รายงานการไปศึกษา / ดูงาน / ฝึกอบรม / ประชุมและสัมมนา

1. ชื่อ นางอัญชลี สกุล สุวจิตตานนท์
ตำแหน่ง รองอธิบดีกรมส่งเสริมการเกษตร ด้านบริหาร
ที่ทำงาน กรมส่งเสริมการเกษตร
ชื่อ นางสาวสุรางค์ศรี สกุล วาเพชร
ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ที่ทำงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมการเกษตร
ชื่อ นายรุ่งศิริ สกุล ประสงค์
ตำแหน่ง ผู้อำนวยการกลุ่มพัฒนาระบบสารสนเทศ
ที่ทำงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมการเกษตร
ไป (~~ดูงาน~~ / ฝึกอบรม / ~~ประชุม หรือสัมมนา~~) เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาครัฐ รุ่นที่ 5 (Government Data Protection Officer : GDPO#5) ในวันที่ 6, 14, 15, 21 และ 22 กันยายน 2566 ณ โรงแรมสยาม แอท สยาม ดีไซด์ โฮเต็ล กรุงเทพมหานคร
รวมระยะเวลา - ปี - เดือน 5 วัน
ผู้ดำเนินการจัด สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA) ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร.

2. ค่าใช้จ่ายที่ใช้ไประหว่างฝึกอบรม / ดูงาน / สัมมนา / ประชุม

ค่าเบี้ยเลี้ยง	-	บาท
ค่าที่พัก	-	บาท
ค่าพาหนะ	-	บาท
อื่น ๆ (ระบุ)	-	บาท

3. รายละเอียดการดูงาน ฝึกอบรม ประชุม สัมมนา ฯลฯ ที่สมควรรายงานให้มีรายละเอียดและเนื้อหามากที่สุดเท่าที่จะทำได้ โดยบรรยายสิ่งที่ได้สังเกต รู้ เห็น หรือได้รับถ่ายทอดมาให้ชัดเจน ถ้ามีเอกสารต่างหากให้แนบไปด้วย

<u>เนื้อหาวิชาการ</u>

การฝึกอบรมหลักสูตรเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลภาครัฐ รุ่นที่ 5 (Government Data Protection Officer : GDPO#5) เป็นหลักสูตรที่เกิดจากความร่วมมือของ 3 หน่วยงาน คือ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือ สคส. และสถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน) หรือ สคช. เพื่อร่วมกันสร้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ให้มีความรู้และทักษะอย่างเพียงพอเพื่อการปฏิบัติหน้าที่ ตามบทบาทที่กฎหมายกำหนด โดยเนื้อหาในหลักสูตรเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงการประยุกต์ใช้ความรู้เพื่อการปฏิบัติงานที่เกี่ยวข้อง โดยการศึกษาพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะมาตราต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติการเตรียมความพร้อมเพื่อรองรับ PDPA แนวปฏิบัติด้านความมั่นคงปลอดภัยและเทคโนโลยีสารสนเทศที่เกี่ยวข้อง หลักการด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล (Privacy and Data Protection Principles) บทบาทหน้าที่

และความรับผิดชอบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Roles and Responsibility) มาตรฐานต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล การบริหารจัดการและการประเมินความเสี่ยง รวมถึงเอกสารอื่นที่จำเป็นในการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1. กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่น ๆ ที่เกี่ยวข้อง

2. บทบาทหน้าที่และแนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

3. การจัดการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management)

3.1 แนวทางปฏิบัติด้านความมั่นคงปลอดภัย (Information Security in Practice)

3.2 มาตรฐานสากลที่เกี่ยวข้อง (Related International Standards)

4. การบริหารจัดการความเสี่ยง

โดยมีเนื้อหาสาระสำคัญในแต่ละหัวข้อ ดังนี้

1. กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่น ๆ ที่เกี่ยวข้อง

1.1 บทบาทหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

1.1.1 หน้าที่ตามกฎหมาย

1) ให้คำแนะนำ ไม่ได้ตัดสินใจแทนผู้ควบคุมข้อมูลส่วนบุคคล/ผู้ประมวลผลข้อมูลส่วนบุคคล

2) การตรวจสอบการดำเนินงานให้เป็นไปตาม พ.ร.บ.

3) ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)

4) การรักษาความลับ

1.1.2 การเข้าถึงข้อมูลและความเป็นอิสระ

1) การเข้าถึงข้อมูลส่วนบุคคล ควรออกแบบการคุ้มครองข้อมูลส่วนบุคคลในองค์กรให้แทรกซึมไปในกระบวนการทำงาน และควรได้รับการสนับสนุนเครื่องมือหรืออุปกรณ์ที่เพียงพอ และการให้ความสะดวกในการเข้าถึงข้อมูลส่วนบุคคล

2) ความเป็นอิสระของ DPO แบ่งเป็น ความเป็นอิสระโดยโครงสร้าง และความเป็นอิสระในความคิด

- DPO ไม่สามารถออกจากงาน หรือเลิกสัญญาจ้างได้ด้วยเหตุผลจากการปฏิบัติหน้าที่
- กรณีมีปัญหาในการปฏิบัติหน้าที่สามารถรายงานไปยังผู้บริหารสูงสุดโดยตรงได้
- การปฏิบัติหน้าที่หรือภารกิจอื่นต้องไม่เป็น Conflict

1.1.3 การร้องเรียน การใช้สิทธิเหตุละเมิด

1) เรื่องร้องเรียน

- DPO ควรออกแบบกระบวนการจัดการเรื่องร้องเรียน
- ในการจัดการเรื่องร้องเรียนต้องมีการกำหนดระยะเวลา
- การรับเรื่องร้องเรียนอันเกี่ยวข้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ต้องมีกระบวนการแจ้งมายัง DPO เพื่อให้ DPO สามารถจัดการได้โดยไม่ชักช้า
- การตอบเรื่องร้องเรียน DPO ควรเป็นผู้ตรวจสอบสุดท้าย

2) การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

- DPO ควรเป็นส่วนหนึ่งในการออกแบบกระบวนการใช้สิทธิ รวมถึงระยะเวลาในแต่ละช่วง
- ทดสอบและซักซ้อมในกระบวนการทำงานให้เข้าใจและปฏิบัติได้ทันกำหนดระยะเวลา 30 วัน
- การขอใช้สิทธิของเจ้าของข้อมูลต้องมีการยืนยันตัวตน เพื่อป้องกันการส่งข้อมูลผิดพลาดไปยังผู้ไม่มีสิทธิ
- หากมีการปฏิเสธการขอใช้สิทธิของเจ้าของข้อมูล ต้องมีการบันทึกการปฏิเสธคำขอตามมาตร 39 (7)

3) เหตุละเมิดและการแจ้งเหตุละเมิด

- กำหนดกระบวนการทำงานทั้งหมดและผู้รับผิดชอบในแต่ละกระบวนการ
- กำหนด Flow ให้พนักงานเห็นภาพเดียวกัน ทั้งองค์กร รวมถึงผู้บริหาร
- กำหนดระยะเวลาของแต่ละช่วงเวลาเป็นลำดับ มีการประเมินความเสี่ยงและผลกระทบ
- เงื่อนไขการประเมินและผลกระทบของเหตุละเมิดที่เกิดขึ้น อยู่ในความเสี่ยงระดับใด
- มีการซักซ้อมแผนฉุกเฉิน
- เมื่อเกิดเหตุวิกฤติขึ้นแล้วการให้บริการประชาชนจะไม่หยุดชะงัก หรือหยุดชะงักในเวลาที่น้อยที่สุด
- ข้อความมาตรฐานในการแจ้งเหตุละเมิด ต่อ สคส. และเจ้าของข้อมูลส่วนบุคคล
- กำหนดเงื่อนไขการเยียวยาเจ้าของข้อมูลส่วนบุคคลไว้เพื่อจะสามารถดำเนินการได้เร็วที่สุดเพื่อลดผลกระทบ
- การแถลงการณ์ต่อสาธารณะหากเหตุละเมิดส่งผลกระทบในวงกว้าง
- ทบทวนระบบหรือกระบวนการทำงานที่ก่อให้เกิดเหตุละเมิด เพื่อนำมาแก้ไขปรับปรุง

1.1.4 การบริหารจัดการของ DPO

1) การทบทวนปรับปรุงระบบภายใน

- ทบทวน : ระเบียบหรือกฎเกณฑ์ภายในให้เป็นปัจจุบัน
- สื่อสาร : ระเบียบหรือกฎเกณฑ์ภายในให้พนักงานในองค์กร
- อบรม : ให้พนักงานในองค์กรอย่างสม่ำเสมอ
- วัดผล : เกณฑ์ในการประเมินขึ้นอยู่กับมาตรฐานขององค์กร ทั้งนี้ ไม่ควรต่ำกว่า 75%

2) การติดตาม ตรวจสอบ รายงาน

- ตรวจสอบ : กำกับดูแลให้มีการดำเนินการตามนโยบายและมาตรการที่วางไว้
- ติดตาม : ติดตามหน่วยงานในองค์กรให้ดำเนินการตามคำแนะนำของ DPO ให้สอดคล้องกับนโยบายและมาตรการภายใน
- รายงาน : รายงานไปยังผู้บริหารสูงสุดขององค์กร

3) การสอบทานการดำเนินงานเกี่ยวกับการประมวลผล

- DPO ต้อง Monitor การประมวลผลภายในองค์กรให้ถูกต้องตามมาตรฐานทางกฎหมายเพื่อป้องกันข้อมูลส่วนบุคคลถูกละเมิด
- การตรวจสอบอาจมีทีม DPO ลงไปสอบทานหรือมอบหมายให้ Internal Audit

4) มาตรการรักษาความมั่นคงปลอดภัย

- การจำกัดสิทธิการเข้าถึง
- ระบบการป้องกันการรั่วไหลของข้อมูล

5) วงจรชีวิตของข้อมูล

- DPO ควรออกแบบระบบหรือกระบวนการทำงานให้มีการลบหรือทำลายข้อมูลส่วนบุคคล ไม่ว่าจะอยู่ในรูปแบบกระดาษ หรือข้อมูลอิเล็กทรอนิกส์ และควรตรวจสอบว่าระบบหรือกระบวนการนั้น ๆ ได้ถูกนำไปใช้จริง

6) ประเมินผลกระทบ

- ความจำเป็น : องค์กรต้องประเมินความจำเป็นว่า ต้องใช้ข้อมูลส่วนบุคคลนั้นหรือไม่
- ความเสี่ยงในการถูกละเมิด : ข้อมูลส่วนบุคคลที่เก็บจะส่งผลกระทบอย่างไรกับเจ้าของข้อมูลและองค์กรบ้าง
- ฐานตามกฎหมาย : ข้อมูลส่วนบุคคลที่จัดเก็บ ใช้ฐานตามกฎหมายใดในการจัดเก็บ
- ระยะเวลา : ควรมีการกำหนดระยะเวลาในการจัดเก็บ ลบ หรือ ทำลายข้อมูลส่วนบุคคล
- 7) การดำเนินการอื่น ๆ
- DPO ต้องกำกับดูแลให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการบันทึกการประมวลผลข้อมูลส่วนบุคคล โดยควรแยกเป็นแต่ละกิจกรรมให้ครบถ้วนและถูกต้อง

2. บทบาทหน้าที่และแนวปฏิบัติสำหรับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

2.1 ประกาศคณะกรรมการฯ เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 20 มิถุนายน 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.2 ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์และวิธีการในการจัดหาและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 20 มิถุนายน 2565 มีผลบังคับใช้เมื่อพ้นกำหนด 180 วันนับแต่วันประกาศฯ

2.3 ประกาศคณะกรรมการฯ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 20 มิถุนายน 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.4 ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์การพิจารณาออกคำสั่งลงโทษปรับทางปกครองของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 20 มิถุนายน 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.5 ระเบียบคณะกรรมการฯ ว่าด้วยการยื่น การไม่รับเรื่อง การยุติเรื่อง การพิจารณา และระยะเวลาในการพิจารณาคำร้องเรียน พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 1 กรกฎาคม 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.6 ประกาศคณะกรรมการฯ เรื่อง คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง และการดำเนินงานอื่นของคณะกรรมการผู้เชี่ยวชาญ พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 11 กรกฎาคม 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.7 ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 12 กันยายน 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.8 ประกาศคณะกรรมการฯ เรื่อง กำหนดแบบบัตรประจำตัวของพนักงานเจ้าหน้าที่ พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 12 กันยายน 2565 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

2.9 ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 15 ธันวาคม 2565 มีผลบังคับใช้ตั้งแต่วันประกาศฯ

2.10 ประกาศคณะกรรมการฯ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำคำสั่งของคณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2565 : ประกาศในราชกิจจานุเบกษา เมื่อ 21 มิถุนายน 2566 มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศฯ

3. การจัดการด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management)

3.1 แนวทางปฏิบัติด้านความมั่นคงปลอดภัย (Information Security in Practice)

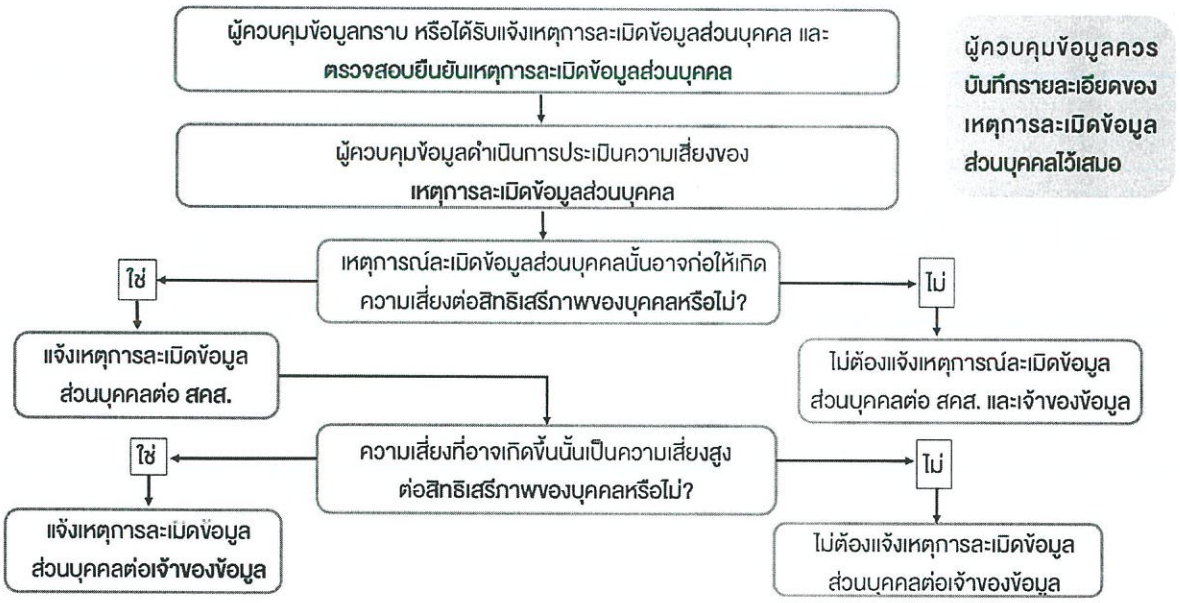
3.1.1 นิยาม “การละเมิดข้อมูลส่วนบุคคล”

- การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ
- อาจเกิดจากเจตนา ความจงใจ หรือความประมาทเลินเล่อข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ หรือเหตุอื่น ๆ
- การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์

3.1.2 ประเภทของกการละเมิด

- การละเมิดความลับของข้อมูล (Confidentiality Breach) : มีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจ หรือ โดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ
- การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach) : การเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน โดยปราศจากอำนาจ หรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ
- การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach) : ทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

3.1.3 ขั้นตอนการดำเนินการเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล



3.1.4 การประเมินความเสี่ยงของเหตุละเมิดข้อมูลส่วนบุคคล

3.1.4.1 ไม่มีความเสี่ยง

1) บันทึกเหตุละเมิดข้อมูลส่วนบุคคล

2) ส่งเอกสารหรือหลักฐานซึ่งแสดงการได้รับยกเว้นการแจ้ง รวมถึงมาตรฐานรักษาความมั่นคงปลอดภัยของข้อมูลให้ สคส.

3.1.4.2 มีความเสี่ยง

1) บันทึกเหตุละเมิดข้อมูลส่วนบุคคล

2) แจ้ง สคส. ภายใน 72 ชั่วโมง นับจากที่ทราบเหตุ

3.1.4.3 มีความเสี่ยงสูง

1) บันทึกเหตุละเมิดข้อมูลส่วนบุคคล

2) แจ้ง สคส. ภายใน 72 ชั่วโมง นับจากที่ทราบเหตุ

3) แจ้งเจ้าของข้อมูลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้า

3.2 มาตรฐานสากลที่เกี่ยวข้อง (Related International Standards)

3.2.1 มาตรฐานสากลด้านการคุ้มครองข้อมูลส่วนบุคคล (ISO/IEC 27701, 27001, 27002 and 29100)

1) ISO/IEC 27701 (2019) Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

2) ISO/ IEC 27001 (2013) Information technology – Security techniques – Information security management systems - Requirements

3) ISO/IEC 27002 (2013) Information Technology – Security techniques – Code of practice for information security controls

4) ISO/IEC 29100 (2011) Information technology – Security Techniques – Privacy framework

4. การบริหารจัดการความเสี่ยง

4.1 กรอบแนวความคิด

4.1.1 DPIA เป็นเครื่องมือสำหรับผู้ควบคุมข้อมูลส่วนบุคคลในการดำเนินการจัดทำระบบการประมวลผลที่ทำให้สามารถบรรลุวัตถุประสงค์ของกฎหมาย และอาจจำเป็นสำหรับกระบวนการประมวลผลข้อมูลบางประเภท

4.1.2 สามารถปรับแต่งตามขนาดขององค์กรได้และสามารถทำได้หลายรูปแบบ

4.1.3 กฎหมายของยุโรปกำหนดให้ต้องดำเนินการและกำหนดเงื่อนไขเบื้องต้นบางประการสำหรับการทำ DPIA

4.1.4 ผู้ควบคุมข้อมูลส่วนบุคคลควรพิจารณาการทำ DPIA ในฐานะเป็นกระบวนการที่เป็นประโยชน์และให้ผลเชิงบวก ที่จะช่วยทำให้การคุ้มครองข้อมูลส่วนบุคคลบรรลุเป้าหมายตามกฎหมาย

4.2 ตาม GDPR ข้อ 35

4.2.1 ในกรณีที่การประมวลผลข้อมูลส่วนบุคคลรายการใดมีการใช้เทคโนโลยีใหม่เป็นการเฉพาะและเมื่อคำนึงถึงลักษณะขอบเขตบริบทของการประมวลผลแล้วน่าจะมีผลกระทบอย่างสูง ต่อสิทธิและเสรีภาพของบุคคลธรรมดา ก่อนทำการประมวลผลผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการประเมินผลกระทบของกระบวนการในการประมวลผลเพื่อคุ้มครองข้อมูลส่วนบุคคล คำว่า “มีผลกระทบสูงต่อสิทธิและเสรีภาพของบุคคล” หมายถึง

- สิทธิเกี่ยวกับการคุ้มครองข้อมูลและความเป็นส่วนตัว
- สิทธิขั้นพื้นฐานอื่น ๆ เช่น การพูด การแสดงความคิดเห็น การเคลื่อนย้าย การไม่เลือกปฏิบัติ ความมีเสรีภาพ มโนธรรม และศาสนา เป็นต้น
- การพิจารณาไม่ทำ DPIA ไม่เป็นการจำกัดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในการใช้มาตรการในการจัดการความเสี่ยงอันเหมาะสมกับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- ในการประมวลผลกิจกรรมใด ผู้ควบคุมฯ ควรประเมินความเสี่ยงอย่างสม่ำเสมอเพื่อระบุว่าเมื่อใดที่การประมวลผลอาจก่อนให้เกิดผลต่อความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล

4.2.2 การประมวลผลครั้งเดียวอาจให้ผลต่อการประมวลผลหลาย ๆ กระบวนการที่ส่งผลกระทบต่อความเสี่ยงสูงที่คล้าย ๆ กัน

4.2.3 ควรขอคำแนะนำจาก DPO ในการประเมินผลกระทบดังกล่าว

4.3 PDPA มาตรา 37

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

4.4 DPIA

4.4.1 กฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

4.4.2 ผู้ควบคุมข้อมูลส่วนบุคคลสามารถกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคล ช่วยเหลือ และให้ข้อมูลที่จำเป็นได้

วิธีการนำเสนอเนื้อหาของวิทยากร

ผู้บรรยายนำเสนอผ่านโปรแกรม Power Point และมี Work Shop ให้ทำทุกวัน โดยจัดฝึกอบรมในรูปแบบ On-Site ในวันที่ 6, 14 – 15, 21 และ 22 กันยายน 2566 ณ โรงแรมสยาม แอท สยาม ดีไซด์ โฮเต็ล กรุงเทพมหานคร

4. ประโยชน์ที่ได้รับ

4.1 ประโยชน์ที่ได้รับต่อตนเอง

1) มีความรู้ความเข้าใจต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) ทราบถึงบทบาท หน้าที่ และความรับผิดชอบของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

3) ทราบแนวทางปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และฝึกปฏิบัติ

4.2 ประโยชน์ที่ได้รับต่อหน่วยงาน

1) นำความรู้มาปรับใช้กับการพัฒนาระบบแอปพลิเคชันของกรมส่งเสริมการเกษตร เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2) สนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ให้ปฏิบัติงานได้ตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด

3) ลดความเสี่ยงต่อการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล

5. ปัญหา อุปสรรค และข้อเสนอแนะ

5.1 ปัญหาอุปสรรค

1) สถานที่จัดอบรมอยู่ในย่านที่มีการจราจรหนาแน่น ทำให้การเดินทางไม่สะดวก

2) เนื้อหาเป็นข้อกฎหมายที่ต้องใช้ความจำและความเข้าใจในรายละเอียดของแต่ละมาตรา ซึ่งส่งผลให้การตีความทำได้ยากเมื่อเจอสถานการณ์จริง

5.2 ข้อเสนอแนะ

1) ควรจัดฝึกอบรมให้มีระยะเวลามากขึ้น จะทำให้ผู้เข้าอบรมสามารถเข้าใจเนื้อหาและสามารถซักถามข้อสงสัยได้อย่างรวดเร็ว และมีประสิทธิภาพมากกว่า

6. ท่านจะนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานอย่างไรบ้าง (โปรดระบุเป็นรายบุคคล)

6.1 นางอัญชลี สุวจิตตานนท์ ตำแหน่ง รองอธิบดีกรมส่งเสริมการเกษตร ด้านบริหาร

นำความรู้มาใช้ในการบริหารจัดการ กำกับ ดูแล การใช้ รวบรวม และเปิดเผยข้อมูลส่วนบุคคลที่กรมส่งเสริมการเกษตรดำเนินการ และใช้ในการปฏิบัติงานในหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ของกรมส่งเสริมการเกษตร เพื่อลดความเสี่ยงต่อการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล

6.2 นางสาวสุรางค์ศรี วาเพชร ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

นำความรู้มาใช้ในการกำกับ ดูแล การใช้ รวบรวม และเปิดเผยข้อมูลส่วนบุคคลที่กรมส่งเสริมการเกษตรดำเนินการ รวมทั้งขับเคลื่อนให้เจ้าหน้าที่ของกรมส่งเสริมการเกษตรมีความรู้ในเรื่องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อลดความเสี่ยงต่อการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล

6.3 นายรุ่งศิริ ประสงค์ ตำแหน่ง ผู้อำนวยการกลุ่มพัฒนาระบบสารสนเทศ

นำความรู้มาปรับใช้กับการพัฒนาระบบแอปพลิเคชันของกรมส่งเสริมการเกษตร เพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ความรู้กับเจ้าหน้าที่ของกรมส่งเสริมการเกษตรให้ทราบถึงวิธีการ แนวทางปฏิบัติในการรักษาไว้ซึ่ง ความลับ ความถูกต้อง และความพร้อมใช้งาน รวมถึงสนับสนุนการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อลดความเสี่ยงต่อการละเมิดสิทธิของเจ้าของข้อมูลส่วนบุคคล

(นายรุ่งศิริ ประสงค์)
ผู้รายงาน

7. ความเห็นของผู้บังคับบัญชา (ระดับผู้อำนวยการกอง/สำนัก/เกษตรจังหวัด หรือเทียบเท่า ขึ้นไป)

.....

.....

.....

.....

.....

(นางสาวสุรางค์ศรี วาเพชร)
ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

หมายเหตุ กรณีที่ไปประชุม / สัมมนา / ฝึกอบรม / ดูงาน เป็นหมู่คณะ โปรดระบุชื่อผู้ร่วมเดินทางและเสนอรายงานเพียงชุดเดียว