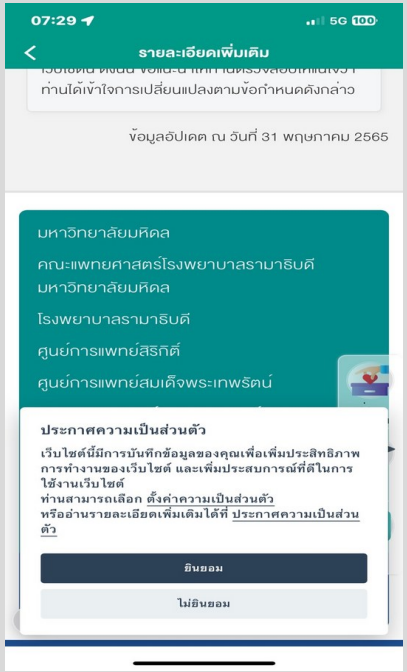
2. **วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน**
โรงพยาบาลวชิระภูเก็ตดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ ดังต่อไปนี้
   1. เพื่อการปกป้องสุขภาพและความปลอดภัยส่วนตัวของท่าน ซึ่งรวมไปถึงทรัพย์สินของท่าน
   2. เพื่อการปกป้องอาคาร สิ่งอำนวยความสะดวกและทรัพย์สินของโรงพยาบาลวชิระภูเก็ตจากความเสียหาย การขัดขวาง การทำลายซึ่งทรัพย์สินหรืออาชญากรรมอื่น
   3. เพื่อสนับสนุนหน่วยงานที่เกี่ยวข้องในการบังคับใช้กฎหมายเพื่อการยับยั้ง ป้องกัน สืบค้น และดำเนินคดีทางกฎหมาย

ป้ายประกาศ

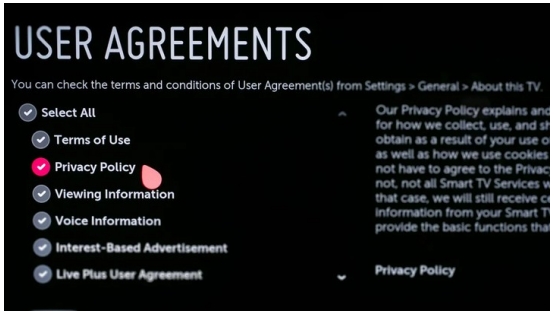
ตัวอย่างการแจ้ง Privacy notice แบบอิเล็กทรอนิกส์

เว็บไซต์

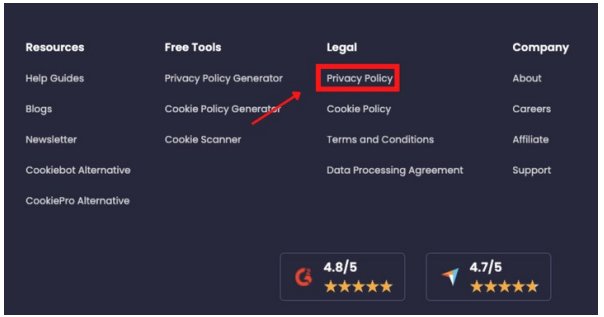
แอปพลิเคชัน



TV



Copy machine



ตัวอย่างการแจ้ง Privacy notice แบบวาจา

ผู้ปฏิบัติงานโดยตรง

ติดต่อธุรกิจ
ติดต่อที่พัก

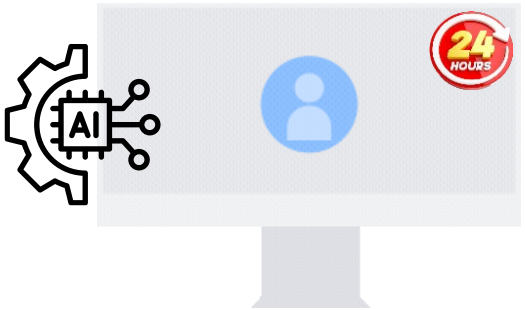
สมัครงาน

การฝึกอบรม

Operators

ธนาคาร
โทรคมนาคม
โรงพยาบาล
โรงแรม
ประกัน
ขนส่ง
หน่วยงานรัฐ

ระบบตอบรับอัตโนมัติ



AI

เก็บข้อมูลจากแหล่งอื่น

มาตรา ๒๕ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา ๒๑ และการแจ้งรายละเอียดตามมาตรา ๒๓ มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

ต้องแจ้ง

สถานการณ์	ประเภทการใช้ข้อมูล
ใช้ข้อมูลเพื่อการตลาด	Marketing / Direct Contact
ใช้ข้อมูลเพื่อเสนอบริการ	Business Development
ได้ข้อมูลจากบริษัทอื่น	Data Sharing ระหว่างองค์กร
ทำ Legal Advisory	Legal Consulting

ไม่ต้องแจ้ง

สถานการณ์	เหตุผลตามกฎหมาย	มาตรา PDPA
ข้อมูลในสำนวนคดี	เจ้าของข้อมูลทราบอยู่แล้ว	มาตรา 25(1)
เตรียมฟ้องคดี	การแจ้งเป็นอุปสรรคต่อการดำเนินคดี	มาตรา 25(2)
ยื่นหลักฐานต่อศาล	กฎหมายกำหนดให้เปิดเผย	มาตรา 25(3)
ข้อมูลจากลูกความ	ความลับวิชาชีพทนาย	มาตรา 25(4)

(๑) เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่หรือรายละเอียดนั้นอยู่แล้ว

(๒) ผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดดังกล่าวไม่สามารถทำได้หรือจะเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ในกรณีนี้ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๓) การใช้หรือการเปิดเผยข้อมูลส่วนบุคคลต้องกระทำโดยเร่งด่วนตามที่กฎหมายกำหนด ซึ่งได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(๔) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ซึ่งล่วงรู้หรือได้มาซึ่งข้อมูลส่วนบุคคลจากหน้าที่หรือจากการประกอบอาชีพหรือวิชาชีพและต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดบางประการตามมาตรา ๒๓ ไว้เป็นความลับตามที่กฎหมายกำหนด

การแจ้งรายละเอียดตามวรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบภายในสามสิบวันนับแต่วันที่เก็บรวบรวมตามมาตรานี้ เว้นแต่กรณีที่นำข้อมูลส่วนบุคคลไปใช้เพื่อการติดต่อกับเจ้าของข้อมูลส่วนบุคคลต้องแจ้งในการติดต่อครั้งแรก และกรณีที่จะนำข้อมูลส่วนบุคคลไปเปิดเผย ต้องแจ้งก่อนที่จะนำข้อมูลส่วนบุคคลไปเปิดเผยเป็นครั้งแรก

PDPA สำหรับทนายความ

ข้อยกเว้นเก็บจากแหล่งอื่น.....อะไรทำได้ – ทำไม่ได้

✓ ทำได้ (ข้อยกเว้น)

1) **เจ้าของข้อมูลรู้อยู่แล้ว**
เช่น คำฟ้อง, พยาน, คู่สัญญา, คู่ความ

2) **แจ้งไม่ได้ / เป็นอุปสรรค**
เช่น คดีแชร์ลูกโซ่, วิเคราะห์ข้อมูลจำนวนมาก

3) **กฎหมายกำหนดให้เปิดเผย**
เช่น ศาลสั่ง, พนักงานสอบสวน

4) **ความลับวิชาชีพทนาย**
ข้อมูลจากลูกความ → ต้องเก็บเป็นความลับ

✗ ห้ามทำ (ผิด-เสี่ยง)

✗ **ใช้ข้อมูลคู่ความ**
→ ทำการตลาด

เปิดเผยข้อมูลลูกความ
→ โดยไม่ได้รับอนุญาต

✗ **ใช้ข้อมูลเกิน**
→ วัตถุประสงค์ของคดี

✗ **เก็บข้อมูล**
→ ไม่ปลอดภัย

Checklist ก่อนใช้ข้อมูล

1. เกี่ยวกับคดี? 2. เจ้าของข้อมูลรู้แล้ว? 3. กฎหมายกำหนด? 4. เป็นความลับ?

Tip: กฎหมายไม่ได้ห้ามเก็บ หรือใช้ข้อมูล แต่ให้ใช้ถูกต้อง และปลอดภัย

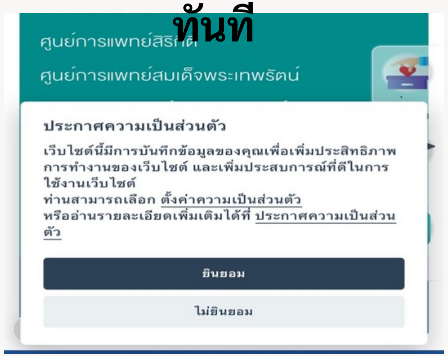
ตัวอย่างการแจ้ง Privacy notice ที่ดี

แบ่งตามประเภท DS

ตัวอย่าง

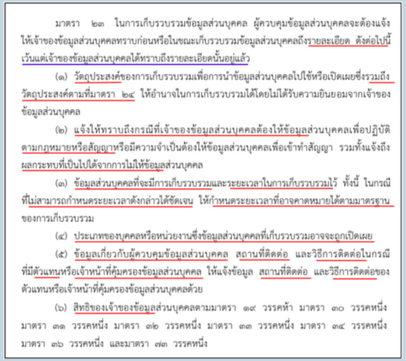
เข้าถึงง่าย

มีลิงค์หาง่าย อ่านได้ทันที



ภาษาตามกลุ่ม DS

รายละเอียดครบ



มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง

เนื้อหา จำนวนหน้าไม่มากเกินไป

ประกาศความเป็นส่วนตัว สำหรับ...............			
วัตถุประสงค์			
ข้อมูลส่วนบุคคล	ข้อมูลทั่วไป	ข้อมูลอ่อนไหว	
ฐานกฎหมาย (ตาม ม.24, 26)			
ระยะเวลาจัดเก็บ (หรือระยะเวลาที่คาดหมายได้ตามมาตรฐานการจัดเก็บ)			
เหตุที่ต้องเก็บตามกฎหมาย หรือสัญญาใด (ตามกฎหมาย หรือสัญญา)			
ผลกระทบ หากไม่ให้ข้อมูล			
ประเภทบุคคล หรือหน่วยงาน ที่ข้อมูลอาจถูกเปิดเผย			
ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล	สถานที่ติดต่อ	วิธีการติดต่อ	
ผู้ควบคุมข้อมูล (DC)			
ตัวแทนผู้ควบคุมข้อมูล (ตัวแทน DC)			
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)			
สิทธิของเจ้าของข้อมูลส่วนบุคคล (ตามมาตรา 19, 30-34,36,73)	สิทธิ	มี	ไม่มี
	ถอนความยินยอม (เมื่อใดก็ได้)		
	ขอเข้าถึง, รับสำเนา, ทราบการได้มา (แหล่งอื่น)		
	โอนข้อมูล (กรณีทำได้โดยอัตโนมัติ)		
	คัดค้าน (เก็บ ใช้ หรือเปิดเผย)		
	ขอลบ ทำลาย ทำให้เป็นข้อมูลนิรนาม		
	ระงับการใช้ หรือเปิดเผย		
	ขอแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน		
	ร้องเรียนกับหน่วยงานกำกับดูแล (สคส.)		

Workshop#2

จงอ่าน Privacy notice จากตัวอย่าง แล้วตอบคำถามดับต่อไปนี้

- **<u>หัวข้อ</u>** ครบถ้วนตามกฎหมายหรือไม่ ?

  (อ่านเทียบกับ ตาม ม.23 มีรายละเอียด 6 ข้อ)

- **<u>ระยะเวลา</u>** ในการเก็บรักษาข้อมูลของท่านนานเท่าไร ?

  (อ่านเนื้ออย่างละเอียดจนครบ)

- **<u>ท่านรู้สึกอย่างไร</u>** กับ Privacy notice ที่อ่าน ในฐานะ DS ?

  (แสดงว่ารู้สึกในฐานะเจ้าของข้อมูลส่วนบุคคล)

(๑) วัตถุประสงค์ของการเก็บรวบรวมเพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยซึ่งรวมถึงวัตถุประสงค์ตามที่มาตรา ๒๔ ให้อำนาจในการเก็บรวบรวมได้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมายหรือสัญญาหรือมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา รวมทั้งแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(๓) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(๔) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(๕) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

(๖) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา ๑๙ วรรคห้า มาตรา ๓๐ วรรคหนึ่ง มาตรา ๓๑ วรรคหนึ่ง มาตรา ๓๒ วรรคหนึ่ง มาตรา ๓๓ วรรคหนึ่ง มาตรา ๓๔ วรรคหนึ่ง มาตรา ๓๖ วรรคหนึ่ง และมาตรา ๗๓ วรรคหนึ่ง

ปตท.
ผู้เข้าใช้เว็บไซต์

ร.พ. รามาธิบดี
ผู้รับบริการดูแลสุขภาพ

ธ.ออมสิน
พนักงานธนาคาร

กลุ่ม ทรู คอร์ปอเรชั่น
(ทุกประเภทของ DS)

สคส.
ผู้มาติดต่อ ผู้รับบริการ

ข้อควรระวัง... สำหรับ Privacy notice

เนื้อหา

- *รายละเอียดไม่ครบ*
- *ใช้ภาษาอ่านยาก จำนวนหน้ามากเกินไป*
- *รวมประกาศฉบับเดียวในทุกกลุ่ม DS*
- *เนื้อหาแตกต่างกันในแต่ละช่องทาง*
- *ตัวหนังสือเล็กเกินไป*
- *ภาษาเจ้าของเจ้าของข้อมูล (หรือภาษาอังกฤษ)*

วิธีการ

- *หาประกาศไม่เจอ/หายาก*
  - *จุดติดตั้งสูงเกินไป หรือเข้าถึงไม่ได้*
  - *ไม่มีลิงค์ที่กดอ่านได้ทันที ต้องค้นหาเอง*
- *Scan QR code ไม่พบประกาศ/ติดโฆษณา*
- *ช่องทางแจ้ง กับการเก็บไม่สอดคล้องกับช่องทางการเก็บข้อมูล*
- *เก็บจากแหล่งอื่น ไม่แจ้งเก็บ,ไม่มีฐานกฎหมาย*

ขาดการตรวจสอบ

- *ระบบ error*
- *ผู้ปฏิบัติงาน (หลงลืม ไม่ได้แจ้ง)*
- *เสื่อมสภาพ (อ่านไม่ได้ ลอก ลบ เลือน)*
- *ขาดกิจกรรมการตรวจสอบ ทดสอบ*
- *ขาดการฝึกอบรม*
- *ไม่ได้ทำเอกสารประกาศ*
- *มีการแก้ไข ไม่ทำการปรับปรุงประกาศ*

แบบฟอร์มประกาศความเป็นส่วนตัวแบบต่าง ๆ

ประกาศความเป็นส่วนตัว (Privacy Notice) สำหรับนักศึกษา

มหาวิทยาลัยราชภัฏสกลนคร

มหาวิทยาลัยราชภัฏสกลนคร ("มหาวิทยาลัย") ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลของท่าน ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล มหาวิทยาลัยจึงขอแจ้งรายละเอียดการประมวลผลข้อมูล ดังนี้:

1. ข้อมูลส่วนบุคคลที่เราเก็บรวบรวม

มหาวิทยาลัยจะเก็บรวบรวมข้อมูลของท่านเท่าที่จำเป็น เพื่อวัตถุประสงค์ในการจัดการศึกษา:

- **ข้อมูลระบุตัวตน:** ชื่อ-นามสกุล, เลขประจำตัวประชาชน, รหัสนักศึกษา, ภาพถ่าย
- **ข้อมูลการติดต่อ:** ที่อยู่, เบอร์โทรศัพท์, อีเมล, ข้อมูลผู้ปกครอง
- **ข้อมูลการศึกษา:** ประวัติการเรียน, ผลการเรียน, เกียรติประวัติ, พฤติกรรมการเรียนผ่านระบบ LMS
- **ข้อมูลอ่อนไหว (Sensitive Data):** ศาสนา (เพื่อสวัสดิการอาหาร), ข้อมูลสุขภาพ (เพื่อการรักษาพยาบาล/กิจกรรมกีฬา), ข้อมูลความพิการ (เพื่อรับทุนหรือสิทธิประโยชน์), และข้อมูลชีวมิติ (Biometrics) เช่น ใบหน้า/ลายนิ้วมือเพื่อเข้าอาคาร

2. วัตถุประสงค์ในการประมวลผลข้อมูล

- เพื่อการรับเข้าศึกษา การลงทะเบียนเรียน และการประมวลผลการเรียน
- เพื่อการจัดสวัสดิการนักศึกษา ทุนการศึกษา และการประกันอุบัติเหตุ
- เพื่อการตรวจสอบและรักษาความปลอดภัยภายในพื้นที่มหาวิทยาลัย
- เพื่อการส่งข้อมูลให้หน่วยงานกำกับดูแล เช่น กระทรวง อว. หรือ กยศ.
- หากไม่ให้ข้อมูลจะไม่สามารถปฏิบัติตามสัญญา และข้อกำหนดทางกฎหมายที่เกี่ยวข้องได้

- 19 ประกาศความเป็นส่วนตัว สำหรับ ตัวการใช้งานกล้องวงจรปิด
- 19 ประกาศความเป็นส่วนตัว สำหรับ นักศึกษา
- 19 ประกาศความเป็นส่วนตัว สำหรับ บุคลากร
- 19 ประกาศความเป็นส่วนตัว สำหรับ ผู้เข้าร่วมกิจกรรม อบรม สัมมนา
- 19 ประกาศความเป็นส่วนตัว สำหรับ ผู้ใช้งานเว็บไซต์และระบบออนไลน์
- 19 ประกาศความเป็นส่วนตัว สำหรับ ผู้สมัครงาน
- 19 ประกาศความเป็นส่วนตัว สำหรับ สำหรับ คู่สัญญาและผู้รับจ้าง
- 19 ประกาศความเป็นส่วนตัว สำหรับ สำหรับ ผู้เข้าร่วมการวิจัย
- 19 ประกาศความเป็นส่วนตัว สำหรับ สำหรับผู้ปกครอง และผู้ติดต่อ


ANY QUESTIONS?


มาตรา 37 (1)
ระดับมหาวิทยาลัย ทุกคนต้องทราบ
Privacy Policy
Introduction
How Data is Used
Data Sharing and Transfers
Types of Data Collected
Data Sharing and Transfers
Data Security Measures
Your Rights

ประกาศความเป็นส่วนตัว (Privacy notice) **คืออะไร?**

POLICY & NOTICE

Privacy *Policy* กับ Privacy *Notice* ต่างกันอย่างไร ?

PART 2

ข้อแตกต่าง	PRIVACY POLICY นโยบายการคุ้มครองข้อมูลส่วนบุคคล	PRIVACY NOTICE ประกาศความเป็นส่วนตัว
สภาพบังคับทางกฎหมาย	กฎหมายไม่ได้กำหนดให้ต้องทำ (แต่ควรทำเพื่อประโยชน์ในการบริหารจัดการข้อมูล)	กฎหมายกำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้ง ตามมาตรา 23
ขอบเขต	เป็นเอกสารที่สื่อสารถึงบุคคลภายในองค์กร	เป็นประกาศที่มีผลเฉพาะเจ้าของข้อมูลส่วนบุคคลเท่านั้น
เนื้อหา	เป็นนโยบายและแนวปฏิบัติขององค์กรในการคุ้มครองข้อมูลส่วนบุคคล	เป็นการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบเงื่อนไขเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

หมายเหตุ : Privacy policy อาจจะครอบคลุม Privacy notice ได้ โดยพิจารณาเนื้อหาภายใน หากครบถ้วนตามที่กฎหมายกำหนด ก็จะถือว่ามีการแจ้งวัตถุประสงค์ ตามมาตรา 23 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว

No.10
V4

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

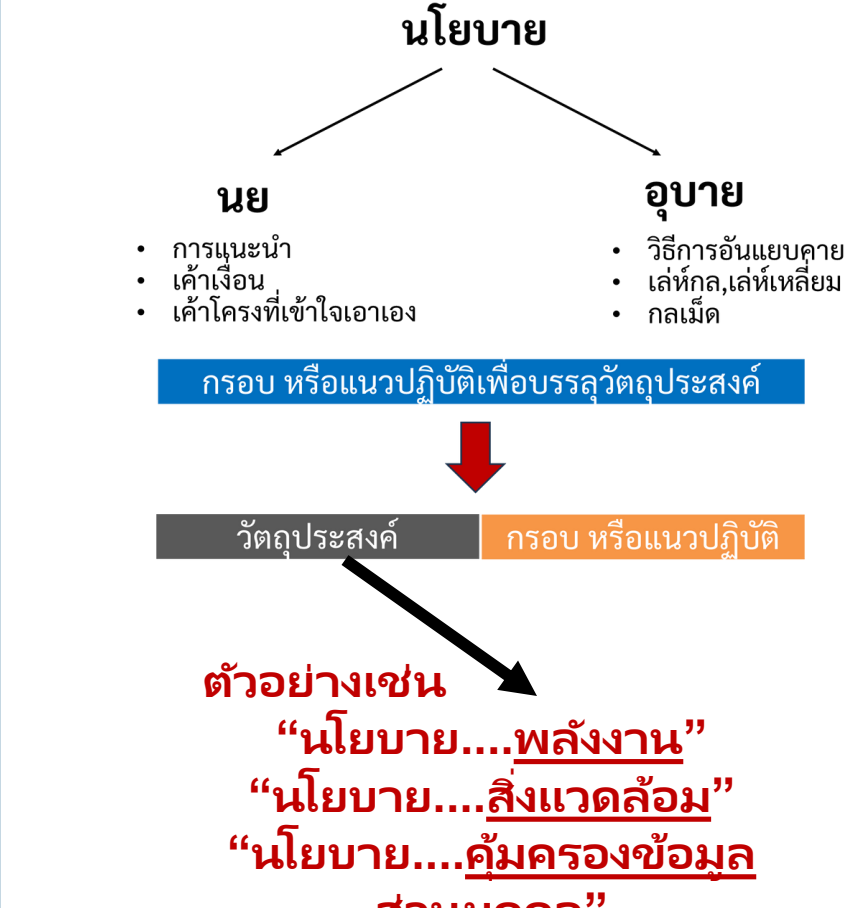
Privacy policy (นโยบายคุ้มครองข้อมูลส่วนบุคคล)

นโยบายคุ้มครองข้อมูลส่วนบุคคล

คือ

กรอบหรือแนวทางการปฏิบัติงาน
เพื่อให้บรรลุวัตถุประสงค์
“การคุ้มครองข้อมูลส่วนบุคคล” ขององค์กร

ประกาศโดยผู้บริหารสูงสุด
เพื่อให้นำไปใช้เป็นแนวทาง
หรือกรอบการปฏิบัติงานของคนในองค์กร
ภายใต้ขอบเขตความรับผิดชอบขององค์กร
เพื่อบรรลุวัตถุประสงค์นั้น



องค์ประกอบของนโยบายคุ้มครองข้อมูลส่วนบุคคล

องค์ประกอบของ นโยบายคุ้มครองข้อมูลส่วนบุคคล

องค์ประกอบหลัก

1. นำเรื่อง/อ้างอิง
2. วัตถุประสงค์
3. ขอบเขต
4. คำนิยาม
5. แนวปฏิบัติ
6. การทบทวนเปลี่ยนแปลง
7. ลงนามผู้บริหารสูงสุด

แนวปฏิบัติ

1. หลักทั่วไป
2. การเก็บรวบรวม
3. การใช้ หรือเปิดเผย
4. การส่งโอนข้อมูลส่วนบุคคล ไปต่างประเทศ
5. สิทธิของเจ้าของข้อมูลส่วนบุคคล
6. หน้าที่ขององค์กรในนามผู้ควบคุมข้อมูลส่วนบุคคล
7. หน้าที่ขององค์กรในนามผู้ประมวลผลข้อมูลส่วนบุคคล
8. หน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

ตัวอย่าง นโยบายคุ้มครองข้อมูลส่วนบุคคล

11 หน้า

องค์การสุรา
กรมสรรพสามิต
LIQUOR DISTILLERY ORGANIZATION

ประกาศองค์การสุรา กรมสรรพสามิต
เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

22 หน้า

สำนักงานส่งเสริมวิสาหกิจขนาดกลาง และขนาดย่อม

7 หน้า

ร.พ. ศิริราช

7 หน้า

สำนักงานปลัด
กระทรวงการคลัง

2 หน้า

มหาวิทยาลัย ธรรมศาสตร์

6 หน้า

มหาวิทยาลัยมหิดล

7 หน้า

กรมส่งเสริมการค้าระหว่างประเทศ

บทกำหนดโทษทางปกครอง...ประกาศความเส่วนตัว

ไม่เกิน 1 ล้านบาท

มาตรา ๘๒ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๓ มาตรา ๓๐ วรรคสี่ มาตรา ๓๙ วรรคหนึ่ง มาตรา ๔๑ วรรคหนึ่ง หรือมาตรา ๔๒ วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๙ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๙ วรรคหก หรือไม่ปฏิบัติตามมาตรา ๒๓ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา ๒๓ ในการเก็บรวบรวมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียด ดังต่อไปนี้ เว้นแต่เจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดนั้นอยู่แล้ว

ไม่เกิน 3 ล้านบาท

มาตรา ๘๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ มาตรา ๒๕ วรรคหนึ่ง มาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๘ มาตรา ๓๒ วรรคสอง หรือมาตรา ๓๗ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา ๒๑ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

มาตรา ๒๕ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้แก่เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

ให้นำบทบัญญัติเกี่ยวกับการแจ้งวัตถุประสงค์ใหม่ตามมาตรา ๒๑ และการแจ้งรายละเอียดตามมาตรา ๒๓ มาใช้บังคับกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่ต้องได้รับความยินยอมตามวรรคหนึ่งโดยอนุโลม เว้นแต่กรณีดังต่อไปนี้

บทกำหนดโทษ...ที่อาจเกี่ยวกับนโยบาย

ไม่เกิน 3 ล้านบาท

มาตรา ๘๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ มาตรา ๒๕ วรรคหนึ่ง มาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๘ มาตรา ๓๒ วรรคสอง หรือมาตรา ๓๗ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา ๒๑ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

(๒) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

ไม่มีนโยบายผิดหรือไม่?

มาตรา ๘๑ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

(๗) มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องรวมถึงการสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness) และการแจ้งนโยบาย แนวปฏิบัติ และมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเหมาะสม ให้บุคลากร พนักงาน ลูกจ้าง หรือบุคคลอื่นที่เป็นผู้ใช้งาน (user) หรือเกี่ยวข้องกับการเข้าถึง เก็บรวบรวม ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล ทราบและถือปฏิบัติ รวมทั้งกรณีที่มีการปรับปรุงแก้ไขนโยบาย แนวปฏิบัติ และมาตรการดังกล่าวด้วย โดยคำนึงถึงลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

นโยบายคุ้มครองข้อมูล => มาตรการเชิงองค์กร

นโยบายคุ้มครองข้อมูล => คำสั่งของใคร?

แบบฟอร์มนโยบายคุ้มครองข้อมูลส่วนบุคคล

นโยบายคุ้มครองข้อมูลส่วนบุคคล

(Personal Data Protection Policy)

มหาวิทยาลัยราชภัฏสกลนครยึดมั่นในการดำเนินงานตามภารกิจอย่างมีจรรยาบรรณ และเคารพในสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล โดยมีความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ที่ส่งผลกระทบต่อสิทธิและเสรีภาพต่อบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล ซึ่งมหาวิทยาลัยราชภัฏสกลนครได้ทำการประมวลผลในกิจกรรมต่างๆ ตามภารกิจที่รับผิดชอบ จึงประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคลนี้ขึ้น เพื่อให้การดำเนินงานของมหาวิทยาลัยราชภัฏสกลนครและบุคลากรทุกคน ภายใต้ขอบเขตการกำกับดูแลรับผิดชอบของมหาวิทยาลัยราชภัฏสกลนครเป็นไปอย่างโปร่งใส เป็นธรรม และถูกต้องตามกฎหมาย สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.วัตถุประสงค์

1.1 เพื่อเป็นแนวทางปฏิบัติ สำหรับการดำเนินงานทุกกิจกรรม สำหรับบุคลากรต่างๆ ภายใต้ขอบเขตการกำกับดูแลรับผิดชอบของมหาวิทยาลัยราชภัฏสกลนครที่มีการประมวลผลข้อมูลส่วนบุคคลสอดคล้อง และถูกต้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.2 เพื่อปกป้องคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายใต้ความรับผิดชอบของมหาวิทยาลัยราชภัฏสกลนคร มิให้เกิดการละเมิด สร้างความเสียหายแก่ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคลที่มหาวิทยาลัยราชภัฏสกลนครได้ทำการประมวลผลในกิจกรรมภายใต้การกำกับดูแลของมหาวิทยาลัยราชภัฏสกลนคร

2. ขอบเขต

ขอบเขตในความรับผิดชอบของมหาวิทยาลัยราชภัฏสกลนครในการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วย

2.1 ด้านกายภาพ และระบบสารสนเทศ ได้แก่ สถานที่ในการประกอบกิจการทั้งหมด รวมถึงทรัพยากรต่างๆ ในการประมวลผลข้อมูลส่วนบุคคลภายใต้กิจกรรมที่มหาวิทยาลัยราชภัฏสกลนครดำเนินการ และรับผิดชอบ ของมหาวิทยาลัยราชภัฏสกลนคร

2.2 ด้านบุคคลการ ได้แก่ บุคคลกรทุกคน ทุกระดับ ทั้งที่เป็น ผู้บริหาร เจ้าหน้าที่ พนักงาน ลูกจ้าง ผู้รับจ้างที่ทำการประมวลผลข้อมูลส่วนบุคคลตามคำสั่ง หรือทำในนามมหาวิทยาลัยราชภัฏสกลนคร

2.3 ด้านกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ได้แก่ กิจกรรมที่ประมวลผลโดยมหาวิทยาลัยราชภัฏสกลนครเอง และที่ประมวลผลโดยผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการตามคำสั่งของมหาวิทยาลัยราชภัฏสกลนคร

3. คำจำกัดความ

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ, ที่อยู่, เบอร์ติดต่อ, ตำแหน่งที่อยู่, ศาสนา, กรุ๊ปเลือด เป็นต้น

“ข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” หมายถึง ข้อมูลเฉพาะผู้ตาย ที่ไม่เชื่อมโยงเกี่ยวข้องกับบุคคลธรรมดาที่ยังมีวิตอยู่ เช่น ชื่อผู้ตาย, เบอร์ติดต่อผู้ตาย, สถานภาพของผู้ตาย เป็นต้น

“ข้อมูลส่วนบุคคลอ่อนไหว” (Sensitive data) หมายถึง ข้อมูลเกี่ยวกับเชื้อชาติ, เผ่าพันธุ์, ความคิดเห็นทางการเมือง, ความเชื่อในลัทธิ ศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสุขภาพ, ความพิการ, ข้อมูลสหภาพแรงงาน, ข้อมูลพันธุกรรม, ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“การประมวลผล” หมายถึง การดำเนินการใดๆ กับข้อมูลส่วนบุคคล เช่น การเก็บรวบรวม บันทึก จัดระบบ ทำโครงสร้าง เก็บรักษา ปรับปรุง เปลี่ยนแปลง กู้คืน ใช้ เปิดเผย ส่งต่อ เผยแพร่ โอน ผสมเข้าด้วยกัน ลบ ทำลาย การทำโปรไฟล์ลิ่ง การตัดสินใจโดยอัตโนมัติด้วยระบบปัญญาประดิษฐ์ (Artificial Intelligence, AI)

“เจ้าของข้อมูลส่วนบุคคล” (Data Subject) หมายถึง บุคคลธรรมดาซึ่งข้อมูลนั้นบ่งชี้ไปถึงทำให้สามารถระบุตัวบุคคลนั้นได้

“ผู้ควบคุมข้อมูลส่วนบุคคล” (Data Controller) หมายถึง บุคคลหรือนิติบุคคลอื่นซึ่งมีอำนาจในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” (Data Processor) หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้
บุคคลหรือนิติบุคคลที่ดำเนินการดังกล่าวไม่เป็นผู้ควบคุมคุมข้อมูลส่วนบุคคล

“การละเมิดข้อมูลส่วนบุคคล” (Data breach) หมายถึง การทำให้สูญเสียความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ของข้อมูลส่วนบุคล (Availability)

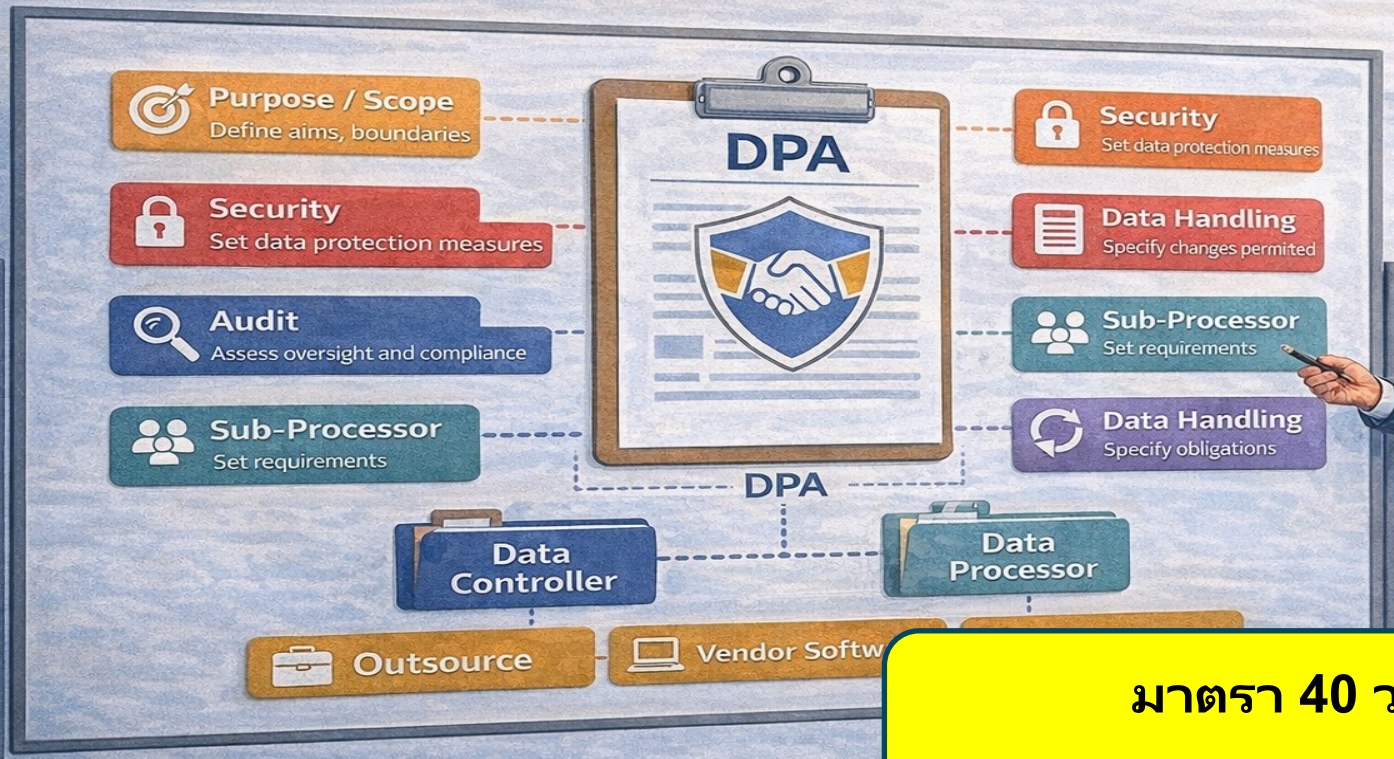
4. แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

4.1 หลักทั่วไป


ANY QUESTIONS?

Data Processing Agreement (DPA)

What is it?	Who is involved?	What is included?	Who needs it?



มาตรา 40 วรรค 3

ระดับมหาวิทยาลัย และคณะ

กฎหมาย PDPA กับ สัญญาการประมวลผล และการแบ่งปันข้อมูลส่วนบุคคล

ม. 40 ว.3

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

กม. ลำดับรอง ม.37(1)

ข้อ ๖ ในการจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลพิจารณากำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องเป็นไปตามมาตรฐานขั้นต่ำตามข้อ ๔ โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการละเมิดข้อมูลส่วนบุคคล

กม. ลำดับรอง ม.37(4)

ข้อ ๘ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือมอบหมายหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของตนเอง ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุไว้ในข้อตกลงหรือในสัญญาที่เกี่ยวข้องให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ผู้ประมวลผลข้อมูลส่วนบุคคลทราบเหตุเท่าที่จะสามารถกระทำได้เช่นกัน

กฎหมาย PDPA กับ สัญญาการประมวลผล และการแบ่งปันข้อมูลส่วนบุคคล

ม. 27 วรรค 1, 2

มาตรา ๒๗ ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา ๒๔ หรือมาตรา ๒๖

บุคคลหรือนิติบุคคลที่ได้รับข้อมูลส่วนบุคคลมาจากการเปิดเผยตามวรรคหนึ่ง จะต้องไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูลส่วนบุคคลในการขอรับข้อมูลส่วนบุคคลนั้น

ม. 37 (1),(2)

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

***** สัญญาข้อตกลง ถือเป็นมาตรการเชิงองค์กร**

ความสำคัญ และประโยชน์ของ สัญญาการประมวลผล และการแบ่งปันข้อมูลส่วนบุคคล

ส่วนที่ ๒
โทษทางปกครอง

มาตรา ๘๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ มาตรา ๒๕ วรรคหนึ่ง มาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๘ มาตรา ๓๒ วรรคสอง หรือมาตรา ๓๗ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา ๒๑ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

***** ไม่มีสัญญาข้อตกลง เป็นมาตรการ**

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

ส่วนที่ ๒
โทษทางปกครอง

มาตรา ๘๖ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๔๐ โดยไม่มีเหตุอันควร หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา ๓๗ (๕) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๓๘ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

***** ไม่มีสัญญาข้อตกลง เป็นมาตรการป้องกัน**

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

การจัดทำสัญญาการประมวลผล และการแบ่งปันข้อมูลส่วนบุคคล

หัวข้อ	NDA (Non-Disclosure Agreement)	DSA (Data Sharing Agreement)	DPA (Data Processing Agreement)
ความหมาย	ข้อตกลงไม่เปิดเผยข้อมูลระหว่างคู่สัญญา	ข้อตกลงแบ่งปันข้อมูลระหว่าง DC	ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่าง DC กับ DP
วัตถุประสงค์	ป้องกันการเปิดเผยข้อมูลลับ	กำหนดขอบเขตและความรับผิดชอบการแบ่งปันข้อมูล	กำหนดบทบาทหน้าที่ตามกฎหมาย PDPA
ความสัมพันธ์	ไม่จำเป็นต้องมีสถานะ DC หรือ DP	DC กับ DC	DC กับ DP
ความรับผิดชอบ	รักษาความลับข้อมูลตามข้อตกลง	DC ต่างกำหนดและใช้ข้อมูลตามวัตถุประสงค์ของตน	DP ประมวลผลตามคำสั่งของ DC
ตัวอย่างกิจกรรม	เปิดเผยข้อมูลให้ที่ปรึกษาภายนอก	รพ. A ส่งข้อมูลให้ รพ. B เพื่อวิเคราะห์	บริษัท outsource ประมวลผลข้อมูลลูกค้าแทน DC

การจัดทำสัญญาการประมวลผล และการแบ่งปันข้อมูลส่วนบุคคล

หลักการเขียนสัญญาทั่วไป

1. ข้อมูลของคู่สัญญา (Parties Information)
2. วัตถุประสงค์ของสัญญา (Purpose of Contract)
3. ขอบเขตของงานหรือข้อกำหนดของสัญญา (Scope of Work/Agreement Terms)
4. ระยะเวลาของสัญญา (Contract Duration)
5. ค่าตอบแทนและเงื่อนไขการชำระเงิน (Payment Terms)
6. สิทธิและหน้าที่ของแต่ละฝ่าย (Rights and Responsibilities)
7. เงื่อนไขการผิดสัญญาและบทลงโทษ (Breach of Contract & Penalty)
8. การยกเลิกสัญญา (Termination Clause)
9. ข้อกำหนดเรื่องกฎหมายที่ใช้บังคับ (Governing Law & Dispute Resolution)
10. เงื่อนไขอื่น ๆ และข้อกำหนดเพิ่มเติม (Miscellaneous Provisions)

หลักการเขียน DPA

1 ต้องประมวลผลข้อมูลตามคำสั่งของ Data Controller เท่านั้น

ระบุข้อกำหนดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลว่า DC ต้องการให้ทำอะไรกับข้อมูลได้บ้าง

2 ต้องมีมาตรการรักษาความปลอดภัยของข้อมูล (Security Measures) ที่เหมาะสม

ควรระบุให้ชัดเจนว่าในการประมวลผลข้อมูลจะมีการคุ้มครองข้อมูลส่วนบุคคลอย่างไรบ้าง

3 ต้องแจ้ง Data Controller ทันทีหากพบเหตุการณ์ข้อมูลรั่วไหล (Data Breach Notification)

4 ห้ามใช้ Sub-Processor (ผู้ประมวลผลย่อย) โดยไม่ได้รับอนุญาตจาก Data Controller

5 ต้องช่วยเหลือ Data Controller ในการปฏิบัติตามกฎหมาย เช่น การตอบสนองคำขอของเจ้าของข้อมูล

6 ต้องลบหรือคืนข้อมูลให้กับ Data Controller เมื่อสิ้นสุดการให้บริการ

7 ผู้ประมวลผลข้อมูลจะไม่นำข้อมูลที่ได้ไปใช้ในวัตถุประสงค์อื่นนอกเหนือจากที่ระบุในข้อตกลงฉบับนี้

8 หากการกระทำใดของผู้ประมวลผลข้อมูลทำให้เกิดข้อพิพาทหรือความเสียหายแก่บริษัท ผู้ประมวลผลข้อมูลต้องรับผิดชอบความเสียหายที่เกิดขึ้นทั้งหมด

หลักการเขียน DSA

1 วัตถุประสงค์ของการแบ่งปันข้อมูล

ระบุว่าข้อมูลถูกแบ่งปันเพื่อวัตถุประสงค์อะไร เช่น การวิจัย การตลาด การตรวจสอบทางกฎหมาย ฯลฯ

2 ประเภทของข้อมูลที่ถูกแบ่งปัน เช่น ข้อมูลลูกค้า ข้อมูลสุขภาพ ข้อมูลทางการเงิน ฯลฯ

3 สิทธิของเจ้าของข้อมูล (Data Subject Rights)

ต้องแจ้งให้ DSทราบว่าใครเป็น DC ที่จะสามารถใช้สิทธิ์ในการเข้าถึง แก้ไข หรือลบข้อมูลได้อย่างไร

4 บทบาทและความรับผิดชอบของแต่ละฝ่าย

ระบุว่าใครเป็นผู้รับผิดชอบต่อการรักษาความปลอดภัยของข้อมูลในเรื่องใดบ้าง

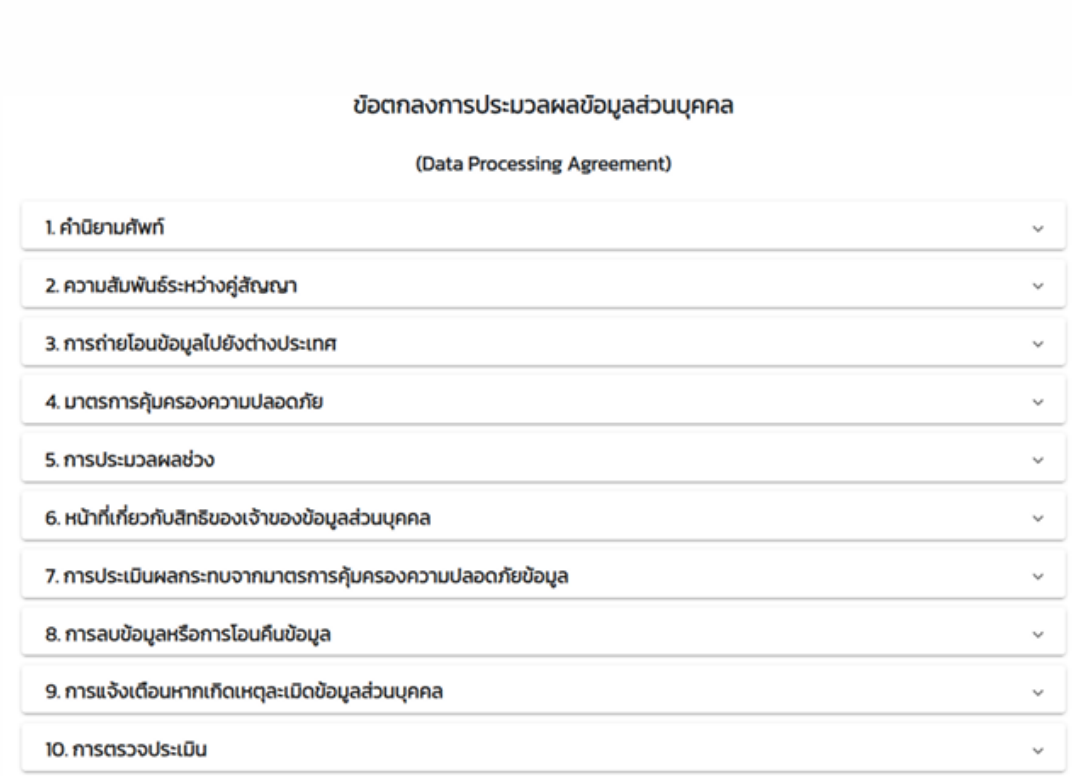
5 มาตรการปกป้องข้อมูล

ต้องมีมาตรการเพื่อป้องกันข้อมูลรั่วไหล และกำหนดแนวทางการรักษาความปลอดภัย

6 การแจ้งเหตุการณ์ข้อมูลรั่วไหล

หากมีการละเมิดข้อมูล (Data Breach) ต้องแจ้งให้ฝ่ายที่เกี่ยวข้องทราบและดำเนินมาตรการแก้ไขอย่างไร

การจัดทำสัญญาการประมวลผล และการแบ่งปันข้อมูลส่วนบุคคล



pdpc สคส. GPPC

แพลตฟอร์มภาครัฐเพื่อรองรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
Government Platform for PDPA Compliance : GPPC

การจัดการความเสี่ยงจากคู่ค้า (Partner Management & DPA)

Partner Checklist (เกณฑ์การประเมินคู่ค้า)

- มีมาตรการรักษาความปลอดภัยของข้อมูล (Data Storage & Security)
- มีการให้ความรู้และอบรมพนักงานภายใน
- มีกระบวนการตรวจสอบภายในและจัดการความเสี่ยงสม่ำเสมอ
- มีประวัติการจัดการข้อร้องเรียนที่โปร่งใส

Data Processing Agreement - DPA (ข้อตกลงการประมวลผลข้อมูล)

- **กฎหลัก:** ผู้ควบคุมข้อมูลต้องทำสัญญากับผู้รับจ้าง/คู่ค้าที่ประมวลผลข้อมูลให้
- **ข้อบังคับสำคัญ:** บังคับให้คู่ค้าต้องแจ้งเหตุ Data Breach กลับมายังผู้ควบคุมข้อมูล **ภายใน 72 ชั่วโมง** ทันทีที่ทราบเหตุ เพื่อให้เราดำเนินการต่อได้ทัน

แบบฟอร์มข้อตกลงการประมวลผลข้อมูล (DPA)

Logo
คู่สัญญา

ข้อตกลงการประมวลผข้อมูลส่วนบุคคล (data processing agreement)

โครงการ.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือหรือสัญญาฉบับหลัก).....

ระหว่าง

มหาวิทยาลัยราช..... กับ.....(ชื่อคู่สัญญา).....

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ทำขึ้น เมื่อวันที่.... (ระบุวันที่ลงนามในข้อตกลง)..... ณ มหาวิทยาลัยราชภัฏ.....

โดยที่ มหาวิทยาลัยราชภัฏ..... ฝ่ายหนึ่ง ได้ตกลงใน.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “(บันทึกความร่วมมือ/สัญญา)” กับ ..... (ระบุชื่อคู่สัญญา)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “.....(ระบุชื่อเรียกคู่สัญญา.....” อีกฝ่ายหนึ่ง

ตาม (ระบุชื่อบันทึกความร่วมมือ/สัญญาหลัก) ดังกล่าวกำหนดให้ มหาวิทยาลัยราชภัฏ..... มีหน้าที่และความรับผิดชอบในส่วนของการ.....(ระบุขอบเขต สิทธิ หน้าที่ของ มหาวิทยาลัยราชภัฏ..... ตามบันทึกความร่วมมือ/สัญญาหลัก)..... ซึ่งในการดำเนินการดังกล่าวประกอบด้วยการมอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา).....เป็นผู้ดำเนินการกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลแทนหรือในนามของ มหาวิทยาลัยราชภัฏ.....

มหาวิทยาลัยราชภัฏ..... ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบและกำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ได้.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้..... (ระบุชื่อคู่สัญญา).....ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. ..... (ระบุวัตถุประสงค์ที่ มหาวิทยาลัยราชภัฏ..... มอบหมายให้คู่สัญญาดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล เช่น เพื่อการรับจ้างทำระบบยืนยันตัวตน เพื่อการรับทำ Survey เพื่อการลงทะเบียนผู้เข้าร่วมงานสัมมนา เพื่อการรับจ้างพิมพ์บัตรพนักงาน เพื่อการรับส่งเอกสาร เป็นต้น).....

๒. .....

โดยข้อมูลส่วนบุคคลที่ มหาวิทยาลัยราชภัฏ..... มอบหมาย.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้.... (ระบุชื่อคู่สัญญา).....ประมวลผล ประกอบด้วย

๑. ..... (ระบุรายการข้อมูลส่วนบุคคลที่ มหาวิทยาลัยราชภัฏ..... มอบหมาย/เปิดเผยให้คู่สัญญาประมวลผล เช่น ชื่อ นามสกุลของเจ้าหน้าที่ เบอร์โทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชันทางรัฐ รายชื่อผู้เข้าร่วมงานสัมมนา เป็นต้น).....

๒. .....

ด้วยเหตุนี้ ทั้งสองฝ่ายจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือข้อตกลงฉบับนี้เป็นส่วนหนึ่ง....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).....เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่ มหาวิทยาลัยราชภัฏ..... มอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา)..... ดำเนินการ อันเนื่องมาจากการดำเนินการตามหน้าที่และความรับผิดชอบตาม.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).....ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายอื่น ๆ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. ..... (ระบุชื่อคู่สัญญา)..... รับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดย..... (ระบุชื่อคู่สัญญา)..... จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

โดยในการดำเนินการตามข้อตกลงนี้ ..... (ระบุชื่อคู่สัญญา).....จะประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก มหาวิทยาลัยราชภัฏ..... แล้วเท่านั้น ทั้งนี้ เพื่อให้ปราศจากข้อสงสัยการดำเนินการประมวลผลข้อมูลส่วนบุคคลโดย..... (ระบุชื่อคู่สัญญา).....ตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).....ถือเป็นการได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก มหาวิทยาลัยราชภัฏ..... แล้ว

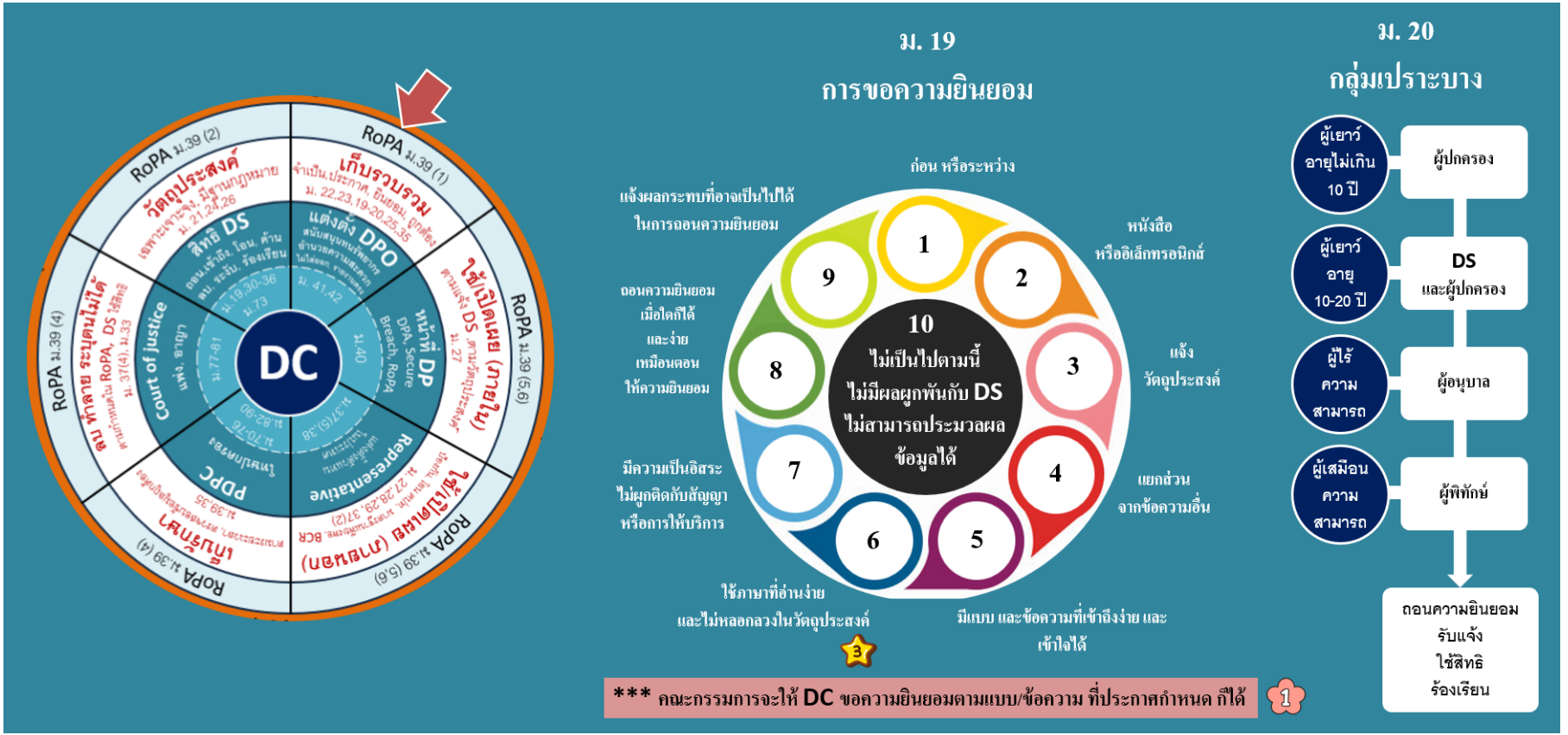
๒. ..... (ระบุชื่อคู่สัญญา).....จะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น และจะดำเนินการเพื่อให้พนักงาน


ANY QUESTIONS?

มาตรา 19

ระดับมหาวิทยาลัย และคณะ (IT)

ขอความยินยอม (Lawfulness, กรณีไม่มีฐานอื่น)



การขอความยินยอม ม.19 ว.4

มาตรา ๑๙ ผู้ควบคุมข้อมูลส่วนบุคคลจะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

การขอความยินยอมต้องทำโดยชัดแจ้ง เป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไปด้วย และการขอความยินยอมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน มีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่าย และไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ดังกล่าว ทั้งนี้ คณะกรรมการจะให้ผู้ควบคุมข้อมูลส่วนบุคคลขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามแบบและข้อความที่คณะกรรมการประกาศกำหนดก็ได้

ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องคำนึงอย่างถึงที่สุดในความเป็นอิสระของเจ้าของข้อมูลส่วนบุคคลในการให้ความยินยอม ทั้งนี้ ในการเข้าทำสัญญาซึ่งรวมถึงการให้บริการใด ๆ ต้องไม่มีเงื่อนไขในการให้ความยินยอมเพื่อเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่มีความจำเป็นหรือเกี่ยวข้องสำหรับการเข้าทำสัญญาซึ่งรวมถึงการให้บริการนั้น ๆ

การเก็บคุกกี้

คุกกี้ (Cookie)
คือ ไฟล์ข้อความ (Text File)
ขนาดเล็ก ที่ถูกบันทึกเอาไว้ใน
คอมพิวเตอร์ของเรา
ไฟล์ Cookie จะถูกสร้างขึ้น

วัตถุประสงค์

1. คุกกี้จำเป็น
(Strictly Necessary Cookie)

2. คุกกี้เพื่อการใช้งานเว็บไซต์
(Functional Cookies)

2. คุกกี้ประเมินผลการใช้งาน(Performance Cookie)

4. คุกกี้โฆษณา
กลุ่มเป้าหมาย
(Targeting Cookies)

ตัวอย่างการขอความความยินยอม

บริษัท ธาริกัน ฟู้ดส์ จำกัด
33 ซอย โพธิ์แก้ว 3 แยก 19 คลองจั่น บางกะปิ กรุงเทพ 10240
Tel: 02 519 5488, 02 946 7295
Fax: 02 519 3820, 02 946 7299

หนังสือให้ความยินยอมในการเก็บรวบรวม ใช้และ/หรือเปิดเผยข้อมูลส่วนบุคคล

วันที่.....

ลูกค้า ผู้จัดจำหน่าย ผู้ให้บริการ และพันธมิตรทางธุรกิจ:

ชื่อ-สกุล:_____ _____อายุ:_____ปี

หมายเลขบัตรประชาชน/หนังสือเดินทาง: _____

บริษัท ธาริกัน ฟู้ดส์ จำกัด ("บริษัทฯ" หรือ "เรา") มีความมุ่งมั่นที่จะให้บริการแก่ท่านด้วยมาตรฐานของบริษัทฯ อย่างไรก็ตาม เพื่อให้เราสามารถดำเนินการตามคำสั่งซื้อ ปฏิบัติตาม สัญญา และ/หรือดำเนินการที่เกี่ยวข้องกับธุรกิจของเรา ให้แก่ท่านได้ เราจึงขอความยินยอมจากท่านในการเก็บรวบรวมใช้และเปิดเผยข้อมูลส่วนบุคคลของท่านภายใต้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (พ.ร.บ.ฯ) เพื่อวัตถุประสงค์ ตามที่ระบุไว้ด้านล่างนี้

ท่านมีสิทธิที่จะปฏิเสธการยินยอมให้เราเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ ตามที่ระบุไว้ด้านล่างนี้เมื่อใดก็ได้

ท่านยินยอมให้เรา หรือพันธมิตรของเรา ประมวลผลข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์ ทางการตลาด และการนำเสนอสินค้า/บริการที่เหมาะสมกับท่าน

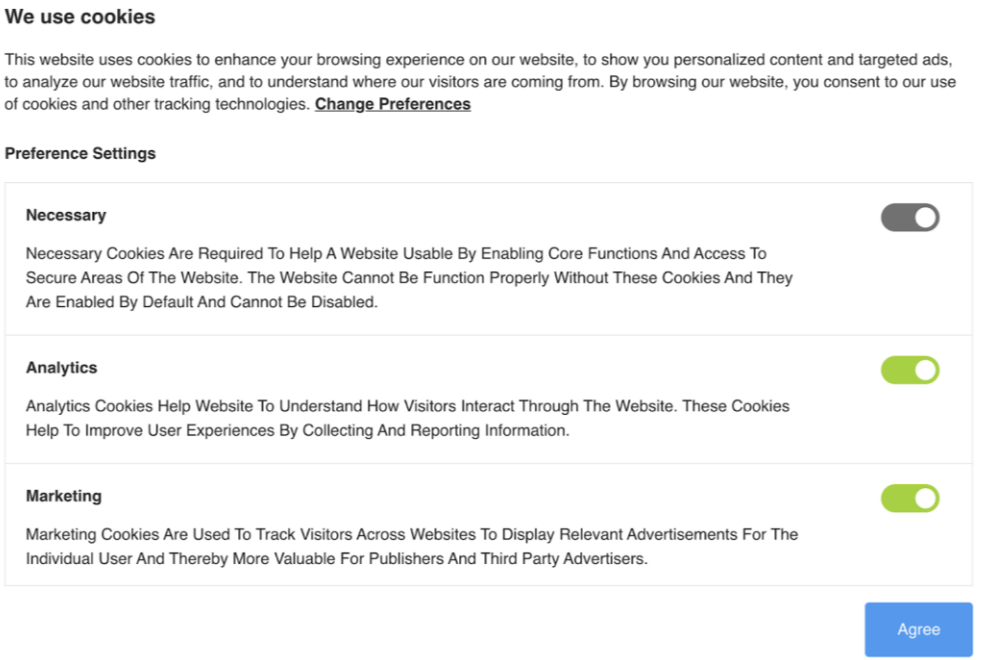
การปฏิเสธหรือเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ด้านล่างนี้ จะไม่ส่งผลต่อการปฏิบัติตามสัญญาที่เรามีหรืออาจมีกับท่าน

1. เพื่อเสนอสินค้า และ/หรือบริการ และ/หรือการส่งเสริมการขายที่เราวิเคราะห์แล้วว่าตรงกับความต้องการของท่าน

☐ ยินยอม ☐ ปฏิเสธ

2. เพื่อเสนอสินค้า และ/หรือบริการและ/หรือการส่งเสริมการขายของเราที่ดำเนินการโดยบริษัทอื่น หรือตัวแทนผู้ให้บริการของเรา

☐ ยินยอม ☐ ปฏิเสธ



ถอนความยินยอม ม.19 ว.5

เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเสียเมื่อใดก็ได้โดยจะต้องถอนความยินยอมได้ง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดสิทธิในการถอนความยินยอมโดยกฎหมายหรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล ทั้งนี้ การถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไปแล้วโดยชอบตามที่กำหนดไว้ในหมวดนี้

ในกรณีที่การถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงผลกระทบจากการถอนความยินยอมนั้น

การขอความยินยอม (Consent)

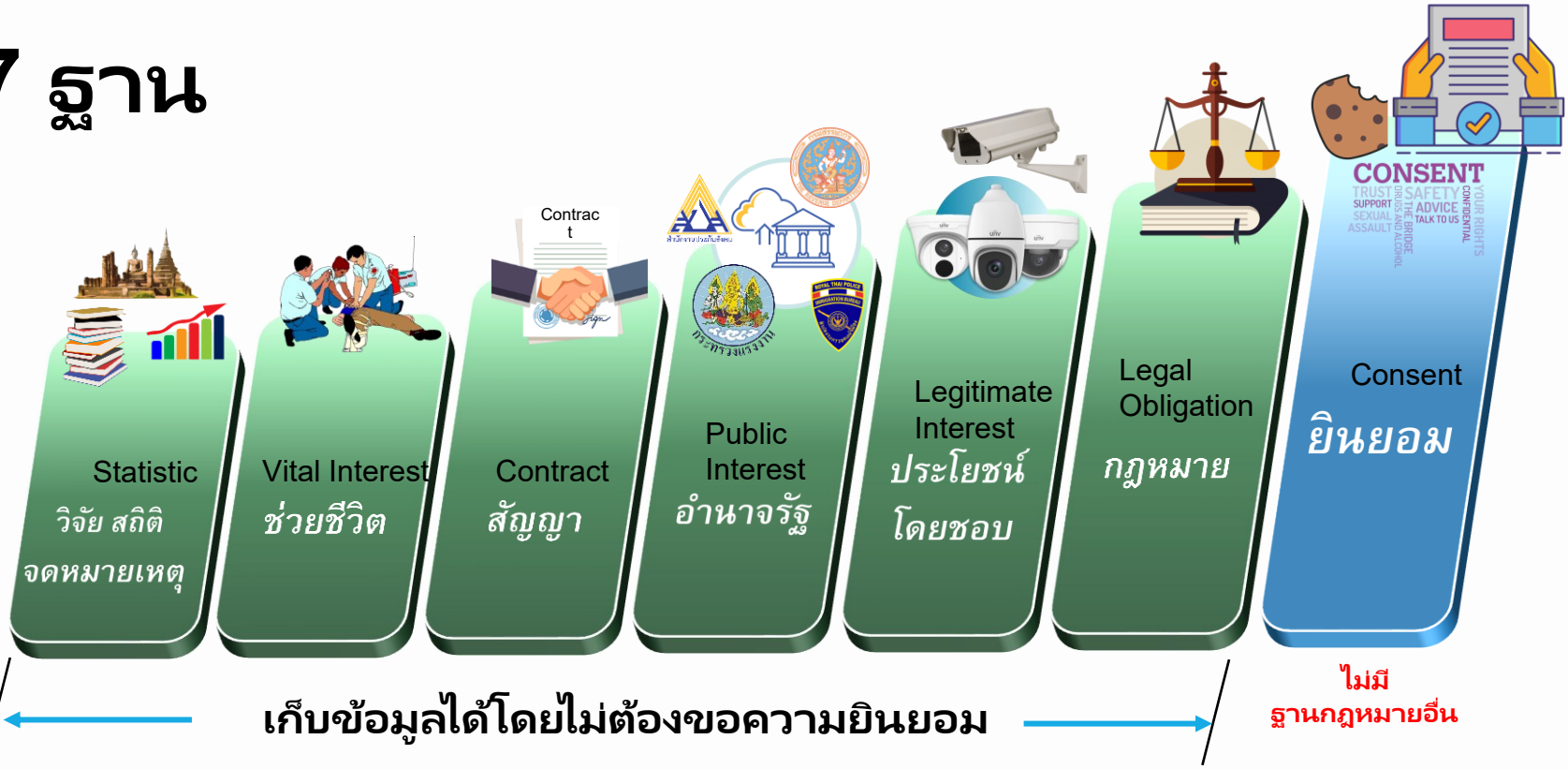
มาตรา 19 และ 20

ทุกระดับของมหาวิทยาลัย

ฐานกฎหมายข้อมูลทั่วไป (มาตรา 24)

ไม่ใช่: เชื้อชาติ, ศาสนา, การเมือง, รสนิยมทางเพศ, ชีวภาพ, ประวัติอาชญากรรม, สุขภาพ, ความพิการ, พันธุกรรม, สหภาพแรงงาน

7 ฐาน



ฐานกฎหมายข้อมูลอ่อนไหว (มาตรา 26)

เชื้อชาติ, ศาสนา, การเมือง, รสนิยมทางเพศ, ชีวภาพ, ประวัติอาชญากรรม, สุขภาพ, ความพิการ, พันธุกรรม, สหภาพแรงงาน, อื่นๆ

ประโยชน์สาธารณะที่สำคัญ

การศึกษาวิจัย

วิทยาศาสตร์ ประวัติศาสตร์ สถิติ ประโยชน์สาธารณะอื่น
เพื่อบรรลุวัตถุประสงค์เท่าที่จำเป็น
จัดมาตรการที่เหมาะสม คุ้มครองสิทธิ, ประโยชน์

การคุ้มครองแรงงาน, ประกันสังคม

หลักประกันสุขภาพแห่งชาติ, สวัสดิการ
รักษาพยาบาลผู้มีสิทธิการรักษาตาม กม.
การคุ้มครองผู้ประกันภัยจากรถ
การคุ้มครองทางสังคม
จัดมาตรการที่เหมาะสม คุ้มครองสิทธิ, ประโยชน์

ประโยชน์สาธารณะด้านสาธารณสุข

การป้องกันโรคติดต่อ ควบคุมมาตรฐาน หรือ
คุณภาพยา เวชภัณฑ์ เครื่องมือแพทย์
จัดมาตรการที่เหมาะสม โดยเฉพาะการรักษาความลับ

เวชศาสตร์ป้องกัน อาชีวเวชศาสตร์

ประเมินความสามารถในการทำงาน
วินิจฉัยโรค รักษาโรค จัดการด้านสุขภาพ บริการสังคมสงเคราะห์
ปฏิบัติตามสัญญาระหว่าง DS กับผู้ประกอบวิชาชีพทางการแพทย์

ระงับหรือป้องกันอันตรายต่อชีวิต ร่างกาย สุขภาพ

DS ไม่สามารถให้ความยินยอมได้

มูลนิธิ, สมาคม, องค์กรไม่แสวงหากำไร

การเมือง,ศาสนา,ปรัชญา, สหภาพแรงงาน
มีการคุ้มครอง, ไม่เปิดเผยข้อมูลไปภายนอก
จัดมาตรการคุ้มครองเหมาะสม

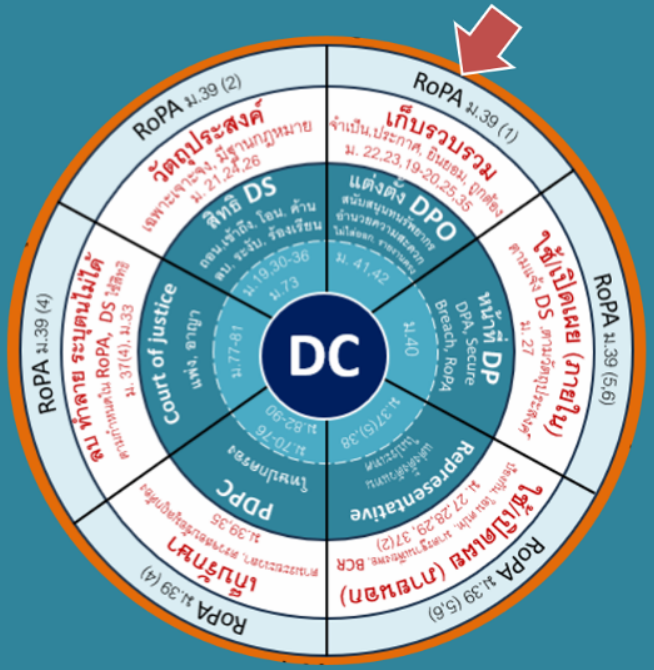
เปิดเผยต่อสาธารณะ

ด้วยความยินยอมโดยชัดแจ้งของ DS

การก่อตั้ง ปฏิบัติ ใช้สิทธิเรียกร้อง ต่อสู้ในชั้นศาล

ตามกฎหมาย

ภาพรวม กฎหมาย กับวงจรชีวิตของข้อมูลส่วนบุคคล



ม. 19
การขอความยินยอม

*** คณะกรรมการจะให้ DC ขอความยินยอมตามแบบ/ข้อความ ที่ประกาศกำหนด ก็ได้

ม. 20
กลุ่มเปราะบาง

- ผู้เยาว์ อายุไม่เกิน 10 ปี → ผู้ปกครอง
- ผู้เยาว์ อายุ 10-20 ปี → DS และผู้ปกครอง
- ผู้ไร้ความสามารถ → ผู้อนุบาล
- ผู้เสมือนความสามารถ → ผู้พิทักษ์

ถอนความยินยอม
รับแจ้ง
ใช้สิทธิ
ร้องเรียน

การขอความยินยอม กลุ่มเปราะบาง (ม.20)

การขอความยินยอม จากผู้เยาว์

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มาตรา 20 กำหนดหลักการเกี่ยวกับความยินยอมของผู้เยาว์ ไว้ดังนี้

1 ผู้เยาว์อายุ **ไม่เกิน 10 ปี** ผู้ควบคุมข้อมูลส่วนบุคคลต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

2 ผู้เยาว์อายุ **ตั้งแต่ 10 ปี แต่ไม่ถึง 20 ปีบริบูรณ์** ต้องขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ก่อน แต่มีบางกรณีที่ผู้เยาว์ให้ความยินยอมเองได้ ดังนี้

1) กรณีผู้เยาว์ทำการเพื่อได้ไปซึ่งสิทธิหรือเพื่อให้หลุดพ้นจากหน้าที่และต้องไม่มีเงื่อนไขใด ๆ เช่น บริษัท ก ทำสัญญาให้ทุนการศึกษากับผู้เยาว์ โดยไม่มีข้อผูกมัดหรือหน้าที่ใด จึงเป็นการทำนิติกรรมที่มีลักษณะเพียงเพื่อได้ไปซึ่งสิทธิในทุนการศึกษา

2) กรณีผู้เยาว์ต้องแสดงเจตนาทำนิติกรรมเองโดยเป็นการเฉพาะตัวไม่อาจให้ผู้อื่นทำการแทน เช่น การทำพินัยกรรมซึ่งผู้เยาว์สามารถกระทำได้เมื่อมีอายุ 15 ปีบริบูรณ์

3) กรณีผู้เยาว์ทำการใด ๆ ซึ่งสมแก่ฐานานุรูป และจำเป็นในการดำรงชีพ เช่น ผู้เยาว์สามารถสั่งซื้ออาหารออนไลน์ หรือเรียกรถรับจ้างผ่านแพลตฟอร์มเรียกรถโดยสารได้ด้วยตนเอง

ตามประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์บรรลุนิติภาวะ เมื่อ (1) มีอายุครบ 20 ปีบริบูรณ์ หรือ (2) โดยการสมรสที่ชอบด้วยกฎหมาย

การขอความยินยอม กลุ่มเปราะบาง

การขอความยินยอม
จาก คนไร้ความสามารถ
หรือ คนเสมือนไร้ความสามารถ

คนไร้ความสามารถ

คือ บุคคลวิกลจริตที่ศาลสั่งให้เป็นคนไร้ความสามารถ ต้องขาดความรู้สึกและขาดความรับผิดชอบอย่างรุนแรงทำภารกิจส่วนตัวไม่ได้ ต้องอยู่ในความดูแลของผู้อนุบาลตามมาตรา 28 ของประมวลกฎหมายแพ่งและพาณิชย์ เช่น ผู้พิการทางสมอง, คนบ้าสมองฟ่อ สมองเสื่อมขั้นรุนแรง

คนเสมือนไร้ความสามารถ

คือ ผู้ที่ศาลได้สั่งให้เป็นคนเสมือนไร้ความสามารถ ต้องจัดอยู่ในความดูแลของผู้พิทักษ์ตามมาตรา 32 ของประมวลกฎหมายแพ่งและพาณิชย์ ซึ่งมีลักษณะอย่างใดอย่างหนึ่ง ได้แก่ เป็นบุคคลมีกายพิการ หรือเป็นบุคคลมีจิตฟั่นเฟือนไม่สมประกอบ หรือเป็นบุคคลประพฤติสุรุ่ยสุร่ายเสเพลเป็นอาจิณ

ผู้อนุบาล ⟵ การขอความยินยอม การใช้สิทธิ ⟶ **ผู้พิทักษ์**

แบบฟอร์มข้อตกลงการประมวลผลข้อมูล (DPA)

เอกสารแสดงความยินยอม (Consent Form)

มหาวิทยาลัยราชภัฏสกลนคร

วันที่_____

ชื่อกิจกรรม _____

ข้าพเจ้า นาย/นาง/นางสาว _____

❒ “ยินยอม” ❒ “ไม่ยินยอม”

ให้_____ ทำการเก็บ/ใช้/เปิดเผยข้อมูลส่วนบุคคลให้กับคู่ค้าและ/หรือพันธมิตรทางธุรกิจ เพื่อวัตถุประสงค์

1) _____ 2) _____

ทั้งนี้ ก่อนการแสดงเจตนา ข้าพเจ้าได้อ่านรายละเอียดจากเอกสารชี้แจงข้อมูล หรือได้รับคำอธิบายจาก_____ ถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคล และมีความเข้าใจดีแล้ว

ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารนี้ด้วยความสมัครใจ ปราศจากการบังคับหรือชักจูง และข้าพเจ้าทราบว่าข้าพเจ้าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้เว้นแต่ในกรณีมีข้อจำกัดสิทธิตามกฎหมายหรือยังมีสัญญาระหว่างข้าพเจ้ากับ_____ ที่ให้ประโยชน์แก่ข้าพเจ้าอยู่

กรณีที่ข้าพเจ้าประสงค์จะขอถอนความยินยอม ข้าพเจ้าทราบว่าการถอนความยินยอมจะมีผลทำให้

1) _____ไม่ได้รับ..... (ความสะดวกในการใช้บริการ)

2) _____ไม่สามารถ..... (เข้าถึงบริการบางอย่างได้)

3) _____ไม่ทราบ.....(ข่าวสาร)

และข้าพเจ้าทราบว่าการถอนความยินยอมดังกล่าว ไม่มีผลกระทบต่อการประมวลผลข้อมูลส่วนบุคคลที่ได้ดำเนินการเสร็จสิ้นไปแล้วก่อนการถอนความยินยอม

ลงชื่อ.....

(.....)

แบบคำขอถอนความยินยอม

(Withdrawal of Consent Form)

โปรดกรอกรายละเอียดในคำขอนี้ให้ครบถ้วน และยื่นคำขอนี้ด้วยตนเอง ณ ที่ทำการบริษัท หรือ อีเมล [dpoarg@ar.co.th]

วันที่ยื่นคำขอ.....

รายละเอียดของเจ้าของข้อมูลส่วนบุคคล

ชื่อ – สกุล	
ที่อยู่	
เบอร์ติดต่อ	
ไปรษณีย์อิเล็กทรอนิกส์ (E-mail)	

ผู้ยื่นคำขอได้แนบเอกสารประกอบการยื่นคำขอใช้สิทธิของเจ้าของข้อมูล ดังนี้

- ☐ สำเนาบัตรประจำตัวประชาชน (กรณีสัญชาติไทย) พร้อมรับรองสำเนาถูกต้อง
- ☐ สำเนาหนังสือเดินทาง (กรณีชาวต่างชาติ) พร้อมรับรองสำเนาถูกต้อง
- ☐ อื่น ๆ (ถ้ามี) .....

ทั้งนี้ บริษัทฯ ขอสงวนสิทธิในการสอบถามข้อมูล หรือเรียกเอกสารเพิ่มเติมจากเจ้าของข้อมูลเพื่อยืนยันสถานะการเป็นเจ้าของข้อมูล และพิจารณาดำเนินการตามคำขอ

ข้อมูลส่วนบุคคลที่ต้องการดำเนินการ

- ☐ ข้อมูลส่วนบุคคลทั้งหมดที่อาศัยฐานความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผย
- ☐ เฉพาะข้อมูลส่วนบุคคลที่อาศัยฐานความยินยอมดังต่อไปนี้ (โปรดระบุ).....

.....

.....

.....

.....

.....

.....

แบบฟอร์มข้อตกลงการประมวลผลข้อมูล (DPA)

แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

Data Subject Rights Request Form

วันที่ .....

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการขอใช้สิทธิดำเนินการต่อข้อมูลส่วนบุคคลของตนซึ่งอยู่ในความดูแลของมหาวิทยาลัยราชภัฏ..... (“**มหาวิทยาลัย**”) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ ท่านสามารถใช้สิทธิดังกล่าวได้โดยการกรอกรายละเอียดในแบบคำร้องนี้ และยื่นคำขอนี้ด้วยตนเองแก่ มหาวิทยาลัย ทาง จดหมายอิเล็กทรอนิกส์ (e-mail) (ระบุช่องทางอื่น หากมี).....

ข้อมูลผู้ยื่นคำร้องขอ

ชื่อ-นามสกุล .....
เลขบัตรประจำตัวประชาชน .....
เบอร์โทรศัพท์ติดต่อ .....
อีเมล .....

ท่านเป็นเจ้าของข้อมูลส่วนบุคคลหรือไม่

❒ ผู้ยื่นคำร้องเป็นเจ้าของข้อมูลส่วนบุคคล

❒ ผู้ยื่นคำร้องเป็นผู้แทนของเจ้าของข้อมูลส่วนบุคคล (โปรดระบุรายละเอียดของเจ้าของข้อมูลส่วนบุคคล)

<u>รายละเอียดของเจ้าของข้อมูลส่วนบุคคล</u>

ชื่อ-นามสกุล .....
ที่อยู่ .....
เบอร์โทรศัพท์ .....
อีเมล .....

เอกสารประกอบการขอใช้สิทธิ

เอกสารเพื่อการยืนยันตัวตนของผู้ยื่นคำร้อง

❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญญาชาติไทย)

❒ สำเนาหนังสือเดินทาง (กรณีไม่มีสัญญาชาติไทย)

เอกสารประกอบการดำเนินการแทน (เฉพาะกรณียื่นคำร้องแทนเจ้าของข้อมูลส่วนบุคคล)

❒ หนังสือมอบอำนาจที่เจ้าของข้อมูลส่วนบุคคลให้อำนาจผู้ยื่นคำร้องใช้สิทธิแทนเจ้าของข้อมูลส่วนบุคคลตามแบบคำร้องขอฉบับนี้ ซึ่งลงนามโดยเจ้าของข้อมูลส่วนบุคคลและผู้ยื่นคำร้องและลงวันที่ก่อนวันที่ยื่น

โปรดระบุสถานะความสัมพันธ์ของท่านที่มีต่อ มหาวิทยาลัย

❒ ลูกค้า / ผู้ใช้งานแอปพลิเคชัน / ผู้เข้าชมเว็บไซต์

❒ เจ้าหน้าที่/ผู้ปฏิบัติงาน

❒ ผู้สมัครงาน

❒ คู่สัญญา/ผู้รับเหมา

❒ ผู้ติดต่อ

❒ อื่น ๆ (โปรดระบุ) .....

โปรดระบุสิทธิที่ท่านประสงค์จะดำเนินการ

❒ เพิกถอนความยินยอม

❒ ขอเข้าถึงหรือรับสำเนาข้อมูลส่วนบุคคล รวมถึงขอให้ มหาวิทยาลัย เปิดเผยที่มาของข้อมูลที่ท่านไม่ได้ให้ความยินยอมในการเก็บรวบรวม

❒ ขอแก้ไขข้อมูลส่วนบุคคล

❒ ขอให้ลบข้อมูลส่วนบุคคล

❒ ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล

❒ ขอระงับการประมวลผลข้อมูลส่วนบุคคล


ANY QUESTIONS?

บันทึกรายการกิจกรรมการประมวลผล

RECORD OF PROCESSING ACTIVITIES

(ROPA)

มาตรา 39 และ 40

ทุกระดับของมหาวิทยาลัย

บันทึกรายการกิจกรรมการประมวลผล (RoPA) **คืออะไร?**

DC

ROPA | Records of Processing Activities

ROPA คือ การบันทึกกิจกรรมการประมวลผลขององค์กรที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ตามมาตรา 39 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะต้องอยู่ในรูปแบบข้อความที่เป็นลายลักษณ์อักษรหรืออิเล็กทรอนิกส์

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

1. ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยให้มีคำอธิบายประเภทเจ้าของข้อมูลส่วนบุคคล และประเภทของข้อมูลส่วนบุคคลด้วย
2. วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
3. ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทนและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) รวมถึงช่องทางการติดต่อ
4. ระยะเวลาในการเก็บรักษา และการลบข้อมูลส่วนบุคคล ประเภทต่าง ๆ
5. สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลนั้น
6. การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอม
7. การปฏิเสธคำขอหรือการคัดค้าน ตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม มาตรา 36 วรรคหนึ่ง
8. อธิบายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัย ตามมาตรา 37 (1)

บันทึกรายการดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรอาจจัดให้อยู่ในรูปแบบหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบได้

ผู้ควบคุมข้อมูลส่วนบุคคลใดไม่ปฏิบัติตามต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท ตามมาตรา 82

DP

หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ซึ่งมีรายละเอียดดังนี้...

1. ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล
2. ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลรับจ้างดำเนินการให้
3. ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
4. ประเภทหรือลักษณะของกิจกรรมการประมวลผล
5. ประเภทของหน่วยงานที่ได้รับข้อมูล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
6. คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

ประกาศฉบับนี้ มีผลบังคับใช้ในวันที่ 17 ธันวาคม 2565

กฎหมายเกี่ยวกับ RoPA

DC
ตัวแทน DC

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

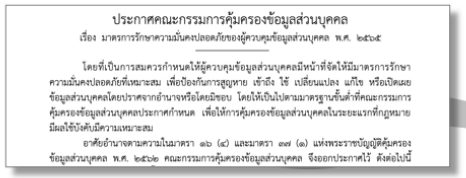
บันทึกในการจัดการสิทธิ

DC อยู่ ตปท. เสนอขายสินค้า/บริการ **ไม่ว่าจะจ่ายเงินหรือไม่ก็ตาม** หรือ เฝ้าติดตามพฤติกรรมคนในประเทศ

ประเมินผลกระทบ (DPIA)

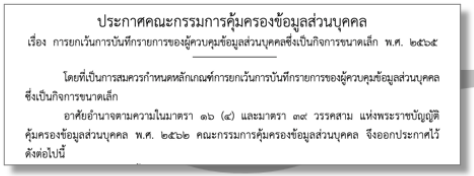
ทำเป็นกิจธุระ

ข้อมูลอ่อนไหว


ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๗ (๑) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้


ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) และมาตรา ๓๙ วรรคสาม แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

RoPA ของ DC แจ้งรายละเอียด **อะไรบ้าง?**

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

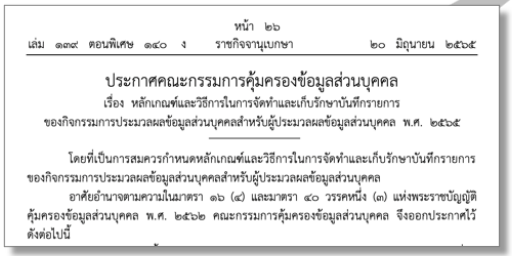
บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)

ม.39 (3)	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์ติดต่อ
ผู้ควบคุมข้อมูล (DC)			abc@gmail.com	
เจ้าที่หน้าที่คุ้มครองข้อมูล (DPO)			xyz@gmail.com	
ตัวแทน DC				

แผนก:	ABC	ม.39(1)		ม.39(2)	ม.39(3)				ม.39(4)		ม.39(5)					ม.39(6)			ม.39(7)			ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล		วัตถุประสงค์แยกประเภท (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล		เปิดเผยไปยังหน่วยงานอื่นๆ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไป ตปท. องค์กรระหว่างประเทศ	มาตรการการรักษาความมั่นคงปลอดภัย ม.37(1)		
				ทั่วไป	อ่อนไหว							ทั่วไป	อ่อนไหว				Confidentiality	Integrity	Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ, ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กฎแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอกำลังคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไข มีสิทธิอ่านเท่านั้น	สแกนเก็บไว้

แผนก:	ABC	ม.39(1)		ม.39(2)	ม.39(4)	ม.39(5)				ม.39(6)			ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล		วัตถุประสงค์แยกประเภท (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล		เปิดเผยไปยังหน่วยงานอื่นๆ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไป ตปท. องค์กรระหว่างประเทศ	มาตรการการรักษาความมั่นคงปลอดภัย ม.37(1)		
				ทั่วไป	อ่อนไหว							ทั่วไป	อ่อนไหว				Confidentiality	Integrity	Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ, ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กฎแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอกำลังคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไข มีสิทธิอ่านเท่านั้น	สแกนเก็บไว้

DP
(ไม่เขียนถึง ตัวแทน DP?)



หน้า ๒๖
เล่ม ๑๓๙ ตอนพิเศษ ๑๔๐ ง ราชกิจจานุเบกษา ๒๐ มิถุนายน ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการ
ของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล
อาศัยอำนาจตามความในมาตรา ๑๖ (๕) และมาตรา ๔๐ วรรคหนึ่ง (๓) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งไม่ปฏิบัติตาม (๑) สำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลใด ให้ถือว่าผู้ประมวลผลข้อมูลส่วนบุคคลเป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น

การดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้

ความใน (๓) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

สัญญาการประมวลผลข้อมูลข้อมูลส่วนบุคคล (DPA)

ประเมินผลกระทบ (DPIA)

ข้อมูลอ่อนไหว

ทำเป็นกิจธุระ

กฎหมายลำดับรอง

RoPA ของ DP

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษา RoPA สำหรับ DP

ข้อ ๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๒) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๓) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๔) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

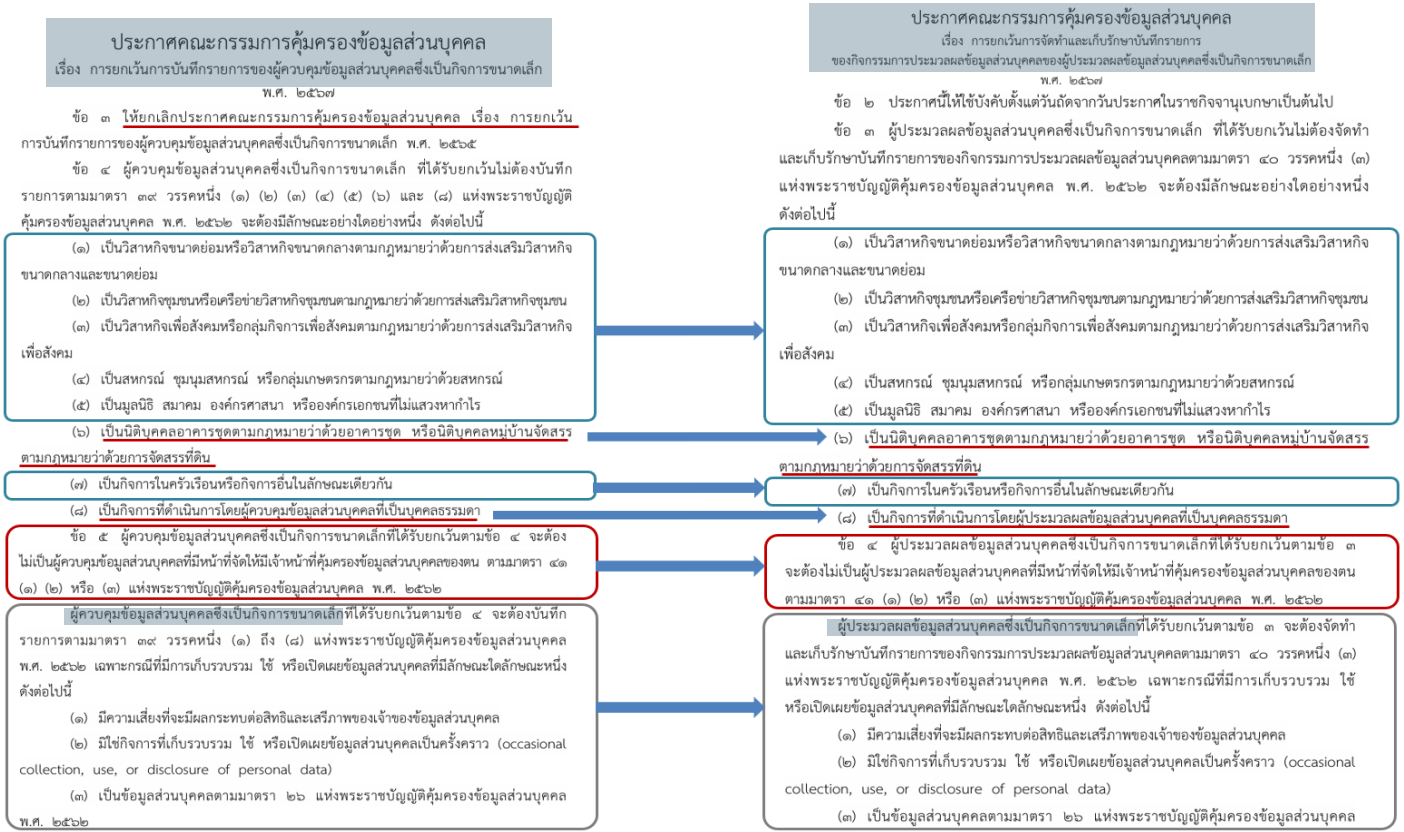
(๕) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(๖) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๔๐ วรรคหนึ่ง (๒)

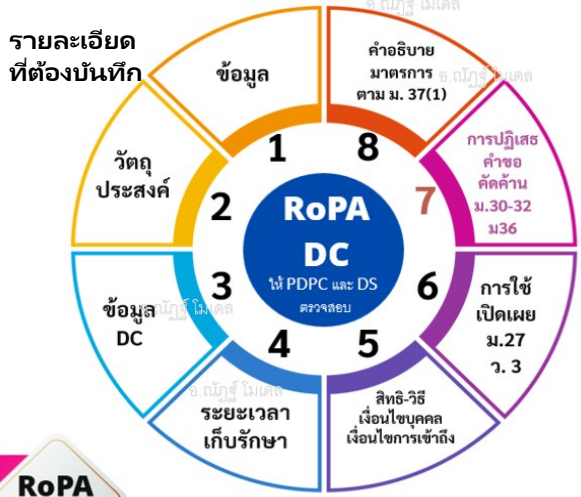
ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือในรูปแบบอิเล็กทรอนิกส์ก็ได้ ทั้งนี้ บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลดังกล่าวจะต้องเข้าถึงได้ง่าย และสามารถแสดงให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล หรือบุคคลที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายตรวจสอบได้อย่างรวดเร็วเมื่อมีการร้องขอ

กิจการขนาดเล็กที่ได้รับการยกเว้น ที่ไม่ต้องทำ RoPA ข้อ 1-6 และ 8

กฎหมายลำดับรอง ม.39 และ 40 เรื่อง กิจการขนาดเล็ก



ภาพรวมของ RoPA สำหรับ DC และ DP



ไม่ต้องบันทึก
ข้อ 1-6 และ 8
บันทึกเฉพาะ ข้อ 7

DC/DP
กิจการขนาดเล็ก

ไม่ต้องบันทึกทุกข้อ (ข้อ 1-6)

RoPA DP

เข้าถึงง่าย ให้ PDPC และ DC ตรวจสอบได้อย่างรวดเร็ว เมื่อร้องขอ

1. ชื่อและข้อมูล DP และตัวแทน (ถ้ามี)
2. ชื่อและข้อมูล DC และตัวแทน (ถ้ามี)
3. ชื่อและข้อมูล DPO สถานที่/วิธีติดต่อ (ถ้ามี)
4. วัตถุประสงค์,ข้อมูล, ประเภท หรือลักษณะการประมวลผลตามคำสั่ง
5. ประเภทบุคคล หรือหน่วยงาน ที่ได้รับข้อมูล กรณีส่งโอนไป ตปท.
6. คำอธิบายมาตรการ ตาม ม.40 วรรค 1 (2)

ประเภทกิจการขนาดเล็ก

อย่างใดอย่างหนึ่ง

	ขายส่ง-ปลีก บริการ	ผลิต
1 วิสาหกิจขนาดย่อม-กลาง	พนง.ไม่เกิน 100 คน รายได้ ไม่เกิน 300 ล้าน/ปี	พนง.ไม่เกิน 200 คน รายได้ ไม่เกิน 500 ล้าน/ปี

2. วิสาหกิจชุมชน หรือเครือข่าย
3. วิสาหกิจ/กลุ่มกิจการเพื่อสังคม
4. สหกรณ์ ชุมนุมสหกรณ์ กลุ่มเกษตรกร
5. มูลนิธิ สมาคม องค์กรศาสนา องค์กรเอกชนไม่แสวงหากำไร
6. นิติบุคคลอาคารชุด/บ้านจัดสรร
7. กิจการในครัวเรือน หรือในลักษณะเดียวกัน
8. กิจการที่ DC หรือ DP เป็นบุคคลธรรมดา

ยกเว้น:

- เข้าเกณฑ์ต้องแต่งตั้ง DPO ตาม ม.41
- ประมวลผลมีความเสี่ยงต่อสิทธิเสรีภาพ DS
- ไม่ใช่กิจการที่มีการประมวลผลเป็นครั้งคราว
- มีการประมวลผลข้อมูลอ่อนไหว

*** ต้องทำ RoPA ทุกข้อ ***
(DC 8 ข้อ, DP 6 ข้อ)

โทษทางปกครอง
(ปรับไม่เกิน)

1 ล้านบาท	3 ล้านบาท
DC (ม.82) ตัวแทน DC (ม.88) ตัวแทน DP (ม.88)	DP (ม.86) (ตัวแทน DP) ปัจจุบันมีแต่ DP
ไม่ทำตาม ม. 39 วรรค 1 (ม.88)	ไม่ทำตาม ม. 40 (3) (ม.86)

กระบวนการ
จัดทำ RoPA

Data Inventory: การทำแผนที่ข้อมูลก่อนเริ่มเก็บรวบรวม

ทำ Data Inventory Mapping ก่อนทำ RoPA

เริ่มจาก **Pain point** ขององค์กร

ลองตอบคำถามว่า

- บริษัทมี **ข้อมูลส่วนบุคคลอะไรบ้าง?**
- เก็บไว้ที่ไหน?
- ใครใช้?
- ส่งให้ใคร?
- เก็บไว้นานเท่าไร?

ท่านตอบได้แค่ไหน...?

การปกป้องข้อมูลส่วนบุคคลได้
“องค์กรต้องรู้ว่าเก็บข้อมูลอะไร อยู่ที่ไหน ใช้อย่างไร”

หากไม่รู้ว่า เก็บข้อมูลอะไร อยู่ที่ไหน ใช้อย่างไร => บริหารความเสี่ยงไม่ได้

Data Inventory Mapping คือ

แผนผังข้อมูล เพื่อให้องค์กรรู้ว่าตั้งแต่การเก็บจนถึงลบทำลายข้อมูล

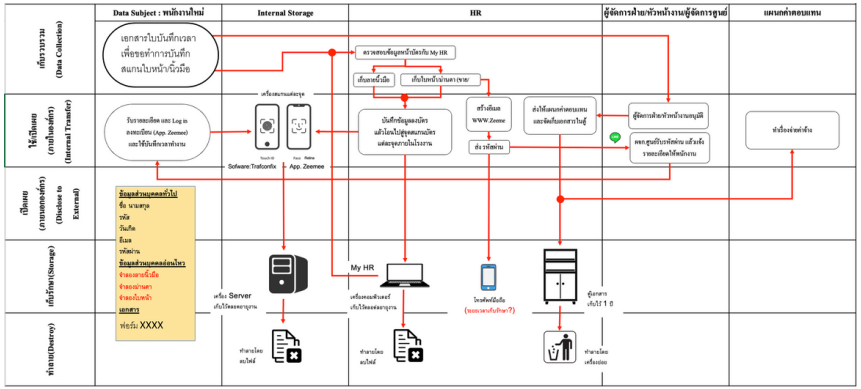
- ได้มาจากไหน?
- ใครเป็นคนเก็บข้อมูล
- เก็บข้อมูลอะไรบ้าง?
- เก็บไว้ที่ไหนบ้าง?
- ใครใช้บ้าง, ใช้เพื่ออะไรบ้าง?
- ส่งโอนต่อให้ใครบ้าง?
- เก็บไว้นานแค่ไหน?
- ลบทำลายที่ไหน, อย่างไร?

ลำดับการทำ DIM-DFD-RoPA

DIM

กิจกรรม			เก็บรวบรวม (ม.19-26)													ใช้/เปิดเผย/ส่ง-โอน (ม.27-29)							การเก็บรักษา และทำลาย (ม.37(3),39(5))							มาตรการรักษาความมั่นคงปลอดภัย (ม.37(1),39(8))		
			ข้อมูล (เท่าที่จำเป็น ม.22)		วัตถุประสงค์ (ม.21,27)	ฐานกฎหมาย (ข้อยกเว้นที่ไม่ต้องขอความยินยอม)		เจ้าของข้อมูล	ประเภทของเจ้าของข้อมูล (ม.20)					แหล่งที่มาของข้อมูล (ม.25)			เอกสารอ้างอิง (สัญญา/แบบฟอร์ม/ใบสมัคร/อื่นๆ)		ประกาศความเป็นส่วนตัว (ม.23)	ใช้ (ในองค์กร)		เปิดเผย (นอกองค์กร)		ส่ง-โอน (ต่างประเทศ)			ทั้งรูปแบบกระดาษ และ อิเล็กทรอนิกส์							ใช้/ เปิดเผย /ส่งโอน/ เก็บรักษา/ ทำลาย		
No.	กระบวนการหลัก	กระบวนการย่อย	ทั่วไป (ม.24)	อ่อนไหว (ม.26)		ข้อมูลทั่วไป (ม.24)	ข้อมูลอ่อนไหว (ม.26)		บรรพบุรุษ	ผู้เยาว์ไม่เกิน 10 ปี	ผู้เยาว์ เกิน 10 ปี	ไร้ความสามารถ	เสมือนไร้ความสามารถ	เจ้าของข้อมูลโดยตรง	ข้อมูลที่อยู่ในองค์	แหล่งอื่น	กระดาษ	อิเล็กทรอนิกส์	ใช้ใน เครื่องหมาย	ใช้โดย หน่วยงานใน หน่วยงานนี้	หน่วยงานอื่น	เปิดเผยไปให้ บุคคล หรือนิติบุคคลอื่น ภายนอกองค์กร	บุคคล นิติบุคคล	ให้บุคคล/นิติบุคคลอื่น (ม.28)	ใช้ใน เครื่องหมาย (ม.29)	อุปกรณ์และระบบที่จัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ระยะเวลาการจัดเก็บ	เกณฑ์อ้างอิงระยะเวลาจัดเก็บ	วิธีการลบทำลาย ทำให้ไม่สามารถระบุตัวบุคคลได้	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาความพร้อมใช้ (Availablity)
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ, ศาสนา	คัดเลือกเข้าทำงาน	สัญญา	กฎหมาย	ผู้สมัครงาน	Y	-	-	-	-	Y	-	-	ชื่อเอกสาร	ชื่อไฟล์	แบบฟอร์มร่วมสมัครงาน	-	N	Y	แผนกที่ขอกำลังคน	คัดเลือกเข้าทำงาน	-	-	-	-	-	ตู้เอกสาร	HR	อ่าน	กฎแจ	ผู้รับผิดชอบเท่านั้น	6 เดือน	รอผลการคัดเลือก	เครื่องย่อยกระดาษ	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไขสิทธิอ่านเท่านั้น	ล็อคกุญแจตู้เอกสาร

DFD



RoPA

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)

ม.39 (3)	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์ติดต่อ
ผู้ควบคุมข้อมูล (DC)			abc@gmail.com	
เจ้าที่หน้าที่คุ้มครองข้อมูล (DPO)			xyz@gmail.com	
ตัวแทน DC				

แผนก:	ABC	ม.39(1)		ม.39(2)	ม.39(4)	ม.39(5)				ม.39(6)				ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล ทั่วไป	ข้อมูลส่วนบุคคล อ่อนไหว	วัตถุประสงค์แยกประเภท (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิ์ในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล ทั่วไป	ฐานประมวลผลข้อมูล อ่อนไหว	เปิดเผยไปยังหน่วยงานในฯ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไปยัง ตปท. ตปท.	มาตรการการทำมาตรการรักษาความมั่นคงปลอดภัย ม.37(1) Confidentiality	Integrity	Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ, ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กฎแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอกำลังคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไขสิทธิอ่านเท่านั้น	สแกนเก็บไว้

การทำ Data Inventroy Mapping (DIM)

รายละเอียดรายการ

กิจกรรม: กิจกรรมหลัก และกิจกรรมย่อย

การเก็บรวบรวม: วัตถุประสงค์, ข้อมูลส่วนบุคคล, ฐานกฎหมาย, เจ้าของข้อมูล, แหล่งที่มา, เอกสารที่ใช้, ประกาศความเป็นส่วนตัว

สร้างการยอมรับ: เกี่ยวข้องกับกฎหมายมาตราใด (มีโทษทางปกครอง ปรับไม่เกิน 1, 3 หรือ 5 ล้านบาท)

กิจกรรม			เก็บรวบรวม (ม.19-26)																		
			ข้อมูล (เท่าที่จำเป็น, ม.22)		วัตถุประสงค์ (ม.21,27)	ฐานกฎหมาย (ข้อยกเว้นที่ไม่ต้องขอความยินยอม		เจ้าของข้อมูล	ประเภทของเจ้าของข้อมูล (ม.20)					แหล่งที่มาของข้อมูล (ม.25)			เอกสารอ้างอิง (สัญญา/แบบฟอร์ม/ใบสมัคร/อื่นๆ)		ประกาศความเป็นส่วนตัว (ม.23)
			ทั่วไป (ม.24)	อ่อนไหว (ม.26)		ข้อมูลทั่วไป (ม.24)	ข้อมูลอ่อนไหว (ม.26)							เจ้าของข้อมูลโดยตรง	ข้อมูลที่อยู่ในองค์	แหล่งอื่น	กระดาษ	อิเล็กทรอนิกส์	
No.	กระบวนการหลัก	กระบวนการย่อย	ข้อมูลเกี่ยวกับบุคคล ที่ทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เว้นแต่ผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ สกุล เลขบัญชี ที่อยู่เลขทะเบียนผู้เสียภาษี ฯลฯ)	ข้อมูลที่มีความเสี่ยงต่อเจ้าของข้อมูลส่วนบุคคลตามกฎหมายบัญญัติ เชื้อชาติ/การเมือง/ศาสนา/สิทธิ ปรัชญา/พฤติกรรมทางเพศ/อาชญากรรม/สุขภาพ/ความพิการ/สหภาพแรงงาน/พันธุกรรม/ชีวภาพ/อื่นๆ		- ระงับอันตราย - สัญญา - อำนาจรัฐ - ประโยชน์โดยชอบ - กฎหมาย - จดหมายเหตุ	- ระงับอันตราย - มูลนิธิ, สมาคม - เปิดเผยโดยสาธารณะของเจ้าของข้อมูล - ก่อตั้งสิทธิ - กฎหมายการแพทย์, สาธารณสุข, คุ้มครองแรงงาน, ศึกษาวิจัย, ประโยชน์สาธารณะที่สำคัญ	บุคคล/กลุ่มบุคคลที่เป็นเจ้าของข้อมูล เช่น ผู้สมัครงาน, พนักงาน, ผู้มาติดต่อ, ลูกค้า, ผู้รับจ้าง เป็นต้น	บรรลุนิติภาวะ	ผู้เยาว์ไม่เกิน 10 ปี	ผู้เยาว์เกิน 10 ปี	ไร้ความสามารถ	เสมือนไร้ความสามารถ	เจ้าของข้อมูลโดยตรง	ระบบที่บริษัทใช้, แผนกอื่นส่งข้อมูลให้, ระบบอื่นๆ	ระบบ website, social media, สื่อสาธารณะ, บุคคลคนอื่น ฯลฯ	ชื่อเอกสาร	ชื่อไฟล์	แจ้งประกาศความเป็นส่วนตัวหรือไม่, วิธีการใด เช่น ประกาศบนหน้าเว็ปไ Y= แจ้ง N = ไม่แจ้ง
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ. ศาสนา	คัดเลือกเข้าทำงาน	สัญญา	กฎหมาย	ผู้สมัครงาน	Y	-	-	-	-	Y	-	-	แบบฟอร์มสมัครงาน	-	N

การทำ DIM (ต่อ)

รายละเอียดรายการ (ต่อ)

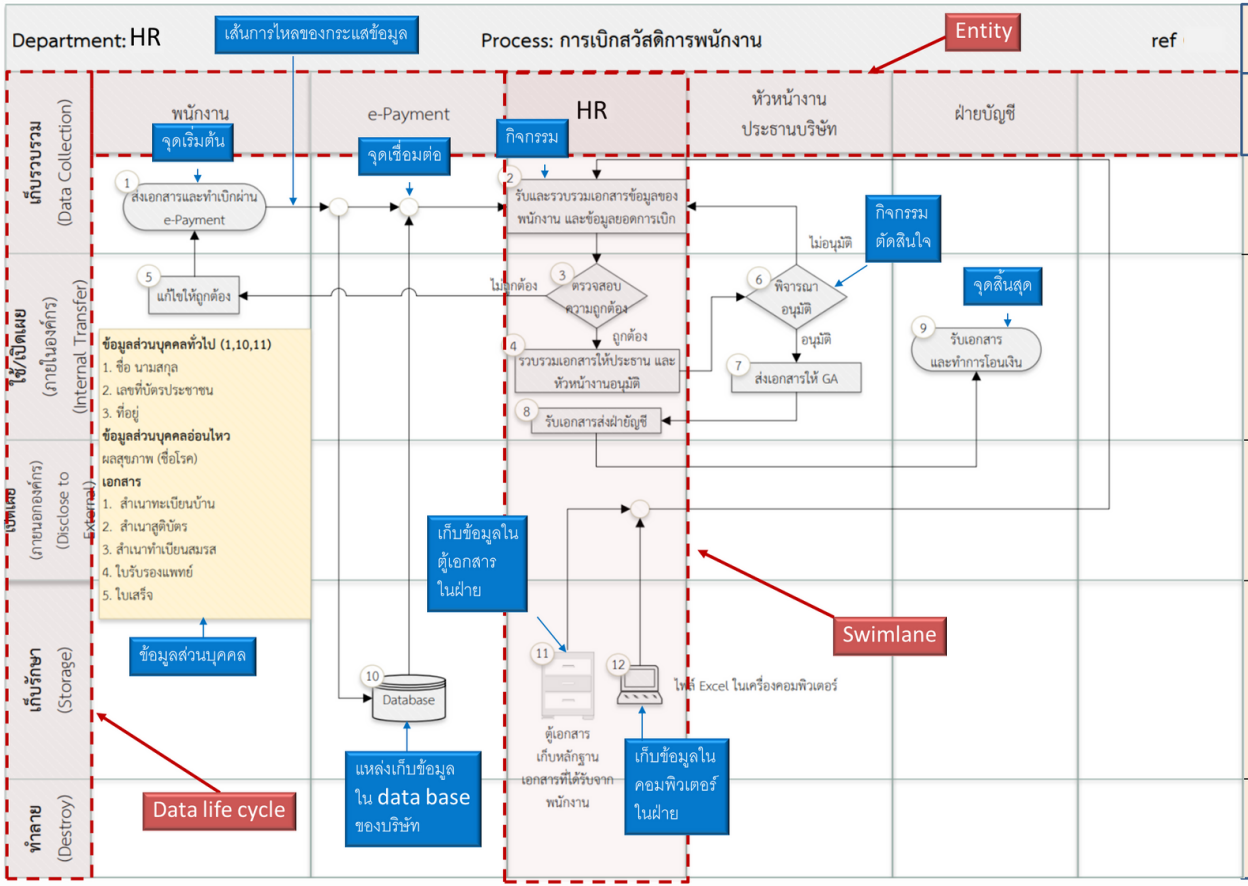
การใช้-เปิดเผย-ส่งโอน: ภายในองค์กร, ภายนอกองค์กร, ส่งโอนไปต่างประเทศ

การเก็บรักษา และทำลาย: อุปกรณ์ หรือระบบ, ผู้มีสิทธิ-วิธีการ-สิทธิการเข้าถึง-เงื่อนไขการเข้าถึง, ระยะเวลาจัดเก็บ, วิธีลบทำลาย

มาตรการ: มาตรการเชิงองค์กร, เชิงเทคนิค, เชิงกายภาพ (ในการรักษาความลับ, ความถูกต้อง, ความพร้อมใช้)

ใช้/เปิดเผย/ส่ง-โอน (ม.27-29)								การเก็บรักษา และทำลาย (ม.37(3),39(5))							มาตรการรักษาความมั่นคงปลอดภัย (ม.37(1),39(8))		
ใช้ (ในองค์กร)			เปิดเผย (นอกองค์กร)		ส่ง-โอน (ต่างประเทศ)			ทั้งรูปแบบกระดาษ และ อิเล็กทรอนิกส์							เชิงองค์กร / เชิงเทคนิค / เชิงกายภาพ		
ใช้เฉพาะในหน่วยงาน	หน่วยงานอื่น		บุคคล นิติบุคคล		ให้บุคคล/นิติบุคคลอื่น (ม.28)		ใช้ในเครือกิจการ (ม.29)	อุปกรณ์และระบบที่จัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ระยะเวลาการจัดเก็บ	เกณฑ์อ้างอิงระยะเวลาจัดเก็บ	วิธีการลบทำลาย ทำให้ไม่สามารถระบุตัวบุคคลได้	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้อง (Integrity)	การรักษาความพร้อมใช้ (Availablity)
	ส่งต่อแบ่งปันให้หน่วยงานอื่นในองค์กร ระบุชื่อหน่วยงานในองค์กรที่ได้รับข้อมูล	วัตถุประสงค์ (ม.21)	เปิดเผยไปให้บุคคลหรือนิติบุคคลอื่นภายนอกองค์กร ระบุชื่อประเภทบุคคลหรือนิติบุคคล	วัตถุประสงค์ (ม.21, 27)	ประเทศปลายทางมีมาตรฐานคุ้มครองข้อมูลที่เพียงพอหรือไม่	วัตถุประสงค์ (ม.21,28)	มีนโยบายการส่งโอนข้อมูลในเครือกิจการที่รับรองโดย สคส. หรือไม่										
Y	แผนกที่ขอกำลังคนเข้าทำงาน	คัดเลือก	-	-	-	-	-	ตู้เอกสาร	HR	อ่าน	กุญแจ	ผู้รับผิดชอบแต่เพียงผู้เดียว	6 เดือน	รอผลการคัดเลือก	เครื่องย่อยกระดาษ	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไขสิทธิอ่านเท่านั้น	ล็อคกุญแจตู้เอกสาร

การทำ Data Flow Diagram (DFD)

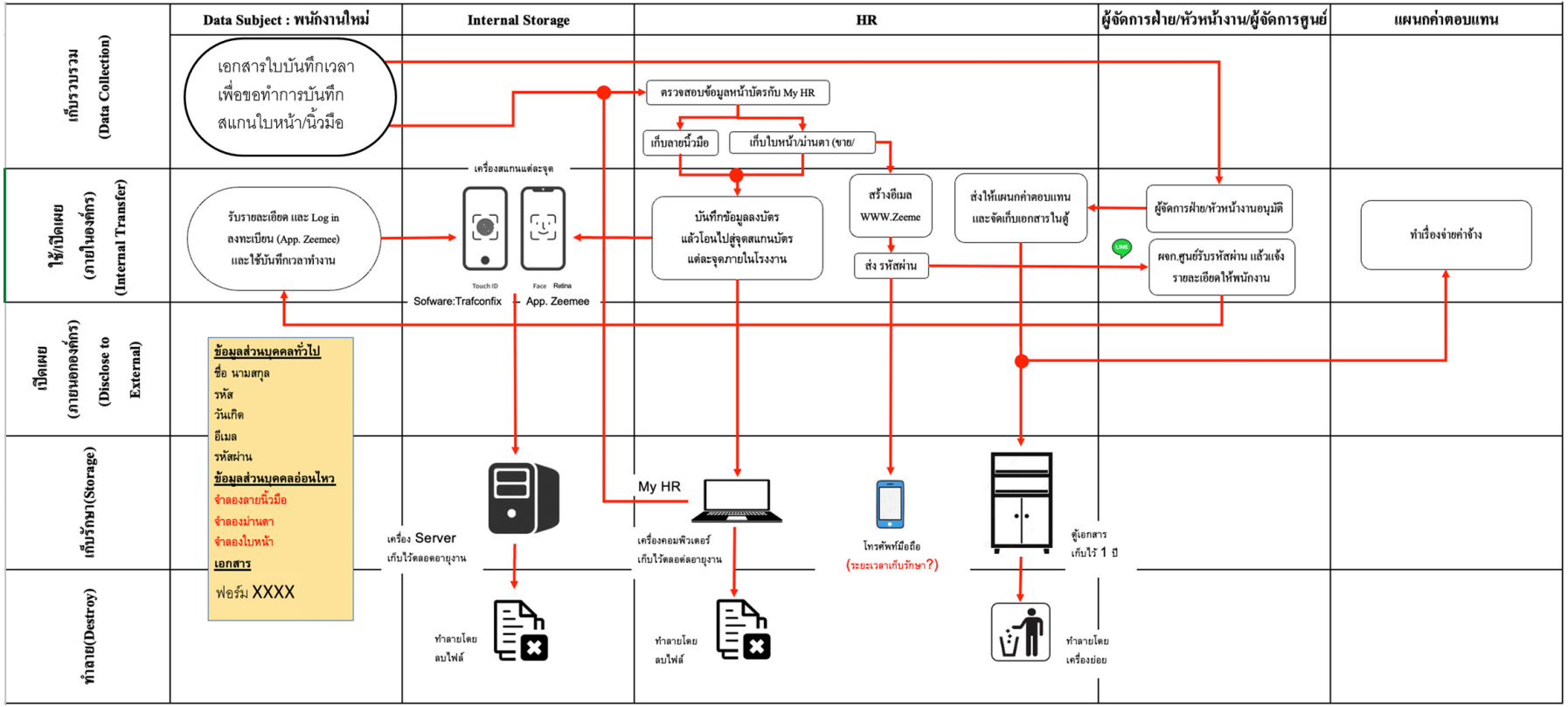


ตรวจสอบจุดอ่อน-รูรั่ว

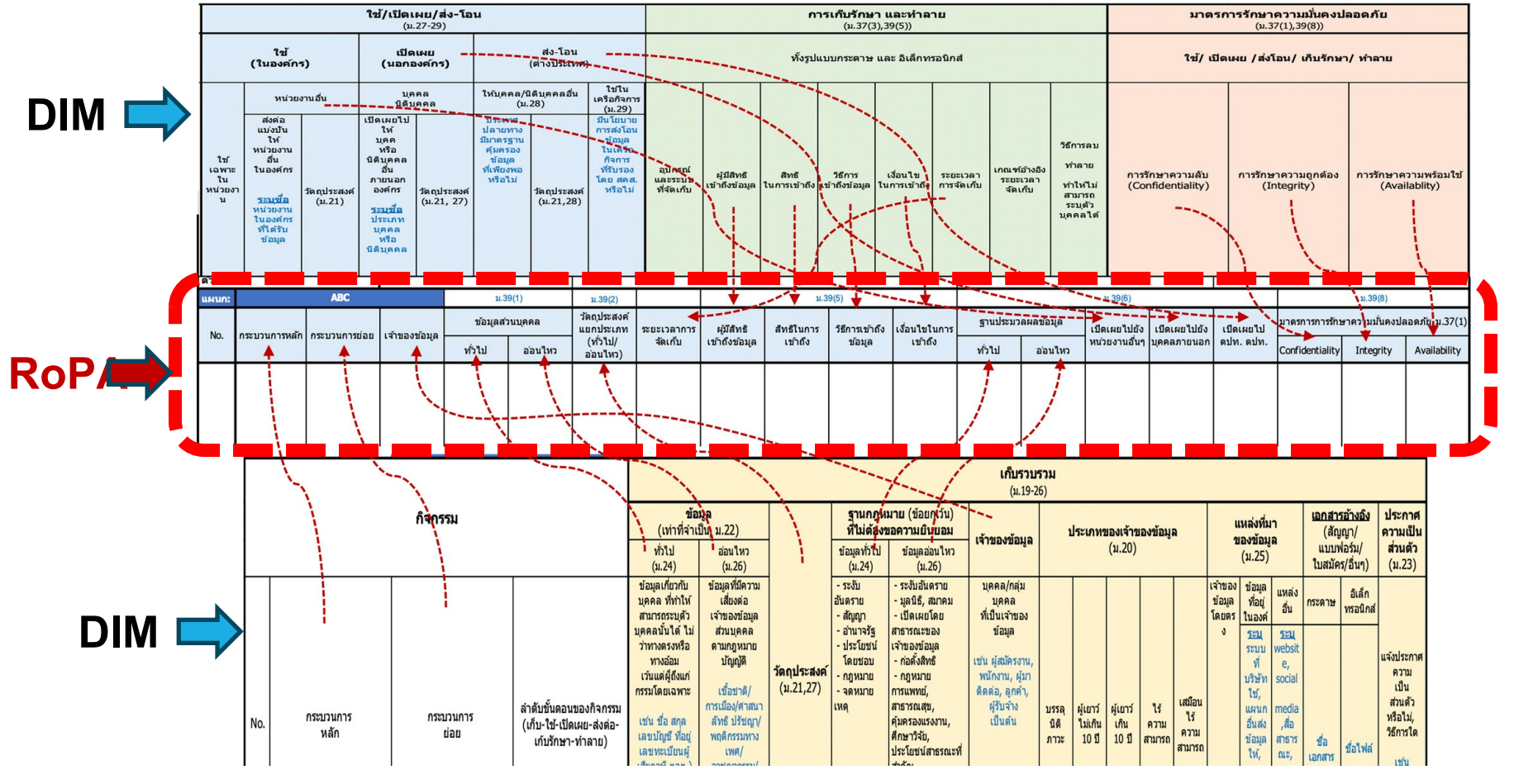
Privacy	Security Measure
❑ Privacy notice ❑ Data minimization ❑ Lawful basic	Confidentiality Integrity Availablity
❑ Follow Privacy notice (Follow objectives)	
❑ DSA ❑ DPA ❑ BCR ❑ NDA	
❑ Storage limitation ❑ Sources of storage ❑ Inspection method	
❑ Disposal method	

ตัวอย่าง DFD

ตัวอย่าง กิจกรรมการขอทำบันทึกเวลาทำงาน



การทำ Record of Processing Activities (RoPA)



บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)

ม.39 (3)	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์ติดต่อ
ผู้ควบคุมข้อมูล (DC)			abc@gmail.com	
เจ้าที่หน้าที่คุ้มครองข้อมูล (DPO)			xyz@gmail.com	
ตัวแทน DC				

แผนก:	ABC			ม.39(1)		ม.39(2)	ม.39(4)	ม.39(5)				ม.39(6)					ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล		วัตถุประสงค์แยกประเภท (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล		เปิดเผยไปยังหน่วยงานอื่นๆ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไป ตปท. ตปท.	มาตรการการรักษาความมั่นคงปลอดภัย ม.37(1)		
				ทั่วไป	อ่อนไหว							ทั่วไป ม.24 (consent)	อ่อนไหว ม.26 (consent)				Confidentiality	Integrity	Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ. ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กุญแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอก่อตั้งคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไข มีสิทธิอ่านเท่านั้น	สแกนเก็บไว้

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ตัวอย่าง RoPA สำหรับ DC

Record of Processing Activities (RoPA) for Processor

ข้อมูลผู้ประมวลผลข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี) (ข้อ 3 (1))		ผู้ประมวลผลข้อมูลส่วนบุคคล	ตัวแทน (ถ้ามี)
	ชื่อ-สกุล/ชื่อองค์ก		
	ที่อยู่		
	อีเมล		
	เบอร์โทรศัพท์		
	DPO (ข้อ 3 (3))	ชื่อ	
		สถานที่ติดต่อ	
		วิธีการติดต่อ	

ข้อมูลผู้ควบคุมข้อมูลส่วนบุคคลและตัวแทน (ถ้ามี) (ข้อ 3 (2))	สัญญาเลขที่/อ้างอิง	ข้อมูลส่วนบุคคล (ข้อ 3 (4))		วัตถุประสงค์ (ข้อ 3 (4))	ประเภท หรือลักษณะการประมวลผล (ตามคำสั่งของ DC) (ข้อ 3 (4))	ประเภทบุคคล/หน่วยงานที่ได้รับข้อมูล ใน ตปท. (ข้อ 3 (5))	มาตรการรักษาความมั่นคงปลอดภัย (ข้อ 3 (6))
		ทั่วไป	อ่อนไหว				
บริษัท... ที่อยู่... เบอร์.....อีเมล.....	xxx.....	ชื่อ เพศ อายุ	...		....	....	....
		....	....		....	....	....

จากสัญญา DPA

ข้อ ๓ ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) ชื่อและข้อมูลเกี่ยวกับผู้ประมวลผลข้อมูลส่วนบุคคล และตัวแทนของผู้ประมวลผลข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๒) ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น และตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีการแต่งตั้งตัวแทน

(๓) ชื่อและข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงสถานที่ติดต่อและวิธีการติดต่อ ในกรณีที่ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(๔) ประเภทหรือลักษณะของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งรวมถึงข้อมูลส่วนบุคคลและวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล

(๕) ประเภทของบุคคลหรือหน่วยงานที่ได้รับข้อมูลส่วนบุคคล ในกรณีที่มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(๖) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๔๐ วรรคหนึ่ง (๒)

ผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งเป็นลายลักษณ์อักษร โดยจะจัดทำเป็นหนังสือหรือ

ตัวอย่าง RoPA สำหรับ DP

การรักษา RoPA ให้ทันสมัย สอดคล้องกับกฎหมายอย่างต่อเนื่อง

✓ ทบทวนของเดิม (กิจกรรมเดิม)

- <u>เป็นระยะ</u> ตามรอบเวลา (เช่น ทุก 1 ปี, ก่อนการตรวจประเมินภายใน หรือภายนอก)
- เมื่อ**<u>มีการเปลี่ยนแปลง</u>** ตามเกณฑ์ที่กำหนด (เช่น ภายใน 1 เดือน)
- เมื่อ**<u>เกิดเหตุการละเมิด</u>** (ที่มีความเสี่ยง)
- **<u>ได้รับคำแนะนำ</u>** เมื่อตรวจพบจากกิจกรรมตรวจติดตามภายใน หรือภายนอก
  - DPO แนะนำ หรือตรวจสอบพบ
  - ทีมตรวจติดตามภายใน หรือภายนอกตรวจสอบพบ

ตัวอย่างชื่อกิจกรรม RoPA

แผนก HR (Human Resources)

Process	Purpose	Personal Data	Data Subject
Recruitment Management	รับสมัครและคัดเลือกพนักงาน	Name, CV, Education, Experience	ผู้สมัครงาน
Employee Management	บริหารข้อมูลพนักงาน	Name, ID number, Address, Phone	พนักงาน
Payroll Management	จ่ายเงินเดือนและสวัสดิการ	Salary, Bank Account, Tax ID	พนักงาน
Employee Performance Evaluation	ประเมินผลการทำงาน	Performance records	พนักงาน
Employee Welfare Management	จัดสวัสดิการพนักงาน	Health data, Family information	พนักงาน

แผนก Marketing

Process	Purpose	Personal Data	Data Subject
Marketing Campaign Management	ทำการตลาดและโปรโมชั่น	Name, Email, Phone	ลูกค้า
Customer Database Management	จัดการฐานข้อมูลลูกค้า	Contact information	ลูกค้า
Newsletter Distribution	ส่งข่าวสารและโปรโมชั่น	Email	ลูกค้า
Event Registration	ลงทะเบียนเข้าร่วมกิจกรรม	Name, Phone, Email	Event Participants
Customer Satisfaction Survey	สำรวจความพึงพอใจ	Feedback, Contact data	ลูกค้า

แผนก Sales

Process	Purpose	Personal Data	Data Subject
Customer Relationship Management	บริหารความสัมพันธ์ลูกค้า	Name, Phone, Email	ลูกค้า
Sales Order Processing	ดำเนินการขายสินค้า	Contact data, Address	ลูกค้า
Quotation Management	จัดทำใบเสนอราคา	Name, Company, Email	ลูกค้า
Contract Management	จัดทำและเก็บสัญญา	Name, Signature, Contact info	ลูกค้า
Customer Communication	ติดต่อประสานงานลูกค้า	Phone, Email	ลูกค้า

แผนก Finance / Accounting

Process	Purpose	Personal Data	Data Subject
Billing Management	ออกใบแจ้งหนี้	Name, Address, Tax ID	ลูกค้า
Payment Processing	รับและตรวจสอบการชำระเงิน	Bank account, Payment data	ลูกค้า
Tax Reporting	จัดทำรายงานภาษี	Tax ID, Financial records	ลูกค้า / พนักงาน
Vendor Payment	ชำระเงินให้คู่ค้า	Bank account, Contact data	Vendors
Expense Reimbursement	เบิกค่าใช้จ่ายพนักงาน	Bank account, Expense records	พนักงาน

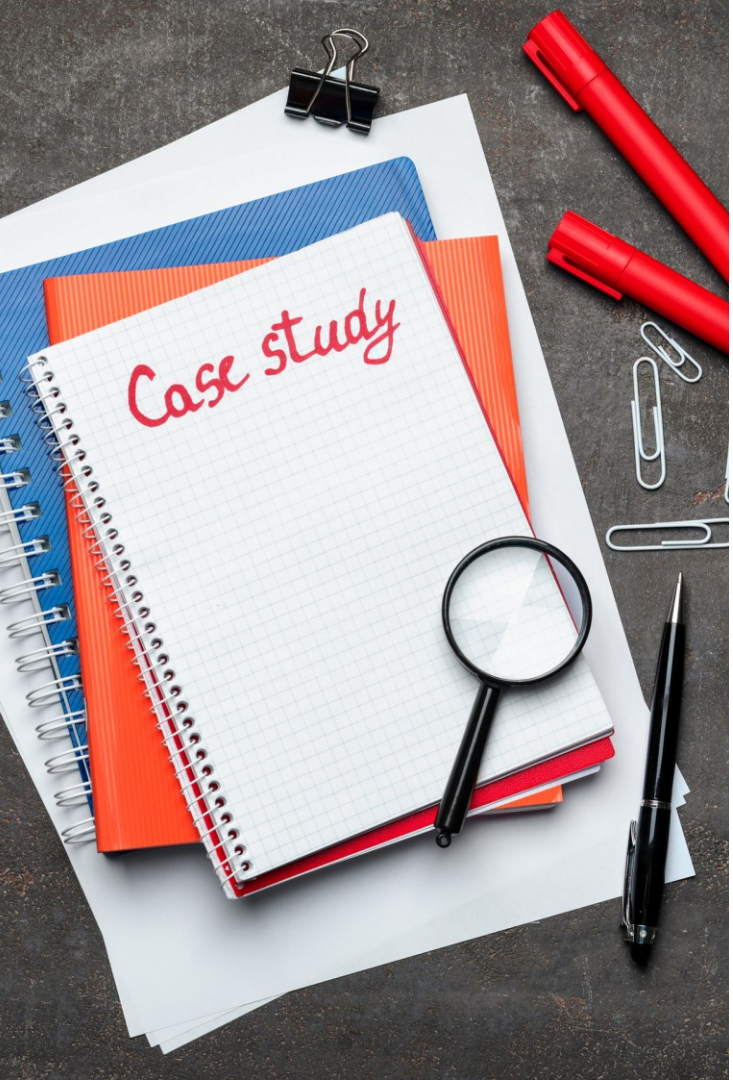
แผนก IT

Process	Purpose	Personal Data	Data Subject
User Account Management	จัดการบัญชีผู้ใช้งานระบบ	Name, Email, Username	พนักงาน
System Log Monitoring	ตรวจสอบความปลอดภัยระบบ	IP address, Login logs	พนักงาน / ผู้ใช้
IT Helpdesk Support	ให้บริการช่วยเหลือ IT	Name, Contact info	พนักงาน
Backup and Recovery	สำรองข้อมูลระบบ	Personal data from systems	ลูกค้า / พนักงาน
Network Security Monitoring	ป้องกันภัยไซเบอร์	IP address, Device ID	ผู้ใช้

แผนก Security / Facilities

Process	Purpose	Personal Data	Data Subject
CCTV Monitoring	ความปลอดภัยสถานที่	Video images	Visitors / พนักงาน
Visitor Management	ลงทะเบียนผู้มาติดต่อ	Name, ID card, Contact	Visitors
Access Control	ควบคุมการเข้าออก	ID card, Access logs	พนักงาน
Incident Reporting	รายงานเหตุการณ์ความปลอดภัย	Name, Incident data	พนักงาน / Visitors
Parking Management	จัดการที่จอดรถ	Vehicle number, Name	พนักงาน / Visitors

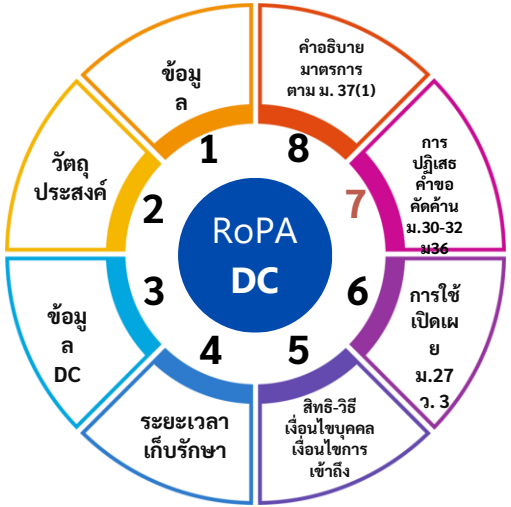
***** ไม่เขียนเป็นแผนก แต่เขียนกระบวนการ หรือกิจกรรมของแผนก *****



ตัวอย่าง การประยุกต์ใช้ RoPA

องค์กร ใช้ประโยชน์จาก RoPA ได้อย่างไร ?

RoPA ให้ข้อมูลอะไรกับองค์กร ?



- เก็บเกินจำเป็น ? => 3 ล้านบาท (ม.22)
- ตรงกับวัตถุประสงค์ ? => 3 ล้านบาท (ม.21)
- เก็บเกินระยะเวลาที่แจ้ง ? => 3 ล้านบาท (ม.37(3))
- ใครเข้าถึงได้บ้าง ? => 3 ล้านบาท (ม.37 (1))
- ใช้-เปิดเผย ไปที่ไหนบ้าง ? => 3, 5 ล้านบาท (ม. 26)
- มาตรการเหมาะสมหรือไม่ ? => 3 ล้านบาท (ม.37 (1))
- **ตรงกับที่แจ้ง Privacy notice หรือไม่ ?**

G	D	D	S
Gap analysis	Data Subject right	Data breach	Security measure

การประยุกต์ใช้ RoPA

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)

แผนก:	ABC			ม.39(1)		ม.39(2)	ม.39(4)	ม.39(5)				ม.39(6)					ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล		วัตถุประสงค์แยกประเภท (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล		เปิดเผยไปยังหน่วยงานอื่นๆ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไป ตปท. ตปท.	มาตรการการรักษาความมั่นคงปลอดภัย ม.37(1)		
				ทั่วไป	อ่อนไหว							ทั่วไป	อ่อนไหว				Confidentiality	Integrity	Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ. ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กุญแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอกำลังคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไข มีสิทธิอ่านเท่านั้น	สแกนเก็บไว้

การจัดการเหตุการละเมิด

- ประเมินความน่าเชื่อถือ
- แก้ไขระงับห้องกันเหตุ
- ประเมินความเสี่ยง
- แจ้งเหตุการละเมิดแก่ สคส.
- ทบทวนมาตรการ

การจัดการสิทธิ

- เข้าถึง-สำเนา, แก้ไข
- คัดค้าน, ระงับ
- ลบทำลาย
- ถอนความยินยอม
- ร้องเรียน

การตรวจประเมินภายใน

- ศึกษากระบวนการ
- หาความเสี่ยง
- หา Gap
- ใช้เป็นหลักฐาน

ประกาศความเป็นส่วนตัว

- กลุ่มใดบ้างที่ต้องแจ้ง
- นำรายละเอียดไปเขียน
- จัดกลุ่มเจ้าของข้อมูลแล้วเขียนเป็นฉบับเดียว
- ใช้ตรวจสอบความทันสมัย

Workshop

- **จงลงบันทึกรายการกิจกรรมการประมวลผลข้อมูล**

"กิจกรรมการรับสมัครพนักงานใหม่ เพื่อพิจารณาสอบสัมภาษณ์"

โดยมีรายละเอียดดังต่อไปนี้ ด้วยแบบฟอร์มที่กลุ่มออกแบบ

แผนก HR ในกิจกรรม**สรรหาพนักงานใหม่** เพื่อพิจารณา**สัมภาษณ์**ในตำแหน่ง เจ้าหน้าที่ด้าน IT โดยมีการเก็บข้อมูลดังต่อไปนี้ คือ ชื่อ, ที่อยู่, วุฒิการศึกษา, วันเกิด, ศาสนา, งานอดิเรก, กีฬาที่ถนัด, สถานะสมรส, ชื่อคู่สมรส, ชื่อบิดา-มารดา, น.น., ส่วนสูง, ยาที่แพ้, อาหารที่แพ้, โรคประจำตัว, พรรคการเมืองที่เป็นสมาชิก โดยผู้สมัครกรอกข้อมูลในกระดาษ, พร้อมเอกสารประกอบได้แก่ สำเนาบัตร ปชช., สำเนาทะเบียนบ้าน, สำเนาวุฒิการศึกษา,รูปถ่ายขนาด 2 นิ้ว 2 รูป, เอกสารเปลี่ยนชื่อ (ถ้ามี), สำเนาเอกสารประวัติการทำงาน, บุคคลอ้างอิง พร้อมเบอร์ติดต่อ และอีเมล

มีการกำหนดเก็บเอกสารใบสมัครไว้ 10 ปี หลังสัมภาษณ์แล้ว โดยเอกสารใบสมัครงานจะถูกเก็บไว้ในตู้เอกสารในห้องทำงานของ HR และมีการสแกนเอกสารใบสมัครไว้ เพื่อเก็บในระบบ และเพื่อส่งอีเมลให้ผู้บริหาร และหัวหน้าฝ่าย IT ใช้เป็นข้อมูลในการสัมภาษณ์ โดย save ไฟล์สแกนไว้ในเครื่อง PC ของ HR ผู้รับผิดชอบงานนี้

ไฟล์สแกนที่ส่งให้นั้นต้องผู้ได้รับต้องลบหลังการสัมภาษณ์เสร็จภายใน 1 เดือน ซึ่งกำหนดในระเบียบแนวปฏิบัติในการลบทำลายข้อมูลของหน่วยงาน

ส่วนมาตรการรักษาความมั่นคงปลอดภัยทำโดยล็อคกุญแจตู้เอกสารเท่านั้น

บทกำหนดโทษ..ทางปกครอง

ไม่เกิน 1 ล้านบาท

มาตรา ๘๒ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๓ มาตรา ๓๐ วรรคสี่ มาตรา ๓๙ วรรคหนึ่ง มาตรา ๔๑ วรรคหนึ่ง หรือมาตรา ๔๒ วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๙ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๙ วรรคหก หรือไม่ปฏิบัติตามมาตรา ๒๓ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

มาตรา ๘๘ ตัวแทนผู้ควบคุมข้อมูลส่วนบุคคลหรือตัวแทนผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๓๙ วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๓๙ วรรคสอง และมาตรา ๔๑ วรรคหนึ่ง ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๔๑ วรรคสี่ ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ไม่เกิน 3 ล้านบาท

มาตรา ๘๖ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๔๐ โดยไม่มีเหตุอันควรหรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา ๓๗ (๕) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๓๘ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้

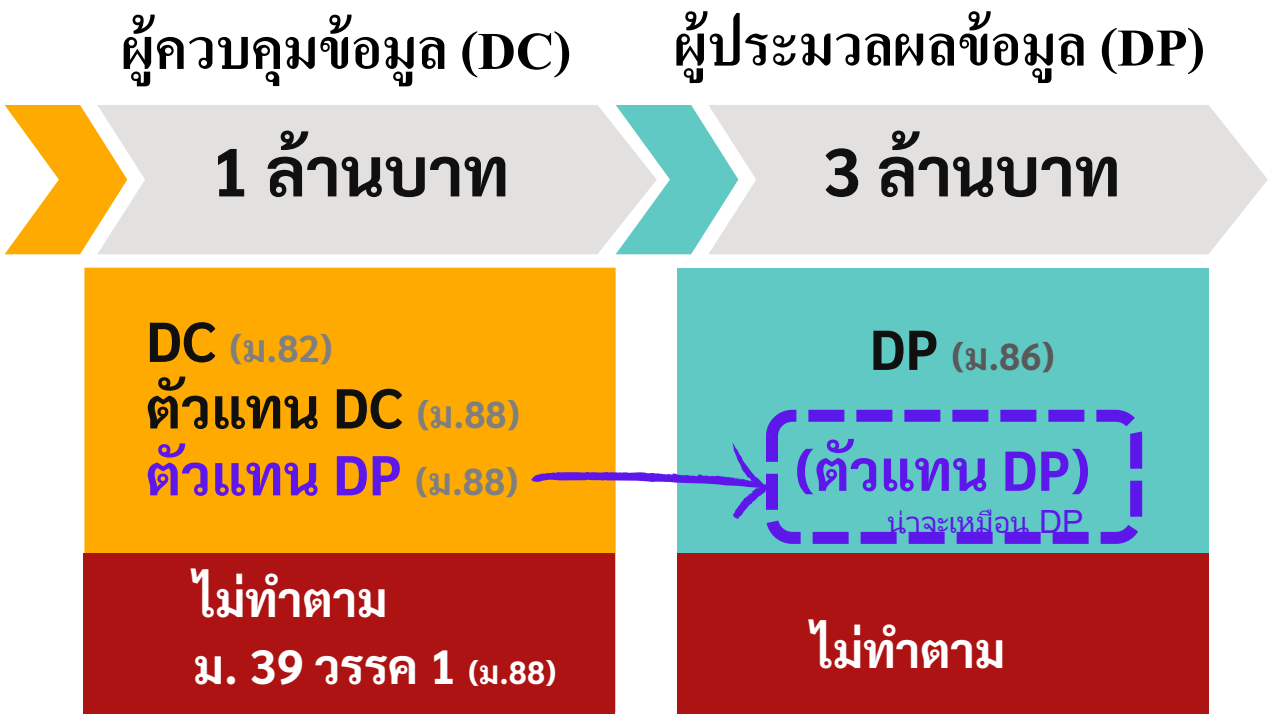
(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

(๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ข้อสังเกต

- ม.40 ไม่พูดถึงตัวแทน DP ว่าต้องทำ RoPA ตาม วรรค 1 (3) โดยอนุโลม
- ม.88 DP ผู้ใดไม่ปฏิบัติตาม ม.39 วรรค 1 => ปรับไม่เกิน 1 ล้านบาท

บทกำหนดโทษ..ทางปกครอง



บันทึกรายการกิจกรรมการประมวลผลข้อมูลระหว่าง **GDPR** กับ **PDPA**

PDPA (ประเทศไทย)

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

GDPR ไม่ระบุ

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

GDPR (สหภาพยุโรป)

ข้อ 30 GDPR: บันทึกกิจกรรมการประมวลผลข้อมูล

1. **DC และผู้แทน (ถ้ามี)** ต้องเก็บ RoPA ที่อยู่ภายใต้ความรับผิดชอบของตน โดยต้องมีข้อมูลดังนี้

(a) ชื่อและข้อมูลติดต่อของ DC และ**DC ร่วม**, ผู้แทน DC และ **DPO** (ถ้ามี)

(b) วัตถุประสงค์

(c) คำอธิบายของหมวด**หมู่ของ DS** และหมวดหมู่ของข้อมูล

(d) **หมวดหมู่ของผู้รับข้อมูล หรือจะได้รับข้อมูล รวมถึงผู้รับใน ตปท.**

(e) หากมีการโอนข้อมูลไป ตปท. ให้**ระบุชื่อประเทศหรือนิติบุคคล**นั้น **พร้อมเอกสารแสดงมาตรการคุ้มครองที่เหมาะสม**

(f) ระยะเวลาที่วางแผนไว้สำหรับการลบข้อมูลในแต่ละหมวดหมู่;

(g) คำอธิบายเกี่ยวกับมาตรการเชิงเทคนิคและองค์กร

2. DP และผู้แทน (ถ้ามี) ต้องเก็บ RoPA ทุกประเภทที่ดำเนินการในนาม DC ต้องมีรายละเอียดดังนี้

(a) ชื่อและข้อมูลติดต่อของ DP และ DC แต่ละราย รวมถึงตัวแทนของ DC หรือ DP (ถ้ามี) และ DPO

(b) หมวดหมู่ของกิจกรรมการประมวลผลที่ดำเนินการในนาม DC แต่ละราย

(c) การโอนข้อมูลไป ตปท. ต้องระบุชื่อประเทศหรือนิติบุคคล พร้อมแสดงมาตรการคุ้มครองที่เหมาะสม

(d) คำอธิบายเกี่ยวกับมาตรการเชิงเทคนิคและองค์กร

3. บันทึกต้องจัดทำเป็นลายลักษณ์อักษร ซึ่งรวมถึงในรูปแบบอิเล็กทรอนิกส์ได้ด้วย

4. DC หรือ DP หรือ ผู้แทน (ถ้ามี) ต้องจัดเตรียมบันทึกให้แก่หน่วยงานกำกับดูแลเมื่อได้รับการร้องขอ

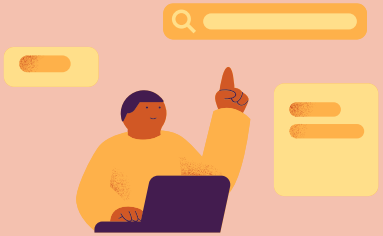
5. **ข้อ 1 และ2 ไม่บังคับใช้กับกิจการหรือองค์กรที่มีพนักงานน้อยกว่า 250 คน** และ ยกเว้นในกรณีที่

- มีแนวโน้มที่จะก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของ DS
- ไม่ใช่การประมวลผลแบบครั้งคราว
- ประมวลผลข้อมูลพิเศษ
- ประมวลผลข้อมูลเกี่ยวกับความผิดทางอาญาหรือการลงโทษทางอาญา

ข้อควรระวัง... สำหรับ RoPA

เนื้อหา

- ใช้แบบฟอร์ม แพลตฟอร์มไม่สมบูรณ์
- บันทึกรายละเอียดผิด
- ลงไม่ครบทุกกิจกรรม/ ลงเป็นแผนก



ขาดการตรวจสอบ

- ไม่ได้กำหนดเงื่อนไขการตรวจสอบ
- มีการเปลี่ยนแปลง-เพิ่ม แต่ไม่แก้ไขตาม
- ผู้เกี่ยวข้องไม่ได้อบรม (พนง.ใหม่,โอนย้าย)
- **RoPA กับ Privacy notice ไม่ตรงกัน**

ขาดความเข้าใจ

- **DPO ทำเอง**
- **ไม่ทราบความสำคัญ** ผลกระทบ
- **ไม่ได้ใช้ประโยชน์**จาก RoPA
- ซื้อแพลตฟอร์มที่ยังไม่สอดคล้อง

แบบที่ 1

39(6) 39(7)

ตัวอย่างที่ 1 บันทึกรายการประมวลผลข้อมูล [131]

ส่วนที่1 ผู้ควบคุมข้อมูล				
	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์โทรศัพท์
ผู้ควบคุมข้อมูล 39(3)				
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)				

ส่วนที่ 2 บันทึกรายการประมวลผลข้อมูล [132]

หน้าที่ (business function)	วัตถุประสงค์ในการประมวลผลข้อมูล 39(2)	ชื่อและข้อมูลติดต่อผู้ควบคุมข้อมูลร่วมกัน (joint controller) ถ้ามี	ประเภทของเจ้าของข้อมูล	ประเภทของข้อมูลส่วนบุคคล 39(1)	ประเภทของบุคคลอื่นที่ข้อมูลอาจจะเปิดเผยไป	สัญญาประมวลผลข้อมูลและผู้ประมวลผลข้อมูล (ถ้ามี)	การโอนข้อมูลไปยังต่างประเทศ (ถ้ามี)	มาตรการคุ้มครองกรณีโอนข้อมูลไปต่างประเทศ (ถ้ามี)	ระยะเวลาการเก็บรักษาข้อมูล 39(4)	คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย 39(8) สิทธิในการเข้าถึง 39(5)
งานบุคคล	การรับสมัครพนักงาน	ไม่มี	ผู้สมัครที่ได้รับคัดเลือก	ข้อมูลติดต่อ คุณสมบัติ ประวัติการจ้างงาน	ไม่มี	ไม่มี	ไม่มี	ไม่มี	10 ปีหลังสิ้นสุดสัญญาจ้าง	การเข้ารหัส และการควบคุมการเข้าถึงโดยคนที่มีหน้าที่ในงานบุคคลเท่านั้น
งานขาย	การทำการตลาดตรง (direct marketing)	ไม่มี	ลูกค้าปัจจุบัน	ข้อมูลติดต่อ ประวัติการซื้อ					เก็บไว้ตลอดระยะเวลาที่เป็นลูกค้าปัจจุบัน	การเก็บและการส่งแบบเข้ารหัส พนักงานฝ่ายการตลาดที่มีส่วนเกี่ยวข้องเท่านั้นสามารถเข้าถึงได้

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

แบบที่ 2

ตัวอย่าง บันทึกรายการ (Record of Processing Activities: ROPA) สำหรับผู้ควบคุมข้อมูลส่วนบุคคล

ส่วนที่ 1: ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล	
ผู้ควบคุมข้อมูลส่วนบุคคล	
ชื่อ-สกุล/ชื่อองค์กร	บริษัท เจ้าป่าเดอะแคท จำกัด
ที่อยู่	565 ซอยรามคำแหง 39 แขวงพลับพลา เขตจตุจักร กรุงเทพฯ 10310
อีเมล	jaopaa@thecat.com
เบอร์โทรศัพท์	XX-XXX-XXX
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) (ถ้ามี)	
ชื่อ-สกุล	คุณต้นสน รักไดโนเสาร์
ที่อยู่	566 ซอยรามคำแหง 40 แขวงพลับพลา เขตจตุจักร กรุงเทพฯ
อีเมล	cooper@thedog.com
เบอร์โทรศัพท์	XX-XXX-XXX

39(3)

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ส่วนที่ 2: บันทึกรายการ

รายละเอียดทั่วไปของการประมวลผลข้อมูลส่วนบุคคล (เก็บรวบรวม ใช้ เปิดเผย)					มาตรการรักษาความมั่นคงปลอดภัย ตามมาตรา 37 (1)
ชื่อกิจกรรม	วัตถุประสงค์	ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม	การใช้ / เปิดเผย	ระยะเวลา	มาตรการรักษาความปลอดภัย
คำอธิบาย: ชื่อกิจกรรมอาจตั้งขึ้นจากรูปแบบการประกอบธุรกิจหรือลักษณะของกิจกรรมที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	คำอธิบาย: การกำหนดวัตถุประสงค์หลักของกิจกรรมจะต้องพิจารณาว่ามีการทำกิจกรรมการประมวลผลเพราะอะไร ซึ่งโดยทั่วไปแล้วกิจกรรมหนึ่งจะมีวัตถุประสงค์เพียงวัตถุประสงค์	คำอธิบาย: ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ควรระบุ - หมวดหมู่ของข้อมูลส่วนบุคคล - กลุ่มของบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล	คำอธิบาย: อธิบายลักษณะการใช้ข้อมูลส่วนบุคคลดังกล่าว หรือการเปิดเผยข้อมูลส่วนบุคคล โดยการอ้างอิงว่าในแต่ละกิจกรรมมีการอาศัยฐานการปฏิบัติตามกฎหมายในมาตรา 24 หรือมาตรา 26	คำอธิบาย: การระบุระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลนั้นเพื่อให้ทราบว่าข้อมูลส่วนบุคคลจะถูกจัดเก็บไว้เป็นระยะเวลานานเพียงใด	คำอธิบาย: ระบุมาตรการรักษาความปลอดภัย
ตัวอย่าง: การจัดเก็บประวัติผู้สมัครงาน	ตัวอย่าง: เพื่อใช้ในการพิจารณาคุณสมบัติผู้สมัครงาน	ตัวอย่าง: ข้อมูลระบุตัวตน และข้อมูลการติดต่อของผู้สมัครเป็นพนักงาน	ตัวอย่าง: ใช้ในการพิจารณาคุณสมบัติผู้สมัครงาน ตามฐานสัญญา (มาตรา 24 (3))	ตัวอย่าง: 3 ปี หลังจากการยื่นใบสมัคร	ตัวอย่าง: การกำหนดสิทธิเข้าถึง (access control) เฉพาะเจ้าหน้าที่ฝ่ายบุคคลและผู้บริหาร
ตัวอย่าง: การจัดเก็บฐานข้อมูลลูกค้า	ตัวอย่าง: เพื่อใช้ในการให้บริการกับลูกค้า	ตัวอย่าง: ข้อมูลระบุตัวตน เบอร์โทร ที่อยู่ ข้อมูลการให้บริการแก่ลูกค้า	ตัวอย่าง: ใช้ในการให้บริการตามฐานสัญญา (มาตรา 24 (3))	ตัวอย่าง: 10 ปี	ตัวอย่าง: การกำหนดสิทธิเข้าถึง (access control) / การจัดเก็บแบบเข้ารหัส (encrypted storage)

การใช้สิทธิ		หมายเหตุ
สิทธิของเจ้าของข้อมูลส่วนบุคคล	การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	
คำอธิบาย: การระบุสิทธิของเจ้าของข้อมูลส่วนบุคคลในกรณีจะเป็นไปตามหมวด 3 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล	คำอธิบาย: การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลอาจจะระบุโดยการทำลิงก์เชื่อมโยงใน Excel ไป sheet อื่นที่ลงรายละเอียดการปฏิเสธสิทธิในกิจกรรมนั้นแต่ละครั้ง	
ตัวอย่าง: สิทธิขอแก้ไขข้อมูล ฯลฯ	ตัวอย่าง: sheet 2	

39(1) 39(2) 39(4) 39(5) 39(6) 39(7) 39(8)

หมายเหตุ ในการจัดทำตารางบันทึกรายการ ผู้ประกอบการควรจะจัดทำตารางเป็นแนวนอนเชื่อมต่อกันไประหว่าง 1) รายละเอียดทั่วไปของการประมวลผลข้อมูลส่วนบุคคล 2) มาตรการรักษาความมั่นคงปลอดภัย 3) การใช้สิทธิ และ 4) หมายเหตุ

คำถามที่พบบ่อย

1. แผนกอื่นต้องมาทำร่วมกันไหม เพราะ RoPA เขียนไปถึงแผนกอื่นด้วย
2. ควรทบทวน RoPA ตอนไหนดี
3. ต้องมีการอนุมัติ RoPA หรือไม่
4. หลังกิจกรรมยกเลิกแล้ว ต้องเก็บ RoPA ไว้อีกนานเท่าไร
5. กิจกรรมไหนต้องเขียน RoPA บ้าง
6. การส่งอีเมลต้องเขียน RoPA การส่งอีเมลด้วยหรือไม่
7. การใช้โปรแกรม Excel กรอกข้อมูล ต้องเขียน RoPA หรือไม่

แบบฟอร์ม RoPA

บันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)

ม.39 (3)	ชื่อ-สกุล/ชื่อองค์กร	ที่อยู่	อีเมล	เบอร์ติดต่อ
ผู้ควบคุมข้อมูล (DC)			abc@gmail.com	
เจ้าที่หน้าที่คุ้มครองข้อมูล (DPO)			xyz@gmail.com	
ตัวแทน DC				

แผนก	ชื่อหน่วยงาน	ม.39(1)		ม.39(2)	ม.39(4)	ม.39(5)				ม.39(6)					ม.39(8)		
No.	กระบวนการหลัก	กระบวนการย่อย	เจ้าของข้อมูล	ข้อมูลส่วนบุคคล		วัตถุประสงค์นอกประเทศ (ทั่วไป/อ่อนไหว)	ระยะเวลาการจัดเก็บ	ผู้มีสิทธิเข้าถึงข้อมูล	สิทธิในการเข้าถึง	วิธีการเข้าถึงข้อมูล	เงื่อนไขในการเข้าถึง	ฐานประมวลผลข้อมูล		เปิดเผยไปยังหน่วยงานอื่นๆ	เปิดเผยไปยังบุคคลภายนอก	เปิดเผยไป ตปท. องค์กร	มาตรการ ม.37(1) เชิงองค์กร/เทคนิค/กายภาพ		
				ทั่วไป	อ่อนไหว							ทั่วไป	อ่อนไหว				รักษาความลับ Confidentiality	รักษาความถูกต้อง Integrity	รักษาความพร้อมใช้ Availability
1	สรรหาบุคลากร	สมัครด้วยตัวเอง	ผู้สมัครงาน	ชื่อ, ที่อยู่, อายุ, วุฒิการศึกษา, เบอร์ติดต่อ, อีเมล, บุคคลอ้างอิง	เชื้อชาติ, ศาสนา	คัดเลือกเข้าทำงาน	6 เดือน	HR	อ่าน	กุญแจ	ผู้รับผิดชอบเท่านั้น	สัญญา	กฎหมาย	แผนกที่ขอคำสั่งคน	-	-	ล็อคกุญแจตู้เอกสาร	กฎระเบียบห้ามแก้ไข มีสิทธิอ่านเท่านั้น	สแกนเก็บไว้
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0


ANY QUESTIONS?

DATA SECURITY for PDPA

Organizational Measures

- Access Policies
- Employee Training

Technical Measures

- Encryption
- Regular Security Audi

Physical Measures

- Secure Facilities

มาตรา 37 (1), (2), (3)

ทุกระดับ และผู้ปฏิบัติงานที่เกี่ยวข้อง

มาตรา ๓๗ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระยะแรกที่กฎหมายมีผลใช้บังคับมีความเหมาะสม

มาตรการรักษาความมั่นคงปลอดภัย ม.37 (1)

ความมั่นคงปลอดภัย คือ
การธำรงไว้ซึ่ง
ความลับ (Confidentiality)
ความถูกต้อง (Integrity)
ความพร้อมใช้ (Availability

ข้อ 3

วัตถุประสงค์ เพื่อ ป้องกัน
สูญหาย, เข้าถึง, ใช้เปลี่ยนแปลง, แก้ไข, เปิดเผย โดยปราศจากอำนาจ

ต้องครอบคลุม
เอกสาร/ อิเล็กทรอนิกส์/อื่นๆ

ข้อ 4 วรรค 1 ช่วงท้าย, 4 (1)

ต้องประอบด้วยมาตรการ
- เชิงองค์กร
- เชิงเทคนิค
- เชิงกายภาพที่จำเป็น

โดยมาตรการ ต้องคำนึงถึง
- ระดับความเสี่ยง
- ตามลักษณะการประมวลผล
- โอกาสเกิด และผลกระทบ จากเหตุการณ์ละเมิด

ข้อ 4 (2)

โดยคำนึงกึง การดำเนินการ
ระบุความเสี่ยงที่สำคัญ
ทรัพย์สินสารสนเทศที่สำคัญ, การป้องกัน, การตรวจสอบ, การเฝ้าระวังภัย, การเผชิญหน้า, การรักษา และฟื้นฟู

ข้อ 4 (3)

เหมาะสมตามระดับความเสี่ยง
- ปัจจัยทางเทคโนโลยี
- บริบทสภาพแวดล้อม
- มาตรฐานที่ยอมรับสำหรับหน่วยงาน หรือกิจการประเภทเดียวกัน หรือใกล้เคียงกัน

ข้อ 4 (4)

ระบบอิเล็กทรอนิกส์
- ครอบคลุมส่วนประกอบต่างๆของระบบการ
- คำนึงถึงการป้องกันเชิงลึก ที่ควรประกอบด้วยการป้องกันหลายชั้น

ข้อ 4 (5)

มาตรการควบคุมการเข้าถึง
ก) หลักสิทธิเท่าที่จำเป็น
ข) จัดการสิทธิการเข้าถึง
ค) กำหนดหน้าที่รับผิดชอบ
ง) จัดให้มีวิธีการตรวจสอบย้อนหลัง

ข้อ 4 (6)

ความตระหนักรู้
(Privacy & Security awareness)
- แจ้งนโยบาย
- แนวปฏิบัติ
- มาตรการด้านการคุ้มครองข้อมูล
- การรักษาความมั่นคงปลอดภัย รวมถึงกรณีการปรับปรุงแก้ไข

ข้อ 4 (7)

ทบทวนมาตราการ
- เมื่อเทคโนโลยีเปลี่ยนแปลงไป
- ระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี
- บริบท สภาพแวดล้อม
- มาตรฐานที่เป็นที่ยอมรับในประเภทเดียวกัน
- วัตถุประสงค์การประมวลผล
- ทรัพยากรที่ใช้ และความเป็นไปได้ประกอบกัน

เมื่อมีเหตุการณ์ละเมิด ให้ถือว่ามีความจำเป็นต้องทบทวน เว้นแต่ การละเมิดดังกล่าวไม่มีความเสี่ยงต่อเจ้าของข้อมูล

ข้อ 5

ในข้อตกลงการประมวลผล (DPA)
- กำหนดให้ DP มีมาตรการรักษาความมั่นคงปลอดภัย เป็นไปตามมาตรฐานขั้นต่ำตามข้อ 4
- กำหนด ให้ DP แจ้งให้ทราบถึงเหตุการละเมิดที่เกิดขึ้น

ข้อ 6

ในข้อตกลงการประมวลผล (DPA)
กฎหมายอื่นมีมาตรการ รักษาความมั่นคงปลอดภัยที่เหมาะสมแล้ว ให้ดำเนินการ ตามกฎหมายนั้น
แต่ต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศนี้ด้วย

ข้อ 7

ข้อ 3. ในประกาศนี้ “ความมั่นคงปลอดภัย” หมายความว่า การธำรงไว้ ซึ่ง

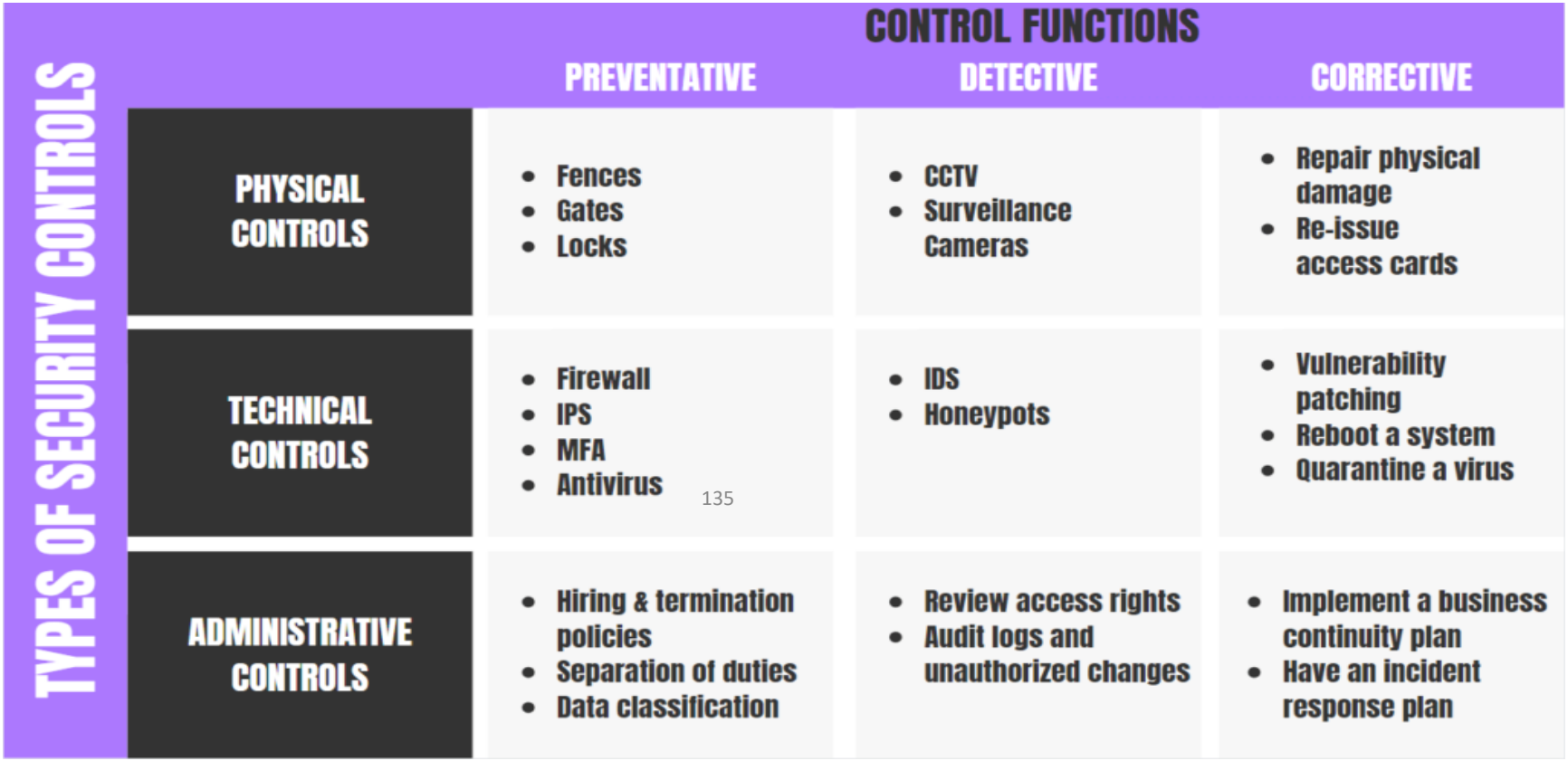
1. ความลับ (Confidentiality)

2. ความถูกต้องครบถ้วน (Integrity) และ

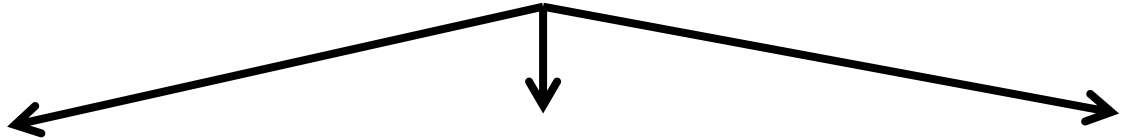
3. สภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกัน

• การสูญหาย • เข้าถึง • ใช้ • เปลี่ยนแปลง • แก้ไข หรือ • เปิดเผย

ข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ


TYPES OF SECURITY CONTROLS
CONTROL FUNCTIONS
PREVENTATIVE
DETECTIVE
CORRECTIVE
PHYSICAL CONTROLS
Fences
Gates
Locks
CCTV
Surveillance Cameras
Repair physical damage
Re-issue access cards
TECHNICAL CONTROLS
Firewall
IPS
MFA
Antivirus
IDS
Honeypots
Vulnerability patching
Reboot a system
Quarantine a virus
ADMINISTRATIVE CONTROLS
Hiring & termination policies
Separation of duties
Data classification
Review access rights
Audit logs and unauthorized changes
Implement a business continuity plan
Have an incident response plan

มาตรา 37(1) และกฎหมายลำดับรอง



มาตรการเชิงองค์กร

- ข้อตกลงและเงื่อนไขการจ้างงาน
- กระบวนการทางวินัย
- ความรับผิดชอบหลังสิ้นสภาพ/เปลี่ยนงาน
- อบรม และสร้างความตระหนัก
- กำหนดขั้นตอนการทำงานที่ชัดเจน
- ทำข้อตกลง NDA, DSA, DPA
- การคืนทรัพย์สิน
- นโยบาย
- ขั้นตอนการทำงาน

มาตรการเชิงเทคนิค

- การเข้ารหัสข้อมูล
- การสำรองข้อมูล
- การตรวจสอบและบันทึกกิจกรรม
- การป้องกันไวรัส และมัลแวร์
- การอัพเดทซอฟต์แวร์
- การจัดการช่องโหว่
- การบันทึกกิจกรรม
- การพิสูจน์ตัวตน
- การทำให้เป็นข้อมูลนิรนาม
- การแฝงข้อมูล

มาตรการเชิงกายภาพ

- การควบคุมการเข้าถึงสถานที่
- ติดตั้งกล้องวงจรปิด
- รักษาความปลอดภัยอุปกรณ์
- ป้องกันจากภัยธรรมชาติ
- การทำลายข้อมูลอย่างปลอดภัย
- การป้องกันการบุกรุก
- จัดเก็บโต๊ะทำงาน และจัดการหน้าจอ
- ระบบสาธารณูปโภคสนับสนุน
- การบำรุงรักษาอุปกรณ์

Org Control 37
People Control 8

Technical Control 34

Physical Control 14

ISO27002:2022 (93 Controls)

การประเมินระดับความเสี่ยง

5x5 Risk Matrix Example

			Severity (Impact to Data Subject)				
			ไม่มีผลกระทบ	ไม่สะดวกเล็กน้อย	ไม่สะดวกมีผลตามมา	ถูกเปิดเผยถูกสวมรอย	ผลต่อชีวิต/อนามัยสิทธิ/เสรีภาพ
			ต่ำมาก (1)	ต่ำ (2)	พอสมควร (3)	สูง (4)	สูงมาก (5)
Likelihood	มีข้อบ่งชี้คาดว่ามีความเป็นไปได้สูงที่จะเกิดในระยะเวลาอันใกล้นี้ (10 ครั้ง/ปี ขึ้นไป)	สูงมาก (5)	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
	มีข้อบ่งชี้คาดว่าจะเกิดในระยะเวลาอันใกล้นี้ (7-9 ครั้ง/ปี)	สูง (4)	Low 4	Medium 8	High 12	Very High 16	Extreme 20
	มีข้อบ่งชี้ว่าจะเกิดในระยะเวลาอันใกล้ (4-6 ครั้ง/ปี)	พอสมควร (3)	Low 3	Medium 6	Medium 9	High 12	Very High 15
	พอจะเป็นไปได้แต่ไม่มีข้อบ่งชี้/ไม่มีข้อพิสูจน์ได้ว่าจะเกิดในระยะเวลาอันใกล้ (1-3 ครั้ง/ปี)	ต่ำ (2)	Very low 2	Low 4	Medium 6	Medium 8	High 10
	ห่างไกล/ไม่อาจเป็นไปได้ (น้อยกว่า 1 ครั้ง/ปี)	ต่ำมาก (1)	Very low 1	Very low 2	Low 3	Low 4	Medium 5

Risk level criteria Example

Risk Level	Point
Extreme	20-25
Very High	15-16
High	10-12
Medium	5-9
Low	3-4
Very low	1-2

เกณฑ์ยอมรับ (ตัวอย่าง)

Very low: *ยอมรับได้โดยไม่ต้องดำเนินการใด ๆ เพิ่มเติม*

Low: *ยอมรับได้โดยไม่ต้องดำเนินการเพิ่มเติม หรืออาจมีการตรวจสอบสถานการณ์เป็นระยะ ๆ*

Medium: *ควรพิจารณาดำเนินการเพื่อลดความเสี่ยงบางส่วน เช่น การเพิ่มมาตรการรักษาความปลอดภัย หรือการฝึกอบรมพนักงานเพิ่มเติม*

High: *ต้องดำเนินการเพื่อลดความเสี่ยงโดยทันที เช่น การปรับปรุงหรือเปลี่ยนแปลงระบบการรักษาความปลอดภัย หรือการเปลี่ยนวิธีการดำเนินงานที่เกี่ยวข้อง*

Very high: *ต้องมีการดำเนินการเพื่อลดความเสี่ยงทันที และอาจต้องพิจารณาทางเลือกใหม่ในการดำเนินการ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้*

Extreme: *ต้องดำเนินการเพื่อลดความเสี่ยงทันที อาจต้องระงับกิจกรรมจนกว่าจะมีมาตรการที่เพียงพอ*

ประเมินความเสี่ยง: โอกาสเกิดการละเมิดข้อมูล

หลักเกณฑ์โอกาสที่จะเกิด (Likelihood criteria)				
1 = ต่ำมาก	2 = ต่ำ	3 = พอสมควร	4 = สูง	5 = สูงมาก
ห่างไกล และไม่อาจเป็นไปได้ (rare)	พอจะเป็นไปได้ แต่ไม่มีข้อบ่งชี้/ข้อพิสูจน์ได้ว่าจะมีโอกาสที่จะเกิดในระยะเวลาอันใกล้ (unlikely)	มีข้อบ่งชี้ว่ามีโอกาสเกิดขึ้นได้ในระยะเวลาอันใกล้ (moderate)	มีข้อบ่งชี้ที่คาดว่าจะเกิดในระยะเวลาอันใกล้นี้ (likely)	• มีข้อบ่งชี้ว่ามีความเป็นไปได้สูงที่จะเกิดในระยะเวลาอันใกล้นี้ • 99.99% (almost certain)

ประเมินความเสี่ยง: ความร้ายแรง (ผลกระทบต่อเจ้าของข้อมูล)

ผลความร้ายแรง (Severity criteria)				
1 = ต่ำมาก	2 = ต่ำ	3 = พอสมควร	4 = สูง	5 = สูงมาก
ไม่มีผลกระทบต่อ data subject	• DS อาจประสบกับความไม่สะดวกเล็กน้อย • แม้จะไม่มีข้อบ่งชี้ว่าจะเกิดความเสียหายร้ายแรงที่ส่งผลกระทบในด้านการเงิน หรือเสียชื่อเสียงของ data subject	• DS จะประสบกับความไม่สะดวกบางประการ หรือผลตามมา • แม้จะมีข้อบ่งชี้ว่าสามารถก้าวข้ามหรือฟื้นฟูความเสียหายได้ในระยะเวลาอันสั้น	• ถูกเปิดเผย ข้อมูลส่วนบุคคล ที่ต้องคุ้มครองตามมาตรฐานวิชาชีพ • ถูกสวมรอยบุคคล (Identify Theft) ส่งผลให้เกิดความเสียหายทางด้านการเงิน ชื่อเสียง	DS ประสบกับร้ายแรง • ต่อชีวิต/ ต่ออนามัย • ต่อสิทธิ/ ต่อเสรีภาพ โดยมีข้อบ่งชี้ว่า DS • จะเกิดความเสียหายอย่างต่อเนื่อง • ไม่สามารถดำเนินงานได้ตามปกติยืดเยื้อ • ไม่สามารถจัดการปัญหาดังกล่าวได้

มาตรการลดความเสี่ยง

แนวทางในการพิจารณามาตรการ

- ✓ พิจารณาทาเลือกในการลดความเสี่ยง
- ✓ เลือกมาตรการประเภทใด ใน 4 แบบ (เลี่ยง, โยน, ลด, รับ)
- ✓ มาตรการดังกล่าว ลดระดับความเสี่ยงได้เพียงใด
- ✓ ทางเลือกที่เหมาะสม และจะผ่านการอนุมัติ

มาตรา 37(1) และกฎหมายลำดับรอง

มาตรการเชิงองค์กร

- เก็บข้อมูลเท่าที่จำเป็น
- ไม่เก็บข้อมูลที่มีความเสี่ยง
- ลดระยะเวลาการเก็บรักษา
- ลดขอบเขตการประมวลผล
- อบรม และสร้างความตระหนัก
- กำหนดขั้นตอนการทำงานที่ชัดเจน
- ทำข้อตกลง NDA, DSA, DPA
- การตรวจสอบภายใน
- ตั้งทีมบริหารความเสี่ยง

มาตรการเชิงเทคนิค

- การเข้ารหัสข้อมูล
- การควบคุมการเข้าถึง
- การสำรองข้อมูล
- การตรวจสอบและบันทึกกิจกรรม
- การป้องกันไวรัสและมัลแวร์
- การอัปเดตซอฟต์แวร์
- การควบคุมการใช้งานอุปกรณ์พกพา
- การตรวจสอบช่องโหว่
- การป้องกันหลายชั้น

มาตรการเชิงกายภาพ

- การควบคุมการเข้าถึงสถานที่
- ติดตั้งกล้องวงจรปิด
- รักษาความปลอดภัยอุปกรณ์
- ป้องกันจากภัยธรรมชาติ
- การทำลายข้อมูลอย่างปลอดภัย
- การป้องกันการบุกรุก

RISK MITIGATION STRATEGIES

1. **Risk Avoidance:**
   Elimination of risk by Avoiding risky activities
2. **Risk Transfer:**
   Shifting of risks to third parties and reducing impact
3. **Risk Reduction:**
   Controlling risk occurrence Probability or its impact
4. **Risk Acceptance:**
   Acknowledging the risks that come along a decision or activity

ภาพรวมมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ ม.37(1)

DC มีหน้าที่จัดให้มีมาตรการ (อย่างน้อย)[4]

วัตถุประสงค์: ป้องกันการสูญหาย เข้าถึง[3],[4] ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย โดยปราศจากอำนาจ หรือโดยมิชอบ

CIA

ความมั่นคงปลอดภัย คือ [3]
ธำรงไว้ซึ่ง: ความลับ (C)
ความถูกต้อง (I)
ความพร้อมใช้ (A)

มาตรการ

เชิง: องค์กร[4-2] เทคนิค กายภาพ
เท่าที่จำเป็น[4-3]
ระดับความเสี่ยง[4-2]
ความสามารถ[4-4]

ตามระดับความเสี่ยง ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการ ประกอบกัน[4-3]

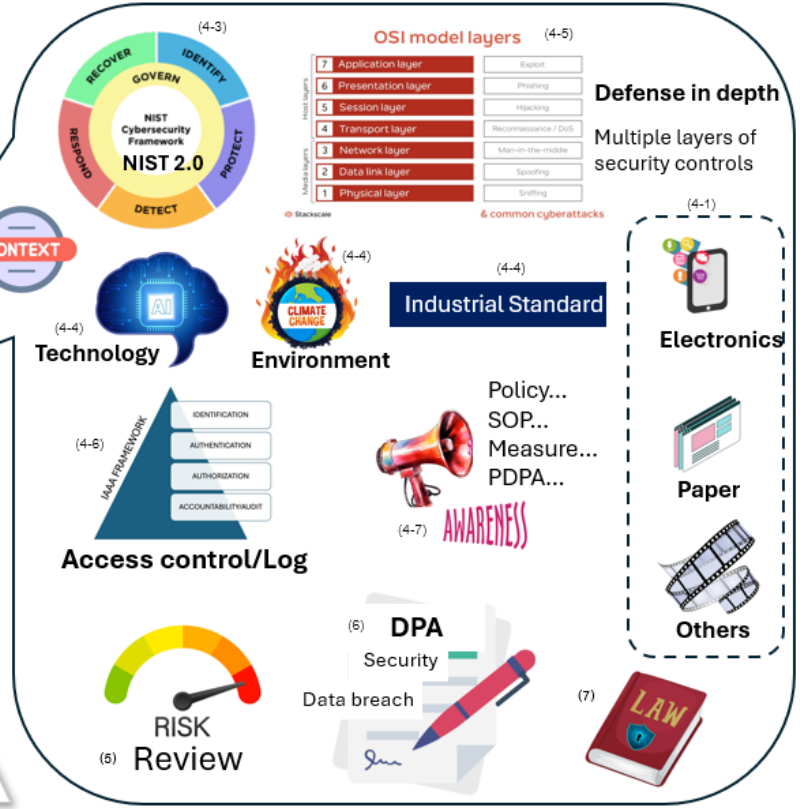
ความเสี่ยง

ระดับความเสี่ยง:[4-2]
- ตามลักษณะการประมวลผล
- โอกาส **X** ผลกระทบ **=** ระดับความเสี่ยง

กิจกรรม

ประมวลผลข้อมูลส่วนบุคคล:[4-1]
กระดาษ, อิเล็กทรอนิกส์, รูปแบบอื่นๆ
อิเล็กทรอนิกส์: ฮาร์ดแวร์, ซอฟต์แวร์

ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล[4-2]



โดย: อ.ณัฏฐ์ ธนวนกุล

สรุป PDPA สำหรับ AI: Privacy by Design

ใส่ PDPA ตั้งแต่ “ตอนออกแบบระบบ AI” ไม่ใช่มาแก้ทีหลัง

1 ฝัง PDPA ตั้งแต่ต้น (Design Stage)

- คิดเรื่อง Data Protection ตั้งแต่ออกแบบระบบ
- ไม่ใช่รอให้ระบบเสร็จแล้วค่อยมาแก้

2 เก็บข้อมูล “เท่าที่จำเป็น” (Data Minimization)

- ใช้ข้อมูลให้น้อยที่สุดเท่าที่ทำงานได้
- หลีกเลี่ยงการ dump data หรือเก็บเผื่ออนาคต

3 ใช้เทคนิคปกป้องข้อมูล (Privacy Enhancing)

- Anonymization ทำให้ระบุตัวไม่ได้
- Pseudonymization แทนค่า ลดความเสี่ยงการระบุตัวบุคคล

4 ตั้งค่า Privacy เป็นค่าเริ่มต้น (Privacy by Default)

- ระบบต้อง “ปลอดภัยตั้งแต่แรก”
- ไม่ใช่เปิดทุกอย่างแล้วให้ user ไปปิดเอง

5 Transparency & Control

- ตรวจสอบได้ (Audit ได้)
- อธิบายได้ (Explainable)
- ควบคุมได้ (Control)

มี Chat History มี Log การใช้งาน ตรวจสอบย้อนหลังได้

BEST PRACTICE (ควรทำ)

- ทำ Privacy by Design checklist ก่อนพัฒนา
- บังคับ Dev / Vendor ทำตาม
- ผูกกับ DPIA
- มี Log + Audit Trail ทุกระบบ AI

สรุป: ระบบ AI ที่ดี = ปลอดภัยตั้งแต่ Design + ใช้ข้อมูลน้อย + ตรวจสอบได้

4 หลักสำคัญของ AI Governance

1. **Transparency & Explainability** (โปร่งใส + อธิบายได้)
   ต้องทำให้: รู้ว่า AI ใช้ข้อมูลอะไร ใช้ไปทำอะไร
   โดยเฉพาะ: Automated decision ต้อง “อธิบายเหตุผลได้”
   ต้องมี Privacy Notice ครอบคลุม AI

2. **Accountability & Human Oversight** (รับผิดชอบ + มนุษย์กำกับ)
   องค์กรต้อง: ปฏิบัติตาม PDPA ครบ กำหนดบทบาทชัด
   (ใครรับผิดชอบอะไร) มีการตรวจสอบ / audit ได้
   ห้ามปล่อย AI ตัดสินใจล้วน ๆ ต้องมี Human-in-the-loop
   เช่น: ให้คน review ผลลัพธ์ AI มีระบบ override

3. **Fairness & Bias Mitigation** (ความเป็นธรรม + ลดอคติ)
   ต้อง: **ใช้ข้อมูลที่ “ถูกต้อง ครบ ไม่ลำเอียง” ป้องกัน AI เลือกปฏิบัติ**
   ข้อมูลอดีต = คนที่ได้ทุนส่วนใหญ่เป็น “บางคณะ” AI คิดว่า “คณะนี้ = สมควรได้ทุน”

4. **Security & Privacy** (ความมั่นคงปลอดภัย + ความเป็นส่วนตัว)
   ใช้ Privacy by Design & Default ใช้ PETs
   เช่น Anonymization Pseudonymization

ถ้านำ AI มาใช้ในมหาวิทยาลัย ต้องแก้ไขเอกสารใดบ้าง

(ร่าง) แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับ AI

(ร่าง) แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล
เกี่ยวกับการพัฒนาและใช้งานเทคโนโลยีปัญญาประดิษฐ์
Draft of Guidelines on Personal Data Protection in the Development and Use of Artificial Intelligence

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

วันที่ 13 มีนาคม 2569

Version 4.9.3

สารบัญ

แบบฟอร์มการประเมินผลกระทบการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

แบบฟอร์มการประเมินความเสี่ยงด้านข้อมูล (DPIA Form)

ขั้นตอนที่ 1: Identify the need for a DPIA

การระบุความจำเป็นในการทำ DPIA ตามประเภทของการประมวลผลข้อมูล หรือโครงการที่จะมีการประมวลผลข้อมูล ทั้งที่เป็นโครงการใหม่หรือที่มีการปรับปรุงเปลี่ยนแปลงการประมวลผลข้อมูลที่มีอยู่เดิม โดยระบุลักษณะที่แสดงถึงความจำเป็น รวมถึงแหล่งอ้างอิงที่เหมาะสม

Project ระบบคัดเลือกเจ้าหน้าที่ และประเมินผลผู้สมัครงานโดยใช้ AI

อ้างอิงตาม

ก. ประกาศหรือบัญชีรายชื่อการประมวลผลข้อมูลส่วนบุคคลของสำนักงานคุ้มครองข้อมูลส่วนบุคคลที่จำเป็นต้องจัดทำ DPIA

ข. แนวปฏิบัติเพื่อประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล [บันทึกลักษณะที่จำเป็นต้องจัดทำ DPIA]

- ☐ การประมวลผลในการให้คะแนน ประเมินผล โปรไฟลลิ่ง ทำนายคาดการณ์พฤติกรรม
- ☑ ใช้ระบบในการตัดสินใจโดยอัตโนมัติ ที่มีผลเกี่ยวเนื่องกับกฎหมาย
- ☐ การเฝ้าติดตามอย่างเป็นระบบ / การใช้ระบบในการตรวจสอบ โดยเจ้าของข้อมูลไม่ทราบว่าใครรับผิดชอบ และทำเพื่ออะไร
- ☐ ข้อมูลอันเกี่ยวกับข้อมูลอ่อนไหว
- ☐ การประมวลผลข้อมูลขนาดใหญ่
- ☐ การประมวลผลจากตั้งแต่ 2 กิจกรรมขึ้นไป เพื่อวัตถุประสงค์ที่แตกต่างกัน กระทำโดย DC คนละราย
- ☐ กลุ่มเป้าหมายที่เปราะบาง ผู้เยาว์ ผู้ไร้ความสามารถ หรือ เสมือนไร้ความสามารถ
- ☑ การประมวลผลข้อมูลด้วยนวัตกรรม หรือเทคโนโลยีใหม่
- ☐ เมื่อการประมวลผลโดยตัวมันเอง ที่ลดทอนสิทธิการเข้าถึง ไม่ให้ใช้สิทธิ์หรือใช้บริการหรือสัญญา

จากข้อมูลข้างต้น Project ดังกล่าว

- ☐ จำเป็น
- ☐ ไม่จำเป็นต้องทำ DPIA เนื่องจาก

ผู้รับรองกรณีไม่ต้องทำ DPIA ..... DPO

ขั้นตอนที่ 2: Describe the processing

อธิบายรายละเอียดของกระบวนการประมวลผลข้อมูลส่วนบุคคลอย่างน้อยต้องประกอบด้วย สภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล?

2.1 [Nature] อธิบายสภาพของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้

- ☐ วิธีการเก็บรวบรวมข้อมูล, การจัดเก็บข้อมูล
  แบบฟอร์มออนไลน์, การสัมภาษณ์
  การเก็บข้อมูลผ่านแบบฟอร์มออนไลน์และระบบ HRM
- ☐ การใช้ข้อมูล และผู้ที่สามารถเข้าถึงข้อมูล
  ใช้เพื่อคัดเลือกผู้สมัครและประเมินผลการปฏิบัติงาน
- ☐ ผู้ที่ได้รับข้อมูล
  ทีม HR และระบบ AI
- ☐ ผู้ประมวลผลข้อมูล
  ระบบ AI
- ☐ ระยะเวลาจัดเก็บข้อมูล
  2 ปี นับจากวันที่สิ้นสุดกระบวนการประเมิน
- ☐ มาตรการความปลอดภัย
  การเข้ารหัสข้อมูลและการควบคุมการเข้าถึง
- ☐ เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล
  AI สำหรับการวิเคราะห์ข้อมูลและการตัดสินใจ
- ☐ กระบวนการแบบใหม่ที่ใช้ในประมวลผลข้อมูล
  เทคโนโลยี AI
- ☐ ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล
  การประมวลผลข้อมูลด้วยเทคโนโลยีใหม่ และการตัดสินใจอัตโนมัติโดย AI

[บันทึกรายละเอียดสภาพของการประมวลผลข้อมูล]

DATA DELETION & D

AUDIT SYSTEM FOR PDPA

Ensure lawful deletion and verifiable destruction of pe
in accordance with PDPA requirements.

มาตรา 37 (3)

ทุกระดับ และผู้ปฏิบัติงานที่เกี่ยวข้อง

1 RETENTION EXPIRY CHECK

- System identifies personal data that has reached the retention period or deletion request.

2 DELETION APPROVAL

- Authorized officer reviews and approves deletion through a formal workflow.

3 SECURE DATA ERASURE

- Data is securely erased using appropriate methods based on storage type and medium.

4 CONFIRMATION & LOGGING

- The system automatically records a detailed deletion log.

5 INDEPENDENT VERIFICATION

- A separate reviewer validates that the data has been properly deleted.

6 FINAL RECORD & REPORTING

- A destruction record is generated and stored for audit and compliance.

KEY SAFEGUARDS

ROLE-BASED ACCESS CONTROL
Only authorized personnel can approve and execute deletion.

AUTOMATED RETENTION POLICY
System enforces deletion when the retention period expires.

SECURE DELETION METHODS
Use of encryption, wiping, or cryptographic erasure to prevent data recovery.

TAMPER-PROOF LOGS
Deletion logs are protected from alteration and unauthorized access.

AUDIT EVIDENCE EXAMPLES

DELETION LOG

Record ID: DEL-20250424-001
User ID: admin01
Date & Time: 24 Apr 2025 14:35:22
Data Category: Student Records
Method: Database Secure Erase
Status: Completed

DELETED

VERIFICATION REPORT

Verified by: DPO Office
Date: 24 Apr 2025

DESTRUCTION CERTIFICATE

Issued by IT Security Team
Date: 24 Apr 2025

BENEFITS

- Ensures compliance with PDPA data deletion requirements.
- Provides verifiable and traceable audit trails.
- Prevents unauthorized data retention.
- Strengthens data protection and trust.

ลบทำลาย (Storage limitation, Security)

แนวทางการเก็บรักษาและลบทำลายข้อมูลส่วนบุคคล

แนวทางการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคล

(Data Retention and Disposal Policy)

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 วรรค 2 ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม และระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่คาดหมายได้ตามมาตรฐานของการเก็บรวบรวม และมาตรา 37(3) ระบุว่าผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดำเนินระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา เมื่อไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ รวมถึงที่เจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ แนวทางการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคลนี้จัดทำขึ้น เพื่อเป็นแนวทางในการเก็บรักษาข้อมูลส่วนบุคคลในทรัพยากรต่าง ๆ ของมหาวิทยาลัยและผู้ให้บริการภายนอกที่เกี่ยวข้องในการเก็บรักษาและการลบทำลายข้อมูลส่วนบุคคลที่มหาวิทยาลัยมีการเก็บรวบรวมไว้ หรือเป็นผลตามการปฏิบัติตามการดำเนินงานให้มีความมั่นคงปลอดภัยและสอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทนิยาม

"มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยภัฏ.....

"การประมวลผลข้อมูลส่วนบุคคล" หมายความว่า การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ทั้งนี้ไม่รวมถึงข้อมูลของนิติบุคคลแม้บุคคลเป็นผู้ก่อตั้งด้วย

"ข้อมูลส่วนบุคคลอ่อนไหว" หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวมิติ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

"ผู้ให้บริการภายนอก" หมายความว่า บุคคลหรือนิติบุคคลที่ สป. มีข้อตกลงหรือสัญญากับมหาวิทยาลัยและมีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลคำสั่งของมหาวิทยาลัย

ข้อ 1. การกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (3) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม และระยะเวลาในการเก็บรวบรวมไว้ ดังนั้น มหาวิทยาลัยกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลแต่ละประเภท ดังนี้

ที่	ประเภทของข้อมูล	สื่อที่ใช้เก็บข้อมูล	ระยะเวลาการเก็บรักษา
1	ข้อมูลเจ้าหน้าที่และผู้บริหาร	- ฐานข้อมูล (Database)	- 10 ปีนับตั้งแต่สิ้นสภาพการเป็นเจ้าหน้าที่ หรือ
		- ระบบจัดเก็บข้อมูล (File Server)	- เท่าที่จำเป็นในการปฏิบัติงาน
		- เครื่องคอมพิวเตอร์ของผู้ปฏิบัติงาน (PC, Notebook)	- 60 สัปดาห์ หลังได้รับแจ้งวันพ้นสภาพการเป็นเจ้าหน้าที่
2	ข้อมูลส่วนบุคคลของผู้ใช้บริการขอใบอนุญาตประเภทใดประเภทหนึ่งที่อยู่ในอำนาจหน้าที่ของมหาวิทยาลัย และ สป. ตามที่กฎหมายกำหนด หรือหน่วยงานภาครัฐหรือผู้บริโภคหรือผู้รับบริการด้านอื่นๆ ที่มาขอใช้บริการจากมหาวิทยาลัย และ สป.	- ฐานข้อมูล (Database)	- ไม่เกิน 2 ปี หรือหลังจากผู้ใช้บริการไม่มีสิทธิและหน้าที่ใด ๆ กับ มหาวิทยาลัย และ สป. หรือสอดคล้องตามกฎหมายระเบียบ ข้อบังคับ และแนวปฏิบัติที่เกี่ยวข้อง
		- ระบบจัดเก็บข้อมูล (File Server)	- สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์
		- เครื่องคอมพิวเตอร์ของผู้ปฏิบัติงาน (PC, Notebook)	
		- กระดาษ (Paper)	- สอดคล้องตามกฎหมาย ว่าด้วยงานสารบรรณ หรือจนกว่าจะมีการแปลงข้อมูลให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์


ANY QUESTIONS?

Data Subject Rights Management for PDPA

มาตรา 19-20, 30-34,36,73, 95

ทุกระดับ และผู้ปฏิบัติงานที่เกี่ยวข้อง

ความสำคัญ และประโยชน์ ของการจัดการสิทธิ

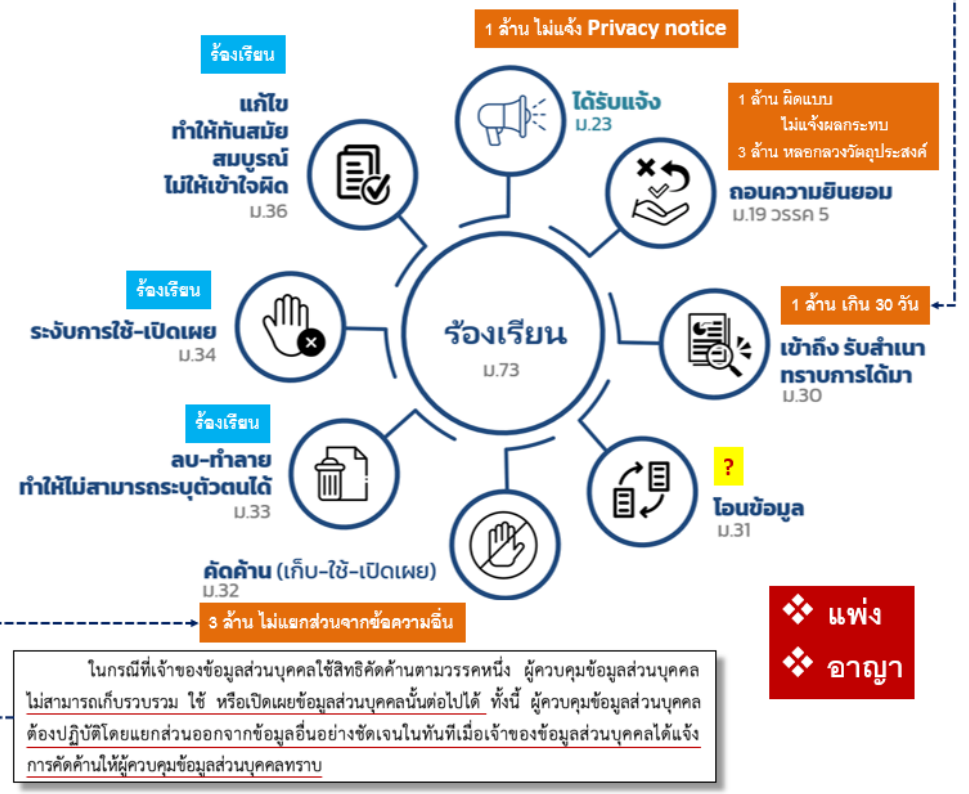
ส่วนที่ ๒
โทษทางปกครอง

มาตรา ๘๒ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๒๓ มาตรา ๓๐ วรรคสี่ มาตรา ๓๙ วรรคหนึ่ง มาตรา ๔๑ วรรคหนึ่ง หรือมาตรา ๔๒ วรรคสองหรือวรรคสาม หรือไม่ขอความยินยอมตามแบบหรือข้อความที่คณะกรรมการประกาศกำหนดตามมาตรา ๑๙ วรรคสาม หรือไม่แจ้งผลกระทบจากการถอนความยินยอมตามมาตรา ๑๙ วรรคหก หรือไม่ปฏิบัติตามมาตรา ๒๓ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาท

มาตรา ๘๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ มาตรา ๒๕ วรรคหนึ่ง มาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๘ มาตรา ๓๒ วรรคสอง หรือมาตรา ๓๗ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา ๒๑ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

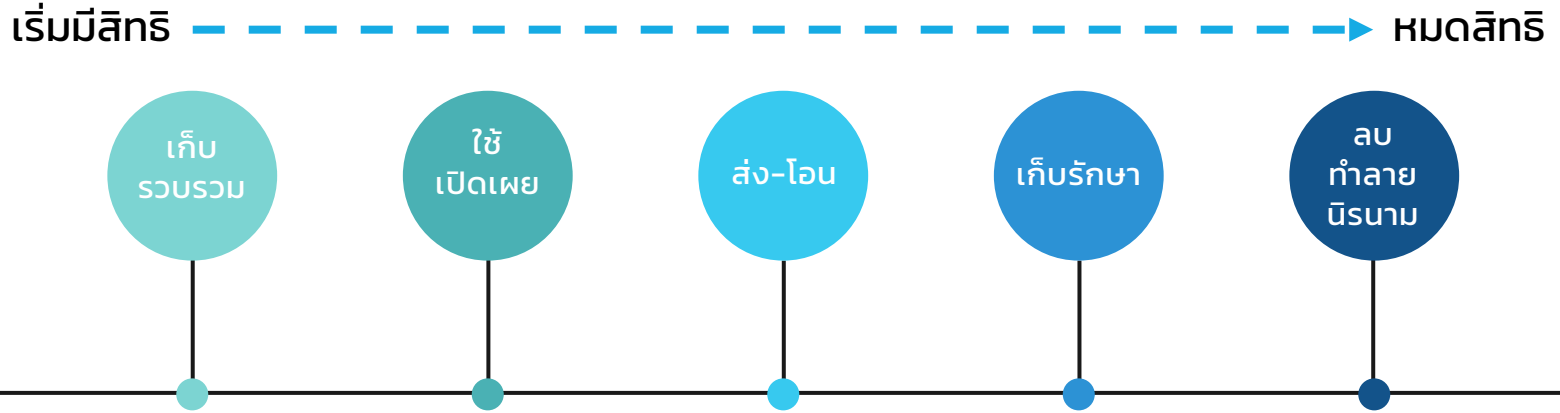
มาตรา ๘๔ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนมาตรา ๒๖ วรรคหนึ่งหรือวรรคสาม หรือฝ่าฝืนมาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง หรือมาตรา ๒๘ อันเกี่ยวกับข้อมูลส่วนบุคคลตามมาตรา ๒๖ หรือส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา ๒๖ โดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท

เมื่อเจ้าของข้อมูลส่วนบุคคลมีคำขอตามวรรคหนึ่งและเป็นกรณีที่ไม่อาจปฏิเสธคำขอได้ตามวรรคสอง ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอโดยไม่ชักช้า แต่ต้องไม่เกินสามสิบวันนับแต่วันที่ได้รับคำขอ



ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิคัดค้านตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไปได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้านให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ

เมื่อไรต้องจัดการการใช้สิทธิ



เริ่มเมื่อมีการเก็บข้อมูลส่วนบุคคล

ต้องจัดให้มีการจัดการการใช้สิทธิของเจ้าของข้อมูล

การจัดการการใช้สิทธิของเจ้าของข้อมูลส่วนยุคคล

- ติดต่อด้วยตนเอง
- อีเมล
- Website
- โทรศัพท์
- จดหมาย

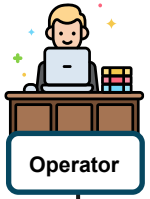
ความรับผิดชอบ การจัดการการใช้สิทธิ

สนับสนุน-ส่งเสริม
อนุมัตินโยบาย
การจัดการการใช้สิทธิ
สนับสนุนงบประมาณ
รับผิดชอบภาพรวม

- ให้คำปรึกษา
- ตรวจสอบแนะนำ

คณะทำงานจัดการสิทธิ

กำกับดูแลให้การทำงาน
เป็นไปตาม
ขั้นตอนการจัดการใช้สิทธิ
ตรวจสอบ
และรายงานผล
หรือปัญหา



ปฏิบัติตาม
ขั้นตอนการจัดการใช้สิทธิ

เหตุผลที่ควรตั้งคณะทำงาน ในการจัดการการใช้สิทธิ

- เพื่อความรวดเร็วและแม่นยำ:
- เพิ่มความโปร่งใสและความน่าเชื่อถือ:
- ลดความเสี่ยงทางกฎหมาย:
- จัดการคำขอได้เป็นระบบ:

องค์ประกอบของคณะทำงานที่ควรมี

- **ผู้รับผิดชอบการคุ้มครองข้อมูล (Data Protection Officer – DPO**

  คอยกำกับดูแลการตอบสนองคำขอให้เป็นไปตามกฎหมายและนโยบาย

- **ฝ่ายกฎหมาย (Legal Team)**

  ตรวจสอบแนะนำความถูกต้องทางกฎหมาย ป้องกันการละเมิดกฎหมาย

- **ฝ่ายเทคโนโลยีสารสนเทศ (IT)**

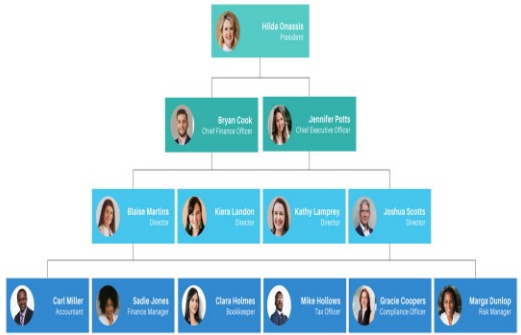
  สนับสนุนการเข้าถึง และการแก้ไข และดูแลเรื่องความปลอดภัยในการจัดการข้อมูล

- **ฝ่ายบริการลูกค้า (Customer Service)**

  เป็นผู้ที่รับคำขอและสื่อสารกับเจ้าของข้อมูล คอยอธิบายสิทธิและขั้นตอน

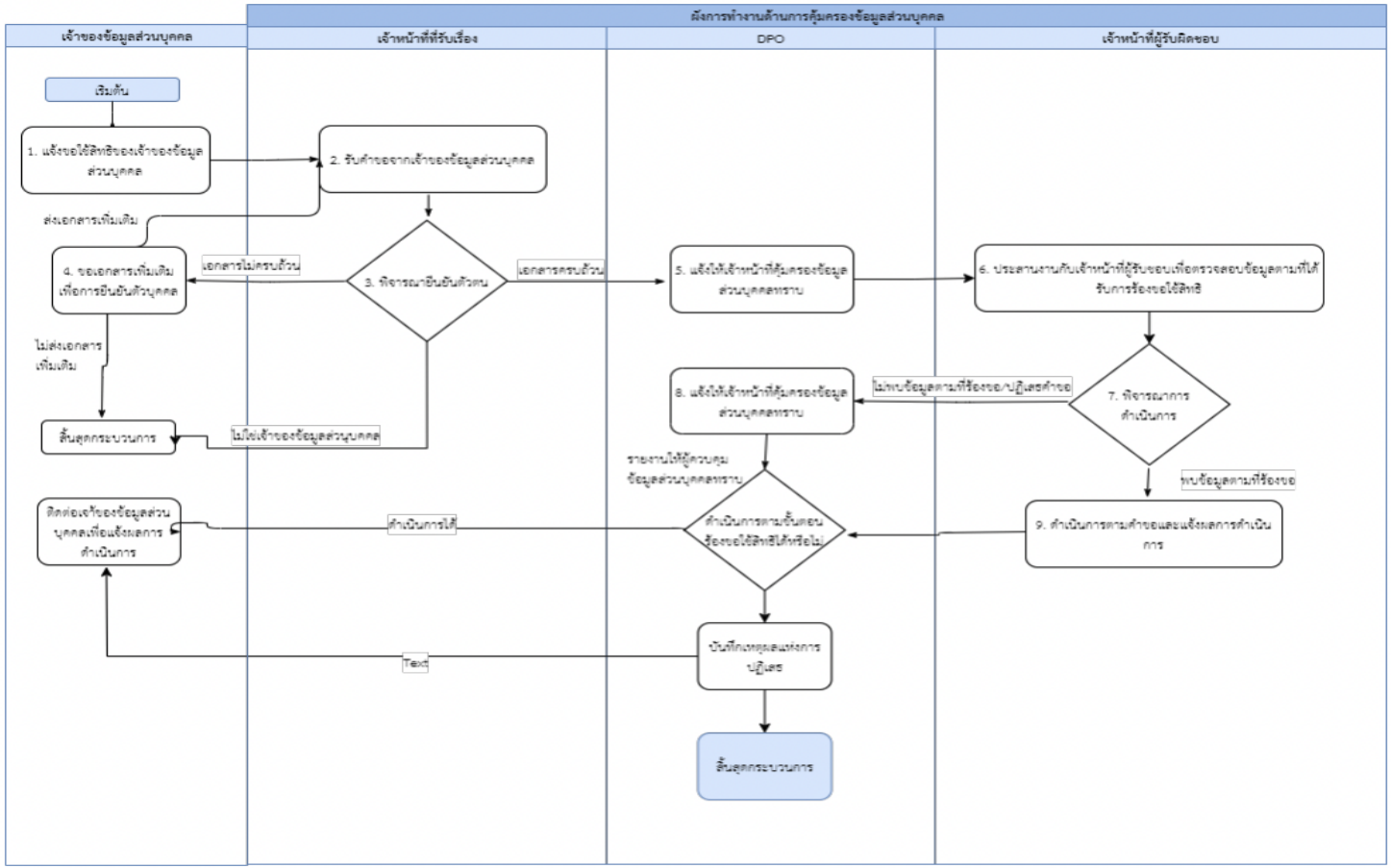
- **ฝ่ายทรัพยากรบุคคล (HR)**

  กรณีที่เจ้าของข้อมูลเป็นพนักงาน สามารถช่วยอำนวยความสะดวกเรื่องสิทธิของพนักงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล



ขั้นตอน การตอบสนองต่อคำขอใช้สิทธิ

ขั้นตอนการตอบสนองต่อคำขอใช้สิทธิ



แบบฟอร์มขอใช้สิทธิของเจ้าของข้อมูล

ขั้นตอนปฏิบัติการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล

ธนาคารแห่งประเทศไทย

มหาวิทยาลัยเทคโนโลยีสุรนารี

รพ. กรุงเทพขอนแก่น

กรมสรรพสามิต

กระบวนการจัดการคำร้องขอใช้สิทธิ (Data Subject Rights Request Flow)

ยืนยันตัวตนเจ้าของข้อมูลหรือผู้รับมอบอำนาจ (ต้องมีหลักฐานชัดเจน)

ตรวจสอบความสมเหตุสมผลและสิทธิทางกฎหมาย

กรอบเวลาบังคับ: ภายใน 30 วัน นับจากได้รับเอกสารครบถ้วน

ข้อยกเว้นที่ปฏิเสธได้ (Rejection Conditions):

⚠️ - ไม่สามารถยืนยันตัวตนได้

⚠️ - คำร้องซ้ำซ้อนหรือเกินความจำเป็นโดยไม่มีเหตุผลอันควร

⚠️ - การเก็บข้อมูลนั้นจำเป็นเพื่อการปฏิบัติตามกฎหมาย สัญญา หรือเพื่อปกป้องสิทธิและเสรีภาพของบุคคลอื่น

สิทธิของเจ้าของข้อมูลส่วนบุคคล vs ฐานการประมวลผลข้อมูลส่วนบุคคล

ฐานประมวลผล	สิทธิ	ถอนยินยอม	รับแจ้ง	เข้าถึง/สำเนา	รับ/โอน	คัดค้าน	ลบ/ทำลาย	ระงับ	แก้ไข	ร้องเรียน
	มาตรา	19 วรรค 5	23/25	30	31	32	33	34	36	73
ความยินยอม	19	●	●	●	●	●	●	●	●	●
จดหมายเหตุ วิจัย สถิติ	24 (1)	✕	●	●	✕	✕	✕	●	●	●
ระงับอันตราย	24 (2)	✕	●	●	✕	✕	●	●	●	●
สัญญา	24 (3)	✕	●	●	●	✕	●	●	●	●
ประโยชน์สาธารณะ/อำนาจรัฐ	24 (4)	✕	●	●	✕	●	✕	●	●	●
ประโยชน์โดยชอบธรรม	24 (5)	✕	●	●	✕	●	●	●	●	●
กฎหมาย	24 (6)	✕	●	●	✕	✕	✕	●	●	●
ข้อยกเว้นตาม PDPA		-	(1), (2), (3)	(4)	(5)	(6), (7), (8)	(7), (9)	(10)	(10)	(ดูกฎหมายลูก)

(1) DS ทราบรายละเอียด และวัตถุประสงค์นั้นอยู่แล้ว
(2) DC ไม่สามารถแจ้งได้ หรือเป็นอุปสรรค โดยเฉพาะเพื่อการศึกษาวิจัย วิทยาศาสตร์ ประวัติศาสตร์ และสถิติ
(3) DC ต้องกระทำโดยเร่งด่วน หรือต้องปิดเป็นความลับ ตามที่กฎหมายกำหนด
(4) DC ปฏิบัติตามกฎหมาย/คำสั่งศาล หรือจะทำให้เกิดความเสียหายต่อสิทธิเสรีภาพบุคคลอื่น
(5) DC เพื่อประโยชน์สาธารณะ ปฏิบัติตามกฎหมาย หรือละเมิดสิทธิเสรีภาพบุคคลอื่น ต้องสามารถทำได้โดยอัตโนมัติ
(6) DC แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า
(7) DC ใช้เพื่อการก่อตั้ง/ปฏิบัติตาม/ใช้/ยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
(8) DC ใช้เพื่อการศึกษาวิจัย/สถิติ เพื่อประโยชน์สาธารณะ
(9) DC ใช้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
(10) การขอแก้ไข/ขอระงับการใช้ ไม่สามารถทำได้ หากกฎหมายไม่อนุญาต

ตารางสรุป: สิทธิของเจ้าของข้อมูลส่วนบุคคล

มาตรา	สิทธิ	รายละเอียด / เงื่อนไขการใช้สิทธิ	ข้อยกเว้น / การปฏิเสธสิทธิ	ระยะเวลาตอบสนองสิทธิ	โทษปกครอง (สูงสุด)	มาตราเกี่ยวข้อง	มาตราโทษ	ประกาศคณะกรรมการ
23	ได้รับแจ้ง Privacy notice	ทุกกรณี (เป็นหน้าที่ของ DC)	DS ทราบรายละเอียดอยู่แล้ว (เก็บจากแหล่งอื่น: ไม่สามารถแจ้งได้ เร่งด่วนตาม กม.,เป็นอุปสรรคต่อสถิติ วิจัย)	แจ้งก่อน หรือระหว่างการประมวลผล	1 ล้านบาท	23	82	
19	ถอนความยินยอม	1. ทำได้ง่าย เช่นเดียวกับการให้ความยินยอม 2. แจ้งผลกระทบจากการถอนความยินยอม	1. มีข้อจำกัดสิทธิทางกฎหมาย 2. สัญญาที่ให้ประโยชน์ต่อ DS	เมื่อใดก็ได้	1 ล้านบาท	19 วรรค 6	82	
30	เข้าถึง ขอรับสำเนา ทราบการได้ข้อมูลฯ ที่ไม่ให้ความยินยอม	ดำเนินการโดยไม่ชักช้า ไม่เกิน 30 วัน นับแต่วันที่ได้รับคำขอ	1. ปฏิเสธตามกฎหมายหรือคำสั่งศาล 2. ส่งผลกระทบต่อบุคคลอื่น	ไม่เกิน 30 วัน	1 ล้านบาท	30 วรรค 4	82	อาจกำหนดหลักเกณฑ์เกี่ยวกับการเข้าถึงและการขอรับสำเนา ขยายระยะเวลา หรืออื่นๆ
31	ขอรับข้อมูล ขอให้ส่งหรือโอนข้อมูลไปยัง DC อื่น ขอรับข้อมูล ที่ DC ส่ง-โอน ไปยัง DC อื่นโดยตรง	1.อยู่ในรูปแบบ ที่ทำงานได้อัตโนมัติ 2. ใช้จากฐานยินยอม หรือสัญญา หรืออื่น ๆ ตาม ม.24 (ตามประกาศ)	1. ไม่สามารถทำได้โดยอัตโนมัติ 2. ปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ 3. ปฏิบัติหน้าที่ ตามกฎหมาย 4. ละเมิดสิทธิหรือเสรีภาพบุคคลอื่น	(แนวทางไม่เกิน 30 วัน)	(1 ล้านบาท)	(30 วรรค 4)	(82)	ข้อมูลที่ขอใช้สิทธิได้ ตามมาตรา 24 อื่น ตามที่คณะกรรมการประกาศกำหนด
32	คัดค้าน (การประมวลผล)	1. เป็นข้อมูล ม.24 (4) หรือ (5) 2. เพื่อการตลาดแบบตรง 3. วิจัย สถิติ	1. เหตุอันชอบด้วย กม.ที่สำคัญกว่า 2. เพื่อก่อตั้งสิทธิเรียกร้อง ตาม กม. 3. สถิติ วิจัย เพื่อประโยชน์สาธารณะ	เมื่อใดก็ได้ (ต้องแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนในทันทีเมื่อ DS ได้แจ้ง)	3 ล้านบาท	32 วรรค 2	83	
33	ลบ ทำลาย ทำให้ข้อมูลเป็นข้อมูล ที่ไม่สามารถระบุตัวบุคคลได้	1. หมดความจำเป็นตามวัตถุประสงค์ 2. ถอนความยินยอม (ไม่มีอำนาจตาม กม.) 3. คัดค้าน ม. 24 (4), (5) และปฏิเสธไม่ได้ 4. เก็บรวบรวม ใช้ เปิดเผย โดยไม่ชอบ	1.วัตถุประสงค์ในการใช้เสรีภาพ ในการแสดงความคิดเห็น 2. วัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) 3. วัตถุประสงค์ตามมาตรา26 (5) (ก) การรักษาทางการแพทย์ฯ หรือ (ข) ประโยชน์ด้านสาธารณสุขฯ 4. การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือ การใช้สิทธิเรียกร้องตามกฎหมาย 5.เพื่อการปฏิบัติ ตามกฎหมาย	ไม่เกิน 90 วัน (กรณีเปิดเผยสาธารณะ ต้องรับผิดชอบทั้งทางเทคโนฯ และค่าใช้จ่ายเพื่อให้เป็นไปตามคาขอ โดยแจ้ง DC อื่นๆ เพื่อให้ได้รับคำตอบในการดำเนินการให้เป็นไปตามคำขอ)	3 ล้านบาท	37(3)	83	ประกาศกำหนดหลักเกณฑ์การลบทำลาย 1. ดำเนินการไม่เกิน 90 วัน 2. รวมถึงสำเนาทั้งหมด 3. ไม่สามารถเรียกคืน ระบุตัวตนได้ ตรง/อ้อม 4. ใช้วิธีอย่างอื่นได้ โดยแจ้ง DS ทราบ 5. ทำนิรนาม ลบข้อมูลทางตรง (รวมถึง ก-ญ) 6. หลังทำนิรนาม ทำข้อมูลแผ่งข้อมูลที่เหลือ 7. เก็บ/ใช้/เปิดเผยไม่ชอบ ลบ/ทำลายเท่านั้น 8. ดำเนินการแล้วให้แจ้ง DS ทราบ 9. ทำนิรนาม แจ้งรายละเอียด DS ทราบ 10. ทำตามคำขอไม่ได้ ให้แจ้ง DS ทราบ
34	ระงับ (การใช้ข้อมูล)	1. ระหว่างเช็คความถูกต้องที่ร้องขอ (ม.36) 2. ต้องลบทำลาย ม.33 (4) แต่ให้ระงับใช้แทน 3. หมดความจำเป็น เพื่อก่อตั้งสิทธิตาม กม. 4. ระหว่างพิสูจน์เพื่อปฏิเสธสิทธิการคัดค้าน	(ปฏิบัติตามกฎหมาย กระทบสิทธิ เสรีภาพผู้อื่น ก่อตั้งสิทธิ ฟ้องร้องทางกฎหมาย ปฏิเสธสิทธิ แก้ไข, ลบ, คัดค้านได้)	(แนวทางไม่เกิน 30 วัน)	(5 ล้านบาท)	(28, 27-29)	(84)	อาจประกาศกำหนดหลักเกณฑ์ในการระงับการใช้ก็ได้ DS ร้องเรียน สคส. ได้
36	แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์	(เมื่อข้อมูลเปลี่ยนแปลง หรือพบว่าไม่ถูกต้อง)	(หลักฐานไม่เพียงพอ, ข้อเท็จจริงในอดีต)	(แนวทางไม่เกิน 30 วัน)	(5 ล้านบาท)	(28, 27-29)	(84)	DS ร้องเรียน สคส. ได้
73	ร้องเรียน สคส.	DS มีสิทธิร้องเรียนในกรณีที่ DC หรือ DP รวมทั้ง ลูกจ้าง หรือผู้รับจ้าง ฝ่าฝืน หรือไม่ปฏิบัติตาม PDPA แล้วทำให้เกิดความเสียหาย	1) รายละเอียดไม่ถูก/ไม่ครบ 2) เคยร้องเรียน และตัดสินแล้ว 3) ไม่ผิดตาม PDPA 4) กม.อื่นมีการพิจารณาแล้ว 5) ผู้ร้องเรียนไม่เกี่ยวข้องโดยตรง 6) ผู้ร้องเรียนถอนการร้องเรียน	เมื่อใดก็ได้	(ตามการพิจารณาของคณะกรรมการ)			การยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน ให้เป็นไปตามระเบียบที่คณะกรรมการประกาศกำหนด

การตอบสนองต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล (DSARs)

1.กำหนดวิธีการ / จุดในการรับคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

↓

2.ตรวจสอบตัวตนของผู้ยื่นคำร้องขอใช้สิทธิ

↓

3.ดำเนินการตามคำขอโดยประสานงานกับผู้ถือ/ผู้ใช้ข้อมูล

↓

4. ค้นหาข้อมูลตามคำร้องเพื่อดำเนินการ

↓

5.ตอบสนองต่อคำขอใช้สิทธิและให้เหตุหากปฏิเสธ

↓

6. ทบทวนและลงระบบบันทึกรายการกิจกรรมการประมวลผล (ROPA) เพื่อการตรวจสอบ

แบบฟอร์มคำร้องขอใช้สิทธิ

แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

Data Subject Rights Request Form

วันที่ .....

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้ให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการขอใช้สิทธิดำเนินการต่อข้อมูลส่วนบุคคลของตนซึ่งอยู่ในความดูแลของ บริษัท _____ "บริษัท") ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

ทั้งนี้ ท่านสามารถใช้สิทธิดังกล่าวได้โดยการกรอกรายละเอียดในแบบคำร้องนี้ และยื่นคำขอนี้ด้วยตนเอง แก่ บริษัท ทาง_____ จดหมายอิเล็กทรอนิกส์ (e-mail) (ระบุช่องทางอื่น หากมี).....

ข้อมูลผู้ยื่นคำร้องขอ

ชื่อ-นามสกุล .....
เลขบัตรประจำตัวประชาชน .....
เบอร์โทรศัพท์ติดต่อ .....
อีเมล .....

ท่านเป็นเจ้าของข้อมูลส่วนบุคคลหรือไม่

❒ ผู้ยื่นคำร้องเป็นเจ้าของข้อมูลส่วนบุคคล
❒ ผู้ยื่นคำร้องเป็นผู้แทนของเจ้าของข้อมูลส่วนบุคคล (โปรดระบุรายละเอียดของเจ้าของข้อมูลส่วนบุคคล)

รายละเอียดของเจ้าของข้อมูลส่วนบุคคล
ชื่อ-นามสกุล .....
ที่อยู่ .....
เบอร์โทรศัพท์ .....
อีเมล .....

เอกสารประกอบการขอใช้สิทธิ

เอกสารเพื่อการยืนยันตัวตนของผู้ยื่นคำร้อง
❒ สำเนาบัตรประจำตัวประชาชน (กรณีสัญญาชาติไทย)
❒ สำเนาหนังสือเดินทาง (กรณีไม่มีสัญญาชาติไทย)

เอกสารประกอบการดำเนินการแทน (เฉพาะกรณียื่นคำร้องแทนเจ้าของข้อมูลส่วนบุคคล)
❒ หนังสือมอบอำนาจที่เจ้าของข้อมูลส่วนบุคคลให้อำนาจผู้ยื่นคำร้องใช้สิทธิแทนเจ้าของข้อมูลส่วนบุคคลตามแบบคำร้องขอฉบับนี้ ซึ่งลงนามโดยเจ้าของข้อมูลส่วนบุคคลและผู้ยื่นคำร้องและลงวันที่ก่อนวันที่ยื่น

โปรดระบุสถานะความสัมพันธ์ของท่านที่มีต่อ บริษัท

❒ ลูกค้า / ผู้ใช้งานแอปพลิเคชัน / ผู้เข้าชมเว็บไซต์
❒ เจ้าหน้าที่/ผู้ปฏิบัติงาน
❒ ผู้สมัครงาน
❒ คู่สัญญา/ผู้รับเหมา
❒ ผู้ติดต่อ
❒ อื่น ๆ (โปรดระบุ) .....

โปรดระบุสิทธิที่ท่านประสงค์จะดำเนินการ

❒ เพิกถอนความยินยอม
❒ ขอเข้าถึงหรือรับสำเนาข้อมูลส่วนบุคคล รวมถึงขอให้ บริษัท เปิดเผยที่มาของข้อมูลที่ท่านไม่ได้ให้ความยินยอมในการเก็บรวบรวม
❒ ขอแก้ไขข้อมูลส่วนบุคคล
❒ ขอให้ลบข้อมูลส่วนบุคคล
❒ ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล
❒ ขอระงับการประมวลผลข้อมูลส่วนบุคคล
❒ ขอให้ บริษัท โอนย้ายข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น

โปรดระบุวัตถุประสงค์และเหตุผลประกอบคำร้องขอของท่าน

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

หมายเหตุ

บริษัท สงวนสิทธิในการติดต่อท่านตามข้อมูลการติดต่อที่ท่านได้ให้ไว้ในคำร้องนี้ เพื่อขอข้อมูลหรือเอกสารหลักฐานเกี่ยวกับคำขอเพิ่มเติม รวมถึงสงวนสิทธิในการดำเนินคดีตามกฎหมายหากพบว่าข้อมูลที่ท่านระบุในแบบคำร้องขอนี้ไม่เป็นความจริงโดยเจตนาทุจริต

การใช้สิทธิของท่านอาจมีเงื่อนไขที่กำหนดไว้ตามกฎหมายหรือกฎ ระเบียบอื่น ทั้งนี้ จำเป็นต้องมีการพิจารณาคำขอเป็นรายกรณีไป บริษัท ขอความร่วมมือให้ท่านโปรดให้ข้อมูลประกอบคำร้องขอของท่านอย่างครบถ้วน เพื่อให้ บริษัท สามารถดำเนินการตามสิทธิของท่านได้อย่างเหมาะสม รวมทั้ง บริษัท ขอสงวนสิทธิในการปฏิเสธคำขอของท่านในกรณีที่ บริษัท มีความจำเป็นต้องดำเนินการตามเงื่อนไขกฎหมายหรือคำสั่งศาล หรือเป็นกรณีการใช้สิทธิของท่านอาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น หรือในกรณีที่ท่านยังมีสัญญากับ บริษัท ที่ให้ประโยชน์แก่ท่านอยู่ ซึ่งการใช้สิทธิของท่านอาจเป็นผลให้ บริษัท ไม่สามารถให้บริการตามสัญญาแก่ท่านได้ โดย บริษัท จะดำเนินการแจ้งให้ท่านทราบถึงผลกระทบของการใช้สิทธิต่อไป

บริษัท จะดำเนินการตามคำร้องขอของท่านภายใน 30 วัน นับแต่วันที่ได้รับคำขอพร้อมเหตุผลและข้อมูลประกอบคำขอต่าง ๆ รวมถึงเอกสารหลักฐานประกอบจากท่านครบถ้วน ทั้งนี้ ขอสงวนสิทธิในการขยายเวลาดังกล่าวออกไป หาก บริษัท ได้รับข้อมูลไม่เพียงพอในการประกอบการดำเนินการ

ในกรณีที่ บริษัท มีความจำเป็นต้องปฏิเสธคำร้องขอใช้สิทธิของท่าน บริษัท จะแจ้งเหตุผลการปฏิเสธแก่ท่านทราบทางจดหมายอิเล็กทรอนิกส์

บริษัท เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลซึ่งท่านได้ให้ไว้ในคำร้องขอนี้เพื่อวัตถุประสงค์ในการตรวจสอบเพื่อยืนยันสิทธิของท่านทั้งในฐานะเจ้าของข้อมูลส่วนบุคคลและผู้แทน และดำเนินการตามคำขอใช้สิทธิของท่าน โดยอาจมีความจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลดังกล่าวแก่บุคคลหรือนิติบุคคลอื่นที่มีความเกี่ยวข้องในการประมวลผลข้อมูลส่วนบุคคลของท่าน ทั้งนี้ การเปิดเผยดังกล่าวจะเป็นไปเพื่อความจำเป็นในการดำเนินการตามคำร้องขอใช้สิทธิของท่านเท่านั้น และข้อมูลดังกล่าวจะถูกเก็บรักษาไว้จนกว่า บริษัท จะปฏิบัติตามคำร้องขอของท่านเสร็จสิ้น หรือจนกว่ากระบวนการโต้แย้งหรือปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลจะสิ้นสุดในกรณีที่ บริษัท ไม่อาจปฏิบัติตามคำร้องขอของท่านได้โดยมีเหตุผลอันสมควรตามที่กฎหมายหรือคำสั่งศาลกำหนด

ผู้ยื่นคำร้องได้อ่านและเข้าใจเนื้อหาของแบบคำร้องขอฉบับนี้แล้ว และยืนยันว่าข้อมูลที่ได้แจ้งแก่ บริษัท มีความถูกต้อง ครบถ้วน สมบูรณ์ทุกประการ รวมทั้งขอยืนยันและรับประกันว่าผู้ยื่นคำร้องมีสิทธิอย่างถูกต้องตามกฎหมาย จึงได้ลงลายมือชื่อตามที่ระบุข้างล่างนี้

..... ผู้ยื่นคำร้องขอ

(.....)

วันที่ .....

***สำหรับเจ้าหน้าที่เท่านั้น**

วันที่ได้รับคำร้องขอ .....

วันที่บันทึกในระบบ .....

วันที่มีหนังสือตอบรับ .....

ผลการพิจารณา .....

เหตุผลในการปฏิเสธ (หากมี) .....

เจ้าหน้าที่ผู้ดำเนินการ .....

ตัวอย่างช่องทางการใช้สิทธิบนเว็บไซต์

แบบฟอร์มคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

ข้อมูลของผู้ยื่นคำร้อง

ชื่อ-นามสกุล: *

อีเมล: *

ที่อยู่:

เบอร์ติดต่อ: *

(___) ___-____

สถานะเจ้าของข้อมูลส่วนบุคคล

- เจ้าของข้อมูลส่วนบุคคลมีอายุไม่เกิน 10 ปี
- เจ้าของข้อมูลส่วนบุคคลมีอายุระหว่าง 10-20 ปี
- เจ้าของข้อมูลส่วนบุคคลเป็นผู้บรรลุนิติภาวะแล้ว

ผู้ยื่นคำร้องเป็นเจ้าของข้อมูลส่วนบุคคลหรือไม่

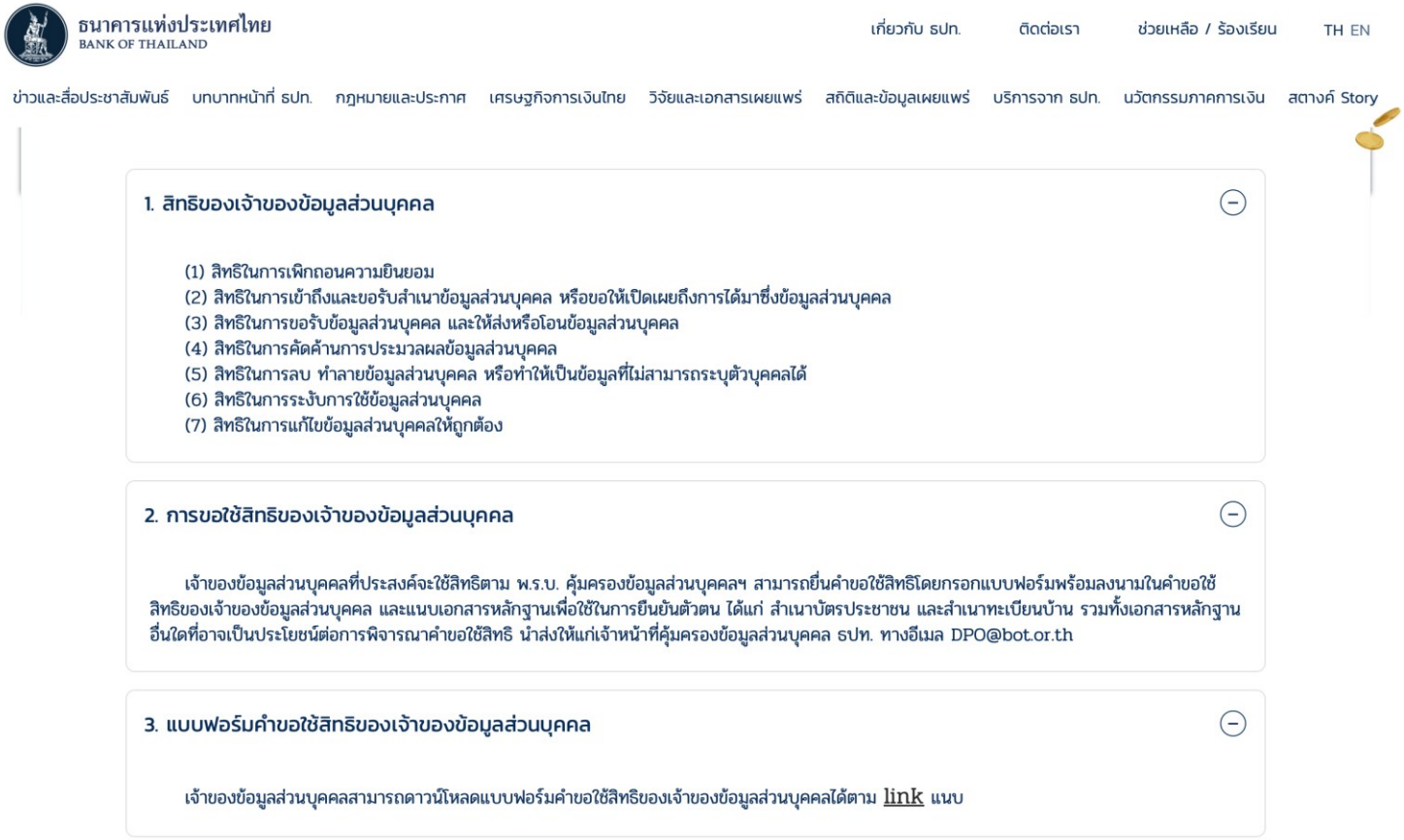
หรือ Scan QR Code

ช่องทางที่ 2 เจ้าของข้อมูลส่วนบุคคล สามารถขอใช้สิทธิเจ้าของข้อมูลส่วนบุคคลโดยใช้แบบฟอร์ม คำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

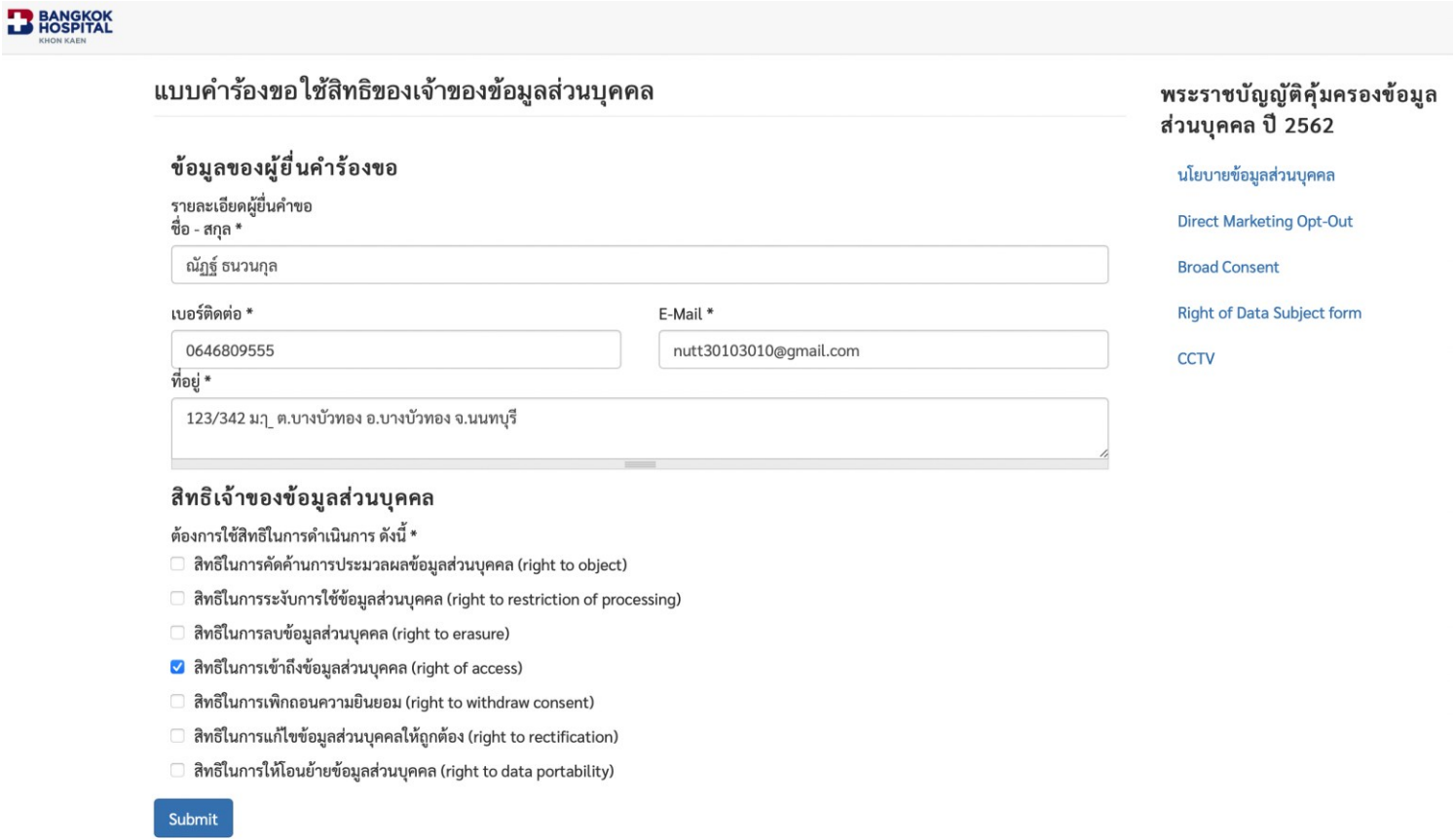
โดยการกรอกรายละเอียดในแบบคำร้องนี้ พร้อมแนบเอกสารสำเนาบัตรประจำตัวประชาชน และยื่นคำขอนี้แก่ มทส. ทางจดหมายอิเล็กทรอนิกส์ (e-mail : dpo@sut.ac.th)

ทั้งนี้มทส. จะดำเนินการตามคำร้องขอของท่านภายใน 30 วัน นับแต่วันที่ได้รับคำขอพร้อมเหตุผลและข้อมูลประกอบคำขอต่าง ๆ รวมถึงเอกสารหลักฐานประกอบจากท่านครบถ้วน

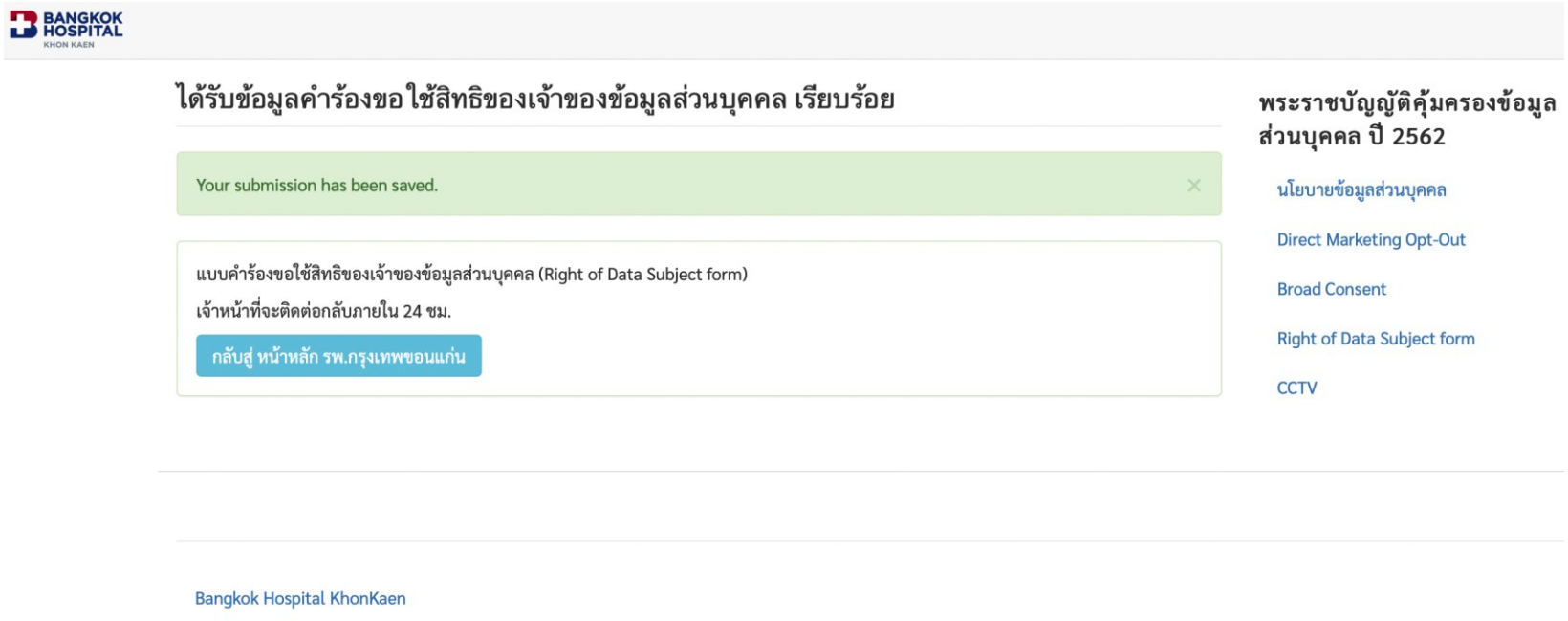
ตัวอย่างช่องทางการใช้สิทธิบนเว็บไซต์



ตัวอย่างช่องทางการใช้สิทธิบนเว็บไซต์



ตัวอย่างช่องทางการใช้สิทธิบนเว็บไซต์



หนังสือตอบกลับการใช้สิทธิ

หนังสือตอบกลับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

Data Subject Rights Responding

วันที่ .....

ตามที่ท่านได้ยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามบทบัญญัติแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตามคำร้องขอเลขที่ ..... ลงวันที่ ..... ต่อ บริษัท_____ (**"บริษัท"**) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลนั้น

บัดนี้ บริษัท ขอเรียนให้ท่านทราบถึงผลการพิจารณาคำขอใช้สิทธิของท่าน โดยมีรายละเอียดดังต่อไปนี้

รายละเอียดคำร้องขอของท่าน	
ชื่อ - นามสกุลผู้ยื่นคำร้องขอ	
ชื่อ - นามสกุลเจ้าของข้อมูลส่วนบุคคล	(โปรดระบุเฉพาะกรณีผู้ยื่นคำร้องขอไม่ใช่เจ้าของข้อมูลส่วนบุคคล)
สิทธิที่ท่านได้ยื่นคำร้องขอ	(โปรดเลือกเฉพาะรายการสิทธิโดยอ้างอิงตามคำร้องขอใช้สิทธิที่เจ้าของข้อมูลส่วนบุคคลยื่น ได้แก่ 1. ขอเพิกถอนความยินยอม 2. ขอเข้าถึงหรือรับสำเนาข้อมูลส่วนบุคคลหรือขอให้เปิดเผยที่มาของข้อมูล 3. ขอแก้ไขข้อมูลส่วนบุคคล 4. ขอให้ลบข้อมูลส่วนบุคคล 5. ขอคัดค้านการประมวลผลข้อมูลส่วนบุคคล 6. ขอระงับการประมวลผลข้อมูลส่วนบุคคล หรือ 7.ขอให้ บริษัท โอนย้ายข้อมูลส่วนบุคคล)

ผลการพิจารณาคำขอ	
❒ ดำเนินการตามคำร้องขอ ❒ ปฏิเสธคำร้องขอ	**รายละเอียด** : .....(โปรดระบุเหตุผลประกอบผลการพิจารณา โดยมีเงื่อนไขดังนี้ - กรณีดำเนินการตามคำร้องขอ โปรดระบุรายละเอียดการดำเนินการ เช่น บริษัท ได้ดำเนินการแก้ไขข้อมูลส่วนบุคคลของท่านเป็นที่เรียบร้อยเมื่อวันที่ ..... - กรณีปฏิเสธคำร้องขอ โปรดระบุรายละเอียดและเหตุผลประกอบการปฏิเสธ เช่น บริษัท ไม่สามารถดำเนินการลบข้อมูลของท่านตามที่ร้องขอได้ เนื่องจากท่านยังมีสัญญา..... กับ บริษัท อยู่ ซึ่งทำให้ บริษัท จำเป็นต้องเก็บรักษาข้อมูลของท่านต่อไปเพื่อการให้บริการตามสัญญา ทั้งนี้ หากท่านยืนยันต้องการให้ลบข้อมูล โปรดดำเนินการเพื่อยกเลิกสัญญาดังกล่าวก่อน โดยติดต่อได้ที่ช่องทาง.....

หากท่านมีข้อสงสัยเกี่ยวกับผลการพิจารณาคำขอดังกล่าว โปรดติดต่อ บริษัท ได้ที่ .....

ขอแสดงความนับถือ

.....

บันทึกการจัดการสิทธิ

บันทึกการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล

		รายละเอียดการขอใช้สิทธิของเจ้าของข้อมูล							การพิจารณาของคณะทำงาน				การตอบสนองสิทธิ						
											ผลการพิจารณา/เหตุผล								
No.	รหัสคำร้อง (ID)	วันที่ได้รับคำร้อง	ช่องทางที่ได้รับ	ชื่อผู้ร้อง/เจ้าของข้อมูล	ความสัมพันธ์กับองค์กร	การยืนยันตัวตน (ผ่าน/ไม่ผ่าน)	สิทธิที่ขอ (เลือกรายการ)	วันครบกำหนด (30 วัน)	ส่วนงานที่เกี่ยวข้อง	วันที่ส่งต่อ	ผลพิจารณา	หากปฏิเสธให้ระบุเหตุผล (บันทึกมาตรา 39 (7))	วิธีการดำเนินการดำเนินการ	วันที่เสร็จสิ้น	วิธีการ/ช่องทางแจ้งผลเจ้าของข้อมูล	วันที่แจ้งผลผู้ใช้สิทธิ	สถานะ (ภายใน/เกินกำหนดเวลา)	บันทึก DPO ตรวจสอบ	หมายเหตุ
1	DSR-001	4/1/2569	อีเมลมหาวิทยาลัย	นาย ก.	(นักศึกษา)	ผ่าน	เข้าถึง	3/2/1969	ฝ่ายทะเบียน	5/1/1969	อนุมัติ	-	ส่งไฟล์ระเบียนประวัติทางอีเมล	7/1/1969	อีเมล	7/1/1969	ภายในกำหนด	ผ่าน	

ระเบียบปฏิบัติการจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล

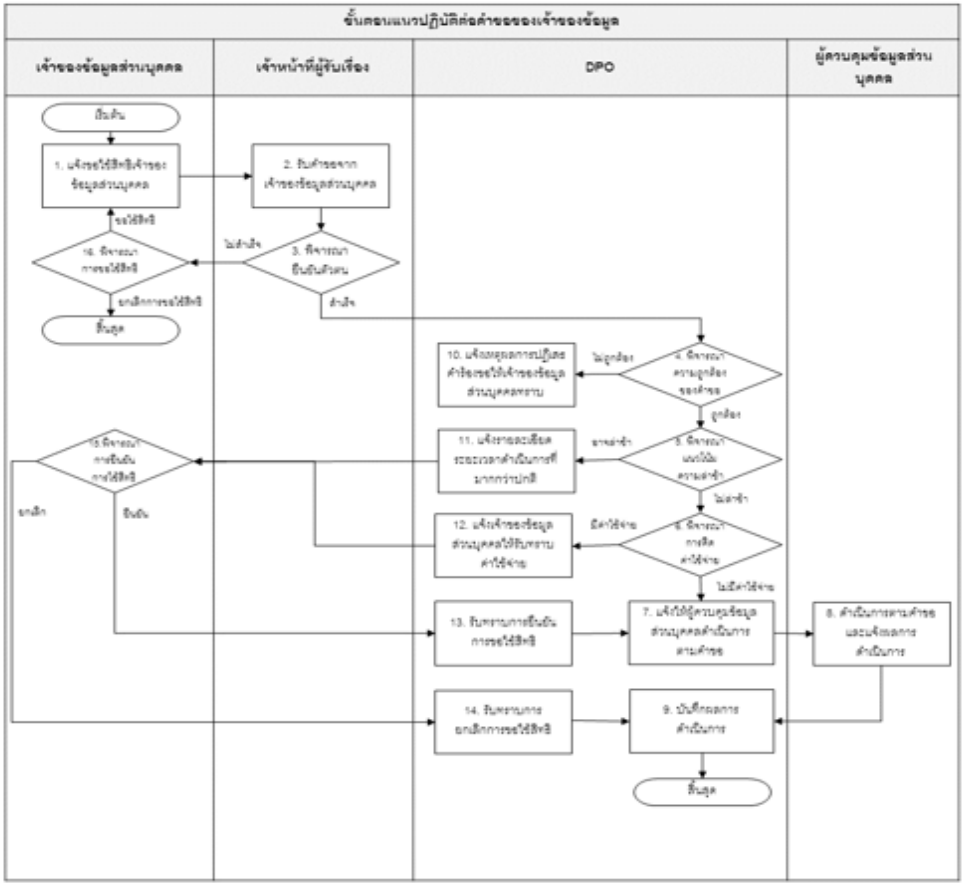
มหาวิทยาลัยราชภัฏสกลนคร

(Kanchanaburi Rajabhat University)

ระเบียบปฏิบัติการจัดการการสิทธิของเจ้าของข้อมูลส่วนบุคคล

(Personal Data Subject right managing procedure)

5.แนวปฏิบัติงาน (Procedure)




ANY QUESTIONS?

Data Breach Management & Incident Reporting

for PDPA

Identifying a Data Breach

- Unusual Activity
- Data Leak
- Cyber Attack

Incident Response Steps

1. Contain the Breach
2. Assess the Impact
3. Notify Authorities

Notification & Mitigation

- Alerting Affected Individuals
- Implementing Safeguards

มาตรา 37 (4)

ทุกระดับ และทุกคน

กฎหมายลำดับรองการแจ้งเหตุการละเมิด

12) การประเมินความเสี่ยง
1) ลักษณะ/ประเภทการละเมิด
2) ลักษณะ/ประเภทของข้อมูล
3) ปริมาณข้อมูล
4) ลักษณะ/ประเภท/สถานะของ DS
5) ความร้ายแรงของผลกระทบ/ความเสียหาย, ประสิทธิผลของมาตรการที่ DC ใช้ หรือจะใช้
6) ผลกระทบในวงกว้างต่อธุรกิจ หรือการดำเนินการของ DC หรือต่อสาธารณะจากเหตุการละเมิด
7) ลักษณะของระบบการจัดเก็บข้อมูลที่เกี่ยวข้อง/มาตรการ
8) สถานะทางกฎหมายของ DC (บุคคลธรรมดา /นิติบุคคล) รวมทั้งขนาด/ลักษณะของกิจการ

5) (1)
- ประเมินความน่าเชื่อถือ
- ตรวจสอบมาตรการ
- ประเมินความเสี่ยงที่กระทบต่อสิทธิ เสรีภาพ

5) (2)
- เมื่อประเมินว่าเสี่ยงสูง ให้ป้องกัน ระงับ แก้ไข ให้สิ้นสุด

5) (3)
- เชื่อว่ามีการละเมิดจริง แจ้งเหตุการณ์ละเมิดแก่สำนักงาน โดยไม่ชักช้าภายใน 72 ชม.
- เว้นแต่ การละเมิดนั้นไม่มีความเสี่ยงต่อสิทธิเสรีภาพของบุคคล

5) (4)
- เมื่อประเมินว่าเสี่ยงสูง ให้แจ้งเจ้าของข้อมูล พร้อมแนวทางการเยียวยาโดยไม่ชักช้า

10)
มีความเสี่ยงสูง ให้ DC แจ้งเหตุการณ์ละเมิด
พร้อมสาระสำคัญดังต่อไปนี้ ให้ DS ทราบเท่าที่จะสามารถกระทำได้ โดยไม่ชักช้า
(1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิด
(2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อ DPO หรือบุคคล ที่ DC มอบหมาย
(3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับ DS
(4) แนวทางการเยียวยาความเสียหายของ DS และข้อมูลโดยสังเขป เกี่ยวกับมาตรการที่จำเป็น และเหมาะสมใช้หรือจะใช้ รวมถึงข้อแนะนาเกี่ยวกับมาตรการที่ DS อาจดำเนินการเพิ่มเติม เพื่อระงับเหตุ หรือเยียวยาความเสียหาย

9) DC อาจยกเว้นการแจ้งเหตุการละเมิดแก่ สคส. เพื่อประกอบการพิจารณาได้ หาก DC พิสูจน์ได้ว่าเหตุการละเมิดไม่มีความเสี่ยง รวมถึงกรณีเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หรือข้อมูลไม่อยู่ในสภาพที่ใช้งานได้ เนื่องจากมีมาตรการทางเทคโนโลยีที่เพียงพอ หรือเหตุอื่นใดที่เชื่อถือได้
ในการยกข้อยกเว้นดังกล่าว DC มีหน้าที่ให้ข้อมูล หรือส่งเอกสาร หรือหลักฐาน เกี่ยวกับเหตุที่ควรได้รับการยกเว้น ซึ่งรวมถึงรายละเอียดเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย หรือข้อมูลอื่นใด ให้ สคส. พิจารณา

6) แจ้งเหตุละเมิดเป็นลายลักษณ์อักษร หรืออิเล็กทรอนิกส์ หรือตามที่สำนักงานกำหนด โดยระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้
(1) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะและประเภทของการละเมิด โดยอาจบรรยายถึงลักษณะและจำนวน DS หรือลักษณะ และจำนวนรายการ (records)
(2) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของ DPO (ถ้ามี) หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ DC มอบหมาย
(3) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการละเมิด
(4) ข้อมูลเกี่ยวกับมาตรการที่ DC ใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือ แก้ไข หรือเยียวยาความเสียหาย

เกิดเหตุ-รับแจ้ง
- เกิดการละเมิด สูญเสีย CIA
- รับแจ้งเบื้องต้นจากบุคคลใดๆ
  - วาจา/หนังสือ/อิเล็กฯ
  - DC ทราบเอง
  - ทราบจาก DP

ประเมิน-แก้ไขเบื้องต้น
- ตรวจสอบเบื้องต้น ว่าละเมิด?
- ตรวจสอบมาตรการ กับส่วนที่เกี่ยวข้อง
- ประเมินความเสี่ยง ต่อสิทธิเสรีภาพ
- เสี่ยงสูง: ป้องกัน ระงับ แก้ไข

แจ้งเหตุการละเมิด
- เสี่ยง (แจ้ง สคส)
- เสี่ยงสูง (แจ้ง สคส/DS)
- ไม่เสี่ยง (เก็บหลักฐาน)
- แจ้งล่าช้า ไม่เกิน 15 วัน

ดำเนินการ
- ดำเนินการมาตรการที่จำเป็น
- ทบทวนมาตรการ

สรุปผล/ขยายผล
- แก้ไขเอกสาร
- ฝึกอบรม
- ติดตามผล
- รายงานผล

8) กรณีมี DPA กับ DP จะต้องระบุไว้ในข้อตกลง หรือในสัญญา ให้ DP มีหน้าที่แจ้งเหตุการณ์ละเมิดแก่ DC โดยไม่ชักช้า ภายใน 72 ชม.

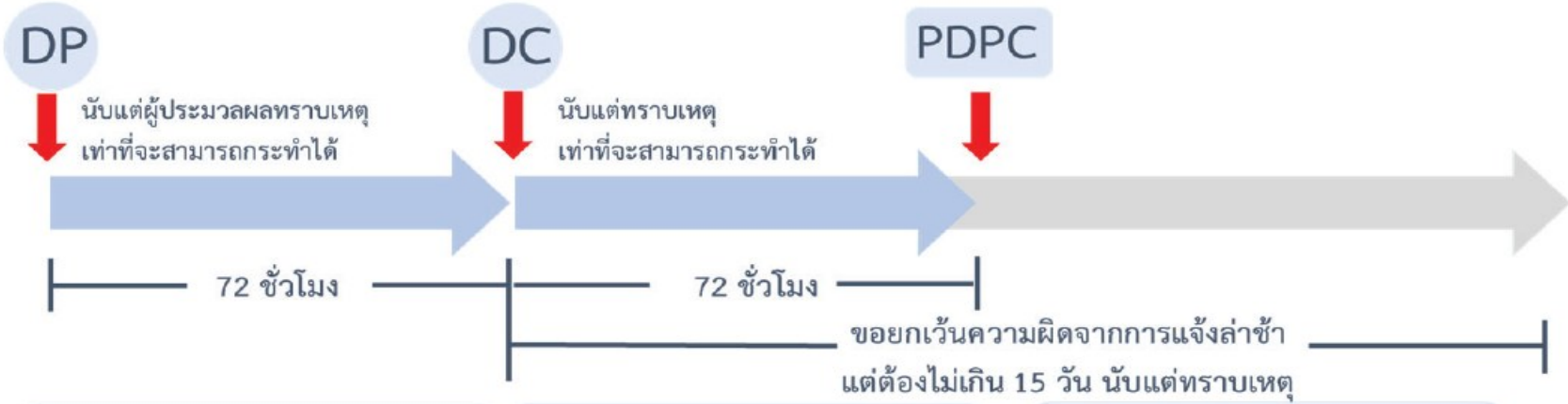
7) กรณีแจ้งล่าช้ากว่า 72 ชม.
ชี้แจงเหตุผลความจำเป็น และรายละเอียดที่เกี่ยวข้องเพื่อแสดงเหตุจำเป็น โดยต้องแจ้งแก่สำนักงานโดยเร็ว ไม่เกิน 15 วันนับแต่ทราบเหตุ

*** การแจ้งเหตุการละเมิดแก่สำนักงานไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดของ DC ตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้น หรือกฎหมายอื่น

5) (5)
- ดำเนินการตามมาตรการที่จำเป็นและเหมาะสม เพื่อ
ระงับ ตอบสนอง แก้ไข หรือฟื้นฟู รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดในลักษณะเดียวกันในอนาคต
- ทบทวนมาตรการฯ ให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยคำนึงถึงระดับความเสี่ยงตามปัจจัยทางเทคโนโลยี บริบท สภาพแวดล้อม มาตรฐานที่เป็นที่ยอมรับสำหรับหน่วยงานหรือ กิจการในประเภทหรือลักษณะเดียวกันหรือใกล้เคียงกัน ลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ทรัพยากรที่ต้องใช้ และความเป็นไปได้ในการดำเนินการประกอบกัน

11) ในการแจ้งเหตุการละเมิดให้ DS อาจแจ้งเป็นกลุ่ม หรือเป็นการทั่วไปผ่านสื่อสาธารณะ สื่อสังคมออนไลน์ หรือวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่ DS ที่ได้รับผลกระทบ หรือบุคคลทั่วไปสามารถเข้าถึงการแจ้งดังกล่าวได้ การแจ้งเป็นกลุ่ม จะต้องไม่ก่อให้เกิดความเสียหาย หรือผลกระทบต่อ DS

ระยะเวลาการแจ้งเหตุการละเมิด



ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดฯ ข้อ 8 + พรบ.คุ้มครองข้อมูลส่วนบุคคลฯ ม.40 (2)

จัดทำ Data Processing Agreement เพื่อกำหนดหน้าที่ของผู้ประมวลผล (ม.40 วรรคสาม)
***อาจกำหนดระยะเวลาต่ำกว่าได้ แต่ทั้งนี้ ต้องไม่เกิน 72 ชั่วโมง

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดฯ ข้อ 5 + พรบ.คุ้มครองข้อมูลส่วนบุคคลฯ ม.37 (4)

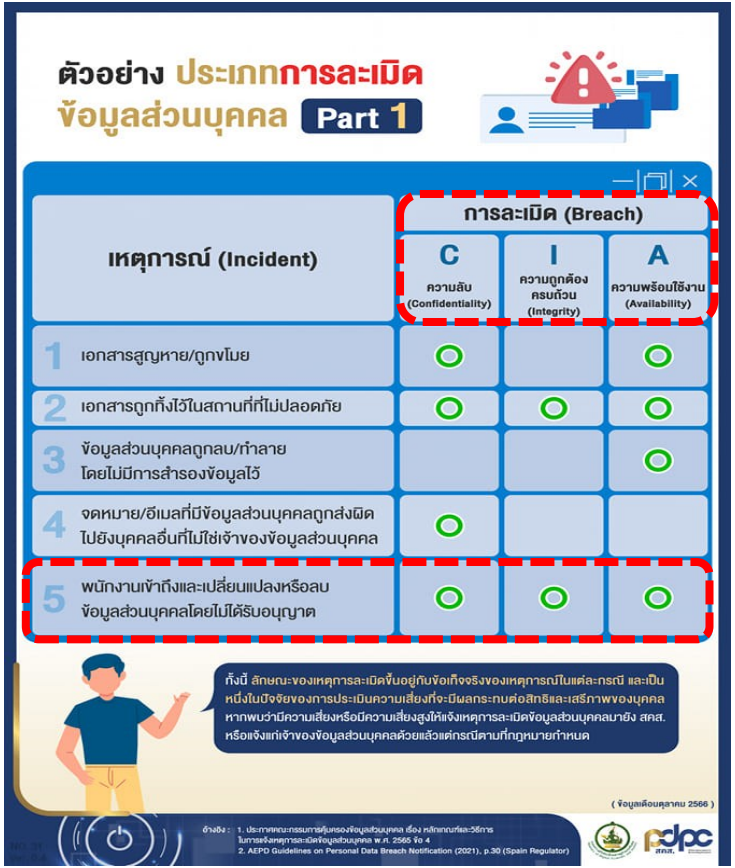
ข้อมูลเบื้องต้นที่ต้องแจ้ง

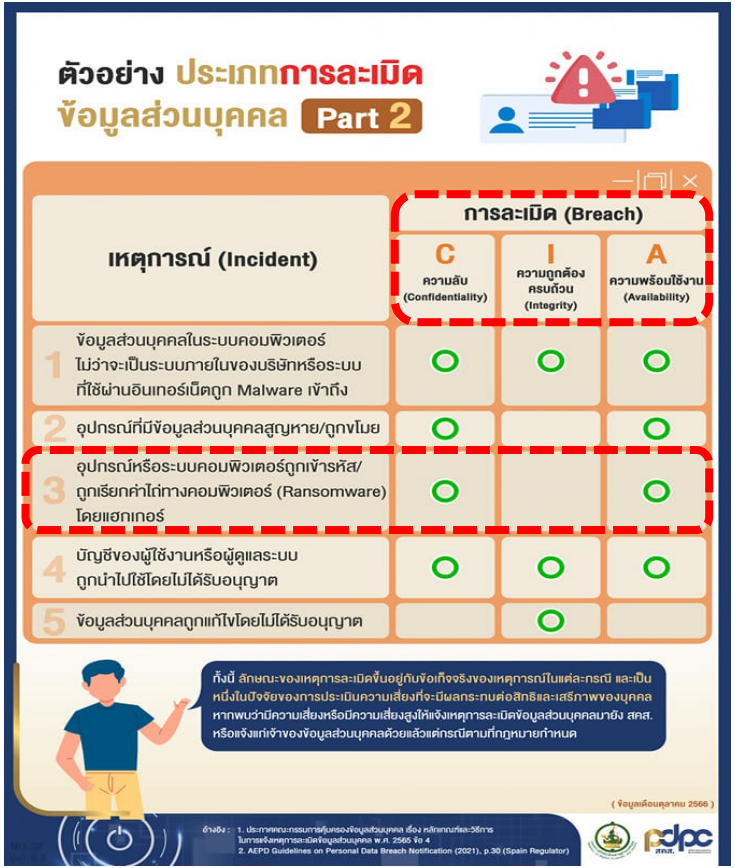
1. ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิด
2. ชื่อ สถานที่ติดต่อ วิธีการติดต่อ DPO/บุคคลที่ DC มอบหมายให้ทำหน้าที่ประสานงาน
3. ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิด
4. ข้อมูลเกี่ยวกับมาตรการที่ DC ใช้หรือจะใช้เพื่อป้องกัน ระงับ หรือแก้ไขเหตุการละเมิด หรือเยียวยาความเสียหาย

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดฯ ข้อ 7

ขอให้สคส.พิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยต้องชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้อง

ประเภทเหตุการละเมิดข้อมูล





ประเมินความเสี่ยงจากเหตุการละเมิดข้อมูล

เหตุ
การละเมิด

ไม่เสี่ยง ต่อสิทธิเสรีภาพ

เสี่ยง ต่อสิทธิเสรีภาพ

เสี่ยงสูง ต่อสิทธิเสรีภาพ

บันทึกไว้
เป็นหลักฐาน
พร้อมให้ สคส. ตรวจสอบ

แจ้ง สคส.
ภายใน 72 ชั่วโมง
(ช้าสุดไม่เกิน 15 วัน)

แจ้ง DS
โดยไม่ชักช้า
พร้อมแนวทางการเยียวยา + มาตรการที่
DS ต้องทำเอง

ต้องแจ้งใครบ้าง

Event	แจ้ง สคส.	แจ้ง DS	เหตุผล
1. ผู้ควบคุมข้อมูลส่วนบุคคล**จัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive** โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา **USB Drive ดังกล่าวสูญหายไป**			
2. **ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์** ต่อมา**เกิดภัยคุกคามทางไซเบอร์** ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล			
3. **ระบบไฟฟ้าใน call center ของผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง** โดย**ไฟดับชั่วคราว**ส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถให้บริการได้ชั่วคราว			
4. ผู้ควบคุมข้อมูลส่วนบุคคล**ถูกภัยคุกคามทางไซเบอร์** โดยถูกโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) ข้อมูลส่วนบุคคลทั้งหมดของผู้ควบคุมข้อมูลส่วนบุคคลถูกเข้ารหัสโดยผู้โจมตี (hacker) และไม่มีข้อมูลสำรอง จึงไม่สามารถที่จะเข้าถึงและใช้งานข้อมูลดังกล่าวได้			
5. ธนาคารได้รับการติดต่อจาก**ลูกค้าธนาคาร ๑ ราย ว่าได้รับใบแจ้งหนี้เรียกเก็บเงินของบุคคลที่ไม่รู้จัก** ผู้ควบคุมข้อมูลส่วนบุคคลทำการตรวจสอบแล้วภายใน ๒๔ ชั่วโมง พบว่า มีการรั่วไหลของข้อมูลส่วนบุคคลจำนวน ๑๐ ราย			

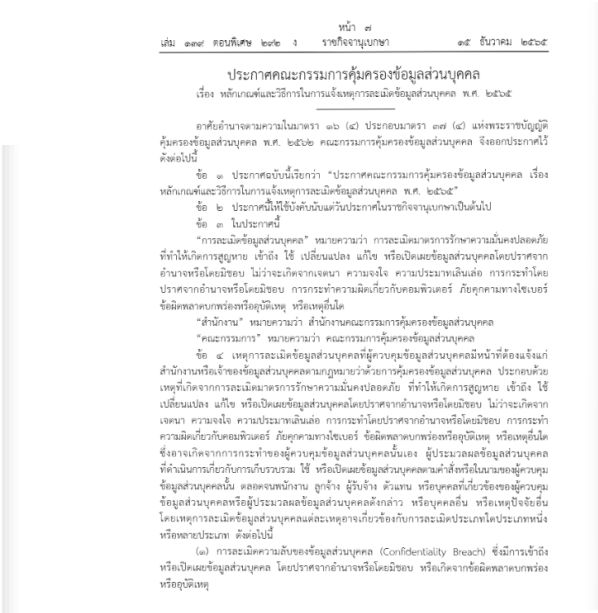
คู่มือ by สคส.

ตัวอย่างการประเมินความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล

รายละเอียดดังต่อไปนี้เป็นตัวอย่างแนวทางในการประเมินความเสี่ยงในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคล ว่าการละเมิดข้อมูลส่วนบุคคลนั้นมีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลเพียงใด

โดยในตัวอย่างแต่ละกรณีจะอธิบายเหตุผลและตัวอย่างการประเมินความเสี่ยงว่ากรณีดังกล่าวต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคลหรือไม่

ตัวอย่าง	แจ้งเหตุแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล	เหตุผล
๑. ผู้ควบคุมข้อมูลส่วนบุคคลจัดเก็บข้อมูลส่วนบุคคลสำรองไว้ใน USB Drive โดยมีการเข้ารหัสด้วยเทคโนโลยีที่น่าเชื่อถือ ต่อมา USB Drive ดังกล่าวสูญหายไป	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ความเสี่ยงต่ำ เนื่องจากเมื่อมีการเข้ารหัสด้วยมาตรการทางเทคโนโลยีที่น่าเชื่อถือแล้ว ข้อมูลดังกล่าวไม่สามารถเปิดใช้งานได้ การที่ USB Drive สูญหายไปจึงไม่มีความเสี่ยงกับเจ้าของข้อมูลส่วนบุคคล
๒. ผู้ควบคุมข้อมูลส่วนบุคคลให้บริการจัดเก็บข้อมูลส่วนบุคคลในระบบออนไลน์ ต่อมาเกิดภัยคุกคามทางไซเบอร์ ส่งผลให้ข้อมูลส่วนบุคคลรั่วไหลจากระบบคอมพิวเตอร์ของผู้ควบคุมข้อมูลส่วนบุคคล	ต้องแจ้ง	ต้องแจ้ง	เนื่องจากข้อมูลส่วนบุคคลดังกล่าวอยู่ในสภาพที่ใช้งานได้และสามารถระบุตัวบุคคลได้ การที่เกิดภัยคุกคามทางไซเบอร์อาจจะก่อให้เกิดปัญหาและผลกระทบซึ่งเกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลจำนวนมาก
๓. ระบบไฟฟ้าใน call center ของผู้ควบคุมข้อมูลส่วนบุคคลขัดข้อง โดยไฟดับชั่วคราว ส่งผลให้ระบบคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของ	ไม่ต้องแจ้ง	ไม่ต้องแจ้ง	ข้อมูลส่วนบุคคลดังกล่าวไม่อยู่ในสภาพพร้อมใช้งาน เนื่องจากปัญหาทางด้านเทคโนโลยี เมื่อระบบไฟฟ้ากลับมาเหมือนเดิม



หน้า ๗
เล่ม ๑๓๙ ตอนพิเศษ ๒๓๒ ง ราชกิจจานุเบกษา ๑๕ ธันวาคม ๒๕๖๕

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) ประกอบมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศฉบับนี้เรียกว่า "ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"การละเมิดข้อมูลส่วนบุคคล" หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด

"สำนักงาน" หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"คณะกรรมการ" หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อ ๔ เหตุการละเมิดข้อมูลส่วนบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งแก่สำนักงานหรือเจ้าของข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ประกอบด้วยเหตุที่เกิดจากการละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด ซึ่งอาจเกิดจากการกระทำของผู้ควบคุมข้อมูลส่วนบุคคลนั้นเอง ผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคลนั้น ตลอดจนพนักงาน ลูกจ้าง ผู้รับจ้าง ตัวแทน หรือบุคคลที่เกี่ยวข้องของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว หรือบุคคลอื่น หรือเหตุปัจจัยอื่นโดยเหตุการละเมิดข้อมูลส่วนบุคคลแต่ละเหตุอาจเกี่ยวข้องกับการละเมิดประเภทใดประเภทหนึ่งหรือหลายประเภท ดังต่อไปนี้

(๑) การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach) ซึ่งมีการเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ

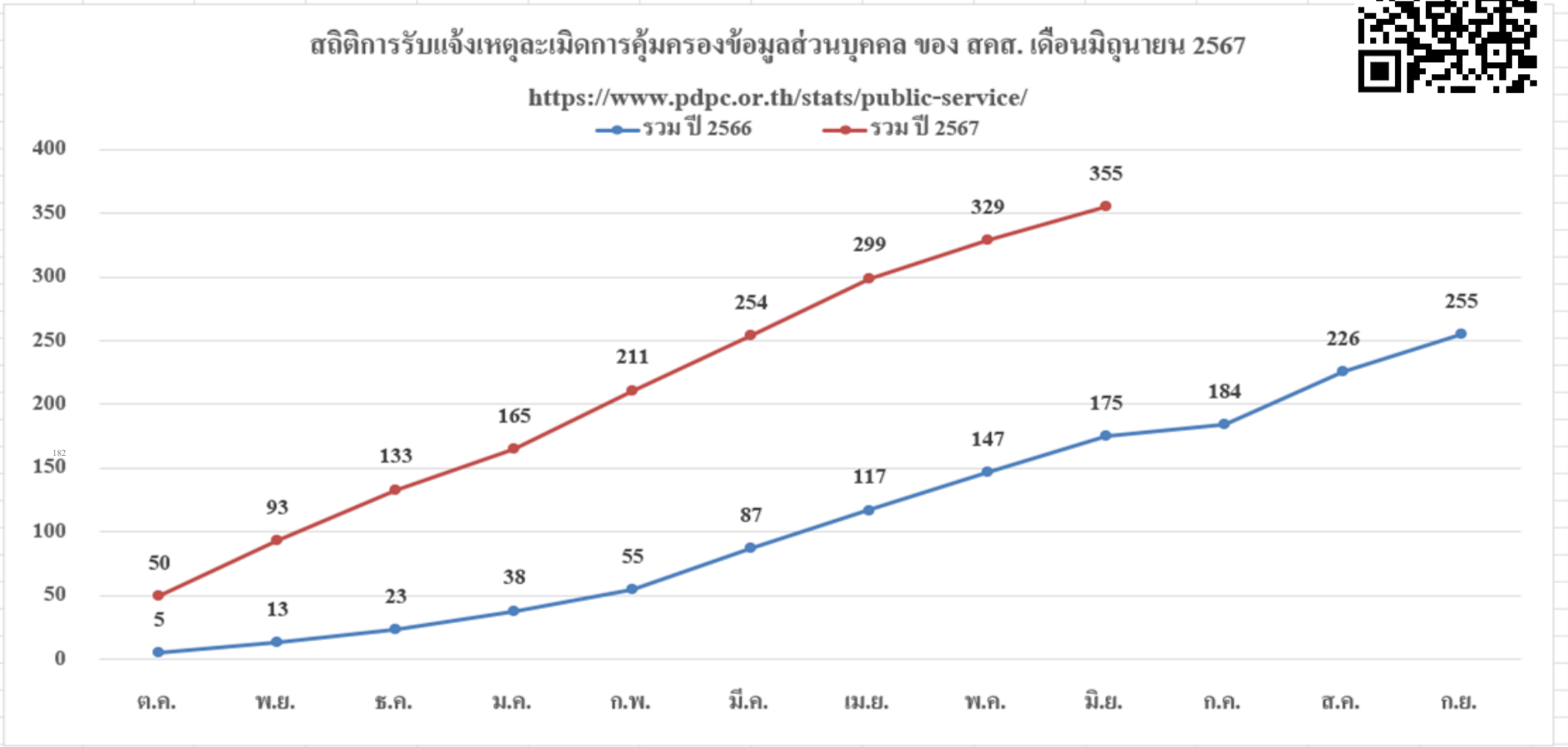
ข้อ ๗ ในกรณีที่มีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้ากว่าเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุ ไม่ว่าจะเกิดจากการตรวจสอบข้อมูลในเบื้องต้น การดำเนินการป้องกัน ระงับหรือแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลที่จำเป็น หรือมีเหตุจำเป็นอื่นอันไม่อาจก้าวล่วงได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานพิจารณายกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้าได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ที่ทำให้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า โดยจะต้องแจ้งแก่สำนักงานโดยเร็ว ทั้งนี้ ต้องไม่เกินสิบห้าวันนับแต่ทราบเหตุ

สำนักงานอาจแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผลหรือข้อเท็จจริงเพิ่มเติมภายหลังได้ และหากสำนักงานพิจารณาแล้วเห็นควรให้ยกเว้นความผิดจากการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลล่าช้า เนื่องจากมีเหตุจำเป็น ให้ถือว่าผู้ควบคุมข้อมูลส่วนบุคคลได้รับยกเว้นการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานตามกำหนดเวลาในมาตรา ๓๗ (๔)

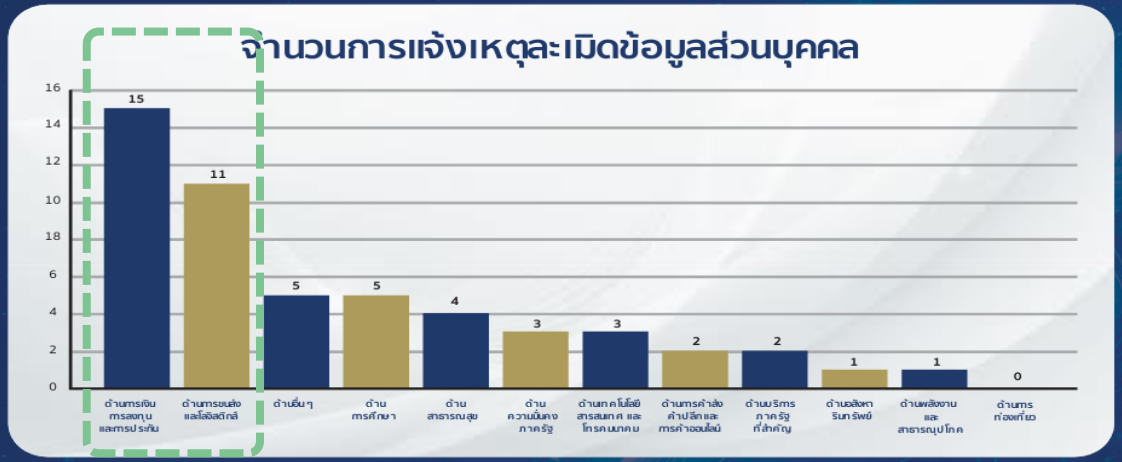
การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานไม่เป็นเหตุยกเว้นหน้าที่หรือความรับผิดของผู้ควบคุมข้อมูลส่วนบุคคลตามกฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้นหรือกฎหมายอื่น

*“เรา**ไม่มีทางป้องกันภัยทั้งภายในและภายนอกได้ 100%** แต่ถ้าเราเปลี่ยนจากคำว่าจะป้องกันอย่างไรมาเป็นควร**ตอบสนอง**อย่างไรเมื่อเกิดการเหตุการละเมิดข้อมูลส่วนบุคคล ก็จะช่วย**ลดความเสียหาย**ที่อาจเกิดขึ้นได้”*

ความสำคัญ และประโยชน์ของ การจัดการเหตุการละเมิดข้อมูลส่วนบุคคล



ภาพรวม | การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล



หมายเหตุ ข้อมูลด้านบนเป็นข้อมูลที่ สคส. ได้รับรายงานในปี 2567

จำนวนการแจ้งเหตุละเมิด

52 หน่วยงาน

ภาครัฐ	ภาคเอกชน
30 หน่วยงาน	22 หน่วยงาน

ข้อสังเกตุ

จากกราฟแสดงให้เห็นว่า หน่วยงานด้านการเงิน การลงทุน และการประกันมีจำนวนการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลมากที่สุด ซึ่งแสดงถึงความเสี่ยงในการคุ้มครองข้อมูลส่วนบุคคลที่อาจเกิดขึ้น

โทษทางปกครอง DC/DP/ตัวแทน

มาตรา ๘๓ ผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา ๒๑ มาตรา ๒๒ มาตรา ๒๔ มาตรา ๒๕ วรรคหนึ่ง มาตรา ๒๗ วรรคหนึ่งหรือวรรคสอง มาตรา ๒๘ มาตรา ๓๒ วรรคสอง หรือมาตรา ๓๗ หรือขอความยินยอมโดยการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ หรือไม่ปฏิบัติตามมาตรา ๒๑ ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๒๕ วรรคสอง หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๑๖ (๔) ประกอบมาตรา ๓๗ (๔) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ดังต่อไปนี้

มาตรา ๔๐ ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้
(๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้
(๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

มาตรา ๘๖ ผู้ประมวลผลข้อมูลส่วนบุคคลผู้ใดไม่ปฏิบัติตามมาตรา ๔๐ โดยไม่มีเหตุอันควร หรือส่งหรือโอนข้อมูลส่วนบุคคลโดยไม่เป็นไปตามมาตรา ๒๙ วรรคหนึ่งหรือวรรคสาม หรือไม่ปฏิบัติตามมาตรา ๓๗ (๕) ซึ่งได้นำมาใช้บังคับโดยอนุโลมตามมาตรา ๓๘ วรรคสอง ต้องระวางโทษปรับทางปกครองไม่เกินสามล้านบาท

ตัวอย่างแนวปฏิบัติการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

สำนักงานปลัดกระทรวงสาธารสุข

รูปแบบความเสียหายและการเยียวยา

1.รูปแบบความเสียหาย

1) **ความเสียหายเป็นทรัพย์สิน** หากเจ้าของข้อมูลส่วนบุคคลได้รับผลกระทบได้รับความเสียหายทางวัตถุหรือทางทรัพย์สิน หรือ สามารถวัดความเสียหายเป็นตัวเงินได้ เช่น ค่าใช้จ่ายในการเปลี่ยนบัตรเครดิต การเปลี่ยนหมายโทรศัพท์ ค่าเสียเวลาในการเปลี่ยนบัตรประชาชนใหม่

2) **การเสียความรู้สึก** หรือความเสียหายทางจิตใจ เช่น ความวิตกกังวล หรือความเครียด ความไม่สบายใจ

2.การเยียวยา

1) ให้เป็นจดหมายหรือหนังสือ หรืออีเมล หรือ SMS หรือลงสื่อมวลชนเพื่อขอโทษ
2) ให้ชดเชยเป็นเงินสด ส่วนลด คูปอง บัตรกำนัล แทนเงินสด
3) ให้ชดเชยเป็นสิ่งของกระเป๋า เสื้อ หมวก
4) ให้ชดเชยเป็นสิ่งของหรือบริการขององค์กร
5) ให้คำปรึกษา หรือจ้างให้คนมาปรึกษา
6) จัดกิจกรรมเฉพาะคนที่ได้รับผลประทบ

การดำเนินคดี: หากผู้ที่ได้รับผลกระทบไม่พอใจกับมาตรการเยียวยาที่ได้รับ อาจดำเนินคดีเพื่อเรียกร้องค่าเสียหายเพิ่มเติม

ตัวอย่างการแจ้งเหตุการละเมิดแบบกลุ่ม

ประกาศกรมควบคุมโรค ฉบับที่ 1
เรื่อง แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

กรมควบคุมโรค
Department of Disease Control

ด้วยเมื่อวันที่ 9 ตุลาคม 2567 เวลา 16.00 น. กรมควบคุมโรคได้รับรายงานเหตุการละเมิดข้อมูลส่วนบุคคลจากระบบฐานข้อมูลเอกสารรับรองการฉีดวัคซีนเพื่อการเดินทางระหว่างประเทศ (Database of International Vaccination Certification) หรือ INTERVAC ซึ่งทันทีที่กรมควบคุมโรคทราบเหตุดังกล่าว กรมควบคุมโรค โดยคณะทำงานเพื่อปฏิบัติหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) กรมควบคุมโรค ได้ดำเนินการตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้า ซึ่งได้มีการประสานและหารือร่วมกันระหว่างกรมควบคุมโรคกับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ตั้งแต่วันที่ 9 ตุลาคม 2567 เวลา 16.30 น. เพื่อประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และตรวจสอบข้อเท็จจริง รวมถึงความเสียหายที่เกิดขึ้น พบว่า ข้อมูลที่มีการเข้าถึงและคัดลอกออกจากระบบโดยมิชอบ เป็นข้อมูลส่วนบุคคลทั่วไป และข้อมูลเกี่ยวกับประวัติการฉีดวัคซีนของผู้ที่มาขอรับบริการออกหนังสือรับรองการสร้างเสริมภูมิคุ้มกันโรค เพื่อใช้สำหรับการเดินทางระหว่างประเทศ อย่างไรก็ดี กรมควบคุมโรคได้ดำเนินการป้องกัน ระงับ และแก้ไข โดยการปิดกั้นการเข้าถึง Internet จากภายนอกประเทศไทย เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดและไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที และตรวจสอบความเสียหายของระบบฐานข้อมูลเอกสารรับรองการฉีดวัคซีนเพื่อการเดินทางระหว่างประเทศ (Database of International Vaccination Certification) หรือ INTERVAC ได้แก่ ตรวจสอบความปลอดภัยทางไซเบอร์ ตรวจสอบระบบฐานข้อมูลที่ข้อมูลรั่วไหล ไม่ให้มีแฮกเกอร์อยู่ในระบบ และปิดช่องโหว่ที่อาจเกิดขึ้นได้ ทั้งนี้ ผลการตรวจสอบ ยังไม่พบความเสียหาย ทำลาย หรือการแก้ไขข้อมูลกับระบบปฏิบัติการที่ใช้ในการกรอกข้อมูลให้บริการออกหนังสือรับรองฯ แต่อย่างใด

การแก้ไขปัญหา

กรมควบคุมโรคร่วมกับศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติได้ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง และแก้ไขเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าวด้านกระบวนการเทคโนโลยี ดังนี้

1. มาตรการที่ดำเนินการทันที ได้แก่

(1) จัดการระบบฐานข้อมูลด้วยการ Block IP Address ที่มีประวัติการเข้าระบบฯ มาคัดลอกข้อมูลแบบผิดปกติโดยทันที

(2) เพิ่มรายละเอียดในการบันทึกข้อมูลก่อนเข้าใช้งานระบบ

(3) จำกัดการเข้าสู่ระบบโดยอนุญาตให้เข้าใช้งานได้เฉพาะ IP Address ในประเทศไทย และ Block การเรียกดูข้อมูลจากการแก้ไข ID ใน URL โดยให้มีการเฝ้าระวังเหตุการณ์ละเมิดอย่างต่อเนื่อง และจำกัดช่วงเวลาเข้าใช้งานระบบให้อยู่ในเฉพาะเวลาราชการ

(4) จำกัดจำนวนรายการที่ผู้ใช้งานในระบบสามารถเข้าถึงได้ต่อวัน

2. มาตรการที่อยู่ระหว่างดำเนินการ คือ เร่งปรับปรุงระบบเพื่อปิดช่องโหว่ส่วนอื่นของระบบที่ได้จากการตรวจสอบระบบทั้งหมด ซึ่งกรมควบคุมโรคได้ขอรับคำปรึกษาจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้คำแนะนำและเป็นที่ปรึกษาในการปรับปรุงระบบคอมพิวเตอร์ของระบบบริการฯ ให้มีความปลอดภัย และมีประสิทธิภาพมากยิ่งขึ้น เพื่อสร้างความมั่นใจในการให้บริการต่อไป

ทั้งนี้ คณะทำงานเพื่อปฏิบัติหน้าที่เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) กรมควบคุมโรค ได้ดำเนินการด้านกฎหมายโดยการรายงานผู้บังคับบัญชาตามลำดับ และดำเนินการแจ้งเหตุการณ์ละเมิดพร้อมเข้าชี้แจงข้อมูลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนรายงานต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรียบร้อยแล้ว และฐานข้อมูลเอกสารรับรองการฉีดวัคซีนเพื่อการเดินทางระหว่างประเทศ (Database of International Vaccination Certification) หรือ INTERVAC สามารถใช้งานได้ปกติ

จากเหตุการละเมิดดังกล่าว กรมควบคุมโรคได้มีกลไกการพิจารณามาตรการป้องกันและจัดการเหตุการณ์ในรูปแบบคณะทำงานจากระดับหน่วยงานนำเสนอต่อคณะทำงานระดับกรม ทั้งมาตรการที่ต้องดำเนินการทันที รวมถึงแผนการดำเนินงานในระยะสั้นและระยะยาว เพื่อการป้องกันและการเก็บรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัยมากยิ่งขึ้น

กรมควบคุมโรคขออภัยในปัญหาที่เกิดขึ้น และจะพัฒนาระบบสารสนเทศให้มีความปลอดภัยเพื่อคุณภาพในการให้บริการให้ดียิ่งขึ้น ทั้งนี้ หากผู้ใดมีข้อสงสัยหรือได้รับผลกระทบที่เกิดจากเหตุการณ์ละเมิดฯ สามารถติดต่อกรมควบคุมโรค ผ่านช่องทางศูนย์รับเรื่องร้องเรียนของกรมควบคุมโรค อาคาร 1 ชั้น 1 กรมควบคุมโรค โทรศัพท์หมายเลข 0 2590 3000, 0 2590 3269 และสายด่วนกรมควบคุมโรค 1422 หรือช่องทางการติดต่อข้อร้องเรียน เช่น เว็บไซต์กรมควบคุมโรค เฟซบุ๊กศูนย์รับเรื่องร้องเรียนกรมควบคุมโรค หรืออีเมล complaintddc@ddc.mail.go.th เป็นต้น

ประกาศ ณ วันที่ 8 พฤศจิกายน 2567

การแจ้งเหตุการณ์การละเมิดให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ช่องทางการแจ้งเหตุ

โทร : 02 142 1033, 02 141 6993

E-mail : saraban@pdpc.or.th

หรือที่ตั้งของสำนักงานฯ : www.pdpc.or.th

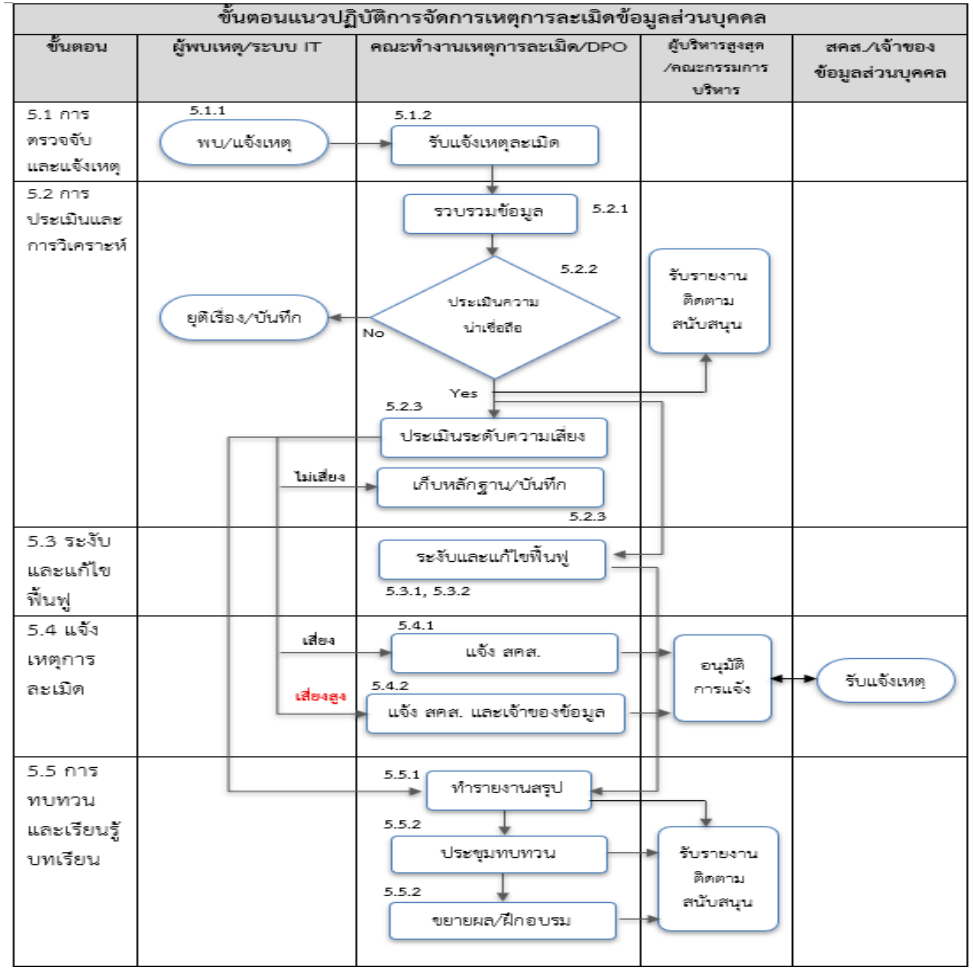
ระเบียบปฏิบัติการจัดการเหตุการละเมิด

มหาวิทยาลัยราชภัฏสกลนคร

(Sakolnakorn Rajabhat University)

ระเบียบปฏิบัติการจัดการเหตุการละเมิดข้อมูลส่วนบุคคล

(Personal Data Breach Management Procedure)



แบบฟอร์มการรับแจ้ง และการแจ้งเหตุการละเมิด

รับแจ้ง (บุคคลใด ๆ)

แบบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล มหาวิทยาลัยราชภัฏสกลนคร

ส่วนที่ 1 ข้อมูลของผู้แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

เพื่อการยืนยันตัวตนของผู้แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ขอให้ท่านกรอกข้อมูลของท่านตามที่ระบุไว้ดังต่อไปนี้ ชื่อ.....นามสกุล.....
ที่อยู่.....
เบอร์โทรศัพท์ที่ติดต่อได้..... อีเมล .....

ส่วนที่ 2 รายละเอียดของเหตุการละเมิดข้อมูลส่วนบุคคล (พร้อมแนบหลักฐาน (หากมี))

.....
.....
.....

ส่วนที่ 3 การดำเนินงานของมหาวิทยาลัย ภายหลังจากที่ได้รับการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

มหาวิทยาลัยฯ ขอขอบคุณที่ท่านกรุณาแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลพร้อมทั้งเอกสารและรายละเอียดที่เกี่ยวข้อง ทั้งนี้มหาวิทยาลัยจะรีบดำเนินการพิจารณาเรื่องดังกล่าวโดยเร็ว หากมีกรณีที่มหาวิทยาลัยฯ อาจต้องการการอธิบายเพิ่มเติมจากท่าน มหาวิทยาลัยฯ จะดำเนินการติดต่อท่านกลับไปตามรายละเอียดที่ท่านได้ให้ไว้ในส่วนที่ 1

ส่วนที่ 4 คำรับรอง

ข้าพเจ้าขอยืนยันว่า ข้าพเจ้าได้อ่านและเข้าใจเนื้อหาและข้อกำหนดตามที่ระบุไว้ในแบบการแจ้งเหตุฉบับนี้ พร้อมทั้งรับรองว่าข้อมูลดังกล่าวที่ข้าพเจ้าให้ไว้ตามเอกสารฉบับนี้ถูกต้องครบถ้วนและสมบูรณ์ ข้าพเจ้าขอยืนยันและรับประกันว่า ข้าพเจ้าไม่มีเจตนาดำเนินการเพื่อก่อให้เกิดความเสียหายกับบุคคลใด ข้าพเจ้าจึงได้ลงลายมือชื่อตามที่ระบุด้านล่างนี้

ลายมือชื่อ.....
(.....)
วันที่.....

เอกสารประกอบการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
1. เอกสารที่สูงบัตรของผู้แจ้งเหตุ
- (กรณีคนไทย) สำเนาบัตรประจำตัวประชาชน พร้อมรับรองสำเนาถูกต้อง 1 ฉบับ (กรณีสัญชาติไทย)
- (กรณีต่างชาติ) สำเนา Passport พร้อมรับรองสำเนาถูกต้อง 1 ฉบับ
2. หลักฐานอื่นๆ ประกอบการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล
"ส่งแบบฟอร์ม พร้อมเอกสารประกอบได้ที่ email : dpo@skn.ac.th หรือ Fax หมายเลข.

ประเมินว่าเสี่ยง

ลับ แจ้ง สคส.

แบบ ตข. ๐๐๑

	ที่อยู่หน่วยงาน : มหาวิทยาลัยราชภัฏสกลนคร
แบบฟอร์มการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	
เรื่อง แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล	
เรียน เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	
รายการ	**รายละเอียด**
หน่วยงาน	(ฐานะความเป็นนิติบุคคลตามกฎหมายของหน่วยงาน)
กลุ่มอุตสาหกรรมเป้าหมาย (เลือกเพียง 1 ข้อ)	☐ ด้านความมั่นคงและด้านอื่นๆ ☐ ด้านหน่วยงานของรัฐ – รัฐวิสาหกิจ ☐ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ☐ ด้านการขนส่งและโลจิสติกส์ ☐ ด้านพลังงาน สาธารณูปโภค และอุตสาหกรรมการผลิต ☐ ด้านสาธารณสุข ☒ ด้านการศึกษา ☐ ด้านการเงิน การลงทุน และการประกัน ☐ **ด้านการท่องเที่ยวและกีฬา** ☐ ด้านการค้าปลีก – ค้าส่ง และการค้าออนไลน์ ☐ ด้านอสังหาริมทรัพย์
ข้อมูลเกี่ยวกับลักษณะการละเมิดข้อมูลส่วนบุคคล	(อธิบายเหตุการละเมิดข้อมูลส่วนบุคคลโดยละเอียด)
ปริมาณของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด	(จำนวนเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลที่เกี่ยวข้องกับเหตุการละเมิด)
ลักษณะหรือประเภทข้อมูลส่วนบุคคลที่ได้รับผลกระทบ	(ชื่อ - สกุล, เบอร์โทรศัพท์, ที่อยู่ หรืออื่นๆ)

แบบฟอร์มแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล แบบกลุ่ม

ประกาศมหาวิทยาลัย

เรื่อง แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

เนื่องด้วยเมื่อวันที่.....เวลา..... น. มหาวิทยาลัยสกลนคร ("มหาวิทยาลัย") ได้รับรายงานเหตุการละเมิดข้อมูลส่วนบุคคล จาก..... ซึ่งทันทีที่มหาวิทยาลัยทราบเหตุดังกล่าว มหาวิทยาลัย โดยคณะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO committee) ได้ดำเนินการ ตรวจสอบข้อเท็จจริงเกี่ยวกับเหตุการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้า เพื่อยืนยันความน่าเชื่อถือของข้อมูลเหตุการละเมิดที่ได้รับ และได้มีการประสานเพื่อหารือร่วมกันระหว่างมหาวิทยาลัยกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ซึ่งเป็นหน่วยงานกำกับดูแลเรื่องการคุ้มครองข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ตั้งแต่วันที่.....เวลา ..... น. เพื่อประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลที่เกี่ยวข้องกับเหตุการณ์ละเมิดในครั้งนี้ รวมทั้งตรวจสอบข้อเท็จจริง และความเสียหายที่อาจจะเกิดขึ้น และมาตรการที่เหมาะสมที่จำเป็นเพื่อแก้ไขป้องกันเหตุการละเมิดในครั้งนี้ ซึ่งมีรายละเอียดดังต่อไปนี้

1) ลักษณะของการละเมิด (ความลับ, ความถูกต้อง, ความพร้อมใช้).....
2) ข้อมูลที่ถูกละเมิดมีดังต่อไปนี้.....
3) ประเภทของเจ้าของข้อมูลหรือความสัมพันธ์กับมหาวิทยาลัยที่เกี่ยวข้องกับเหตุการละเมิด คือ.....
4) ผลกระทบที่อาจเกิดขึ้นกับท่านที่เป็นเจ้าของข้อมูลที่ถูกละเมิด คือ.....
5) แนวทางการเยียวยาความเสียหายสำหรับเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ คือ.....
6) มาตรการที่ทางมหาวิทยาลัยจะดำเนินการแก้ไขป้องกันเหตุการละเมิดในครั้งนี้ คือ.....
7) สิ่งที่ท่านที่เป็นเจ้าของข้อมูลที่ต้องดำเนินการเพิ่มเติมสำหรับการเยียวยาในครั้งนี้ คือ.....
8) มาตรการป้องกันที่ท่านต้องดำเนินการด้วยตัวเอง เพื่อป้องกันแก้ไขเหตุการละเมิด เพื่อป้องกันผลกระทบที่อาจเกิดขึ้น คือ.....
9) ท่านสามารถติดต่อสอบถามเพิ่มเติมได้ที่.....(ชื่อ สถานที่ติดต่อ และวิธีการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคล ที่ได้รับมอบหมาย)

อย่างไรก็ดี มหาวิทยาลัย ได้ดำเนินการตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยการรายงานผู้คับบัญชาตามลำดับ และดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นหนังสือ และแจ้งให้ท่านที่เป็นเจ้าของข้อมูลส่วนบุคคลรับทราบตามประกาศฉบับนี้

มหาวิทยาลัยรู้สึกเสียใจ และต้องขออภัยเป็นอย่างสูงกับเหตุการละเมิดในครั้งนี้ มหาวิทยาลัยจะดำเนินการทบทวน ตรวจสอบ และปรับปรุง มาตรการ และกิจกรรมที่เกี่ยวข้อง หรือใกล้เคียงกัน เพื่อเป็นการขยายผลและพัฒนามาตรการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัยให้ดียิ่งขึ้น เพื่อสร้างความมั่นใจแก่ท่านที่เป็นเจ้าของข้อมูลส่วนบุคคลต่อไป

หากท่านที่เป็นเจ้าของข้อมูลส่วนบุคคลจากเหตุการละเมิดในครั้งนี้ เกิดมีข้อสงสัยหรือได้รับผลกระทบจากเหตุการละเมิดนี้ ท่านสามารถติดต่อทางมหาวิทยาลัย ผ่านช่องทางตามข้อ 9

ประกาศ ณ วันที่.....

ลงชื่อ.....


ANY QUESTIONS?

www.pdpc.or.th