DPIA คือ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

หมายเหตุ สังเกตว่า GDPR เป็นเครื่องมือสำหรับบริหารจัดการความเสี่ยง โดยพิจารณาสิทธิ เสรีภาพของเจ้าของข้อมูลส่วนบุคคล (data subject) เป็นที่ตั้ง

ผู้จัดทำ =data controller ร่วมกันกับ DPO และ data processor

สรุป DPIA เป็นแนวทางที่เป็นประโยชน์สำหรับ data controller ที่จะช่วยให้การพัฒนาระบบประมวลผลข้อมูลที่มีความเสี่ยงสูงเป็นไปตาม GDPR

DPIA เป็นกลไกการกำกับดูแลและเตือนภัยล่วงหน้า (ex-ante mechanism) โดยมุ่งเป้าไปที่การระบุผลกระทบเชิงลบที่อาจเกิดขึ้นและบรรเทาผลกระทบของความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคล

เราจะต้องดำเนินการ DPIA ก่อนการประมวลผลข้อมูลที่มีแนวโน้มว่าอาจทำให้เกิดความเสี่ยงสูงต่อสิทธิ์และเสรีภาพของตัวบุคคล โดยเฉพาะอย่างยิ่งการประมวลผลโดยใช้เทคโนโลยีใหม่

กรณีที่ต้องทำ dpia

1 การประมวลผลที่เป็นระบบและกระทบคนจำนวนมาก มีการประมวลผลโดยอัตโนมัติ และผลการตัดสินใจจากระบบมีผลทางกฎหมายต่อบุคคล
2 การประมวลผลข้อมูลอ่อนไหว (sensitive data) ในปริมาณมากหรือต่อบุคคลจำนวนมาก หรือ ข้อมูลส่วนบุคคลที่เกี่ยวกับประวัติอาชญากรรม
3การติดตามตรวจการอย่างเป็นระบบในพื้นที่เปิดสาธารณะที่มีการเก็บและประมาณข้อมูลปริมาณมาก หรือเกี่ยวเนื่องกับบุคคลจำนวนมาก

นอกจากกรณี 3 ข้างต้นซึ่งระบุชัดเจนตรง ๆ แล้ว ยังมีประเด็นของความเสี่ยงแฝง (inherent risk) ด้วย คือมิได้แสดงความเสี่ยงชัดเจนแต่เป็นลักษณะมีโอกาสหรือแนวโน้ม (สะท้อนคำว่า “likely to result in a high risk”) โดย**การพิจารณาความเสี่ยงแฝงให้พิจารณาลักษณะการประมวลผลตาม 9 เกณฑ์** ดังนี้

1 มีการให้คะแนนหรือประเมิน (รวมถึงการจำแนกหรือทำนาย) ข้อมูลส่วนบุคคล จากมุมมองต่าง ๆ เช่น พฤติกรรมการทำงาน สถานะภาพทางเศรษฐกิจ สุขภาพ ความชอบ ความสนใจ พฤติกรรมส่วนตัว ตำแหน่ง หรือการเคลื่อนที่เดินทาง
2 มีการตัดสินใจแบบอัตโนมัติ ที่ส่งผลทางกฎหมาย (หรือคล้ายคลึง) ต่อ data subject เช่น ผลการตัดสินใจอาจนำไปสู่การยกเว้น การแบ่งแยกกลุ่ม/ประเภทบุคคล (discrimination) อย่างไม่เป็นธรรม

3 การตรวจตราอย่างเป็นระบบ (systematic monitoring) เป็นการประมวลผลที่ใช้เพื่อ สังเกต ตรวจตรา หรือควบคุม data subject รวมถึงข้อมูลที่รวบรวมจากเครือข่ายสื่อสาร หรือ การตรวจตราพื้นที่สาธารณะ สาเหตุที่ประเด็นนี้สำคัญเนื่องจาก data subject อาจไม่รู้ตัวว่ากำลังถูกใครติดตามและบันทึกข้อมูลหรือไม่ อย่างไร ยิ่งไปกว่านั้น อาจทำให้ data subject มิอาจจะหลีกเลี่ยงการประมวลผลดังกล่าวได้เมื่อตนเข้าในพื้นที่สาธารณะนั้น
4 มีการประมวลผลข้อมูลอ่อนไหว หรือมีความเป็นส่วนตัวสูง
5 การประมวลผลข้อมูลปริมาณมาก (GDPR ไม่ได้ระบุว่าขนาดไหนจึงเรียกว่ามาก) โดยเกณฑ์คร่าว ๆ ที่ใช้ประเมินว่าเป็น large scale หรือไม่ มี 4 ข้อด้านล่าง

5.1 จำนวน data subject ไม่ว่าจะระบุเป็นจำนวนตรงๆ หรือ เป็นสัดส่วนของประชากร
5.2 ปริมาณข้อมูล (จำนวน record) หรือความหลากหลาย (จำนวน field)
5.3 ระยะเวลาดำเนินการ
5.4 ขอบเขตทางภูมิศาสตร์ เช่น ระดับเมือง หรือ หลายพื้นที่เล็ก ๆ กระจายกัน

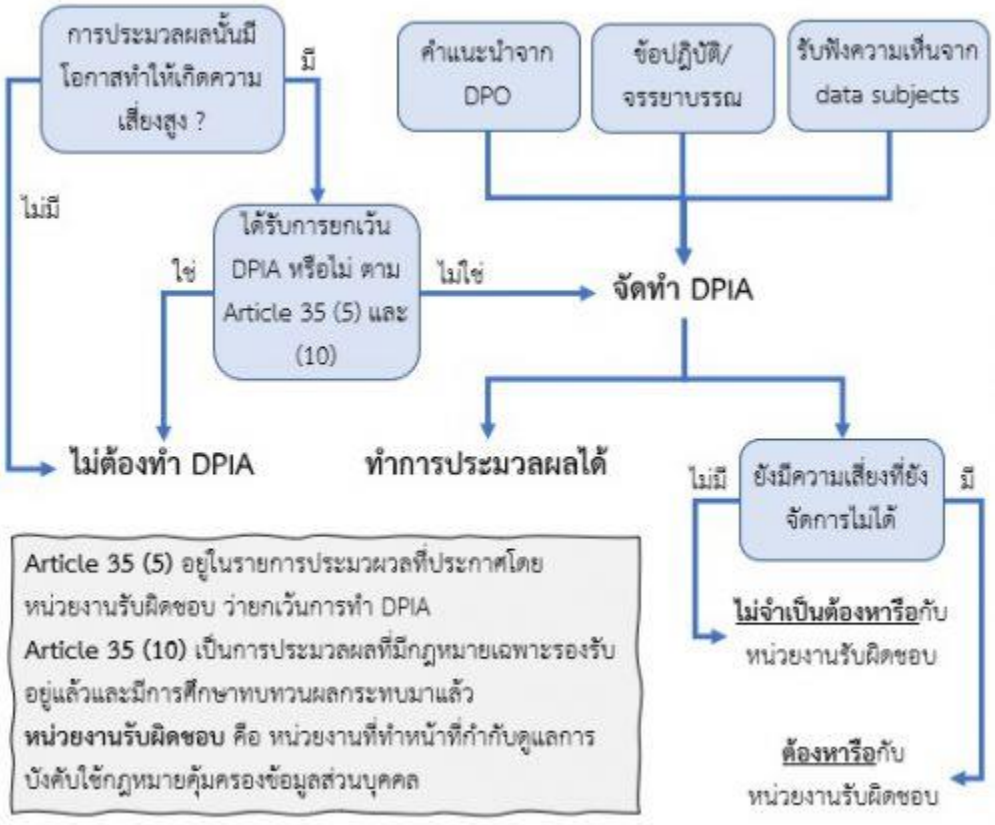
6 การจับคู่ข้อมูล (data matching) หรือ การหลอมรวมข้อมูล (data merging) หมายถึง การประมวลผลที่เกิดกับข้อมูลตั้งแต่ 2 แหล่งมารวมกัน (อาจจะมาจากต่าง data controllers กัน) ซึ่งอาจก่อให้เกิดผลกระทบในลักษณะทวีคูณเทียบกับเมื่อประมวลผลแยกกัน

7 การประมวลผลข้อมูลที่เกี่ยวข้องกับ data subject ที่ถือว่าเปราะบาง เช่น ผู้เยาว์ ลูกจ้าง ผู้มีอาการทางจิต คนเร่ร่อน คนชรา หรือ ผู้ป่วย เช่นนี้ เรียกว่าการประมวลผลนั้นมีแนวโน้มที่จะมีความเสี่ยงสูง เนื่องจากอาจเกิดความไม่สมดุลระหว่าง data subject กับ data controller เนื่องจาก data subject อาจไม่ทราบ หรือ ไม่สามารถปฏิเสธการประมวลผลเหล่านี้ เนื่องจากตนยังไม่สมบูรณ์ (หรือมีความบกพร่อง) ทางกาย ทางจิตใจ หรือทางนิติภาวะ

8 การใช้เชิงนวัตกรรม หรือ ทดลองเทคโนโลยี หรือ ทดลอง solution เช่น การรวมลายนิ้วมือกับการรู้จำใบหน้าเพื่อการอนุญาตให้ผ่านเข้าออกพื้นที่ ในเมื่อเป็นการทดลอง จึงอาจมีความเสี่ยงที่ยังคาดไม่ถึง เพราะอาจต้องใช้การเก็บและใช้ข้อมูลรูปแบบใหม่ ตัวอย่างเช่น IoT มีการเก็บข้อมูลตลอดเวลา และรวดเร็ว อาจจะนำมาซึ่งผลกระทบต่อ data subject ที่คาดไม่ถึง

9 เมื่อการประมวลผลนั้นจำกัด data subject จากการได้รับสิทธิประโยชน์ หรือบริการบางอย่าง เช่น ธนาคารประมวลผลข้อมูลประวัติเครดิตในการตัดสินใจว่าจะให้ลูกค้ากู้ยืมหรือไม่

ขั้นตอนและหลักการพื้นฐานในการทำ DPIA



data controller ต้องทำการสำรวจความคิดเห็นของ data subject ด้วย

- การได้มาเพียงความยินยอมให้เก็บรวบรวมข้อมูล (consent) ไม่ใช่การสำรวจความเห็น
- เนื่องจากการประมวลผล ยังไม่เกิดขึ้นจริง จึงเป็นเพียงการสำรวจความเห็นของผู้ที่คาดว่าจะเป็น data subject (prospect data subject)
- หากการตัดสินของ data controller ไม่ตรงกับความเห็นของ data subject จะต้องมีการเขียนอธิบายเหตุผลไว้ด้วยว่าเหตุใดจึงตัดสินทำ หรือ ไม่ทำอะไร
- หาก data controller ตัดสินใจไม่ดำเนินการสำรวจความเห็นของ data subject ก็จะต้องทำการบันทึกเหตุผลเป็นเอกสารไว้ด้วย เช่น ถ้าทำอาจทำให้เกิดความลับทางธุรกิจรั่วไหล แผนธุรกิจ หรือเป็นเรื่องไม่เหมาะสม หรือปฏิบัติไม่ได้เนื่องด้วยข้อจำกัดอย่างอื่น

-เมื่อใดจึงควรต้องขอความเห็นจากหน่วยงานผู้รับผิดชอบ ?

<u>คำตอบ</u> เมื่อมีความเสี่ยงที่ยังจัดการไม่ได้ และความเสี่ยงนั้นมีโอกาสเกิดได้สูง และ/หรือ มีผลกระทบสูง เช่น การประมวลผลข้อมูลสุขภาพของคนจำนวนมาก ถือว่ามีความเสี่ยงสูง

-เมื่อมีความเสี่ยงสูง จึงต้องหามาตรการออกมารองรับ เช่น กรณีฮาร์ดดิสค์ของคอมพิวเตอร์พนักงาน มีความเสี่ยงเนื่องจากใช้เก็บและประมวลผลข้อมูลส่วนบุคคล จึงต้องมีมาตรการทางเทคนิคและทางการจัดการรักษาความปลอดภัยด้วย เช่น

- ทำการเข้ารหัส (encrypt) ข้อมูลทั้งหมดในฮาร์ดดิสค์
- การบริหารจัดการและให้มีกุญแจสำหรับไขเข้าออกห้องทำงานหรือห้องคอมพิวเตอร์
- การตรวจจับการเข้าถึง (access control) ผ่านระบบ
- การสำรองข้อมูลที่มั่นคงปลอดภัย

-ตัวอย่างของความเสี่ยงสูงที่ไม่ได้ถูกบริหารจัดการแก้ไข เช่น พบว่ามีโอกาสที่ผู้ไม่ประสงค์ดีจะเข้าถึงข้อมูลของ data subjects และนำไปสู่การคุกคามชีวิต การทำให้ตกงาน ความเสี่ยงต่อทรัพย์สินเงินทอง และ/หรือ เห็นได้ชัดว่าความเสี่ยงดังกล่าวอาจขึ้นได้ง่าย เนื่องจากไม่มีมาตรการดูแลอย่างเพียงพอ หรือไม่สามารถควบคุมผู้เข้าถึงข้อมูลและนำไปใช้ได้เพราะมีการแชร์ข้อมูล ใช้ หรือแจกจ่าย หรือ เมื่อจุดอ่อน ของระบบที่เสี่ยงต่อการถูกโจมตีไม่ได้มีการจัดการ

กรณีที่ไม่ต้องทำ DPIA

- เมื่อประเมินแล้วพบว่าน่าจะมีความเสี่ยงต่ำ (not likely to result in a high risk)
- มี DPIA ที่คล้ายคลึงกันได้ถูกจัดทำไว้แล้ว (สามารถนำมาใช้โดยไม่ต้องจัดทำซ้ำ)
- ได้รับการตรวจสอบจากหน่วยงานรับผิดชอบและได้รับการอนุมัติให้ดำเนินการก่อนพฤษภาคม 2018 (ปีที่ GDPR ประกาศบังคับใช้)
- มีฐานกฎหมายรองรับ ได้แก่ Article 6 (c) ประมวลผลเนื่องจากจำเป็นต้องทำตามกฎหมายกำหนดอำนาจหน้าที่ให้ทำ หรือ Article 6 (e) ทำเพื่อประโยชน์สาธารณะ ทั้งนี้ใน 2 กรณีนี้ มักมีกฎหมายควบคุมการดำเนินการอยู่แล้ว และ DPIA อาจได้ถูกจัดทำไปแล้วในเชิงภาพรวมในระหว่างที่ร่างกฎหมายควบคุมนั้น ๆ อย่างไรก็ตามหน่วยงานรับผิดชอบอาจเห็นควรให้ทำ DPIA อีกเป็นการเฉพาะก็ได้ (อ้างจาก Article 35 (10))
- อยู่ในรายการประมวลผล ที่ไม่จำเป็นต้องทำ DPIA ซึ่งกำหนดและประกาศโดยหน่วยงานผู้รับผิดชอบ (เทียบได้กับ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของไทย) ทั้งนี้สามารถกำหนดเงื่อนไขประกอบต่าง ๆ ให้ผู้ปฏิบัติตรวจสอบได้ด้วยว่าการประมวลผลดังกล่าว ตกหรือตรงกับรายการประมวลผลที่ประกาศหรือไม่ ซึ่งหน่วยงานรับผิดชอบจะต้องรายงาน EPDB ด้วย อ้างอิงตาม Article 35 (5)

ตารางแสดงตัวอย่างการประเมินว่าการประมวลผลใดต้องทำ DPIA หรือไม่ โดยระบุเกณฑ์ว่าตรงกับข้อใดบ้าง

ตัวอย่างการประมวลผล	เกณฑ์ที่เกี่ยวข้อง	ต้องทำ DPIA หรือไม่
โรงพยาบาลแห่งหนึ่งประมวลผลข้อมูลพันธุกรรมและข้อมูลสุขภาพของผู้ป่วย (ผ่านระบบสารสนเทศของโรงพยาบาล)	• ข้อมูลอ่อนไหว หรือมีความเป็นส่วนตัวสูง • ข้อมูลที่อาจส่งผลต่อความเสียหายของ data subject • การประมวลผลข้อมูลกับบุคคลจำนวนมาก	ต้อง
การใช้ระบบกล้อง CCTV เพื่อตรวจตราพฤติกรรมการขับรถบนทางหลวง โดย data controller วางแผนจะใช้ระบบวิเคราะห์วิดีโออัตโนมัติ เพื่อจำแนกรถและป้ายทะเบียน	• การตรวจตราโดยใช้ระบบ • มีการใช้นวัตกรรมและ/หรือ ประยุกต์ใช้วิธีการแก้ปัญหาเชิงเทคโนโลยีและเชิงการจัดการ	ต้อง
การรวบรวมข้อมูลจาก social media สาธารณะสำหรับทำ profile (จัดกลุ่มบุคคล)	• มีการประเมินค่า หรือให้คะแนน • ประมวลผลข้อมูลปริมาณมาก หรือ กับบุคคลจำนวนมาก • การจับคู่ หรือ การหลอมรวมข้อมูล • ข้อมูลอ่อนไหว หรือมีความเป็นส่วนตัวสูง	ต้อง
สถาบันระดับชาติที่รวบรวมข้อมูลเครดิตและการฉ้อโกง	• มีการประเมินค่า หรือให้คะแนน • มีการประเมินและตัดสินใจแบบอัตโนมัติซึ่งส่งผลทางกฎหมายหรือเทียบเคียง • ส่งผลให้เกิดการจำกัด data subject ในการใช้สิทธิ หรือ รับบริการ หรือ ทำสัญญา • ข้อมูลอ่อนไหว หรือมีความเป็นส่วนตัวสูง	ต้อง
คลังข้อมูลเพื่อใช้เก็บข้อมูลอ่อนไหวที่ถูกทำให้เสมือนนิรนามแล้ว (pseudonymized) ซึ่งเดิมจัดเก็บไว้เพื่อการโครงการวิจัยหรือการทดสอบการรักษาด้านการแพทย์	• ข้อมูลอ่อนไหว • หากถูกละเมิดเสี่ยงที่จะมีผลเสียต่อ data subject ได้ง่าย • ส่งผลให้เกิดการจำกัด data subject ในการใช้สิทธิ หรือ รับบริการ หรือ ทำสัญญา	ต้อง

นิตยสารออนไลน์ใช้ข้อมูลรายการอีเมล์เพื่อที่จะส่งอีเมล์สรุปเนื้อหารายวันให้กับสมาชิก	• มีการประมวลผลข้อมูลบุคคลจำนวนมาก	ไม่ต้อง
เว็บขายของออนไลน์แสดงโฆษณาอาไหล่รถย้อนยุค โดยอาศัยการจัดกลุ่มลูกค้าที่เข้าชมเว็บไซต์และอิงกับรายการสินค้าที่ดูหรือซื้อ ทั้งนี้เพื่อให้เลือกแสดงโฆษณาดังกล่าวกับเฉพาะผู้ที่สนใจ	• มีการประเมินค่า หรือให้คะแนน	ไม่ต้อง

รายการหัวข้อที่ควรปรากฏใน DPIA

- คำอธิบายการประมวลผลที่คาดการณ์และจุดประสงค์การประมวลผล
- การประเมินความจำเป็น และความสมเหตุผลในการประมวลผล
- การประเมินระดับความเสี่ยง ที่มีต่อสิทธิและเสรีภาพของ data subject มีแง่มุมไหนอะไรบ้าง
- มาตรการที่ใช้ (ลดความเสี่ยง) ต้องแสดงให้เห็นว่า
- จะลดความเสี่ยงได้อย่างไร
- แสดงให้เห็นว่าสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างไร ข้อไหน

เกณฑ์สำหรับ DPIA

1. **มีการอธิบายกระบวนการประมวลผลอย่างเป็นระบบ (ระบุใน Article 35(7) (a)) โดยมีหัวข้อต่อไปนี้**
    1. อธิบายธรรมชาติ ขอบเขต บริบท และจุดประสงค์ ของการประมวลผล (GDPR Recital 90)
    2. รายการข้อมูลส่วนบุคคล ผู้รับ และระยะเวลาซึ่งข้อมูลส่วนบุคคลนั้นจะถูกจัดเก็บและบันทึกไว้
    3. คำอธิบายฟังก์ชั่นการทำงานที่เกี่ยวกับประมวลผลข้อมูล เพื่อให้ทราบว่าประมวลผลอย่างไร
    4. สินทรัพย์และเครื่องมือต่าง ๆ ที่เกี่ยวข้องและนำมาใช้กับการประมวลผลข้อมูลส่วนบุคคล (hardware, software, เครือข่าย, บุคลากร, เอกสาร และช่องทางการส่งเอกสาร)
    5. การปฏิบัติตามกฎหมายฯ พร้อมระบุหัวข้อในจรรยาบรรณธุรกิจ ที่สอดคล้องกัน (กำหนดไว้ใน Article 35(8))
2. **มีการประเมินความจำเป็นและความเหมาะสม (Article 35(7)(b))**
    1. วางมาตรการลดความเสี่ยงล่วงหน้า โดยนำ Article 35(7)(d) และ Recital 90 มาพิจารณาร่วมด้วย
        1. ระบุจุดประสงค์ที่ชัดเจนและมีเหตุผลประกอบ (Article 5(1)(b))
        2. ระบุฐานกฎหมายที่ใช้ในการประมวลผล (เลือกที่เหมาะสมตามที่ระบุใน Article 6)
        3. รายการข้อมูลที่จำเป็นต้องใช้ประมวลผล Article 5(1)(c)
        4. ระยะเวลาที่จัดเก็บข้อมูลไว้ Article 5(1)(e)
    2. มาตรการที่ให้การดูแลสิทธิของ data subject
        1. ให้ข้อมูลแก่ data subject ทราบ (ตามที่ระบุใน Articles 12, 13 and 14)
        2. สิทธิในการเข้าถึงข้อมูลและสิทธิเกี่ยวกับการถ่ายโอนข้อมูลให้ผู้บริการรายอื่น (กรณี data subject ต้องการเปลี่ยนผู้ให้บริการ) (Articles 15 and 20)
        3. สิทธิในการขอให้แก้ไขข้อมูลและให้ลบข้อมูล (Articles 16, 17 and 19)
        4. สิทธิในการคัดค้านและจำกัดการประมวลผล (Article 18, 19 and 21)
        5. ลักษณะความสัมพันธ์ระหว่างdata controller กับ data processor (Article 28)
        6. การระวังป้องกันข้อมูลกรณีมีการถ่ายโอนข้ามประเทศ (ปฏิบัติตาม Chapter 5 Transfers of personal data to third countries or international organizations ซึ่งประกอบด้วย Article 44-50)
        7. การปรึกษาหารือ (prior consultation) กับหน่วยงานรับผิดชอบ (Article 36)

3. **ความเสี่ยงต่อสิทธิและเสรีภาพของ data subject ได้รับการใส่ใจและจัดการ Article 35 (7)(c)**
    1. ต้นต่อของความเสี่ยงถูกนำมาพิจารณา
    2. ผลกระทบต่อสิทธิและเสรีภาพของ data subjects ได้รับการชี้จำเพาะแยกเป็นประเด็น ๆ สำหรับเหตุการณ์ต่าง ๆ เช่น การเข้าถึงข้อมูลโดยมิชอบด้วยกฎหมาย การแก้ไขข้อมูลโดยไม่รับอนุญาต และการสูญหายของข้อมูล
    3. การคุกคามที่อาจนำไปสู่การเข้าถึงข้อมูลโดยมิชอบด้วยกฎหมายและการแก้ไขข้อมูลโดยไม่รับอนุญาต

4. มีการประเมินโอกาสที่จะเกิดเหตุและระดับความรุนแรง (Recital 90)
5. กำหนดมาตรการรองรับความเสี่ยงต่าง ๆ ที่ได้วิเคราะห์ไว้ (Article 35(7)(d) and Recital 90)

4. การมีส่วนร่วมของฝ่ายต่างๆ ที่เกี่ยวข้อง

1. มีการรับคำปรึกษาจาก Data Protection Officer (Article 35(2))
2. รับฟังความคิดเห็นจาก data subject (หรือตัวแทน) Article 35(9)