นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

(Personal Data Protection Act Policy)

บริษัท เอส 11 กรุ๊ป จำกัด (มหาชน)

จัดทำโดยบริษัท เอส 11 กรุ๊ป จำกัด(มหาชน)

ฉบับวันที่ 21 มกราคม พ.ศ. 2568

นโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

(Personal Data Protection Policy)

บริษัท เอส 11 กรุ๊ป จำกัด (มหาชน) ได้ตระหนักถึงความสำคัญและหน้าที่ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ให้ความสำคัญในการเคารพสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลและผู้มีส่วนได้ส่วนเสีย โดยบริษัท เอส 11 กรุ๊ป จำกัด(มหาชน) มีความมุ่งมั่นที่จะคุ้มครอง ปกป้องและใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้ยินยอมให้ไว้ จึงได้จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้นมาเพื่อจะทำการคุ้มครองข้อมูลอย่างมีหลักเกณฑ์และมีวิธีปฏิบัติสอดคล้องไปในแนวทางเดียวกัน และทำให้เจ้าของข้อมูลมั่นใจได้ว่า ข้อมูลส่วนบุคคลจะได้รับการคุ้มครองอย่างเหมาะสมเพียงพอ สอดคล้องกับความเสี่ยงและวิธีการดำเนินธุรกิจของบริษัทได้อย่างเหมาะสม

วัตถุประสงค์

1. เพื่อให้เจ้าของข้อมูลส่วนบุคคล และผู้มีส่วนได้ส่วนเสียทราบถึงวัตถุประสงค์ของการเก็บรวบรวม ใช้ และ/หรือ เปิดเผยข้อมูลส่วนบุคคล ตลอดสิทธิต่างๆของเจ้าของข้อมูลตามกฎหมาย
2. เพื่อกำหนดหลักเกณฑ์ และแนวทางปฏิบัติโดยให้เป็นมาตรฐานเดียวกันสอดคล้องกับความเสี่ยงและวิธีการดำเนินธุรกิจของบริษัท ได้อย่างเหมาะสม
3. เพื่อความโปร่งใสและเป็นธรรมในการใช้ข้อมูลส่วนบุคคล

ขอบเขตของนโยบาย

นโยบายฉบับนี้ให้มีผลบังคับใช้กับทุกกิจกรรมการดำเนินงานของบริษัทที่เกี่ยวข้องกับข้อมูลส่วนบุคคลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โครงสร้างและหน้าที่ความรับผิดชอบในการกำกับดูแลและบริหารจัดการ ในด้านการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการบริหารความเสี่ยง	ปฏิบัติหน้าที่ในการกำกับดูแลเทคโนโลยีสารสนเทศ
ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ	ปฏิบัติหน้าที่ในการบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศทั้งหมดของบริษัท และปฏิบัติหน้าที่ในการกำกับดูแลควบคุมข้อมูลส่วนบุคคล
System Admin	ปฏิบัติหน้าที่ในการควบคุมดูแลระบบเชื่อมต่อและด้าน Hardware
Database Admin	ปฏิบัติหน้าที่ในการควบคุมดูแลระบบฐานข้อมูลและ ด้าน Software และปฏิบัติหน้าที่บริหารจัดการข้อมูลส่วนบุคคล รวมทั้งปฏิบัติหน้าที่ในฐานะเป็นผู้คุ้มครองข้อมูลส่วนบุคคล
เจ้าหน้าที่เทคโนโลยีสารสนเทศ	ปฏิบัติหน้าที่ในการปรับปรุงและพัฒนาระบบงานเทคโนโลยีสารสนเทศ

คำนิยาม

ข้อความ	ข้อความภาษาอังกฤษ	คำอธิบาย
บริษัท	Company	หมายถึง บริษัท เอส 11 กรุ๊ป จำกัด(มหาชน) และรวมถึงบุคคลที่บริษัทมอบหมายด้วย
เจ้าของข้อมูล	Data Subject	หมายถึง บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล
ข้อมูลส่วนบุคคล	Personal Data	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลส่วนบุคคลที่มีความอ่อนไหว	Sensitive Personal Data	เป็นข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคลแต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรมจึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ
ผู้ควบคุมข้อมูลส่วนบุคคล	Data Controller	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หน่วยงาน หรือองค์กรใดซึ่งเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูล	Data Processor	บุคคลธรรมดาหรือนิติบุคคล หน่วยงานของรัฐ หน่วยงาน หรือองค์กรใดซึ่งประมวลผลข้อมูลแทนผู้ควบคุมข้อมูล
การประมวลผลข้อมูล	Processing	การดำเนินการหรือชุดการดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก จัดระบบ จัดโครงสร้าง การเก็บรักษาหรือเปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบหรือการทำลาย
ข้อมูลส่วนบุคคลรั่วไหล	Personal Data Breach	การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลทำให้เกิด ความเสียหายสูญหายเปลี่ยนแปลงเปิดเผยโดยไม่ได้รับอนุญาตหรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน
การจัดทำข้อมูลนิรนาม	Anonymization	กระบวนการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถใช้เพื่อระบุตัวตนของบุคคลใดบุคคลหนึ่งได้
การแฝงข้อมูล	Pseudonymization	กระบวนการแปลงข้อมูลส่วนบุคคลในลักษณะที่ไม่สามารถระบุตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ โดยมีการเก็บข้อมูลเพิ่มเติมไว้แยกออกจากกันและอยู่ภายใต้มาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการเพื่อประกันว่าไม่สามารถระบุไปถึงเจ้าของข้อมูลได้

1. หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles)

หลักการสำคัญสำหรับแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลจะอาศัยหลักการในการประมวลผลข้อมูลส่วนบุคคลและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งเป็นสิ่งพึงระลึกก่อนทำการประมวลผลข้อมูลตามความเหมาะสม ซึ่งแบ่งออกเป็น 7 หลักการดังนี้

1.1 หลักการที่ 1 การประมวลผลข้อมูลโดยชอบด้วยกฎหมาย มีความเป็นธรรมและโปร่งใส

(Principle 1: "Lawfulness, Fairness, and Transparency")

- **การประมวลผลข้อมูลส่วนบุคคลโดยชอบด้วยกฎหมาย (Lawfulness)**

หมายถึงผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องสามารถระบุฐานทางกฎหมาย(Lawful Basis) ในการประมวลผลให้ได้ฐานใดฐานหนึ่ง และจะต้องมีความระมัดระวังมากขึ้นในการประมวลผลข้อมูลที่มีความอ่อนไหว(Sensitive Personal Data) โดยหากผู้ควบคุมข้อมูลไม่สามารถระบุฐานทางกฎหมายในการประมวลผลข้อมูลได้ จะเป็นการขัดต่อหลักการข้อนี้ รวมทั้งอาจเป็นการขัดต่อกฎหมายซึ่งเจ้าของข้อมูลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลดำเนินการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุถึงเจ้าของข้อมูลได้

- **ความเป็นธรรม (Fairness)**

หมายถึงความเป็นธรรมในการประมวลผลข้อมูลจะต้องทำในลักษณะที่สมเหตุสมผลตามวัตถุประสงค์ของเจ้าของข้อมูลมีความยุติธรรมไม่เป็นการละเมิดสิทธิและประโยชน์ของเจ้าของข้อมูล

- **ความโปร่งใส (Transparency)**

หมายถึงการประมวลผลข้อมูลโดย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแสดงรายละเอียดในการประมวลผลข้อมูลอย่างชัดเจน เพื่อให้เจ้าของข้อมูลเข้าใจถึงการประมวลผลข้อมูลของตนได้ เช่น ผู้เก็บรวบรวมข้อมูลส่วนบุคคลแสดงตนว่าใครเป็นผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีการประมวลผลข้อมูลส่วนบุคคลอย่างไร รวมทั้งสามารถเปิดเผยให้แก่เจ้าของข้อมูลทราบและสามารถตรวจสอบได้ นอกจากนั้นควรแจ้งให้เจ้าของข้อมูลทราบด้วยภาษาที่ง่ายต่อความเข้าใจไม่ซับซ้อนหรือทำให้เกิดความเข้าใจผิด

1.2 หลักการที่ 2การเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องเก็บเฉพาะที่เกี่ยวข้องจำเป็น

(Principle 2: "Purpose Limitation")

การเก็บรวบรวบรวมข้อมูลส่วนบุคคลจะต้องเก็บเฉพาะที่เกี่ยวข้องจำเป็น เพื่อประมวลผลข้อมูลตามวัตถุประสงค์อันชอบด้วยกฎหมายที่ระบุไว้อย่างชัดเจน และชอบธรรม อีกทั้งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่นำไปประมวลผลต่อในลักษณะที่ไม่สอดคล้องกับวัตถุประสงค์เหล่านั้นและไม่สามารถนำไปใช้กับวัตถุประสงค์ใหม่ที่นอกเหนือจากวัตถุประสงค์ในการเก็บรวบรวมที่ระบุไว้ในตอนแรก ทั้งนี้ให้รวมถึงการใช้เปิดเผยและโอนข้อมูลส่วนบุคคลด้วย

1.3 หลักการที่ 3การประมวลผลข้อมูลจะดำเนินการตามวัตถุประสงค์

(Principle 3: "DataMinimisation")

การประมวลผลข้อมูลส่วนบุคคล ตั้งแต่กระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย รวมถึงระยะเวลาในการเก็บ ผู้ควบคุมข้อมูลส่วนบุคคลควรจะดำเนินการเท่าที่จำเป็น เกี่ยวข้อง และจำกัดตามวัตถุประสงค์ในการประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวมใช้ หรือเปิดเผยให้เจ้าของข้อมูลทราบ

1.4 หลักการที่ 4ความสมบูรณ์ถูกต้อง

(Principle 4: "DataAccuracy")

ข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่ไม่ถูกต้องจะถูกลบหรือแก้ไขโดยไม่ล่าช้า

1.5 หลักการที่ 5การประมวลผลข้อมูลตามระยะเวลาที่กฎหมายกำหนด

(Principle 5: "Storage Limitation")

ข้อมูลส่วนบุคคลจะต้องไม่เก็บเกินความจำเป็นตามระยะเวลาที่เหมาะสมเพื่อวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือเก็บตามระยะเวลาที่กฎหมายกำหนด

1.6 หลักการที่ 6การประมวลผลข้อมูลเป็นไปด้วยความซื่อสัตย์และรักษาความลับ

(Principle 6: " Integrity and Confidentiality")

ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีมาตรการที่ทำให้มั่นใจได้ว่ามีการรักษาความปลอดภัยของข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลมีความสมบูรณ์ถูกต้อง โดยจัดให้มีมาตรการทั้งในเชิงบริหารจัดการและเชิงเทคนิคที่มีความเหมาะสม และมีการป้องกันการประมวลผลจากบุคคลที่ไม่ได้รับอนุญาตหรือการประมวลผลอันมิชอบด้วยกฎหมาย มีการป้องกันการสูญหาย เสียหาย หรือการถูกทำลาย โดยไม่ได้ตั้งใจ

1.7 หลักการที่ 7ความรับผิดชอบ

(Principle 7: "Accountability")

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่และความรับผิดชอบในการประมวลผลข้อมูลให้เป็นไปตามหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Principles)

2. การเก็บรวบรวมข้อมูลส่วนบุคคล

2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล บริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลของเจ้าของข้อมูลจากแหล่งต่างๆ ประกอบไปด้วย

- ได้รับข้อมูลจากเจ้าของข้อมูลโดยตรง บริษัทจะดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยอาศัยข้อกำหนดทางกฎหมาย
- ได้รับข้อมูลส่วนบุคคลของเจ้าของข้อมูลจากแหล่งอื่น เช่น ลูกค้าของบริษัท ตัวแทนหรือผู้ให้บริการของบริษัท ,หน่วยงานราชการ หรือองค์กรอื่น เช่น บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด กรมสรรพากร สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานประกันสังคม เป็นต้น

บริษัทอาจเก็บรวบรวมข้อมูลส่วนบุคคลของบุคคลอื่นที่ได้ให้ไว้กับบริษัท เช่น ข้อมูลเกี่ยวกับคู่สมรส ข้อมูลเกี่ยวกับสมาชิกในครอบครัว ข้อมูลเกี่ยวกับบุตร ผู้อุปการะ ผู้อยู่ในอุปการะ ข้อมูลเกี่ยวกับผู้ค้ำประกัน ข้อมูลเกี่ยวกับผู้รับประโยชน์ หากมีการให้ข้อมูลส่วนบุคคลของบุคคลอื่นแก่บริษัท เจ้าของข้อมูลมีหน้าที่รับผิดชอบในการแจ้งรายละเอียดตามประกาศฉบับนี้ให้แก่บุคคลดังกล่าวทราบ ตลอดจนขอความยินยอมจากบุคคลนั้น

บริษัทจะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์อันชอบด้วยกฎหมาย ซึ่งในแต่ละกิจกรรมการประมวลผลข้อมูลจะต้องสามารถระบุ “ฐานทางกฎหมาย”(Lawful Basis)ประกอบด้วย

1. **ฐานความยินยอม (Consent)**

สามารถใช้ฐานความยินยอมในการประมวลผลข้อมูลในกรณีที่เจ้าของข้อมูลสมัครใจ และยินยอมอย่างชัดแจ้ง(Explicit Consent) เป็นไปตามวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูล อย่างไรก็ตาม ฐานความยินยอมนั้นเหมาะสมสำหรับการขอความยินยอมเพื่อประมวลผลข้อมูลในเรื่องที่ไม่จำเป็นในการปฏิบัติตามสัญญาและไม่สามารถอ้างฐานอื่นใดในการประมวลผลข้อมูลทางกฎหมายได้ โดยการให้ความยินยอมนั้นจะต้องเป็นสิ่งที่เจ้าของข้อมูลสามารถเลือกได้ว่าจะให้ความยินยอมหรือปฏิเสธอย่างไรก็ได้ ทั้งนี้หากเจ้าของข้อมูลเลือกที่จะปฏิเสธ การปฏิเสธดังกล่าวจะต้องไม่ส่งผลกระทบต่อการได้รับบริการตามสัญญา

2. **ฐานสัญญา(Contract)**

สามารถใช้ฐานสัญญาในการประมวลผลข้อมูล ในกรณีที่การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาตามที่ตกลงกันไว้ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูล หรือเมื่อจำเป็นต้องประมวลผลข้อมูลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญา หากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม โดยฐานนี้ใช้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ทั้งนี้ไม่สามารถใช้ฐานสัญญาในการประมวลผลข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) ได้

3. ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

กรณีที่การประมวลผลจำเป็นต่อการปกป้องผลประโยชน์ที่สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น โดยเป็นการป้องกันอันตรายอันเกิดต่อสุขภาพและชีวิต ผู้ควบคุมข้อมูลส่วนบุคคลสามารถใช้ฐานการประมวลผลข้อมูลส่วนบุคคลนี้ได้ หากเจ้าของข้อมูลอยู่ในสภาพที่ไม่สามารถให้ความยินยอมได้

4. ฐานภารกิจของรัฐ (Public Task)

ใช้ในกรณีที่การประมวลผลนั้นมีความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบหมายให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งการประมวลผลดังกล่าวจะต้องสามารถอ้างอิงได้อย่างชัดเจนว่ากระทำภายใต้กฎหมายใดและมีการรักษาความปลอดภัยของข้อมูลเช่นเดียวกันกับฐานอื่น โดยเจ้าของข้อมูลไม่สามารถใช้สิทธิในการ ลบ หรือโอนย้ายข้อมูลได้ แต่ยังคงมีสิทธิในการคัดค้านการประมวลผลเท่านั้น

5. ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

การใช้ฐานประโยชน์อันชอบธรรมควรใช้ในกรณีที่การประมวลผลข้อมูลเป็นแบบที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผลอีกทั้งมีผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลเพียงเล็กน้อย หรือใช้ในกรณีที่บริษัทมีเหตุผลในการประมวลผลอย่างสมเหตุสมผลซึ่งบริษัท สามารถอธิบายได้โดยใช้ดุลพินิจอย่างมากในการประมวลผล และการคุ้มครองสิทธิเสรีภาพของเจ้าของข้อมูลโดยคำนึงถึงประโยชน์ทั้งประโยชน์อันชอบธรรมของบริษัทกับสิทธิและประโยชน์ของเจ้าของข้อมูล ซึ่งการได้ประโยชน์อันชอบธรรมดังกล่าวจะต้องไม่เป็นการละเมิดหรือกระทบต่อสิทธิขั้นพื้นฐานและเสรีภาพของเจ้าของข้อมูลโดยเฉพาะอย่างยิ่งกับผู้เยาว์

ในการประเมินการใช้ฐานผลประโยชน์อันชอบธรรม สามารถพิจารณาจาก 3 องค์ประกอบ ได้แก่

- **ระบุผลประโยชน์อันชอบธรรม (Identify a legitimate interest)**

  การประมวลผลข้อมูลภายใต้ผลประโยชน์อันชอบธรรมอาจเป็นผลประโยชน์ของบริษัทหรือผลประโยชน์ของบุคคลที่สาม รวมถึงผลประโยชน์เชิงพาณิชย์ และผลประโยชน์แก่สาธารณะ

- **การประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นต่อบริษัทในการบรรลุวัตถุประสงค์ (Show that the processing is necessary to achieve it)**

  การประมวลผลข้อมูลอันมีความจำเป็นที่ส่งผลให้บริษัทสามารถบรรลุถึงเป้าหมายและวัตถุประสงค์หลักขององค์กร แต่ทั้งนี้ให้พิจารณาผลกระทบต่อความเป็นส่วนตัวของเจ้าของข้อมูลประกอบด้วย

- **การรักษาสมดุลระหว่างผลประโยชน์อันชอบธรรมของบริษัทหรือของบุคคลที่สามกับประโยชน์และสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Balance it against the individual's interests, rights and freedoms)**

บริษัท จะต้องพิจารณาระหว่างผลประโยชน์อันชอบธรรมของบริษัทกับสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล หากการประมวลผลนั้นไม่เป็นไปตามความคาดหมายอย่างสมเหตุสมผลหรืออาจก่อให้เกิดความไม่เป็นธรรมกับเจ้าของข้อมูลบริษัทจะต้องให้ประโยชน์และสิทธิเสรีภาพของเจ้าของข้อมูลแทนที่ผลประโยชน์อันชอบธรรมของบริษัท นั่นคือการให้สิทธิในการคัดค้านการประมวลผลข้อมูลแก่เจ้าของข้อมูล อย่างไรก็ตามประโยชน์อันชอบธรรมของบริษัทไม่จำเป็นต้องสอดคล้องกับประโยชน์ของเจ้าของข้อมูลเสมอไป หากมีข้อโต้แย้งเกี่ยวกับสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูล บริษัทยังสามารถประมวลผลได้เพื่อประโยชน์อันชอบธรรมดังกล่าวของบริษัทตราบเท่าที่บริษัทจะแสดงให้เห็นอย่างสมเหตุสมผลและชัดเจนในเรื่องของผลกระทบต่อเจ้าของข้อมูล

นอกจากนั้นบริษัทจะต้องทำการเก็บบันทึกประเมินการใช้ฐานผลประโยชน์อันชอบธรรม (LIA) เพื่อให้มั่นใจว่าการประมวลผลมีความจำเป็นและมีความสมเหตุสมผลในการใช้ฐานดังกล่าวเพื่อใช้แสดงแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลหากมีความจำเป็นและบริษัทจะต้องทำการระบุกิจกรรมการประมวลผล (Data Processing Activities) ที่ใช้ฐานผลประโยชน์อันชอบธรรมไว้ในนโยบายความเป็นส่วนตัวของบริษัท(Privacy Notice)เพื่อเป็นการแจ้งให้ทราบแก่บุคคล ซึ่งในทางปฏิบัติบริษัทสามารถใช้ฐานการประมวลผลอันชอบธรรมได้ในกรณีต่อไปนี้

- บริษัทสามารถประมวลผลข้อมูลเพื่อวัตถุประสงค์ทางการตลาดได้ หากบริษัทสามารถแสดงให้เห็นถึงความเหมาะสมในการใช้ข้อมูล และมีผลกระทบเพียงเล็กน้อยต่อความเป็นส่วนตัวของเจ้าของข้อมูล และเจ้าของข้อมูลสามารถคาดหมายต่อกิจกรรมเหล่านั้นของบริษัทได้ หรือเจ้าของข้อมูลไม่มีแนวโน้มที่จะคัดค้านกิจกรรมการประมวลผลเหล่านั้นได้
- บริษัทสามารถประมวลผลข้อมูลของผู้เยาว์ภายใต้ฐานประโยชน์อันชอบธรรมได้ แต่จะต้องกระทำอย่างระมัดระวังเป็นพิเศษเพื่อให้แน่ใจว่าสิทธิและผลประโยชน์ของผู้เยาว์นั้นได้รับการคุ้มครองอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการทำโปรไฟล์ลิ่งข้อมูลของผู้เยาว์ที่เกี่ยวกับการวิเคราะห์ข้อมูลเพื่อวัตถุประสงค์ทางการตลาด สำหรับกรณีนี้บริษัทอาจต้องพิจารณาการจัดทำDPIA(Data Protection Impact Assessment)เพื่อประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประมวลผลข้อมูลและแนวทางในการจัดการกับความเสี่ยงดังกล่าว

6. ฐานการปฏิบัติตามกฎหมาย (Legal Obligation)

ผู้ควบข้อมูลส่วนบุคคลสามารถใช้ฐานดังกล่าวได้ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ประมวลผลข้อมูลตามที่กฎหมายกำหนด โดยจะต้องสามารถระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใด หากเจ้าของข้อมูลคัดค้านการประมวลผลแต่

การประมวลผลดังกล่าวเป็นไปตามฐานการปฏิบัติตามกฎหมาย บริษัทสามารถปฏิเสธคำร้องขอการคัดค้านการประมวลผลได้ โดยการระบุเหตุแห่งการปฏิเสธประกอบด้วย

7. **ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (Research)**

กรณีที่บริษัทมีความจำเป็นในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการศึกษาวิจัยทางวิทยาศาสตร์ประวัติศาสตร์ หรือสถิติ หรือสาธารณประโยชน์อื่น ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น โดยจะต้องมีฐานอื่นประกอบการประมวลผลสำหรับฐานนี้เสมอไม่สามารถอ้างฐานนี้เพียงอย่างเดียวได้ นอกจากนั้นการประมวลผลบนฐานนี้มีความจำเป็นที่จะต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลตามที่คณะกรรมการประกาศกำหนด เนื่องจากการประมวลผลข้อมูลภายใต้ฐานนี้จำเป็นจะต้องมีมาตรการที่ความสอดคล้องกับมาตรฐานจริยธรรม และระเบียบในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติด้วย

2.2 การจำแนกข้อมูลส่วนบุคคล เป็นกระบวนการที่เกี่ยวข้องกับการประเมินชุดข้อมูลและรักษาความปลอดภัยของข้อมูล อันได้แก่ ข้อมูลความลับ ข้อมูลที่มีความอ่อนไหว ข้อมูลที่ต้องจัดให้มีเพื่อความพร้อมในการใช้งาน และข้อมูลที่ต้องเปิดเผยตามข้อกฎหมายกำหนด เพื่อให้สามารถใช้ข้อมูลได้อย่างเหมาะสม อีกทั้งยังเป็นกระบวนการรักษาความปลอดภัยของข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่สำคัญ อยู่ในระดับความเสี่ยงที่เหมาะสม ไม่ว่าข้อมูลนั้นจะถูกใช้งานหรือถูกเก็บไว้ในที่ใดก็ตาม สามารถจำแนกข้อมูลส่วนบุคคล ได้ดังนี้

ประเภทข้อมูล	รายละเอียด
ข้อมูลส่วนบุคคลทั่วไป	ชื่อ นามสกุล เลขบัตรประจำตัวประชาชน วันเกิด อายุ อาชีพ เพศ สถานภาพทางการสมรส รูปถ่าย หมายเลขโทรศัพท์ ที่อยู่ปัจจุบัน ลายมือชื่อ อีเมล ไอดีไลน์ และรายละเอียดข้อมูลติดต่ออื่น ๆ
ข้อมูลและประวัติเกี่ยวกับการทำงาน	ชื่อบริษัท ที่อยู่ที่ทำงาน หน่วยงานต้นสังกัด ตำแหน่งงาน ระยะเวลาการทำงาน
ข้อมูลทางการเงิน	รายได้ แหล่งที่มาของรายได้ เงินเดือน เลขบัญชีธนาคาร รายละเอียดเกี่ยวกับการเคลื่อนไหวบัญชี
ข้อมูลรายละเอียดผลิตภัณฑ์และ/หรือบริการที่เคยซื้อ	ประวัติการเป็นลูกค้าสินเชื่อประเภทต่าง ๆ ประวัติการชำระเงิน
ข้อมูลที่ต้องตรวจสอบ	ข้อมูลที่เกี่ยวข้องกับกระบวนการทำความรู้จักลูกค้า การระบุตัวตน(KYC)และข้อมูลสำหรับตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (CDD) ข้อมูลในการตรวจสอบ การจัดระดับความเสี่ยงด้านการป้องกันและปราบปรามการฟอกเงินหรือ

ประเภทข้อมูล	รายละเอียด
	การสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง
ข้อมูลการใช้งาน	ข้อมูลที่ใช้งานผ่านระบบเทคโนโลยีสารสนเทศ ของบริษัทอาทิ เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มต่างๆ เป็นต้น
ข้อมูลการสื่อสาร	อีเมล ไฟล์บันทึกข้อมูลการสนทนา และข้อมูลบันทึกการสื่อสาร เป็นต้น

วัตถุประสงค์ของการประมวลผลข้อมูล

บริษัทจะทำการประมวลผลข้อมูลของเจ้าของข้อมูลเท่าที่จำเป็นเพื่อให้เป็นไปตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมไว้ โดยใช้ฐานการประมวลผลข้อมูลส่วนบุคคลที่ชอบธรรม(Lawful Basis of Processing)มีรายละเอียดสำหรับแต่ละกิจกรรม ดังนี้

วัตถุประสงค์	ประเภทข้อมูล	ฐานการประมวลผลข้อมูลส่วนบุคคลที่ชอบธรรม
เพื่อทำสัญญา	- ข้อมูลที่เกี่ยวข้องกับการทำสัญญา - ข้อมูลการติดต่อ	- เพื่อความจำเป็นในการปฏิบัติตามสัญญาให้บริการ
เพื่อทำการตลาดแบบตรงในการนำเสนอสินค้าและบริการ อื่นๆ ที่ลูกค้าอาจให้ความสนใจ	- ข้อมูลการติดต่อ - ข้อมูลการสื่อสาร	- เพื่อความจำเป็นในการปฏิบัติตามสัญญาให้บริการ - เพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท ในการนำเสนอสินค้าและการบริการที่ลูกค้าอาจให้ความสนใจโดยวิธีการทำการตลาดโดยตรงกับลูกค้า
เพื่อวิเคราะห์ข้อมูลพฤติกรรมการบริโภคสินค้าและบริการของลูกค้า	- ข้อมูลที่เกี่ยวข้องกับการทำสัญญา - ข้อมูลการติดต่อ - ข้อมูลการใช้งาน - ข้อมูลการสื่อสาร - ข้อมูลด้านเทคนิค	- เพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท ในการนำข้อมูลมาจัดทำรายงานสถิติเพื่อประกอบการตัดสินใจสำหรับในการวางแผนดำเนินธุรกิจ และการพัฒนาสินค้าและบริการ
เพื่อเป็นการพัฒนาสินค้าและบริการ	- ข้อมูลการติดต่อ - ข้อมูลการใช้งาน	- เพื่อความจำเป็นในการปฏิบัติตามสัญญาให้บริการ - เพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท ในการนำข้อมูลมาใช้เพื่อปรับปรุงและพัฒนาการสินค้า

วัตถุประสงค์	ประเภทข้อมูล	ฐานการประมวลผล ข้อมูลส่วนบุคคลที่ชอบธรรม
		และบริการที่ให้แก่ลูกค้าอันจะตอบสนองได้ตรงความต้องการที่ลูกค้าต้องการบริโภค
เพื่อเป็นการแก้ไขปัญหาในเชิงเทคนิค ของบริษัท	- ข้อมูลการติดต่อ - ข้อมูลด้านเทคนิค	- เพื่อความจำเป็นในการปฏิบัติตามสัญญาให้บริการ - เพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท ในการนำข้อมูลมาใช้เพื่อปรับปรุงและพัฒนาเชิงเทคนิคสำหรับระบบเทคโนโลยีสารสนเทศของบริษัท
เพื่อเป็นการเสริมสร้างความสัมพันธ์อันดีกับลูกค้า	- ข้อมูลการติดต่อ - ข้อมูลการสื่อสาร	- เพื่อความจำเป็นในการปฏิบัติตามสัญญาให้บริการ - เพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท ในการส่งเสริมภาพลักษณ์ที่ดีของบริษัท และเป็นการเสริมสร้างความสัมพันธ์อันดีระหว่างบริษัท กับลูกค้าในการใช้สินค้าและบริการ โดยผ่านช่องทางการสื่อสารประชาสัมพันธ์ของบริษัท

2.3 ความยินยอม (Consent)

เงื่อนไขในการใช้ฐานความยินยอมมีดังต่อไปนี้

- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้
- เจ้าของข้อมูลสามารถถอนความยินยอมเมื่อใดก็ได้
- การใช้ฐานความยินยอมนั้น จะต้องให้สิทธิเจ้าของข้อมูลสามารถปฏิเสธไม่ให้ความยินยอมได้
- การขอความยินยอมจะต้องกระทำอย่างชัดเจนไม่คลุมเครือ ดังนั้น บริษัทจึงควรออกแบบแบบฟอร์มการขอความยินยอมที่ทำให้เจ้าของข้อมูลสามารถเห็นได้อย่างชัดเจนว่าบริษัทขอความยินยอมในการประมวลผลข้อมูลเพื่อวัตถุประสงค์ใด
- ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงอิสระของเจ้าของข้อมูลในการให้ความยินยอม ทั้งนี้การขอความยินยอมจะต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน ไม่นำมารวมอยู่ในเงื่อนไขการให้บริการ (Terms & Conditions) หรือข้อความในสัญญา
- การขอความยินยอมจะทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้

การขอ และให้ความยินยอม

การขอความยินยอมจะต้องกระทำโดยชอบด้วยกฎหมาย เป็นธรรมและโปร่งใส โดยระบุวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจนว่าจะขอความยินยอมในเรื่องใด และจะต้องไม่ใช้ข้อความที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลเข้าใจผิดในวัตถุประสงค์ ทั้งยังต้องคำนึงถึงความเป็นอิสระของเจ้าของข้อมูลในการตัดสินใจให้ความยินยอม ด้วยความสมัครใจ

โดยในส่วนของการให้ความยินยอมนั้นเจ้าของข้อมูลสามารถเลือกได้ว่าจะยินยอมหรือปฏิเสธย่อมกระทำได้ ซึ่งการปฏิเสธดังกล่าวจะไม่ส่งผลกระทบต่อการได้รับบริการตามสัญญา

ในกรณีหากต้องการประมวลผลเพื่อวัตถุประสงค์อื่นที่นอกเหนือจากที่เคยได้รับความยินยอมไปแล้ว ต้องดำเนินการขอความยินยอมจากเจ้าของข้อมูลใหม่อีกครั้ง เว้นแต่หากพิจารณาแล้วว่าเป็นการประมวลผลภายใต้ฐานกฎหมายอื่น

วิธีการขอความยินยอม

- **การขอความยินยอมจากการเลือกการยินยอม (Opt-in Consent)**

  ผู้ควบคุมข้อมูลส่วนบุคคลได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดเจน เป็นลายลักษณ์อักษร โดยที่ควรออกแบบให้เจ้าของข้อมูลต้องมีการกระทำการให้ความยินยอมอย่างชัดเจน (Clear Affirmative Action) เช่น การทำเป็นช่องเช็คถูก (Check Box) โดยให้เจ้าของข้อมูลเลือก หรือเขียนเองได้(Signatures or Ticks Indicating Consent)

- **การขอความยินยอมในรูปแบบวาจา (Verbal Consent)**

  ผู้ควบคุมข้อมูลส่วนบุคคลจะใช้ในกรณีที่มีการบันทึกความยินยอมในรูปแบบเสียง (Voice Record) ด้วยระบบดิจิทัล เช่น บันทึกผ่านการติดต่อกับเจ้าของข้อมูลทาง Contact Center หรือผ่านทางระบบ Interactive Voice Response (IVR) โดยขอให้เจ้าของข้อมูลกดปุ่มยืนยันการให้ความยินยอม เป็นต้น ซึ่งจะต้องมีกระบวนการพิสูจน์และยืนยันตัวตนของเจ้าของข้อมูลก่อนทำการขอความยินยอมเพื่อให้มั่นใจว่าคู่สนทนาเป็นเจ้าของข้อมูลจริง นอกจากนั้นควรให้ข้อมูลแก่เจ้าของข้อมูลอย่างเพียงพอสำหรับการตัดสินใจ ให้มีทางเลือก และเนื้อหาชัดเจนไม่ก่อให้เกิดความเข้าใจผิด และให้เจ้าของข้อมูลสามารถให้ความยินยอมหรือไม่ให้ความยินยอมก็ได้โดยสมัครใจ โดยไม่เป็นการบังคับ

การถอนความยินยอม (Withdraw of Consent)

เจ้าของข้อมูลมีสิทธิที่จะขอถอนความยินยอม (Right to Withdraw of Consent) ที่เคยให้ไว้เมื่อใดก็ได้ โดยบริษัทจะต้องดำเนินการหยุดการประมวลผลของเจ้าของข้อมูลนั้น หากบริษัทไม่มีฐานโดยชอบด้วยกฎหมายอื่นในการประมวลผลข้อมูลต่อไปโดยดำเนินการลบข้อมูลออก ซึ่งการใช้สิทธิถอนความยินยอมดังกล่าวผู้

ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางที่เจ้าของข้อมูลสามารถใช้สิทธิกระทำได้โดยง่ายในระดับเดียวกับการให้ความยินยอม

การขอความยินยอมจากผู้เยาว์

การขอความยินยอมจากผู้เยาว์ (ผู้เยาว์หมายถึง ผู้ที่มีอายุไม่ครบ 20 ปีบริบูรณ์ หรือ ไม่ได้จดทะเบียนสมรสกันก่อนอายุ20 ปีโดยอายุไม่ต่ำกว่า 17 ปี) ต้องกระทำโดยระมัดระวังเป็นพิเศษ เนื่องจากความสามารถในการเข้าใจวัตถุประสงค์ของผู้เยาว์นั้นไม่เท่ากับผู้ที่บรรลุนิติภาวะแล้วดังนั้นการขอความยินยอมจากผู้เยาว์จึงต้องทำอย่างถูกต้อง เป็นธรรมและโปร่งใสใช้ภาษาที่ง่ายเหมาะสม ชัดเจน ไม่ก่อให้เกิดความเข้าใจผิดได้ง่าย และจะต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำแทนผู้เยาว์ด้วยเว้นแต่ เป็นไปตาม มาตรา 22 23 และ 24 แห่งประมวลกฎหมายแพ่งและพาณิชย์ ผู้เยาว์จึงจะสามารถให้ความยินยอมตามลำพังได้ในกรณีที่ผู้เยาว์มีอายุไม่เกินสิบปีให้ขอความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์ ดังนั้นหากมีความจำเป็นที่จะต้องประมวลผลข้อมูลของผู้เยาว์ควรจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ก่อน เพื่อประเมินผลกระทบที่อาจเกิดขึ้น และหาวิธีการลดความเสี่ยงจากการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์นอกจากนั้นยังต้องคำนึงถึงการคุ้มครองสิทธิของผู้เยาว์อีกด้วย

การขอความยินยอมในการเก็บคุกกี้ (Cookie Consent)

“คุกกี้ (Cookie)” หมายถึง ข้อความขนาดเล็กที่บริษัท ทำการเก็บรวบรวมจากหน้าเวปไซต์หรือแอปพลิเคชันของบริษัท โดยจะถูกจัดเก็บลงในอุปกรณ์คอมพิวเตอร์ หรือเครื่องมือสื่อสารที่เข้าใช้งานของผู้ใช้งานเว็บไซต์หรือแอปพลิเคชัน ทั้งนี้คุกกี้จะถูกนำมาใช้เพื่อทำให้ผู้ใช้งานเว็บไซต์หรือแอปพลิเคชันสามารถใช้งานได้อย่างต่อเนื่อง อย่างไรก็ตาม คุกกี้บางประเภทอาจส่งผลกระทบกับความเป็นส่วนตัวของผู้ใช้งาน เช่น ใช้ในการวิเคราะห์ความสนใจของผู้ใช้งานพฤติกรรมการเยี่ยมชม หรือเพื่อนำเสนอสื่อให้เหมาะสมกับความสนใจของผู้ใช้งาน รวมถึงอาจมีการติดตามการใช้งานเว็บไซต์ หรือแอปพลิเคชันที่ผู้ใช้งานเยี่ยมชม

ทั้งนี้บริษัท สามารถใช้ข้อมูลคุกกี้ประเภทที่มีความจำเป็นต่อการใช้งานเว็บไซต์หรือแอปพลิเคชัน (Necessary Cookies) ได้โดยไม่ต้องขอความยินยอมจากผู้ใช้งาน แต่สำหรับคุกกี้ประเภทอื่น ๆ เช่น คุกกี้ที่ใช้ในการวิเคราะห์ข้อมูล (Analytic Cookies) คุกกี้ที่ใช้ในการโฆษณา (Targeting Cookies) เป็นต้น คุกกี้ประเภทนี้เป็นคุกกี้ประเภทที่ไม่ได้จำเป็นต่อการใช้งานดังนั้นจึงต้องได้รับความยินยอมจากผู้ใช้งานเว็บไซต์หรือแอปพลิเคชันดังกล่าวก่อน หรืออาจจัดให้ผู้ใช้งานสามารถจัดการฟังก์ชันคุกกี้เองได้ กล่าวคือ ผู้ใช้งานสามารถเลือกเปิดหรือปิดค่าคุกกี้ในแต่ละประเภทในหน้าเว็บไซต์หรือแอปพลิเคชันได้ด้วยตนเอง

ในการขอความยินยอมคุกกี้จากผู้ใช้งานเว็บไซต์หรือแอปพลิเคชันนั้น ผู้ใช้งานสามารถยอมรับหรือปฏิเสธคุกกี้ได้ โดยการปฏิเสธนั้นจะไม่เป็นการส่งผลกระทบต่อการใช้งานเว็บไซต์หรือแอปพลิเคชันของผู้ใช้งานดังกล่าว

2.4 ข้อมูลส่วนบุคคลที่มีความอ่อนไหว(Sensitive Personal Data)

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว(Sensitive Personal Data) หมายถึง ข้อมูลส่วนบุคคลที่สามารถพิจารณาได้ว่าเป็นเรื่องส่วนตัวของเจ้าของข้อมูล อาทิเช่น เชื้อชาติ เผ่าพันธุ์ประวัติอาชญากรรม ความเห็นทางการเมืองความเชื่อลัทธิศาสนา ปรัชญาพฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลความพิการ ข้อมูลสุขภาพจิตข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูล

ห้ามเก็บข้อมูลส่วนบุคคลที่มีความอ่อนไหว หากไม่ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของ (Explicit Consent) เว้นแต่ในกรณีที่ได้รับการยกเว้นตามกฎหมายไม่ได้ต้องขอความยินยอม ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความอ่อนไหว

2.5 การประกาศความเป็นส่วนตัว (Privacy Notice)

ประกาศความเป็นส่วนตัวต้องอธิบายในรายละเอียดเกี่ยวกับการประมวลผลทั้งหมด ในภาษาที่เข้าใจได้ง่าย เพื่อเป็นการแจ้งให้กับเจ้าของข้อมูลทราบว่ากำลังเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้างเพื่อบรรลุวัตถุประสงค์อะไร และมีการเปิดเผยข้อมูลส่วนบุคคลให้แก่ประเภทของบุคคลหรือหน่วยงานใดบ้าง และจะทำการเก็บข้อมูลไว้เป็นระยะเวลาเท่าใด รวมถึงสิทธิของเจ้าของข้อมูลเป็นต้น

อีกทั้งจะต้องทำการแจ้งประกาศความเป็นส่วนตัวแก่เจ้าของข้อมูลได้รับทราบ ด้วยวิธีการหรือช่องทางที่สามารถเข้าถึงได้โดยง่าย ซึ่งอาจทำในรูปแบบเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ก็ได้ โดยการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นจะต้องแจ้งเจ้าของข้อมูลก่อนหรือขณะเก็บรวบรวม เกี่ยวกับรายละเอียดในการประมวลผลไว้ในประกาศความเป็นส่วนตัว

3. การใช้และเปิดเผยข้อมูลส่วนบุคคล (Data Usage and Data Disclosure)

การเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่นที่เกี่ยวข้อง สามารถกระทำได้เพื่อบรรลุวัตถุประสงค์ในการประมวลผลข้อมูล หรือเป็นการเปิดเผยโดยมีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ดังกล่าว หรือเป็นการเปิดเผยเพื่อปฏิบัติตามกฎหมายหรือเป็นไปตามคำสั่งของหน่วยงาน

โดยจะต้องมีการแจ้งกับเจ้าของข้อมูลถึงความจำเป็นในการใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์ใดก่อนหรือขณะเก็บรวบรวมข้อมูลจากเจ้าของข้อมูลอีกทั้งต้องระบุประเภทของบุคคลหรือหน่วยงานที่ข้อมูลส่วนบุคคลอาจถูกทำการเปิดเผยอย่างชัดเจนไว้ในประกาศความเป็นส่วนตัว (Privacy Notice)

3.1 แนวปฏิบัติในการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการในประเทศ

ในกรณีที่บริษัทอาจมีโครงสร้างการถือหุ้นโดยมีบริษัทแม่หรือมีบริษัท Holding Company ที่ถือหุ้นของบริษัทในเครืออยู่ บริษัทจึงอาจมีความจำเป็นในการเปิดเผยข้อมูลส่วนบุคคลระหว่างกันภายในกลุ่มบริษัทในเครือที่อยู่ในประเทศ เช่น เพื่อวัตถุประสงค์ในการให้บริการแก่ลูกค้า เพื่อการบริหารความเสี่ยงภายในกลุ่มเครือกิจการ เป็นต้น ให้บริษัททำการแจ้งรายละเอียดแก่เจ้าของข้อมูลไว้ในประกาศความเป็นส่วนตัว (Privacy Notice) โดยระบุถึงความจำเป็นในการเปิดเผยข้อมูลภายในบริษัทในเครือ และประเภทของบุคคลหรือหน่วยงานด้วย สำหรับฐานตามกฎหมายในการเปิดเผยข้อมูลส่วนบุคคลนั้น ขึ้นอยู่กับกิจกรรมการประมวลผลข้อมูล อย่างไรก็

ตามแม้ว่าจะเป็นการเปิดเผยข้อมูลระหว่างบริษัทในเครือเดียวกัน บริษัทควรจะต้องจัดทำนโยบายในการเปิดเผยข้อมูลระหว่างเครือกิจการ เพื่อให้บริษัทในเครือมีแนวปฏิบัติเป็นไปในทิศทางเดียวกัน เป็นมาตรฐานเดียวกัน และพนักงานทุกคนจะต้องทราบและปฏิบัติตามซึ่งนโยบายควรมีการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลอย่างเหมาะสม ให้เพียงเฉพาะบุคคลหรือแผนกที่จำเป็นต้องใช้ในการประมวลผลตามวัตถุประสงค์เท่านั้น ภายใต้หลักการ “Need to know” และ“Need to use” เพื่อเป็นการป้องกันการเข้าถึง เปลี่ยนแปลง แก้ไขข้อมูลโดยมิชอบหรืออาจถูกนำไปใช้นอกเหนือจากวัตถุประสงค์ในการประมวลผลข้อมูล มีมาตรการในรักษาความปลอดภัยของข้อมูล ทั้งในเชิงบริหารจัดการและเชิงเทคนิค และมีการตรวจสอบ ติดตามผลการปฏิบัติตามนโยบายหรือแนวปฏิบัติการปฏิบัติงานอย่างสม่ำเสมอ

แนวปฏิบัติการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ (Cross-border data transfer)

ในกรณีที่อาจมีความจำเป็นจะต้องส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ หรือองค์การระหว่างประเทศ ประเทศที่รับข้อมูลส่วนบุคคลดังกล่าวจะต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและเป็นไปตามประกาศกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ ซึ่งสามารถทำได้ในกรณีดังต่อไปนี้

ประเทศหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

การพิจารณาความเพียงพอของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศที่รับโอนข้อมูลส่วนบุคคล (Adequacy of the Level of Protection) พิจารณาจาก

- กฎหมายของประเทศดังกล่าวว่ามีการคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐานจากกฎหมายที่เกี่ยวข้องทั้งในภาพรวมหรือกฎหมายเฉพาะรวมถึงการรักษาความมั่นคงของชาติ กฎหมายอาญา การเข้าถึงข้อมูลส่วนบุคคลของหน่วยงานรัฐ การบังคับใช้กฎหมาย กฎเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคล กฎเกณฑ์ของผู้ประกอบวิชาชีพ มาตรการในการรักษาความปลอดภัยของข้อมูล กฎเกณฑ์ในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ ความมีประสิทธิภาพในการบังคับใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล มาตรการเยียวยาแก่เจ้าของข้อมูลหากข้อมูลส่วนบุคคลที่ถูกโอนนั้นถูกละเมิด

- การมีอยู่และการทำงานขององค์กร/หน่วยงานอิสระในต่างประเทศหรือหน่วยงานระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล ว่ามีอำนาจหน้าที่ในการบังคับใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และอำนาจหน้าที่ในการให้ความช่วยเหลือเจ้าของข้อมูลส่วนบุคคล ในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลและอำนาจหน้าที่ในการร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของราชอาณาจักรไทย
- ข้อผูกพันระดับนานาชาติของประเทศหรือองค์การระหว่างประเทศที่รับโอนข้อมูลส่วนบุคคล เกิดจากการที่ประเทศหรือองค์การระหว่างประเทศผู้รับโอนได้เข้าผูกพันทางกฎหมาย โดยเฉพาะที่เกี่ยวข้องกับการ

คุ้มครองข้อมูลส่วนบุคคล เช่น อนุสัญญาที่มีผลบังคับผูกพันทางกฎหมาย หรือ การเข้าร่วมในระบบพหุภาคีหรือภูมิภาค

กรณีที่ได้รับการยกเว้นตามกฎหมาย

สามารถทำการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศได้ แม้ว่ามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางมีไม่เพียงพอหากเข้ากรณียกเว้นตามกฎหมายดังต่อไปนี้

- เป็นการปฏิบัติตามกฎหมาย
- ได้รับการยินยอมจากเจ้าของข้อมูลโดยได้แจ้งให้เจ้าของข้อมูลทราบถึงมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
- เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลก่อนเข้าทำสัญญานั้น
- เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูล
- เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลไม่สามารถให้ความยินยอมในขณะนั้นได้
- เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

กรณีที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ(Transfers Subject to Appropriate Safeguards)

- การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน สามารถทำได้ตามข้อกำหนดของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)
- ใช้มาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม ที่สามารถบังคับสิทธิของเจ้าของข้อมูลแทนได้ ดังนี้
    - ข้อสัญญาที่เกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Standard Data Protection Clauses) ที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอนุมัติ
    - หลักปฏิบัติด้านจรรยาบรรณ (Code of Conduct) ซึ่งจะต้องมีผลผูกพันและบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศหรือองค์การระหว่างประเทศ ในการจัดให้มีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม รวมถึงการบังคับใช้สิทธิของเจ้าของข้อมูล
    - คำรับรองเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Certification Mechanism) ซึ่งคำรับรองดังกล่าวต้องมีผลผูกพันและบังคับใช้กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศหรือองค์การระหว่างประเทศ ในการจัดให้มีมาตรการคุ้มครองข้อมูลอย่างเหมาะสม รวมถึงการบังคับใช้สิทธิของเจ้าของข้อมูล

- ข้อสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Contractual Clauses) กับผู้ประมวลผลหรือผู้รับข้อมูลส่วนบุคคลในประเทศปลายทาง
- ข้อบัญญัติเพิ่มเติม ในข้อตกลงการบริหารงานระหว่างหน่วยงานสาธารณะ (Provision to be Inserted into Administrative Arrangements Between Public Authorities) ซึ่งมีผลบังคับใช้กับการใช้สิทธิของเจ้าของข้อมูล

แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเมื่อมีการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศ

กรณีการเปิดเผยข้อมูลภายในกลุ่มเครือกิจการหรือเครือธุรกิจเดียวกันซึ่งอยู่ต่างประเทศ ให้มีแนวปฏิบัติดังนี้

ให้มี นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)เพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือประกอบธุรกิจร่วมกัน ซึ่งนโยบายดังกล่าวเป็นการกำหนดแนวทางในการปฏิบัติของกลุ่มเครือกิจการในการโอนข้อมูลระหว่างกัน โดยจะต้องมีการบังคับใช้กับทุกบริษัทในเครือ ซึ่งมีสาระสำคัญของนโยบายดังต่อไปนี้

- กำหนดให้นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการมีสภาพบังคับตามกฎหมายและให้มีผลบังคับใช้กับทุกสมาชิกของบริษัทในเครือ รวมถึงลูกจ้างและพนักงานของสมาชิก
- กำหนดให้นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการรับรองสิทธิของเจ้าของข้อมูลที่เกี่ยวกับการประมวลผลข้อมูล
- โครงสร้างและรายละเอียดการติดต่อของแต่ละสมาชิกของกลุ่มกิจการหรือกลุ่มบริษัทที่มีส่วนร่วมในการประกอบกิจการร่วมกัน
- อธิบายขอบเขตของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทในเครือรวมถึงสภาพของการส่งหรือโอนข้อมูล ประเภทเจ้าของข้อมูลส่วนบุคคล และประเทศที่อยู่ในขอบเขต
- การใช้หลักการในการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะอย่างยิ่งการประมวลผลข้อมูลตามวัตถุประสงค์ การเก็บรวบรวมข้อมูลเฉพาะเท่าที่จำเป็น ระยะเวลาในการเก็บ การรักษาความปลอดภัยของข้อมูล ฐานการประมวลผลข้อมูลตามกฎหมาย เป็นต้น
- สิทธิของเจ้าของข้อมูลและวิธีการหรือช่องทางในการใช้สิทธิของเจ้าของข้อมูล
- หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) หรือบุคคลที่ทำหน้าที่รับผิดชอบในการตรวจสอบการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของสมาชิกของกลุ่มเครือกิจการ อีกทั้ง การติดตามการฝึกอบรมให้ความรู้แก่พนักงาน การจัดการกับข้อร้องเรียน
- กลไกในการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มเครือกิจการ เพื่อให้มั่นใจว่ามีการตรวจสอบและประเมินการปฏิบัติตาม นโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการรวมทั้งตรวจสอบการปกป้อง

สิทธิของเจ้าของข้อมูล เช่น การดำเนินการตามเรื่องร้องขอของเจ้าของข้อมูล การดำเนินการแก้ไขเมื่อได้รับเรื่องร้องเรียน

- การอบรมให้ความรู้แก่พนักงานที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้
- มาตรการรับเรื่องร้องเรียนที่เหมาะสม
- กำหนดหน้าที่ในการให้ความร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ควรติดตามความเหมาะสมของการใช้งานข้อมูลส่วนบุคคลว่ามีการใช้ข้อมูลส่วนบุคคลเป็นไปตามข้อกำหนดในนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการหรือไม่ และมีการตรวจสอบให้แน่ใจว่ามีการทำลายข้อมูลส่วนบุคคลอย่างเหมาะสมหลังจากที่สิ้นสุดความจำเป็นในการใช้งานหรือตามระยะเวลาการเก็บข้อมูลส่วนบุคคลที่กำหนดในนโยบายดังกล่าว

3.2 การประมวลผลข้อมูลเพื่อวัตถุประสงค์เฉพาะ

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรง (Direct Marketing)

การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ในการทำการตลาดแบบตรงซึ่งทำผ่านช่องทางต่างๆ เช่น การโทรติดต่อ การส่งอีเมล ข้อความSMS โทรสาร หรืออื่นๆ เพื่อนำเสนอข้อมูลเกี่ยวกับผลิตภัณฑ์แก่ลูกค้า สามารถแบ่งได้เป็นหลากหลายกรณีดังต่อไปนี้

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทอื่น**

  สามารถประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรมเพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ให้เหมาะสมกับความต้องการของลูกค้ามากยิ่งขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำการเสนอผลิตภัณฑ์อื่นๆ

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกันหรือใกล้เคียงกันกับที่ลูกค้ามีอยู่**

  สามารถประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรมเพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ให้เหมาะสมกับความต้องการของลูกค้ามากยิ่งขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำข้อเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียงกับที่ลูกค้ามีอยู่ก่อนแล้ว

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทอื่น ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ (กรณีที่มีการเปิดเผยข้อมูลส่วนบุคคล)**

  ต้องทำการขอความยินยอมจากลูกค้า (ตาม Market Conduct) ในกรณีที่ต้องการเปิดเผยข้อมูลส่วนบุคคลที่มีอยู่ให้กับกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจสำหรับการประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทาง

ธุรกิจให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์อื่นของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกัน/ ใกล้เคียงกับที่ลูกค้ามีอยู่ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ (กรณีที่มีการเปิดเผยข้อมูลส่วนบุคคล)**

  ต้องทำการขอความยินยอมจากลูกค้า (ตาม Market Conduct) ในกรณีที่ต้องการเปิดเผยข้อมูลส่วนบุคคลที่มีอยู่ให้กับกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจสำหรับการประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนา ผลิตภัณฑ์ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น หรือเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเทภเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์อื่น ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจ**
  (กรณีที่ไม่ได้มีการเปิดเผยข้อมูลส่วนบุคคล)

  สามารถประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานประโยชน์อันชอบธรรม เพื่อวัตถุประสงค์ในการนำเสนอผลิตภัณฑ์ของกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจให้เหมาะสมกับความต้องการของลูกค้ามากขึ้น และเพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียง รวมถึงผลิตภัณฑ์อื่น ซึ่งผลิตภัณฑ์และบริการที่นำเสนอแก่ลูกค้าจะเป็นผลิตภัณฑ์ที่สามารถนำเสนอได้ภายใต้ใบอนุญาตที่มีอยู่ โดยมิได้มีการเปิดเผยข้อมูลลูกค้าออกไปยังกลุ่มธุรกิจทางการเงินและ/หรือพันธมิตรทางธุรกิจแต่อย่างใด

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์อื่น(ข้อมูลที่เก็บอยู่ก่อนวันที่1 มิ.ย.2565)**

  สำหรับข้อมูลที่เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ ซึ่งบริษัท ได้ทำการเก็บรวบรวมและใช้ข้อมูล ตามวัตถุประสงค์เดิม อันได้แก่ เพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการทำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียงกับที่ลูกค้ามีอยู่ รวมทั้งการนำเสนอผลิตภัณฑ์อื่น การประมวลผลดังกล่าวบริษัทสามารถทำได้ภายใต้ฐานประโยชน์อันชอบธรรม

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลเพื่อการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์อื่น (ข้อมูลที่เก็บอยู่หลังวันที่1 มิ.ย.2565)**

  สำหรับข้อมูลที่เก็บรวบรวมไว้หลังวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลมีผลใช้บังคับ ซึ่งบริษัท ได้ทำการเก็บรวบรวมและใช้ข้อมูล ตามวัตถุประสงค์เดิม อันได้แก่ เพื่อขยายสิทธิประโยชน์แก่ลูกค้าผ่านการนำเสนอผลิตภัณฑ์ประเภทเดียวกันกับที่ลูกค้ามีอยู่หรือผลิตภัณฑ์ประเภทที่ใกล้เคียง

กับที่ลูกค้ามีอยู่ รวมทั้งการนำเสนอผลิตภัณฑ์อื่นบริษัทสามารถทำได้ภายใต้ฐานประโยชน์อันชอบธรรม

- **การวิเคราะห์ข้อมูลหรือการใช้ข้อมูลส่วนบุคคลจากแหล่งอื่น (Lead Management)**

ในกรณีที่บริษัทได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น เช่น การซื้อข้อมูลลูกค้าจากบริษัทอื่นข้อมูลดังกล่าวมีรายละเอียดของเจ้าของข้อมูลส่วนบุคคล อันได้แก่ ชื่อ นามสกุล รายละเอียดการติดต่อ บริษัทไม่ต้องขอความยินยอมซ้ำจากเจ้าของข้อมูลส่วนบุคคลอีก แต่ให้บริษัทที่ทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้ขอความยินยอมในการเปิดเผยข้อมูลให้กับบริษัทแต่แรกจากเจ้าของข้อมูลส่วนบุคคล โดยบริษัทสามารถเก็บรวบรวม ใช้ข้อมูลส่วนบุคคลได้ตามวัตถุประสงค์ที่เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมไว้

ในกรณีที่บริษัท ได้มีการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งข้อมูลสาธารณะเช่น กรมพัฒนาธุรกิจการค้า เฟสบุ๊ค หรือเว็บไซต์สาธารณะอื่นๆ บริษัทจะต้องขอความยินยอมจากลูกค้าในการเก็บรวบรวมใช้ข้อมูลส่วนบุคคลภายในระยะเวลา 30 วัน หลังจากได้รับข้อมูลดังกล่าว และเมื่อลูกค้าให้ความยินยอมแล้ว บริษัทจึงจะสามารถใช้ข้อมูลดังกล่าวต่อไปได้

อย่างไรก็ตามกรณีที่กล่าวข้างต้นใดที่บริษัทไม่ได้ทำการขอความยินยอมจากลูกค้าในรูปแบบของ Opt-in Consent แต่ทำการเก็บรวบรวม ใช้ เพื่อวัตถุประสงค์ในการวิเคราะห์/วิจัย/พัฒนาผลิตภัณฑ์ หรือเพื่อวัตถุประสงค์ทางการตลาด ภายใต้ฐานผลประโยชน์อันชอบธรรม บริษัทสามารถประมวลผลข้อมูลภายใต้ฐานดังกล่าวได้ หากบริษัทสามารถพิสูจน์ได้ว่าผลประโยชน์อันชอบธรรมของบริษัทหรือของบุคคลที่สามมีความสำคัญมากกว่าสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

ทั้งนี้บริษัทจะแจ้งรายละเอียดหรือวิธีการใด ๆ ที่ให้เจ้าของข้อมูลส่วนบุคคลทราบเพื่อให้เจ้าของข้อมูลส่วนบุคคลจะสามารถแจ้งความประสงค์ในการปฏิเสธการรับข่าวสาร (Opt-out) หรือใช้สิทธิคัดค้านการประมวลผลได้ โดยการใช้สิทธินั้นสามารถทำได้ผ่านช่องทางการติดต่อที่ง่ายและสะดวกในการจัดการและการเข้าถึงรวมทั้งมีกระบวนการภายในที่จะสามารถแยกข้อมูลลูกค้าที่จะไม่ประสงค์รับการติดต่อจากบริษัทในการขายผลิตภัณฑ์ได้

4. การเก็บข้อมูลส่วนบุคคลและระยะเวลาในการเก็บ (Data Retention)

บริษัท จะทำการเก็บข้อมูลส่วนบุคคลตามระยะเวลาในการเก็บรักษาเฉพาะเท่าที่จำเป็นตามที่ต้องบรรลุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลหรือตามที่เจ้าของข้อมูลร้องขอหรือเก็บตามข้อกำหนดของกฎหมายที่บริษัท จำเป็นต้องปฏิบัติ เมื่อสิ้นสุดระยะเวลาในการเก็บรักษาแล้วบริษัท จะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลดังกล่าวตามมาตรฐานของการเก็บรวบรวมข้อมูลนั้น ๆ

แนวปฏิบัติเกี่ยวกับระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลตามหลักการในการคุ้มครองข้อมูลส่วนบุคคล โดยจะมีการระบุระยะเวลาในการเก็บรักษาตามเกณฑ์ที่บริษัทใช้ในการพิจารณาระยะเวลาในการเก็บข้อมูลส่วนบุคคลตามแต่ละกรณี เช่น ภาระผูกพันตามกฎหมายที่ต้องเก็บตามระยะเวลาที่กำหนดไว้ในนโยบายความเป็นส่วนตัวหรือนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้ บริษัท ยังจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลดำเนินการร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคลหรือถอนความยินยอมบริษัทจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลนั้น เว้นแต่เป็นไปตามข้อยกเว้นตามกฎหมาย

การลบหรือทำลายข้อมูลส่วนบุคคล (Data Deletion or Data Destruction)

เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล หรือไม่เกี่ยวข้องเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล บริษัทจะดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล โดยการทำให้ข้อมูลส่วนบุคคลนั้นถูกลบออกจากระบบและไม่อาจกู้คืนได้โดยตัวเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ทั้งนี้ ไม่ว่าในเวลาใด ๆ หรือทำให้ข้อมูลส่วนบุคคลอยู่ในลักษณะที่ไม่สามารถระบุตัวบุคคลของเจ้าของข้อมูลส่วนบุคคลได้

อีกทั้งบริษัท ยังจัดให้มีระบบการตรวจสอบข้อมูลเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อสิ้นสุดความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลดำเนินการร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคล หรือถอนความยินยอม เว้นแต่เป็นกรณีที่ได้รับยกเว้นตามกฎหมาย โดยบริหารจัดการข้อมูลส่วนบุคคลด้วยมาตรการเชิงเทคนิคและ/หรือมาตรการเชิงบริหารจัดการ เพื่อเพิ่มมาตรฐานในการรักษาความปลอดภัยในการคุ้มครองข้อมูลอย่างเหมาะสมและมีประสิทธิภาพ สามารถทำการตรวจสอบได้ว่าข้อมูลจะต้องถูกลบและทำลายภายใต้เงื่อนไขใด เช่น เมื่อสิ้นสุดระยะเวลาในการเก็บ เป็นต้น

ทั้งนี้ บริษัท อาจพิจารณาการลบ ทำลายข้อมูล หรืออาจทำข้อมูลให้อยู่ในรูปของข้อมูลนิรนาม (Anonymization) ซึ่งเป็นวิธีการที่จะทำให้ข้อมูลไม่สามารถระบุตัวตนได้ ในการนี้บริษัท จะพิจารณาเลือกใช้วิธีการใดโดยประเมินจากผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล (Impact) และโอกาสที่อาจเกิดขึ้น (Likelihood) จากการถูกละเมิดข้อมูลส่วนบุคคล

แนวปฏิบัติเกี่ยวกับการทำข้อมูลนิรนาม (Data Anonymization)

การจัดทำข้อมูลนิรนาม หมายถึงกระบวนการแปลงข้อมูลส่วนบุคคลให้เป็นข้อมูลที่ไม่สามารถใช้ระบุตัวตนของบุคคลใดบุคคลหนึ่งได้ และทำเพื่อเหตุผลให้ข้อมูลส่วนบุคคลมีความเหมาะสมสำหรับการใช้งานมากกว่าในรูปแบบเดิมอีกด้วย ทั้งนี้ข้อมูลที่ถูกทำการนิรนาม ตามกฎหมายจะไม่ถือว่ามีสถานะเป็นข้อมูลส่วนบุคคลอีกต่อไป และเป็นการทำให้ความเสี่ยงจากผลกระทบที่อาจเกิดขึ้นเนื่องจากการถูกละเมิดความปลอดภัยของข้อมูลลดลง

บริษัท อาจจัดทำข้อมูลนิรนามโดยใช้มาตรการเชิงเทคนิควิธีใดวิธีหนึ่งโดยเฉพาะหรือใช้หลายวิธีร่วมกันตามความเหมาะสม และเป็นไปตามนโยบายการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศของบริษัท โดยมีวิธีการต่างๆ กล่าวคือ การแฝงข้อมูล (Pseudonymisation), การรวมกลุ่มข้อมูล (Aggregation), การแทนที่ (Replacement), การสกัดกั้นข้อมูล (Data Suppression), การกล่าวอย่างกว้าง (Data recoding or generalization), การสับเปลี่ยนข้อมูล (Data Shuffling), การบังข้อมูล (Masking)

ในกรณีที่ข้อมูลส่วนบุคคลที่บริษัทได้เก็บรวบรวมไว้ก่อนวันที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลใช้บังคับบริษัทจะดำเนินการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปตามวัตถุประสงค์เดิม ทั้งนี้บริษัท จะกำหนดวิธีการยกเลิกความยินยอมและเผยแพร่ประชาสัมพันธ์ให้กับเจ้าของข้อมูลที่ไม่ประสงค์ให้บริษัทเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่ายและหากเจ้าของข้อมูลถอนความยินยอมแล้วบริษัทจะไม่ทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ถูกถอนไปแล้วอีกเว้นแต่จะเข้าข้อยกเว้นตามกฎหมาย

5. แนวปฏิบัติเกี่ยวกับการดำเนินการตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

บริษัท ได้ดำเนินการให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานรับเรื่องร้องเรียน หรือContact Center ของบริษัท ทำหน้าที่ในการรับเรื่องจากเจ้าของข้อมูลสำหรับการร้องขอใช้สิทธิของเจ้าของข้อมูล ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ในเรื่องต่างๆ ดังนี้

1. สิทธิในการถอนความยินยอม (Right to Withdraw of Consent)

เจ้าของข้อมูลมีสิทธิในการขอเพิกถอนความยินยอมที่เคยให้ไว้กับผู้ควบคุมข้อมูลส่วนบุคคล ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลเมื่อใดก็ได้ โดยผ่านช่องทางที่เจ้าของข้อมูลสามารถใช้สิทธิกระทำได้โดยง่ายในระดับเดียวกับการให้ความยินยอม

หากไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยต่อไป ผู้ควบคุมข้อมูลส่วนบุคคลจะดำเนินการลบข้อมูลออกโดยไม่ล่าช้านับแต่ที่ได้ทราบถึงการใช้สิทธิของเจ้าของข้อมูล ทั้งนี้ระยะเวลาในการปฏิบัติตามสิทธิให้เป็นไปตามนโยบายที่เหมาะสมของผู้ควบคุมข้อมูลส่วนบุคคล อีกทั้งดำเนินการแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่นๆ เพื่อให้ปฏิบัติตามคำขอดังกล่าวด้วย รวมทั้งให้มีการบันทึกรายการคำขอดังกล่าวประกอบด้วย

2. สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (Right to Access)

เจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนที่อยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลดังกล่าวที่เจ้าของข้อมูลไม่ได้ให้ความยินยอมไว้ เพื่อเป็นการยืนยันจากผู้ควบคุมข้อมูลส่วนบุคคลว่า ข้อมูลส่วนบุคคลดังกล่าวกำลังถูกประมวลผลหรือไม่อย่างไร

เมื่อได้รับคำขอแล้วให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามคำขอดังกล่าวโดยไม่ชักช้าและต้องไม่เกิน 30 วัน โดยไม่มีค่าธรรมเนียมใดๆ ในการใช้สิทธิเว้นแต่เจ้าของข้อมูลมีการขอรับ

สำเนาเพิ่มเติมมากจนเกินความจำเป็นแต่ทั้งนี้ ผู้ควบคุมส่วนบุคคลสามารถปฏิเสธคำขอดังกล่าวได้ โดยให้มีการบันทึกการปฏิเสธดังกล่าวพร้อมด้วยเหตุผลประกอบ ในกรณีต่อไปนี้

- เป็นการปฏิเสธตามกฎหมาย หรือ ตามคำสั่งศาล
- การใช้สิทธิในการเข้าถึงและการขอรับสำเนาข้อมูลส่วนบุคคลนั้นส่งผลกระทบที่อาจก่อให้เกิดความเสียหายต่อสิทธิและเสรีภาพของบุคคลอื่น

ทั้งนี้ หากข้อมูลที่เก็บรวบรวมมีข้อมูลส่วนบุคคลของบุคคลที่สามรวมเกี่ยวข้องอยู่ด้วย ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะไม่เปิดเผยข้อมูลเฉพาะของบุคคลที่สามได้ แต่ไม่สามารถปฏิเสธการเข้าถึงข้อมูลและขอรับสำเนาของเจ้าของข้อมูลได้

3. สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (Right to Rectification)

เจ้าของข้อมูลมีสิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง สมบูรณ์ เป็นปัจจุบันเพื่อไม่ก่อให้เกิดความเข้าใจผิด อันได้แก่

- กรณีที่ข้อมูลไม่สมบูรณ์ คือการที่ข้อมูลที่ผู้ควบคุมข้อมูลส่วนบุคคลมีอยู่นั้นถูกต้องแต่ได้รับข้อมูลมาไม่ครบถ้วน ไม่เพียงพอต่อการนำไปประมวลผลตามวัตถุประสงค์
- กรณีที่ข้อมูลไม่ถูกต้อง คือการที่ข้อมูลไม่ตรงกับความจริง

ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการแก้ไขโดยไม่ชักช้า ในระหว่างการดำเนินการแก้ไขนั้น เจ้าของข้อมูลมีสิทธิที่จะขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการประมวลผลชั่วคราวในระหว่างการตรวจสอบความถูกต้องของข้อมูล และดำเนินการแก้ไขข้อมูลส่วนบุคคลก่อนประมวลผลอีกครั้ง

อย่างไรก็ตามเพื่อป้องกันผลกระทบจากการประมวลผลข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ผู้ควบคุมข้อมูลส่วนบุคคลจะทำการระงับการประมวลผลแม้ว่าเจ้าของข้อมูลจะใช้สิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการประมวลผลข้อมูลส่วนบุคคลหรือไม่ก็ตาม

นอกจากนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะทำการแจ้งแก่บุคคลที่สามที่ข้อมูลส่วนบุคคลถูกเปิดเผย เช่น ผู้ประมวลผลข้อมูลส่วนบุคคล ให้ทราบถึงการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลจะพิสูจน์ได้ว่าเป็นไปไม่ได้หรือเกินความพยายามตามสมควร ทั้งนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกคำร้องขอของเจ้าของข้อมูลพร้อมด้วยเหตุผล

บริษัท อาจกำหนดหลักเกณฑ์ในการพิสูจน์ความถูกต้องของข้อมูลส่วนบุคคล เช่น ให้เจ้าของข้อมูลนำหลักฐานที่เกี่ยวข้องมาประกอบการพิจารณา อย่างไรก็ตาม แม้เจ้าของข้อมูลจะมีสิทธิในการแก้ไขแต่บริษัท ยังคงมีหน้าที่ที่ต้องดำเนินการตามหลักการในการประมวลผลข้อมูล

ส่วนบุคคลอย่างถูกต้องเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลควรมีความถูกต้อง สมบูรณ์และเป็นปัจจุบัน ไม่ก่อให้เกิดความเข้าใจผิดและข้อมูลที่ไม่ถูกต้องจะต้องถูกลบหรือได้รับการแก้ไข

4. สิทธิในการลบหรือทำลายข้อมูลส่วนบุคคล (Right to Erasure or Right to be Forgotten)

เจ้าของข้อมูลมีสิทธิในการขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลดังกล่าวกลายเป็นข้อมูลที่ไม่สามารถใช้ระบุตัวตนของเจ้าของข้อมูลได้ ทั้งนี้ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการ และบันทึกการทำรายการคำขอดังกล่าวประกอบด้วยเหตุดังนี้

- ข้อมูลส่วนบุคคลดังกล่าวหมดความจำเป็นในการเก็บรักษาไว้ตามวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอีกต่อไป
- เจ้าของข้อมูลทำการถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคลไม่มีฐานโดยชอบด้วยกฎหมายอื่นที่จะทำการเก็บรวบรวม ใช้ หรือเปิดเผยอีกต่อไป
- เจ้าของข้อมูลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ในกรณีที่บริษัท เก็บรวบรวมข้อมูลส่วนบุคคลของตนไว้โดยได้รับยกเว้นไม่ต้องขอความยินยอม ภายใต้ฐานภารกิจของรัฐ หรือฐานประโยชน์อันชอบธรรม และบริษัท ไม่สามารถพิสูจน์ได้ว่ามีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าประโยชน์และสิทธิเสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล หรือเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เจ้าของข้อมูลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน เพื่อวัตถุประสงค์ที่เกี่ยวกับการตลาดแบบตรง
- เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมาย

อย่างไรก็ตามบริษัท สามารถปฏิเสธคำร้องขอในกรณีดังกล่าวข้างต้นได้หากพิสูจน์ได้ว่าการประมวลผลข้อมูลนั้นมีความจำเป็นในเรื่องดังต่อไปนี้

- บริษัท พิสูจน์ได้ว่า การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลนั้นได้แสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่า ประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล
- เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น
- เพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

- เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้รับมอบให้แก่บริษัท
- เป็นการจำเป็นเพื่อบรรลุวัตถุประสงค์เกี่ยวกับเวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ หรือประโยชน์ด้านสาธารณสุข

5. สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล (Right to Restriction of Processing)
   - -เจ้าของข้อมูลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของตน เพื่อวัตถุประสงค์ที่เกี่ยวกับการตลาดแบบตรง
   - -เมื่อบริษัท อยู่ในระหว่างการตรวจสอบข้อมูลตามคำร้องขอใช้สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง
   - -เมื่อเป็นข้อมูลที่ต้องทำการลบหรือทำลาย เนื่องจากการประมวลผลข้อมูลส่วนบุคคลอันมิชอบด้วยกฎหมาย แต่เจ้าของข้อมูลใช้สิทธิในการขอให้ระงับการใช้แทนการลบหรือทำลายข้อมูลส่วนบุคคลของตน
   - -เมื่อข้อมูลส่วนบุคคลไม่จำเป็นในการเก็บรักษาไว้ ตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลอีกต่อไป แต่เจ้าของข้อมูลมีความจำเป็นที่ต้องขอให้การเก็บรักษาไว้ เพื่อใช้ในการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
   - เมื่อบริษัท อยู่ในระหว่างการพิสูจน์ข้ออ้างที่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลนั้นมีเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล
   - บริษัท อยู่ในระหว่างการตรวจสอบเพื่อดำเนินการปฏิเสธการคัดค้านการประมวลผลของเจ้าของข้อมูล ในกรณีที่บริษัท เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ว่าเป็นไปตามข้อยกเว้นที่บริษัท สามารถประมวลผลได้เนื่องจากเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของบริษัท

กรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำร้องขอดังกล่าวและอยู่ในระหว่างการโต้แย้งกับเจ้าของข้อมูลที่ร้องขอใช้สิทธิ บริษัท จะจัดให้มีมาตรการที่เหมาะสม ในการระงับการประมวลผลข้อมูลในระบบของบริษัท เช่น การระงับการให้ผู้ใช้ข้อมูลเข้าถึงข้อมูลชั่วคราว หรือการแยกส่วนข้อมูลที่ถูกระงับออกจากข้อมูลอื่นชั่วคราว เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นจะไม่ถูกนำไปประมวลผลข้อมูลส่วนบุคคล

6. สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (Right to Object)

เจ้าของข้อมูลมีสิทธิในการคัดค้านการประมวลผลข้อมูลของตนเมื่อใดก็ได้ เมื่อเข้าเงื่อนไข ดังต่อไปนี้

กรณีที่ข้อมูลส่วนบุคคลที่บริษัท ทำการเก็บรวบรวมได้รับยกเว้นไม่ต้องขอความยินยอม เฉพาะในกรณีดังนี้

- เพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่บริษัท
- เป็นการจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของบริษัท หรือของบุคคลอื่น

อย่างไรก็ตามกรณีนี้ บริษัท สามารถปฏิเสธคำร้องขอดังกล่าวได้หากบริษัท สามารถพิสูจน์ได้ว่าการประมวลผลข้อมูลนั้นแสดงให้เห็นถึงเหตุอันชอบด้วยกฎหมายที่สำคัญยิ่งกว่าผลประโยชน์ สิทธิ เสรีภาพขั้นพื้นฐานของเจ้าของข้อมูล หรือการประมวลผลข้อมูลส่วนบุคคลนั้นทำเพื่อก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย ทั้งนี้ให้ทำบันทึกคำร้องขอของเจ้าของข้อมูลพร้อมด้วยเหตุผลประกอบ

กรณีที่บริษัท ทำการประมวลผลข้อมูลส่วนบุคคล เพื่อวัตถุประสงค์ที่เกี่ยวข้องกับการตลาดแบบตรง (Direct marketing)

กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ

อย่างไรก็ตามกรณีนี้ บริษัท สามารถปฏิเสธคำร้องขอดังกล่าวได้หากเป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะของบริษัท ทั้งนี้ให้ทำบันทึกคำร้องขอของเจ้าของข้อมูลพร้อมด้วยเหตุผลประกอบ

หากไม่มีกรณีปฏิเสธคำร้องขอ ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติโดยแยกส่วนออกจากข้อมูลอื่นอย่างชัดเจนและดำเนินการในทันที เมื่อเจ้าของข้อมูลได้แจ้งการคัดค้านดังกล่าวให้ทราบ

7. สิทธิในการขอรับหรือโอนย้ายข้อมูลส่วนบุคคล (Right to Data Portability)

เจ้าของข้อมูลมีสิทธิขอรับข้อมูลที่เกี่ยวกับตนจากบริษัท ในกรณีที่มีการทำให้ข้อมูลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือ ใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรือ อุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยได้ด้วยวิธีการอัตโนมัติ รวมทั้ง มีสิทธิขอให้บริษัทส่งหรือโอนข้อมูลในรูปแบบดังกล่าวไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นเมื่อสามารถทำได้ด้วยวิธีการอัตโนมัติ

อย่างไรก็ตามกรณีนี้ บริษัทสามารถปฏิเสธคำร้องขอได้หากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะหรือเป็นการปฏิบัติหน้าที่ตามกฎหมายหรือ

การใช้สิทธินั้นเป็นการละเมิดสิทธิเสรีภาพของบุคคลอื่น โดยผู้ควบคุมข้อมูลส่วนบุคคลจะทำการบันทึกคำร้องขอของเจ้าของข้อมูลพร้อมด้วยเหตุผลประกอบ

มีสิทธิขอรับข้อมูลที่บริษัท ส่งหรือโอนข้อมูลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่นโดยตรง เว้นแต่สภาพทางเทคนิคไม่สามารถทำได้

จากที่กล่าวข้างต้นบริษัท จึงจัดให้มีกระบวนการบริหารจัดการที่ชัดเจนในกรณีที่เจ้าของข้อมูลมายื่นคำร้องขอใช้สิทธิของตน โดยมอบหมายงานหรือจัดตั้งหน่วยงานภายใน ในการดูแลรับเรื่องดังกล่าว พร้อมทั้งแต่งตั้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เป็นผู้รับผิดชอบในการพิจารณาการใช้สิทธิของเจ้าของข้อมูลว่าสามารถดำเนินการให้ได้หรือไม่ พร้อมทั้งจัดให้มีช่องทางการติดต่อที่เหมาะสมในการยื่นคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

6. แนวปฏิบัติเกี่ยวกับหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล (Guideline on Data Controller and Data Processor Roles and Responsibilities)

6.1 การระบุสถานะในการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

บริษัท อาจทำหน้าที่เป็นทั้งผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งขึ้นอยู่กับชุดข้อมูลที่ทำการประมวลผล โดยหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลจะเป็นผู้ที่กำหนดวัตถุประสงค์และสามารถตัดสินใจในเรื่องของการประมวลผลข้อมูลส่วนบุคคลได้เอง แต่หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลจะปฏิบัติตามที่ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น

6.2 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller Roles and Responsibilities)

- ทำการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์อันชอบด้วยกฎหมายภายใต้มาตรการรักษาความปลอดภัยที่เหมาะสม ทั้งมาตรการเชิงเทคนิค(Technical Measure) และมาตรการเชิงบริหารจัดการ (Organizational Measure) ทั้งนี้เพื่อป้องกันการสูญหาย เข้าถึง ใช้ หรือเปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลโดยมิชอบ อีกทั้งทบทวนมาตรการการรักษาความปลอดภัยของข้อมูลเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงและปลอดภัยอย่างเหมาะสมอยู่เสมอ
- ในกรณีที่ต้องเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลหรือนิติบุคคลอื่น จะต้องดำเนินการป้องกัน ไม่ให้ผู้นั้นนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยมิชอบ
- จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการเก็บรักษาหรือที่ไม่เกี่ยวข้องเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลร้องขอ หรือที่เจ้าของข้อมูลได้ถอนความยินยอม เว้นแต่จะทำการเก็บรักษาไว้ภายใต้ข้อยกเว้นตามกฎหมาย

- หากเกิดเหตุการณ์ละเมิดขึ้น จะต้องแจ้งแก่ผู้กำกับดูแลข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับจากที่ได้รับทราบเหตุ เว้นแต่การละเมิดนั้นไม่มีความเสี่ยงที่จะส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล แต่หากเหตุการณ์ละเมิดนั้นมีความเสี่ยงสูงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลให้รีบแจ้งเหตุละเมิดนั้นแก่เจ้าของข้อมูลได้รับทราบด้วย รวมถึงหาแนวทางในการแก้ไขและเยียวยาโดยเร็วที่สุด
- จัดให้มี เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) เพื่อให้เจ้าของข้อมูลได้ติดต่อแจ้งความประสงค์ในการใช้สิทธิ และตรวจสอบการประมวลผลข้อมูลส่วนบุคคล หรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมาก หรือกิจกรรมหลักของบริษัท เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ทั้งนี้จะประกาศแจ้งช่องทางการติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไว้ใน Privacy Notice/ Privacy Policy ของบริษัท เพื่อให้เจ้าของข้อมูลสามารถติดต่อได้โดยง่าย
- ทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment : DPIA) ในกรณีที่การประมวลผลข้อมูลมีความเสี่ยงอันอาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
- ดำเนินการให้เป็นไปตามสิทธิของเจ้าของข้อมูล หากเจ้าของข้อมูลมีการร้องขอใช้สิทธิโดยไม่ชักช้า หากมีการปฏิเสธคำร้องขอตามเหตุแห่งการปฏิเสธการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลนั้น จะต้องทำการบันทึกคำร้องขอของเจ้าของข้อมูล พร้อมด้วยระบุเหตุผลการปฏิเสธ
- ทำการเลือกผู้ประมวลผลข้อมูลส่วนบุคคลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผลและการรักษาความมั่นคงปลอดภัยของข้อมูล
- จัดให้มีการทำข้อตกลงกันระหว่างบริษัท ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคล หรือที่เรียกว่า Data Processing Agreement เพื่อให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการให้เป็นไปตามกฎหมาย
- หากมีการโอนข้อมูลส่วนบุคคลระหว่างประเทศจะต้องทำโดยชอบด้วยกฎหมาย กล่าวคือ จะต้องมั่นใจว่าประเทศปลายทางที่รับข้อมูลส่วนบุคคลนั้นมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมเพียงพอ
- จัดให้มีการเก็บบันทึกเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ เพื่อให้เจ้าของข้อมูลและคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ภายหลัง โดยเก็บบันทึกรายการอย่างน้อย ประกอบด้วยดังนี้
    - ข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวม
    - วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
    - ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
    - ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
    - สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล

- การใช้หรือเปิดเผย
- การปฏิเสธคำขอหรือการคัดค้านตามข้อกำหนดของกฎหมาย
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยสำหรับหน้าที่ในการเก็บบันทึก

- กรณีที่บริษัท อยู่นอกราชอาณาจักรแต่อยู่ภายใต้การบังคับใช้ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล จะต้องแต่งตั้งตัวแทนของบริษัท ต่างประเทศ (ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล)เป็นหนังสือ ซึ่งตัวแทนดังกล่าวจะต้องอยู่ในราชอาณาจักร โดยจะต้องได้รับมอบอำนาจให้กระทำการแทนบริษัท ที่อยู่นอกราชอาณาจักรแบบไม่มีข้อจำกัดความรับผิดชอบใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ตามวัตถุประสงค์ของบริษัท ที่อยู่นอกราชอาณาจักร อย่างไรก็ตามจะได้รับยกเว้นไม่ต้องแต่งตั้งตัวแทนในราชอาณาจักรในกรณีที่บริษัท ที่อยู่นอกราชอาณาจักรไม่ได้มีการประมวลผลข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว และไม่ได้ประมวลผลข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
- มีหน้าที่ในการให้ความร่วมมือกับองค์กรกำกับดูแล หรือทำหน้าที่ตามกฎหมาย หรือตามคำสั่งของหน่วยงานรัฐ หรืออำนาจโดยชอบในการเข้าถึงข้อมูลส่วนบุคคล
- กรณีได้มีการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกอื่นใด แต่ละฝ่ายจะมีหน้าที่และความรับผิดชอบในฐานะผู้ควบคุมข้อมูลส่วนบุคคลแยกต่างหากจากกันตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

6.3 หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor Roles and Responsibilities)

การประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุมข้อมูลส่วนบุคคลอื่นจะต้องทำการประมวลผลข้อมูลตามที่ได้ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีข้อตกลงหรือสัญญาในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement)

แต่หากทำการประมวลผลนอกเหนือหรือขัดต่อคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล การกระทำดังกล่าวให้ถือว่าเป็นการทำหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลสำหรับการประมวลผลข้อมูลนั้นซึ่งจะต้องปฏิบัติตามหน้าที่และความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลสำหรับกรณีดังกล่าวด้วยสำหรับแนวปฏิบัติของผู้ประมวลผลข้อมูลส่วนบุคคล จะมีดังนี้

- ดำเนินการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น ไม่ทำการประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากที่ตกลงกับผู้ควบคุมข้อมูลส่วนบุคคลหากไม่ได้รับอนุญาตเป็นลายลักษณ์อักษร เว้นแต่คำสั่งดังกล่าวนั้นขัดต่อกฎหมาย
- จัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสม มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการ เพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง เพื่อป้องกันการสูญหาย การใช้ เปลี่ยนแปลง แก้ไข หรือการเปิดเผยข้อมูลโดยมิชอบ

- จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด เว้นแต่เป็นกิจการขนาดเล็ก อย่างไรก็ตามหากการประมวลผลข้อมูลนั้นก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีและเสรีภาพของเจ้าของข้อมูลหรือมีการประมวลผลข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือเป็นการประมวลผลข้อมูลอาชญากรรม ให้ทำการเก็บบันทึกการประมวลผลข้อมูลส่วนบุคคล โดยจะต้องจัดให้มีรายละเอียดการเก็บบันทึกรายการประมวลผลข้อมูลส่วนบุคคล เป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ประกอบด้วยดังนี้

    - ชื่อและข้อมูลการติดต่อกับบริษัท และผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทนหรือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
    - ประเภทการประมวลผลซึ่งกระทำแทนผู้ควบคุมข้อมูลส่วนบุคคล
    - การส่งข้อมูลไปยังต่างประเทศ (หากมี)
    - คำอธิบายเกี่ยวกับมาตรการเชิงเทคนิคและเชิงบริหารจัดการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

- ทำการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) หากมีการประมวลผลข้อมูลส่วนบุคคลมีความจำเป็นที่ต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการกำหนด หรือมีกิจกรรมหลักเป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว
- ทำการแจ้งเหตุแก่ผู้ควบคุมข้อมูลส่วนบุคคล กรณีที่ข้อมูลส่วนบุคคลเกิดการรั่วไหล (Data Breach) โดยไม่ชักช้าหลังจากทราบเหตุ

7. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นบุคคลที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำ ปรึกษา หรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้เป็นไปตามหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 อีกทั้งเป็นการบริหารความเสี่ยงในการบริหารจัดการข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพและประสิทธิผล

การแต่งตั้งและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

บริษัท สามารถแต่งตั้งจากบุคคลหรือคณะทำงานจากบุคลากรของบริษัท หรือสรรหาจากบุคคลภายนอกก็ได้ โดยจะต้องมีความรู้ความเข้าใจในด้านกฎหมายการคุ้มครองข้อมูลส่วนบุคคล มีความเข้าใจกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและ การรักษาความปลอดภัยของข้อมูลส่วนบุคคล งานด้านเทคโนโลยีสารสนเทศ อีกทั้งเข้าใจถึงภาพรวมธุรกิจของบริษัทและมีความสามารถในการสร้างวัฒนธรรมขององค์กรในการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Responsibility of DPO)

- ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล (ซึ่งหมายถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ควรให้คำแนะนำแก่พนักงานทุกคนของบริษัท รวมถึงผู้รับจ้างให้ทำการประมวลผลข้อมูลส่วนบุคคลของบริษัท)
- ทำการตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลประสานงานและให้ความร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่เกิดปัญหาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- รักษาความลับของข้อมูลส่วนบุคคลที่ได้ล่วงรู้หรือ

เพื่อให้การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เป็นไปอย่างมีประสิทธิภาพ และมีความเป็นอิสระในการปฏิบัติงาน จึงให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท สามารถรายงานตรงต่อผู้บริหารสูงสุดของบริษัท อีกทั้งได้รับสิทธิในเข้าถึงข้อมูลส่วนบุคคลที่จำเป็นเพื่อการปฏิบัติหน้าที่ อีกด้วย

นอกจากนั้น บริษัท ได้เล็งเห็นถึงความสำคัญของหน้าที่ในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวจึงให้เจ้าหน้าที่ทุกคนทุกระดับชั้น ให้ความร่วมมือในการปฏิบัติหน้าที่กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยการให้ข้อมูลหรือแจ้งเหตุความเป็นไปได้ที่จะเกิดการละเมิดของข้อมูลส่วนบุคคล หรือปัญหาต่างๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูล แก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับทราบเพื่อหาแนวทางการแก้ไขต่อไป

8. แนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

8.1 การกำหนดหน่วยงานเจ้าของข้อมูล (Information Owner หรือ Data Owner หรือ Data Owners)

กำหนดให้มีผู้บริหารจัดการข้อมูลเพื่อให้มั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย โดยมีหน้าที่ทำการทบทวนและอนุมัติ การดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล อาทิ การให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูลอย่างปลอดภัยและเหมาะสม ภายใต้ผู้กำกับดูแลข้อมูล

8.2 แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล (Data Classification)

การจำแนกข้อมูล หมายถึง กระบวนการที่เกี่ยวข้องกับการประเมินชุดข้อมูลและการรักษาความปลอดภัยของข้อมูล อันได้แก่ ข้อมูลความลับ ข้อมูลที่มีความอ่อนไหว ข้อมูลที่ต้องจัดให้มีเพื่อพร้อมสำหรับการใช้งาน และข้อมูลที่ต้องเปิดเผยตามข้อกำหนดของกฎหมาย เพื่อให้สามารถใช้ข้อมูลได้อย่างเหมาะสม อีกทั้งยังเป็นกระบวนการที่ทำให้การรักษาความปลอดภัยของข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่สำคัญอยู่ในระดับความเสี่ยงที่เหมาะสม ไม่ว่าข้อมูลนั้นจะถูกนำไปใช้งานหรือถูกเก็บไว้ในที่ใดก็ตาม

โดยได้นำหลักการการกำหนดผลกระทบที่อาจเกิดขึ้นจากการถูกละเมิดความปลอดภัยของข้อมูลส่วนบุคคลมากำหนดวัตถุประสงค์ด้านความปลอดภัย (Security Objective) ของข้อมูลแบ่งออกเป็น 3 ด้าน ดังนี้

- การรักษาความลับของข้อมูล (Confidentiality) คือ การจำกัดการเข้าถึง การเปิดเผย การปกป้องความเป็นส่วนตัว และสิทธิของข้อมูล
- ความถูกต้องสมบูรณ์ของข้อมูล (Integrity)คือ การรักษาความปลอดภัยของข้อมูลจากการดัดแปลงหรือถูกทำลายโดยไม่เหมาะสมรวมถึงการทำให้มั่นใจว่าข้อมูลมีความถูกต้อง
- ความพร้อมใช้งานของข้อมูล (Availability) คือ การทำให้มั่นใจว่าสามารถเข้าถึงข้อมูลและใช้งานได้อย่างทันเวลาและเชื่อถือได้

ทั้งนี้ บริษัท จัดให้มีการบริหารความเสี่ยงอย่างเหมาะสมจากการจำแนกข้อมูลตามความเสี่ยงและผลกระทบ โดยกำหนดระดับความเสี่ยงของข้อมูลส่วนบุคคลในชุดต่าง ๆ (Data Risk Level) และผลกระทบที่อาจเกิดขึ้น (Impact) หากถูกละเมิดความปลอดภัย ซึ่งสามารถแบ่งได้เป็น 3 ระดับ ดังนี้

- ผลกระทบระดับต่ำ (Low) คือ มีแนวโน้มที่จะมีผลกระทบอย่างจำกัด (Limited Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กร และบุคคล
- ผลกระทบระดับปานกลาง (Moderate)คือ มีแนวโน้มที่จะมีผลกระทบอย่างมาก (Serious Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล
- ผลกระทบระดับสูง (High) คือ มีแนวโน้มที่จะมีผลกระทบอย่างร้ายแรงหรือหายนะ (Severe or Catastrophic Adverse Effect) ต่อองค์กร ทรัพย์สินขององค์กรและบุคคล

โดยการแบ่งระดับของผลกระทบที่อาจเกิดขึ้นหากถูกละเมิดความปลอดภัยข้างต้น สอดคล้องกับนโยบายบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัท ที่กำหนดไว้

9. แนวปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

เพื่อเป็นการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล จะกระทำในกรณีที่การประมวลผลข้อมูลส่วนบุคคลนั้นมีระดับความเสี่ยงสูงอันอาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งจะช่วยให้สามารถกำกับดูแลการปฏิบัติตามกฎเกณฑ์ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งขึ้น ทั้งยังเป็นการสร้างความเชื่อมั่นและความไว้วางใจให้กับเจ้าของข้อมูลและผู้มีส่วนได้ส่วนเสีย อีกทั้งยังเป็นการลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่ไม่เหมาะสม โดยมีแนวทางปฏิบัติดังนี้

ความแตกต่างระหว่าง กระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล(Data Protection Impact Assessment :DPIA) กับ กระบวนการวิเคราะห์การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (PrivacyImpactAssessment :PIA)

กระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลเป็นกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลสำหรับกิจกรรมประมวลผลข้อมูลส่วนบุคคลต่าง ๆ ซึ่งทำเฉพาะกับระดับความเสี่ยงสูง นั่นคือมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล กระบวนการในจัดทำDPIA ได้แก่ การระบุความเสี่ยงและผลกระทบที่อาจเกิดขึ้นรวมถึงแนวทางการลดความเสี่ยงที่อาจเกิดขึ้นจากกิจกรรมการประมวลผลนั้น และต้องมีการทบทวนความเหมาะสมอยู่เสมอ เนื่องจากความเสี่ยงอาจเปลี่ยนแปลงได้จากปัจจัยหลายอย่าง เช่น การเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็วอาจทำให้ความเสี่ยงที่จะเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลมีระดับสูงขึ้น เป็นต้น

ส่วนกระบวนการวิเคราะห์การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นกระบวนการที่เกี่ยวข้องกับการวิเคราะห์ การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลว่าจะทำอย่างไร โดยที่ PIA เป็นกระบวนการที่ใช้ในการป้องกันในเรื่องของการจัดทำ Privacy by Design นั่นคือ การที่คำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบ ซึ่งมักทำเมื่อมีการเริ่มหรือเข้าควบรวมกิจการอื่น มีการใช้กระบวนการใหม่หรือออกผลิตภัณฑ์ใหม่ทั้งนี้อาจทำDPIA เพียงอย่างเดียวหรืออาจจัดทำPIA เข้ากับ DPIA ก็ได้เนื่องจากแนวทางในการจัดทำนั้นมีความคล้ายคลึงกัน อย่างไรก็ตามอาจพิจารณาการทำ PIA เพิ่มเติมเมื่อเห็นว่ามีความจำเป็น

9.1 แนวทางปฏิบัติเกี่ยวกับการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล(Data Protection Impact Assessment :DPIA)

มีกระบวนการที่จะต้องปฏิบัติตาม 4 ขั้นตอนต่อไปนี้เป็นอย่างน้อย

- ทำรายละเอียดของกิจกรรมการประมวลผลอย่างเป็นระบบ อันได้แก่กระบวนการหรือวิธีการประมวลผลข้อมูล วัตถุประสงค์ในการประมวลผลข้อมูลและประโยชน์อันชอบด้วยกฎหมายของบริษัท
- การประเมินความจำเป็นและสัดส่วนในการใช้ข้อมูลอย่างเหมาะสม ที่เกี่ยวข้องกับการประมวลผลตามวัตถุประสงค์
- การประเมินความเสี่ยงที่อาจเกิดผลกระทบกับความเป็นส่วนตัว สิทธิและเสรีภาพของเจ้าของข้อมูล
- แนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น รวมถึงมาตรการในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมเพื่อให้แน่ใจได้ว่ามีการคุ้มครองสิทธิเสรีภาพและประโยชน์อันชอบธรรมของเจ้าของข้อมูลหรือบุคคลอื่นที่มีความเสี่ยงที่จะได้รับผลกระทบ หากพิจารณาแล้วว่าระดับของความเสี่ยงนั้นสูงเกินกว่าที่สามารถจัดให้มีมาตรการในการลดความเสี่ยงนั้นได้ ควรพิจารณาไม่กระทำการประมวลผลข้อมูลส่วนบุคคลหรือปรึกษาคณะกรรมคุ้มครองข้อมูลส่วนบุคคลก่อนการจัดทำDPIA

9.2 การพิจารณาและขั้นตอนจัดทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

การพิจารณาเพื่อตัดสินใจว่ากรณีใดที่มีความจำเป็นที่จะต้องทำ DPIA ให้พิจารณาจากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่เข้าข่ายตามเกณฑ์ตั้งแต่ 2 ข้อที่จะกล่าวต่อไป ดังนี้

- Evaluation or Scoringเป็นกระบวนการทำโปรไฟลิ่งหรือการประเมินผลหรือให้คะแนนโดยระบบอัตโนมัติ และการใช้ข้อมูลส่วนบุคคลเพื่อการคาดการณ์ (prediction) โดยเฉพาะเมื่อการประมวลผลนั้นมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเชิงลึก เช่น พฤติกรรมความชอบสุขภาพหรือ ตำแหน่งที่ตั้ง เป็นต้น

- Automated-Decision Making with Legal or Similar Significant Effect หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีการใช้เทคโนโลยีเพื่อทำการตัดสินใจอัตโนมัติในเรื่องที่ส่งผลกระทบกับกฎหมายหรือในเรื่องที่ส่งผลกระทบกับบุคคลอย่างมีนัยสำคัญ เช่น อาจทำให้ถูกเลือกปฏิบัติ

- Systematic Monitoring ระบบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการติดตามการสังเกตสอดส่อง หรือควบคุมบุคคลโดยเฉพาะในพื้นสาธารณะที่บุคคลสามารถเข้าถึงได้ (PublicAccessibleArea)เช่นระบบเฝ้าระวังหรือตรวจตราในพื้นที่สาธารณะโดยที่บุคคลไม่อาจทราบถึงหรือไม่รู้ล่วงหน้าว่ามีกิจกรรมการประมวลผลนี้ หรือไม่ทราบว่ามีผู้ควบคุมข้อมูลส่วนบุคคลเป็นใครและกำลังทำอะไรอยู่ ส่งผลให้เป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะสามารถหลีกเลี่ยง หรือ ปฏิเสธการมีส่วนร่วมได้

- Sensitive Data เมื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น เชื้อชาติเผ่าพันธุ์ประวัติอาชญากรรมความเห็นทางการเมือง เป็นต้น

- Data Processed on a Large Scale หากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก โดยพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องปริมาณข้อมูลหรือเนื้อหาของข้อมูลส่วนบุคคลระยะเวลาของกิจกรรมประมวลผลและ ขอบเขตทางภูมิศาสตร์ของกิจกรรมการประมวลผล

- Datasets That Have Been Matched or Combined ชุดข้อมูลที่เกิดจากการรวบรวมหรือเปรียบเทียบข้อมูลส่วนบุคคลที่มาจากแหล่งข้อมูลหลายแหล่ง ที่มีวัตถุประสงค์ในการประมวลผลข้อมูลต่างกัน ข้อมูลที่ถูกนำมารวมหรือเปรียบเทียบไม่จำกัดว่าเป็นข้อมูลที่ถูกประมวลผลแล้วและไม่จำกัดว่าแหล่งข้อมูลที่มาจากผู้ควบคุมส่วนบุคคลเองหรืออาจมาจากผู้ควบคุมข้อมูลส่วนบุคคลอื่นก็ได้ ซึ่งการทำเช่นนี้อาจทำให้การประมวลผลข้อมูลส่วนบุคคลนั้นผิดไปจากวัตถุประสงค์ที่ได้มีการแจ้งเจ้าของข้อมูลที่ให้ไว้ในตอนแรก อีกทั้งอาจไม่เป็นไปตามความคาดหมายอย่างสมเหตุสมผลของเจ้าของข้อมูลได้

- Data Concerning Vulnerable Data Subjectsหากองค์กรมีการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวกับผู้เปราะบาง (Vulnerable Person) เช่น ผู้เยาว์ผู้อพยพ ผู้ป่วยทางจิต หรือผู้สูงวัยให้จัดได้ว่ากิจกรรมการประมวลผลนั้นมีความเสี่ยงที่จะทำให้เกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล เนื่องจากผู้เปราะบางอาจไม่อยู่ในสภาพที่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคลได้ รวมถึงการทำโปรไฟลิ่งข้อมูลของผู้เยาว์หรือการให้บริการออนไลน์แก่ผู้เยาว์โดยเฉพาะเพื่อวัตถุประสงค์การทำการตลาดแบบตรงอีกด้วย

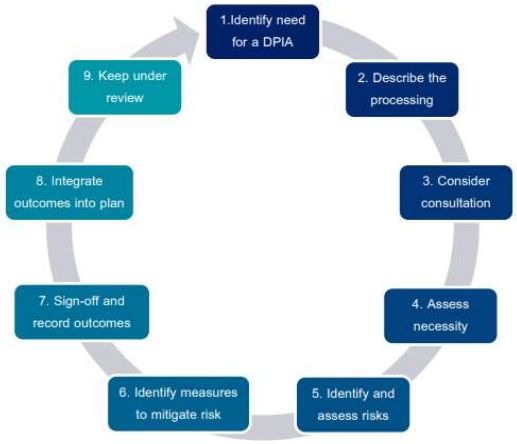
- InnovativeUseor Applying Technologicalor Organizational Solutions เมื่อมีการประมวลผลข้อมูลส่วนบุคคลซึ่งเกิดจากเทคโนโลยีใหม่ที่มีการใช้อย่างกว้างขวางในชีวิตประจำวันของเจ้าของข้อมูล เช่น การสแกนลายนิ้วมือ และใบหน้า ซึ่งอาจจะนำไปสู่ความเสี่ยงที่นอกเหนือความคาดหมายได้ เนื่องด้วยเทคโนโลยีดังกล่าวยังไม่เคยปรากฏหรือใช้มาก่อนจึงอาจไม่มีข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นได้ต่อเจ้าของข้อมูล

- Data Transfer Across Bordersหากมีการโอนข้อมูลไปยังต่างประเทศ นอกจากจะต้องพิจารณากฎหมายและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางแล้ว ยังต้องพิจารณาถึงความเป็นไปได้ที่ข้อมูลนั้นอาจถูกส่งต่อด้วย

- Prevents Data Subjects from Exercising a Right or Using a Service or a Contractหากกิจกรรมการประมวลผลนั้นอาจส่งผลให้เกิดการเปลี่ยนแปลงหรืออาจถูกปฏิเสธสิทธิของเจ้าของข้อมูล หรืออาจถูกปฏิเสธการได้รับบริการหรือการเข้าทำสัญญาของเจ้าของข้อมูล เช่น มีกระบวนการคัดกรองลูกค้าจากการประมวลผลข้อมูลของลูกค้ากับฐานข้อมูลเพื่อตรวจสอบข้อมูลเครดิตและตัดสินใจว่าจะให้ลูกค้าเข้าทำสัญญาหรือไม่

อย่างไรก็ตามถึงแม้มีกิจกรรมประมวลผลข้อมูลที่เข้าข่ายตามเกณฑ์ที่ได้ระบุไว้ดังที่กล่าวข้างต้นมากกว่าสองข้อ แต่สามารถเลือกที่จะไม่ทำ DPIA ก็ย่อมได้ หากพิจารณาแล้วว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะไม่ส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลทั้งนี้ควรที่จะทำการปรึกษากับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก่อนเพื่อพิจารณาถึงความเหมาะสม รวมถึงทำการจดบันทึกถึงเหตุผลที่ใช้ในการตัดสินใจในการไม่ทำ DPIAหรือกรณีที่แม้เข้าข่ายเพียงแค่หนึ่งข้อแต่อาจส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงกับเจ้าของข้อมูลก็จำเป็นจะต้องจัดทำDPIA

การจัดทำDPIA **เป็นกระบวนการที่ควรเริ่มจัดทำ**ก่อนการทำการประมวลผลข้อมูลและดำเนินการควบคู่ไปกับกระบวนการวางแผนและพัฒนา และทำอย่างต่อเนื่อง หากขั้นตอนในการจัดทำDPIA มีความละเอียดและ**ชัดเจน ก็จะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการประมวลผลข้อมูลอย่างเหมาะสม** โดยอาจพิจารณาขั้นตอนในการจัดทำDPIA **ดังนี้**



ขั้นตอนในการจัดทำ DPIA (Steps carry out a DPIA)

อย่างไรก็ตามการพิจารณาจัดทำDPIA นั้นกำหนดให้จำเป็นต้องทำเมื่อมีกิจกรรมการประมวลผล**ข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ซึ่งสามารถ**พิจารณาจาก**กิจกรรมการประมวลผลที่เข้าข่าย**ที่เป็นกิจกรรมที่มีความเสี่ยงสูง ได้จาก

- Systematic and Extensive Profiling with Significant Effectsการประมวลผลข้อมูลด้วยระบบอัตโนมัติ หรือ การทำ Profiling ที่อาจมีผลกระทบอย่างมีนัยสำคัญ
- Process Special Category or Criminal Offence Data on a Large Scale**การประมวลผลข้อมูลที่มีความ**อ่อนไหว เช่น ข้อมูลประวัติอาชญากรรม ข้อมูลพฤติกรรมทางเพศ เป็นจำนวนมาก
- Systematically Monitor Publicly Accessible Places on a Large Scale**ระบบการตรวจตราที่ใช้เฝ้าดูพื้นที่**สาธารณะเป็นจำนวนมาก เช่น ศูนย์การค้า ห้องสมุด เป็นต้น

10. แนวปฏิบัติเกี่ยวกับการบริหารจัดการและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

เพื่อให้การบริหารจัดการข้อมูลและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นผลสำเร็จจึงได้จัดให้มีการแบ่งหน้าที่ในเรื่องของการป้องกันและการรักษาความปลอดภัยของข้อมูลส่วนบุคคลอย่างชัดเจน เพื่อให้แน่ใจได้ว่าผู้มีส่วนได้ส่วนเสียทุกคนได้รับ**ทราบและตระหนักถึงหน้าที่และความรับผิดชอบ**ของตนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างเหมาะสม และยังกำหนดให้**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล จะต้องปฏิบัติหน้าที่**อย่างเป็นกลาง มีความเป็นอิสระจากการประมวลผลข้อมูลส่วนบุคคล ไม่ทำหน้าที่ในการกำ**หนดวัตถุประสงค์รวมทั้งวิธี**ในการประมวลผลข้อมูล ดังนี้

- หน่วยงานปฏิบัติงาน (Operational Function) ทำหน้าที่ในการกำหนดวัตถุประสงค์และวิธีการในการดำเนินการในการประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นหน้าที่ตามสายงานทางธุรกิจ เช่นหน่วยงานปฏิบัติงานเพื่อทำหน้าที่ในการเก็บรวบรวมข้อมูลจากเจ้าของข้อมูล การบันทึกข้อมูลลงในระบบฐานข้อมูล เป็นผู้กำหนดวัตถุประสงค์และวิธีการในการดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล อีกทั้งรับผิดชอบในการตรวจสอบคุณภาพของข้อมูลที่เก็บรวบรวมเพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องครบถ้วน ตามข้อกำหนดของกฎหมาย และเป็นไปตามข้อกำหนดของหน่วยงานกำกับดูแลข้อมูลของบริษัท

- หน่วยงานบริหารความเสี่ยงความเสี่ยง (Risk Management Function) ทำหน้าที่ในการควบคุมกำกับดูแลบริษัทในภาพรวม เช่น ทำหน้าที่กำกับดูแลการปฏิบัติงาน วางแนวทาง กรอบแนวคิด เงื่อนไขและขั้นตอนปฏิบัติงานให้กับหน่วยงานที่ปฏิบัติงานคอยสอดส่อง ตรวจตราหาช่องว่างในการปฏิบัติงานในส่วนที่ไม่ชัดเจน (Gray Areas) ของบริษัทเพื่อหาทางป้องกันและแก้ไข รวมทั้งเพื่อกำหนดแนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น โดยหน่วยงานในขั้นตอนนี้อาจรวมถึงหน่วยงานที่มีหน้าที่กำกับดูแลเฉพาะด้าน เช่นหน่วยงานบัญชีและการเงิน หน่วยงานด้านเทคโนโลยีสารสนเทศ หน่วยงานบริหารบุคคล หน่วยงานวางแผนงบประมาณ หน่วยงานบริหารอาคารสถานที่ ทั้งนี้หน่วยงานบริหารความเสี่ยงให้รวมถึงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมอยู่ด้วย โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบริษัทอาจแต่งตั้งเป็นบุคคลหรือหน่วยงานก็ได้ เช่น สำนักงานข้อมูลส่วนกลาง (Central Data Office) หน่วยงานกำกับดูแลข้อมูล (Data Governance Function) สำนักงานจัดการข้อมูล (Data Management Office) หรือ ผู้ดูแลข้อมูลระดับสูง (Chief Data Officer) เป็นต้น โดยมีหน้าที่ในการควบคุม กำกับ การประมวลผลข้อมูล เช่น กำหนดนโยบายที่เกี่ยวข้องกับการบริหารจัดการข้อมูล บริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และกำหนดตัวชี้วัดคุณภาพของข้อมูล รวมทั้งทำการติดตามผลเพื่อเป็นการสร้างกลไกในการยกระดับมาตรฐานในการเก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล และเพื่อให้เป็นไปตามข้อกำหนดของกฎหมายและเป็นไปตามนโยบายของบริษัท นอกจากนี้ ยังทำหน้าที่เป็นผู้ที่ให้คำปรึกษาในเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเมื่อมีความจำเป็น รวมถึงทำหน้าที่ในการติดต่อประสานงานกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กรอื่นๆ ภายนอก

- จัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่ในการตรวจสอบภายใน เพื่อให้มั่นใจได้ว่ามีการปฏิบัติงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการบริหารความเสี่ยง เป็นไปตามข้อกำหนดของกฎหมายและนโยบายที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของบริษัทและเพื่อให้มั่นใจได้ว่าบริษัทมีนโยบายที่เพียงพอและเหมาะสมสำหรับโครงสร้างของสายการรายงาน โดยกำหนดให้สามารถรายงานตรงต่อคณะกรรมการตรวจสอบได้ ทั้งนี้ในกรณีที่เกิดเหตุการณ์ที่อาจกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล บริษัทอาจกำหนดให้เป็นหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือหน่วยงานอื่นใดในการรายงานต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามแต่จะเห็นสมควร

เหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล (Personal Data Breach)

การรั่วไหลของข้อมูลส่วนบุคคล หมายถึง การที่ข้อมูลส่วนบุคคลถูกทำลาย สูญหายแก้ไขเปลี่ยนแปลงการเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บ รักษาหรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุในกรณีที่มีการรั่วไหลของข้อมูลส่วนบุคคลเกิดขึ้นในบริษัทผู้ที่ทราบเหตุจะต้องแจ้งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยเร็วที่สุด เพื่อที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการตรวจสอบถึงสาเหตุที่มาและระบุจุดต้นเหตุของการรั่วไหล รวมทั้งออกมาตรการเยียวยาเหตุการณ์รั่วไหลของข้อมูล พร้อมทั้งแจ้งแก่เจ้าของข้อมูลและ/หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดโดยไม่ชักช้า

โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จดบันทึกการรั่วไหลของข้อมูลส่วนบุคคล และประเมินความเสี่ยงเมื่อเกิดการรั่วไหลของข้อมูลส่วนบุคคลขึ้น ในการประเมินความเสี่ยงจากการรั่วไหลของข้อมูลนั้นอาจพิจารณาถึงผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลเนื่องจากหากพิจารณาแล้วว่า ไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสามารถทำการจดบันทึกไว้และอาจไม่จำเป็นต้องมีการแจ้งแก่เจ้าของข้อมูลหรือแจ้งต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลถึงเหตุการณ์การรั่วไหลที่เกิดขึ้น แต่หากผลของการประเมินแสดงให้เห็นว่าการรั่วไหลของข้อมูลที่อาจจะทำให้เกิดความเสี่ยงสูง ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องมีการดำเนินการแจ้งแก่เจ้าของข้อมูลรวมทั้งแนวทางในการเยียวยาอีกทั้งแจ้งเหตุละเมิดของข้อมูลส่วนบุคคลแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายในระยะเวลา 72 ชั่วโมง นับจากทราบเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคล

ให้มีการจัดทำแบบฟอร์มบันทึกการรั่วไหลของข้อมูลส่วนบุคคลขึ้นเพื่อเป็นแนวทางในการจดบันทึกอย่างถูกต้องและครบถ้วน โดยให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือพนักงานผู้พบเหตุการณ์การรั่วไหลของข้อมูลเป็นผู้ทำการบันทึกแทนเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก็ได้แล้วแต่กรณีพร้อมทั้งแจ้งแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการณ์การรั่วไหลของข้อมูลที่เกิดขึ้นด้วย เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการหาสาเหตุและมาตรการเยียวยา รวมถึงติดตามผลการดำเนินงานการแก้ไขปัญหาการรั่วไหลของข้อมูลส่วนบุคคล

การระบุความเสี่ยงต่อการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล

ระบุความเสี่ยงต่อการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคลไว้ 3 ระดับ กล่าวคือ

ระดับของความเสี่ยงต่อการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล	ลักษณะ	รายละเอียด
ระดับต่ำ	ความเสี่ยงต่ำ โอกาสที่ข้อมูลส่วนบุคคลจะถูกละเมิดหรือรั่วไหลต่ำ	มีการใช้ข้อมูลส่วนบุคคลเพื่อบรรลุวัตถุประสงค์ในการให้บริการ โดยเจ้าของข้อมูลสามารถคาดหวังได้ว่าข้อมูลส่วนบุคคลของตนจะถูกใช้งานในแบบนั้น
ระดับปานกลาง	ความเสี่ยงปานกลาง โอกาสที่ข้อมูลส่วนบุคคลจะถูกละเมิดหรือรั่วไหลปานกลาง	มีการใช้ข้อมูลส่วนบุคคลเพื่อวิเคราะห์พฤติกรรมการใช้บริการเพื่อทำการตลาดกับเจ้าของข้อมูล หรือมีการใช้ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ของเจ้าของข้อมูล แต่ยังไม่ถึงขั้นที่จะก่อให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอย่างมีนัยสำคัญ
ระดับสูง	ความเสี่ยงสูง โอกาสที่ข้อมูลส่วนบุคคลจะถูกละเมิดหรือรั่วไหลสูง	มีการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก โดยระบบอัตโนมัติ หรือมีการใช้ข้อมูลส่วนบุคคลเพื่อจัดประเภทของบุคคลตามพฤติกรรม (Profiling) หรือมีการประมวลผลข้อมูลส่วนบุคคลที่อ่อนไหวจำนวนมาก ที่ก่อให้เกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลอย่างมีนัยสำคัญ

รายละเอียดการติดต่อในเรื่องที่เกี่ยวกับข้อมูลส่วนบุคคล

บริษัท จะจัดให้มีผู้ดำเนินการรับผิดชอบในการกำกับดูแลและบริหารจัดการ รวมถึงช่องทางการติดต่อสำหรับให้เจ้าของข้อมูล และ/หรือผู้มีส่วนได้ส่วนเสียสามารถติดต่อในเรื่องที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ดังนี้

ผู้ควบคุมข้อมูล :

บริษัท เอส 11 กรุ๊ป จำกัด (มหาชน)

S11GROUPPUBPLICCOMPANYLIMITED

ผู้กำกับดูแลในเรื่องที่เกี่ยวกับข้อมูลส่วนบุคคลของบริษัท :

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)

สถานที่ติดต่อ:

เลขที่ 888 ซอยจตุโชติ10 ถนนจตุโชติ แขวงออเงิน เขตสายไหม กรุงเทพฯ 10220

888Soi.Chatuchot10,ChatuchutRoad,Ao-NgoenSub-district,SaimaiDistrict,Bangkok10220

ช่องทางการติดต่อ:

โทรศัพท์ |Tel:0-2022-8888

โทรสาร |Fax:0-2158-7948

Email |dpo@sgroup.co.th

Website |www.sgroup.co.th

การเผยแพร่ ประชาสัมพันธ์และฝึกอบรม (Training and awareness)

บริษัท จะดำเนินการฝึกอบรม เผยแพร่และประชาสัมพันธ์ อาทิ คู่มือปฏิบัติในเรื่องการคุ้มครองข้อมูลส่วนบุคคลสำหรับแต่ละหน่วยงาน(PDPA Handbook) นโยบายความเป็นส่วนตัวและข้อมูลส่วนบุคคล (Privacy Policy) นโยบายเกี่ยวกับการใช้คุกกี้ (Cookie Policy) คำประกาศเกี่ยวกับความเป็นส่วนตัว (Privacy Notice)ในทุกช่องทางประชาสัมพันธ์ของบริษัท เพื่อได้รับทราบและเข้าใจในหลักเกณฑ์ปฏิบัติร่วมกันและเป็นการลดความเสี่ยงที่อาจก่อให้เกิดผลกระทบต่อข้อมูลส่วนบุคคลให้อยู่ในระดับที่ยอมรับได้รวมทั้งบรรลุเป้าหมายและวัตถุประสงค์หลักขององค์กรได้อย่างมีประสิทธิภาพ

การทบทวนนโยบาย

บริษัทจะมีการทบทวนนโยบายฉบับนี้เป็นประจำทุกหรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเพื่อให้สอดคล้องกับกฎหมาย ข้อบังคับ และแนวปฏิบัติที่เกี่ยวข้องกับบริษัท

บทกำหนดโทษ

ผู้ที่มีหน้าที่รับผิดชอบในการดำเนินงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ในการปฏิบัติงาน หรือสั่งการ หรือทำการอย่างใดอย่างหนึ่งในหน้าที่ที่รับผิดชอบ หากละเลยหรือละเว้น อันเป็นการฝ่าฝืนนโยบายและแนวปฏิบัติฉบับนี้หรือตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนด จนก่อให้เกิดความเสี่ยงอันเป็นเหตุให้เกิดความผิดตามกฎหมายหรือสร้างความเสียหายขึ้น ผู้นั้นต้องได้รับโทษตามระเบียบของบริษัท และยังต้องรับโทษทางกฎหมายตามความผิดที่เกิดขึ้น ทั้งนี้หากความผิดดังกล่าวก่อให้เกิดความเสียหายแก่บริษัท หรือบุคคลอื่นใด บริษัทอาจพิจารณาดำเนินคดีตามกฎหมายเพิ่มเติมต่อไป

ทั้งนี้ให้ผู้คุ้มครองข้อมูลส่วนบุคคล ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศและคณะกรรมการบริหารความเสี่ยงร่วมกันกำกับดูแลและบริหารจัดการในการพิจารณาข้อโต้แย้งต่างๆ ที่เกี่ยวกับข้อมูลส่วนบุคคลของบริษัท

จากนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว บริษัทจะประกาศใช้ในองค์กรเพื่อให้บุคลากรและผู้มีส่วนได้ส่วนเสียได้รับทราบ และปฏิบัติใช้ให้เป็นไปในแนวทางเดียวกัน อันจะส่งผลให้บริษัท สามารถบรรลุเป้าหมายและวัตถุประสงค์หลักขององค์กรได้อย่างมีประสิทธิภาพ