สาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

เลื่อนการบังคับใช้ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ออกไปจนถึงวันที่ 31 พ.ค. 2565 เหตุเพราะ ผลกระทบจากการแพร่ระบาดของโรคติดเชื้อโควิด-19 โดยที่กฎหมายมีรายละเอียดซับซ้อน ต้องใช้เทคโนโลยีขั้นสูง และมีบทลงโทษทั้งความรับผิดทางแพ่ง และโทษทางปกครองและอาญา ค่อนข้างแรง

กฎหมายที่เกี่ยวข้องและมีการคุ้มครองข้อมูลส่วนบุคคลอยู่

- พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544
- พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545
- พ.ร.บ. สุขภาพแห่งชาติ พ.ศ. 2550
- พ.ร.บ. กสทช. พ.ศ. 2553

โดยสาระสำคัญและข้อยกเว้นมีดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

พนักงาน ไม่ใช่ ผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคล ตามนิยามใน กม.แต่ พนักงานต้องปฏิบัติตามข้อกำหนดและหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตามที่องค์กรกำหนด

ตัวอย่างของข้อมูลส่วนบุคคล (Personal Data) ได้แก่ ชื่อ - นามสกุล, เลขประจำตัวประชาชน, ที่อยู่, เบอร์โทรศัพท์, วันเกิด, อีเมล, การศึกษา, เพศ, อาชีพ, รูปถ่าย, ข้อมูลทางการเงิน นอกจากนี้ยังรวมถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ด้วย เช่น ข้อมูลทางการแพทย์หรือสุขภาพ, ข้อมูลทางพันธุกรรมและไบโอเมทริกซ์, เชื้อชาติ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสหภาพแรงงาน เป็นต้น

สาระสำคัญของ พ.ร.บ. ฉบับนี้ มี 3 ประเด็นหลัก ดังนี้

1. เจ้าของข้อมูลต้องให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกแล้วเท่านั้น กล่าวคือ ต้องขออนุมัติจากเจ้าของข้อมูลก่อน เช่น หากแอปพลิชันหนึ่งจะเก็บข้อมูลบัตรเครดิตของเราไว้ในระบบ ก็ต้องมีข้อความให้เรากดยืนยันเพื่อยินยอม พร้อมแจ้งวัตถุประสงค์ในการเก็บรวบรวม และการใช้ หากเราไม่ยินยอมให้ใช้ข้อมูลบัตรเครดิต ผู้ให้บริการแอปพลิเคชันนั้นก็ไม่สามารถใช้ข้อมูลบัตรเครดิตของเราได้
2. ผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล เช่น สถานพยาบาลจะต้องเก็บข้อมูลของผู้ป่วยให้เป็นความลับและไม่เปิดเผยให้กับผู้อื่น ธนาคารต้องเก็บรักษาข้อมูลเกี่ยวกับรายการถอน
3. เจ้าของข้อมูลมีสิทธิ์ถอนความยินยอม ขอให้ลบหรือทำลายข้อมูลเมื่อใดก็ได้ หากเป็นความประสงค์ของเจ้าของข้อมูล

วัตถุประสงค์ของกฎหมายฉบับนี้

เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพโดยกำหนดหน้าที่และความรับผิดชอบที่เหมาะสม
เพื่อส่งเสริมการใช้ข้อมูลในการพัฒนานวัตกรรมอย่างมั่นคงปลอดภัย
เพื่อให้มีมาตรการเยียวยาจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ
เพื่อสร้างความโปร่งใสและเป็นธรรม ในการใช้ข้อมูลส่วนบุคคล

การเก็บข้อมูลส่วนบุคคล

-เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย
-ต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อน หรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังนี้

1.วัตถุประสงค์ของการเก็บรวบรวม
2.กรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลเพื่อปฏิบัติตามกฎหมายหรือสัญญา
3.ข้อมูลที่จะเก็บรวบรวมและระยะเวลาในการเก็บรวบรวม
4.ประเภทของบุคคลหรือหน่วยงานซึ่งมีข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
5.ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ
6.สิทธิของเจ้าของข้อมูลส่วนบุคคล

*****ข้อห้าม*****

ห้ามเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่ได้ทำการแจ้งเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 30 วัน นับตั้งแต่วันที่ทำการเก็บรวบรวมข้อมูลและได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นการเก็บรวลรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม

ข้อยกเว้นของกฎหมายฉบับนี้

1) การเก็บรวบรวม ใช้ หรือเปิดเผย เพื่อประโยชน์ส่วนตน หรือ เพื่อกิจกรรมในครอบครัวของบุคคลนั้น
2) การดำเนินการของหน่วยงานรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ความมั่นคงทางการคลังของรัฐ การรักษาความปลอดภัยของประชาชน การป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ การรักษาความมั่นคงปลอดภัยทางไซเบอร์
3) การเก็บรวบรวมเพื่อกิจการสื่อสารมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพ หรือเป็นประโยชน์สาธารณะเท่านั้น
4) สภาผู้แทนราษฎร วุฒิสภา รัฐสภา คณะกรรมาธิการ ตามอำนาจและหน้าที่ของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา และคณะกรรมาธิการ
5) การพิจารณาพิพากษาคดีของศาล การดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี การวางทรัพย์ การดำเนินงานตามกระบวนการยุติธรรมทางอาญา
6) การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

หลักการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป มาตรา 24 และ มาตรา 27

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวบรวมข้อมูลส่วนบุคคล โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่
1. เพื่อจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัย สถิติ (Scientific or research)
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต (Vital Interest)
3. มีความจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูล (Necessary for the performance of contracts)
4. มีความจำเป็นเพื่อดำเนินการเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูล (Public Task) หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบหมายแก่ผู้ควบคุมข้อมูลส่วนบุคคล
5. มีความจำเป็นในการดำเนินการเพื่อผลประโยชน์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูล แต่ต้องไม่ก่อให้เกิดการละเมินสิทธิและเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล (Legitimate Interest)
6. เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล (Legal Obligation)

หลักการ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลทั่วไป มาตรา 26 และ มาตรา 27

ห้ามมิให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

1. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
2. ป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ
3. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล
4. แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล ภายใน 72 ชม. นับแต่ทราบเหตุ
5. แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีเป็นผู้ควบคุมข้อมูลส่วนบุคคลต่างชาติ
6. จัดทำบันทึกรายการ (มาตรา 39)

หน้าที่ของผู้ประมวลข้อมูลส่วนบุคคล

1. ทำตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น
2. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
3. แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
4. จัดทำและเก็บรักษารายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
5. แต่งตั้งตัวแทนภายในราชอาณาจักร กรณีเป็นผู้ประมวลผลข้อมูลส่วนบุคคลต่างชาติ

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1.สิทธิขอเข้าถึงและขอรับส าเนา มาตรา 30 (Right of Access)

2.สิทธิขอให้โอนข้อมูล มาตรา 31 (Right to data portability)

3.สิทธิคัดค้าน มาตรา 32 (Right to object)

4.สิทธิขอให้ลบหรือท าลาย มาตรา 33 (Right to be forgotten)

5. สิทธิขอให้แก้ไขข้อมูลให้ถูกต้อง มาตรา 35 มาตรา 36 (Right to rectification)

6. สิทธิขอให้ระงับการใช้มาตรา 34 (Right to restrict processing)

การร้องเรียน ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

หน้าที่ของคณะกรรมการเชี่ยวชาญ มาตรา 72

1. พิจารณาเรื่องร้องเรียน

2. ตรวจสอบการกระทำใด ๆ ของผู้ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของ ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

3. ไกล่เกลี่ยข้อพิพาทเกี่ยวกับข้อมูลส่วนบุคคล

4. ออกคำสั่งให้ปฏิบัติหรือดำเนินการแก้ไขการกระทำ/สั่งห้ามกระทำการเพื่อระงับความเสียหาย

หน้าที่ของพนักงานเจ้าหน้าที่ มาตรา 76

1.มีหนังสือแจ้งให้บุคคลมาให้ข้อมูล หรือส่งเอกสารหรือหลักฐานใด ๆ

2. ตรวจสอบและรวบรวมข้อเท็จจริง แล้วรายงานต่อคณะกรรมการผู้เชี่ยวชาญ

บทลงโทษ

ความรับผิดทางแพ่ง

ค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

โทษทางปกครอง

- ไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ ไม่จัดทำบันทึกรายการ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของ DPO เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่ได้แจ้งวัตถุประสงค์การใช้งานใหม่ เก็บข้อมูลเกินความจ าเป็น

- ขอความยินยอมที่เป็นการหลอกลวงให้เข้าใจผิด ไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่แจ้งเหตุเมื่อมีการละเมิดข้อมูล โอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย ไม่ตั้งตัวแทนในราชอาณาจักร โทษปรับไม่เกิน 3,000,000 บาท โทษปรับไม่เกิน 1,000,000 บาท

- เก็บรวบรวม ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย โทษปรับไม่เกิน 5,000,000 บาท

โทษอาญา

-ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบ

ด้วยกฎหมายทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย จำคุก < 6 เดือน หรือปรับ < 500,000 บาท
เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น จำคุก < 1 ปี หรือปรับ < 1,000,000 บาท

-ผู้ใด ล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตามพ.ร.บ.นี้ ห้ามนำไปเปิดเผยแก่ผู้อื่น เว้นแต่เปิดเผยตามหน้าที่ หรือเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี หรือได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือเปิดเผยให้หน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย หรือข้อมูลคดีต่างๆ ที่เปิดเผยต่อสาธารณะ จำคุก < 6 เดือน หรือปรับ < 500,000 บาท

-ผู้กระทำความผิดที่เป็นนิติบุคคล หากกรรมการหรือผู้จัดการ หรือ บุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น สั่งการหรือกระทำหรือละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิดต้องรับโทษในส่วนที่กำหนดโทษอาญาไว้ด้วย

ข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนวันที่ พ.ร.บ. นี้ใช้บังคับ

- ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม

- ต้องกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย

- การเปิดเผยและการดำเนินการอื่นที่มิใช่การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัตินี้