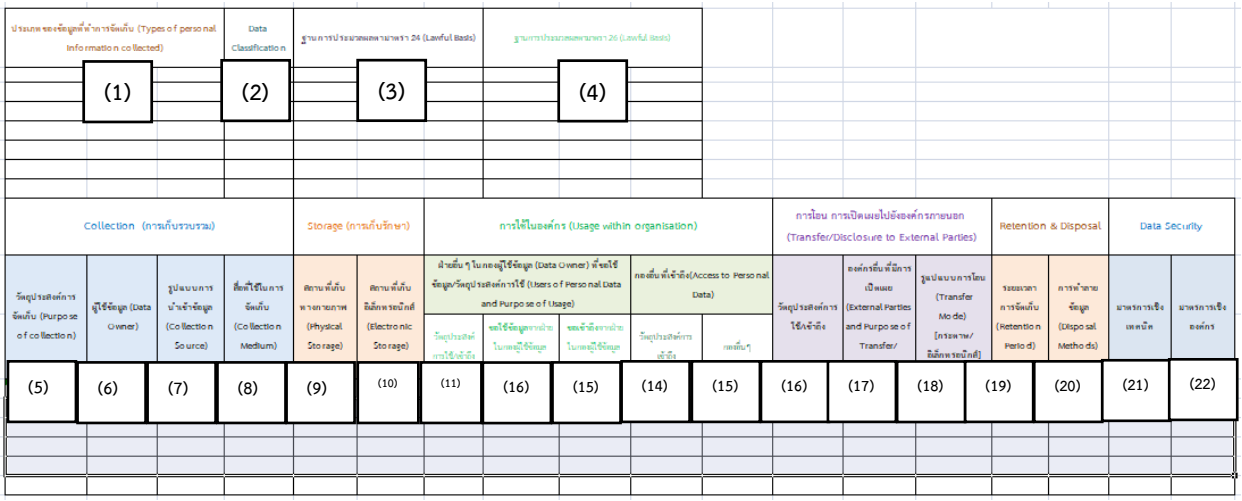
แนวทางการจัดทำบันทึกรายการกิจกรรม (ROPA)



1. **ประเภทของข้อมูล**

   ให้กรอกรายละเอียดของข้อมูลที่ทำการจัดเก็บ อาทิ

   1.1 ชื่อ/นามสกุล

   1.2 หมายเลขบัตรประจำตัวประชาชน

   1.3 หมายเลขโทรศัพท์

   1.4 บุคคลใกล้ชิด

   1.5 ที่อยู่

   1.6 อาการของโรค/ประวัติการรักษา

   ฯลฯ

2. **Data Classification**

   ในกรณีที่มีการจัดทำประเภทของข้อมูลเอาไว้ด้วย โดยอ้างอิงจากมาตรา 26 ที่แบ่งข้อมูลส่วนบุคคลเป็น 2 ประเภทหลัก คือ

   ข้อมูลส่วนบุคคลพื้นฐาน (Personal Data) ได้แก่ ข้อมูลพื้นฐานที่ใช้ระบุตัวตนของเจ้าของข้อมูลได้ ไม่ว่าจะเป็น ชื่อ นามสกุล อายุ รูปถ่าย หมายเลขโทรศัพท์ ที่อยู่ อีเมล และหมายเลขบัตรประชาชน รวมถึงประวัติการทำงานด้วย

   ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ได้แก่ ข้อมูลเกี่ยวกับความเชื่อ ทัศนคติ และประวัติด้านอาชญากรรม สุขภาพ และ อื่น ๆ เช่น เชื้อชาติ ชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อและความเห็นด้านศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลด้านสุขภาพ ความพิการ ไปจนถึง ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลสุขภาพ อย่างเช่น ใบรับรองแพทย์เป็นต้น

3. ฐานการประมวลผลตามมาตรา 24

ให้กรอกฐานการประมวลผลตามมาตรา 24 กรณีใดกรณีหนึ่ง ดังต่อไปนี้

3.1 เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ ตามที่คณะกรรมการประกาศกำหนด

3.2 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

3.3 เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือ เพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

3.4 เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

3.5 เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญ น้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

3.6 เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

3.7 ความยินยอม

4. ฐานการประมวลผลตามมาตรา 26

ให้กรอกฐานการประมวลผลตามมาตรา 26 กรณีใดกรณีหนึ่ง ดังต่อไปนี้

4.1 เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูล ส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม

4.2 เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กร ที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

4.3 เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

4.4 เป็นการจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

4.5 เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(1) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติ ตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพ

หรือวิชาชีพหรือผู้มีหน้าที่ รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของ ข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(2) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพ ของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือ ตามจริยธรรมแห่งวิชาชีพ

(3) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับ การรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูล ส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐาน และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(4) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มีมาตรการ ที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการ ประกาศกำหนด

(5) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครอง สิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5. วัตถุประสงค์การจัดเก็บ

ให้กรอกวัตถุประสงค์ของการเก็บรวบรวมข้อมูล อาทิ

5.1 การจัดทำบัญชีเงินเดือน

5.2 การเบิกจ่ายสวัสดิการ

5.3 การจัดทำสัญญาจ้าง

5.4 การรักษาพยาบาล/การวินิจฉัยโรค

5.5 การจัดทำฐานข้อมูลสุขภาพภาครัฐ

5.6 การเฝ้าระวังภัยคุกคามทางไซเบอร์

ฯลฯ

6. ผู้ใช้ข้อมูล (Data Owner)

ให้ระบุฝ่าย/แผนก/กอง ที่เป็นผู้ใช้ข้อมูล/เก็บข้อมูล

6.1 กลุ่มงานอัตรากำลัง กองบริหารทรัพยากรบุคคล

6.2 กลุ่มบริหารพัสดุและจัดซื้อจัดจ้าง กองบริหารการคลัง

6.3 กลุ่มงานคดีทางการแพทย์ กองกฎหมาย

6.4 กลุ่มงานพัฒนาหลักประกันสุขภาพ กองเศรษฐกิจสุขภาพและหลักประกันสุขภาพ

ฯลฯ

7. รูปแบบการนำเข้าข้อมูล

ให้ระบุวิธีการเก็บรวบรวมข้อมูลส่วนบุคคล

7.1 จากระบบงานภายใน

7.2 จากเจ้าของข้อมูลส่วนบุคคลโดยตรง

7.3 จากผู้ให้บริการข้อมูล (บุคคลที่สาม)

ฯลฯ

8. ส่วนที่ใช้ในการจัดเก็บ

ให้ระบุชื่อ/ช่องทางที่นำเข้าข้อมูล อาทิ

8.1 เอกสาร/ใบสมัคร

8.2 ออนไลน์ฟอร์ม

ฯลฯ

9. สถานที่จัดเก็บทางกายภาพ

ให้ระบุสถานที่ที่ข้อมูลถูกเก็บรักษาไว้ อาทิ

9.1 ตู้เอกสาร/ห้องเอกสาร

9.2 เข้าแฟ้ม

9.3 โต๊ะทำงาน

9.4 คลังเอกสาร

9.5 ห้องปฏิบัติการคอมพิวเตอร์ หรือ Data Center

ฯลฯ

10. สถานที่เก็บทางอิเล็กทรอนิกส์

ให้ระบุสถานที่เก็บทางอิเล็กทรอนิกส์ อาทิ

10.1 ระบบฐานข้อมูล (ระบุชื่อถ้ามี)

10.2 Shared Drived

10.3 เทป

10.4 โปรแกรมระบบงาน

10.5 หน่วยความจำแบบแฟลช (Flash Memory) เช่น Flash Drive, Solid State Drive และ Memory Card

10.6 สื่อเก็บข้อมูลแสง (Optical Storage Device) เช่น CD, DVD หรือ Blu-ray Disc

ฯลฯ

11. วัตถุประสงค์การใช้/เข้าถึงข้อมูล

ให้ระบุว่ามีฝ่ายใดอีกบ้างที่ใช้ข้อมูลและให้ระบุวัตถุประสงค์การใช้ด้วย อาทิ

11.1 เพื่อทำเบิกจ่าย

11.2 เพื่อการจัดทำสัญญา

ฯลฯ

12. กลุ่มงานในกองผู้ใช้ข้อมูล (Data Owner) ขอใช้ข้อมูล

ให้ระบุว่ามีกลุ่มใดอีกบ้างที่ใช้ข้อมูล อาทิ

12.1 กลุ่มงานอัตรากำลัง กองบริหารทรัพยากรบุคคล

12.2 กลุ่มบริหารพัสดุและจัดซื้อจัดจ้าง กองบริหารการคลัง

12.3 กลุ่มงานคดีทางการแพทย์ กองกฎหมาย

12.4 กลุ่มงานพัฒนาหลักประกันสุขภาพ กองเศรษฐกิจสุขภาพและหลักประกันสุขภาพ

ฯลฯ

13. กลุ่มงานในกองผู้ใช้ข้อมูล (Data Owner) ขอใช้ข้อมูล

ให้ระบุว่ามีกลุ่มงานอื่นๆในองค์กรที่เข้าถึงแต่อาจไม่ได้ใช้ข้อมูลหรือไม่ โดยส่วนใหญ่มักจะเป็นฝ่าย IT เป็นต้น

14. กองอื่น มีวัตถุประสงค์การใช้/เข้าถึงข้อมูล

ให้ระบุว่ามีฝ่ายใดอีกบ้างที่ใช้ข้อมูลและให้ระบุวัตถุประสงค์การใช้ด้วย อาทิ

14.1 เพื่อทำเบิกจ่าย

14.2 เพื่อการจัดทำสัญญา

ฯลฯ

15. กองอื่นที่เข้าถึง (Access to Personal Data)

ให้ระบุว่ามีกลุ่มใดอีกบ้างที่ใช้ข้อมูล อาทิ

15.1 กลุ่มงานอัตรากำลัง กองบริหารทรัพยากรบุคคล

15.2 กลุ่มบริหารพัสดุและจัดซื้อจัดจ้าง กองบริหารการคลัง

15.3 กลุ่มงานคดีทางการแพทย์ กองกฎหมาย

15.4 กลุ่มงานพัฒนาหลักประกันสุขภาพ กองเศรษฐกิจสุขภาพและหลักประกันสุขภาพ

ฯลฯ

16. วัตถุประสงค์การขอใช้/เข้าถึงไปยังภายนอก

16.1 เพื่อทำเบิกจ่าย

16.2 เพื่อการจัดทำสัญญา

ฯลฯ

17. การโอน การเปิดเผยไปยังภายนอก

ให้ระบุว่ามีการโอนข้อมูลไปยังบุคคล/องค์กรภายนอกหรือไม่ พร้อมทั้งระบุวิธีการโอน/เปิดเผยด้วย

17.1 บริษัท xxx (ผู้ประมวลผลข้อมูลส่วนบุคคล/การเชื่อมต่อ AP)

17.2 กรม xxx /รูปแบบแฟ้มเอกสาร

18. รูปแบบการโอน (Transfer Mode)

18.1 กระดาษ

18.2 อิเล็กทรอนิกส์

19. ระยะเวลาการจัดเก็บ

ให้ระบุระยะเวลาการจัดเก็บข้อมูล อาทิ

19.1 3 ปี นับตั้งแต่เริ่มสภาพการเป็นพนักงาน

19.2 5 ปี นับตั้งแต่สิ้นสุดการใช้

19.3 10 ปี นับตั้งแต่ (ระบุเงื่อนไข)

ฯลฯ

20. การทำลาย

ให้ระบุวิธีการทำลายข้อมูล โดยขึ้นอยู่กับรูปแบบของการจัดเก็บ อาทิ

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

21. มาตรการด้านความมั่นคงปลอดภัย

ให้ระบุวิธีการปกป้องข้อมูล อาทิ

21.1 แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. ๒๕๖๕

21.2 มาตรการเชิงองค์กร

- การกำหนดสิทธิการเข้าถึง
- นโยบายในการใช้อุปกรณ์ส่วนตัว

21.3 มาตรการเชิงเทคนิค

- การเข้ารหัส
- DLP Tool
- Malware Detection Tool

ฯลฯ

แนวทางการจัดทำบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้องค์กรมีหน้าที่ตามมาตรา 39 ในการจัดให้มีบันทึกรายการกิจกรรมอย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ซึ่งได้แก่คำอธิบายเกี่ยวกับประเภทของบุคคล (categories of individual) หรือประเภทของข้อมูลส่วนบุคคล (categories of personal data) ที่องค์กรทำการประมวลผล

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ได้แก่ ชื่อ และรายละเอียดการติดต่อขององค์กร รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม กล่าวคือ หากองค์กรใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 องค์กรต้องบันทึกการใช้หรือเปิดเผยนั้นไว้ในรายการตามมาตรา 39 ด้วย ซึ่งในทางปฏิบัติหมายความถึง (1) ให้ระบุฐานทางกฎหมายในการประมวลผล (2) ให้ระบุการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก และ (3) ให้ระบุการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

(7) การบันทึกรายละเอียดการปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 30 วรรคสาม (สิทธิในการเข้าถึง) มาตรา 31 วรรคสาม (สิทธิในการขอให้โอนข้อมูล) มาตรา 32 วรรคสาม (สิทธิในการคัดค้านการประมวลผล) และมาตรา 36 วรรคหนึ่ง (สิทธิในการขอแก้ไขข้อมูลให้ถูกต้อง) ตามเงื่อนไขที่กฎหมายกำหนด

(8) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

โดยในการจัดทำบันทึกรายการกิจกรรมฯ หรือ Record of Processing Activities (ROPA) องค์กรอาจจัดเตรียมบันทึกรายการกิจกรรมฯ โดยพิจารณาดังนี้

(1) องค์กรที่มีหน้าที่ต้องจัดให้มีการบันทึกรายการกิจกรรมฯ ต้องสอบทานในส่วนของวัตถุประสงค์การประมวลผล การเปิดเผยข้อมูลส่วนบุคคล และระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(2) องค์กรต้องสามารถให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบบันทึกรายการกิจกรรมฯ ได้

(3) บันทึกรายการกิจกรรมฯ ช่วยให้องค์กรสามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเด็นอื่น ๆ ได้ดียิ่งขึ้น และช่วยสร้างธรรมาภิบาลของข้อมูล

(4) ทั้งผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ในการจัดทำเอกสารบันทึกรายการกิจกรรมฯ

(5) การทำผังวงจรชีวิตของข้อมูลจะช่วยตรวจสอบกิจกรรมการประมวลผลข้อมูลส่วนบุคคลในองค์กรให้ถูกต้องเป็นปัจจุบัน

(6) บันทึกรายการกิจกรรมฯ ต้องมีความถูกต้องเป็นปัจจุบันและสะท้อนการประมวลผลข้อมูลส่วนบุคคลในองค์กร ดังนั้น เมื่อมีความเปลี่ยนแปลงเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่มีผลกระทบต่อความถูกต้องสมบูรณ์ของบันทึกรายการกิจกรรมฯ อาทิ มีการโอนข้อมูลเพิ่มเติมไปยังองค์กรอื่น ๆ ทั้งในและต่างประเทศ หรือมีการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล จึงต้องมีการแก้ไขบันทึกรายการกิจกรรมฯ ด้วย เป็นต้น

ในส่วนข้อแนะนำในการจัดทำบันทึกรายการกิจกรรมฯ มีข้อแนะนำเพิ่มเติมตามแนวปฏิบัติที่ดีของ UK ICO ซึ่งเป็นหน่วยงานบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของอังกฤษ ดังนี้

1) ในการทำบันทึกกิจกรรมฯ องค์กรควรดำเนินการ ดังนี้

1.1) ทบทวนการประมวลผลขององค์กรว่ามีการเก็บรวบรวมข้อมูลส่วนบุคคลประเภทใดบ้าง

1.2) มีการสอบทานข้อเท็จจริงกับบุคคลต่าง ๆ ในองค์กรเพื่อให้ได้ข้อมูลที่ถูกต้องเกี่ยวกับกิจกรรมการประมวลผล

1.3) ได้ทำการทบทวนนโยบาย แนวทางปฏิบัติ สัญญาหรือข้อตกลงซึ่งเกี่ยวข้องกับระยะเวลาการจัดเก็บข้อมูล มาตรการด้านความมั่นคงปลอดภัย และการเปิดเผยหรือการโอนข้อมูล

2) ในการจัดทำบันทึกรายการกิจกรรมฯ องค์กรได้ทำการเชื่อมโยงข้อมูลดังนี้

2.1) ข้อมูลที่ต้องแจ้งหรือเปิดเผยในประกาศความเป็นส่วนตัว (Privacy Notice)

2.2) บันทึกความยินยอม

2.3) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

2.4) แหล่งที่เก็บของข้อมูลส่วนบุคคล

2.5) การประเมินความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

2.6) บันทึกเหตุการละเมิดข้อมูลส่วนบุคคล

2.7) องค์กรควรจัดทำบันทึกรายการกิจกรรมในรูปแบบอิเล็กทรอนิกส์ ซึ่งสามารถเพิ่มเติม ลบออก และแก้ไขข้อมูลได้โดยง่าย

นอกจากนี้ ตามพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังอาจกำหนดเงื่อนไขบางประการเพิ่มเติมเกี่ยวกับการจัดทำบันทึกรายการกิจกรรมฯ ได้ดังนี้

(1) กำหนดยกเว้นให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการฯ กำหนดไม่ต้องจัดทำบันทึกรายการกิจกรรมฯ

(2) กำหนดให้ “ผู้ประมวลผลข้อมูลส่วนบุคคล” มีหน้าที่จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมฯ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการฯ ประกาศกำหนด

ซึ่งในปัจจุบันได้มีประกาศคณะกรรมการฯ ตามข้อ (1) แล้ว ได้แก่ ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การยกเว้นการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก พ.ศ. 2565 ซึ่งเมื่อพิจารณาคู่มือปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงสาธารณสุขแล้วพบว่า ประกาศฉบับดังกล่าวไม่เกี่ยวข้องกับกระทรวงสาธารณสุข เนื่องจากกระทรวงสาธารณสุขไม่อยู่ในลักษณะของผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็ก ที่กฎหมายกำหนดให้มีการยกเว้นการดำเนินการตามมาตรา 39 วรรคหนึ่ง (1) (2) (3) (4) (5) (6) และ (8) ในเรื่องการบันทึกรายการของผู้ควบคุมข้อมูลส่วนบุคคลแต่อย่างใด

สำหรับประกาศตามข้อ (2) นั้นปัจจุบันได้มีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. 2565 ซึ่งเมื่อพิจารณาแล้วพบว่า ประกาศฉบับดังกล่าวใช้บังคับกับ “ผู้ประมวลผลข้อมูลส่วนบุคคล” ที่จะต้องจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของแต่ละประเภทกิจกรรมไว้ (รายละเอียดกำหนดไว้ตามประกาศ ข้อ 3) ดังนั้นเมื่อพิจารณาบริบทของกระทรวงสาธารณสุข แล้วพบว่า กระทรวงสาธารณสุข เป็น “ผู้ควบคุมข้อมูลส่วนบุคคล” ดังนั้น ประกาศฉบับดังกล่าวจึงไม่ใช้บังคับกับกระทรวงสาธารณสุข แต่อย่างใด

ทั้งนี้ในส่วนของ 2 ประเด็นข้างต้นนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) ได้กำหนดหลักเกณฑ์ ไว้ดังนี้

1) ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำบันทึกรายการของกิจกรรมฯ มีรายละเอียดอย่างน้อย ดังนี้

1.1) ชื่อและสถานที่ติดต่อของผู้ประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคล
รวมถึงผู้แทนและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ถ้าหากมี

1.2) ประเภทของกิจกรรมการประมวลผลที่ดำเนินการให้แก่ผู้ว่าจ้างแต่ละราย

1.3) รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

1.4) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

2) GDPR กำหนดยกเว้นให้องค์กรที่มีพนักงานน้อยกว่า 250 คน ได้รับยกเว้นไม้ต้องจัดทำบันทึกรายการของกิจกรรมฯ เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว

ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ การที่องค์กรใดมีหน้าที่ต้องจัดทำบันทึกรายการกิจกรรมฯ แต่ไม่ดำเนินการให้ถูกต้องตามเงื่อนไขที่กฎหมายกำหนดอาจต้องระวางโทษปรับทางปกครองไม่เกินหนึ่งล้านบาทอีกด้วย และนอกจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่สามารถเข้าถึงหรือขอตรวจสอบบันทึกรายการของกิจกรรมฯ ได้ กฎหมายยังกำหนดให้ “เจ้าของข้อมูลส่วนบุคคล” สามารถเข้าถึงหรือขอตรวจสอบบันทึกรายการของกิจกรรมฯ ได้อีกด้วย