

แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล

7 ฐานการประมวลผลข้อมูล ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล



ฐานความ**ยินยอม** (Consent)



ฐานการปฏิบัติตาม**สัญญา** (Contract)



ฐานการปฏิบัติ**หน้าที่ตามกฎหมาย**ของผู้ควบคุมข้อมูลส่วนบุคคล
(Legal Obligation)



ฐานการ**ป้องกันหรือระงับอันตราย**ต่อชีวิต ร่างกาย หรือสุขภาพของ
บุคคล (Vital Interest)



ฐานการปฏิบัติหน้าที่เพื่อ**ประโยชน์สาธารณะ** (Public Interest)



ฐาน**ประโยชน์อันชอบด้วยกฎหมาย**ของผู้ควบคุมข้อมูลส่วนบุคคล
(Legitimate Interest)



ฐาน**จัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ** หรือเพื่อประโยชน์
สาธารณะ หรือการศึกษาวิจัยหรือสถิติ (Historical & Statistic Research)



หมายเหตุ

1. ในการประมวลผลแต่ละครั้ง ผู้ควบคุมข้อมูลจะต้องระบุฐานในการประมวลผล
2. และต้องมีการแจ้งฐานในการประมวลผลกับเจ้าของข้อมูล
3. มีการดำเนินการกับข้อมูลนั้น ๆ ด้วยข้อจำกัดที่แตกต่างกัน
4. มีการเก็บบันทึกการประมวลผลด้วย ว่าใช้ฐานใดในการประมวลผล
5. ข้อมูลชุดเดียวกัน อาจมีฐานในการประมวลผลข้อมูลไม่เหมือนกัน
6. การขอความยินยอม อาจไม่ใช่ฐานในการประมวลผลที่ดีที่สุด
7. การเปลี่ยนฐานการประมวลผล ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ
8. ผู้ควบคุมข้อมูลสามารถแจ้งฐานในการประมวลผลมากกว่า 1 ได้ (ต้องชัดเจน ไม่ระบุคลุมเครือ) ซึ่งจะช่วยลดขั้นตอนการติดต่อเจ้าของข้อมูลส่วนบุคคล หลังการขอความยินยอมหรือหลังสัญญาสิ้นสุดบังคับใช้

ฐานความยินยอม (Consent)

1. ความยินยอมสามารถใช้เป็นฐานการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลได้สมัครใจ ให้ผู้ควบคุมข้อมูลประมวลผลข้อมูลได้ โดยผู้ควบคุมข้อมูลจะต้องดำเนินการขอความยินยอมจากเจ้าของข้อมูล ด้วยการจัดทำแบบฟอร์มขอความยินยอมเป็นหนังสือ หรือทำผ่านระบบอิเล็กทรอนิกส์ในลักษณะที่ชัดเจน แยกส่วนจากข้อความอื่น รูปแบบเข้าถึงและเข้าใจได้ง่าย และเป็นภาษาที่อ่านง่ายไม่หลอกลวง และเจ้าของข้อมูล สามารถเลือกปฏิเสธได้กรณีนี้ผู้ควบคุมข้อมูลจะไม่สามารถประมวลผลได้
2. ความยินยอมจะต้องไม่เป็นเงื่อนไขของการรับบริการ การใช้ความยินยอมเป็นฐานในการประมวลผล มักใช้กับบริการเสริมจากบริการหลักที่ไม่ครอบคลุมตามสัญญา การประมวลผลข้อมูลบนฐานความยินยอมต้องยึดหลักตามความจำเป็น ต้องทำให้ข้อมูลมีความถูกต้อง
3. เมื่อเจ้าของข้อมูลขออนุญาตความยินยอม ผู้ควบคุมข้อมูลต้องหยุดการประมวลผลข้อมูล ตามที่พรบ.คุ้มครองข้อมูลส่วนบุคคล กำหนดในมาตรา 19 และหากเป็นการประมวลผลในฐานสัญญา ไม่ความจำเป็นต้องขอความยินยอม

ตัวอย่าง การประมวลผลข้อมูลเพื่อซื้อขายสินค้า สามารถทำได้ตามฐานสัญญาโดยไม่ต้องขอความยินยอม แต่หากเสนอบริการเสริมเพิ่มเติม ที่ไม่เกี่ยวข้องกับสัญญาซื้อขายนั้น ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

ฐานความยินยอม (Consent)

4. เงื่อนไขของความยินยอม

- ความยินยอมจะต้องขอก่อนการประมวลผลข้อมูลเกิดขึ้น
- ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการหลัก ผู้ควบคุมข้อมูลต้องไม่นำฐานความยินยอม (consent) และฐานสัญญา (contract) มาปะปนกัน และต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นต่อการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น
- ผู้ควบคุมข้อมูลจะต้องระบุประโยชน์ที่จะเกิดขึ้นแก่ตนและเจ้าของข้อมูล หากได้รับความยินยอม เช่น จะทำให้การใช้บริการ สะดวกรวดเร็วมากขึ้น ลดขั้นตอนและระยะเวลาการตรวจสอบตัวตน

ตัวอย่าง

- ❖ กรณีที่แอปพลิเคชันแต่งรูปขอประมวลผลข้อมูลตำแหน่งที่อยู่ของผู้ใช้บริการเพื่อนำไปประมวลผลสำหรับการโฆษณาตามลักษณะพฤติกรรม ทั้งที่ข้อมูลตำแหน่งที่อยู่และการโฆษณาตามพฤติกรรมต่างไม่มีความจำเป็นต่อการให้บริการแต่งรูปและไม่เกี่ยวข้องกับการให้บริการหลัก แต่ผู้ให้บริการไม่สามารถใช้แอปพลิเคชันได้โดยไม่ยินยอมกับการประมวลผลเช่นนี้ กรณีเช่นนี้ ความยินยอมกลายเป็นเงื่อนไขของการให้บริการ จึงไม่ถือเป็นความยินยอมที่ให้ตามความสมัครใจโดยอิสระ

ฐานความยินยอม (Consent)

เงื่อนไขของความยินยอม

- ความยินยอมต้องแยกส่วนกับเงื่อนไขในการให้บริการ
- วัตถุประสงค์ของการประมวลผลต้องเฉพาะเจาะจง
 - การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในขอความยินยอมครั้งเดียวได้
 - หากใช้ชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกว่าจะยินยอมสำหรับวัตถุประสงค์ใดบ้าง
- ความยินยอมต้องชัดเจนไม่คลุมเครือ การให้ความยินยอมต้องเกิดจากความสมัครใจจากเจ้าของข้อมูล
- การขอความยินยอมผ่านการเคลื่อนไหวทางกายภาพ เช่น การเลื่อนตำแหน่งที่กำหนดบนหน้าจออุปกรณ์ อาจถือเป็นการกระทำที่ให้ความยินยอมอย่างชัดเจนได้ แต่ต้องออกแบบลำดับขั้นตอนการขอความยินยอมให้ชัดเจนว่า พฤติกรรมแต่ละอย่างหมายถึงอะไร การขอความยินยอมมีวัตถุประสงค์ใด ผู้ควบคุมข้อมูลจะต้องเก็บข้อมูลได้ด้วยว่าใช้วิธีใดในการขอความยินยอม
- ออกแบบทางเลือกให้สามารถปฏิเสธความยินยอมได้ หรือถอนความยินยอมได้ ผู้ควบคุมข้อมูลต้องประเมินและแยกแยะให้ชัดเจนว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาให้บริการ และข้อมูลใดจำเป็นต้องขอความยินยอมเพื่อให้บริการเสริม ดังนั้นเมื่อเจ้าของข้อมูลปฏิเสธการให้ความยินยอม หรือถอนความยินยอมจะต้องไม่กระทบการให้บริการหลักแม้จะมีประสิทธิภาพการให้บริการอาจน้อยลง

ฐานความยินยอม (Consent)

เงื่อนไขของความยินยอม

- เนื้อหาความยินยอมเข้าใจง่ายและเข้าถึงง่าย
- การขอความยินยอมจะต้องมีรายละเอียดข้อมูลต่าง ๆ อย่างครบถ้วน
 - เนื้อหาจะต้องไม่ยาวจนเกินไป โดยอาจใช้เทคนิคเสริม เช่น FAQs, pop-up screen, chatbot ทำให้การให้ขอมูลนั้นชัดเจนมากขึ้น
 - การให้ขอมูลอาจกระทำได้หลายรูปแบบ ทั้งขอเขียน ปากเปล่า วิดีโอ ขอความเสียง หรือขอความอิเล็กทรอนิกส์ก็ได้ ตราบใดที่ขอมูลเหล่านั้นสามารถเข้าถึงได้ง่ายและมีความชัดเจนแยกออกจากเนื้อหาเรื่องอื่น ๆ
 - ใช้ภาษาให้เหมาะสมกับระดับความสามารถในการเข้าใจในบริบทของผู้ใช้บริการ

[เนื้อหาหลักของเว็บไซต์]

[เนื้อหาการขอความยินยอม]

เราต้องการเปิดเผยข้อมูลเกี่ยวกับการท่องเที่ยวของเรากับ **เบรนดและพาร์ทเนอร์ผู้ช่วยวิเคราะห์** (คลิกเพื่อดูรายละเอียดเพิ่มเติม) เพื่อจะเสนอสินค้าและประสบการณ์ที่ดีให้กับคุณได้ และช่วยให้เราปรับปรุงเว็บไซต์ให้ดีขึ้นได้ด้วย

ข้อมูลนี้จะถูกลบหลังจาก 6 เดือนผ่านไป คุณสามารถถอนการอนุญาตให้เก็บข้อมูลนี้ได้ทุกเมื่อโดยเข้าไปที่ **ข้อมูลของฉัน**

คุณสามารถเข้าถึงรายละเอียดอื่นๆ เกี่ยวกับสิทธิของคุณในการจัดการข้อมูลส่วนบุคคลได้ที่ **ที่นี่**

คุณรับทราบและยินยอมให้เราเก็บรวบรวมข้อมูลการท่องเที่ยวของเราหรือไม่

NO OK

ฐานความยินยอม (Consent)

เงื่อนไขของความยินยอม

- การขอความยินยอมแบบชัดเจน (Explicit Consent) สำหรับข้อมูลที่อ่อนไหว **การประมวลผลข้อมูลที่อ่อนไหวใช้การทำตามสัญญาเป็นฐานไม่ได้ จึงต้องใช้ฐานความยินยอม** หรือฐานภารกิจของหน่วยงานรัฐ หรือฐานประโยชน์อันชอบธรรมเป็นหลัก ผู้ควบคุมข้อมูลควรขอความยินยอมเป็นขอเขียน และอาจให้ลงลายมือชื่อกำกับไว้ด้วยเพื่อลดความเสี่ยง หากเป็นการขอความยินยอมด้วยช่องทางอิเล็กทรอนิกส์ อาจใช้วิธีอื่นๆ เช่น ส่งอีเมล อัปโหลดเอกสารสแกนที่มีลายมือชื่อ หรือใช้ลายมือชื่ออิเล็กทรอนิกส์
- การให้ความยินยอมปากเปล่าก็เป็นความยินยอมแบบชัดเจนได้ แต่อาจยากต่อการพิสูจน์ ในกรณีของโทรศัพท์อาจทำได้หากให้ข้อมูลเพียงพอ มีทางเลือก และเนื้อหาชัดเจน โดยขอให้ผู้ให้บริการกดปุ่มยืนยันหรือให้ความยินยอมปากเปล่าอย่างชัดเจน และมีการอัดเสียงบันทึกไว้
- เนื้อหาของการขอความยินยอม ควรต้องประกอบด้วย
เนื้อหาดังต่อไปนี้

ใคร?	☐ ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูล (ชื่อ ที่อยู่ DPO ฯลฯ)
อะไร?	☐ วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจง ☐ ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้
อย่างไร?	☐ วิธีการประมวลผลข้อมูล ☐ การใช้ระบบตัดสินใจอัตโนมัติ หรือ โปรไฟล์ (profiling) (หากมี) ☐ การโอนข้อมูลไปต่างประเทศ ☐ การเปิดเผยข้อมูลต่อบุคคลอื่น
เมื่อไร?	☐ ระยะเวลาในการจัดเก็บข้อมูล
หากมีปัญหา?	☐ วิธีการถอนความยินยอม ☐ สิทธิต่างๆ ของเจ้าของข้อมูล โดยเฉพาะสิทธิในการถอนความยินยอม

ฐานความยินยอม (Consent)

5. ข้อควรระวังในการจัดการความยินยอม

- (1) ขอความยินยอมเมื่อจำเป็นต่อประมวลผลขอมูลนั้นเท่านั้น
- (2) บันทึกเนื้อหาขอมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม
- (3) แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้
- (4) กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง
- (5) กระบวนการก่อนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม
- (6) เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเจ้าของขอมูล โดยเฉพาะการถอนความยินยอมได้อย่างรวดเร็ว
- (7) ต้องไม่หลงใหลหรือทำให้เจ้าของขอมูลเสียประโยชน์เมื่อก่อนความยินยอม



ฐานความยินยอม (Consent)

6. ความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้ (ก่อนมีกฎหมาย พ.ศ. 2563)

- มาตรา 95 ของพรบคุ้มครองข้อมูลส่วนบุคคลฯ อนุญาตให้ประมวลผลข้อมูลบนฐานของความยินยอมที่เกิดขึ้นก่อนพระราชบัญญัติจะมีผลบังคับใช้ได้ตามขอบเขตวัตถุประสงค์เดิม แต่ผู้ควบคุมข้อมูลจะต้องประชาสัมพันธ์ให้สามารถถอนความยินยอมได้โดยง่าย
- "การกำหนดวิธีการยกเลิกความยินยอม"นั้นอาจทำได้โดยเผยแพร่ช่องทางการยกเลิกความยินยอม เช่น ทางเว็บไซต์ของผู้ควบคุมข้อมูล และควรแจ้งแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลหรือนโยบายความเป็นส่วนตัว (privacy policy) ด้วย
- ในกรณีที่ความยินยอมที่เก็บไว้ก่อนพ.ร.บ. มีขอบเขตวัตถุประสงค์ที่กว้างขวางคลุมเครือจนขัดแย้งกับมาตรา 19 โดยชัดเจน เช่น เป็นการขอความยินยอมแบบเหมารวมทุกกรณี หรือเป็นการขอความยินยอมแบบไม่แยกระหว่างฐานความยินยอมกับฐานสัญญา ต้องถือว่าความยินยอมนั้นมีผลเฉพาะส่วนที่ขอบเขตวัตถุประสงค์ชัดเจนเท่านั้น
- การอ้างอิงความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้นั้นมีความเสี่ยงค่อนข้างมาก โดยเฉพาะหากความยินยอมนั้นมีขอบเขตวัตถุประสงค์ที่กว้างขวางคลุมเครือ จนมีลักษณะขัดแย้งกับมาตรา 19 โดยอย่างเห็นได้ชัด จึงควรปรับปรุงโดยขอความยินยอมใหม่จากเจ้าของข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติให้ไ้มากที่สุด

ฐานความยินยอม (Consent)

ความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะมีผลบังคับใช้ (ก่อนมีกฎหมาย พ.ศ. 2563)

- การขอความยินยอมใหม่นั้น ยอมทำได้ไม่ว่าสำหรับลูกค้าหรือผู้ใช้บริการที่มีการติดต่อสื่อสารกันเป็นประจำอยู่แล้ว เช่น กรณีที่เมื่อลูกค้าอื่นเข้ามาใช้บริการ ก่อนจะไปถึงหน้าที่เป็นการให้บริการ ก็แจ้งให้รับทราบเงื่อนไขความยินยอมก่อน เป็นต้น
- การอ้างความยินยอมเก่าก่อนพระราชบัญญัติจะมีผลบังคับใช้นั้น ควรทำเฉพาะในกรณีของลูกค้าเก่า ที่ติดต่อเพื่อขอความยินยอมใหม่โดยยากและจำเป็นต้องประมวลผลข้อมูลของลูกค้ารายนั้นจริงๆ เท่านั้น
- กฎหมาย GDPR กำหนดไว้ว่าไม่สามารถอ้างถึงการขอความยินยอมที่เก็บรวบรวมไว้ก่อน พรบ.มีผลบังคับใช้ ทำให้ผู้ควบคุมข้อมูล ที่ประมวลผลข้อมูลส่วนบุคคลของคนสหภาพยุโรป หรือมีการดำเนินธุรกรรมกับสหภาพยุโรป จะต้องขอความยินยอมใหม่

ฐานความยินยอม (Consent)

7. ขอบควรระวังเกี่ยวกับความยินยอมระหว่างบุคคลที่มีอำนาจต่อรองไม่เท่ากัน

- เนื่องจากความยินยอมจะต้องเกิดขึ้นโดยสมัครใจอย่างแท้จริง ในกรณีที่อำนาจต่อรองของผู้ควบคุมข้อมูลและเจ้าของข้อมูลแตกต่างกันมากๆ จึงมักใช้ความยินยอมเป็นฐานไม่ได้ เช่น ในกรณีของการดำเนินการกิจหน่วยงานของรัฐ และความสัมพันธ์ระหว่างนายจ้างกับลูกจ้าง

ตัวอย่าง : กรณีหน่วยงานของรัฐสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

- ❖ หน่วยงานของรัฐแจ้งข่าวสารทางเว็บไซต์ทางการและช่องทางอื่นๆ อยู่แล้ว แต่ขออีเมลของผู้เกี่ยวข้องเพื่อแจ้งข่าวสารเพิ่มเติมโดยตรง โดยบอกชัดเจนว่าไม่ใช่หน้าที่ของเจ้าของข้อมูลที่จะต้องให้อีเมล และจะใช้อีเมลเพื่อวัตถุประสงค์นี้เท่านั้น (และแม้ไม่ให้อีเมลเพื่อรับข่าวสาร ก็ยังสามารถรับข่าวสารจากช่องทางอื่นได้)
- ❖ หน่วยงานของรัฐสองแห่งขอรวม (merge) ไฟล์ข้อมูลส่วนบุคคลเพื่อความสะดวกในการบริหารจัดการ ถ้าหากเจ้าของข้อมูลปฏิเสธก็ยังดำเนินงานบนไฟล์แยกได้อยู่
- ❖ โรงเรียนรัฐขอรูปถ่ายนักเรียนไปใช้ในวารสารประชาสัมพันธ์ โดยที่นักเรียนสามารถปฏิเสธที่จะไม่ให้รูปได้

ตัวอย่าง : กรณีนายจ้างสามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลส่วนบุคคล

- ❖ นายจ้างขอให้ลูกจ้างปรากฏตัวบนหนังสือพิมพ์ที่มารถถ่ายที่บริษัท โดยลูกจ้างสามารถปฏิเสธได้โดยง่าย และจัดให้สามารถไปนั่งในบริเวณอื่นที่ไม่ถูกถ่ายได้

ฐานความยินยอม (Consent)

8. การทำการตลาดแบบตรง (Direct Marketing)

- การประมวลผลข้อมูลเพื่อการทำการตลาดแบบตรงต้องใช้ฐานความยินยอมเป็นหลัก ไม่สามารถใช้ฐานอื่นได้ เนื่องจากเป็นการติดต่ออย่างเฉพาะเจาะจง จึงรุกร้าความเป็นส่วนตัว ดังนั้นการบริหารจัดการข้อมูลภายในองค์กรก็ต้องแยกแยะออกจากข้อมูลที่ใช้ในการทำโฆษณาแบบไม่เฉพาะเจาะจงด้วย
- ความยินยอมเพื่อการทำการตลาดแบบตรงนั้น ต้องเป็นไปอย่างเฉพาะเจาะจง ไม่แอบแฝงในรูปของวัตถุประสงค์อื่น เช่น การทำวิจัยตลาดที่ต้องการทราบภาพรวมของตลาดเพื่อนำไปวิเคราะห์นโยบาย โดยไม่ได้นำไปใช้เพื่อเสนอขายสินค้า
- ต้องเปิดโอกาสให้เจ้าของข้อมูลสามารถถอนความยินยอม ออกได้โดยง่ายด้วย
- หากมีความจำเป็นต้องส่งต่อข้อมูลไปยังบุคคลที่สาม ต้องตรวจสอบว่าเป็นบุคคลที่สามารถไว้วางใจได้และจะปฏิบัติกับข้อมูลส่วนบุคคลด้วยมาตรฐานการคุ้มครองข้อมูลที่เหมาะสม ต้องแจ้งการเปิดเผยข้อมูลต่อบุคคลเหล่านั้นด้วย และต้องบันทึกรายละเอียดของความยินยอมไว้อย่างชัดเจน
- การทำการตลาดแบบตรงที่ไม่ได้มีลักษณะรุกร้าความเป็นส่วนตัวมาก อาจใช้ฐานผลประโยชน์อันชอบธรรมได้ เช่น การส่งข้อมูลเกี่ยวกับผลิตภัณฑ์ให้กับลูกค้าที่ลงทะเบียนเป็นสมาชิกของซูเปอร์มาร์เก็ต

ฐานความยินยอม (Consent)

9. ระบบสมาชิกสะสมแต้ม (Loyalty Program)

- การประมวลผลข้อมูลเพื่อดำเนินการระบบสมาชิกสะสมแต้มใช้ฐานความยินยอมเป็นหลัก เนื่องจากเป็นบริการเสริมที่เป็นตัวเลือกเพิ่มเติมจากบริการหลัก
- หากการประมวลผลมีวัตถุประสงค์อื่น นอกเหนือการสะสมแต้มเพื่อรับสิทธิประโยชน์ต่าง ๆ จะต้องขอความยินยอมแยกส่วนออกมาจากระบบสมาชิกสะสมแต้ม
- ไม่ควรขอข้อมูลมากเกินไปในการสมัครระบบสมาชิกสะสมแต้ม ผู้ควบคุมข้อมูลควรพิจารณาขอเฉพาะข้อมูลที่จำเป็น
- หากมีความจำเป็นต้องส่งต่อข้อมูลไปยังบุคคลที่สาม ต้องตรวจสอบว่าเป็นบุคคลที่สามารถไว้วางใจได้และจะปฏิบัติกับข้อมูลส่วนบุคคลด้วยมาตรฐานการคุ้มครองข้อมูลที่เหมาะสม ต้องแจ้งการเปิดเผยข้อมูลต่อบุคคลเหล่านั้นด้วย และต้องบันทึกรายละเอียดของความยินยอมไว้อย่างชัดเจน
- การบันทึกข้อมูลส่วนบุคคลไม่ควรเกินไปกว่าระยะเวลาอายุการเป็นสมาชิก เว้นแต่มีข้อยกเว้นให้ต้องเก็บบันทึกข้อมูลไว้ เช่น ตามหน้าที่ในกฎหมายอื่น
- ะมัดระวังการแสดงผลสมาชิก หรือแสดงผลหน้าจอเพื่อยืนยันตัวตนสมาชิกเพื่อใช้แต้มสะสม มิให้เกิดการเปิดเผยข้อมูลต่อบุคคลอื่น ๆ ที่ไม่เกี่ยวข้อง (ที่บังเอิญอยู่บริเวณนั้น) เช่น การแสดงผลหน้าจอที่จุดให้บริการให้ปรากฏเฉพาะข้อมูลที่จำเป็น เช่น ชื่อ-นามสกุล รหัสสมาชิกเท่านั้น ตัวอย่างที่ไม่ดีคือ การแสดงเบอร์โทรศัพท์ หรือ ภาพถ่ายหรือชื่อบัญชีผู้ใช้ social media ที่เชื่อมต่อกับระบบสมาชิกสะสมแตมนั้นๆ บนหน้าจอ

ฐานความยินยอม (Consent)

10. การใช้ข้อมูลเครือข่ายสังคมเพื่อกระตุนยอดขาย(Social Network)

- การใช้ข้อมูลเครือข่ายสังคม (social network) เพื่อกระตุนยอดขายจำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล การขอความยินยอมต้องทำโดยแจ้งวัตถุประสงค์ชัดเจน การนำข้อมูลไปใช้ประโยชน์ต้องเป็นไปตามที่แจ้งเท่านั้น และควรแจ้งให้ชัดเจนว่าขอข้อมูลใดบ้าง นำข้อมูลนั้นไปใช้งานอะไร มีผลลัพธ์ที่เป็นประโยชน์กับตัวผู้ใช้บริการอย่างไร
- เนื่องจากข้อมูลเครือข่ายสังคม (เช่น รายชื่อเพื่อน รายชื่อในสมุดโทรศัพท์) ควรต้องระมัดระวังในการไม่เปิดเผยข้อมูลต่อบุคคลที่สามโดยไม่จำเป็น ควรออกแบบค่าพื้นฐาน (default) เป็นการไม่เปิดเผยไว้ก่อน แล้วค่อยให้ผู้ใช้เลือกที่จะเปิดเผยเอง

ฐานความยินยอม (Consent)

11. การโฆษณาตามพฤติกรรมออนไลน์ (Online Behavioural Advertisement)

- การโฆษณาตามพฤติกรรมออนไลน์ (Online Behavioural Advertisement) หรือ targeted advertisement เป็นการโฆษณาแบบเจาะจงที่ต้องอาศัยข้อมูลที่เฉพาะเจาะจงรายบุคคล ต้องใช้ฐานความยินยอม
- การสร้างข้อมูลโปรไฟล์ (profiling) ของเป้าหมายที่ต้องการทำการโฆษณาจากข้อมูลการใช้บริการออนไลน์ เช่น การเก็บข้อมูล cookies หรือ IP Address หรือ Location นั้นมีลักษณะที่รุกล้ำความเป็นส่วนตัว เช่น การทำ profile พฤติกรรมการท่องเว็บ การเสนอสินค้า บริการจากพฤติกรรมต่าง ๆ นั้น การขอความยินยอมจึงต้องยิ่งกระทำอย่างรัดกุม อีกทั้งเจ้าของข้อมูลส่วนบุคคลยังมีสิทธิที่จะคัดค้านการประมวลผลเพื่อทำโปรไฟล์สิ่งใดอีกด้วย
- การทำโปรไฟล์ลง เป็นตัวอย่างของการตัดสินใจอัตโนมัติ (automatic decision) ซึ่งจะขัดต่อ GDPR หากการกระทำนั้นส่งผลกระทบสำคัญในทางกฎหมายต่อตัวเจ้าของข้อมูล แต่มีข้อยกเว้น เช่น ทำโปรไฟล์นั้นเป็นไปเพื่อปฏิบัติตามหน้าที่ตามสัญญาหรือเขาสุการทำสัญญา หรือได้รับความยินยอมอย่างชัดเจนแล้ว

ฐานความยินยอม (Consent)

12. การขอความยินยอมจากผู้เยาว์

- ผู้เยาว์ ที่ยังไม่บรรลุนิติภาวะสามารถให้ความยินยอมโดยลำพังได้ หากเข้าข่ายตามมาตราที่ 22, 23 และ 24 ของประมวลกฎหมายแพ่งและพาณิชย์ (อันว่าด้วยเรื่องการใด ๆ ที่ผู้เยาว์สามารถกระทำเองโดยลำพัง)
- นอกเหนือจากนั้น ให้ขอความยินยอมจากผู้ปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ประกอบด้วย
- คนไร้ความสามารถ ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ
- คนเสมือนไร้ความสามารถ ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ
- ควรใช้ภาษาที่ผู้เยาว์สามารถเข้าใจได้ง่าย
- พิจารณาใช้เครื่องมือในการป้องกันไม่ให้เกิดการเก็บข้อมูลส่วนบุคคลของผู้เยาว์โดยไม่สมควร เช่น
 - สอบถามว่าผู้ใช้บริการอายุเกินเกณฑ์แล้วหรือไม่
 - การแจ้งเตือนให้มีผู้ปกครองให้ความยินยอม
 - กำหนดให้มีการตั้งค่าโดยผู้ปกครอง (parental setting หรือ parental mode) ในการใช้บริการเพื่อป้องกันมิให้ผู้เยาว์ให้ข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์

ฐานความยินยอม (Consent)

การขอความยินยอมจากผู้เยาว์

- บริการออนไลน์ประเภท Information Society Services เช่น บริการเกมออนไลน์ การขายสินค้าออนไลน์ ที่มุ่งให้บริการแก่ผู้เยาว์โดยตรง โดยให้ผู้ควบคุมข้อมูล ต้องได้รับความยินยอมจากผู้ปกครองจากผู้เยาว์ที่อายุต่ำกว่า 16 ปี หรือต่ำกว่า 13 ปี หากมีกฎหมายภายในของประเทศนั้น ๆ กำหนดไว้ (แต่หากเป็นการประมวลผลบนฐานอื่น ๆ เช่น ฐานสัญญานั้นก็สามารถทำได้ โดยต้องคำนึงถึงข้อจำกัดเกี่ยวกับความสามารถของผู้เยาว์ตามกฎหมายแพ่ง)
- บริการออนไลน์หลายประเภทที่ดำเนินการประมวลผลบนฐานความยินยอม เช่น โซเชียลมีเดียที่ต้องประมวลผลข้อมูลส่วนบุคคลในปริมาณมาก และมีการทำการตลาดโดยอาศัยข้อมูลเหล่านั้น จึงมักไม่อนุญาตให้ผู้ที่อายุต่ำกว่า 13 ปีเปิดเผยข้อมูลเพื่อลดความเสี่ยง ซึ่งหากมีความจำเป็นต้องขอความยินยอมจากผู้เยาว์จริงๆ ควรจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

ฐานปฏิบัติตามสัญญา (Contract)

1. สัญญา คือ การตกลงแลกเปลี่ยนกันทั้งสองฝ่าย ซึ่งเราสามารถประมวลผลข้อมูลได้ในกรณีที่มีความจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลและเจ้าของข้อมูลส่วนบุคคล เช่น

- การประมวลผลข้อมูลธุรกรรมของบุคคลเพื่อคำนวณดอกเบี้ยของธนาคาร
- การตรวจสอบข้อมูลส่วนบุคคลก่อนการเปิดบัญชี หรือยื่นกู้
- การประมวลผลชื่อและที่อยู่ของบุคคลเพื่อดำเนินการจัดส่งสินค้าของบริษัทขนส่ง

หากมีการใช้สัญญาแล้ว ไม่ต้องขอความยินยอมเพิ่มเติม โดยฐานนี้จะสามารถใช้ได้กับการประมวลผลข้อมูลส่วนบุคคลทั่วไปเท่านั้น (ไม่สามารถใช้กับการประมวลผล Sensitive Data ได้)

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

ฐานปฏิบัติตามสัญญา (Contract)

2. การประมวลผลข้อมูลบนฐานสัญญา จะจำกัดการประมวลผลเฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญาเท่านั้น การประมวลผลบุคคลที่สาม จะต้องใช้ฐานอื่น ๆ เช่น การประมวลผลข้อมูลของกลุ่มสมรส เพื่อเอาประกัน -> ใช้ฐานความยินยอม หรือฐานผลประโยชน์อันชอบธรรม
3. กรณีที่ผู้ประมวลผลข้อมูลทำงานให้กับผู้ควบคุมข้อมูล ถือเป็นการประมวลผลตามฐานสัญญา ผู้ประมวลผลไม่ต้องขอความยินยอมเพิ่ม
4. ผู้ควบคุมข้อมูลไม่ควรขอความยินยอมพร่ำเพรื่อ เพราะจะทำให้ผู้ใช้บริการเกิดความเข้าใจผิดว่าสามารถขอถอนความยินยอมได้ ทั้งที่นิติสัมพันธ์ทางสัญญากันอยู่
5. การประมวลผลข้อมูลอาจใช้ฐานสัญญามากกว่า 1 ฉบับ เช่น ผู้ป่วย (เจ้าของข้อมูลส่วนบุคคล) เข้ารับบริการกับทางโรงพยาบาล และโรงพยาบาลส่งข้อมูลค่าใช้จ่ายให้บริษัทประกัน เพื่อเบิกค่ารักษา ทำให้มีสัญญา 2 ฉบับ คือสัญญาการรับบริการระหว่างผู้ป่วยกับโรงพยาบาล และสัญญาประกันสุขภาพระหว่างผู้ป่วยกับบริษัทประกัน
6. ข้อควรระวัง **"ความจำเป็นในการปฏิบัติตามสัญญา"** ผู้ควบคุมข้อมูลต้องพิจารณาขอบเขตสัญญา เพื่อทราบขอบเขตข้อมูลในการปฏิบัติตามสัญญา ซึ่งจะเป็นไปอย่างเฉพาะเจาะจงตามที่ระบุในสัญญา เช่น ไม่สามารถนำข้อมูลส่วนบุคคลที่ระบุในสัญญา มาประมวลผลอื่นใดเพื่อประโยชน์ทางธุรกิจ
7. **"ความจำเป็นในการปฏิบัติตามสัญญา"** ไม่รวมถึงกรณีที่เกิดปัญหาหรือข้อพิพาทที่เกี่ยวข้องกับสัญญา เช่น การใช้หน่วยงานภายนอกติดตามทวงหนี้ การรวบรวมข้อมูลเพื่อฟ้องร้องต่อการไม่ปฏิบัติตามสัญญา , การเปิดประมูลสินทรัพย์เพื่อชดใช้หนี้ ซึ่งผู้ควบคุมข้อมูลต้องอ้างฐานอื่นๆ เช่น ฐานความยินยอม หรือฐานผลประโยชน์อันชอบด้วยกฎหมาย

ฐานสัญญา (Contract)

หรือ ฐานความยินยอม (Consent)

จำเป็น สำหรับสัญญา	ทางเลือก ของเจ้าของข้อมูล
ที่อยู่สำหรับจัดส่งสินค้า อีเมลสำหรับส่งใบเสร็จ	อีเมลสำหรับการส่งจดหมายข่าว
ข้อมูลบัตรเครดิตสำหรับจองโรงแรม	ข้อมูลบัตรเครดิตที่เลือกให้เว็บไซต์จำไว้เพื่อความสะดวกในการจ่ายเงินครั้งต่อไป

ฐานปฏิบัติตามกฎหมาย (Legal Obligation)

ผู้ควบคุมข้อมูลสามารถประมวลผลข้อมูลส่วนบุคคลของผู้อื่นได้ หากเป็นการปฏิบัติตามหน้าที่ตามกฎหมาย และต้องสามารถระบุได้ว่ากำลังปฏิบัติหน้าที่ตามกฎหมาย หรือ กระทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจตามกฎหมาย

ในกรณีที่ประมวลผลตามฐานนี้ **ไม่ต้องขอความยินยอม** และ เจ้าของข้อมูลจะไม่มีสิทธิในการขอลบ โอนย้ายข้อมูล หรือคัดค้าน การประมวลผล

ตัวอย่าง

- ❖ นายจ้างเปิดเผยข้อมูลเงินเดือนของลูกจ้างต่อกรมสรรพากรเพื่อแจกแจงรายละเอียดในการคำนวณรายได้ รายจ่ายของกิจการตามมาตรา 65 ประมวลรัษฎากร
- ❖ สถาบันการเงินแจ้งผลการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินให้กับคณะกรรมการป้องกัน และปราบปรามการทุจริตแห่งชาติตามมาตรา 112 ของพระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการป้องกัน และปราบปรามการทุจริต
- ❖ การดำเนินการประมวลผลข้อมูลตามคำสั่งศาล
- ❖ บริษัทผู้ให้บริการบัตรโดยสารสาธารณะขอสำเนาประชาชนเพื่อปฏิบัติตามกฎเกณฑ์เรื่องการป้องกันและ ปราบปรามการฟอกเงิน โดยเก็บไว้เฉพาะข้อมูลที่เกี่ยวข้องเท่านั้น (ตัดข้อมูลที่ไม่เกี่ยวข้อง เช่น กรู๊ปเลือด ศาสนา ออกไป)
- ❖ ผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่เก็บข้อมูลจราจรตามที่กำหนดในพระราชบัญญัติคอมพิวเตอร์

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติตามกฎหมาย ไม่ต้องขอความยินยอม Legal Obligations

จำเป็นสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมตามที่กฎหมายกำหนด

หน้าที่ตามกฎหมายแห่งกฎหมาย



หน้าที่ตามคำสั่งของหน่วยงานรัฐที่มีอำนาจ

เช่น เก็บรวบรวม ใช้ หรือเปิดเผยเงินเดือนของลูกจ้างเพื่อส่งให้สำนักงานประกันสังคม
ร้านค้าที่ให้บริการเชื่อมต่อ WiFi เก็บรวบรวมข้อมูลจราจรตามที่กำหนดในพ.ร.บ.คอมพิวเตอร์

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(6)

ฐานภารกิจของรัฐ (Public Interest)

ผู้ที่สามารถใช้ฐานนี้ในการประมวลผลข้อมูลได้มักเป็นเจ้าหน้าที่หรือองค์กรของรัฐ เช่น สำนักงานสถิติแห่งชาติ สำนักงานศาลยุติธรรม สำนักงานเลขาธิการสภาผู้แทนราษฎรและวุฒิสภา เจ้าหน้าที่ของกระทรวงต่างๆ ที่ปฏิบัติตามภารกิจตามกฎหมาย รวมถึงหน่วยงานเอกชน ที่ปฏิบัติหน้าที่ในการใช้อำนาจที่รัฐได้มอบหมายให้เพื่อผลประโยชน์สาธารณะตามกฎหมาย

- เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ "จำเป็น" ต่อการดำเนินการของรัฐ
- ยังต้องคำนึงถึงหลักความได้สัดส่วนในการใช้ข้อมูล และผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูล
- ผู้ควบคุมข้อมูลยังคงต้องมีหน้าที่รักษาความปลอดภัยของข้อมูล

ตัวอย่าง

- ❖ กรมสรรพากรคิดคำนวณข้อมูลเงินเดือนของลูกจ้างเพื่อตรวจสอบการรายการรายได้รายจ่ายที่กิจการนั้นๆ ยื่น
- ❖ คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติเก็บรวบรวมข้อมูลเกี่ยวกับการตรวจสอบความถูกต้องของรายการทรัพย์สินและหนี้สินจากสถาบันการเงิน

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

ปฏิบัติการของรัฐ ไม่ต้องขอความยินยอม Public Task



หากจำเป็นต่อการดำเนินการของรัฐเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจรัฐ
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจการนั้น
ไม่ต้องขอความยินยอม

แม้ไม่ต้องขอความยินยอม
แต่ผู้ควบคุมยังคงมีหน้าที่ในการ
รักษาความปลอดภัยของข้อมูล



คำนึงถึงหลักความได้สัดส่วน
ความจำเป็นในการใช้ข้อมูล และผลกระทบต่อ
ความเป็นส่วนตัวของเจ้าของข้อมูล



ดังนั้น ผู้ควบคุมข้อมูลจึงเป็นองค์กรของรัฐที่ปฏิบัติตามกฎหมาย
รวมถึงหน่วยงานเอกชนที่ปฏิบัติหน้าที่โดยอาศัยอำนาจที่ได้รับมอบหมายจากรัฐ

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(4)



สำนักงานคณะกรรมการ
คุ้มครองข้อมูลส่วนบุคคล

ฐานปฏิบัติตามกฎหมาย
(Legal Obligation)

หรือ

ฐานภารกิจสาธารณะ ?
(Public Task)

(ผู้ควบคุมข้อมูล) ปฏิบัติตามกฎหมายที่ ต้องทำอยู่แล้ว	(เจ้าหน้าที่) ปฏิบัติหน้าที่เพื่อบรรลุภารกิจ สาธารณะ
บริษัทแจ้งข้อมูลการจ่ายเงินเดือนพนักงานต่อ สรรพากร	สรรพากรประมวลผลข้อมูลเงินเดือน
องค์กรทางการเงินส่งข้อมูลการทำธุรกรรมที่ น่าสงสัยให้หน่วยงานปราบปรามการฟอกเงิน	หน่วยงานปราบปรามการฟอกเงินประมวลผล ข้อมูลธุรกรรมที่น่าสงสัยเพื่อนำไปตรวจสอบต่อ

ฐานการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล (Vital Interest)

- เป็นการเก็บรวบรวม ใช้ เปิดเผย "ข้อมูลส่วนบุคคล (Personal Data)" โดยมีวัตถุประสงค์เพื่อป้องกันหรือระงับอันตรายรักษาชีวิต ร่างกายหรือสุขภาพเจ้าของข้อมูลส่วนบุคคลรวมถึงเพื่อประโยชน์สาธารณะสามารถทำได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (ตาม มาตรา 24(2))
- ผู้ควบคุมข้อมูลสามารถใช้ฐานนี้เพื่อประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับสุขภาพ หรือข้อมูลอ่อนไหวอื่น ๆ ได้ (เฉพาะเมื่อเจ้าของข้อมูลอยู่ในสถานะไม่สามารถให้ความยินยอม)

ตัวอย่าง

- ❖ โรงพยาบาลหนึ่งเปิดเผยประวัติสุขภาพต่ออีกโรงพยาบาลเพื่อช่วยเหลือผู้ป่วยประสบอุบัติเหตุทางรถยนต์ที่ต้องการการรักษาอย่างเร่งด่วนและหมดสติ
- ❖ โรงพยาบาลประมวลผลข้อมูลของพ่อแม่เพื่อป้องกันอันตรายที่อาจเกิดกับชีวิตของลูก
- ❖ หน่วยงานด้านสาธารณสุขประมวลผลข้อมูลเกี่ยวกับการติดเชื้อของประชาชนเพื่อติดตามเฝ้าระวังสถานการณ์โรคระบาด
- ❖ ข้อมูลการเดินทางไปต่างประเทศถือเป็นข้อมูลส่วนบุคคลทั่วไป หากเป็นข้อมูลเกี่ยวกับข้อมูลสุขภาพจะต้องอาศัยฐานของมาตรา 26 ซึ่งกำกับการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหวแทน

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

ฐานประโยชน์อันชอบธรรม(Legitimate Interest)

- เป็นการประมวลผลข้อมูลที่จำเป็น เพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลหรือบุคคลอื่น สำคัญคือ ประโยชน์อันชอบธรรมนั้น 'ต้องไม่เกินไปกว่าความคาดหมายของเจ้าของข้อมูล' เช่น
 - การติดตั้ง CCTV หน้าประตูทางเข้าบริษัท ย่อมคาดหมายได้ว่าเป็นไปเพื่อการรักษาความปลอดภัย ผู้ควบคุมข้อมูลสามารถทำให้เจ้าของข้อมูลมีความคาดหมายที่ถูกต้องเพิ่มเติมได้โดยการแปะป้าย " CCTV กำลังทำงาน "
 - การประมวลผลข้อมูลเพื่อรักษาความปลอดภัยของระบบและเครือข่าย
 - การส่งต่อข้อมูลในเครือข่ายเพื่อการบริหารจัดการและประโยชน์ของพนักงาน เป็นต้น
- ผู้ควบคุมข้อมูลจะต้องใช้ดุลยพินิจ เพื่อชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรม กับสิทธิและประโยชน์เจ้าของข้อมูลส่วนบุคคล ดังนั้น ผู้ควบคุมข้อมูลส่วนบุคคลต้องระบุได้ว่าอะไรคือประโยชน์อันชอบธรรมที่จะได้รับและความจำเป็นในการประมวลผลข้อมูลทั้งยังมีหน้าที่ปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลให้สมดุลกับประโยชน์อันชอบธรรมที่จะได้รับด้วย (มาตรา 24(5))

ตัวอย่าง หากติดตั้ง CCTV ในสถานที่ เช่น ภายในห้องน้ำ นอกจากเกินกว่าที่บุคคลทั่วไปจะคาดหมายได้แล้ว ยังละเมิดความเป็นส่วนตัว และสร้างความเสี่ยงต่อเจ้าของข้อมูลมากเกินไปจนสมควร กรณีนี้ก็จะไม่สามารถอ้างประโยชน์อันชอบธรรมได้

ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

- นอกจากนี้ ในการปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล ผู้ควบคุมข้อมูลควรมีระบบรักษาความปลอดภัยในการใช้ข้อมูลที่เหมาะสม ไม่เปิดเผยให้ผู้อื่นเข้าถึงได้โดยง่าย ก็จะเป็นมาตรการที่ช่วยคุ้มครองเจ้าของข้อมูลได้อีกทางหนึ่ง (Safeguard)

การเก็บรวบรวมข้อมูลส่วนบุคคลตาม PDPA

กรณีจำเป็น/ชอบด้วยกฎหมาย
Legitimate Interest

จำเป็นต่อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น
โดยเจ้าของข้อมูลต้องสามารถคาดการณ์ได้
ผู้ควบคุมจึงต้องใช้ดุลยพินิจชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรมไม่ให้ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล

ไม่มีวิธีอื่นในการบรรลุวัตถุประสงค์

ผลประโยชน์อันชอบธรรมมีความชัดเจน

ประโยชน์อันชอบธรรม

มีมาตรการปกป้องและคุ้มครองข้อมูล

มีความจำเป็นในการประมวลผล

ไม่ส่งผลกระทบในเชิงลบกับเจ้าของข้อมูล

สิทธิ/ประโยชน์ของเจ้าของข้อมูล

ที่มา: พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 24(5)
*การประมวลผล หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

ฐานประโยชน์อันชอบธรรม(Legitimate Interest)

ตัวอย่าง

- ❖ **ยืนยันตัวตนลูกค้า** ธนาคารดำเนินการตามแนวปฏิบัติของตนเพื่อตรวจสอบข้อมูลส่วนบุคคลเพื่อยืนยันตัวตนของลูกค้าที่ต้องการเปิดบัญชีใหม่กับธนาคาร และบันทึกว่าได้ใช้ข้อมูลใดเพื่อยืนยันตัวตน ในกรณีเช่นนี้ผลประโยชน์ของผู้ควบคุมข้อมูลนั้นชอบธรรมและเนื้อหาของข้อมูลที่ประมวลผลก็มีจำนวนน้อยและจำกัด ทั้งยังเป็นมาตรฐานเดียวกันกับธนาคารอื่นๆ และมีได้ทำให้เกิดผลกระทบอย่างไม่ได้สัดส่วนต่อเจ้าของข้อมูล จึงสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้ หรือในกรณีที่หน่วยงานผู้กำกับดูแลออกเป็นกฎให้ต้องยืนยันตัวตนด้วยวิธีเฉพาะ ก็จะสามารถอ้างฐานปฏิบัติตามกฎหมายได้ด้วย
- ❖ **ข้อมูลการทำงานของลูกจ้าง** บริษัทเก็บรวบรวมข้อมูลจำนวนชั่วโมงทำงานของนายที่ปรึกษาเพื่อคิดคำนวณค่าใช้จ่ายและโบนัส ในกรณีนี้บริษัทได้รับผลประโยชน์ในการบริหารจัดการภายใน และนายที่ปรึกษาไม่ได้ถูกละเมิดความเป็นส่วนตัวมากนักจนเกินไป ระบบค่อนข้างมีความโปร่งใสทำให้ตัวลูกจ้างสามารถโต้แย้งได้ด้วย จึงสามารถอ้างฐานผลประโยชน์อันชอบธรรมได้ และอาจอ้างฐานการปฏิบัติตามสัญญาได้ด้วยหากสอดคล้องกับเนื้อหาสัญญาว่าจ้าง
- ❖ **ข้อมูลการทำงานของลูกจ้าง** บริษัทเฝ้าระวังการใช้งานอินเทอร์เน็ตของพนักงานเพื่อป้องกันไม่ให้พนักงานใช้ทรัพยากรไอทีของบริษัทไปเพื่อการส่วนตัวมากเกินไป ข้อมูลที่เก็บรวบรวมเพื่อการเฝ้าระวังนี้รวมถึงข้อมูลคุกกี้ที่แสดงประวัติการเข้าชมเว็บไซต์และการดาวน์โหลด การเฝ้าระวังนี้กระทำโดยมิได้แจ้งให้พนักงานหรือสหภาพแรงงานทราบก่อน และไม่ได้แจ้งรายละเอียดของการประมวลผลข้อมูลอย่างชัดเจน ในกรณีเช่นนี้แม้บริษัทจะมีผลประโยชน์อันชอบธรรม แต่ว่าเป็นการขัดกับสิทธิความเป็นส่วนตัวของพนักงานอย่างมาก รวมไปถึงการเก็บรวบรวมข้อมูลอาจกระทำเกินจำเป็น ไม่ได้สัดส่วน และไม่โปร่งใส อีกทั้งยังมีวิธีอื่นที่ละเมิดสิทธิของพนักงานน้อยกว่า เช่น จำกัดการเข้าชมเว็บไซต์บางประเภทจากคอมพิวเตอร์ของบริษัท เป็นต้น จึงไม่สามารถอ้างฐานผลประโยชน์อันชอบธรรมได้

- ❖ **ข้อมูลเพื่อช่วยเหลือผู้ลี้ภัย** องค์การการกุศลเพื่อช่วยเหลือผู้ลี้ภัยประมวลผลข้อมูลส่วนบุคคลของผู้ลี้ภัยเพื่อการจัดสรรทรัพยากรที่มีจำกัด ซึ่งไม่อาจใช้ฐานความยินยอมรายบุคคลได้เนื่องจากอาจกระทบต่อสวัสดิภาพผู้ลี้ภัยโดยรวม กรณีเช่นนี้เจ้าของข้อมูลส่วนบุคคลได้รับประโยชน์ด้วยและคาดหวังได้ว่าผู้ควบคุมข้อมูลคือองค์การการกุศลนี้จะดำเนินการประมวลผลข้อมูลส่วนบุคคลของตน ซึ่งผู้ควบคุมข้อมูลจะต้องระมัดระวังอย่างมากในการส่งต่อข้อมูลที่มีความอ่อนไหวที่อาจนำไปสู่อันตรายหรือก่อให้เกิดการเลือกปฏิบัติต่อผู้ลี้ภัยด้วย โดยตรวจสอบบุคคลที่จะเข้าถึงข้อมูลเหล่านั้นอย่างจริงจัง
- ❖ **การแบ่งปันข้อมูลเพื่อยกระดับมาตรฐานการทำงานอุตสาหกรรม** บริษัทในธุรกิจเดียวกัน เช่น ธุรกิจธนาคาร ธุรกิจประกันภัย ธุรกิจค้าปลีก ฯลฯ แบ่งปันข้อมูลลูกค้าหรือข้อมูลของผู้ประกอบการอื่นๆ เพื่อยกระดับมาตรฐานของวงการและป้องกันการฉ้อโกง เช่น ร่วมมือกันสร้าง industry watch-list หรือ sanction-list

โดยต้องผ่านการตรวจสอบข้อมูลว่าถูกต้องเป็นจริง มีการระมัดระวังความมั่นคงปลอดภัยของข้อมูล มีระบบการตรวจสอบที่โปร่งใสไม่เอื้อต่อการใช้ดุลยพินิจในทางไม่ชอบ และไม่กระทบกระเทือนสิทธิของบุคคลหรือเป็นการเลือกปฏิบัติ การแบ่งปันข้อมูลเช่นนี้จะช่วยสร้างประสิทธิภาพในการทำงานและเป็นประโยชน์ต่อตัวเจ้าของข้อมูลที่เป็นผู้ใช้บริการด้วย แต่จะต้องทำโดยมีมาตรฐานและมีการตรวจสอบจากหลายฝ่ายในกลุ่มที่มีลักษณะเป็นสมาคมธุรกิจ ไม่ใช่การส่งต่อข้อมูลระหว่างบริษัทด้วยกันเองโดยไม่ได้รับการตรวจสอบ ซึ่งอาจจะขัดต่อกฎหมายอื่นๆ เรื่องการเลือกปฏิบัติหรือกฎหมายแรงงานที่เกี่ยวกับการกีดกันการจ้างงานอีกด้วย

- ❖ **การแจ้งไม่รับจดหมายข่าว/โทรศัพท์ (do-not-call)** ในกรณีที่ลูกค้าร้องขอไม่ให้ส่งจดหมายข่าวมาอีกนั้น บริษัทอาจอ้างฐานผลประโยชน์อันชอบธรรมในการที่จะเก็บข้อมูลชื่อและช่องทางการติดต่อลูกค้ารายนั้นเพื่อไม่ให้เกิดการส่งจดหมายข่าวแบบไม่เฉพาะเจาะจงไปให้อีกในอนาคตได้
- ❖ **ข้อมูลการเข้าออกห้องโรงแรม** โรงแรมเก็บข้อมูลการเข้าออกห้องพักของผู้เข้าพักและพนักงานผ่านการใช้คีย์การ์ด เพื่อบริหารจัดการในกรณีที่เกิดข้อพิพาทหรือต้องสอบสวนพนักงาน การเก็บข้อมูลนี้เป็นการเก็บชั่วคราวและจะถูกลบออกภายในเวลา 30 วัน ข้อมูลเชิงสถิติอาจนำไปใช้เพื่อปรับปรุงการให้บริการในอนาคตได้

ฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ หรือการศึกษาวิจัย สถิติ (Historical & Statistic Research)

- ไม่มีฐานการประมวลผลนี้ใน GDPR
- หากมีการอ้างกฎหมาย GDPR เช่น การประมวลผลข้อมูลของบุคคลที่มาจากสหภาพยุโรป การประมวลผลข้อมูลฐานนี้ต้องระบุงการประมวลผลข้อมูลฐานอื่น ๆ ประกอบ เช่น ขอเก็บตามฐานภารกิจของรัฐ (Public Task) ฐานการปฏิบัติตามกฎหมาย (Legal Obligation) หรืออาจต้องอาศัยการตัดสินใจตามฐานความยินยอม (Consent) กับเจ้าของข้อมูล
- ผู้ควบคุมข้อมูลสามารถนำเอาข้อมูลส่วนบุคคลมาประมวลผลได้ เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ โดยต้องเป็นไปตามมาตรฐานการวิจัย หรือมาตรฐานวิชาชีพ มาตรฐานจริยธรรมของสาขาวิชาต่าง ๆ ที่เกี่ยวข้อง และสอดคล้องกับหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล คือ หลักความจำเป็น หลักความได้สัดส่วน และการเคารพสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล
- มีมาตรการปกป้องคุ้มครองข้อมูลนั้นอย่างเหมาะสม สอดคล้องกับหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล หรืออย่างน้อยเป็นไปตามที่คณะกรรมการประกาศกำหนด (รอประกาศจากกระทรวง)

ตัวอย่างเช่น บริษัทผลิตยาทำการประมวลผลข้อมูลส่วนบุคคลเพื่อใช้ในการวิจัยพัฒนายารักษาโควิด-19

ที่มา

- Thailand Data Protection Guidelines 3.0

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

- หลักการเก็บรวบรวมข้อมูลส่วนบุคคล-กฎหมายคุ้มครองข้อมูลส่วนบุคคล PDPA

<https://www.hrconsultant.training/post/lawful-basis-for-processing>

- TDPG 2.0 : Building Trust with Data Protection

<https://www.law.chula.ac.th/wp-content/uploads/2019/10/Slides.pdf>