กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

โดย ดรณภา สุกกรี[1] สมัญญา ถาวรศักดิ์ และบูชิตา มานตรี[2]

ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ซึ่งในโลกยุคปัจจุบัน ข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งข้อมูลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ผ่านการทำธุรกรรมออนไลน์ การลงชื่อเข้าใช้โปรแกรมคอมพิวเตอร์และสื่อโซเชียล โดยรวมถึงข้อมูลส่วนบุคคลที่ได้ให้ไว้กับหน่วยงานของรัฐและภาคเอกชนเมื่อมีการขอใช้บริการ โดยข้อมูลส่วนบุคคลได้ถูกนำมาใช้ตรวจสอบ วิเคราะห์ ประเมินผล เปิดเผยข้อมูลส่วนบุคคล และมีการนำไปใช้หาผลประโยชน์ในทางธุรกิจโดยปราศจากการรับรู้ของผู้ที่เป็นเจ้าของข้อมูลซึ่งเป็นการละเมิดต่อสิทธิความเป็นส่วนตัวของปัจเจกชนที่เป็นเจ้าของข้อมูล นอกจากนี้ การเปิดเผยข้อมูลนอกจากจะเป็นการละเมิดความเป็นส่วนตัวก่อให้เกิดความเดือดร้อนรำคาญแล้วยังอาจส่งผลต่อความปลอดภัยและทรัพย์สินแก่ผู้เป็นเจ้าของข้อมูลเนื่องจากอาจถูกแสวงประโยชน์โดยกลุ่มองค์กรอาชญากรรม

การคุ้มครองข้อมูลส่วนบุคคลได้ถูกกำหนดไว้ในปฏิญญาสากลว่าด้วนสิทธิมนุษยชนของสหประชาชาติ ซึ่งนำไปสู่ความตกลงระหว่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลหลายฉบับ เช่น การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) ข้อตกลงสหภาพยุโรป และการคุ้มครองข้อมูลส่วนบุคคลตามข้อบังคับสหภาพยุโรป (European Union Directive 95/46/EC) ซึ่งเป็นกฎหมายที่มีผลบังคับใช้มากว่า 20 ปีแล้ว และด้วยการเปลี่ยนแปลงของเทคโนโลยีที่มีผลต่อวิถีชีวิตของประชาชนมากขึ้น ส่งผลให้ในทุกธุรกรรมออนไลน์ไม่ว่าจะโดยตั้งใจหรือมิได้ตั้งใช้มีการทิ้งร่องรอยดิจิตัล (Digital Footprint) เอาไว้ โดยข้อมูลส่วนตัวเหล่านี้ถูกนำไปวิเคราะห์ ประเมินผล และนำมาใช้เป็นเครื่องชี้นำพฤติกรรมผู้บริโภค (Marketing Manipulation) หรือการชี้นำการตัดสินใจทางการเมืองของบุคคลเฉพาะกลุ่มเป้าหมาย (Political Microtargeting) ทำให้สหภาพยุโรปออกกฎหมายฉบับใหม่เกี่ยวกับการคุ้มครองข้อมูล (EU General Data Protection Regulation) หรือ “GDPR” ซึ่งมีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2561 โดย GDPR ของสหภาพยุโรปเป็นมาตรฐานการรับรองข้อมูลส่วนบุคคลใหม่ของโลก โดยบทบัญญัติของกำหนดให้ขอความยินยอมจากเจ้าของข้อมูลอย่างชัดเจนและชัดแจ้ง ต้องทำการแจ้งเตือนเมื่อข้อมูลรั่วไหล กำหนดให้ผู้ควบคุมข้อมูลจะต้องแจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลจะมีการใช้ไปอย่างไร เพื่อวัตถุประสงค์ใด กำหนดรับรองสิทธิที่จะถูกลืมโดยขอให้หน่วยงานควบคุมข้อมูลลบข้อมูลของตนได้ และการใช้อำนาจนอกอาณาเขต (Extraterritorial Jurisdiction) เป็นการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปไม่ว่าจะอยู่ที่ใดในโลกซึ่งส่งผลสำคัญ ส่งผลให้ผู้ประกอบการที่ทำธุรกิจกับ

[1] นิติศาสตร์บัณฑิต (เกียรตินิยมอันดับสอง), LL.M. (International and Comparative Law)

[2] นิติศาสตร์บัณฑิต

สหภาพยุโรปรวมถึงผู้ประกอบการไทยจะต้องปฏิบัติตามมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลและมาตรการความปลอดภัยทางไซเบอร์ตามที่ GDPR กำหนด

ประเทศไทยมีกฎหมายที่ให้การคุ้มครองข้อมูลส่วนบุคคลหลายฉบับ ดังต่อไปนี้

- ***รัฐธรรมนูญแห่งราชอาณาจักรไทย*** ที่ได้กำหนดรับรองคุ้มครองสิทธิของบุคคล เกียรติยศหรือชื่อเสียง และความเป็นอยู่ส่วนตัว
- ***ประมวลกฎหมายอาญา*** มาตรา 264 (ความผิดฐานปลอมเอกสาร) เป็นการคุ้มครองข้อมูลส่วนบุคคลในขั้นตอนการจัดเก็บข้อมูล
- ***พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540*** เป็นกฎหมายที่บัญญัติเรื่องข้อมูลข่าวสารที่อยู่ในอำนาจหน้าที่ของหน่วยงานราชการโดยกำหนดห้ามมิให้หน่วยงานของรัฐห้ามเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่เป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร และต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นพยายามเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง และต้องมีการจัดระบบรักษาความปลอดภัยให้แก่ข้อมูลข่าวสารส่วนบุคคล
- ***พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540*** เป็นกฎหมายที่บัญญัติเรื่องข้อมูลข่าวสารที่อยู่ในอำนาจหน้าที่ของ**หน่วยงานราชการ** ได้มีบทบัญญัติให้หน่วยงานของรัฐห้ามเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่เป็นการรุกล้ำสิทธิส่วนบุคคลโดยไม่สมควร[3] และต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นพยายามเก็บข้อมูลจากเจ้าของข้อมูลโดยตรง และต้องมีการจัดระบบรักษาความปลอดภัยให้แก่ข้อมูลข่าวสารส่วนบุคคล[4]
- ***พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545*** เป็นกฎหมายที่บัญญัติเรื่องข้อมูลที่เกี่ยวข้องกับการประกอบธุรกิจเครดิต โดยได้บัญญัติให้ห้ามจัดเก็บข้อมูลของบุคคลธรรมดาที่ไม่เกี่ยวกับการรับบริการ การขอสินเชื่อหรือที่มีผลกระทบต่อความรู้สึก หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน คือ (1) ลักษณะพิการทางร่างกาย (2) ลักษณะทางพันธุกรรม (3) ข้อมูลของบุคคลที่อยู่ในกระบวนการสอบสวนหรือพิจารณาคดีอาญา (4) ข้อมูลอื่นที่คณะกรรมการกำหนด[5] และต้องจัดให้มีระบบรักษา

[3] มาตรา 15 (5) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

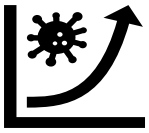
[4] มาตรา 23 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

[5] มาตรา 3 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

ความลับและความปลอดภัยของข้อมูลอีกด้วย[6] โดยในการเปิดเผยข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนทุกครั้ง[7]

- ***ประมวลกฎหมายแพ่งและพาณิชย์ลักษณะละเมิด*** มาตรา 420 ซึ่งการละเมิดนั้นต้องมีความเสียหายเกิดขึ้น
- ***พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*** ต้องเป็นการใช้งานผ่าน “ระบบคอมพิวเตอร์” ทำให้กฎหมายฉบับนี้ยังไม่สามารถนำไปปรับใช้แก่กรณีการใช้อุปกรณ์อิเล็กทรอนิกส์อื่น ๆ

กฎหมายดังกล่าวข้างต้นยังมิใช่กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีผลใช้บังคับเป็นการทั่วไป[8]เนื่องจากมิได้ให้ความคุ้มครองข้อมูลส่วนบุคคลอย่างคลอบคลุมและยังไม่ได้มาตรฐานสากล ต่อมา **จึงได้มีการตรา** **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (มีผลบังคับใช้เมื่อวันที่ 27 พฤกษภาคม 2563) และได้กำหนดให้บทบัญญัติในส่วนที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และการลงโทษทางอาญาและมาตรการทางปกครองตามที่กำหนดในกฎหมายฉบับนี้มีผลบังคับใช้นับตั้งแต่วันที่ 1 มิถุนายน 2564 เป็นต้นไป**



นอกจากนี้ ด้วยสถานการณ์การแพร่ระบาดโรคติดเชื้อไวรัสโคโรนาสายพันธุ์ใหม่ 2019 (โควิด – 19) ส่งผลให้หน่วยงานภาครัฐและเอกชนไม่สามารถปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ”) ดังกล่าวได้อย่างเคร่งครัด ดังนั้น ในวันที่ 20 พฤษภาคม 2563 จึงได้มีการออก *พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563*[9] กำหนดยกเว้นให้ 22 หน่วยงานและกิจการ[10] ไม่อยู่ในบังคับ

---

[6] มาตรา 17 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

[7] มาตรา 20 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

[8] สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, ความเป็นมาของกฎหมายคุ้มครองข้อมูลข่าวสารในประเทศไทย, สืบค้นเมื่อ 22 กุมภาพันธ์ 2564 โปรดดู http://www.oic.go.th/FILEWEB/CABIWEBSITE/DRAWER01/GENERAL/DATA0024/00024967.PDF

[9] พระราชกฤษฎีกา กำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563 โปรดดู http://www.ratchakitcha.soc.go.th/DATA/PDF/2563/A/037/T_0001.PDF

[10] หน่วยงานและกิจการที่ ไม่อยู่ในบังคับของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นการชั่วคราว (ระหว่างวันที่ 27 พฤกษภาคม 2563 - 31 พฤกษภาคม 2564) คือ (1) หน่วยงานของรัฐ (2) หน่วยงานของรัฐต่างประเทศและองค์การระหว่างประเทศ (3) มูลนิธิ สมาคม องค์กรศาสนา และองค์กรไม่แสวงหากำไร (4) กิจการด้านเกษตรกรรม (5) กิจการด้านอุตสาหกรรม (6) กิจการด้านพาณิชยกรรม (7) กิจการด้านการแพทย์และสาธารณสุข (8) กิจการด้านพลังงาน ไอน้ำ น้ำ และการกำจัดของเสีย รวมทั้งกิจการที่เกี่ยวข้อง (9) กิจการด้านการก่อสร้าง (10) กิจการด้านการซ่อมและการบำรุงรักษา (11) กิจการด้านการคมนาคม ขนส่ง และการเก็บสินค้า (12) กิจการด้านการท่องเที่ยว (13) กิจการด้านการสื่อสาร โทรคมนาคม คอมพิวเตอร์ และดิจิทัล (14) กิจการด้านการเงิน การธนาคาร และการประกันภัย (15) กิจการด้านอสังหาริมทรัพย์ (16) กิจการด้านการประกอบวิชาชีพ (17) กิจการด้านการบริหารและบริการสนับสนุน (18) กิจการด้านวิทยาศาสตร์และเทคโนโลยี วิชาการ สังคมสงเคราะห์ และศิลปะ (19) กิจการด้านการศึกษา (20) กิจการด้านความบันเทิงและนันทนาการ (21) กิจการด้านการรักษาความปลอดภัย และ (22) กิจการในครัวเรือนและวิสาหกิจชุมชน ซึ่งไม่สามารถจำแนกกิจกรรมได้อย่างชัดเจน

ของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เป็นการชั่วคราวเป็นเวลา 1 ปี (ระหว่างวันที่ 27 พฤกษภาคม 2563 – 31 พฤษภาคม 2564) อย่างไรก็ตาม หากปรากฏว่าในช่วงระยะเวลาที่มีการทุเลาการบังคับกฎหมายนี้ หากหน่วยงานและกิจการทั้ง 22 ประเภท ได้มีใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยไม่มีเหตุที่ชอบด้วยกฎหมาย หรือนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย โดยประการที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย อาจต้องรับผิดชดใช้ค่าเสียหายทางละเมิด แต่ยังไม่ได้ต้องรับผิดทางอาญาและทางปกครองตามที่กำหนดใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

สาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act (PDPA) ประกาศใช้เมื่อวันที่ 24 พฤษภาคม 2562 แต่ได้กำหนดให้หมวดที่สำคัญซึ่งเกี่ยวกับเนื้อหาการคุ้มครองข้อมูลส่วนบุคคลและการกำหนดโทษกรณีที่มีการละเมิดกฎหมายให้มีผลบังคับใช้อย่างเป็นทางการในวันที่ 1 มิถุนายน 2564

กิจกรรมที่ไม่อยู่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

กิจกรรมของการเก็บรวบรวมข้อมูลข่าวสารดังต่อไปนี้ไม่อยู่ในการบังคับของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ[11]

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัว
- การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐ หรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
- บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะ
- สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมาธิการที่แต่งตั้งโดยสภาดังกล่าวซึ่งเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมาธิการ แล้วแต่กรณี
- การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

[11] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 4

- การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิตและสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ขอบเขตการใช้บังคับ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ให้ใช้บังคับแก่ การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลสส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล**ที่อยู่ในราชอาณาจักร** ไม่ว่าการเก็บรวบรวม ใช้ เปิดเผย ได้กระทำในหรือนอกราชอาณาจักร และถึงแม้ว่าผู้ควบคุมข้อมูลส่วนบุคคล หรือ ผู้ประมวลผลข้อมูลส่วนบุคคลอยู่จะนอกราชอาณาจักร แต่ถ้าหากเป็นการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล**ของเจ้าของข้อมูลที่อยู่ในราชอาณาจักร** เมื่อเป็นการทำกิจกรรมในเรื่อง การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม รวมถึงการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร การเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลนั้นก็ให้อยู่ในบังคับของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ[12]

ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งสามารถทำให้ระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลได้ ไม่ว่าโดยทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ[13]

การประมวลผลข้อมูล คือ การดำเนินการหรือชุดการดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่[14]

บุคคลที่อยู่ภายใต้พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

บุคคลที่อยู่ภายใต้พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มีดังนี้

- เจ้าของข้อมูล คือ บุคคลธรรมดาที่ข้อมูลนั้นบ่งชี้ไปถึง
- ผู้ควบคุมข้อมูล คือ ผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล
- ผู้ประมวลผลข้อมูล คือ ผู้ที่ประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล

[12] มาตรา 5 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[13] มาตรา 6 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[14] ปิยะบุตร บุญอร่ามเรือง,พัฒนาพร โกวพัฒนกิจ,พีรพัฒ โชคสุวัฒนสกุล,เสกสิริ นิวัติศัยวงศ์,ปิติ เอี่ยมจำรูญลาภ,ชวิน อุ่นภัทร,ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล, ภูมิศิริ ดำรงวุฒิ,โมกข์พิศุทธิ์ รตารุณ, แนวปฏิบัติคุ้มครองข้อมูลส่วนบุคคล (พิมพ์ครั้งที่ 1 สำนักพิมพ์โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย 2563)

การขอความยินยอม

ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการประมวลผลข้อมูลส่วนบุคคลได้ก็ต่อเมื่อ เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้ก่อนหรือขณะนั้น

เนื้อหาของความยินยอม (Consent)	วิธีการขอความยินยอม
- ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูล - วัตถุประสงค์การประมวลผล - ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้ - วิธีการประมวลผลข้อมูล - การโอนข้อมูลไปต่างประเทศ - การเปิดเผยข้อมูลต่อบุคคลอื่น - ระยะเวลาในการจัดเก็บข้อมูล - วิธีการถอนความยินยอม - สิทธิต่าง ๆ ของเจ้าของข้อมูล	- ความยินยอมต้องชัดแจ้ง - ต้องแยกออกจากส่วนอื่นโดยชัดเจน - แบบหรือข้อความต้องเข้าใจง่ายและเข้าถึงได้ - หลีกเลี่ยงกรณีที่ความยินยอมเป็นเงื่อนไขในการบริการ โดยต้องคำนึงถึงความเป็นอิสระในการตัดสินใจให้ความยินยอมของเจ้าของข้อมูล - หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับกรณีใดบ้าง - ออกรูปแบบให้สามารถถอนความยินยอมได้โดยง่าย (ไม่กระทบถึงข้อมูลที่ได้ให้ความยินยอมไปแล้ว) - คำนึงถึงอายุของผู้ให้ความยินยอม (โดยเฉพาะกรณีผู้เยาว์) รวมถึงกรณีของผู้ไร้ความสามารถ และผู้เสมือนไร้ความสามารถ (มาตรา 20)

การขอความยินยอมจะต้องเป็นไปตามหลักเกณฑ์ที่กำหนดไว้ดังกล่าว ดังนั้นถ้าหากฝ่าฝืน ไม่มีผลผูกพันเจ้าของข้อมูล ในกรณีของเจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์หากเป็นกรณีที่ผู้เยาว์อาจให้ความยินยอมได้โดยลำพัง ผู้เยาว์ไม่จำเป็นต้องขอความยินยอมจากผู้ใช้อำนาจปกครอง แต่ผู้เยาว์ซึ่งมีอายุไม่เกิน 10 ปี ผู้ใช้อำนาจปกครองต้องเป็นผู้ให้ความยินยอมแทนผู้เยาว์[15] โดยในการให้ความยินยอมนั้น เจ้าของข้อมูลจะ**ถอนความยินยอมเสียเมื่อใดก็ได้** ซึ่งการถอนความยินยอมจะต้องทำได้โดยง่ายเช่นเดียวกับการให้ความยินยอม เว้นแต่มีข้อจำกัดโดยกฎหมายหรือสัญญา แต่อย่างไรก็ตามการถอนความยินยอมไม่กระทบถึงการประมวลผลข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไปแล้ว[16]

[15] มาตรา 20 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[16] มาตรา 19 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน้าที่ของผู้ควบคุมข้อมูล

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ ผู้ที่สามารถกำหนดวัตถุประสงค์ ตลอดจนวิธีการดำเนินการต่าง ๆ ของข้อมูลส่วนบุคคลได้ โดยหลักการสำคัญของการประมวลผลข้อมูล คือ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการประมวลผลข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูลและเจ้าของข้อมูลได้ให้ความยินยอมในการประมวลผลข้อมูลตามวัตถุประสงค์นั้น[17] ซึ่งก่อนเริ่มการประมวลผลข้อมูลนั้น ผู้ควบคุมข้อมูลจะต้องแจ้งเจ้าของข้อมูลก่อนหรือขณะเก็บข้อมูล ถึงรายละเอียดต่อไปนี้[18]

- ชื่อหรือรายละเอียดการติดต่อองค์กรผู้ควบคุมและตัวแทน (ถ้าหากมี)
- วัตถุประสงค์ในการเก็บข้อมูลส่วนบุคคล
- ฐานที่ชอบด้วยกฎหมายของการประมวลผลข้อมูล
- ประเภทของข้อมูลที่ได้รับ
- บุคคลที่ 3 ที่เป็นผู้รับข้อมูล
- รายละเอียดการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่ 3 ที่ต่างประเทศหรือองค์การระหว่างประเทศ (ถ้าหากมี)
- ระยะเวลาในการจัดเก็บ
- สิทธิต่าง ๆ ของเจ้าของข้อมูล
- แหล่งที่มาของข้อมูล (กรณีที่ได้รับข้อมูลมาจากแหล่งอื่น)

การเก็บบันทึกรายการประมวลผลข้อมูล ต้องมีรายการดังต่อไปนี้[19]

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูล
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล
- ระยะเวลาในการเก็บข้อมูล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขของบุคคลและการเข้าถึงของข้อมูลส่วนบุคคล
- การใช้หรือเปิดเผยข้อมูล
- การปฏิเสธคำขอ หรือการคัดค้านของเจ้าของข้อมูล
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

[17] มาตรา 21 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[18] มาตรา 23 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[19] มาตรา 39 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในการประมวลผลข้อมูล ผู้ควบคุมข้อมูลจะต้องจัดให้มี**มาตรการรักษาความปลอดภัยที่เหมาะสม** โดยในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลอื่นต้องป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยโดยปราศจากอำนาจโดยมิชอบ อีกทั้งต้องมีการจัดให้ระบบตรวจสอบข้อมูลเพื่อลบหรือทำลายเมื่อข้อมูลส่วนบุคคลนั้นไม่มีความจำเป็นหรือสิ้นระยะเวลาการจัดเก็บ และเมื่อมีเหตุละเมิดข้อมูลส่วนบุคคลจะต้องแจ้งการละเมิดข้อมูลส่วนบุคคลโดยไม่ชักช้า[20] ซึ่งผู้ควบคุมข้อมูลยังมีหน้าที่ในการดำเนินการให้ข้อมูลนั้นถูกต้อง สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด[21]

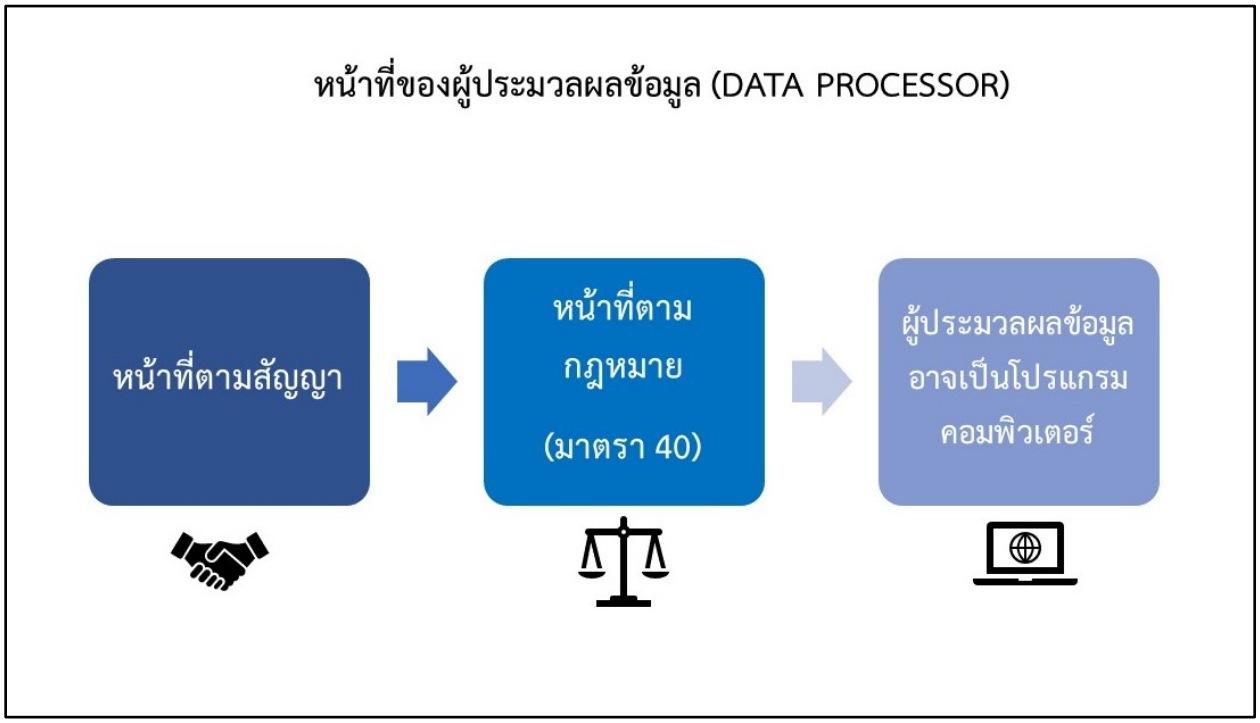
แผนภาพแสดงหน้าที่ของผู้ควบคุมข้อมูล

[20] มาตรา 37 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[21] มาตรา 35 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน้าที่ของผู้ประมวลผลข้อมูล

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ดำเนินการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล โดยผู้ประมวลผลข้อมูลมีหน้าที่ตามสัญญาจะต้องประมวลผลข้อมูลตามข้อตกลงหรือคำสั่งระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูล นอกจากนั้นยังมีหน้าที่ตามกฎหมายที่จะต้องประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล และจัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม รวมถึงการจัดทำและเก็บรักษาบันทึกกิจกรรมการประมวลผลข้อมูล[22] ซึ่งในการทำสัญญาว่าจ้างผู้ประมวลผลข้อมูลนั้นควรทำข้อตกลงเรื่องการประมวลผลข้อมูลแยกออกมาให้ชัดเจน



แผนภาพแสดงหน้าที่ของผู้ประมวลผลข้อมูล

[22] มาตรา 40 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

การประมวลผลข้อมูล

ก่อนการประมวลผลข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเสียก่อน และจะต้องทำการประมวลผลข้อมูลภายในวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมเท่านั้น เว้นแต่ในกรณีดังต่อไปนี้ ***ไม่จำต้องขอความยินยอม***จากเจ้าของข้อมูลก่อนการประมวลผลข้อมูล[23]

- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุ เพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูล (ตามที่คณะกรรมการกำหนด)
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา
- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล
- เป็นการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

การเก็บข้อมูลอ่อนไหว

ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว (Sensitive data) ได้แก่ ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดทำนองเดียวกันตามที่คณะกรรมการกำหนด ซึ่งการเก็บ**ข้อมูลอ่อนไหวจะต้องได้รับความยินยอมโดยชัดแจ้งเสียก่อน** เว้นแต่กรณี ดังต่อไปนี้[24]

- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลไม่สามารถให้ความยินยอมได้

[23] มาตรา 24 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[24] มาตรา 26 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสภาพแรงงาน ให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่อย่างสม่ำเสมอกับมูลนิธิ โดยไม่เปิดเผยข้อมูลยังภายนอก
- เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูล
- เป็นการจำเป็นเพื่อการก่อตั้ง ปฏิบัติ การใช้ หรือการยกข้อต่อสู้ซึ่งสิทธิเรียกร้องตามกฎหมาย
- เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การแพทย์ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ หรือประโยชน์สาธารณะด้านการสาธารณสุข หรือการคุ้มครองแรงงาน การประกันสังคม หรือการศึกษาวิจัย หรือประโยชน์สาธารณะสำคัญ

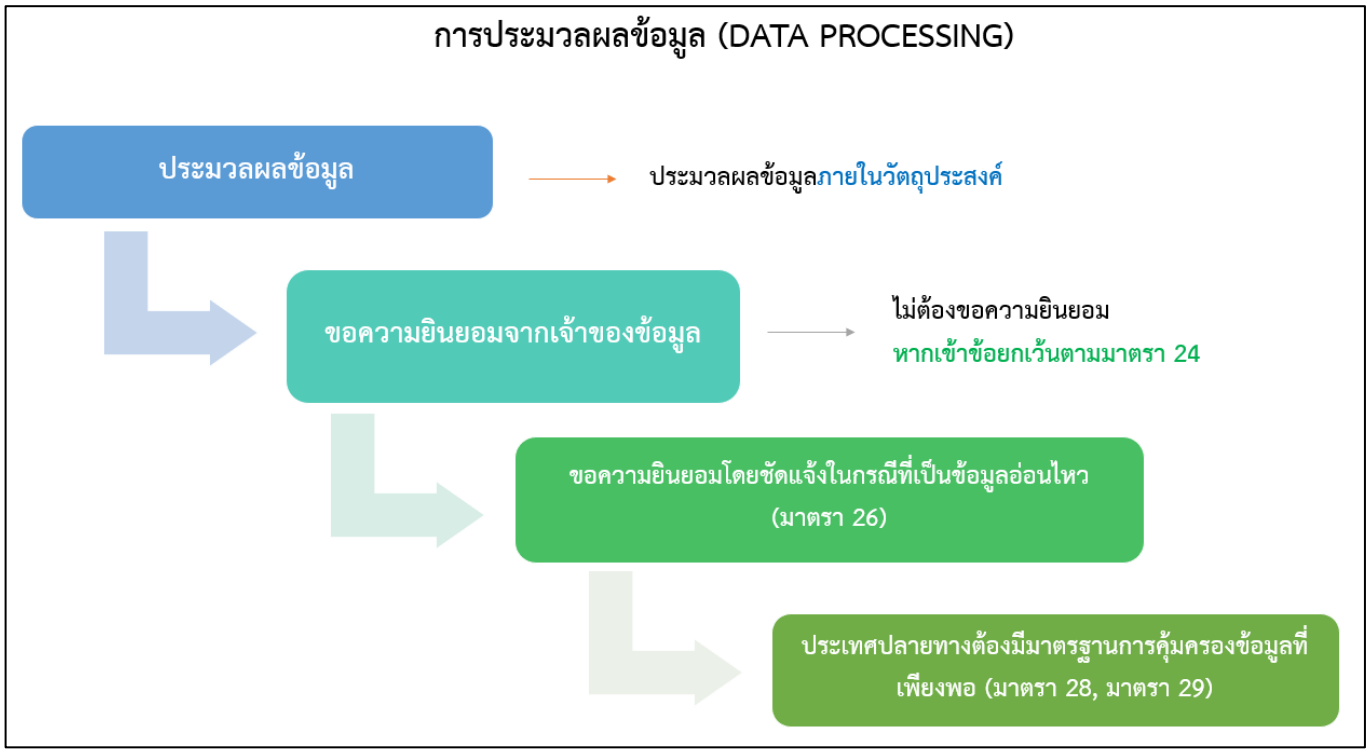
การส่งข้อมูลไปยังต่างประเทศ

ในกรณีที่มีการส่งข้อมูลไปยังต่างประเทศ ประเทศปลายทางนั้นจะต้องมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ เว้นแต่เป็นการปฏิบัติตามกฎหมาย หรือเจ้าของข้อมูลทราบถึงมาตรการที่ไม่เพียงพอของประเทศปลายทางและได้ให้ความยินยอม หรือเป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาหรือตามคำขอของเจ้าของข้อมูล หรือเป็นการกระทำตามสัญญาเพื่อประโยชน์ของเจ้าของข้อมูล หรือเพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย สุขภาพของเจ้าของข้อมูล ซึ่งไม่สามารถให้ความยินยอมได้ในขณะนั้น หรือเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะเป็นสำคัญ[25]

นอกจากนั้น**เจ้าของข้อมูลยังมีสิทธิ**ในการเข้าถึงและขอรับสำเนาข้อมูล ขอรับข้อมูลที่เกี่ยวกับตนในรูปแบบอิเล็กทรอนิกส์ คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่เกี่ยวกับตนเมื่อใดก็ได้ ขอให้ลบ ทำลาย หรือทำให้เป็นข้อมูลที่ไม่สามารถระบุตัวตนได้ หรือขอให้ระงับการใช้ข้อมูล[26]

[25] มาตรา 28 และมาตรา 29 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

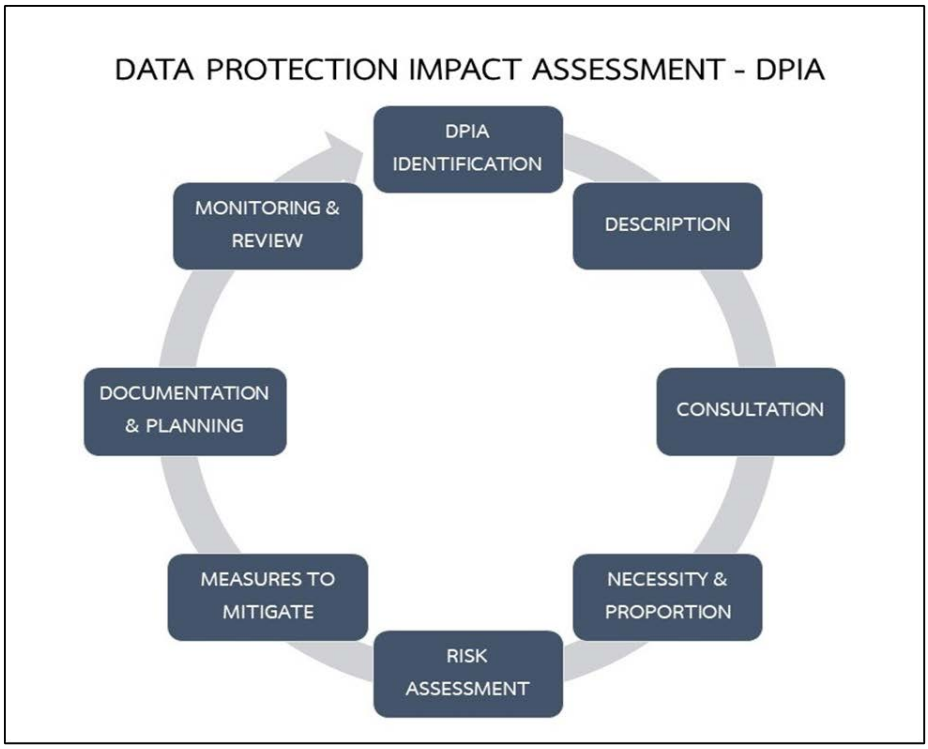
[26] มาตรา 30 – 34 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



แผนภาพแสดงการประมวลผลข้อมูล

ขั้นตอนการดำเนินการเมื่อข้อมูลมีความเสี่ยงสูงส่งผลกระทบต่อสิทธิเสรีภาพของบุคคล (Data Protection Impact Assessment หรือ DPIA)

การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล หรือ DPIA เป็นกระบวนการที่มีการพัฒนาขึ้นมาและเป็นที่ยอมรับในสากล สำหรับการประเมิน**ข้อมูลที่มีความเสี่ยงสูง**ที่จะกระทบต่อสิทธิเสรีภาพของบุคคล เพื่อการมีขั้นตอนที่เหมาะสมสำหรับการประมวลผลข้อมูลนั้น โดยการที่จะประเมินผลข้อมูลใดว่าเป็นข้อมูลที่มีความเสี่ยงสูงหรือไม่ ไม่ได้พิจารณาถึงแต่มีเพียงสภาพของข้อมูลเท่านั้น แต่จำต้องพิจารณาถึงสภาพในการเข้าถึงข้อมูลดังกล่าวด้วย เช่น บุคคลทั่วไปในองค์กรที่ไม่มีความเกี่ยวข้องใดกับการประมวลผลข้อมูล สามารถเข้าถึงข้อมูลได้หรือไม่ ตัวอย่างเช่น ถึงแม้เป็นข้อมูลเลขประจำตัวประชาชนของเจ้าของข้อมูล แต่ได้มีการกำหนดระดับของผู้ที่สามารถเข้าถึงข้อมูลได้ โดยผู้ที่จะเข้าถึงข้อมูลได้ต้องใส่รหัสในการเข้าถึงข้อมูล เช่นนี้ก็เป็นข้อมูลที่ไม่มีความเสี่ยงสูง เพราะบุคคลทั่วไปไม่สามารถเข้าถึงข้อมูลได้ เป็นต้น



แผนภาพแสดงขั้นตอนการจัดทำ DPIA

ขั้นตอนการดำเนินการตาม DPIA

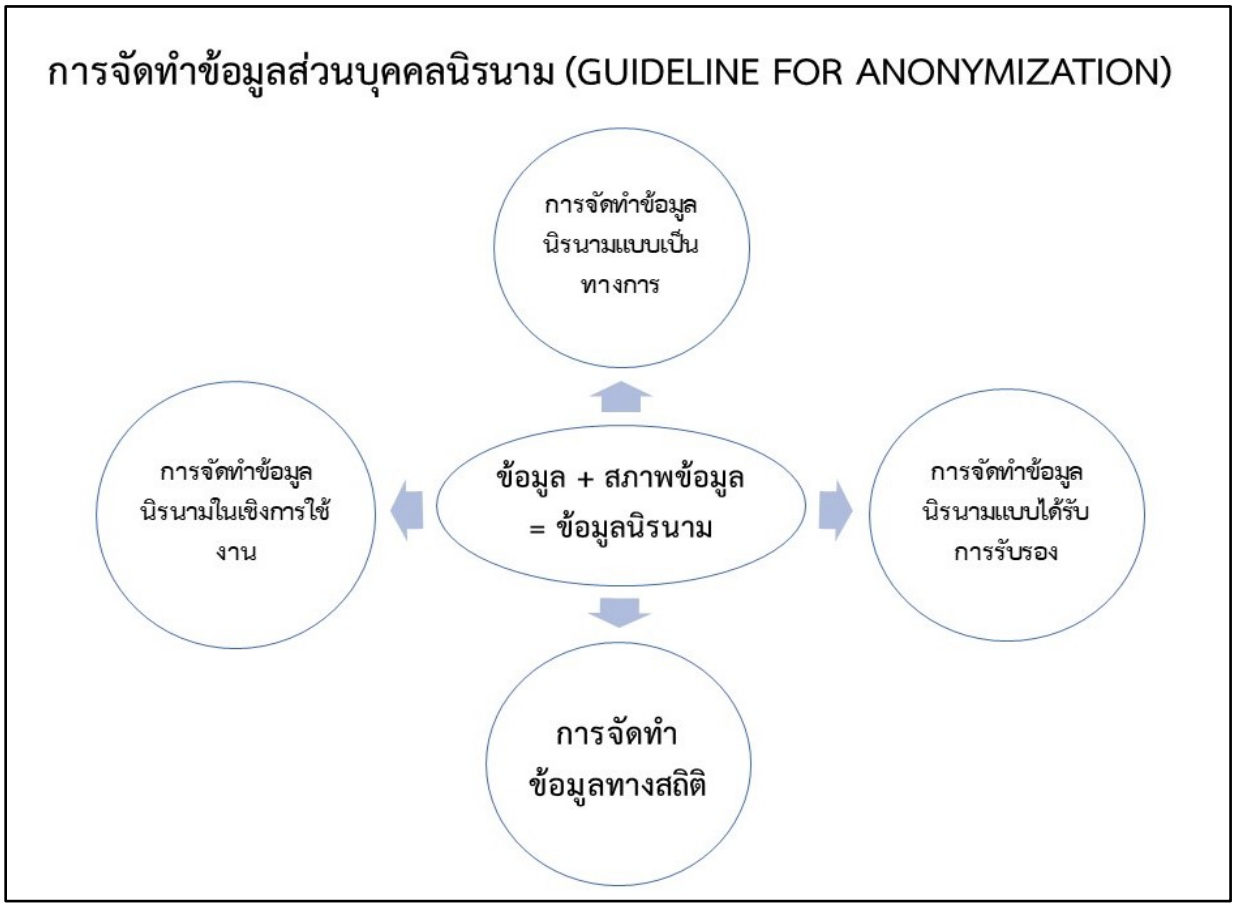
1. ประเมินว่าเป็นข้อมูลที่มีความเสี่ยงสูงหรือไม่ (DPIA Identification)
2. อธิบายรายละเอียดการประมวลผลข้อมูล (Description)
3. ฟังความเห็นของผู้ที่เกี่ยวข้อง (Consultation)
4. แสดงให้เห็นถึงความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล (Necessity & Proportion)
5. ประมวลผลความเสี่ยงของผลกระทบในการประมวลผลข้อมูล ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน (Risk Assessment)
6. ระบุมาตรการลดความเสี่ยง (Measures to mitigate)
7. สรุปการจัดทำ DPIA โดยควรจะต้องบันทึกรายละเอียดที่ผ่านมา (Documentation & Planning)ติดตามและทบทวนผลของการทำ DPIA (Monitoring & Review)
8. ติดตามและทบทวนผลของการทำ DPIA (Monitoring & Review)

การจัดทำข้อมูลส่วนบุคคลนิรนาม (Guideline for Anonymization)

การจัดทำข้อมูลนิรนามเพื่อให้เป็นไปตาม มาตรา 37 ของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ที่กำหนดให้ผู้ควบคุมข้อมูลต้องมีระบบรักษาความปลอดภัย โดยข้อมูลใดจะเป็นข้อมูลนิรนามหรือไม่ ต้องพิจารณาถึงตัวข้อมูลนั้นร่วมกับสภาพแวดล้อมของข้อมูล กล่าวคือ ข้อมูลนั้นสามารถระบุตัวผู้ที่เป็นเจ้าของข้อมูลได้หรือไม่ โดย**หลักการสำคัญของการจัดทำข้อมูลนิรนาม** คือ การที่ทำให้ข้อมูลนั้นไม่มีความเสี่ยงในการระบุตัวเจ้าของข้อมูล โดยไม่ได้คำนึงถึงการใช้ประโยชน์จากข้อมูลนั้นเท่านั้น ถึงแม้ในบางกรณีการใช้ประโยชน์จากข้อมูลนั้นไม่อาจทำให้ระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ แต่เมื่อวิเคราะห์ข้อมูลทุกฉบับ จะทำให้สามารถทราบได้ว่าใครเป็นเจ้าของข้อมูล ก็ควรจัดทำข้อมูลให้อยู่ในลักษณะที่เป็นการยากที่จะระบุตัวตนย้อนกลับมายังตัวเจ้าของข้อมูลได้

วิธีการจัดทำข้อมูลนิรนาม

1. **การจัดทำข้อมูลนิรนามแบบเป็นทางการ (Formal anonymization)** คือ การกำจัด หรือ ซ่อนตัวการระบุเจ้าของข้อมูลโดยตรง
2. **การจัดทำข้อมูลนิรนามแบบได้รับรอง (Guarantee anonymization)** คือ การจัดทำข้อมูลที่อยู่บนชุดของสมมติฐานใดสมมติฐานหนึ่ง โดยเฉพาะอย่างยิงสมมติฐานบนความรู้เบื้องต้นของผู้ล่วงละเมิด
3. **การจัดทำข้อมูลทางสถิติ (Statistical anonymization)** คือ การผสมข้อมูล (Scrambling) การปิดทับข้อมูล (Masking) การให้เจ้าของข้อมูลเลือกวิธี (Personalised anonymization) การลดความชัดเจนของข้อมูล (Blurring or Noising)
4. **การจัดทำข้อมูลนิรนามในเชิงการใช้งาน (Functional anonymization)** คือ การคำนึงถึงแรงจูงใจของผู้รุกล้ำข้อมูลส่วนบุคคล ผลกระทบของการถูกเปิดเผยของข้อมูลนิรนาม โอกาสที่จะเกิดเหตุการณ์ที่ข้อมูลถูกเปิดเผยโดยไม่ตั้งใจ ความสัมพันธ์ระหว่างความเสี่ยงในการระบุตัวตนเจ้าของข้อมูลกับการจัดการข้อมูลของผู้มีหน้าที่ เป็นต้น



แผนภาพแสดงการจัดทำข้อมูลส่วนบุคคลนิรนาม

ความรับผิดตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แบ่งความรับผิดออกเป็น ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครองอีก ซึ่งมีรายละเอียดของความรับผิด ดังนี้

ความรับผิดทางแพ่ง[27]

ผู้ฝ่าฝืนพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ จะมีความรับผิดทางแพ่งต้องชำระค่าสินไหมทดแทนให้กับผู้ที่เป็นเจ้าของข้อมูล โดยค่าสินไหมทดแทนในความรับผิดทางแพ่งแบ่งออกเป็น 2 ประเภท ดังนี้

- **ค่าสินไหมทดแทนที่แท้จริง** คือ เมื่อผู้ควบคุมข้อมูลหรือประมวลผลข้อมูลกระทำการฝ่าฝืนโดยจงใจหรือประมาทเลินเล่อ เว้นแต่จะพิสูจน์ได้ว่าความเสียหายนั้นเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย โดยค่าสินไหมทดแทนที่แท้จริงนี้ หมายความรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นเพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้ว
- **ค่าสินไหมทดแทนเพื่อการลงโทษ** ซึ่งค่าสินไหมทดแทนประเภทนี้เป็นค่าสินไหมที่กำหนดขึ้นโดยมีจุดประสงค์เพื่อลงโทษผู้กระทำความผิดให้หลาบจำและเพื่อป้องกันการกระทำผิดซ้ำ โดยจะต้องกำหนดเพิ่มขึ้นไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง และค่าสินไหมทดแทนทั้งสองประการมีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล หรือ 10 ปีนับแต่วันที่มีการละเมิด

ความรับผิดทางอาญา[28]

ผู้ควบคุมข้อมูลจะมีความรับผิดในทางอาญาก็ต่อเมื่อ ใช้หรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอม ใช้หรือเปิดเผยข้อมูลนอกเหนือไปจากวัตถุประสงค์ ส่งข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศซึ่งประเทศปลายทางไม่มีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ โดยประการที่น่าจะทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย หรือเพื่อการแสดงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น อย่างไรก็ตามความผิดดังกล่าวเป็นความผิดอันยอมความได้

[27] มาตรา 77 – 78 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

[28] มาตรา 79 – 81 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

และ**ผู้ที่ได้ล่วงรู้ข้อมูลส่วนบุคคล**ของผู้อื่นอันเนื่องมาจากการปฏิบัติหน้าที่ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แล้วนำข้อมูลนั้นไปเปิดเผยแก่ผู้อื่น เมื่อไม่เข้าข้อยกเว้นตามกฎหมาย อันได้แก่ การเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือการพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่มีอำนาจตามกฎหมาย การเปิดเผยที่ได้รับความยินยอมเป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูล การเปิดเผยข้อมูลที่เกี่ยวกับการฟ้องร้องคดีที่เปิดเผยต่อสาธารณะ ผู้นั้นต้องรับโทษทางอาญา อีกทั้ง**นิติบุคคล**อาจต้องรับผิดอาญาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ หากปรากฏว่าการกระทำนั้นเกิดจากการสั่งหรือมีหน้าที่แต่ละเว้นของ กรรมการ ผู้จัดการ บุคคลใดซึ่งต้องรับผิดชอบในการดำเนินงาน

โทษทางปกครอง[29]

ความรับผิดในโทษทางปกครองนั้น สามารถอุทธรณ์โต้แย้งตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองในฐานะคำสั่งทางปกครอง ซึ่งสามารถแยกการพิจารณาได้ ดังนี้

ความรับผิดของผู้ควบคุมข้อมูล

ผู้ควบคุมดูแลข้อมูลอาจต้องรับโทษทางปกครองเมื่อมีการกระทำความผิดพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ในกรณีใดกรณีหนึ่ง ดังต่อไปนี้

- ทำการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย (มาตรา 24 , มาตรา 27) การประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม เมื่อไม่ใช่กรณีที่กฎหมายยกเว้นให้ทำได้แม้ไม่ได้รับความยินยอม หรือการประมวลผลข้อมูลนอกวัตถุประสงค์ที่เจ้าของข้อมูลให้ความยินยอมมีโทษปรับไม่เกิน 3,000,000 บาท
- การไม่ขอความยินยอมให้ถูกต้องหรือไม่แจ้งผลกระทบจากการไม่ให้ความยินยอม (มาตรา19) การขอความยินยอมนั้นต้องทำโดยชัดแจ้งเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ โดยสภาพไม่อาจขอความยินยอมด้วยวิธีการดังกล่าวได้ การขอความยินยอมไม่ถูกต้องตามแบบที่กฎหมายกำหนด มีโทษปรับ ไม่เกิน 1,000,000 บาท
- เก็บรวบรวม ใช้ เปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ (มาตรา 21) การประมวลผลข้อมูลนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้กับเจ้าของข้อมูล มีโทษปรับ ไม่เกิน 3,000,000 บาท
- เก็บรวบรวมข้อมูลเกินกว่าที่จำเป็น (มาตรา 22) การเก็บข้อมูลนั้นต้องทำเท่าที่จำเป็นภายใต้วัตถุประสงค์เท่านั้น มีโทษปรับ ไม่เกิน 3,000,000 บาท

[29] มาตรา 82 – 90 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- การเก็บข้อมูลจากแหล่งอื่นโดยต้องห้าม (มาตรา 25) การเก็บข้อมูลต้องเก็บรวบรวมจากเจ้าของข้อมูลโดยตรง โดยจะเก็บข้อมูลจากแหล่งอื่นได้ก็ต่อเมื่อเจ้าของข้อมูลให้ความยินยอมหรือเป็นการเก็บข้อมูลที่เข้าข้อยกเว้นไม่จำต้องขอความยินยอมจากเจ้าของข้อมูล มีโทษปรับ ไม่เกิน 3,000,000 บาท
- การขอความยินยอมโดยการหลอกหลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ (มาตรา19 วรรค 3) การขอความยินยอมต้องทำให้เจ้าของข้อมูลเข้าใจง่าย ไม่เป็นการหลอกลวงให้เข้าใจผิดในวัตถุประสงค์ มีโทษปรับ ไม่เกิน 3,000,000 บาท
- การเก็บรวบรวม ใช้ เปิดเผย การโอน ข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย (มาตรา 26, มาตรา 27, มาตรา 28, มาตรา 29) การเก็บข้อมูลอ่อนไหวโดยไม่ได้รับความยินยอมโดยชัดแจ้ง เมื่อไม่เข้ากรณียกเว้น หรือการโอนข้อมูลอ่อนไหวไปประเทศปลายทางที่ไม่มีมาตรฐานคุ้มครองข้อมูลที่เพียงพอ มีโทษปรับ ไม่เกิน 5,000,000 บาท
- การไม่แจ้งเจ้าข้อมูลในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงหรือทางอ้อม (มาตรา 23, 25) คือ การไม่แจ้งเจ้าของข้อมูลให้ทราบถึงรายละเอียดในการเก็บข้อมูล หรือการไม่แจ้งเจ้าของข้อมูลในกรณีเก็บข้อมูลจากแหล่งอื่น มีโทษปรับ ไม่เกิน 1,000,000 บาท
- การไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ (มาตรา 30) การไม่ให้เจ้าของข้อมูลเข้าถึงสิทธิในการขอรับสำเนาข้อมูล หรือสิทธิในการขอให้เปิดเผยข้อมูล หรือสิทธิในการเข้าถึงข้อมูลในส่วนของตน หรือสิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเกี่ยวกับตน หรือสิทธิในการขอให้ลบหรือทำลายหรือทำให้เป็นข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลได้ หรือสิทธิในการระงับการใช้ข้อมูลส่วนบุคคลที่เกี่ยวกับตน มีโทษปรับ ไม่เกิน 1,000,000 บาท
- การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล (มาตรา 32 วรรค 2) เมื่อเจ้าของข้อมูลใช้สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลที่เกี่ยวกับตนเมื่อใด ผู้ควบคุมข้อมูลต้องไม่ดำเนินการประมวลผลข้อมูลอีก มีโทษปรับ ไม่เกิน 3,000,000 บาท
- การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41) การต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเมื่อเป็นการประมวลผลข้อมูลในกิจกรรมที่จำต้องมีการตรวจสอบอย่างสม่ำเสมอเนื่องด้วยมีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือกิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หรือผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลหน่วยงานของรัฐตามที่คณะกรรมการกำหนด มีโทษปรับ ไม่เกิน 1,000,000 บาท
- การไม่จัดให้มีการสนับสนุนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การให้ออก เลิกจ้าง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา 42) ในกิจกรรมที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลต้องให้การสนับสนุนการปฏิบัติหน้าที่ของ

เจ้าของข้อมูลส่วนบุคคล และจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกจ้างเนื่องจากการปฏิบัติหน้าที่ไม่ได้ มีโทษปรับ ไม่เกิน 1,000,000 บาท

- การโอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 28, มาตรา 29) การโอนข้อมูลไปยังต่างประเทศประเทศปลายทางต้องมีมาตรฐานการคุ้มครองข้อมูลที่เพียงพอ มีโทษปรับ ไม่เกิน 3,000,000 บาท
- การไม่จัดให้มีมาตรการในการรักษาความปลอดภัย ไม่จัดให้มีระบบลบหรือทำลายข้อมูล การไม่แจ้งเหตุละเมิดข้อมูล การไม่ตั้งตัวแทนนอกราชอาณาจักร (มาตรา 37) ผู้ควบคุมข้อมูลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ในกรณีที่ต้องให้ข้อมูลแก่บุคคลอื่นต้องป้องกันไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูล จัดให้มีระบบการตรวจสอบข้อมูลเพื่อลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาในการจัดเก็บ แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบ ผู้ควบคุมหรือผู้ประมวลผลข้อมูลที่อยู่นอกราชอาณาจักรเมื่อจะประมวลผลข้อมูลที่เจ้าของข้อมูลอยู่ในราชอาณาจักร จะต้องตั้งตัวแทนเป็นหนังสือและตัวแทนต้องอยู่ในราชอาณาจักร มีโทษปรับ ไม่เกิน 3,000,000 บาท

ความรับผิดของผู้ประมวลผลข้อมูล

ความรับผิดทางปกครองของผู้ประมวลผลข้อมูล ได้แก่ การกระทำการไม่ชอบด้วยพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ดังต่อไปนี้

- การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41) การต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเมื่อเป็นการประมวลผลข้อมูลในกิจกรรมที่จำต้องมีการตรวจสอบอย่างสม่ำเสมอเนื่องด้วยมีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือกิจกรรมหลักเป็นการประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว หรือผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลหน่วยงานของรัฐตามที่คณะกรรมการกำหนด มีโทษปรับ ไม่เกิน 1,000,000 บาท
- การไม่จัดให้มีการสนับสนุน การให้ออก เลิกจ้าง เพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา 42) ในกิจกรรมที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลต้องให้การสนับสนุนการปฏิบัติหน้าที่ของเจ้าของข้อมูลส่วนบุคคล และจะให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกจ้างเนื่องจากการปฏิบัติหน้าที่ไม่ได้ มีโทษปรับ ไม่เกิน 1,000,000 บาท
- การไม่ปฏิบัติตามหน้าที่โดยกฎหมายของผู้ประมวลผลข้อมูล (มาตรา 40) ผู้ประมวลผลข้อมูลจะต้องดำเนินการประมวลผลข้อมูลภายใต้คำสั่งที่ได้รับจากผู้ควบคุมข้อมูล จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลตามที่คณะกรรมการกำหนด มีโทษปรับ ไม่เกิน 3,000,000 บาท

- การโอนข้อมูลไปต่างประเทศโดยมิชอบ (มาตรา 29) การกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเมื่อโอนข้อมูลไปยังผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลซึ่งอยู่ในต่างประเทศและอยู่ในเครือเดียวกัน มีโทษปรับไม่เกิน 3,000,000 บาท
- การไม่ตั้งตัวแทนในราชอาณาจักรเมื่อกฎหมายกำหนด (มาตรา 38 วรรค 2, มาตรา 37(5)) การประมวลผลข้อมูลที่อยู่นอกราชอาณาจักรเมื่อจะประมวลผลข้อมูลที่เจ้าของข้อมูลอยู่ในราชอาณาจักร จะต้องตั้งตัวแทนเป็นหนังสือและตัวแทนต้องอยู่ในราชอาณาจักร มีโทษปรับ ไม่เกิน 3,000,000 บาท
- การโอนข้อมูลอ่อนไหวไปต่างประเทศโดยมิชอบ (มาตรา 29, มาตรา 26) การกำหนดนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเมื่อโอนข้อมูลไปยังผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลซึ่งอยู่ในต่างประเทศและอยู่ในเครือเดียวกัน เมื่อเป็นข้อมูลส่วนบุคคลอ่อนไหว มีโทษปรับ ไม่เกิน 5,000,000 บาท

ความรับผิดของบุคคลอื่น

- ตัวแทนของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลไม่จัดให้มีการบันทึกรายการประมวลผลข้อมูล (มาตรา 88) โดยตัวแทนที่ถูกแต่งตั้งโดยผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลจะต้องจัดให้มีบันทึกรายการประมวลผลข้อมูลด้วย มีโทษปรับ ไม่เกิน 1,000,000 บาท
- ผู้ที่ขัดคำสั่งของคณะกรรมการผู้เชี่ยวชาญ (มาตรา 89, มาตรา 75, มาตรา 76 (1)) เมื่อคณะกรรมการผู้เชี่ยวชาญสั่งให้บุคคลใดส่งเอกสารหรือข้อมูลเพื่อชี้แจ้งข้อเท็จจริงหรือให้ส่งข้อมูลหรือเอกสารเพื่อการดำเนินการตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แต่บุคคลดังกล่าวฝ่าฝืน มีโทษปรับ ไม่เกิน 500,000 บาท

บรรณานุกรม

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562” (27 พฤษภาคม 2562) ราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก, น. 52.

“พระราชกฤษฎีกากำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พ.ศ. 2563” (21 พฤษภาคม 2563) ราชกิจจานุเบกษา เล่ม 137 ตอนที่ 37 ก, น. 1.

ปิยะบุตร บุญอร่ามเรือง,พัฒนาพร โกวพัฒนกิจ,พีรพัฒ โชคสุวัฒนสกุล,เสกสิริ นิวัติศัยวงศ์,ปิติ เอี่ยมจำรูญลาภ,ชวิน อุ่นภัทร,ฐิติรัตน์ ทิพย์สัมฤทธิ์กุล,ภูมิศิริ ดำรงวุฒิ,โมกข์พิศุทธิ์ รตารุณ, “แนวปฏิบัติคุ้มครองข้อมูลส่วนบุคคล”, พิมพ์ครั้งที่ 1 สำนักพิมพ์โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย 2563.

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, “ความเป็นมาของกฎหมายคุ้มครองข้อมูลข่าวสารในประเทศไทย”, สืบค้นเมื่อ 22 กุมภาพันธ์ 2564, http://www.oic.go.th/FILEWEB/CABIWEBSITE/DRAWER01/GENERAL/DATA0024/00024967.PDF