

## PDPA เกี่ยวข้องกับใครในองค์กร

นางสาวดุจดวงมณี เครือแก่นแก้ว  
นิติกร สังกัดกองกฎหมาย สำนักงานอธิการบดี  
มหาวิทยาลัยขอนแก่น

เมื่อมีการบังคับใช้กฎหมาย เราจำเป็นที่จะต้องทำความเข้าใจว่า “ ใคร ” คือผู้ที่เกี่ยวข้องในกฎหมายนี้ๆ โดยเฉพาะอย่างยิ่งกฎหมายใหม่มาแรงที่เราต้องทำความเข้าใจ โดยหลายๆท่านอาจจะเคยได้ยินผ่านหูถึงชื่อกฎหมาย PDPA โดยผู้เขียนขออธิบายว่า กฎหมาย PDPA นั้น เป็นกฎหมายที่จะเข้ามาคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลของแต่ละคน ไม่ว่าจะเป็นการเก็บรวบรวม ใช้ หรือแม้กระทั่งการเผยแพร่ข้อมูลส่วนบุคคลซึ่งจะมีบุคคลใดบ้างที่เกี่ยวข้องกับกฎหมาย PDPA ดังนั้น จึงมีความจำเป็นที่ทุกท่านจะต้องทำความเข้าใจเกี่ยวกับบุคคลที่เกี่ยวข้องในกฎหมายดังกล่าวให้มากยิ่งขึ้น

PDPA ย่อมาจาก Personal Data Protection Act เป็น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งให้ความคุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลของแต่ละบุคคล โดยมีการกำหนดรายละเอียด สิทธิ และหน้าที่ของบุคคลที่เกี่ยวข้องเอาไว้อย่างชัดเจน ไม่ว่าจะเป็นสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject) หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Collector) หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เป็นต้น โดยผู้เขียนจะขออธิบายหน้าที่ของบุคคลดังกล่าว ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังต่อไปนี้

### **1. เจ้าของข้อมูลส่วนบุคคล (Data Subject)**

เจ้าของข้อมูลส่วนบุคคล คือ บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล และหมายรวมถึงผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ หรือผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ ซึ่งเจ้าของข้อมูลก็มีสิทธิในข้อมูลของตนเองตามกฎหมาย และสามารถใช้สิทธินั้นได้โดยแบ่งออกได้ ดังนี้

- **สิทธิที่จะได้รับการแจ้งให้ทราบ** ถึงรายละเอียดในการเก็บข้อมูล การนำไปใช้ และการเผยแพร่ข้อมูลนั้นๆ ก่อนหรือขณะเก็บรวบรวมข้อมูล ไม่ว่าจะเป็นเรื่องของวัตถุประสงค์ การนำไปใช้ ระยะเวลาในการเก็บข้อมูล สถานที่ และวิธีการติดต่อกับผู้ควบคุมข้อมูลส่วนบุคคล ไปจนถึงผลกระทบที่อาจจะเกิดขึ้นจากการไม่ให้ข้อมูลอีกด้วย

- **สิทธิในการขอเข้าถึงข้อมูลส่วนบุคคล และขอรับสำเนาข้อมูลส่วนบุคคล** ที่เกี่ยวกับตนเองจากผู้ควบคุมข้อมูลส่วนบุคคลได้ แต่จะต้องไม่ขัดต่อกฎหมายหรือคำสั่งศาล และไม่ละเมิดสิทธิและเสรีภาพของบุคคลอื่น
- **สิทธิในการได้รับและโอนถ่ายข้อมูล** ในกรณีที่เจ้าของข้อมูลต้องการให้ผู้ควบคุมข้อมูลส่วนบุคคลรายแรกโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมรายอื่น ก็สามารถขอให้ผู้ควบคุมรายแรกจัดทำข้อมูลที่สามารถเข้าถึงหรือจัดทำข้อมูลในรูปแบบที่เข้าถึงได้ด้วยวิธีการอัตโนมัติ และโอนไปยังผู้ควบคุมรายอื่นได้ ซึ่งข้อมูลที่โอนไปนั้น เจ้าของข้อมูลก็ยังขอรับข้อมูลนั้นจากผู้ควบคุมข้อมูลรายแรกได้อีกด้วย แต่การใช้วิธีการนี้จะต้องไม่ขัดต่อกฎหมาย สัญญา หรือละเมิดสิทธิเสรีภาพของผู้อื่น
- **สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล** โดยร้องขอต่อผู้ควบคุมข้อมูลเมื่อไรก็ได้ โดยร้องขอผ่านแบบฟอร์มที่ผู้ให้บริการจัดไว้ หรือติดต่อกับผู้ดูแลระบบ
- **สิทธิในการขอให้ลบ หรือทำลายข้อมูลส่วนบุคคล** ในกรณีที่ข้อมูลส่วนบุคคลหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ หรือผู้ควบคุมนำข้อมูลไปเผยแพร่ในที่สาธารณะ หรือข้อมูลนั้นสามารถเข้าถึงได้ง่าย เจ้าของข้อมูลมีสิทธิขอให้ผู้ควบคุมลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนได้
- **สิทธิในการเพิกถอนความยินยอม** กรณีเจ้าของข้อมูลเคยให้ความยินยอมในการใช้ข้อมูลไป ต่อมาเกิดเปลี่ยนใจ ก็สามารถยกเลิกความยินยอมนั้นเมื่อไรก็ได้ โดยการยกเลิกจะต้องไม่ขัดต่อข้อจำกัดสิทธิในการถอนความยินยอมทางกฎหมาย หรือสัญญาที่ให้ประโยชน์แก่เจ้าของข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปก่อนหน้านี้
- **สิทธิในการขอระงับการใช้ข้อมูล** เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลระงับการใช้ข้อมูลได้ ไม่ว่าจะในกรณีที่เกิดเปลี่ยนใจไม่ต้องการให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อครบกำหนดที่ต้องทำลาย เพราะมีความจำเป็นต้องนำข้อมูลไปใช้ในทางกฎหมาย หรือการใช้สิทธิเรียกร้อง ก็สามารถทำได้
- **สิทธิขอให้แก้ไขข้อมูล** เจ้าของข้อมูลมีสิทธิที่จะขอแก้ไขข้อมูลส่วนบุคคลของตนเองให้มีความถูกต้องเป็นปัจจุบัน และไม่ก่อให้เกิดความเข้าใจผิดได้ โดยการแก้ไขนั้นจะต้องเป็นไปด้วยความสุจริต และไม่ขัดต่อหลักกฎหมาย
- **สิทธิในการร้องเรียน** เจ้าของข้อมูลมีสิทธิร้องเรียนต่อพนักงานเจ้าหน้าที่และคณะกรรมการตาม PDPA ได้ ถ้าผู้ควบคุม ผู้ประมวลผล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุม ผู้ประมวลผล ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย รวมถึงมีสิทธิในการเรียกค่าสินไหมทดแทนทางศาลด้วย

## 2. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

ผู้ควบคุมข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล โดยจะมีหน้าที่ในการดำเนินการตามมาตรา 37 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังต่อไปนี้

- จัดให้มีมาตรการในการรักษาความปลอดภัยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลให้ดี
- ดำเนินการป้องกันไม่ให้เกิดการใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม
- จัดให้มีการลบหรือทำลายข้อมูลส่วนบุคคลหลังจากพ้นระยะเวลาในการเก็บข้อมูล
- ในกรณีที่มีการละเมิดข้อมูลส่วนบุคคล ให้ผู้ควบคุมข้อมูลนั้นแจ้งต่อสำนักงานคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง นับตั้งแต่ทราบเรื่อง
- แต่งตั้งตัวแทนอยู่ในราชอาณาจักร

อีกทั้งผู้ควบคุมข้อมูลส่วนบุคคล ยังมีหน้าที่ในการดำเนินการตามมาตรา 39 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังต่อไปนี้

- บันทึกรายการข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูล เงื่อนไขบุคคล เงื่อนไขการเข้าถึง
- การใช้หรือการเปิดเผยตามมาตรา 27 วรรคสาม
- การปฏิเสธคำขอหรือการคัดค้าน
- คำอธิบายมาตรการการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1)

## 3. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

ผู้ประมวลผลข้อมูลส่วนบุคคล คือ บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล “ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล” ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล และมีหน้าที่ในการดำเนินการตามมาตรา 40 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังต่อไปนี้

- ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
- จัดมาตรการรักษาความปลอดภัยของข้อมูลที่เหมาะสม
- จัดทำ บันทึก และประมวลผลของข้อมูลส่วนบุคคลให้เหมาะสม

#### 4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล คือ บุคคลที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลส่วนบุคคล โดยที่จะต้องมีความรู้และความเข้าใจเกี่ยวกับกฎหมายข้อมูลส่วนบุคคลและประมวลผลข้อมูลองค์กร ซึ่งจะมีหน้าที่ในการดำเนินการตามมาตรา 42 แห่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ดังต่อไปนี้

- ให้คำแนะนำแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- ตรวจสอบและดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล
- รักษาความลับข้อมูลส่วนบุคคล
- กรณีมีปัญหาการเก็บรวบรวม ใช้ เปิดเผยข้อมูล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการจัดการปัญหาต่างๆ

ดังนั้นแล้ว ทุกท่านจะเห็นได้ว่า กฎหมาย PDPA เป็นกฎหมายที่มุ่งคุ้มครองสิทธิของเจ้าของ “ข้อมูลส่วนบุคคล” โดยการสร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้มีความปลอดภัย และถูกนำไปใช้อย่างถูกต้องประสงค์ตามที่เจ้าของข้อมูลส่วนบุคคลให้การอนุญาตไว้ อีกทั้งยังได้มีการกำหนดหน้าที่และความรับผิดชอบให้บุคคล หน่วยงาน และองค์กรที่จะต้องปฏิบัติตามที่กฎหมายบัญญัติเอาไว้ โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องมีการกำหนดนโยบายความปลอดภัยของข้อมูลส่วนบุคคลภายในองค์กรและให้ความรู้แก่บุคลากรในองค์กร และรู้ขอบเขตการเก็บรวบรวม การใช้ การเผยแพร่ข้อมูลส่วนบุคคล มีระบบการจัดเก็บข้อมูลส่วนบุคคลที่ปลอดภัย มีการจำกัดการเข้าถึงข้อมูลส่วนบุคคล และมีการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล เป็นต้น อีกทั้ง กฎหมาย PDPA ยังให้ความสำคัญต่อมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ความเป็นธรรมในการใช้ข้อมูล และความโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามหลักการคุ้มครองสิทธิความเป็นส่วนตัวตามที่กฎหมายบัญญัติไว้อีกด้วย