สิ่งที่ส่งมาด้วย 1

สภากาชาดไทย
THAI RED CROSS SOCIETY

ประกาศสภากาชาดไทย

เรื่อง แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล สภากาชาดไทย พ.ศ. 2564

เพื่อให้การปฏิบัติเป็นไปอย่างถูกต้องรัดกุมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎระเบียบของสภากาชาดไทย อาศัยอำนาจตามความในข้อ 6 (2) แห่งระเบียบสภากาชาดไทยว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564 และเพื่อให้หน่วยงานสามารถใช้เป็นกรอบแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลได้โดยเพิ่มเติมให้เหมาะสมตามภารกิจและความจำเป็น จึงกำหนดกรอบแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลดังนี้

1. การแต่งตั้งและแบ่งแยกหน้าที่บุคลากรในหน่วยงาน

ให้หัวหน้าหน่วยงานในฐานะที่ทำหน้าที่เป็นเจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลประจำหน่วยงาน (Data Owners) กำหนดอำนาจและหน้าที่ของบุคลากร โดยอาจระบุเป็นตัวบุคคลหรือหน่วยงานที่เกี่ยวข้อง เพื่อการปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

1.1 เจ้าหน้าที่เก็บรวบรวมข้อมูล

1.2 เจ้าหน้าที่เก็บรักษาข้อมูลทั้งในรูปแบบเอกสาร หรืออิเล็กทรอนิกส์ และเจ้าหน้าที่ทำลายเอกสารและลบข้อมูล

1.3 เจ้าหน้าที่หรือหน่วยงานที่รับเอกสารการจากเจ้าของข้อมูล หรือตัวแทนที่ต้องการใช้สิทธิ์ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

1.4 เจ้าหน้าที่เปิดเผย หรือส่งข้อมูลให้กับบุคคลภายนอก

1.5 เจ้าหน้าที่รับเรื่องร้องเรียน และนำส่งเรื่องร้องเรียน

1.6 เจ้าหน้าที่ตรวจสอบการละเมิด หรือการรั่วไหลของข้อมูล

1.7 เจ้าหน้าที่ที่มีอำนาจอนุมัติ

กรณีหน่วยงานที่มีอัตรากำลังไม่เพียงพอ หัวหน้าหน่วยงานสามารถพิจารณาให้บุคลากรรับผิดชอบได้มากกว่า 1 หน้าที่ และสำหรับกรณีที่จะไม่ปฏิบัติตามระเบียบนั้นจะต้องดำเนินการตามความในข้อ 5 แห่งระเบียบว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2564 อย่างเคร่งครัด

2. วิธีการเก็บรวบรวมข้อมูล และการเปิดเผยข้อมูลส่วนบุคคล

2.1 วิธีการเก็บรวบรวมข้อมูลส่วนบุคคล

หน่วยงานต่างๆ ของสภากาชาดไทย สามารถดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลรวมทั้งเอกสารอ้างอิง เช่น บัตรประจำตัวประชาชน ของผู้รับบริการเท่าที่จำเป็นต่อการประมวลผลและการดำเนินงานด้านต่างๆ ตามภารกิจหลักและวัตถุประสงค์ในการให้บริการของหน่วยงาน ที่ระบุไว้ใน**หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคลและแบบหนังสือยินยอม** โดยใช้แบบฟอร์มที่หน่วยงานกำหนดและได้รับอนุมัติแล้วเท่านั้น ทั้งนี้แบบฟอร์มที่ใช้มีรูปแบบเป็น

ก. แบบเอกสาร

ข. แบบฟอร์มในระบบอิเล็กทรอนิกส์

กรณีที่หน่วยงานจำเป็นต้องเก็บ **ข้อมูลอ่อนไหว** หน่วยงานจะต้องขอหนังสือยินยอมจากเจ้าของข้อมูล เว้นแต่ได้รับยกเว้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เช่น เพื่อการรักษาพยาบาล และอื่นๆ หรือได้รับคำวินิจฉัยยกเว้นจาก สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีที่หน่วยงานต้องการออกแบบฟอร์มหรือเอกสารแบบใหม่ที่ไม่ได้เป็นไปตามเอกสารตามที่ระบุไว้ในระเบียบสภากาชาดไทยว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ 2564 แบบฟอร์มหรือเอกสารนั้นจะต้องรับการพิจารณาและทบทวนโดยคณะกรรมการที่เกี่ยวข้องก่อนนำไปใช้

2.2 การใช้และการเปิดเผยข้อมูลส่วนบุคคล

การใช้และเปิดเผยข้อมูลส่วนบุคคลมี 2 ลักษณะ

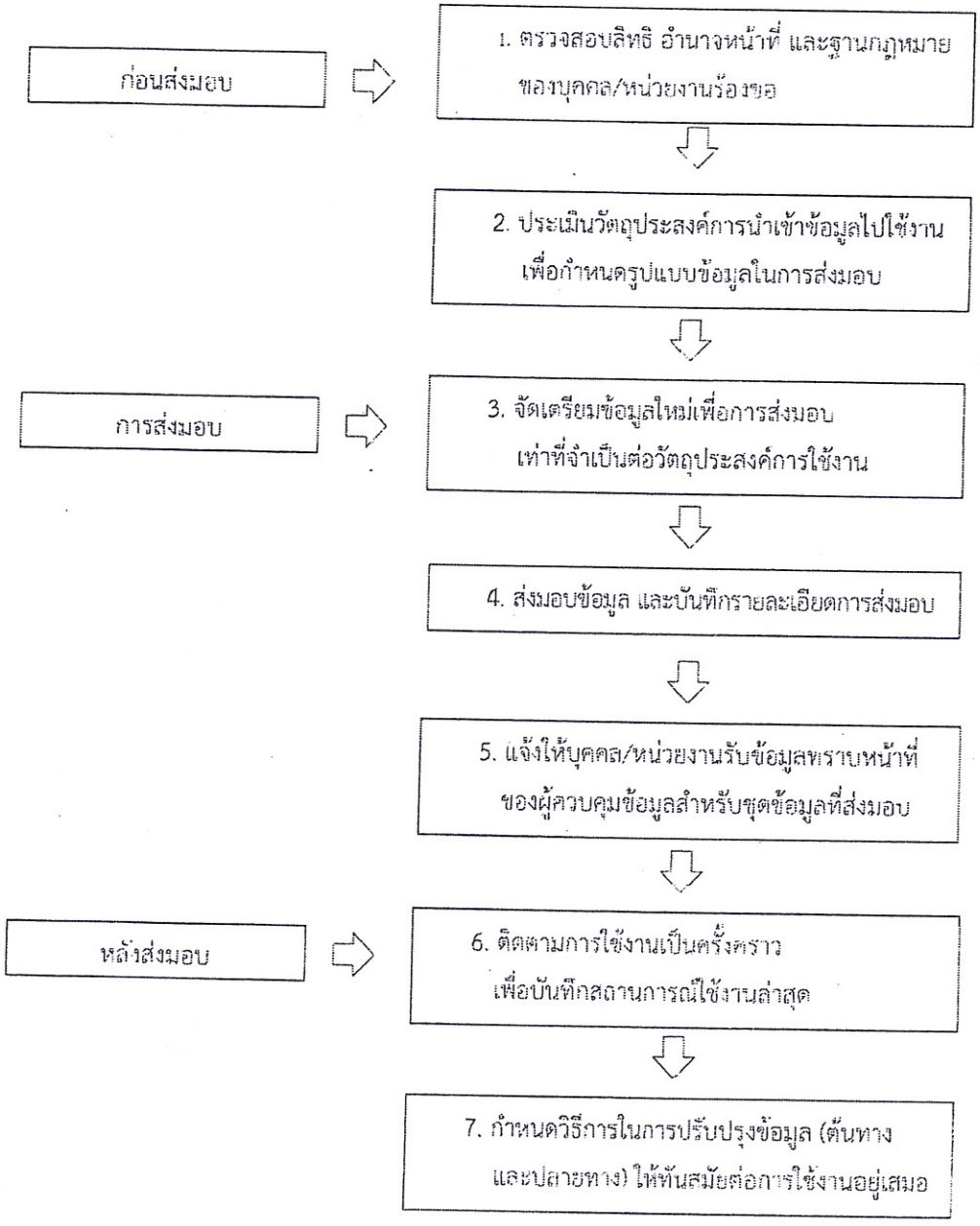
2.2.1 **ใช้และเปิดเผยข้อมูลภายในหน่วยงาน** จะต้องจัดทำโดยเจ้าหน้าที่ที่ได้รับการแต่งตั้ง และเป็นการใช้ตามวัตถุประสงค์ของการเก็บรวบรวม จัดเก็บ ข้อมูลที่ได้แจ้งและ/หรือขอความยินยอมไว้ตามที่หน่วยงานระบุไว้ในหนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคลและแบบหนังสือยินยอม เท่านั้น ผู้บริหารหรือผู้ที่ได้รับมอบหมายของหน่วยงานต้องกำกับดูแลบุคลากรให้ปฏิบัติตามอย่างเคร่งครัด ในกรณีที่หน่วยงานใช้ข้อมูลเพื่อดำเนินธุรกรรมนอกเหนือจากที่ระบุไว้ หน่วยงานจะต้องให้เจ้าของข้อมูลลงลายมือชื่อใน**หนังสือยินยอม** ที่ระบุธุรกรรมที่จะมีเพิ่มเติม

2.2.2 **การส่ง การโอน หรือการเปิดเผยข้อมูลต่อบุคคลภายนอกหรือหน่วยงานภายนอก** รวมทั้งการเบิกใช้เอกสาร จะต้องจัดทำโดยเจ้าหน้าที่ที่ได้รับมอบหมาย และได้รับอนุมัติจากผู้อนุมัติจากหัวหน้าหน่วยงานก่อนการส่ง โอน หรือเปิดเผยต่อหน่วยงานหรือบุคคลภายนอก

หน่วยงานหรือบุคคลภายนอก ได้แก่

- **หน่วยงานราชการตาม พ.ร.บ. ระเบียบบริหารราชการแผ่นดิน พ.ศ. 2534** ที่มีอำนาจหน้าที่ตามกฎหมาย เช่น กรมสรรพากร (มีอำนาจหน้าที่เกี่ยวกับด้านภาษีอากร) ศาล (มีอำนาจหน้าที่เฉพาะที่เกี่ยวข้องกับคดีความ) พนักงานสอบสวน (มีอำนาจหน้าที่เฉพาะที่เกี่ยวกับคดีในความรับผิดชอบ) เป็นต้น
- **หน่วยงานราชการทั่วไป** ที่ไม่มีอำนาจหน้าที่ตามกฎหมายในเรื่องนั้นๆ
- **นิติบุคคลในประเทศ** ที่ไม่ต้องใช้สัญญาประมวลผลข้อมูล
- **นิติบุคคลต่างประเทศ** ซึ่งต้องมีกฎหมาย PDPA ทัดเทียมกับประเทศไทย
- **คู่สัญญา** ที่เป็นผู้ประมวลผลข้อมูล

ขั้นตอนการใช้และเปิดเผยข้อมูลส่วนบุคคล สรุปได้ดังนี้



2.3 การปฏิบัติต่อข้อมูลที่มีอยู่ก่อน พระราชบัญญัตินี้ใช้บังคับ

หน่วยงานเจ้าของข้อมูลส่วนบุคคลสามารถดำเนินการกับข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมไว้ก่อนพระราชบัญญัตินี้บังคับใช้ ให้หน่วยงานดำเนินการกับข้อมูลส่วนบุคคลนั้นต่อไปได้ตามปกติโดยไม่ต้องส่ง Consent ให้เซ็นยินยอมใหม่ โดยต้องเป็นไปตามวัตถุประสงค์เดิมเท่านั้น แต่ต้องกำหนดวิธีการยกเลิกความยินยอม และประชาสัมพันธ์แจ้งให้เจ้าของข้อมูลทราบ เพื่อให้เจ้าของข้อมูลที่ไม่ต้องการให้เก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าว สามารถแจ้งยกเลิกความยินยอมได้โดยง่าย ทั้งนี้ หน่วยงานต้องแจ้งเตือนสิทธิและผลกระทบจากการยกเลิกความยินยอมให้เจ้าของข้อมูลทราบก่อนยกเลิกความยินยอมนั้น

3. ระยะเวลาการเก็บข้อมูลส่วนบุคคล การลบ การทำลาย การทบทวน และการตรวจสอบการเก็บข้อมูลส่วนบุคคล

3.1 ระยะเวลาในการเก็บรักษา

หน่วยงานต้องกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคล ที่ชัดเจนและสอดคล้องกับวัตถุประสงค์การใช้ข้อมูล ในกรณีทั่วไป ระยะเวลาการจัดเก็บข้อมูลสูงสุดคือ 10 ปี เว้นแต่จะมีระเบียบหรือกฎหมายกำหนดไว้เป็นอย่างอื่นๆ เช่น เก็บจนกว่าคดีสิ้นสุด เป็นต้น

3.2 การลบหรือทำลายข้อมูลส่วนบุคคล

หน่วยงานต้องกำหนดวิธีการและขั้นตอน และบันทึกรายงานการลบและทำลายข้อมูลส่วนบุคคล เมื่อพ้นระยะเวลาจัดเก็บข้อมูลส่วนบุคคล หรือปฏิบัติตามระเบียบและวิธีปฏิบัติที่มีการประกาศใช้ในสภากาชาดไทย

การลบหรือทำลายข้อมูลตามระยะเวลาที่กำหนด หน่วยงานต้องจัดให้มีผู้ทำหน้าที่ตรวจสอบและรวบรวมรายการข้อมูลส่วนบุคคลที่ต้องดำเนินการลบหรือทำลาย เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา ทั้งในระบบอิเล็กทรอนิกส์ และในรูปแบบเอกสารต่างๆ โดยจัดทำรายการข้อมูลที่ต้องดำเนินการลบแจ้งต่อผู้บังคับบัญชา เพื่อขออนุมัติดำเนินการลบทำลายข้อมูล

กรณีข้อมูลส่วนบุคคลที่มีการใช้เพื่อดำเนินคดีตามกฎหมาย และหรือมีการบังคับคดี หน่วยงานให้ทำการเก็บข้อมูลเอกสาร และฐานข้อมูลดังกล่าวไว้เพื่อใช้ในการดำเนินคดี จนกว่าคดีจะถึงที่สุด จึงจะทำลายเอกสารที่เป็นข้อมูลส่วนบุคคลนั้นได้

4. การรักษาความมั่นคงปลอดภัย

หน่วยงานต้องดำเนินการจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและบุคคล (หรือนิติบุคคล) อื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เพื่อป้องกันการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหน้าที่หรือโดยมิชอบ

หน่วยงานต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสภากาชาดไทย (Information Security Policy) พ.ศ. 2561 หรือนโยบายอื่นๆ ที่มีการประกาศใช้ในสภากาชาดไทย เช่น

- เสริมสร้างความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่ผู้บริหารและบุคลากร
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อจำกัดการเข้าถึงข้อมูลส่วนบุคคลเฉพาะเจ้าหน้าที่ที่มีความจำเป็นต้องใช้ข้อมูลในการปฏิบัติงานตามหน้าที่ และจัดให้มีการบันทึกและทำสำรองข้อมูลการเข้าถึงหรือการเข้าใช้งานในระยะเวลาที่เหมาะสม และสามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ในบางกรณี อาจใช้การเข้ารหัสเพื่อรักษาความมั่นคงปลอดภัยในการส่งผ่านข้อมูล
- จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง
- กำหนดให้มีมาตรการรักษาความลับ และความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญหรือเป็นข้อมูลที่อาจกระทบต่อความสงบเรียบร้อย และศีลธรรมอันดีของประชาชน

5. วิธีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่มิใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

หน่วยงานจะต้องเก็บรวบรวมข้อมูลส่วนบุคคลจากผู้เป็นเจ้าของข้อมูลโดยตรง จะเก็บจากแหล่งอื่นไม่ได้ หากต้องการจัดเก็บข้อมูลจากแหล่งข้อมูลอื่นในบางกรณีสามารถทำได้ เช่น ประโยชน์ต่อชีวิตหรือสุขภาพ โดยหน่วยงานสามารถรวบรวมข้อมูลส่วนบุคคลของผู้รับบริการจากแหล่งอื่นๆ เช่น ที่อยู่ปัจจุบันของผู้รับบริการ (สำนักบริหารการทะเบียน กรมการปกครอง กระทรวงมหาดไทย) เป็นต้น รวมเข้ากับข้อมูลส่วนบุคคลที่เจ้าของข้อมูลให้ข้อมูลไว้ เพื่อทำให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลมีความครบถ้วนและถูกต้อง เป็นปัจจุบัน และช่วยให้หน่วยงานสามารถให้บริการตามภารกิจหลัก หรือเพื่อประโยชน์ต่อชีวิต หรือสุขภาพของเจ้าของข้อมูล และเพื่อประโยชน์สาธารณะ ได้ดียิ่งขึ้น รวมถึงข้อมูลที่ผ่านโซเชียลมีเดียแพลตฟอร์มตามที่ระบุไว้ หรือ เผยแพร่ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย พ.ศ. 2564

6. สิทธิของเจ้าของข้อมูล วิธีการใช้สิทธิของเจ้าของข้อมูล และการดำเนินการที่ต้องปฏิบัติตามหรือไม่ปฏิบัติตามการใช้สิทธิของเจ้าของข้อมูล

6.1 หลักเกณฑ์และวิธีการใช้สิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลมีสิทธิในการคัดค้าน การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเมื่อใดก็ได้ และมีสิทธิขอให้ผู้ควบคุมข้อมูล ดำเนินการลบ ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ หรือขอระงับการใช้ข้อมูลส่วนบุคคลได้

สิทธิของเจ้าของข้อมูลตามพระราชบัญญัตินี้ ได้แก่

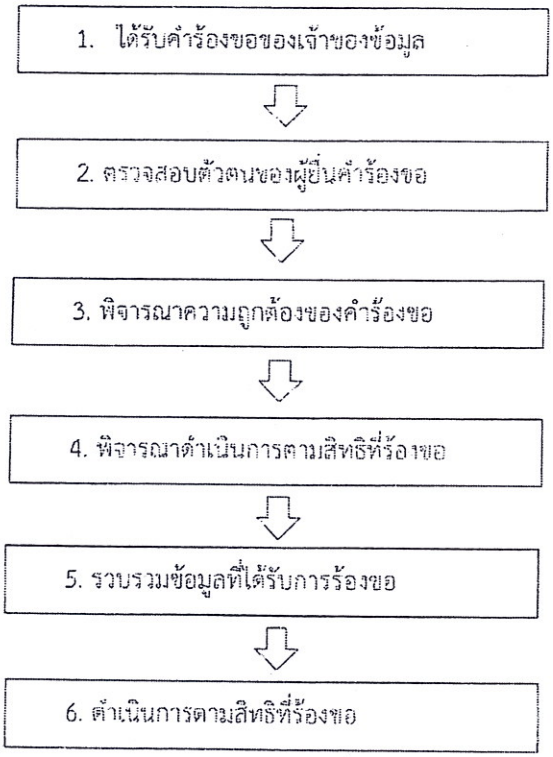
1) สิทธิในการได้รับแจ้งข้อมูล
2) สิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคล
3) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
4) สิทธิในการโอนถ่ายข้อมูลส่วนบุคคล
5) สิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลนั้นได้
6) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล
7) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล
8) สิทธิในการเพิกถอนความยินยอม

ให้หน่วยงานดูรายละเอียดในแต่ละหัวข้อที่ หนังสือแจ้งการประมวลผลข้อมูลส่วนบุคคล ในเอกสารแนบท้ายนี้

6.2 แนวปฏิบัติตามคำร้องขอของเจ้าของข้อมูล

กรณีที่เจ้าของข้อมูลมีความประสงค์จะใช้สิทธิ์ตามข้อ 6.1 ข้างต้น ด้วยตนเอง หรือมอบอำนาจให้ตัวแทนมาทำการแทน ให้ใช้แบบคำร้องขอใช้สิทธิของเจ้าของข้อมูล พร้อมเอกสารประกอบคำร้องเพื่อยืนยันตัวตนตามที่กำหนดไว้ เช่น สำเนาบัตรประจำตัวประชาชนหรือสำเนาหนังสือเดินทางของเจ้าของมูล และหรือตัวแทนผู้รับมอบอำนาจ หนังสือมอบอำนาจ ให้แก่หน่วยงาน

ขั้นตอนการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล เมื่อเจ้าของข้อมูลร้องขอ สรุปได้ดังนี้



ขั้นตอนการปฏิบัติงานมีดังนี้

ขั้นตอน	คำอธิบาย	ระยะเวลา	บุคคลที่เกี่ยวข้อง
1. ได้รับคำร้องขอของเจ้าของข้อมูล	● เจ้าของข้อมูลยื่นแบบคำร้องขอใช้สิทธิ ตามแบบฟอร์มที่สภาการพยาบาลกำหนด		หน่วยงาน
	● บันทึกรายการเกี่ยวกับคำร้องขอ เช่น วันที่ได้รับ ผู้ขอ ผู้รับเรื่อง เป็นต้น เพื่อใช้เป็นหลักฐานในการตรวจสอบการรับ และการปฏิบัติตามคำขอ	ทันทีที่ได้รับแบบคำขอ	เจ้าหน้าที่ของหน่วยงานที่มีหน้าที่บันทึกรายการ
	● หน่วยงานแต่งตั้งผู้รับผิดชอบในการตรวจสอบความคืบหน้าของการดำเนินการตามคำร้องขอจากบันทึกข้างต้น เพื่อให้แน่ใจ	ตรวจสอบบันทึกทุกๆ สัปดาห์ หรือที่หน่วยงาน	เจ้าหน้าที่ตรวจสอบของหน่วยงาน

ขั้นตอน	คำอธิบาย	ระยะเวลา	บุคคลที่เกี่ยวข้อง
	ว่าคำขอได้รับการจัดการทันท่วงทีภายในระยะเวลาที่กำหนด	กำหนดแต่ต้องน้อยกว่า 1 เดือน	
2. ตรวจสอบตัวตนของผู้ยื่นคำร้องขอ	● หน่วยงานต้องตรวจสอบตัวตนของผู้ยื่นคำร้อง โดยในกรณีที่เป็นเจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอด้วยตนเอง ให้พิจารณาเอกสารที่เกี่ยวข้องเพื่อระบุตัวตนว่าเป็นเจ้าของข้อมูลที่แท้จริง ได้แก่ บัตรประจำตัวประชาชน หรือหนังสือเดินทาง	ทันทีที่ได้รับแบบคำขอ	เจ้าหน้าที่หน่วยงาน
	● ในกรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น หน่วยงานจะต้องพิจารณาต่อไปว่าบุคคลดังกล่าวเป็นบุคคลที่มีอำนาจเต็มในการดำเนินการแทนเจ้าของข้อมูลหรือไม่ เช่น หนังสือมอบอำนาจ (กรณีมอบอำนาจ) หรือผู้ปกครอง (ในกรณีเจ้าของข้อมูลเป็นเด็ก) หรือผู้อนุบาล ผู้พิทักษ์ (ในกรณีเจ้าของข้อมูลเป็นคนไร้ความสามารถ หรือเสมือนไร้ความสามารถ)		
	● หากหน่วยงานมีความจำเป็นให้ผู้ยื่นคำร้องขอหรือเจ้าของข้อมูลจัดเตรียมข้อมูลเพิ่มเติมเพื่อพิจารณายืนยันตัวตน หน่วยงานจะต้องแจ้งให้แก่บุคคลดังกล่าวทราบโดยไม่ชักช้า		หน่วยงาน
3. พิจารณาความถูกต้อง/สมเหตุสมผลของคำขอ	● หน่วยงานต้องพิจารณาว่าคำร้องขอดังกล่าวถูกต้อง สมบูรณ์จะเป็นคำร้องขอที่มีอาศัยสิทธิตามที่กฎหมาย รับรองหรือไม่ คำขอนั้นสมเหตุสมผล (Unfounded) และไม่ฟุ่มเฟือยเกินความจำเป็น (Excessive) หรือไม่เป็นเหตุที่จะปฏิเสธการดำเนินการ	ทันทีที่ได้รับแบบคำขอ	เจ้าหน้าที่หน่วยงาน หัวหน้าหน่วย งาน หรือผู้มีอำนาจตัดสินใจปฏิเสธที่จะดำเนินการ
	● ในกรณีที่หน่วยงานประสงค์จะคิดค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอนั้น หน่วยงานจะต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า และหน่วยงานมีสิทธิยังไม่		

ขั้นตอน	คำอธิบาย	ระยะเวลา	บุคคลที่เกี่ยวข้อง
	ดำเนินการตามคำร้องขอจนกว่าจะได้รับชำระเงินค่าใช้จ่ายดังกล่าว		
4. พิจารณาดำเนินการตามสิทธิที่ร้องขอ	● ในกรณีที่มีการปฏิเสธ การกำหนดเงื่อนไขเพิ่มเติม เช่น การคิดค่าใช้จ่ายเพิ่มเติมกับเจ้าของข้อมูล หรือเกิดความล่าช้าในการดำเนินการตามคำร้องขอ หน่วยงานต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลสนับสนุนของการนั้น โดยจะต้องระบุถึงสิทธิของเจ้าของข้อมูลในการร้องทุกข์ต่อหน่วยงานกำกับดูแลที่เกี่ยวข้องต่อไปได้ และสิทธิในการเรียกร้องค่าสินไหมทดแทนทางศาล (Judicial Remedy) ด้วย	โดยไม่ชักช้า แต่ไม่เกิน 1 เดือนนับแต่วันที่ได้รับคำร้องขอ	หน่วยงาน
5. รวบรวมข้อมูลที่ได้รับการร้องขอ	● หน่วยงานจะต้องติดต่อกับฝ่ายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ ที่เกี่ยวข้องเพื่อดำเนินการตามคำร้องขอของเจ้าของข้อมูล	ภายใน 1 เดือน นับแต่วันที่ได้รับคำร้องขอ	หน่วยงานจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ฝ่ายที่เกี่ยวกับการเก็บรักษาข้อมูล
6. ดำเนินการตามสิทธิที่ร้องขอ	● ดำเนินการตามสิทธิที่ร้องขอ ● กรณีที่อาจจะต้องขยายระยะเวลา เนื่องจากมีความซับซ้อน หรือมีมีปริมาณคำร้องจำนวนมากในการดำเนินการ การขยายเวลาจะทำได้ไม่เกิน 2 เดือน	ภายใน 1 เดือน หรือ 2 เดือน(กรณีขยายระยะเวลานับแต่วันที่ได้รับคำร้องขอ	หน่วยงานจัดการข้อมูล/ฝ่ายที่รับผิดชอบ/ฝ่ายที่เกี่ยวกับการเก็บรักษาข้อมูล

6.3 กรณีหน่วยงานตรวจพบความไม่ถูกต้องหรือความไม่สมบูรณ์ของข้อมูล

กรณีที่หน่วยงานพบว่า ข้อมูลที่เก็บรวบรวมมีความไม่ถูกต้อง อันเนื่องจากความผิดพลาดในการพิจารณาและสอบทาน หรือข้อมูลไม่สมบูรณ์และจำเป็นต้องปรับปรุงหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลเพื่อประโยชน์ของผู้รับบริการในภายหลัง หน่วยงานจะต้องแจ้งให้เจ้าของข้อมูลทราบ และให้เจ้าของข้อมูลจัดทำ**คำร้องขอใช้สิทธิ** ให้แก่หน่วยงานเพื่อที่จะได้แก้ไขข้อมูลให้ถูกต้อง

การแก้ไขปรับปรุง เปลี่ยนแปลงข้อมูล จะต้องได้รับการอนุมัติจากผู้บริหาร หรือผู้ที่รับการแต่งตั้งก่อนการดำเนินการ

7. การดำเนินการ และกระบวนการแจ้งเหตุ กรณีมีการละเมิดข้อมูล หรือข้อมูลรั่วไหล

เมื่อเกิดเหตุละเมิดข้อมูล หรือมีข้อมูลรั่วไหล ให้หน่วยงานปฏิบัติ ดังนี้

1) ให้ผู้พบเหตุใช้แบบฟอร์มรายงานอุบัติการณ์ (Incident Report) แจ้งเหตุการณ์ละเมิดข้อมูลและข้อมูลรั่วไหล ให้ผู้รับผิดชอบข้อมูล (Data Owners) หรือผู้ที่ได้รับมอบหมาย รับทราบ **ทันทีที่ประสบเหตุ**

2) เจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลประจำหน่วยงาน หรือผู้ที่ได้รับมอบหมาย ดำเนินการรวบรวมรายละเอียด หลักฐาน และสาเหตุของการละเมิดข้อมูล หรือการรั่วไหลของข้อมูล เช่น ฐานข้อมูลถูกโจมตีโดยแฮกเกอร์

3) เจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลประจำหน่วยงาน หรือผู้ที่ได้รับมอบหมาย ทำการประเมินความเสี่ยงและวิเคราะห์ผลกระทบเบื้องต้นว่า มีความเสี่ยงต่อเจ้าของข้อมูลมากน้อยเพียงใด รวมทั้งเสนอแนะการแก้ไขเยียวยา

4) เจ้าหน้าที่ผู้ดูแลข้อมูลส่วนบุคคลประจำหน่วยงาน หรือผู้ที่ได้รับมอบหมาย ส่งเรื่องให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย (DPC) ของ Cluster ที่หน่วยงานสังกัด

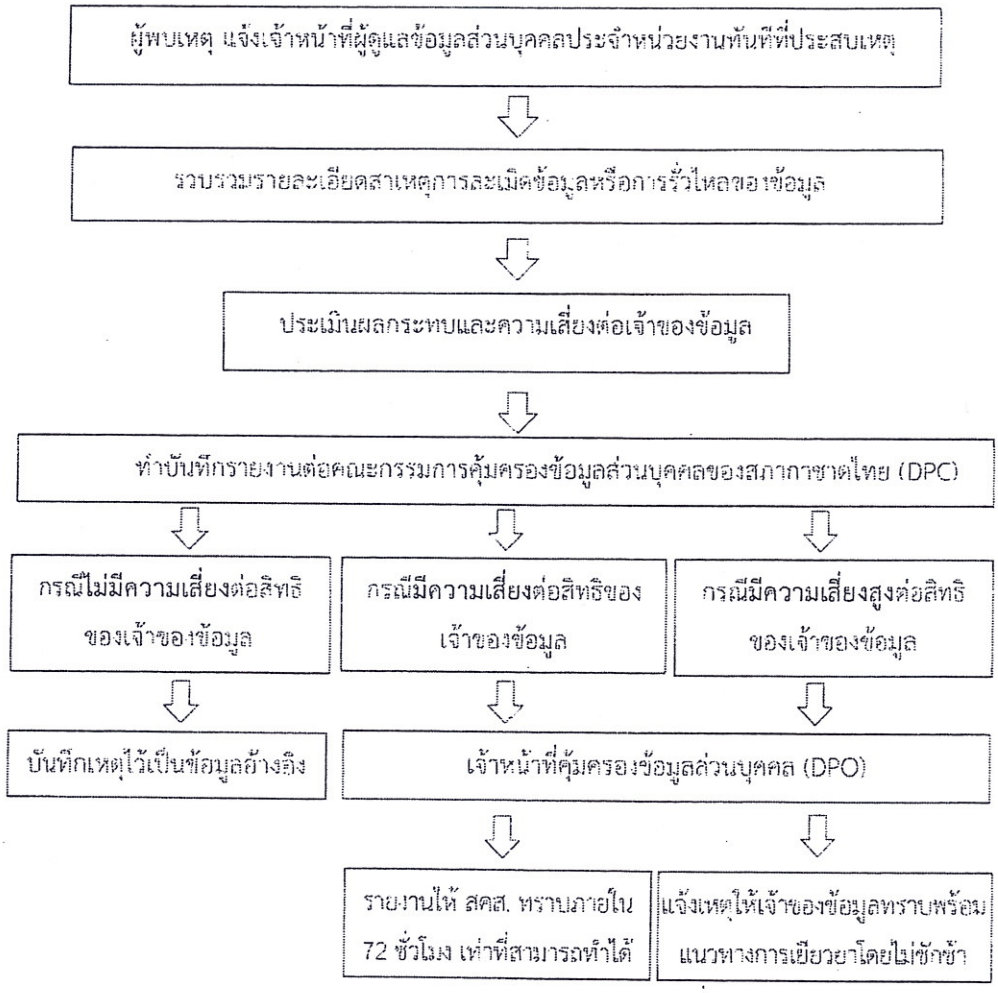
5) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย (DPO) สอบทานการวิเคราะห์ความเสี่ยงของผลกระทบและมาตรการตอบสนองเพื่อหยุดยั้งเหตุละเมิดข้อมูล ของรายงานที่ได้รับ และให้ความเห็นชอบ/อนุมัติของผลการประเมินและมาตรการการตอบสนอง

6) กรณีการละเมิดข้อมูล หรือการรั่วไหลข้อมูลมีความเสี่ยง และความเสี่ยงสูง ที่จะกระทบต่อสิทธิของเจ้าของข้อมูล หรือก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล ให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย (DPC) ทำบันทึก/รายงานต่อคณะเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย(DPO) เพื่อแจ้งให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และเจ้าของข้อมูลทราบเช่นกัน พร้อมแนวทางบรรเทาผลกระทบและแนวทางตอบสนองเพื่อหยุดยั้งการละเมิดข้อมูลส่วนบุคคล **ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ**

กรณีที่หน่วยงานไม่ได้จัดทำรายงานภายในกำหนดเวลา จะมีบทลงโทษจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีการละเมิดข้อมูล หรือการรั่วไหลของข้อมูลดังกล่าวไม่มีความเสี่ยง หรือมีความเสี่ยงต่ำที่จะกระทบกับสิทธิของเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกรายละเอียดของเหตุการณ์เพื่อเก็บไว้เป็นข้อมูลตรวจสอบย้อนหลังก็เพียงพอ ไม่จำเป็นต้องแจ้งทั้ง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลทราบ

ขั้นตอนการดำเนินการ และกระบวนการแจ้งเหตุ กรณีละเมิดข้อมูล หรือข้อมูลรั่วไหล สรุปได้ดังนี้



สคส. หมายถึง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

DPC หมายถึง คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสภาการชาติไทย

8. การควบคุม กรณีมีการจ้างผู้ประมวลผลข้อมูล (Data Processor)

กรณีที่มีการจ้างผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ภายนอก หน่วยงานจะต้องมีการทำสัญญา หรือมีข้อตกลงกับผู้รับจ้างประมวลผลว่าต้องปฏิบัติตามข้อตกลง หรือตามคำสั่งของหน่วยงานเท่านั้น รวมทั้งหน้าที่ในการแจ้งเหตุแก่หน่วยงานในกรณีมีการรั่วไหลของข้อมูลส่วนบุคคล

9. บันทึกการประมวลผลข้อมูลส่วนบุคคล (Record of Processing หรือ "RoP")

หน่วยงานจะต้องจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) ซึ่งอาจอยู่ในรูปแบบอิเล็กทรอนิกส์หรือเอกสาร ตามความเหมาะสมของแต่ละหน่วยงาน ทั้งนี้ รายการประมวลผลข้อมูลส่วนบุคคล ประกอบด้วยหัวข้อต่างๆ ได้แก่

1) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล เช่น ชื่อและที่อยู่หน่วยงาน และข้อมูลการติดต่อ (ชื่อเจ้าหน้าที่หรือผู้ประสานงาน) เป็นต้น
2) ข้อมูลรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) เช่น
   - ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
   - วัตถุประสงค์ของการเก็บรวบรวม
   - ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
   - สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล
   - การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
   - การรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล

10. ศูนย์รับเรื่องร้องเรียน

1) อ้างอิงตามประกาศสภากาชาดไทย เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสภากาชาดไทย พ.ศ. 2564 ในข้อ 5. การติดต่อกับสภากาชาดไทย หรือ

2) หากหน่วยงานต้องการจัดตั้งศูนย์รับเรื่องร้องเรียนของหน่วยงานเอง โปรดระบุรายละเอียดการติดต่อ เช่น ที่อยู่ อีเมล เบอร์โทรศัพท์ โดยชัดแจ้ง

สิ่งที่ส่งมาด้วย 1

แบบฟอร์มรับสมัครเป็นอาสาสมัครสภากาชาดไทย (TRC Volunteer)

1. จังหวัดที่ต้องการอาสา..... เลขบัตรประชาชน.....

2. คำนำหน้าชื่อ.....ชื่อ.....นามสกุล.....

3. เพศ.....วัน/เดือน/ปีเกิด (พ. ศ.) .....สัญชาติ.....

4. เบอร์โทรศัพท์มือถือ ☐☐☐-☐☐☐☐☐☐

5. ที่อยู่ติดต่อได้

เลขที่.....หมู่ที่.....ซอย.....ถนน.....

อำเภอ/เขต.....ตำบล/แขวง.....

จังหวัด.....รหัสไปรษณีย์.....

6. สถานะการทำงานปัจจุบัน

☐ รับราชการ	☐ พนักงานรัฐวิสาหกิจ/เอกชน	☐ นักเรียน/นักศึกษา
☐ เจ้าของธุรกิจ	☐ พ่อบ้าน/แม่บ้าน	☐ รับจ้างใช้แรงงาน
☐ เกษียณ	☐ เกษตรกร	☐ พระภิกษุ/นักบวช
☐ อาสาสมัคร	☐ อาชีพอิสระ	☐ ครู/อาจารย์
☐ อื่นๆ.....	☐ ไม่ได้ประกอบอาชีพ	

<u>หมายเหตุ</u> ข้อ 1 - 6 สำหรับอาสาสมัครต้องการกรอกข้อมูลผ่านแบบฟอร์ม ไม่สะดวกใช้ Application TRC Volunteer ในการสมัคร

7. TRC Volunteer Application: QR Code (ใช้สำหรับอาสาสมัครต้องการกรอกข้อมูลผ่าน Application)

ANDRIOD

IOS

เหล่ากาชาดจังหวัด Call Center :