รายการประเมินคู่ค้า/คู่สัญญา

(Vendor/Contractor Assessment)

ให้หน่วยงานที่รับผิดชอบจัดทำแบบการประเมินนี้ประกอบกับการจัดซื้อจัดจ้างผู้ประมวลผลข้อมูลส่วนบุคคลทุกกรณี

- รายการใดที่ไม่เกี่ยวข้องกับกิจกรรมการประมวลผลตามสัญญา ให้ระบุว่า “N/A”
- การประเมินให้อ้างอิงไปยังกิจกรรมที่ระบุไว้ตาม ROP ของหน่วยงานเป็นหลัก
- กรณีที่ผลการประเมินระดับความเสี่ยงสูง ให้หน่วยงานหลีกเลี่ยงไม่ใช้บริการดังกล่าว ในกรณีที่จำเป็นจะต้องให้เหตุผลชี้แจงประกอบการพิจารณาอนุมัติ
- กรณีที่ผลการประเมินระดับความเสี่ยงปานกลาง ให้หน่วยงานคัดเลือกผู้ใช้บริการด้วยความระมัดระวัง และอาจกำหนดเงื่อนไขการทำงานร่วมกันเพิ่มเติมตามที่เหมาะสมประกอบการพิจารณาอนุมัติ
- ให้หน่วยงานที่รับผิดชอบทำความเห็นประกอบไว้ว่าเหมาะสมที่จะใช้บริการหรือไม่ อย่างไร
- ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำความเห็นประกอบ
- ให้ทบทวนการประเมินดังกล่าวเป็นอย่างน้อยปีละหนึ่งครั้ง หรือตามที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกำหนด

๑. ข้อมูลทั่วไป

ชื่อคู่ค้า / คู่สัญญา	
รายละเอียดของคู่ค้า / คู่สัญญา * ประเภทของบริการและรายละเอียดที่เกี่ยวข้อง	
สถานะการให้บริการ / การดำเนินการ * ดำเนินการอยู่ / ไม่มีการดำเนินการ	
ที่อยู่ที่ติดต่อ	
หน่วยงานที่รับผิดชอบ * ส่วนงานหรือฝ่ายงานที่ใช้บริการ	
กิจกรรมการประมวลผลที่ใช้บริการ * อ้างอิงไปที่กิจกรรมใน ROP ID	
ระบบงานที่เกี่ยวข้องกับการบริการ * อ้างอิงไปที่ Assets/Databases	
สัญญาการใช้บริการ * อ้างอิงไปที่สัญญาและกองกฎหมายที่ตรวจสอบ	

การจ้างช่วง (Sub-Processor) * มีการจ้างช่วงหรือไม่	
สถานที่ที่จัดเก็บข้อมูล (Hosting Location) * ระบุสถานที่และประเทศที่ตั้ง	
ผู้ให้บริการจัดเก็บข้อมูล (Hosting Provider) * ระบุผู้ให้บริการ	
เอกสารมาตรฐานที่ได้รับรอง * ISO27001 / NIST / GDPR Approved Code of Conduct etc.	
มีข้อมูลส่วนบุคคลที่ส่งให้ดำเนินการหรือไม่ * มี / ไม่มี	
ประเภทเจ้าของข้อมูลที่เกี่ยวข้อง * อ้างอิงตาม ROP	
ข้อมูลส่วนบุคคลที่ส่งให้ดำเนินการ * ระบุ field ข้อมูล	

๒. การคุ้มครองข้อมูลส่วนบุคคล

มาตรการความเป็นส่วนตัว	
ข้อมูลส่วนบุคคลที่ส่งให้เป็นข้อมูลที่เปิดเผยสาธารณะอยู่ก่อนแล้วหรือไม่ * ใช่ / ไม่ใช่	
มีการแจ้งรายละเอียดการประมวลผลข้อมูลส่วนบุคคลหรือไม่ * มี / ไม่มี	
ลักษณะของการแจ้งรายละเอียดการประมวลผล * อ่านง่ายเข้าใจง่าย * เข้าถึงง่าย * ไม่มีค่าใช้จ่าย	
ระดับความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานที่รับผิดชอบประเมิน * สูง / กลาง / ต่ำ * หน่วยงานประเมินจากข้อมูลข้างต้นประกอบกับกิจกรรมตาม ROP ที่ระบุ	

มาตรการความมั่นคงปลอดภัย	
มาตรการเชิงเทคนิคเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล ระบุรายละเอียด เช่น * SOPs * Access control lists * Secure email * Virtual privacy networks * File-based encryption * Secure, dedicated line transfer	
มาตรการเชิงองค์กรเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล ระบุรายละเอียด เช่น * Security card access – building * Security card access – room or work area * Locked file cabinets * Clean Desk Policy / Procedure * Data Breach Notification	
มาตรการทางกายภาพเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูล ระบุรายละเอียด เช่น * Secure zones be defined and protected by appropriate entry controls * Intruder detection systems * Automatic fire suppression system	
ระดับความเสี่ยงของความมั่นคงปลอดภัยข้อมูลส่วนบุคคลที่หน่วยงานที่รับผิดชอบประเมิน * สูง / กลาง / ต่ำ * หน่วยงานประเมินจากข้อมูลข้างต้นประกอบกับกิจกรรมตาม ROP ที่ระบุ	
มาตรการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	
มีการส่งข้อมูลส่วนบุคคลไปนอกองค์กรหรือไม่ * มี / ไม่มี	
มีการส่งข้อมูลส่วนบุคคลไปต่างประเทศหรือไม่ * มี / ไม่มี	
ประเทศที่รับข้อมูลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequacy Decision) หรือไม่ * มี / ไม่มี	
มาตรการความปลอดภัยที่เหมาะสม (Appropriate Safeguards) อื่นๆ * ISO27001 / NIST / GDPR Approved Code of Conduct etc.	

ความเห็นของส่วนงาน
* เช่น กรณีจำเป็นต้องใช้บริการที่มีระดับความเสี่ยงของความมั่นคงปลอดภัยสูง หรือมีการส่งข้อมูลส่วนบุคคลตามคำถามข้างต้น แต่ไม่มีมาตรการรองรับที่เหมาะสม เป็นต้น
ความเห็นของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล