



# การจัดการองค์ความรู้ (KM)

## เรื่องที่ 4

การคุ้มครองข้อมูลส่วนบุคคลของท้องถิ่น



จัดทำโดย

องค์การบริหารส่วนตำบลน้ำร้อน อำเภอเมืองตาก จังหวัดตาก



## KM การคุ้มครองข้อมูลส่วนบุคคล PDPA

หัวข้อการจัดการองค์ความรู้ : การคุ้มครองข้อมูลส่วนบุคคลในหน่วยงานท้องถิ่น

วันที่ 26 เดือน มกราคม พ.ศ.2566



สำหรับการจัดการองค์ความรู้ในเดือนมกราคม 2566 นี้ ได้คัดเลือกหัวข้อที่จะได้พูดคุยกันเกี่ยวกับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งทุกสำนัก/กอง ของ อบต.น้ำริน จะต้องนำไปถือปฏิบัติในการทำงานในทุกๆ กระบวนการที่เกี่ยวกับทั้งบุคคลภายใน และบุคคลภายนอก โดยให้ความรู้เกี่ยวกับกฎหมาย PDPA และระดมความคิดเห็นในการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลระดับองค์กร

โดยสามารถสรุปการจัดการองค์ความรู้ ได้ดังนี้

1.การคุ้มครองข้อมูลส่วนบุคคล มีผลต่อทั้งบุคลากรในหน่วยงาน พนักงาน ลูกจ้างทุกคน ก็เป็นเจ้าของข้อมูลของตนเอง ดังนั้น อบต.น้ำริน จะต้องมึนโยบายในการคุ้มครองข้อมูลส่วนบุคคลให้กับพนักงาน-ลูกจ้างทุกระดับ

2.การคุ้มครองข้อมูลส่วนบุคคล สำหรับผู้มีติดต่อราชการ หรือบุคคลภายนอกองค์กร ต้องจัดทำแบบคำยินยอมให้ใช้ จัดเก็บ และเผยแพร่ข้อมูลส่วนบุคคลที่จำเป็นสำหรับการปฏิบัติงานในเรื่องเฉพาะเท่านั้น

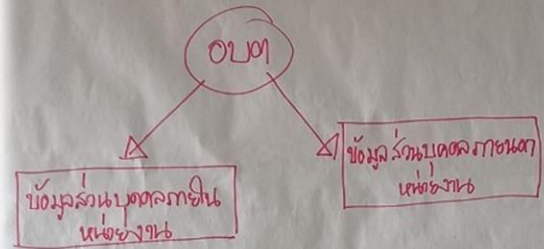
3.ร่วมกันกำหนดกิจกรรมที่ สำนัก/กอง จะต้องดำเนินการภายใต้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล : PDPA



# KM : PDPA #2562

(Personal Data Protection Act)

- |                         |
|-------------------------|
| ① เก็บรวบรวม            |
| ② การใช้ (ข้อมูล)       |
| ③ การเปิดเผย (ข้อมูล)   |
| ④ การเก็บรักษา (ข้อมูล) |
| ⑤ การทำลาย (ข้อมูล)     |



## กิจกรรมที่ต้องทำ

1. สร้างการตระหนักรู้ (ผู้บริหาร/คณาฯ/บุคลากร)
2. ตั้ง ตำแหน่ง/ทีมงาน
3. ตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
4. ฝึกอบรมคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
5. ฝึกอบรมหน่วยงานที่มีนโยบายคุกกี้ (Cookies Policy)
6. 10กรฟอร์มขอความยินยอม (Consent form)
7. คู่มือการทำงานภายใน เกี่ยวกับ ข้อมูลส่วนบุคคล
8. ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA)
9. การทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (RoPA)
10. มีช่องทาง การใช้สิทธิ์ ควบคุมของข้อมูล.



10 ฝึกอบรมบุคลากรเกี่ยวกับ  
 8 ฝึกอบรมหน่วยงานที่มีนโยบายคุกกี้ (Cookies Policy)  
 6 10กรฟอร์มขอความยินยอม (Consent form)



# สรุปองค์ความรู้ และข้อตกลงร่วมกันในการดำเนินงาน PDPA ของ อบต.น้ำรั่ม

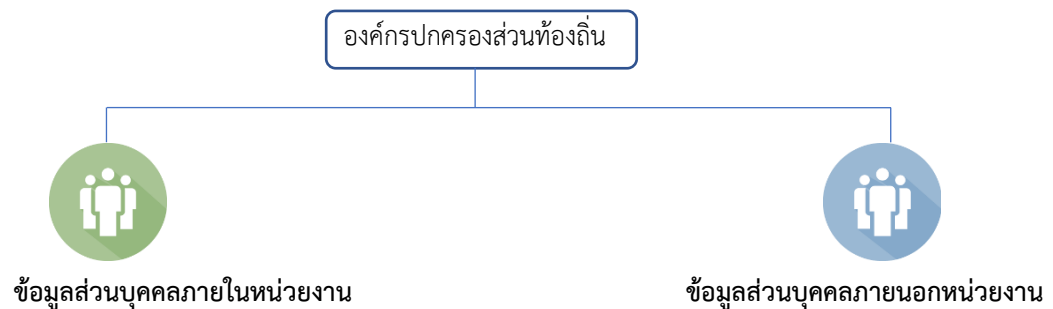
PDPA ย่อมาจาก Personal Data Protection Act B.E. 2562 (2019) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยกฎหมาย PDPA Thailand (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ 1 มิถุนายน 2565



การเตรียมความพร้อมทั้งการเสริมสร้างความรู้ความเข้าใจในบทกฎหมาย ความรับรู้ และตระหนักของบุคลากรเจ้าหน้าที่ ตลอดจนการเตรียมปรับปรุงการบริหารเอกสารและการจัดทำเอกสารที่เกี่ยวข้องตั้งแต่เริ่มต้น เพื่อเป็นแนวทางให้ท้องถิ่นดำเนินการคุ้มครองข้อมูลส่วนบุคคลอย่างถูกต้องและมีประสิทธิภาพสอดคล้องกับเจตนารมณ์ของกฎหมาย โดยสามารถแบ่งกิจกรรมออกเป็น 2 ส่วน ได้แก่

- (1) ขั้นตอนการเตรียมความพร้อมองค์กรในการปฏิบัติตามกฎหมาย
- (2) กิจกรรมที่ควรเร่งดำเนินการในระยะเริ่มแรก

## ขั้นตอนการเตรียมความพร้อมขององค์กร



โดยการเตรียมความพร้อม แบ่งออกเป็น 5 ขั้นตอน ดังนี้

### 1. เก็บรวบรวม :

- 1.1 เก็บเท่าที่จำเป็น : ภายใต้วัตถุประสงค์ที่ชอบด้วย กม.
- 1.2 เก็บโดยได้รับความยินยอม
  - (1) ข้อมูลส่วนบุคคลทั่วไป
  - (2) ข้อมูลส่วนบุคคลที่อ่อนไหว
- 1.3 แจ้งวัตถุประสงค์
  - (1) วัตถุประสงค์ของการเก็บเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเผยแพร่
  - (2) แจ้งให้เจ้าของข้อมูลส่วนบุคคลมีหน้าที่ปฏิบัติตามกฎหมายหรือสัญญาที่ต้องให้ข้อมูลส่วนบุคคล รวมถึงแจ้งผลกระทบจากการไม่ให้ข้อมูลส่วนบุคคล

- (3) แจ้งระยะเวลาในการจัดเก็บรวบรวม
- (4) แจ้งประเภท/หน่วยงาน ซึ่งอาจมีการเปิดเผยข้อมูลส่วนบุคคล
- (5) แจ้งข้อมูลผู้ควบคุมข้อมูล
- (6) แจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

**2.การใช้ :** ต้องใช้โดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น

ผู้ควบคุมข้อมูล : มีหน้าที่ ต้องใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่แจ้งในขณะเก็บรวบรวมเท่านั้น จะใช้นอกวัตถุประสงค์ไม่ได้ เช่น ท้องถิ่นมีการจัดเก็บเบอร์โทรผู้ใช้สิทธิสวัสดิการผู้สูงอายุ เบอร์โทรนี้สามารถใช้เพื่อติดต่อสื่อสารเกี่ยวกับการเบิกสวัสดิการผู้สูงอายุเท่านั้น ท้องถิ่นจะนำเบอร์โทรไปใช้เพื่อประชาสัมพันธ์กิจกรรมอื่นๆไม่ได้



### 3.เปิดเผย :

3.1 การเปิดเผย/เผยแพร่ข้อมูลส่วนบุคคล จะเปิดเผยได้โดยได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่จะมีข้อยกเว้น

3.2 บุคคล/นิติบุคคล ที่ได้รับข้อมูลส่วนบุคคลจากการเปิดเผย จะต้องไม่ใช่สิทธิหรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกจากวัตถุประสงค์ที่ได้แจ้งไว้กับผู้ควบคุมข้อมูล



#### ควรเตรียมอะไรบ้าง?

-เตรียมเอกสารเกี่ยวกับข้อตกลง ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)



**4.เก็บรักษา :** ผู้ควบคุมข้อมูล มีหน้าที่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยไม่ชอบ และต้องทบทวนมาตรการดังกล่าว เมื่อมีความจำเป็น หรือมีเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

- (1) การทำให้ข้อมูลส่วนบุคคลนั้นเป็นความลับ
- (2) การทำให้ข้อมูลส่วนบุคคลนั้นมีความถูกต้อง
- (3) การทำให้ข้อมูลส่วนบุคคลนั้นมีสภาพพร้อมใช้งาน

#### แนวทาง

-สำรวจการจัดเก็บฐานข้อมูล / แยกประเภทของวิธีการจัดเก็บ เช่น

1.เอกสารกระดาษ : เก็บไว้ในตู้เอกสาร มีกุญแจล็อก กำหนดให้มีผู้มีสิทธิเข้าถึงเอกสาร หรือมีผู้อนุมัติ

2.เอกสารอิเล็กทรอนิกส์ : เก็บไว้ในโทรศัพท์หน่วยงาน กำหนดสิทธิการเข้าถึงไฟล์ และหากมี จันท.โอนย้าย/ลาออก ให้ยกเลิกสิทธิเข้าถึงด้วย

**5.ทำลาย :** ผู้ควบคุมข้อมูล มีหน้าที่จัดให้มีระบบตรวจสอบเพื่อดำเนินการ ลบ ทำลายข้อมูลส่วนบุคคล เมื่อพ้นกำหนดระยะเวลาการ จัดเก็บรักษา ที่ไม่เกี่ยวข้อง เกินความจำเป็น ตามวัตถุประสงค์ในการเก็บรวบรวม ตามที่เจ้าของข้อมูลร้องขอ หรือเจ้าของข้อมูลได้ถอน ความยินยอม



## กิจกรรมที่ควรเร่งดำเนินการในระยะเริ่มแรก

ในส่วนของการดำเนินการในระดับแรกของการเตรียมความพร้อมของ องค์กร.น้ำเริ่ม มีรายการกิจกรรม 10 กิจกรรม ที่ควรดำเนินการอย่างเร่งด่วนเพื่อขับเคลื่อนการคุ้มครองข้อมูลส่วนบุคคลและเป็นแนวทางการปฏิบัติสำหรับ บุคคลากรของท้องถิ่นในการปฏิบัติตามกฎหมาย ดังนี้

- (1) สร้างการตระหนักรู้ ให้กับผู้บริหารท้องถิ่น เจ้าหน้าที่ ลูกจ้างภายในหน่วยงาน
- (2) ตั้งคณะทำงาน โดยมาจากหัวหน้างานหรือเจ้าหน้าที่ในแต่ละส่วนงานที่มีการทำงานเกี่ยวข้องกับข้อมูลส่วนบุคคล
- (3) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) : ทำหน้าที่ให้คำแนะนำ และตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลในหน่วยงาน
- (4) นโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
- (5) เว็บไซต์ของหน่วยงานมีนโยบายคุกกี้ (Cookies Policy)
- (6) เอกสารขอความยินยอม (Consent form)
- (7) คู่มือการทำงานภายในเกี่ยวกับข้อมูลส่วนบุคคล
- (8) ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement : DPA)
- (9) การทำบันทึกกิจกรรมประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities : RoPA)
- (10) มีช่องทางการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

## ข้อมูลส่วนบุคคล คือ ???

ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดให้ข้อมูลส่วนบุคคลมีความหมายว่า “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ” โดยมี 4 หลักเกณฑ์ในการพิจารณา ดังนี้

**1. สิ่งนั้นต้องเป็นข้อมูล :** ข้อมูลในที่นี้หมายถึงข้อเท็จจริงที่ครอบคลุมทั้งข้อเท็จจริงที่รับรู้เป็นที่ประจักษ์โดยไม่ขึ้นอยู่กับความเห็นส่วนตัว (Objective) และข้อเท็จจริงที่เป็นไปตามความคิดเห็นส่วนตัวของบุคคลใดบุคคลหนึ่ง (Subjective)

**2. ข้อมูลนั้นมีความเกี่ยวข้องกับบุคคล :** ความเกี่ยวข้องอาจเกิดจากเนื้อหาของข้อมูล วัตถุประสงค์ของการใช้ข้อมูล และผลลัพธ์ของการใช้ข้อมูล

**3. ข้อมูลนั้นสามารถระบุตัวตนของบุคคล :** ข้อมูลที่มีความเกี่ยวข้องกับบุคคลมีความสามารถเพียงพอที่จะระบุตัวตนได้ทันที (Identified) เป็นข้อมูลที่สามารถระบุตัวตนได้โดยตรง (Direct identification) หรือสามารถระบุตัวตนได้ในกรณีที่มีการดำเนินการเพิ่มเติม (identifiable) จึงสามารถระบุตัวตนได้ (Indirect identification)

**4. ข้อมูลของบุคคลธรรมดา :** ข้อมูลส่วนบุคคลจะไม่ครอบคลุมถึงนิติบุคคลและบุคคลที่ถึงแก่ความตาย อย่างไรก็ตาม เรื่องดังกล่าวทำให้ภาครัฐไม่มีหน้าที่ในการปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ต่อข้อมูลดังกล่าวเท่านั้น แต่ภาครัฐอาจมีความจำเป็นที่จะต้องคุ้มครองข้อมูลดังกล่าวตามหน้าที่ในกฎหมายฉบับอื่น เช่น พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.2540 เป็นต้น

\*\*\*\*\*