ตารางแสดงวงเงินงบประมาณที่รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

1. **ชื่อโครงการ** การจ้างที่ปรึกษาตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและส่งเสริมการดำเนินงานขององค์กรให้สอดคล้องกับข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPC Regulator Checklist)
2. **หน่วยงานเจ้าของโครงการ** ฝ่ายกำกับการปฏิบัติงาน
3. **วงเงินงบประมาณที่ได้รับจัดสรร** 6,000,000.00 บาท (หกล้านบาทถ้วน)
4. **วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่** 29 เม.ย. 2568
   เป็นเงิน 5,995,119.50 บาท (ห้าล้านเก้าแสนเก้าหมื่นห้าพันหนึ่งร้อยสิบเก้าบาทห้าสิบสตางค์)
5. **ค่าตอบแทนบุคลากร** 5,205,673.00 บาท
   5.1 ประเภทที่ปรึกษา กลุ่มวิชาชีพเฉพาะ (กลุ่มวิจัย)
   5.2 คุณสมบัติที่ปรึกษา

5.2.1 ผู้จัดการโครงการ (Project Manager)	ไม่ต่ำกว่าวุฒิปริญญาโท	มีประสบการณ์ในการทำงานไม่น้อยกว่า 10 ปี และ มีประสบการณ์ในการบริหารงานโครงการ (Project Manager) ไม่น้อยกว่า 5 ปี และ มีประสบการณ์ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่เกี่ยวข้อง ไม่น้อยกว่า 3 ปี
5.2.2 ผู้เชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล	ไม่ต่ำกว่าวุฒิปริญญาโท (ด้านกฎหมาย)	มีประสบการณ์ในการทำงานไม่น้อยกว่า 5 ปี และ มีประสบการณ์ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล ไม่น้อยกว่า 3 ปี
5.2.3 ผู้ช่วยผู้เชี่ยวชาญด้านกฎหมาย	ไม่ต่ำกว่าวุฒิปริญญาโท (ด้านกฎหมาย)	มีประสบการณ์ในการทำงานไม่น้อยกว่า 5 ปี และ มีประสบการณ์ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่เกี่ยวข้อง ไม่น้อยกว่า 3 ปี
5.2.4 เจ้าหน้าที่สนับสนุน	ไม่ต่ำกว่าวุฒิปริญญาตรี	มีประสบการณ์ในการทำงานไม่น้อยกว่า 5 ปี และ มีประสบการณ์ด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือกฎหมายอื่นที่เกี่ยวข้อง ไม่น้อยกว่า 3 ปี

   5.3 จำนวนที่ปรึกษา

5.3.1 ผู้จัดการโครงการ	ไม่น้อยกว่า 1 คน
5.3.2 ผู้เชี่ยวชาญด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคล	ไม่น้อยกว่า 1 คน
5.3.3 ผู้ช่วยผู้เชี่ยวชาญด้านกฎหมาย	ไม่น้อยกว่า 2 คน
5.3.4 เจ้าหน้าที่สนับสนุน	ไม่น้อยกว่า 2 คน

6. **ค่าวัสดุอุปกรณ์** 20,000.00 บาท
7. **ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี)** -
8. **ค่าใช้จ่ายอื่นๆ** 769,446.50 บาท
9. **รายชื่อผู้รับผิดชอบกำหนดราคากลาง**
   9.1 นางธีรวรรณ กตัญญุตานนท์ ผู้ช่วยผู้บริหารฝ่ายกฎหมายและนิติกรรม
   9.2 นายอนุรักษ์ ชูศักดิ์ ผู้บริหารส่วนกำกับการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ / ฝ่ายกำกับการปฏิบัติงาน
   9.3 นางสาวภามาส จินาพันธ์ ผู้ช่วยผู้บริหารส่วนจัดซื้อทั่วไป 1 / ฝ่ายจัดซื้อและธุรการ
10. **ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง)**
    10.1 ตามหนังสือคณะกรรมการวินิจฉัยปัญหาการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ด่วนที่สุด ที่ กค (กวจ) 0405.3/ว 1203 ลงวันที่ 27 กันยายน 2565
    10.2 ค่าใช้จ่ายตรง ใช้ราคาที่ได้มาจากการสืบราคาจากท้องตลาด จำนวน 3 ราย
       10.2.1 บริษัท ติลลิกีแอนด์กิบบินส์ อินเตอร์เนชั่นแนล จำกัด
       10.2.2 บริษัท ราจา แอนด์ ทานน์ (ประเทศไทย) จำกัด
       10.2.3 บริษัท แชนด์เล่อร์ โมริ ฮะมะดะ จำกัด

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างที่ปรึกษาตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและส่งเสริมการดำเนินงานขององค์กรให้สอดคล้องกับข้อกำหนดด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPC Regulator Checklist)

ผู้เสนอราคาต้องเสนอการให้บริการการจ้างที่ปรึกษาตรวจสอบการปฏิบัติตามกฎหมายและส่งเสริมการดำเนินงานด้านการคุ้มครองข้อมูลส่วนบุคคลตามขอบเขตงานที่กำหนด เป็นระยะเวลา 3 ปี ดังนี้

1. จัดทำแผนงานโครงการ (Project Plan) พร้อมระยะเวลาดำเนินงานของโครงการ รวมทั้งแผนการสื่อสารสร้างความเข้าใจการดำเนินโครงการให้กับบุคลากรภายในธนาคาร (Project Communication Plan) แบ่งเป็นแผนระยะยาว 3 ปี และแผนแต่ละปีตามขอบเขตงาน

2. ตรวจประเมินตามแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลทั้ง 10 ด้านที่เป็นปัจจุบันของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ประกอบด้วย

(1) ด้านที่ 1 องค์กรและการกำกับดูแล (Organizational and Oversight)

บทบาทของผู้นำองค์กรที่เข้มแข็งและการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลที่ดีถือเป็นพื้นฐานที่สำคัญขององค์กรในการดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ ซึ่งรวมถึงการสร้างความมั่นใจว่าพนักงานขององค์กรมีหน้าที่และความรับผิดชอบที่ชัดเจนในการปฏิบัติงานทางด้านการคุ้มครองข้อมูลส่วนบุคคลทั้งในระดับกลยุทธ์และในระดับปฏิบัติการ ทั้งนี้ บางองค์กรได้ถูกกฎหมายกำหนดให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) แต่งานทางด้านการคุ้มครองข้อมูลส่วนบุคคลก็ไม่ควรเป็นภาระของ DPO เพียงคนเดียว แท้จริงแล้วงานดังกล่าวควรถูกแบ่งให้พนักงานที่เกี่ยวข้องทุกคนภายใต้การจัดสรรทรัพยากรที่เพียงพอต่อการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม โดยเริ่มต้นจากผู้บริหารระดับสูงขององค์กร

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. กำหนดโครงสร้างองค์กรให้ชัดเจน
2. แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือบุคคลที่รับผิดชอบงานคุ้มครองข้อมูลส่วนบุคคลขององค์กร
3. มีการรายงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม
4. กำหนดบทบาทหน้าที่ในการปฏิบัติงานคุ้มครองข้อมูลส่วนบุคคล
5. จัดให้มีคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล
6. จัดประชุมคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคล

(2) ด้านที่ 2 นโยบายและแนวปฏิบัติ (Policies and Procedures)

การดำเนินการในเรื่องการคุ้มครองข้อมูลส่วนบุคคลขององค์กรจะต้องมีการจัดทำให้มีแนวทางที่ชัดเจนผ่านการจัดทำนโยบายที่ผู้บริหารขององค์กร จะต้องมีการประชุม และหารือร่วมกันในการให้ความเห็นชอบกับนโยบายในการคุ้มครองข้อมูลส่วนบุคคลขององค์กร โดยนโยบายต้องมีความชัดเจนและสอดคล้องกับหลักการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และจะต้องมีการสื่อสารนโยบายและแนวทางในการคุ้มครองข้อมูลส่วนบุคคลให้พนักงานในองค์กรได้ทราบ เพื่อให้เกิดความรู้ความเข้าใจ ทั้งนี้องค์กรควรจัดทำแนวปฏิบัติงานเพื่อให้พนักงานเข้าใจในการปฏิบัติงานให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการทำงานของตนซึ่งอาจมีความแตกต่างกันไปในแต่ละฝ่ายงาน นโยบายและแนวปฏิบัติที่ดีจะช่วยให้การทำงานของพนักงานเป็นไปอย่างถูกต้อง ไม่เกิดข้อผิดพลาด สามารถปฏิบัติงานตามขั้นตอนของตนให้ถูกต้องตามหลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

<u>สิ่งที่ต้องดำเนินการตรวจประเมิน</u>

1. การกำหนดทิศทางและการสนับสนุนการคุ้มครองข้อมูลส่วนบุคคลสำหรับการปฏิบัติงานขององค์กร
2. การทบทวนและอนุมัตินโยบายการคุ้มครองข้อมูลส่วนบุคคลขององค์กร
3. การสร้างความตระหนักรู้ให้แก่พนักงานเรื่องการปฏิบัติงานให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
4. การกำหนดค่าเริ่มต้นสำหรับการทำงาน หรือ การออกแบบผลิตภัณฑ์ขององค์กรเพื่อคุ้มครองข้อมูลส่วนบุคคล (Data protection by design and by default)

(3) ด้านที่ 3 การอบรมและการสร้างความตระหนักรู้ (Training and Awareness)

องค์กรต้องจัดฝึกอบรมแก่พนักงานในองค์กรเพื่อสร้างความรู้ ความเข้าใจในการปฏิบัติหน้าที่ตามความรับผิดชอบของพนักงานให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างความมั่นใจให้แก่พนักงานในองค์กรในการทำงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ซึ่งการจัดการอบรมจะต้องดำเนินการให้มีความเหมาะสมทั้งในส่วนของเนื้อหาการอบรม ผู้ทำการอบรมที่มีคุณสมบัติเหมาะสม รวมถึงกำหนดหน้าที่และความรับผิดชอบที่เกี่ยวข้องซึ่งจะเป็นส่วนสำคัญที่ทำให้มีการปฏิบัติงานตามนโยบายและแนวปฏิบัติที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยองค์กรที่พนักงานได้รับการอบรมตามเงื่อนไขที่กำหนดจะช่วยสร้างความโดดเด่นให้แก่องค์กร การอบรมอาจมีการดำเนินการโดยหน่วยงานภายนอกที่ทำการอบรมโดยเฉพาะและได้รับการรับรองมาตรฐานของการอบรมจากหน่วยงานผู้กำกับดูแล ทั้งนี้ จะต้องจัดให้มีการติดตามและประเมินผลที่ได้จากการอบรมและสร้างความตระหนักรู้ที่ได้จากการอบรมให้แก่พนักงาน

ในเรื่องของการปฏิบัติงานในหน้าที่ตามความรับผิดชอบให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. หลักสูตรการอบรมแก่พนักงานขององค์กร เพื่อสร้างความตระหนักในเรื่องการปฏิบัติงานให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2. หลักสูตรการฝึกอบรมเพื่อสร้างปูพื้นฐาน และทบทวนในเรื่องการปฏิบัติงานให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
3. หลักสูตรการอบรมสำหรับพนักงานผู้มีหน้าที่ที่เกี่ยวกับการปฏิบัติงานให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยเฉพาะในแต่ละตำแหน่งหรือหน้าที่
4. การติดตามและประเมินผลภายหลังจากการฝึกอบรม
5. การสร้างความตระหนักในเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับการปฏิบัติงานให้กับพนักงานในองค์กร

(4) ด้านที่ 4 สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual Rights)

วัตถุประสงค์ที่สำคัญประการหนึ่งของกฎหมายคุ้มครองข้อมูลส่วนบุคคลคือการให้สิทธิแก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิในฐานะที่ตนเป็นเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดไว้ เช่น สิทธิในการเข้าถึงข้อมูล สิทธิขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้เป็นปัจจุบัน สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลโอนข้อมูลของตนไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น เป็นต้น ซึ่งองค์กรผู้ควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะต้องอำนวยความสะดวกให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิต่าง ๆ ตามที่กฎหมายกำหนดไว้

ดังนั้น องค์กรควรมีกระบวนการภายในขององค์กรในการอำนวยความสะดวกให้เจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิของตนตามที่กฎหมายกำหนด เริ่มตั้งแต่การแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลให้ได้ทราบสิทธิตามกฎหมายของตนนับตั้งแต่เวลาที่ได้เริ่มต้นเก็บข้อมูลส่วนบุคคล การจัดสรรทรัพยากรภายในองค์กรให้มีความเหมาะสม เช่น มีแบบฟอร์มการขอใช้สิทธิซึ่งอาจอยู่ในรูปแบบอิเล็กทรอนิกส์หรือกระดาษ มีพนักงานขององค์กรที่จะดำเนินการในเรื่องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะและมีจำนวนที่เพียงพอเพื่อไม่ให้เกิดความล่าช้าในการดำเนินงานให้เป็นไปตามความต้องการในการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การมีระบบบันทึกและติดตามผลของการดำเนินการให้เป็นไปตามความต้องการในการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล การดำเนินการต้องอยู่ภายใต้กรอบระยะเวลาที่เหมาะสม ไม่ล่าช้า การมีกระบวนการและแบบฟอร์มเฉพาะในการอำนวยความสะดวกให้แก่เจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของตนตามกฎหมาย เช่น การแก้ไขข้อมูลที่ไม่ถูกต้อง การลบ การระงับ การโอนย้าย

ข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ การประมวลผลโดยระบบอัตโนมัติ รวมถึงการร้องเรียนในกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องการร้องเรียนผู้ควบคุมข้อมูลส่วนบุคคลเนื่องจากพบปัญหาในการขอใช้สิทธิของตนตามกฎหมายการปฏิบัติตามกฎหมายในเรื่องการให้สิทธิต่างๆ แก่เจ้าของข้อมูลส่วนบุคคลนี้จะช่วยลดความเสี่ยงแก่องค์กร และช่วยให้องค์กรเกิดการปฏิบัติตามเงื่อนไขต่างๆ ตามที่กฎหมายกำหนด ซึ่งจะช่วยให้องค์กรมีความน่าเชื่อถือในการสร้างความเชื่อมั่นและความมั่นใจ และเป็นส่วนหนึ่งในการสร้างชื่อเสียงแก่องค์กรในเรื่องการจัดการข้อมูลส่วนบุคคล

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. การแจ้งสิทธิตามกฎหมายให้เจ้าของข้อมูลส่วนบุคคลได้ทราบ
2. ทรัพยากรที่องค์กรต้องจัดเตรียมเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิตามกฎหมายได้
3. การบันทึกการเข้าระบบและการติดตามการใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคล
4. การตอบสนองคำขอใช้สิทธิตามกฎหมายของเจ้าของข้อมูลส่วนบุคคลภายในระยะเวลาตามที่กฎหมายกำหนด หรือตามระยะเวลาสมควร
5. การติดตามและประเมินผลการปฏิบัติงานในเรื่องการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
6. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลแก้ไขข้อมูลที่ไม่ถูกต้อง
7. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคล
8. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการระงับการใช้ข้อมูลส่วนบุคคล
9. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการโอนย้ายข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์
10. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการประมวลผลโดยระบบอัตโนมัติ
11. การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลในการร้องเรียนต่อผู้ควบคุมข้อมูลส่วนบุคคล

(5) ด้านที่ 5 ความโปร่งใส (Transparency)

ความโปร่งใสถือเป็นหลักการที่สำคัญในการบริหารจัดการข้อมูลส่วนบุคคลขององค์กร โดยสามารถแสดงถึงความชัดเจน เปิดเผย และตรงไปตรงมาในการดำเนินการขององค์กร เพื่อเอื้อให้เจ้าของข้อมูลส่วนบุคคลมีอำนาจในการควบคุมการใช้หรือเปิดเผยข้อมูลส่วนบุคคลของตนโดยองค์กรอย่างเหมาะสมโดยเฉพาะอย่างยิ่งในกรณีที่มีการใช้วิธีการที่ซับซ้อนแบบการตัดสินใจโดยระบบอัตโนมัติและการทำโปรไฟล์ลิ่งหรือเมื่อเกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์ ความโปร่งใสในการเปิดเผยอย่างตรงไปตรงมาใน

การจัดการกับข้อมูลส่วนบุคคลจะช่วยทำให้องค์กรได้รับความไว้วางใจจากสาธารณชนและหน่วยงานกำกับดูแล

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. การจัดทำและการแจ้งประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)
2. การตัดสินใจโดยระบบอัตโนมัติและการทำโปรไฟล์ลิ่ง (Automated decision making and profiling)
3. ความตระหนักรู้ของพนักงาน
4. การทบทวนประกาศการคุ้มครองข้อมูลส่วนบุคคล (Privacy Notice)
5. เครื่องมือเพื่อช่วยสนับสนุนความโปร่งใส่และการควบคุม

(6) ด้านที่ 6 การบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมาย (ROPA & lawful Basis)

การจัดทำบันทึกรายการกิจกรรมประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมายเป็นเกณฑ์ที่กฎหมายกำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การจัดทำบันทึกรายการกิจกรรมทำให้องค์กรทราบว่ามีข้อมูลส่วนบุคคลอะไรบ้าง อยู่ที่ใด เก็บรักษาไว้อย่างไร และมีการใช้หรือเปิดเผยข้อมูลส่วนบุคคลอย่างไรบ้าง ทำให้องค์กรสามารถดำเนินการตามธรรมาภิบาลข้อมูลและปฏิบัติตามข้อกำหนดของกฎหมายได้อย่างครบถ้วน นอกจากนี้ในการประมวลผลข้อมูลส่วนบุคคลต้องเป็นไปตามกรอบที่กฎหมายกำหนด หากเป็นการเก็บรวบรวมและประมวลข้อมูลโดยใช้ข้อยกเว้นที่เป็นฐานทางกฎหมาย องค์กรต้องมีหลักในการพิจารณาอย่างเหมาะสมและมีหลักฐานเพื่อใช้ในการตรวจสอบได้

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. มีการจัดทำแผนผังข้อมูล (Data-mapping)
2. มีการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ให้มีรายละเอียดครบถ้วนตามที่กฎหมายกำหนด
3. มีการบันทึกฐานทางกฎหมาย
4. มีการทำตามเกณฑ์ที่กฎหมายกำหนดเรื่องการขอความยินยอม
5. มีระบบตรวจสอบความเสี่ยงในการประมวลผลข้อมูลผู้เยาว์
6. มีการประเมินการใช้ฐานเพื่อประโยชน์อันชอบธรรม

(7) ด้านที่ 7 ข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement: DSA) และข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)

ในการแบ่งปันข้อมูลผู้ควบคุมข้อมูลส่วนบุคคลควรจัดเตรียมให้มีข้อตกลงที่เป็นลายลักษณ์อักษรซึ่งจะทำให้คู่สัญญาเข้าใจและตระหนักถึงภาระหน้าที่ของแต่ละฝ่าย

วัตถุประสงค์ของการแบ่งปันข้อมูลและกระบวนการที่เกี่ยวข้อง ซึ่งจะช่วยทำให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลแสดงให้เห็นได้ว่ามีความเข้าใจและปฏิบัติตามหลักเกณฑ์ที่กฎหมายกำหนด ตลอดจนเข้าใจถึงภาระผูกพันความรับผิดชอบและความรับผิดต่างๆ

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. มีนโยบายและแนวปฏิบัติเกี่ยวกับการแบ่งปันข้อมูล (Data sharing policies and procedures)
2. มีการจัดทำข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement: DSA)
3. มีขั้นตอนการโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Restricted transfers)
4. มีขั้นตอนการดำเนินงาน/แนวปฏิบัติที่เหมาสะสมกับการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคล (Processors)
5. มีการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA)
6. มีการตรวจสอบผู้ประมวลผลข้อมูลส่วนบุคคล (Processor due diligence checks)
7. มีการตรวจสอบการปฏิบัติตามสัญญา (Processor compliance reviews)
8. การให้บริการโดยบุคคลที่สาม (Third party products and services)
9. องค์กรดำเนินการเชิงรุกเพื่อให้มั่นใจว่าการเปิดเผยหรือการแบ่งปันข้อมูลส่วนบุคคลกับองค์กรอื่นจะทำเพียงเท่าที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ที่จำกัด (Purpose limitation)

(8) ด้านที่ 8 การประเมินความเสี่ยงและผลกระทบความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Risk and Data Protection Impact Assessment)

การประเมินความเสี่ยงและผลกระทบความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (Risk and Data Protection Impact Assessment: Risks and DPIAs) คือ การประเมินความเสี่ยงและผลกระทบความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลเพื่อประเมินว่าการใช้หรือเปิดเผยข้อมูลส่วนบุคคลในกิจกรรมนั้นขององค์กรมีความเสี่ยงที่กระทบต่อสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคลในด้านใด และจะมีมาตรการใดที่ออกมาเพื่อลดผลกระทบนั้น โดยที่ DPIA เป็นเครื่องมือที่องค์กรใช้ในการบริหารจัดการความเสี่ยงด้านข้อมูลส่วนบุคคลให้เป็นระบบและสามารถใช้เป็นเอกสารหลักฐานสนับสนุนการปฏิบัติตามกฎหมาย ทั้งนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรองมีข้อกำหนดที่เกี่ยวข้องกับการทำ DPIA

สิ่งที่ต้องดำเนินการตรวจประเมิน

1. องค์กรจัดให้มีการระบุ การบันทึก และการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล โดยมีการกำหนดเป็นนโยบาย ขั้นตอน และมาตรการ
2. องค์กรต้องปกป้องข้อมูลโดยการออกแบบและกำหนดเป็นค่าเริ่มต้น (Data protection by design and by default) ในการจัดการความเสี่ยง และกำหนดนโยบายและขั้นตอนให้มีการจัดทำ DPIA ตามความเหมาะสมและตามปัจจัยความเสี่ยง
3. องค์กรมีการพิจารณาว่าจำเป็นต้องทำ DPIA หรือไม่ หรือจัดทำเป็นแนวปฏิบัติที่ดีว่าควรทำ DPIA และองค์กรมีนโยบายและขั้นตอน DPIA ที่ชัดเจน
4. เนื้อหาของ DPIA มีข้อมูลที่ครบถ้วนและจัดทำเป็นเอกสาร
5. องค์กรมีการดำเนินการที่เหมาะสมและมีประสิทธิภาพเพื่อลดหรือจัดการความเสี่ยงใด ๆ ที่ DPIA ระบุ และองค์กรมีกระบวนการตรวจสอบทบทวน DPIA ได้

(9) ด้านที่ 9 ด้านมาตรการรักษาความมั่นคงปลอดภัย (Data Security)

การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายถึง การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยจะต้องครอบคลุมการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม ทั้งนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัย ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ตามกฎหมายอื่นในการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามกฎหมายนั้น แต่มาตรการรักษาความมั่นคงปลอดภัยดังกล่าวของผู้ควบคุมข้อมูลส่วนบุคคลจะต้องเป็นไปตามมาตรฐานขั้นต่ำที่กำหนดในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล นอกจากนี้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 40 ยังได้กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

สิ่งที่ต้องดำเนินการตรวจประเมิน

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 (มีผลบังคับใช้ตั้งแต่วันที่ 21 มิถุนายน 2565) ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมองค์กรจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ประกอบด้วย

1. มาตรการเชิงองค์กรหรือด้านการบริหารจัดการ
2. มาตรการเชิงเทคนิค
3. มาตรการทางกายภาพ ซึ่งครอบคลุมถึง การป้องกัน การตรวจจับ การเยียวยาแก้ไขและการตอบสนอง

(10) ด้านที่ 10 ด้านการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Breach Response)

เพื่อกำหนดเป็นแนวทางในการจัดการกับเหตุการละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Management) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เมื่อองค์กรทราบถึงการละเมิดข้อมูลส่วนบุคคลต้องแจ้งเหตุดังกล่าวให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่เหตุละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุละเมิดนั้นให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมแนวทางการเยียวยาโดยไม่ชักช้า ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

สิ่งที่ต้องดำเนินการตรวจประเมิน

เมื่อองค์กรได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด ไม่ว่าโดยทางวาจา เป็นหนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือเป็นกรณีที่องค์กรทราบเองว่ามีหรือน่าจะมีเหตุการละเมิดข้อมูลส่วนบุคคล องค์กรต้องดำเนินการดังต่อไปนี้

การดำเนินการ	คำอธิบาย
1. Detection and Analysis	องค์กรมีขั้นตอนปฏิบัติเพื่อประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดข้อมูลส่วนบุคคลในเบื้องต้นโดยไม่ชักช้าเท่าที่จะสามารถกระทำได้ ว่ามีเหตุอันควรเชื่อได้ว่ามีการละเมิดข้อมูลส่วนบุคคลหรือไม่ เพื่อให้องค์กรสามารถยืนยันได้ว่ามีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้นหรือไม่

การดำเนินการ	คำอธิบาย
	รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
2. Containment, Eradication and Recovery	องค์กรมีขั้นตอนปฏิบัติในกรณีระหว่างการตรวจสอบตามข้อ 1. หากพบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้องค์กรดำเนินการด้วยตนเองหรือสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลหรือผู้เกี่ยวข้องดำเนินการป้องกัน ระงับ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูลส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันทีเท่าที่จะสามารถกระทำได้
3. Response	องค์กรมีขั้นตอนปฏิบัติเมื่อพิจารณาจากข้อเท็จจริงตามข้อ 1. แล้วเห็นว่า มีเหตุอันควรเชื่อว่ามีการละเมิดข้อมูลส่วนบุคคลจริง ให้องค์กรแจ้งเหตุการละเมิดแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล
4. Notify	องค์กรมีขั้นตอนปฏิบัติในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้องค์กรแจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย
5. Recover	ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการละเมิดข้อมูลส่วนบุคคลดังกล่าว
6. Post Incident Response	ป้องกันและลดผลกระทบจากการเกิดเหตุการละเมิดข้อมูลส่วนบุคคลในลักษณะเดียวกันในอนาคต ซึ่งรวมถึงการทบทวนมาตรการรักษาความมั่นคงปลอดภัยเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ อาจรวมถึง องค์กรมีการกำหนดตัวชี้วัดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการจัดการข้อมูลและองค์กรสามารถประเมินข้อมูลต่าง ๆ เพื่อทราบผลการประเมิน
7. External audit or compliance check and Internal audit program	องค์กรมีการตั้งผู้ตรวจสอบภายนอกเพื่อตรวจสอบและทบทวนการดำเนินการให้สอดคล้องกับกฎหมาย รวมถึง องค์กรมีขั้นตอนการตรวจสอบภายใน ขั้นตอนดังกล่าวครอบคลุมถึงด้านการคุ้มครองข้อมูลส่วนบุคคลและการจัดการข้อมูล และข้อมูลการจัดการที่เกี่ยวข้องทั้งหมดและผลลัพธ์ของกิจกรรมการติดตามและทบทวนถูกสื่อสารไปยังผู้มีส่วนได้ส่วนเสียภายในที่เกี่ยวข้อง รวมถึงผู้บริหารระดับสูงตามความเหมาะสม

ผู้ตรวจประเมินพร้อมให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ และแนวทางการปรับปรุง แก้ไข จัดทำเพื่อให้สอดคล้องตาม แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลทั้ง 10 ด้าน

3. ดำเนินการปรับปรุง แก้ไข และพัฒนาระบบกระบวนการทำงาน และเอกสารที่เกี่ยวข้องตามคำปรึกษา/ความเห็น/ข้อเสนอแนะ และแนวทางการปรับปรุง แก้ไข เพื่อให้สอดคล้องตาม แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลทั้ง 10 ด้าน พร้อมทั้งจัดทำรายงานสรุปผลการดำเนินงานในการปรับปรุง พร้อมทั้งระบุ ปัญหา อุปสรรค และข้อเสนอแนะ หรืออื่น ๆ เพิ่มเติม (ถ้ามี)

4. ตรวจสอบและติดตามการประเมินการจัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities หรือ ROPA) ของหน่วยงานภายในธนาคารทุกฝ่ายงานที่จัดเก็บไว้ในรูปแบบไฟล์ในระบบงาน พร้อมให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ และแนวทางการปรับปรุง แก้ไข หรืออื่น ๆ เพิ่มเติม (ถ้ามี) เพื่อให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง และกฎหมายอื่น ๆ ที่เกี่ยวข้อง พร้อมทั้งจัดทำรายงานสรุปผลการตรวจสอบและผลการประเมินการจัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities หรือ ROPA)

5. ตรวจสอบขั้นตอนการทำงานและระบบอิเล็กทรอนิกส์ที่เกี่ยวข้องกับกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง และกฎหมายอื่น ๆ ที่เกี่ยวข้อง รวมถึงที่มีการเปลี่ยนแปลง พร้อมทั้งจัดทำรายงานสรุปผลการตรวจสอบและผลการประเมินระบบงาน และข้อเสนอแนะ (ถ้ามี)

6. ตรวจประเมิน จัดทำ ทบทวน แก้ไข นโยบาย ระเบียบ คู่มือ/แนวทางปฏิบัติของธนาคารที่เกี่ยวกับการคุ้มครองและบริหารจัดการข้อมูลส่วนบุคคล รวมถึงสารจากประธานกรรมการ สารจากกรรมการผู้จัดการ หลักการความเป็นส่วนตัว ของ ธสน. และของ พนักงาน รายงานประจำปี การให้คำปรึกษา/ความเห็น/ข้อแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล แบบฟอร์มความยินยอม แบบฟอร์มอื่น ๆ สัญญา ตลอดจนเอกสารทางกฎหมายที่สำคัญ พร้อมให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ และแนวทางการปรับปรุง แก้ไข หรืออื่น ๆ เพิ่มเติม (ถ้ามี) เพื่อให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรองและกฎหมายอื่น ๆ ที่เกี่ยวข้อง (ทั้งภาษาไทยและภาษาอังกฤษ) และจัดทำรายงานสรุปผลการตรวจสอบ การให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ และปรับปรุง แก้ไข ให้สอดคล้องกับผลการตรวจสอบ

7. ตรวจประเมิน จัดทำ ทบทวน แก้ไข คู่มือการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) รวมทั้งตรวจการปฏิบัติหน้าที่ของ DPO ประกอบด้วย

7.1 สอบทานแนวทางการปฏิบัติงาน โครงสร้างและความเป็นอิสระ เครื่องมือ

7.2 สอบทานระบบงานที่เกี่ยวข้องกับการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) พร้อมให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ และแนวทางการปรับปรุง แก้ไข หรืออื่น ๆ เพิ่มเติม (ถ้ามี) เพื่อให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรองและกฎหมายอื่น ๆ ที่เกี่ยวข้อง

7.3 สอบทานรายงานผลการปฏิบัติงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำปี (DPO Annual Report)

7.4 จัดทำรายงานผลการดำเนินการของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO Annual Report) ประจำปี

7.5 จัดทำตัวชี้วัด (KPI) ประเมินประสิทธิภาพและการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคล ให้เป็นไปตามหลักเกณฑ์การประเมินความสอดคล้องด้านการคุ้มครองข้อมูลส่วนบุคคลของ สคส.

7.6 จัดทำรายงานสรุปผลการประเมิน การให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) พร้อมทั้งปรับปรุง แก้ไข ให้สอดคล้องกับผลการตรวจประเมิน

8. ตรวจประเมิน จัดทำ ทบทวน แก้ไข หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศ (Cross-Border Transfer of Personal Data) ของ ธสน. ให้สอดคล้องกับให้สอดคล้องกับมาตรา 28 มาตรา 29 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง และกฎหมายอื่น ๆ ที่เกี่ยวข้อง รวมทั้งเสนอให้ สคส. ตรวจสอบและรับรองเนื้อหาว่าเป็นไปตามหลักเกณฑ์ตามที่กฎหมายกำหนด พร้อมจัดทำรายงานสรุปผลการจัดทำ/ทบทวน การให้คำปรึกษา/ความเห็น/ข้อเสนอแนะ และปรับปรุง แก้ไข ให้สอดคล้องกับผลการตรวจสอบ

9. ให้คำปรึกษา ข้อเสนอแนะ ตอบข้อซักถาม แก้ไขปัญหาและอุปสรรค ที่เกิดขึ้นในช่วงการทำงานตามขอบเขตงาน เพื่อให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรองและกฎหมายอื่น ๆ ที่เกี่ยวข้อง พร้อมจัดทำรายงานสรุปการประชุม/การให้คำปรึกษา ข้อเสนอแนะ ตอบข้อซักถาม แก้ไขปัญหาและอุปสรรค พร้อมทั้งประชุมสรุปผู้บริหาร (Summary Report) ทุกครั้ง

10. จัดหลักสูตรอบรมให้ความรู้และความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล การปฏิบัติตามให้สอดคล้องกับความต้องการของกฎหมาย มาตรการทั่วไปที่จำเป็นและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่ธนาคารต้องนำมาปรับใช้งาน ตลอดจนฝึกปฏิบัติเพื่อพัฒนาทักษะที่จำเป็น ไม่น้อยกว่า 90 นาที พร้อมทั้งจัดทำสื่อการสอน โครงสร้างหลักสูตร เอกสารประกอบการสอน และเทปบันทึกการสอน (VDO) พร้อมข้อสอบจำนวน 50 ข้อ 3 ชุด โดยหัวข้ออย่างน้อยประกอบด้วย

- สาระสำคัญของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรอง สิ่งที่ธนาคารต้องปฏิบัติตามเพื่อให้สอดคล้องกับกฎหมายตามนโยบาย ระเบียบ คู่มือต่าง ๆ อันเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลภายในธนาคาร ตลอดจนโครงสร้างของหน่วยงานกำกับดูแลข้อมูลส่วนบุคคล บทบาท และหน้าที่ความรับผิดชอบ นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล การขอความยินยอมและการขอใช้สิทธิโดยเจ้าของข้อมูลส่วนบุคคล มาตรฐานและมาตรการสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

- การประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล การประเมินด้านความมั่นคงปลอดภัยสารสนเทศของระบบงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล การรับมือกับการละเมิดความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- พร้อมยกตัวอย่างกรณีศึกษา

ทั้งนี้ ภาพและเสียงทั้งหมดที่นำมาใช้จัดทำสื่อการเรียนรู้จะต้องไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญาของบุคคลอื่นใด และสื่อการเรียนรู้ที่จัดทำจะต้องถือเป็นกรรมสิทธิของธนาคาร โดยผู้เสนอราคาที่ได้รับการคัดเลือกจะต้องจัดทำหนังสือรับรองสิทธิโดยชอบธรรมในการใช้งานให้กับธนาคาร หากมีการฟ้องร้องเกี่ยวกับลิขสิทธิ์จากบุคคลอื่นใด ผู้เสนอราคาที่ได้รับการคัดเลือกต้องเป็นผู้รับผิดชอบทั้งหมด

ทั้งนี้ ในระหว่างดำเนินโครงการ ผู้เสนอราคาที่ได้รับการคัดเลือกจะต้องติดตามการบังคับใช้กฎหมายลำดับรอง นำเสนอความเห็น และดำเนินการปรับปรุง แก้ไข งานที่จะต้องส่งมอบให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล กฎหมายลำดับรอง และกฎหมายอื่น ๆ ที่เกี่ยวข้อง