วาง
โลโก้
ที่นี่

แนวปฏิบัติในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA Implementation Guide)

สารบัญ

สารบัญ (ต่อ)

1. บทนำ

วัตถุประสงค์ของคู่มือฉบับนี้มีไว้เพื่อช่วยเตรียมความพร้อมให้องค์กรของคุณสามารถดำเนินการที่เกี่ยวข้องให้ถูกต้องสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยใช้คู่มือฉบับนี้เป็นแนวทางในการปฏิบัติตาม ซึ่งการจะทำให้องค์กรดำเนินการให้ถูกต้องตามข้อกำหนดของกฎหมายอาจมีได้หลายวิธี หนึ่งในวิธีดังกล่าวคือรูปแบบและเนื้อหาที่ปรากฏในเอกสารเหล่านี้ กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นกฎหมายที่มีความซับซ้อน ดังนั้น คู่มือฉบับนี้จะช่วยให้คุณเข้าใจประเด็นสำคัญของกฎหมายดังกล่าว โดยจะนำเสนอออกมาในรูปแบบที่ง่ายต่อการทำความเข้าใจ ทั้งนี้ เพื่อให้คุณสามารถดำเนินการที่เกี่ยวข้องได้ทันทีที่สามารถทำได้

1.1 ความสำคัญของความเห็นด้านกฎหมาย

สิ่งที่จะนำเสนอต่อไปนี้ (รวมถึงสิ่งที่อยู่ในคู่มือ) เป็นความเข้าใจของเราเกี่ยวกับสิ่งที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อให้การดำเนินการถูกต้องสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ สืบเนื่องจากการที่อยู่ในวงการไอทีและอุตสาหกรรมด้านการคุ้มครองข้อมูลมาหลายปี รวมทั้ง จากการวิเคราะห์เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลตลอดจนการประชุม หนังสือ การสัมมนาออนไลน์ การนำเสนองาน หรือการตรวจสอบ อย่างไรก็ดีก่อนที่คุณจะเริ่มเข้าสู่เนื้อหา เราขอแจ้งให้ทราบก่อนว่า พวกเราไม่ใช่นักกฎหมาย และเนื้อหาดังต่อไปนี้ไม่สามารถใช้แทนความเห็นทางกฎหมายได้ จึงควรมีการพิจารณาตรวจสอบแหล่งที่มาของข้อมูลต่าง ๆ ก่อนทำการตัดสินใจ โดยการศึกษาทำความเข้าใจในกฎหมายคุ้มครองข้อมูลส่วนบุคคลก่อน

1.2 ความสำคัญของการคุ้มครองข้อมูล

ความเกี่ยวสัมพันธ์ระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลและแนวคิดเกี่ยวกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System หรือ ISMS) โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลไม่ได้อยู่ภายใต้ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) หรือ ระบบบริหารจัดการข้อมูลส่วนบุคคล (Personal Information Management System หรือ PIMS) ซึ่งเป็นระบบที่เกี่ยวกับมาตรฐานสากลสำหรับเรื่องความมั่นคงปลอดภัยของสารสนเทศ กล่าวคือ ISO/IEC 27001 และเมื่อต้องให้หน่วยงานกำกับดูแลเห็นว่าคุณได้มีการดำเนินการในเรื่องความปลอดภัยของข้อมูลส่วนบุคคล การมีกรอบการทำงานที่มาช่วยวางแผนงาน บริหารความเสี่ยง และพิจารณาทบทวนเพื่อให้เกิดผลสำเร็จ ก็จะช่วยให้งานของคุณมีประสิทธิภาพมากขึ้น ความเกี่ยวสัมพันธ์ระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลและแนวคิดเกี่ยวกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System หรือ ISMS) ตัวอย่างเช่น ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 กับรายละเอียดใน ISO/IEC 27001:2013 มาตรฐาน ISO ที่สามารถนำไปประยุกต์ใช้ให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีดังต่อไปนี้

- ISO/IEC 27001:2013 (Information Security Management System) ระบบบริหารจัดการความมั่นปลอดภัยสารสนเทศ
- ISO/IEC 27701:2019 (Privacy Information Security Management Systems) เป็นส่วนที่เพิ่มเติมจากมาตรฐาน ISO/IEC 27001 และ ISO/IEC 27002 ซึ่งกล่าวถึงการบริหารจัดการข้อมูลส่วนบุคคลโดยเฉพาะ

2. สรุปสาระสำคัญ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศในราชกิจจานุเบกษาเมื่อ 27 พฤษภาคม 2562 และมีผลบังคับใช้เมื่อ 28 พฤษภาคม 2562 แล้วในบางส่วน ได้แก่ หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และ หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยระหว่างวันที่ 27 พฤษภาคม 2563 ถึงวันที่ 31 พฤษภาคม 2564 เป็นช่วงที่พระราชบัญญัตินี้ได้รับการยกเว้นไม่ต้องปฏิบัติตามกฎหมายนี้ ซึ่งจะมีผลให้กฎหมายนี้มีผลบังคับใช้ทั้งฉบับในวันที่ 1 มิถุนายน 2564 โดยเหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้คือ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และรวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้ขึ้น ทั้งนี้ มีความพยายามที่จะทำให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลง่ายสำหรับองค์กร และขณะเดียวกันก็พยายามทำให้ธุรกิจสามารถดำเนินต่อไปได้ ดังนั้นจึงไม่ได้เป็นกฎหมายที่ให้ประโยชน์ฝ่ายใดฝ่ายหนึ่งฝ่ายเดียว อย่างไรก็ดี มีหลายสิ่งที่สำคัญที่จะต้องทำความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลก่อนที่จะเข้าสู่เนื้อหา

ประการที่หนึ่ง กฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้นได้กระทำในหรือนอกราชอาณาจักรก็ตาม รวมถึง กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักรที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร และมีการดำเนินกิจกรรมต่อไปนี้ (1) เสนอขายสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม หรือ (2) มีการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร กฎหมายคุ้มครองข้อมูลส่วนบุคคลก็มีผลบังคับใช้กับบุคคลเหล่านี้ด้วย ดังนั้นจะเห็นได้ว่าพระราชบัญญัตินี้ครอบคลุมทั้งภายในและภายนอกราชอาณาจักรไทย

ประการที่สอง ถ้าองค์กรของคุณไม่ได้ดำเนินการจัดทำข้อมูลอย่างที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดให้ทำ องค์กรของคุณก็จะต้องได้รับบทลงโทษตามที่พระราชบัญญัติดังกล่าวกำหนด โดยในกรณีที่มีความรุนแรง บทลงโทษดังกล่าวก็ถูกกำหนดขึ้นมาเพื่อจะลงโทษ

ประการที่สาม หากคุณได้ละเมิดข้อมูลส่วนบุคคล คุณก็จะไม่มีทางเลือกอื่น และจำเป็นต้องแจ้งหน่วยงานกำกับดูแลที่เกี่ยวข้องทราบ อย่างไรก็ดีจะมีข้อยกเว้นซึ่งจะกล่าวถึงในลำดับถัดไป แต่การเก็บเรื่องการละเมิดข้อมูลส่วนบุคคลไว้กับตัวไม่ได้เป็นทางเลือกอย่างแน่นอน อย่างไรก็ตาม หลักการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล คือ การบังคับให้องค์กรต้องปฏิบัติตามเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของบุคคลอย่างจริงจัง

2.1 รูปแบบของกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีความยาว 37 หน้า ประกอบด้วย 7 หมวด ได้แก่ หมวดที่ 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หมวดที่ 2 การคุ้มครองข้อมูลส่วนบุคคล หมวดที่ 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล หมวดที่ 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หมวดที่ 5 การร้องเรียน หมวดที่ 6 ความรับผิดทางแพ่ง หมวดที่ 7 บทกำหนดโทษ

2.2 คำนิยาม

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดคำนิยามไว้ในมาตรา 6 มีรายละเอียดดังนี้

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“คณะกรรมการ” หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2.3 หลักการ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ได้กำหนดหลักการทางกฎหมายและมีโครงสร้างโดยใช้ข้อกำหนดดังนี้ (แต่ละหลักการสามารถสรุปสั้นๆ ได้ดังนี้)

1. หลักความถูกต้อง ยุติธรรม และความโปร่งใส – การทำให้ถูกกฎหมายและเป็นกลางโดยการระบุให้ชัดเจนว่าจะนำข้อมูลไปทำอะไร
2. กำหนดวัตถุประสงค์ – ไม่ทำนอกเหนือจากวัตถุประสงค์ที่ได้แจ้ง
3. การจำกัดข้อมูล – เก็บรวบรวมข้อมูลเท่าที่จำเป็น
4. ความถูกต้อง – อัปเดตข้อมูลให้เป็นปัจจุบัน และแก้ไขหากข้อมูลไม่ถูกต้อง
5. ระยะเวลาจัดเก็บ – ไม่เก็บข้อมูลนานเกินจำเป็น
6. ความซื่อตรงและการรักษาความลับ – เก็บรักษาข้อมูลให้ปลอดภัยขณะที่มี
7. ความรับผิดชอบ – สามารถแสดงได้ว่ามีการปฏิบัติตามให้สอดคล้องตามหลักการข้างต้น

หากคุณสามารถจำและปฏิบัติตามหลักการเหล่านี้ได้ คุณก็อาจจะมั่นใจได้ว่าไม่ทำผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2.4 หลักความชอบด้วยกฎหมาย

การประมวลผลข้อมูลข้อมูลส่วนบุคคลจะต้องเป็นไปโดยถูกต้องตามกฎหมาย โดยการประมวลข้อมูลจะต้องประกอบด้วยฐานในการประมวลผลข้อมูลอย่างน้อยหนึ่งข้อ โดยขั้นแรกจะต้องทราบว่า ข้อมูลส่วนบุคคลที่เกี่ยวข้องมีอะไรบ้าง ใช้เพื่อวัตถุประสงค์อะไร และฐานการประมวลผลข้อมูลฐานใด

ฐานในการประมวลผลข้อมูล ประกอบด้วย 7 ฐาน มีรายละเอียดดังต่อไปนี้

1. การขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (Consent)
2. เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ (Scientific and Research)
3. เป็นการป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย สุขภาพของเจ้าของข้อมูลส่วนบุคคล (Vital Interest)
4. เป็นการจำเป็นเพื่อปฏิบัติตามสัญญาระหว่างองค์กรของคุณและเจ้าของข้อมูล หรือเพื่อใช้ดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญา (Contract)
5. เรื่องเกี่ยวกับภารกิจเพื่อประโยชน์สาธารณะ หรือเป็นการใช้อำนาจของรัฐ (Public task)
6. เพื่อประโยชน์โดยชอบด้วยกฎหมายของคุณ ตราบเท่าที่ไม่ส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Legitimate interest)
7. เป็นการปฏิบัติตามกฎหมายของคุณ (Legal obligation)

ดังนั้น ความยินยอมจึงเป็นเรื่องที่สำคัญในแง่ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งไม่ใช่เฉพาะกรณีรวบรวมข้อมูลและประมวลผลข้อมูลส่วนบุคคลที่จะทำให้ถูกต้องตามกฎหมาย แต่อันที่จริงแล้วคุณจะเห็นว่าสิ่งที่สำคัญในการดำเนินการและประมวลผลไม่ใช่เรื่องความยินยอม แต่ขึ้นอยู่กับว่าแต่ละข้อมูลใช้ฐานอะไรในการประมวลผล เช่น การให้ความช่วยเหลือลูกค้า (ใช้ฐานสัญญา) การจ่ายเงินให้ลูกจ้าง (ใช้ฐานสัญญา/ฐานการปฏิบัติตามกฎหมาย) หรือ การแจ้งข้อมูลภาษีให้เจ้าหน้าที่ทราบ (ใช้ฐานการปฏิบัติตามกฎหมาย) อย่างไรก็ดีการจะได้มาซึ่งความยินยอมอาจจะทำให้เกิดการเปลี่ยนแปลงในการดำเนินธุรกิจ และระบบงาน

ดังนั้นจะต้องมั่นใจว่าไม่มีฐานอื่นใช้บังคับกับเรื่องนั้น ๆ แล้วในหลายกรณี การจะใช้หลักประโยชน์โดยชอบด้วยกฎหมายในการประมวลผลข้อมูลจะต้องใช้ความระมัดระวัง หากจะเลือกใช้หลักเกณฑ์นี้จะต้องทำการประเมินพิจารณาให้รอบคอบในทุกแง่มุม

2.5 ความยินยอม

ถ้าคุณคิดว่าการประมวลผลข้อมูลของคุณได้ปฏิบัติอย่างถูกต้องตามกฎหมาย เนื่องจากคุณได้รับความยินยอมจากเจ้าของข้อมูล คุณจะต้องสามารถพิสูจน์ได้ ทั้งนี้ คุณไม่สามารถรวมเรื่องความยินยอมในสัญญา และคาดหวังว่าจะสามารถหลุดพ้นจากเรื่องนี้ได้ ดังนั้นจะต้องมีแบบฟอร์มที่เข้าถึงได้ ใช้ภาษาที่เข้าใจง่าย และชัดแจ้ง (มาตรา 19 วรรค 2 และ 3) หากไม่มีแล้วก็จะถือว่าไม่มีการขอความยินยอม และการประมวลผลข้อมูลของคุณก็จะถูกพิจารณาว่าไม่ถูกต้องตามกฎหมาย

2.6 สิทธิของเจ้าของข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนดสิทธิของเจ้าของข้อมูล ที่เมื่อเจ้าของข้อมูลจะใช้สิทธิ ผู้ควบคุมข้อมูลซึ่งมีข้อมูลจะต้องตอบสนองหรือทำการโต้ตอบ ซึ่งโดยปกติจะต้องดำเนินการภายใน 1 เดือน

1. **สิทธิที่จะได้รับการแจ้งให้ทราบ :** สิทธิในการได้รับแจ้งว่าข้อมูลที่ถูกเก็บจะนำไปทำอะไร เก็บทำไม โดยใครเป็นผู้เก็บ วัตถุประสงค์ในการเก็บคืออะไร และข้อมูลที่จัดเก็บจะไปอยู่ที่ไหน
2. **สิทธิในการเข้าถึงข้อมูลส่วนบุคคล :** สิทธิที่จะขอเข้าถึงข้อมูลส่วนบุคคลที่ถูกจัดเก็บ
3. **สิทธิแก้ไขข้อมูลส่วนบุคคล :** สิทธิที่จะแก้ไขข้อมูลส่วนบุคคล หากข้อมูลนั้นไม่ถูกต้อง
4. **สิทธิในการลบข้อมูลส่วนบุคคล :** สิทธิที่จะขอลบหรือทำลายข้อมูล หากข้อมูลนั้นไม่มีความจำเป็นอีกต่อไป
5. **สิทธิระงับการประมวลผลข้อมูลส่วนบุคคล :** สิทธิที่จะขอระงับการใช้ข้อมูล หากต้องการ
6. **สิทธิให้โอนย้ายข้อมูล :** สิทธิในการได้รับข้อมูลและถ่ายโอนข้อมูลดังกล่าวไปยังผู้ประมวลผลข้อมูลคนอื่น

7. **สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล :** สิทธิในการคัดค้านการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล
8. **สิทธิร้องเรียน :** เจ้าของข้อมูลมีสิทธิร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ปฏิบัติตาม PDPA

สิทธิของเจ้าของข้อมูลเหล่านี้มาจากหลักการซึ่งได้อธิบายไปข้างต้น โดยมีวัตถุประสงค์เพื่อรับรองว่าข้อมูลส่วนบุคคลถูกใช้อย่างเหมาะสมและโปร่งใส และเจ้าของข้อมูลก็สามารถกระทำการบางอย่างได้หากไม่ได้เป็นไปตามวัตถุประสงค์

เจ้าของข้อมูลจะต้องมีสิทธิได้รับการแจ้งว่าข้อมูลของเขาจะถูกนำไปใช้ทำอะไร ทำไม และจะถูกเก็บข้อมูลเมื่อไร (หรือภายในหนึ่งเดือน หากข้อมูลมาจากแหล่งข้อมูลอื่น) โดยรายละเอียดข้อมูลดังกล่าวจะต้องมีการแจ้งเตือนความเป็นส่วนตัวโดยทันที เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวม โดยตัวอย่างการแจ้งเตือนความเป็นส่วนตัวก็สามารถเห็นได้จากหลายเว็บไซต์

2.7 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

จะขึ้นอยู่กับองค์กรและกิจกรรมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ดังนั้นคุณอาจจำเป็นต้องมีหรือไม่จำเป็นต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้ อย่างไรก็ดีคุณอาจจะต้องมี หากเป็นกรณีต่อไปนี้

- เป็นหน่วยงานของรัฐ ตามประกาศคณะกรรมการคุ้มครองข้อมูลกำหนด
- มีการประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมาก ตามประกาศคณะกรรมการคุ้มครองข้อมูลกำหนด
- กิจกรรมหลักองค์กรของคุณมีการประมวลผลข้อมูลส่วนบุคคลอ่อนไหว (Sensitive personal data)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจจะเป็นพนักงานในองค์กร หรือจะจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมระหว่างองค์กรก็ได้ หรือจะว่าจ้างผู้ให้บริการภายนอกก็ได้ แต่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องเป็นอิสระ และข้อมูลของเจ้าหน้าที่ดังกล่าวต้องสามารถเข้าถึงได้ โดยจะต้องทำการแจ้งข้อมูลของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบด้วย เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นผู้ติดต่อหลักกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและจะต้องเกี่ยวข้องในเรื่องที่เกี่ยวกับข้อมูลส่วนตัวและการคุ้มครองข้อมูลที่อยู่ในองค์กรนั้น ๆ เช่น การประเมินผลกระทบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจำเป็นต้องทราบเกี่ยวกับกฎหมายข้อมูลส่วนบุคคลเพื่อที่จะสามารถปฏิบัติหน้าที่ได้ (ปัจจุบันยังไม่ได้มีการกำหนดคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล)

2.8 สัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีลักษณะเฉพาะ เนื่องจากมีการกำหนดให้ต้องมีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้เพื่อควบคุมการดำเนินงานของผู้ประมวลผลข้อมูลส่วนบุคคลในการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคล โดยทั่วไปสัญญาจะต้องมีรายละเอียดเกี่ยวกับวัตถุประสงค์ และระยะเวลาในการดำเนินการ ประเภทของข้อมูลส่วนบุคคลที่จะเกี่ยวข้อง และผลที่อาจกระทบเจ้าของข้อมูล ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องผูกพันข้อกำหนดหรือเงื่อนไขขั้นต่ำที่เกี่ยวข้องกับการคุ้มครองข้อมูล โดยสัญญาที่มีอยู่แล้วก็จะต้องถูกแก้ไขให้มีรายละเอียดดังที่กล่าวมาด้วย

สิ่งที่องค์กรขนาดใหญ่อย่างเช่น Google, Amazon Web Services และ Microsoft ทำ คือ จะให้ลูกค้าเซ็นสัญญายอมรับข้อกำหนดและเงื่อนไข โดยมีเรื่องการประมวลผลข้อมูลในนั้นด้วย ทั้งนี้ก็เพื่อประหยัดเวลาให้กับทุกฝ่าย

2.9 การออกแบบโดยคำนึงถึงความเป็นส่วนตัว (Privacy by design) และการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลส่วนบุคคล (Data Protection Impact Assessment)

ในการที่จะผสมผสานความเป็นส่วนตัวของข้อมูลเข้ากับการประมวลผลหรือระบบใหม่ ๆ นั้น การคุ้มครองข้อมูลส่วนบุคคลนั้นอาจจำเป็นต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้เพื่อประเมินว่ามีความเสี่ยงต่อเจ้าของข้อมูลมาเกี่ยวข้องด้วยหรือไม่ ซึ่งการประมวลผลนี้จะต้องอาศัยความเข้าใจลักษณะข้อมูลส่วนบุคคลและลักษณะความเสี่ยง โดยจะต้องมีวิธีการกำกับดูแลที่เหมาะสม

2.10 หลักการปฏิบัติ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้นได้กระทำในหรือนอกราชอาณาจักรก็ตาม อีกทั้ง ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร แต่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร และเป็นการเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร ก็ให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีผลบังคับใช้ร่วมด้วย ดังนั้นจะเห็นได้ว่าพระราชบัญญัตินี้ครอบคลุมทั้งในและนอกราชอาณาจักร

ในส่วนของมาตรฐานความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลนั้น ได้มีประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 กำหนดรายละเอียดไว้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่แตกต่างไปจากประกาศฉบับนี้ได้ หากมาตรฐานดังกล่าวมีมาตรการรักษาความมั่นคงปลอดภัยไม่ต่ำกว่าที่กำหนดในประกาศนี้