## **ตัวอย่างแบบฟอร์มการทำDPIA**

# Step 1: Identify the need for a DPIA

|  |
| --- |
| **ขั้นตอนที่ 1 [DPIA Identification] การระบุความจำเป็นในการทำ DPIA** ตามประเภทของการประมวลผลข้อมูล หรือโครงการที่จะมีการประมวลผลข้อมูล ทั้งที่เป็นโครงการใหม่หรือที่มีการปรับปรุงเปลี่ยนแปลงการประมวลผลข้อมูลที่มีอยู่เดิม โดยระบุลักษณะที่แสดงถึงความจำเป็น รวมถึงแหล่งอ้างอิงที่เหมาะสม |
|  จำเป็น อ้างอิงตาม  ประกาศหรือบัญชีรายชื่อการประมวลผลข้อมูลส่วนบุคคลของสำนักงานคุ้มครองข้อมูลส่วนบุคคลที่จำเป็นต้องจัดทำ DPIA  Thailand Data Protection Guidelines 2.0 ส่วนที่ E1[บันทึกลักษณะที่จำเป็นต้องจัดทำ DPIA]  [Scoring]  [Automated-decision with legal effect]  [Sensitive data]  [Large scale]  [Combining datasets]  [Vulnerable data subjects]  [Innovative use]  [Prevent data subjects’ right or access] |
|  ไม่จำเป็น [บันทึกเหตุผลที่ไม่จำเป็นต้องจัดทำ DPIA] |

# Step 2: Describe the processing

|  |
| --- |
| **ขั้นตอนที่ 2 [Description] อธิบายรายละเอียดของกระบวนการประมวลผลข้อมูลส่วนบุคคล** อย่างน้อยต้องประกอบด้วย สภาพ (nature), ขอบเขต (scope), บริบท (context) และวัตถุประสงค์ (purpose) ของการประมวลผล |
| **2.1 [Nature] อธิบายสภาพของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดตอไปนี้** การเก็บรวมรวมขอมูล การจัดเก็บข้อมูล การใช้ข้อมูล ผู้ที่สามารถเข้าถึงข้อมูล ผู้ที่ได้รับข้อมูล ผู้ประมวลผลข้อมูล ระยะเวลาจัดเก็บข้อมูล มาตรการความปลอดภัย เทคโนโลยีใหม่ที่ใช้ในการประมวลผลข้อมูล กระบวนการแบบใหม่ที่ใช้ในประมวลผลข้อมูล ปัจจัยที่ทำให้มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล[บันทึกรายละเอียดสภาพของการประมวลผลข้อมูล] |

|  |
| --- |
| **2.2 [Scope] ระบุขอบเขตของการประมวลผลข้อมูล โดยรวมถึงรายละเอียดต่อไปนี้** สภาพและลักษณะของข้อมูลส่วนบุคคล ปริมาณและความหลากหลายของข้อมูลส่วนบุคคล ความอ่อนไหวของข้อมูลส่วนบุคคล ระดับและความถี่ของการประมวลผลข้อมูล ระยะเวลาของการประมวลผลข้อมูล จำนวนของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง พื้นที่เชิงภูมิศาสตร์ที่การประมวลผลข้อมูลครอบคลุมไปถึง[บันทึกรายละเอียดขอบเขตของการประมวลผลข้อมูล] |

|  |
| --- |
| **2.3 [Context] อธิบายบริบทของการประมวลผลข้อมูล ทั้งปัจจัยภายในและภายนอกที่อาจส่งผลต่อความ****คาดหวังและผลกระทบของการประมวลผลข้อมูล** โดยรวมถึงรายละเอียดต่อไปนี้ แหล่งข้อมูลส่วนบุคคล ลักษณะของความสัมพันธ์กับเจ้าของข้อมูลส่วนบุคคล ระดับความสามารถในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล ระดับความคาดหวังของเจ้าของข้อมูลที่มีต่อการประมวลผลข้อมูล มีข้อมูลส่วนบุคคลของผู้เยาว์หรือผู้เปราะบางหรือไม่ ประสบการณ์ที่ผ่านมาของการประมวลผลข้อมูลแบบเดียวกัน ความก้าวหน้าทางเทคโนโลยีหรือมาตรการความปลอดภัยทางสารสนเทศที่เกี่ยวข้อง ประเด็นที่เป็นข้อวิตกกังวลของสาธารณะ มีการปฏิบัติตามมาตรฐานหรือแนวปฏิบัติที่เกี่ยวข้องหรือไม่[บันทึกรายละเอียดบริบทของการประมวลผลข้อมูล] |
| **2.4 [Purpose] อธิบายวัตถุประสงค์ของการประมวลผลข้อมูล** โดยรวมถึงรายละเอียดต่อไปนี้ ผลลัพธ์ที่ต้องการสำหรับผู้ควบคุมข้อมูล ฐานประโยชน์อันชอบธรรม (legitimate interest) (ถ้ามี) ผลลัพธ์ที่ต้องการสำหรับบุคคล ประโยชน์ที่คาดว่าจะได้รับสำหรับผู้ควบคุมข้อมูลหรือสังคมโดยรวม[บันทึกรายละเอียดวัตถุประสงค์ของการประมวลผลข้อมูล] |

# Step 3: Consultation process

|  |
| --- |
| **ขั้นตอนที่ 3 [Consultation] ระบุ เหตุผล, วิธีการ, และช่วงเวลาที่จะปรึกษาหารือและรับฟังความเห็น รวมถึง****กรณีที่จะไม่ปรึกษาหารือและรับฟังความเห็นด้วย** อย่างน้อยจากผู้เกี่ยวข้องต่อไปนี้ |
|  [Data subject] เจ้าของข้อมูลส่วนบุคคล [Data processor] ผู้ประมวลผลข้อมูลส่วนบุคคล [Internal stakeholders] ผู้เกี่ยวข้องภายในองค์กร รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) [Independent experts] ผู้เชี่ยวชาญทางกฎหมายและผู้เชี่ยวชาญด้านที่เกี่ยวข้องจากภายนอก [Data Protection Agency] สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อื่นๆ (โปรดระบุ)[บันทึกรายละเอียดการปรึกษาหารือและรับฟังความเห็น] |

# Step 4: Assess necessity and proportionality

|  |
| --- |
| ขั้นตอนที่ **4 [Necessity and proportionality]** อธิบายความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล **โดยอาจระบุเนื้อหาดังต่อไปนี้** |
|  การประมวลผลข้อมูลส่วนบุคคลดังกล่าวช่วยให้ได้ผลลัพธ์ที่ประสงค์หรือไม่ อย่างไร มีช่องทางอื่นหรือไม่ที่สามารถดำเนินการได้ตามสมควรเพื่อให้ได้ผลลัพธ์ที่ประสงค์เดียวกัน ฐานในการประมวลผลข้อมูลตามกฎหมาย แนวทางป้องกันไม่ให้มีการประมวลผลข้อมูลที่ไม่เหมาะสม แนวทางดำเนินการเพื่อประกันคุณภาพของข้อมูล แนวทางดำเนินการเพื่อประกันการจัดเก็บข้อมูลเท่าที่จำเป็น (data minimization) ทั้งในแง่ของประเภทข้อมูลและระยะเวลาการจัดเก็บข้อมูล แนวทางการแจ้งข้อมูลการประมวลผลข้อมูลที่เกี่ยวข้องแก่เจ้าของข้อมูล แนวทางดำเนินการเพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล มาตรการเพื่อประกันการปฏิบัติตามขั้นตอนของผู้ประมวลผลข้อมูลส่วนบุคคล มาตรการคุ้มครองการส่งข้อมูลระหว่างประเทศ[บันทึกรายละเอียดการพิจารณาความจำเป็นและความได้สัดส่วน] |

# Step 5: Identify and assess risks

|  |
| --- |
| ขั้นตอนที่ **5 [Risk assessment]** การประเมินความเสี่ยงที่จะมีผลกระทบตอสิทธิเสรีภาพของบุคคล ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน โดยคำนึงถึง “ความน่าจะเป็น” **(likelihood)** และ “ความร้ายแรง”**(severity) โดยแต่ละความเสี่ยงอย่างน้อยควรระบุถึงรายละเอียดต่อไปนี้** |
| **- บ่อเกิดของความเสี่ยงต่างๆ และความน่าจะเป็นที่จะเกิดเหตุการณ์และผลกระทบจากเหตุการณ์เหล่านั้น เช่น การเข้าถึงระบบโดยมิชอบ, การดัดแปลงหรือสูญเสียข้อมูล เป็นต้น****- ผลกระทบจากกการประมวลผลข้อมูลดังกล่าวที่จะมีต่อเจ้าของข้อมูลส่วนบุคคล ทั้งในเชิงร่างกาย จิตใจและทรัพย์สิน ว่าจะมีผลกระทบต่อเจ้าของข้อมูลหรือไม่****- ความน่าเป็น (ต่ำ / พอสมควร / สูง)****- ความร้ายแรง (น้อย / พอสมควร / มาก)****- ผลการประเมินความเสี่ยง (ต่ำ / กลาง / สูง)****[บันทึกรายละเอียดการประเมินความเสี่ยง]** |
| บ่อเกิดของความเสี่ยง | ผลกระทบ | ความร้ายแรง(ต่ำ/ พอสมควร/สูง) | ความร้ายแรง(น้อย/ พอสมควร/ มาก) | **ผลการ ประเมิน ความเสี่ยง** (ต่ำ/กลาง/ สูง) |
| ความเสี่ยงที่ (1)ความเสี่ยงที่ (2)ความเสี่ยงที่ (3)ความเสี่ยงที่ (4)ความเสี่ยงที่ (5) | ตัวอย่างเช่น- ทำให้ไม่สามารถใช้สิทธิได้ตามสมควร ทั้งที่เป็นสิทธิความเป็นส่วนตัว และสิทธิอื่น ๆ- ทำให้ไม่สามารถเข้าถึงบริการ หรือเสียโอกาสบางอย่าง- ทำให้ไม่สามารถควบคุมการใช้งานข้อมูลส่วนบุคคลของตนได้- ทำให้ถูกเลือกปฏิบัติ- ทำให้ถูกสวมรอยบุคคล (identity theft) หรือหลอกลวงได้- ทำให้เกิดความเสียหายทางการเงิน- ทำให้เกิดความเสียหายแก่ชื่อเสียง- ทำให้เกิดความเสียหายแก่ร่างกาย- ทำให้สูญเสียความลับ- ทำให้ข้อมูลส่วนบุคคลที่ผ่านกระบวนการแฝงข้อมูล (pseudonymization) สามารถระบุตัวบุคคลได้- ผลกระทบอื่นๆ ทางเศรษฐกิจและสังคมที่มีนัยสำคัญ |  |  |  |

# Step 6: Identify measures to reduce risk

|  |
| --- |
| ขั้นตอนที่ **6 [Mitigating measures]** ระบุมาตรการเพื่อลดความเสี่ยง**แต่ละรายการจากขั้นตอนที่ 5 โดยควรระบุว่ามาตรการดังกล่าวสามารถลดหรือกำจัดความเสี่ยงได้หรือไม่ อย่างไร ข้อดีและข้อเสียของแต่ละมาตรการที่เลือกใช้** |
| ความเสี่ยง | มาตรการที่จะดำเนินการ | ผลต่อความเสี่ยง**(หมดไป/ลดลง/ยอมรับได้)** | ความเสี่ยงที่เหลืออยู่**(ต่ำ/กลาง/สูง)** | ผลการพิจารณา**(อนุมัติ/ไม่อนุมัติ)** |
| ความเสี่ยงที่ (1)ความเสี่ยงที่ (2)ความเสี่ยงที่ (3)ความเสี่ยงที่ (4)ความเสี่ยงที่ (5) | ตัวอย่างเช่น- การไม่จัดเก็บข้อมูลบางประเภท- การลดขอบเขตของการประมวลผลข้อมูล- การลดระยะเวลาการจัดเก็บข้อมูล- การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย- การฝากอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้- การแฝงข้อมูลหรือการทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้- การกำหนดแนวปฏิบัติภายในเพื่อลดความเสี่ยง- การเพิ่มขั้นตอนที่ดำเนินการโดยมนุษย์เพื่อทบทวนการประมวลผลด้วยระบบอัตโนมัติ- การใช้เทคโนโลยีที่แตกต่างกัน- การจัดให้มีข้อตกลงการใช้ข้อมูลร่วมกัน (data sharing) ที่ชัดเจน- การปรับปรุงข้อมูลแจ้งเตือนเกี่ยวกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล- การจัดให้มีช่องทางที่เจ้าของข้อมูลส่วนบุคคลสามารถเลือกที่จะไม่ให้ความยินยอม- การจัดให้มีระบบอำนวยความสะดวกแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของเขา |  |  |  |

# Step 7: Sign off and record outcomes

|  |
| --- |
| ขั้นตอนที่ **7 [Documentation and planning]** บันทึกรายละเอียดของแต่ละขั้นตอนที่ผ่านมาข้างต้น **โดยระบุว่าความเสี่ยงบางกรณีอยู่ในระดับที่ยอมรับได้ โดยควรปรึกษาหารือกับ DPO ว่าการดำเนินการตามแผนที่สรุปมาเป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่** |
| **[บันทึกรายละเอียดและแผนงาน]** |
| **Item** | ความเห็น / คำสั่ง | ผู้มีอำนาจตัดสินใจ / วันที่ |
| มาตรการที่เสนอดำเนินการ1.2.3. | [เช่น ให้กำหนดไว้ในแผนการดำเนินงานของโครงการ ................................................................................................ ตั้งแต่วันที่ ............................................................................... ผู้รับผิดชอบคือ .......................................................................] |  |
| ความเสี่ยงที่เหลืออยู่1.2.3. |  |  |
| ความเห็นของ DPO  | [เห็นดวย / ไมเห็นดวย พรอมเหตุผลประกอบ] |  |
| ผลจากการปรึกษาหารือและรับฟง ความเห็น | [เห็นดวย / ไมเห็นดวย พรอมเหตุผลประกอบ] |  |
| **ขั้นตอนที่ 8 [Monitoring and review] การติดตามตรวจสอบและทบทวน ตาม DPIA ฉบับนี้** | ใหติดตามตรวจสอบโดย - DPO หรือหนวยงาน.................................................. - ผูรับผิดชอบโครงการหรือการประมวลผลขอมูลตาม DPIA นี้มีหนาที่รายงาน DPO หรือหนวยงาน ..................................................................................... เมื่อมีการปรับปรุงเปลี่ยนแปลงการประมวลผล |  |
| การเผยแพรเอกสาร DPIA ฉบับนี้ | ใหเผยแพรทาง ........................................................................ โดยปกปดเฉพาะขอมูล ........................................................................ |  |