

สรุปลงประกาศ
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
“PDPA – Privacy for All”

- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ลงประกาศในราชกิจจานุเบกษาเมื่อวันที่ ๒๗ พฤษภาคม ๒๕๖๒
- หมวด ๑ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และหมวด ๔ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึง บทเฉพาะกาล ที่บัญญัติเกี่ยวกับการจัดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในวาระเริ่ม มีผลใช้บังคับตั้งแต่วันที่ ๒๘ พฤษภาคม ๒๕๖๒ เพื่อให้มีระยะเวลาการเตรียมความพร้อมในด้านการคุ้มครองข้อมูลของประเทศในภาพรวม
- บทบัญญัติในหมวดอื่นจะมีผลบังคับใช้ในวันที่ ๒๗ พฤษภาคม ๒๕๖๓
- บทเฉพาะกาล กำหนดให้ สป.ดศ. ทำหน้าที่ สำนักงานตามพระราชบัญญัตินี้ และ รมว.ดศ. แต่งตั้ง
รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่ เลขาธิการคณะกรรมการฯ

หลักการสำคัญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๑. ข้อมูลส่วนบุคคล (Personal Data)

- ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-สกุล , ที่อยู่ , เลขบัตรประชาชน , ข้อมูลสุขภาพ , หมายเลขโทรศัพท์ , e-mail , ประวัติอาชญากรรม เป็นต้น

๒. บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

● เจ้าของข้อมูลส่วนบุคคล (Data Subject)

ตามกฎหมายไม่ได้ให้คำนิยามไว้ แต่โดยหลักการทั่วไปแล้วหมายถึง บุคคลที่ข้อมูลนั้นระบุไปถึง

● ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

- บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ **ตัดสินใจ** เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐ หรือเอกชนโดยทั่วไป ที่เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนหรือลูกค้าที่มาใช้บริการ
- ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่สำคัญที่กฎหมายกำหนดไว้ เช่น จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล , ดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ , แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้สำนักงานคุ้มครองข้อมูลส่วนบุคคลทราบภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ , แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อตรวจสอบการทำงานของตน เป็นต้น

● ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

- บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล **ตามคำสั่งหรือในนาม**ของผู้ควบคุมข้อมูลส่วนบุคคล เช่น บริการ cloud service เป็นต้น
- ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่หลัก คือ ดำเนินการตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

๓. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวจะชอบด้วยกฎหมาย หากดำเนินการตามหลักการใด หลักการหนึ่ง ดังต่อไปนี้

● Consent

- เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- ต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- มีแบบหรือข้อความที่อ่านแล้วเข้าใจได้ง่าย และต้องไม่เป็นการหลอกลวง
- เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ ถ้าไม่มีข้อจำกัดสิทธิ เช่น มีกฎหมาย

ที่กำหนดให้เก็บรวบรวมข้อมูลส่วนบุคคลนั้นไว้ก่อน

● Scientific or Historical Research

- จัดทำเอกสารประวัติศาสตร์ , จดหมายเหตุ , การศึกษาวิจัย , สถิติ

- **Vital Interest**
 - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล เช่น การเข้ารับบริการทางการแพทย์ ณ โรงพยาบาล
- **Contract**
 - เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญา เช่น เจ้าของข้อมูลส่วนบุคคลทำสัญญากู้ยืมเงินจากธนาคาร ธนาคารสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ตามวัตถุประสงค์ของสัญญา
- **Public Task**
 - เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ เช่น หน่วยงานของรัฐจัดทำ Big Data เพื่อแก้ปัญหาความยากจนของเกษตรกร
- **Legitimate Interest**
 - เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่น เช่น บริษัทเอกชนติดตั้งกล้องวงจรปิดภายในอาคารเพื่อรักษาความปลอดภัย ซึ่งบริษัทสามารถเก็บรวบรวมภาพถ่ายซึ่งเป็นข้อมูลส่วนบุคคลของบุคคลที่อยู่ในบริเวณดังกล่าวได้
- **Legal Obligations**
 - เป็นการปฏิบัติตามกฎหมาย

นอกจากหลักการข้างต้นแล้ว มีข้อมูลส่วนบุคคลอีกประเภทซึ่งเรียกว่า **ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data)** เช่น เชื้อชาติ , ประวัติอาชญากรรม , ข้อมูลพันธุกรรม , พฤติกรรมทางเพศ เป็นต้น การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวจะมีหลักการที่เข้มงวดกว่าข้อมูลส่วนบุคคลทั่วไป โดยจะกระทำได้หากดำเนินการตามหลักการใดหลักการหนึ่ง เช่น ได้รับความยินยอมโดยชัดแจ้ง (Explicit Consent) จากเจ้าของข้อมูลส่วนบุคคล , เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ เป็นต้น

๔. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

- ประเทศปลายทางที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์ที่คณะกรรมการประกาศ

๕. สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right) เช่น

- **สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)**
 - เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล
- **สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล (Right to erasure (also known as right to be forgotten))**
 - เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ หากข้อมูลส่วนบุคคลที่หมดความจำเป็น หรือข้อมูลส่วนบุคคลที่ขอลอนความยินยอมแล้ว

๖. การร้องเรียน

- เจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิดข้อมูลส่วนบุคคลสามารถร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญ ซึ่งมีหน้าที่พิจารณาเรื่องร้องเรียนตามพระราชบัญญัตินี้ได้

๗. ความรับผิดและบทลงโทษ

๗.๑ ความรับผิดทางแพ่ง

- ผู้กระทำละเมิดข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนให้กับเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ก็ตาม
- ศาลมีอำนาจสั่งให้ชดใช้ค่าสินไหมทดแทนเพิ่มเติมได้สองเท่าของค่าสินไหมทดแทนที่แท้จริง

๗.๒ โทษอาญา

- กำหนดบทลงโทษทางอาญาไว้สำหรับความผิดร้ายแรง เช่น การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนโดยมิชอบ , ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นแล้วนำไปเปิดเผยแก่ผู้อื่นโดยมิชอบ
- ระวังโทษสูงสุดจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ
- ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล กรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นอาจต้องร่วมรับผิดในความผิดอาญาที่เกิดขึ้น

๗.๓ โทษทางปกครอง

- กำหนดโทษปรับทางปกครองสำหรับการกระทำความผิดที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามที่กฎหมายกำหนด เช่น ไม่แจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลส่วนบุคคลทราบ , ขอความยินยอมโดยหลอกลวงเจ้าของข้อมูลส่วนบุคคล , ไม่แต่งตั้ง DPO เป็นต้น
 - โทษปรับทางปกครองสูงสุด ๕,๐๐๐,๐๐๐ บาท
-