



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ดร. สุนทรีย์ ส่งเสริม
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

20 มกราคม 2564

ประโยชน์ที่ได้รับจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประชาชน

- ☐ รับทราบวัตถุประสงค์ของการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลอย่างแจ่มชัด
- ☐ ขอให้ลบ ทำลาย หรือขอให้ระงับการใช้ข้อมูลส่วนบุคคลได้
- ☐ สามารถร้องเรียนและขอให้ชดเชยค่าสินไหมทดแทน หากมีการใช้ข้อมูลฯ นอกเหนือจากวัตถุประสงค์ที่แจ้งไว้แต่แรก
- ☐ ลดความเดือดร้อนรำคาญ หรือความเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคล

หน่วยงานรัฐและเอกชน

- ☐ ยกระดับความเชื่อมั่นในมาตรฐานการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล ในระบับ นานาชาติ
- ☐ มีขอบเขตในการจัดเก็บ ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลที่ชัดเจน
- ☐ การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลมีความโปร่งใส รับผิดชอบต่อสังคม ตรวจสอบได้

ประเทศ

- ☐ มีมาตรการในการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล ส่งเสริมภาพลักษณ์ที่ดีของประเทศ
- ☐ มีเครื่องมือในการกำกับการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคล
- ☐ สามารถสร้างสังคมที่เข้มแข็ง เนื่องจากสามารถตรวจสอบการดำเนินงานภาครัฐและภาคธุรกิจ เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้มีความถูกต้องเหมาะสม

ประโยชน์ที่ได้รับ

การบังคับใช้กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

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

ประกาศในราชกิจจานุ 27 พ.ค. 62

บังคับใช้ระยะที่ 1

28 พ.ค. 62 (หมวด 1 คณะกรรมการฯ และ หมวด 4 สำนักงานฯ) และบทเฉพาะกาลที่เกี่ยวข้อง

บังคับใช้ระยะที่ 2

27 พ.ค. 63 บังคับใช้ครบทุกหมวด ได้แก่

▶ หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล

▶ หมวด 5 การร้องเรียน

▶ หมวด 7 บทกำหนดโทษ (โทษอาญา-ปกครอง)

▶ หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล

▶ หมวด 6 ความรับผิดชอบทางแพ่ง

พ.ร.ฎ. กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคล
ไม่อยู่ภายใต้บังคับแห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.
2562 พ.ศ. 2563 ใช้บังคับตั้งแต่ 27 พ.ค. 63 ถึง 31 พ.ค. 64

บทเฉพาะกาล มาตรา 96

การออกระเบียบและประกาศตาม พ.ร.บ. นี้

ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปี

นับแต่วันที่ พ.ร.บ. นี้ใช้บังคับ (27 พ.ค. 64)

พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับ
แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ใช้บังคับตั้งแต่ 27 พฤษภาคม 2563 ถึง 31 พฤษภาคม 2564 ยกเว้นให้ผู้ควบคุมข้อมูลส่วนบุคคล 22 หน่วยงานหรือกิจการ ยังไม่ต้องปฏิบัติตามบางหมวดในกฎหมาย
ได้แก่ การคุ้มครองข้อมูลส่วนบุคคล สิทธิของเจ้าของข้อมูล การร้องเรียน ความรับผิดชอบทางแพ่ง และบทกำหนดโทษ

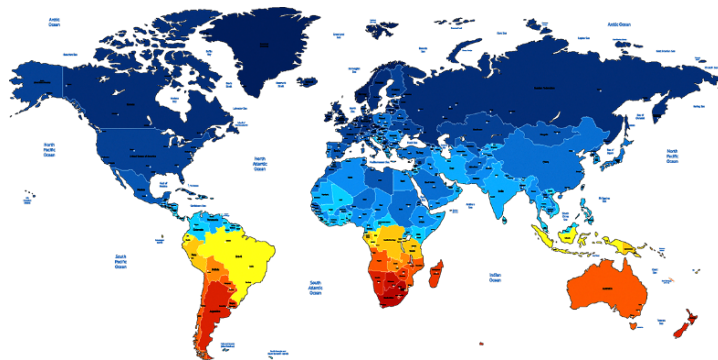
- | | |
|--|--|
| 1 หน่วยงานของรัฐ | 12 กิจการด้านการท่องเที่ยว |
| 2 หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ | 13 กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล |
| 3 มูลนิธิ สมาคม องค์การศาสนา และองค์กรไม่แสวงหาผลกำไร | 14 กิจการด้านการเงิน การธนาคาร และการประกันภัย |
| 4 กิจการด้านเกษตรกรรม | 15 กิจการด้านอสังหาริมทรัพย์ |
| 5 กิจการด้านอุตสาหกรรม | 16 กิจการด้านการประกอบวิชาชีพ |
| 6 กิจการด้านพาณิชยกรรม | 17 กิจการด้านการบริหารและบริการสนับสนุน |
| 7 กิจการด้านการแพทย์และสาธารณสุข | 18 กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ |
| 8 กิจการด้านพลังงาน ใต้น้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง | 19 กิจการด้านการศึกษา |
| 9 กิจการด้านการก่อสร้าง | 20 กิจการด้านความบันเทิงและนันทนาการ |
| 10 กิจการด้านการซ่อมและการบำรุงรักษา | 21 กิจการด้านการรักษาความปลอดภัย |
| 11 กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า | 22 กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรมได้อย่างชัดเจน |

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลให้เป็นไปตาม

มาตรฐานที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนด

- ◆ ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
- ◆ แจกมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล ให้แก่บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบ เพื่อให้ปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด
- ◆ จัดให้มีมาตรการเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วย
 - ① การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผล
 - ② การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
 - ③ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
 - ④ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
 - ⑤ การจัดให้มีวิธีการตรวจสอบย้อนหลังการเข้าถึงข้อมูลส่วนบุคคลได้
- ◆ สามารถใช้มาตรฐานความมั่นคงปลอดภัยที่สูงกว่าประกาศฉบับนี้ได้

- ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร
- มีผลใช้บังคับถึงกรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร หากมีกิจกรรมดังนี้
 - (1) เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่
 - (2) การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร



หน่วยงานภาครัฐ

หน่วยงานภาคเอกชน



บุคคลธรรมดา

ข้อมูลในรูปแบบดิจิทัล

ข้อมูลในรูปแบบกระดาษ

ข้อมูลส่วนบุคคล (Personal Data)

มาตรา 6

ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล ฯลฯ

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)

มาตรา 26

ข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล เช่น
เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ
ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ
ทั้งนี้ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

มาตรา 6

บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น กรมสรรพากร ร้านค้าออนไลน์ Lazada Shopee JDCentral ฮาชั้นอาหารทะเลตากแห้ง ธนาคารกรุงเทพ บริษัท ขนส่ง จำกัด บริษัท ไปรษณีย์ไทย จำกัด

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

มาตรา 6

บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล (และไม่ใช่เจ้าหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล)

เช่น บริษัท รปภ. จำกัด (รับดูแลระบบการรักษาความปลอดภัยของหน่วยงาน)
บริษัท

การเก็บข้อมูลส่วนบุคคล

หลักการ เก็บรวบรวมข้อมูลส่วนบุคคล

มาตรา 22 - 23

เก็บเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย และ **จะต้องแจ้งวัตถุประสงค์** ให้เจ้าของข้อมูลส่วนบุคคลทราบ

หลักการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป

มาตรา 24 และ 27

- 1 ได้รับความยินยอมจากเจ้าของข้อมูล (Consent)
- 2 เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research)
- 3 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)
- 4 มีความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (Necessary for the performance of contracts)
- 5 มีความจำเป็นเพื่อดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล หรือปฏิบัติหน้าที่ในการใช้อำนาจอรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล (Public Task)
- 6 มีความจำเป็นในการดำเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมิดสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
- 7 เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด **โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล**

เว้นแต่

- 1 ป้องกันหรือระงับอันตรายต่อชีวิต
- 2 ขอบด้วยกฎหมายของมูลนิธิ สมาคม องค์กร
- 3 เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้ง
- 4 การก่อตั้งสิทธิเรียกร้องตามกฎหมาย
- 5 จำเป็นในการปฏิบัติตามกฎหมาย

ก) เวชศาสตร์ป้องกัน การวินิจฉัยโรคและการรักษาทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคมหรือด้านสังคมสงเคราะห์

ข) ประโยชน์สาธารณะด้านการสาธารณสุข

ค) คัมครองแรงงาน ประกันสังคม หลักประกันสุขภาพแห่งชาติ

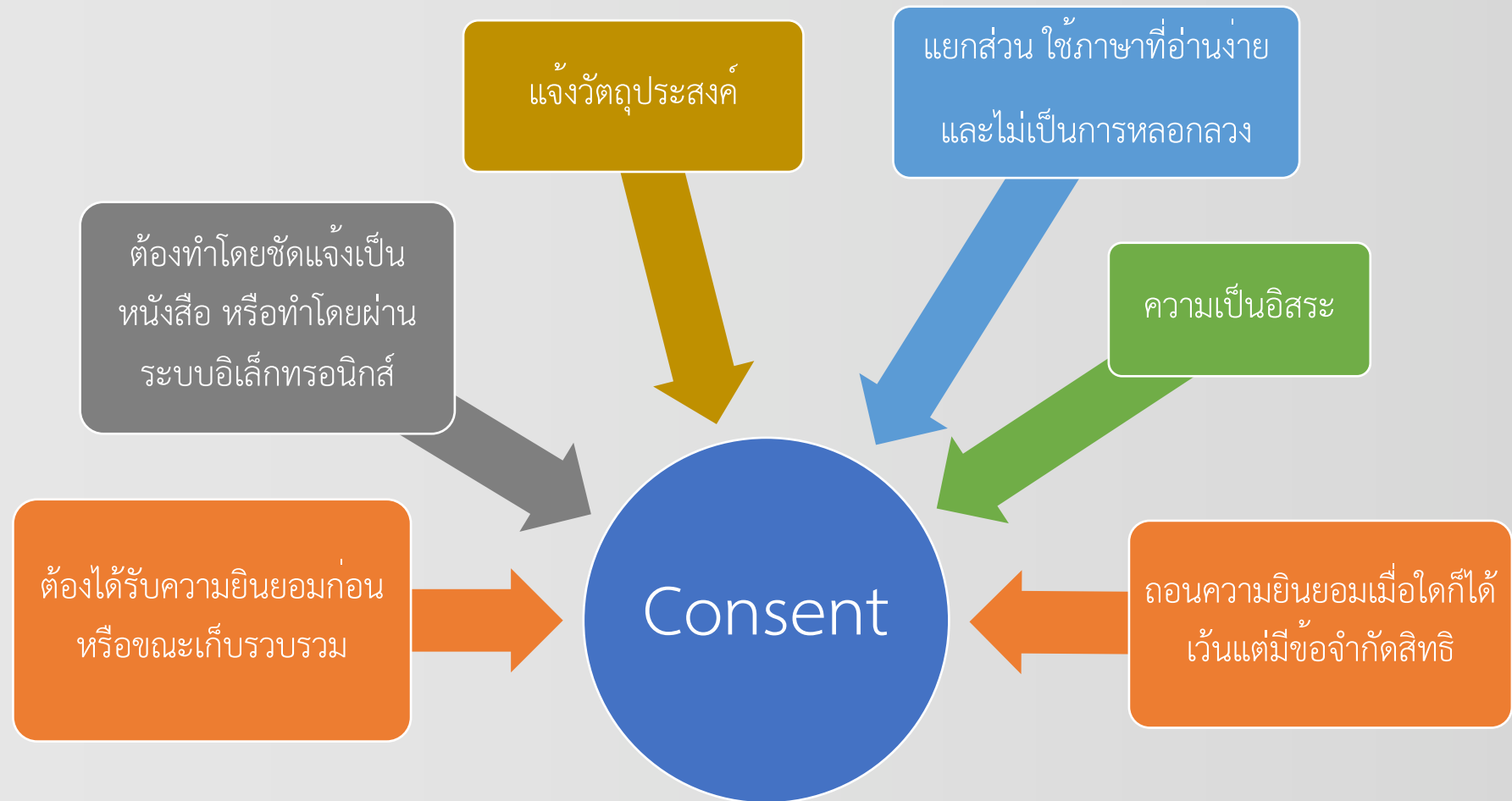
ง) วิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ สถิติ

จ) ประโยชน์สาธารณะที่สำคัญ โดยมีมาตรการเพื่อคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคล
จากแหล่งอื่นที่ไม่ใช่จากเจ้าของ
ข้อมูลส่วนบุคคลโดยตรง

ข้อยกเว้น

- (1) แจ้งเจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า
แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม
และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
- (2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคล
ที่ได้รับการยกเว้นไม่ต้องขอความยินยอม



สิทธิของเจ้าของข้อมูลส่วนบุคคล

สิทธิขอเข้าถึงและขอรับสำเนา มาตรา 30 (Right of Access)



เจ้าของข้อมูลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลที่เกี่ยวข้องกับตนหรือขอให้เปิดเผยถึงที่มาของข้อมูลที่ไม่ได้ให้ความยินยอม ผู้ควบคุมจะปฏิเสธได้ก็เฉพาะเมื่อเป็นการปฏิเสธตามคำสั่งศาลหรือตามกฎหมาย หรือเป็นการขอเข้าถึงที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพผู้อื่น

สิทธิขอให้โอนข้อมูล มาตรา 31 (Right to data portability)



จะใช้สิทธินี้ได้ต้องเป็นข้อมูลที่เก็บรวบรวมจากการให้ความยินยอมหรือฐานสัญญาตามมาตรา 24 (3) เท่านั้น

สิทธิคัดค้าน มาตรา 32 (Right to object)



จะใช้สิทธินี้ได้ต้องเป็นข้อมูลที่เก็บรวบรวมจากฐานภารกิจของรัฐตามมาตรา 24 (4) และฐานการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายตามมาตรา 24 (5) หรือเก็บรวบรวมเพื่อการตลาดแบบตรง หรือเพื่อการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติเท่านั้น

สิทธิขอให้ลบหรือทำลาย มาตรา 33 (Right to be forgotten)



ไม่สามารถใช้สิทธินี้ได้หากเก็บข้อมูลไว้เพื่อการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือเป็นการศึกษาวิจัยหรือสถิติตามมาตรา 24 (1) หรือเพื่อดำเนินภารกิจของรัฐตามมาตรา 24 (4) หรือเป็นข้อมูลอ่อนไหวเพื่อประโยชน์ทางการแพทย์หรือการสาธารณสุขตามมาตรา 26 (5) (ก) หรือ (ข)

สิทธิขอให้ระงับการใช้ มาตรา 34 (Right to restrict processing)



มีสิทธิขอให้ระงับการใช้ได้ชั่วคราว

สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง มาตรา 35 (Right to rectification)



มีสิทธิขอให้ผู้ควบคุมแก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด



หน้าที่ของผู้เกี่ยวข้อง

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 37



- 1 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
- 2 ป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
- 3 จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
- 4 แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชม. นับแต่ทราบเหตุ
- 5 แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่างชาติ
- 6 จัดทำบันทึกการ (มาตรา 38)

หน้าที่ของผู้ประมวลข้อมูลส่วนบุคคล

มาตรา 40

หากประมวลผลข้อมูลส่วนบุคคล นอกเหนือคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล ให้ถือว่า
ผู้ประมวลผลข้อมูลส่วนบุคคล เป็น ผู้ควบคุมข้อมูลส่วนบุคคล

- 1 ทำตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
- 2 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
- 3 แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- 4 จัดทำและเก็บรักษารายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- 5 แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีเป็นผู้ประมวลผลข้อมูลส่วนบุคคลต่างชาติ

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มี DPO

มาตรา 41

- 1 หน่วยงานของรัฐ ตามที่ประกาศกำหนด
- 2 การดำเนินกิจกรรมในการเก็บรวบรวม ใช้ หรือเปิดเผยจำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่ประกาศกำหนด
- 3 กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บรวบรวม ใช้ หรือเปิดเผย Sensitive Personal Data



หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

มาตรา 42

- 1 ให้คำแนะนำ
- 2 ตรวจสอบการดำเนินงานเกี่ยวกับการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล
- 3 ประสานงานและให้ความร่วมมือกับสำนักงานฯ
- 4 รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามกฎหมายนี้

หน้าที่การบันทึกรายการ ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มาตรา 39, 40

- การบันทึกรายการตามมาตรา 39 อาจยกเว้นให้กับ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นกิจการขนาดเล็ก ตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่การประมวลผลนั้นมีความเสี่ยงที่จะกระทบสิทธิของเจ้าของข้อมูลส่วนบุคคล หรือมีใช้กิจการที่มีการประมวลผลเป็นครั้งคราว หรือ ประมวลผลข้อมูลตามมาตรา 26
- ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่ในการบันทึก การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิ

การตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) มาตรา 41 (2)

- การดำเนินกิจกรรมของ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก ตามที่คณะกรรมการประกาศกำหนด



หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

มาตรา 37

- แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล แก่สำนักงาน ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ
- จัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
- กรณีที่การละเมิดมีความเสี่ยงสูงที่กระทบบุคคล ให้แจ้งเหตุให้เจ้าของข้อมูลส่วนบุคคล พร้อมแนวทางเยียวยา

หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

มาตรา 40

- ดำเนินงาน ตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล
- ทำตามข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล
- หาก ดำเนินงานนอกเหนือจากที่ได้รับมอบหมาย ให้ถือว่าเป็น ผู้ควบคุมข้อมูลส่วนบุคคล

ความรับผิดทางแพ่ง

ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

โทษทางอาญา

มีโทษอาญากรณีละเมิดข้อมูลส่วนบุคคลอ่อนไหวตามมาตรา 26 กรณีความผิดส่วนบุคคล และกรณีความผิดของนิติบุคคล

มาตรา 79 –81

โทษทางปกครอง

คณะกรรมการผู้เชี่ยวชาญมีอำนาจสั่งโทษปรับทางปกครองได้โดยคำนึงถึงความร้ายแรงของพฤติกรรม
ขนาดของกิจการ กำหนดโทษปรับทางปกครอง

โทษปรับทางปกครอง ตั้งแต่ 1,000,000 – 5,000,000 บาท

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. นี้ใช้บังคับ

- 1 ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม
ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูล
- 2 ส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถ
แจ้งยกเลิกความยินยอมได้โดยง่าย
- 3 การเปิดเผยและการดำเนินการอื่นที่มีใช้การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้เป็นไปตาม
พระราชบัญญัตินี้



การเตรียมความพร้อมระดับองค์กร

1. การตั้งคณะทำงาน (Working Group) ภายในองค์กร

การตั้งคณะทำงานภายในองค์กรควรประกอบไปด้วยกลุ่มคนต่อไปนี้

ฝ่ายกำหนดนโยบายและยุทธศาสตร์ขององค์กร

ฝ่ายกฎหมาย

ฝ่ายเทคโนโลยีสารสนเทศ

ฝ่ายบุคคล หรือฝ่ายที่เกี่ยวข้องกับขบวนการทางธุรกิจขององค์กร



เพื่อศึกษาและทำความเข้าใจบริบทของกฎหมาย และเตรียมความพร้อมในการตรวจสอบ และปรับปรุง การดำเนินขององค์กรให้สอดคล้องตามข้อกำหนดของกฎหมาย



2. การสำรวจข้อมูล (Data Inventory)

รวบรวมกิจกรรมที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลทุกประเภทขององค์กร

- สำรวจข้อมูลที่มีอยู่ในองค์กรตามกระบวนการไหลของข้อมูล (Data flows)
- จำแนกข้อมูลให้เป็นหมวดหมู่ ข้อมูลธุรกิจ ข้อมูลความลับ ข้อมูลส่วนบุคคลทั่วไป ข้อมูลส่วนบุคคลอ่อนไหว

จัดทำรายการข้อมูลส่วนบุคคลที่มีใช้ในปัจจุบัน โดยระบุแหล่งที่มา การจัดเก็บ และการใช้งานข้อมูล

- ระบุแหล่งที่มาของข้อมูลส่วนบุคคล วิธีการจัดเก็บ จัดเก็บไว้ด้วยเหตุผลใด และใครมีสิทธิเข้าถึงข้อมูลเหล่านั้นบ้าง
- พิจารณาฐานการประมวลผลที่ชอบด้วยกฎหมาย (Lawfulness of processing) ทั้งในส่วน of ข้อมูลส่วนบุคคลแบบทั่วไป (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) ตามมาตรา 24 และมาตรา 26 โดยลำดับ

3. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

- อธิบายขอบเขตและวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล (จัดเก็บ ใช้เปิดเผย)
- ประเมินความจำเป็นในการประมวลผลข้อมูลส่วนบุคคล
- จัดระดับความเสี่ยงที่จะมีผลกระทบต่อเสรีภาพของบุคคล การดำเนินธุรกิจ ชื่อเสียงและความเสียหายด้านการเงิน
- กำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานให้เหมาะสมกับความเสี่ยงและผลกระทบที่จะเกิดขึ้น



4. จัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน



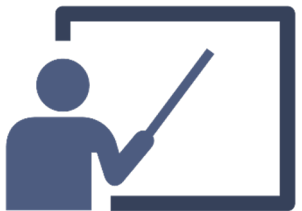
หน่วยงานควรพิจารณาจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่มีเนื้อหาครอบคลุมตามหลักการอย่างน้อย ดังนี้ การเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น การกำหนดวัตถุประสงค์ที่ชัดเจน การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามฐานการประมวลผล การรักษาความมั่นคงปลอดภัยข้อมูล วิธีการติดต่อและการใช้สิทธิของเจ้าของข้อมูล

5. จัดทำบันทึกการกิจกรรมที่เกี่ยวข้อง (Record of Processing)

ตามมาตรา 39 และ 40 หน่วยงานต้องจัดทำบันทึกการกิจกรรม เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานตรวจสอบได้ ซึ่งประกอบด้วย

- 1) ข้อมูลที่มีการจัดเก็บ
- 2) วัตถุประสงค์ของการจัดเก็บ
- 3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- 4) ระยะเวลาการเก็บ
- 5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล
- 6) การใช้หรือเปิดเผยข้อมูลที่ได้รับการยกเว้นไม่ต้องขอความยินยอม
- 7) เหตุผลในการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- 8) คำอธิบายเกี่ยวกับมาตรการการรักษาความมั่นคงปลอดภัย

6. สร้างความตระหนักรู้ และฝึกอบรม



หน่วยงานต้องสร้างความตระหนักรู้ สำคัญรับผิดชอบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล และหน้าที่ความรับผิดชอบของหน่วยงาน รวมถึงการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และผลกระทบที่เกิดขึ้นจากการละเมิดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ให้แก่บุคลากรของหน่วยงาน โดยการเผยแพร่ข้อมูลข่าวสาร และการฝึกอบรมให้ความรู้ที่เกี่ยวข้องเป็นประจำสม่ำเสมอ

7. กำกับดูแลและตรวจสอบอย่างสม่ำเสมอ



หน่วยงานจะต้องมีการกำกับดูแล และตรวจสอบการดำเนินงานบุคคลากร และผู้เกี่ยวข้องเพื่อให้เกิดการปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่หน่วยงานทำการรวบรวม จัดเก็บ และเผยแพร่ถูกควบคุมภายใต้มาตรการที่กำหนดไว้

8. ทบทวนหรือปรับปรุงกระบวนการงานและมาตรการที่เกี่ยวข้อง

หน่วยงานต้องทบทวนหรือปรับปรุงกระบวนการงานและมาตรการที่เกี่ยวข้องกับการรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล เมื่อพบว่ามีความเสี่ยง หรือพบว่ามีการดำเนินงานที่ไม่สอดคล้องกับข้อกำหนดของกฎหมาย โดยทบทวนตามวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้ เปิดเผย ลบหรือทำลายข้อมูล





Thailand Data Protection Guidelines 3.0

แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

จัดทำโดย ศูนย์วิจัยกฎหมายและการพัฒนา

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

<https://www.law.chula.ac.th/wp-content/uploads/2020/12/TDPG3.0-C5-20201208.pdf>

ใครเป็นใครใน PDPA

1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ประชาชนทุกคน

หากเป็นหน่วยงานทั่วไปก็หมายถึง ลูกค้า พนักงาน รวมถึง Outsource ด้วย
กล่าวอีกนัยหนึ่งคือเป็นบุคคลที่ข้อมูลชี้ไปถึง แต่ไม่รวมถึงคนตายและนิติบุคคล
*ทั้งนี้เจ้าของข้อมูลส่วนบุคคลไม่ใช่เจ้าของกรรมสิทธิ์ในข้อมูลนั้น



2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

หน่วยงาน / องค์กร / สถาบัน ที่กำหนดวัตถุประสงค์
วิธีการประมวลผล และใช้ประโยชน์จากข้อมูลส่วนบุคคล
บุคคลธรรมดาที่อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน



3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
โดยหลักคือ Outsource ที่รับจ้าง

*ไม่ใช่พนักงานหรือส่วนหนึ่งของหน่วยงาน / องค์กร / สถาบัน



4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ
หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ
หน่วยงาน / องค์กร / สถาบัน ให้เป็นไปตามกฎหมาย



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

หลักการเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA (Lawful Basis for Processing)



1

ความยินยอม Consent

2

ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย
หรือสุขภาพ Vital Interest

3

ปฏิบัติตามสัญญา Contract

4

ประโยชน์สาธารณะ Public Task

5

จำเป็น/ชอบด้วยกฎหมาย
Legitimate Interest

6

ปฏิบัติตามกฎหมาย Legal Obligations

7

เอกสารประวัติศาสตร์/วิจัย/สถิติ Research

*เป็นกรณีเฉพาะ รอคณะกรรมการประกาศกำหนด



ที่มา: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

พนักงาน ไม่ใช่ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ตามนิยามใน กม.
แต่ พนักงาน ต้องปฏิบัติตามข้อกำหนดและหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามที่องค์กรกำหนด



การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

กรณีป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ



Vital Interest



เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูล
หรือเพื่อประโยชน์สาธารณะ เช่น ป้องกันโรคระบาด
ผู้ควบคุมสามารถประมวลผลข้อมูลส่วนบุคคลได้โดยไม่ต้องได้รับความยินยอม

ข้อมูลส่วนบุคคลนั้นรวมถึงข้อมูลเกี่ยวกับชีวิต ร่างกาย หรือสุขภาพทุกประเภท



อุบัติเหตุ



การบริการทางการแพทย์



การป้องกันโรคระบาด

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(2) และ 26(1)

*การประมวลผล ได้แก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติตามสัญญา ไม่ต้องขอความยินยอม
Contract



จำกัดเฉพาะข้อมูลของเจ้าของข้อมูล
ผู้เป็นคู่สัญญาเท่านั้น

เฉพาะข้อมูลส่วนบุคคลทั่วไปเท่านั้น
ข้อมูลอ่อนไหวไม่สามารถใช้
ฐานสัญญาได้*

เมื่อไม่ใช่เรื่องความยินยอม
จึงไม่อาจถอนความยินยอมได้
เป็นเรื่องของนิติสัมพันธ์ตามสัญญา



ภายใต้ขอบเขตของสัญญา
ตามที่ตกลงกัน

ถ้าผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่จำเป็น
ในการปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลเพื่อเข้าทำสัญญา หรือเพื่อปฏิบัติตามสัญญา
ก็ไม่ต้องขอความยินยอมจากเจ้าของข้อมูลเพิ่มเติมอีก

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(3)

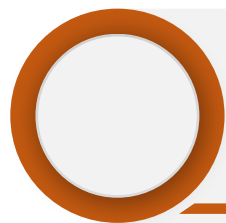
*การปฏิบัติตามสัญญาไม่เพียงพอที่จะนำไปเก็บรวบรวม ใช้ หรือเปิดเผยสำหรับข้อมูลอ่อนไหว
เว้นแต่เป็นกรณีสัญญาให้บริการทางการแพทย์ที่เข้าเงื่อนไขตามกฎหมายตามมาตรา 26(5)(ก)



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล



Thank you

pdpc@mdes.go.th

02 142 1033