บริษัท ฟู้ดแพชชั่น จำกัด

นโยบายคุ้มครองข้อมูลส่วนบุคคล

(Data Protection Policy)

สารบัญ

หน้า

1. คำนิยาม

ในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ คำหรือข้อความสามารถนิยามได้ดังนี้

กฎหมายคุ้มครองข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และที่จะมีการแก้ไขเพิ่มเติม รวมถึงกฎ ระเบียบ และคำสั่งที่เกี่ยวข้อง
การเข้าถึงข้อมูล (Access)	สิทธิในการอ่าน/ดู บันทึก คัดลอก เก็บสำรอง จัดเก็บ สืบค้น ดาวน์โหลด หรือแก้ไข (อัพเดท แทรก/เพิ่ม ลบ) ข้อมูล รวมถึงการจัดการสิทธิการเข้าถึงนั้น ๆ
การบันทึก (Record)	ข้อมูลหรือสารสนเทศในรูปแบบเฉพาะ ซึ่งถูกสร้างขึ้นหรือได้มาจากกิจกรรมบุคคลหรือกิจกรรมองค์กร และได้สำรอง (เก็บรักษา) ไว้เป็นหลักฐานของกิจกรรมนั้น ๆ เพื่อใช้อ้างอิงในอนาคต
การประมวลผลข้อมูลส่วนบุคคล (Processing)	การดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อม ใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
ข้อมูล/สารสนเทศ	ข้อมูลในรูปแบบใดก็ตามทั้งในแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ เช่น ข้อมูลในสิ่งพิมพ์ซึ่งอยู่ในระบบภายในหรือระบบภายนอกที่นอกเหนือการควบคุมขององค์กรและปรากฏเงื่อนไขดังต่อไปนี้ ▪ ข้อมูลที่พนักงานขององค์กรหรือบุคคลที่ได้รับมอบหมายได้มา ประมวลผล จัดการ และ/หรือ ดูแล (เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษา) เพื่อปฏิบัติหน้าที่ ▪ ข้อมูลที่เกี่ยวเนื่องกับการจัดการ การปฏิบัติงาน วางแผน รายงาน หรือการตรวจสอบการดำเนินงานขององค์กร ข้อมูลที่ใช้อ้างอิงหรือจำเป็นต่อการทำงานของหน่วยงานอย่างน้อยหนึ่งหน่วย
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (มาตรา 6 พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562) เช่น ชื่อ นามสกุล อีเมล์ รูป ลายนิ้วมือ รหัสประชาชน ซึ่งสามารถระบุตัวบุคคลได้ในทางตรง หรือการเก็บ Location หรือ Cookie เป็นการเก็บข้อมูลซึ่งทำให้สามารถระบุตัวบุคคลได้ในทางอ้อม นอกจากนี้ ข้อมูลที่โดยพื้นฐานแล้วไม่สามารถนำไประบุตัวบุคคลได้แต่เมื่อนำไปใช้ร่วมกับข้อมูลอื่นแล้วก่อให้เกิดชุดข้อมูลที่สามารถระบุข้อมูลส่วนบุคคลได้ ก็ถือเป็นข้อมูลส่วนบุคคลเช่นกัน เช่น ที่อยู่ เพศ และอายุ ที่เมื่อนำมารวมกันแล้วสามารถระบุตัวบุคคลได้

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม
บริษัท	บริษัท ฟู้ดแพชชั่น จำกัด
บุคคลภายนอก (Third Parties)	บุคคลธรรมดา หรือนิติบุคคล สำนักงานราชการ หน่วยงานราชการ หรือบุคคลอื่นที่มิใช่เจ้าของข้อมูลส่วนบุคคล มิใช่บริษัท มิใช่ผู้ประมวลผลข้อมูลส่วนบุคคล และมิใช่บุคคลผู้ได้รับอำนาจจากบริษัท หรือ ได้รับอำนาจจากผู้ประมวลผลข้อมูลส่วนบุคคลให้ทำการประมวลผลข้อมูลส่วนบุคคลโดยตรง
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	ผู้ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
ผู้ให้บริการภายนอก (Outsource)	ผู้ประมวลผลข้อมูลส่วนบุคคล ที่เป็นบุคคลธรรมดาหรือนิติบุคคล ซึ่งไม่ใช่พนักงานหรือหน่วยงานของบริษัททำหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัทฯ
หน่วยงานเจ้าของสารสนเทศ	สายงาน ฝ่ายงาน หรือหน่วยงานปฏิบัติงานภายใต้ความรับผิดชอบของบริษัท มีหน้าที่และความรับผิดชอบในการจัดระดับชั้นความลับของข้อมูล ควบคุมการเข้าถึงข้อมูล ดูแลรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูล

2. วัตถุประสงค์

บริษัท ฟู้ดแพชชั่น จำกัด (“**บริษัท**”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการรับผิดชอบต่อสังคมและเป็นรากฐานในการสร้างความสัมพันธ์ที่น่าเชื่อถือกับคู่ค้าและความเชื่อมั่นแก่ลูกค้า บริษัทจึงยึดมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ ข้อบังคับอื่น ๆ ที่เกี่ยวข้อง

เอกสารฉบับนี้ได้รับการจัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

- เพื่อชี้แจงความรับผิดชอบของบริษัทที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- เพื่อกำหนดมาตรฐานและแนวทางบริหารข้อมูลส่วนบุคคล โดยครอบคลุมถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

3. ขอบเขต

นโยบายฉบับนี้ใช้บังคับการจัดเก็บข้อมูลส่วนบุคคลซึ่งมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล โดยครอบคลุมถึงบุคลากรทั้งหมด ได้แก่ พนักงานประจำ พนักงานชั่วคราว พนักงานสัญญาจ้าง รวมถึงสายงาน หน่วยงาน ภายใต้การควบคุมของบริษัท รวมถึงพันธมิตรของบริษัทซึ่งมีส่วนร่วมในการเข้าถึงหรือประมวลผลข้อมูลของสำนักงานนอกจากนี้ยังครอบคลุมถึงการส่งต่อข้อมูลสู่องค์กรภายนอก หน่วยงานราชการ หรือบุคคลที่ได้รับอนุญาตตามกฎหมาย ข้อบังคับ หรือข้อบังคับกฎหมายอื่น ๆ และใช้บังคับกับข้อมูลทุกรูปแบบ ทั้งข้อมูลอิเล็กทรอนิกส์ และไม่ใช่อิเล็กทรอนิกส์

4. คำแถลงนโยบาย

4.1 นโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy)

- นโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) ต้องจัดให้มีการประกาศและสื่อสารไปยังพนักงานและหน่วยงานที่เกี่ยวข้อง และกำหนดให้มีการทบทวนและปรับปรุงนโยบายฉบับนี้ให้เป็นปัจจุบันอย่างสม่ำเสมอ
- การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามกฎหมาย มีความเป็นธรรมและมีความโปร่งใส
- การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องมีความเหมาะสมตามวัตถุประสงค์ที่กำหนด เป็นไปตามฐานในการประมวลผลข้อมูลส่วนบุคคลที่กำหนด
- การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการประมวลผลข้อมูลส่วนบุคคลอย่างจำกัด และสอดคล้องตามวัตถุประสงค์ที่กำหนด
- การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการปรับปรุงอยู่เสมอ รวมทั้งจะต้องมีการกำหนดขั้นตอนในการตรวจสอบ เพื่อให้ข้อมูลส่วนบุคคลมีความถูกต้องเป็นไปตามกฎหมายหรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกำหนด

- บริษัทอนุญาตให้จัดเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่บริษัทกำหนดเท่านั้น ข้อมูลส่วนบุคคลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด ผู้รับผิดชอบจะต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
- การประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ การลบหรือทำลายข้อมูลทั้งโดยความตั้งใจและไม่ตั้งใจ และรวมถึงการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่องค์กรยอมรับได้

4.2 นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)

บริษัทมีการกำหนดแนวทางในการจัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลของบริษัทเพื่อให้มั่นใจว่าเอกสาร รวมถึงเอกสารในรูปแบบอิเล็กทรอนิกส์ ที่มีข้อมูลส่วนบุคคลจะไม่ถูกเก็บไว้นานเกินความจำเป็น และมีมาตรการในการจัดเก็บที่สอดคล้องกับข้อกำหนดทางธุรกิจและกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

1. สถานที่จัดเก็บข้อมูล

1.1 เอกสารในรูปแบบอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ (อีเมล) และ บันทึกมัลติมีเดีย (Multimedia)
เอกสารในรูปแบบอิเล็กทรอนิกส์ อีเมล และบันทึกมัลติมีเดียทั้งหมดจะต้องจัดเก็บภายในสถานที่ที่เหมาะสมเพื่อให้แน่ใจว่ามีการใช้มาตรการรักษาความปลอดภัยที่เป็นไปตามมาตรฐานที่กำหนดโดยกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมถึง กฎหมายอื่น แนวปฏิบัติ และคำสั่งที่เกี่ยวข้อง

1.2 เอกสารในรูปแบบกระดาษ
การจัดเก็บเอกสารในรูปแบบกระดาษที่จำเป็นสำหรับการดำเนินธุรกิจในแต่ละวัน ต้องเก็บไว้ในตู้เก็บเอกสารและลิ้นชักโต๊ะทำงานเมื่อไม่ได้ใช้งาน และพนักงานจะต้องล็อคกุญแจตู้เก็บเอกสารและลิ้นชักที่จัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลเมื่อสิ้นวันทำการ

2. การปกป้องเอกสาร

เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยเอกสารที่มีข้อมูลส่วนบุคคลซึ่งอยู่ในการควบคุมของบริษัทโดยมิชอบหรือโดยปราศจากอำนาจ เอกสารทั้งในรูปแบบกระดาษและรูปแบบอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลจะถูกเก็บไว้ในที่ปลอดภัยจนกว่าจะถูกทำลาย บริษัทจะใช้เทคโนโลยีและกระบวนการต่าง ๆ ที่ได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล

3. การทำลายเอกสาร

เมื่อพ้นกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลหรือหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลแล้ว เอกสารในรูปแบบประเภทกระดาษที่มีข้อมูลส่วนบุคคลจะถูกทำลายโดยการย่อยเอกสาร โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว ส่วนข้อมูลส่วนบุคคลที่จัดเก็บทางอิเล็กทรอนิกส์จะถูกลบออกจากสื่อที่ใช้เก็บข้อมูล เช่น ฮาร์ดดิสก์จะถูกทำลาย หรือ ถูกลบข้อมูลโดยวิธีที่ไม่สามารถกู้คืนข้อมูลได้ โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว

4. การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทจะกำหนดระยะเวลาการจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ในการเก็บรวบรวมสำหรับการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน โดยอาจเป็นไปตามระยะเวลาที่กำหนดตามกฎหมาย แนวปฏิบัติของธุรกิจ หรือมาตรฐานของการประมวลผล โดยบริษัทจะดำเนินการกำหนดระยะเวลาไว้ในเอกสารบันทึกการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) ของบริษัท

บริษัทจะจัดให้มีกระบวนการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษาที่ได้กำหนดไว้ หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเป็นไปตาม**นโยบายในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)**

4.3 นโยบายการแยกประเภทของข้อมูลส่วนบุคคล (Personal Data Classification Policy)

1. แนวทางการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล

1.1 บริษัทมีการกำหนดชั้นความลับของสารสนเทศไว้ 4 ระดับ ได้แก่ ข้อมูลทั่วไป (Public Data) ข้อมูลใช้ภายใน (Internal Use Data) ข้อมูลความลับ (Confidential Data) และข้อมูลความลับที่สุด (Secret Data) โดยมีการกำหนดนิยาม รวมทั้งแนวทางในการควบคุมและป้องสารสนเทศตามระดับชั้นความลับของข้อมูล ผู้ที่เกี่ยวข้องจะต้องปฏิบัติตามโดยเคร่งครัด หากกลุ่มของสารสนเทศประกอบไปด้วยสารสนเทศหลายระดับชั้นความลับ ให้หน่วยงานเจ้าของสารสนเทศกำหนดระดับชั้นความลับของสารสนเทศนั้นตามระดับชั้นความลับของสารสนเทศระดับสูงสุดของกลุ่มสารสนเทศ

1.2 หน่วยงานเจ้าของสารสนเทศมีหน้าที่กำหนดและทบทวนระดับชั้นความลับของข้อมูลส่วนบุคคล ที่อยู่ภายใต้ความรับผิดชอบในของตนอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับระดับความสำคัญของสารสนเทศที่อาจมีการเปลี่ยนแปลงตามระยะเวลา รวมทั้งจัดให้มีการควบคุมที่เหมาะสมกับระดับชั้นความลับของข้อมูล โดยหน่วยงานเจ้าของสารสนเทศอาจมอบหมายกิจกรรมการควบคุมข้างต้นให้กับผู้ดูแลสารสนเทศ และอาจขอการสนับสนุนและความช่วยเหลือทางด้านเทคนิคจากหน่วยงานเทคโนโลยีสารสนเทศ อย่างไรก็ดีหน่วยงานเจ้าของสารสนเทศยังเป็นผู้รับผิดชอบที่แท้จริงในการจัดระดับชั้นความลับและการควบคุมความมั่นคงปลอดภัยของสารสนเทศที่ตนเป็นผู้รับผิดชอบ

1.3 หน่วยงานเจ้าของสารสนเทศควรเก็บข้อมูลส่วนบุคคลเป็นความลับและเปิดเผยต่อบุคคลที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมายและกฎเกณฑ์ที่บังคับใช้เท่านั้น

1.4 หน่วยงานเจ้าของสารสนเทศและหน่วยงานอื่นที่เกี่ยวข้อง ต้องร่วมดำเนินการให้มีมาตรการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น และได้รับอนุญาตให้เข้าถึงข้อมูลในระยะเวลาที่เหมาะสมเท่านั้น

1.5 การขอสิทธิเพื่อเข้าถึงข้อมูลส่วนบุคคลนอกเหนือจากสิทธิที่กำหนดไว้จะต้องผ่านการพิจารณาจากหน่วยงานเจ้าของสารสนเทศ

1.6 การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศที่บริษัทกำหนด

1.7 การเก็บรักษาข้อมูลส่วนบุคคลต้องเก็บรักษาตามระยะเวลาเท่าที่จำเป็น เพื่อให้เป็นไปตามวัตถุประสงค์ในการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาที่ระบุไว้ใน **นโยบายการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)**

1.8 การลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม ให้เป็นไปตาม**นโยบายการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)**

1.9 หากมีการว่าจ้างผู้ให้บริการภายนอกที่ต้องมีการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องมีการปฏิบัติตาม**นโยบายในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)** และต้องมีการจัดระดับชั้นความลับของข้อมูลส่วนบุคคลโดยหน่วยงานเจ้าของสารสนเทศที่ได้ทำการว่าจ้างผู้ให้บริการภายนอกนั้น ๆ

1.10 การจัดระดับชั้นความลับของข้อมูลส่วนบุคคล ต้องมีการกำหนดความเสี่ยงเพื่อจัดระดับชั้นความลับของข้อมูลส่วนบุคคล ดังนี้

ระดับชั้นความลับข้อมูลสารสนเทศ	คำนิยามระดับชั้นความลับข้อมูลสารสนเทศ
ความลับที่สุด (Secret)	เป็นข้อมูลที่มีการประเมินแล้วว่า หากมีการเปิดเผยโดยไม่ได้รับอนุญาตจะสามารถสร้างความเสียหายทั้งในด้านการเงินและด้านอื่น ๆ ต่อบริษัทอย่างร้ายแรง ข้อมูลที่จัดอยู่ในกลุ่มนี้จะต้องได้รับการดูแลเป็นพิเศษ ทั้งจากหน่วยงานเจ้าของสารสนเทศ และผู้ที่จำเป็นต้องใช้ข้อมูลตามหน้าที่ของงานที่รับผิดชอบ ทุกคนที่สามารถเข้าถึงข้อมูลเหล่านี้จำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือในกรณีที่เป็นบริษัทในเครืออาจจัดทำเป็นข้อตกลงในการรักษาความลับระหว่างบริษัทซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย *ตัวอย่างข้อมูลความลับที่สุด เช่น แผนกลยุทธ์ทางธุรกิจ (ก่อนประกาศอย่างเป็นทางการ)*
ความลับ (Confidential)	ข้อมูลซึ่งหากเปิดเผยโดยไม่ได้รับอนุญาต จะเป็นการฝ่าฝืนกฎ ข้อบังคับของบริษัทก่อให้เกิดผลกระทบด้านชื่อเสียง การเงิน เสียเปรียบในการแข่งขันทางการค้าต่อบริษัท ผู้ที่สามารถเข้าถึงข้อมูลประเภทนี้ได้จึงถูกจำกัดเพียงพนักงานเป็นรายบุคคล กลุ่มพนักงานหรือบุคคลที่สาม ที่มีความสัมพันธ์กันตามสัญญา โดยกลุ่มคนที่ระบุจำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) ในนามรายบุคคลหรือบริษัทต้นสังกัด ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย *ตัวอย่างข้อมูลความลับ เช่น รหัสผ่าน คีย์การเข้ารหัส ข้อมูลทางการเงิน ข้อมูลงบประมาณ ข้อมูลลูกค้า ข้อมูลที่เกี่ยวข้องกับระบบความปลอดภัย ข้อมูลจำลองลายนิ้วมือ ข้อมูลเงินเดือน <u>ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว</u> เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ข้อมูลพันธุกรรม ข้อมูลสุขภาพ ข้อมูลชีวภาพ เป็นต้น*
ใช้ภายใน (Internal Use)	ข้อมูลที่เปิดเผยได้เฉพาะภายในบริษัทและบุคคลภายนอกที่มีความสัมพันธ์ทางการค้าซึ่งได้รับสิทธิเท่านั้น ไม่เหมาะที่จะเปิดเผยต่อสาธารณชนเป็นการทั่วไป *ตัวอย่างข้อมูลใช้ภายใน เช่น เอกสารภายใน E-mail ภายในสำนักงาน นโยบาย และมาตรฐานของสำนักงานสมุดรายชื่อโทรศัพท์ ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ อีเมล เบอร์โทรศัพท์*
ทั่วไป (Public)	ข้อมูลสารสนเทศที่ไม่ได้กระทบอย่างมีนัยสำคัญต่อการดำเนินงาน และผู้บริหารอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดีข้อมูลสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้กับลูกค้ารวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท *ตัวอย่างข้อมูลทั่วไป เช่น แผ่นพับประชาสัมพันธ์ด้านการตลาด ข่าวประชาสัมพันธ์ ข่าวประกาศผู้ถือหุ้น*

ตัวอย่างการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use)
ข้อมูลที่ใช้ในการพิสูจน์หรือยืนยันตัวตน	รหัสผ่าน	✓	
	คีย์การเข้ารหัสข้อมูล (Encryption keys)	✓	
	ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า (Face recognition) ข้อมูลจำลองม่านตา หรือข้อมูลจำลองลายนิ้วมือ	✓	
	บันทึกกิจกรรมการเข้าถึงระบบ (Authentication logs)	✓	
ข้อมูลบัตรอิเล็กทรอนิกส์ (เช่น บัตรเดบิต บัตรเครดิต เป็นต้น)	ชื่อผู้ถือบัตรอิเล็กทรอนิกส์	✓	
	เลขบัตรอิเล็กทรอนิกส์	✓	
	PIN, PIN block	✓	
	CVV, CVV2, CVC2, CID	✓	
	ข้อมูลบัตรบนแถบแม่เหล็ก	✓	
ข้อมูลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information (PII))	ชื่อ นามสกุล		✓
	เลขบัตรประชาชน		✓
	เลขหนังสือเดินทาง		✓
	เลขบัตรประกันสังคม		✓
	เลขใบอนุญาตขับขี่		✓
	เลขประจำตัวผู้เสียภาษี		✓
	รหัสพนักงาน		✓
	เลขบัญชีธนาคาร		✓
	เลขที่กรมธรรม์		✓
	วันเดือนปีเกิด		✓
	อายุ		✓
	เพศ		✓
	ที่อยู่		✓
	เบอร์โทรศัพท์		✓
	อีเมล		✓
	ข้อมูลเงินเดือน	✓	
	ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID		✓

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use)
	ข้อมูลชีวมิติ (Biometric) เช่น รูปภาพใบหน้า, ลายนิ้วมือ, ฟิล์มเอกซเรย์, ข้อมูลสแกนม่านตา, ข้อมูลอัตลักษณ์เสียง, ข้อมูลพันธุกรรม	✓	
	ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์, โฉนดที่ดิน		✓
	ข้อมูลการจ้างงาน		✓
	ประวัติการทำงาน		✓
	ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง		✓
	ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file		✓
ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว	ความเชื่อในลัทธิ ศาสนาหรือปรัชญา	✓	
	ความคิดเห็นทางการเมือง	✓	
	เชื้อชาติ เผ่าพันธุ์	✓	
	ข้อมูลพันธุกรรม	✓	
	ประวัติอาชญากรรม	✓	
	พฤติกรรมทางเพศ	✓	
	ข้อมูลประวัติทางการแพทย์ สุขภาพ หมู่เลือด ความพิการ หรือข้อมูลสุขภาพจิต	✓	
	ข้อมูลสหภาพแรงงาน	✓	

ในกรณีที่ไม่สามารถกำหนดระดับชั้นความลับของสารสนเทศบางประเภทตามคำนิยามหรือตัวอย่างที่ได้กล่าวไว้ข้างต้น ให้หน่วยงานเจ้าของสารสนเทศเป็นผู้ตัดสินใจในการกำหนดระดับชั้นความลับของสารสนเทศดังกล่าวโดยสามารถขอคำแนะนำจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท

2. แนวทางในการควบคุมและป้องกันสารสนเทศ

การควบคุมและป้องกันสารสนเทศครอบคลุมในด้านการจัดทำ การจัดเก็บ การจัดพิมพ์และการทำสำเนา การจัดส่ง การทำลายและการนำกลับมาใช้ใหม่ของสารสนเทศทั้งในรูปแบบของเอกสารและอิเล็กทรอนิกส์ โดยมีรายละเอียดการควบคุมที่จำเป็น ดังต่อไปนี้

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การจัดทำข้อมูล				
การทำเครื่องหมายหรือสัญลักษณ์แสดงชั้นความลับเอกสารฉบับพิมพ์ (Hard Copy) และอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ควรระบุคำว่า “ข้อมูลใช้ภายใน” หรือ “INTERNAL USE” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน ยกเว้นกรณีที่เป็นเทป backup จะไม่ทำเครื่องหมายสัญลักษณ์ เพื่อป้องกันข้อผิดพลาดทางเทคนิค	ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน กรณีทำได้ควรระบุทุกหน้า ยกเว้นกรณีที่เป็นเทป backup จะไม่ทำเครื่องหมายสัญลักษณ์ เพื่อป้องกันข้อผิดพลาดทางเทคนิค	ระบุคำว่า “ลับที่สุด” หรือ “SECRET” ในเอกสารหรือสื่อบันทึกข้อมูลให้ชัดเจน กรณีทำได้ควรระบุทุกหน้า และควรระบุชื่อหน่วยงานเจ้าของเรื่อง เลขที่ชุดของจำนวนชุดทั้งหมด และเลขที่หน้าของจำนวนหน้าทั้งหมดด้วย
		กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ข้อมูลใช้ภายใน [ชื่อบริษัท] ” หรือ “[ชื่อบริษัท] INTERNAL USE” หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น	กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ลับ [ชื่อบริษัท]” หรือ “[ชื่อบริษัท] CONFIDENTIAL” หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น	กรณีใช้สื่อสารกับบุคคลภายนอกให้ระบุคำว่า “ลับที่สุด [ชื่อบริษัท]” หรือ “[ชื่อบริษัท] SECRET” หรือข้อความอื่น ๆ ที่แสดงถึงการจำกัดขอบเขตการใช้งานเฉพาะผู้เกี่ยวข้องเท่านั้น

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การพิมพ์ออกทางเครื่องพิมพ์ (Printer) เอกสารฉบับพิมพ์	ไม่มีข้อบังคับพิเศษ	เมื่อพิมพ์เอกสารเสร็จจะต้องเก็บทันทีโดยไม่ปล่อยเอกสารทิ้งไว้ที่เครื่องพิมพ์	1) ตรวจสอบเครื่องพิมพ์ปลายทางให้แน่ใจว่าถูกต้องทุกครั้งก่อนสั่งพิมพ์ 2) เมื่อพิมพ์เอกสารเสร็จจะต้องเก็บทันทีโดยไม่ปล่อยเอกสารทิ้งไว้ที่เครื่องพิมพ์ 3) หากมีการพิมพ์ไปที่เครื่องพิมพ์ซึ่งเชื่อมต่อกับระบบเครือข่ายที่มีการใช้งานโดยผู้ใช้หลายคน ผู้สั่งพิมพ์ต้องเป็นผู้ไปรับเอกสารด้วยตนเอง โดยรอเอกสารตั้งแต่เริ่มพิมพ์จนกระทั่งเอกสารพิมพ์เสร็จ 4) ห้ามพิมพ์เอกสารภายนอกบริษัท เช่น โรงแรม ศูนย์ประชุม สนามบิน เป็นต้น	
การจัดเก็บข้อมูล				
เอกสารฉบับพิมพ์ (Hard Copy) หรือสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในที่เหมาะสมกับการปฏิบัติงานและมีการจัดเก็บอย่างเป็นระบบ	เก็บไว้ในที่มิดชิดและสามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น การเก็บในตู้ใส่กุญแจเมื่อไม่ได้ใช้งาน หรือการเก็บในตู้นิรภัย	
การจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่าย (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	ไม่จำเป็นต้องเข้ารหัส (Unencrypted) แต่ต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และมีการกำหนดสิทธิในการเข้าถึง	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และมีการกำหนดสิทธิในการเข้าถึง	
การจัด เก็บข้อมูลในระบบ Cloud (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	มีมาตรการในการควบคุม และมีการกำหนดสิทธิในการเข้าถึง	จัดเก็บในแฟ้มข้อมูลที่มีการเข้ารหัส (Encrypted) หรือต้องจัดเก็บภายในโฟลเดอร์ที่มีมาตรการในการควบคุม และกำหนดสิทธิในการเข้าถึง	
การจัดเก็บข้อมูลในโทรศัพท์เคลื่อนที่ (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	มีการตั้งค่าการพิสูจน์ตัวตนก่อนการเข้าถึง เช่น pin-code หรือรหัสผ่าน เพื่อป้องกันการเข้าถึงข้อมูล กรณีโทรศัพท์สูญหายหรือถูกขโมย		

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การจัดเก็บข้อมูลบนสื่อบันทึกข้อมูล (Media) เช่น USB, Memory Stick, SD Card, CD, DVD, External Hard Disk (ข้อมูลอิเล็กทรอนิกส์)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	มีการเข้ารหัส (Encrypted) แฟ้มข้อมูลหรือสื่อบันทึกข้อมูล เช่น • Zip file ด้วย AES-256 • BitLocker • Utility ที่เจ้าของผลิตภัณฑ์มีให้	
การจัดเก็บข้อมูล (เมื่อนำข้อมูลออกนอกสถานที่)				
เมื่อนำข้อมูลไปด้วยระหว่างการเดินทาง เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	ข้อมูลจะต้องอยู่ภายใต้การดูแลตลอดเวลา หรือเก็บในที่ที่สามารถป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต เช่น ใส่ซองปิดผนึกไว้ในห้องโรงแรมที่มีการใส่กุญแจ หรือเก็บในตู้นิรภัย		
เมื่อนำข้อมูลไปด้วยในรถ เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	เก็บไว้ในรถที่มีการล็อคและไว้ในจุดที่ไม่สามารถมองเห็นได้จากภายนอก		
การส่ง/รับ และการโอนข้อมูล				
การจัดส่งผ่านทางไปรษณีย์ เอกสารฉบับพิมพ์ (Hard copy) หรือสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	ใส่เอกสารในซองทึบปิดผนึก	ใส่เอกสารในซองทึบปิดผนึก และประทับตราที่ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL”	ไม่ควรส่งผ่านไปรษณีย์ หากจำเป็นจะต้องได้รับอนุญาตจากหน่วยงานเจ้าของสารสนเทศก่อน โดยวิธีการปฏิบัติ ให้ปฏิบัติเช่นเดียวกับข้อมูลความลับ
การส่งด้วยมือ เอกสารฉบับพิมพ์ (Hard Copy) หรือสื่อบันทึกข้อมูล (Media)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	1) ใส่เอกสารในซองทึบ ปิดผนึก และประทับตราที่ระบุคำว่า “ลับ” หรือ “CONFIDENTIAL”	1) ต้องทำการปิดผนึกซองเอกสารก่อนจัดส่งให้ไม่สามารถสังเกตได้จากภายนอก ใส่

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
			2) จัดทำบันทึกการส่งและการรับไว้เป็นหลักฐาน	เอกสารในซอง 2 ชั้น 2) ซองชั้นในให้ระบุระบุคำว่า “ลับที่สุด” หรือ “SECRET” และซองชั้นนอกห้ามระบุระดับชั้นความลับเอกสาร 3) จัดทำบันทึกการส่งและรับไว้เป็นหลักฐาน 4) จัดส่งให้บุคคลที่ได้รับมอบหมายเท่านั้น
การส่งผ่านเครื่องโทรสาร	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	1) ต้องระบุชื่อรายละเอียดของผู้รับและผู้ส่งให้ชัดเจนครบถ้วน 2) ตรวจสอบหมายเลขปลายทางให้แน่ใจว่าถูกต้องทุกครั้ง 3) ต้องส่งโทรสารไปยังสถานที่ปลายทางที่มีความมั่นคงปลอดภัยเพียงพอ 4) ผู้ส่งต้องอยู่รอจนการส่งเสร็จสิ้น	ห้ามส่งผ่านเครื่องโทรสาร

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
			แล้วจึงเก็บเอกสารกลับไปโดยไม่ลืมไว้ที่เครื่องโทรสาร 5) ผู้รับเอกสารที่ปลายทางต้องเป็นผู้ได้รับอนุญาตเท่านั้น	
การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ (Email, FTP)	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	ต้องแลกเปลี่ยนข้อมูลให้มีความมั่นคงปลอดภัย เช่น ต้องมีการเข้ารหัส หรือ ใส่รหัสผ่านโดยต้องไม่ส่งรหัสผ่านไปพร้อมกับข้อมูล หรือส่งรหัสผ่านคนละช่องทางกับการส่งข้อมูลครั้งนั้น เป็นต้น	ไม่ควรมีการแลกเปลี่ยนข้อมูลทาง Electronic หากจำเป็นต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน โดยวิธีการปฏิบัติ ให้ปฏิบัติเช่นเดียวกับข้อมูลความลับ
การจัดการกรณีข้อมูลสูญหาย				
ข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	กรณีข้อมูลสูญหายหรือถูกขโมยให้รายงานต่อผู้จัดการหน่วยงานเจ้าของสารสนเทศทันทีที่ทราบเหตุ เพื่อดำเนินการลดความเสียหายให้มากที่สุดเท่าที่จะเป็นไปได้ เช่น การเปลี่ยนรหัสผ่าน หรือล็อคการเข้าสู่บัญชีผู้ใช้กรณีเครื่องคอมพิวเตอร์ถูกขโมย หรือการลบข้อมูล (wipe data) ในโทรศัพท์เคลื่อนที่ กรณีโทรศัพท์เคลื่อนที่สูญหาย		
เอกสารฉบับพิมพ์ (Hard copy)	ไม่มีข้อบังคับพิเศษ	กรณีข้อมูลสูญหายหรือถูกขโมยให้รายงานผู้จัดการหน่วยงานเจ้าของสารสนเทศทันทีที่ทราบเหตุ		
อื่น ๆ				
เอกสารฉบับพิมพ์ (hard copy) หรือข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ไม่มีข้อบังคับพิเศษ	กรณีที่ข้อมูลลับหรือข้อมูลลับที่สุดใดไม่มีเครื่องหมายแสดงชั้นความลับไว้ แต่หากพนักงานรู้ หรือควรจะรู้ข้อเท็จจริงว่าข้อมูลนั้น	

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
			ได้มีการกำหนดชั้นความลับไว้แล้ว ให้ปฏิบัติกับข้อมูลนั้น ๆ เช่นเดียวกับข้อมูลที่มีเครื่องหมายแสดงชั้นความลับไว้ และให้พนักงานจัดทำหรือแจ้งหน่วยงานเจ้าของสารสนเทศให้จัดทำเครื่องหมายแสดงชั้นความลับโดยเร็ว	

4.4 นโยบายการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)

บริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จึงกำหนดให้มีการลบทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลตาม**นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)** หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม และสอดคล้องกับการรักษาความลับของข้อมูลส่วนบุคคล

ทั้งนี้เพื่อป้องกันการสูญหาย การเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย ให้ดำเนินการตามแนวทางในการควบคุมและป้องกันสารสนเทศที่กำหนดใน**นโยบายการแยกประเภทของข้อมูลส่วนบุคคล (Personal Data Classification Policy)**

1. แนวทางในการลบหรือทำลายข้อมูล

บริษัทมีการเก็บรักษาข้อมูลทั้งในรูปแบบกระดาษ สื่อบันทึกข้อมูลและอิเล็กทรอนิกส์ ซึ่งมีแนวทางการลบหรือทำลายด้วยวิธีที่มีความมั่นคงปลอดภัยอย่างเหมาะสมกับระดับชั้นความลับของข้อมูลและประเภทของข้อมูลแตกต่างกัน รายละเอียดดังนี้

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การทำลายข้อมูล				
เอกสารฉบับพิมพ์ (Hard Copy)	ไม่มีข้อบังคับพิเศษ	ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร	ใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร	ต้องส่งเอกสารคืนกลับให้หน่วยงานเจ้าของข้อมูลเพื่อทำการทำลาย หรือใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) เท่านั้น โดยต้องได้รับอนุมัติจากระดับผู้จัดการฝ่ายขึ้นไปของหน่วยงานเจ้าของสารสนเทศก่อนทำลาย
การทำลายข้อมูลอิเล็กทรอนิกส์	ไม่มีข้อบังคับพิเศษ	ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser	ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes หรือ Dumping ข้อมูล **กรณีที่มีการคืนอุปกรณ์ให้กับหน่วยงานภายนอกให้ใช้ซอฟต์แวร์ Low Level Format	
การทำลายข้อมูลค่า Configuration และข้อมูลที่จัดเก็บบนอุปกรณ์	ไม่มีข้อบังคับพิเศษ	Reset ค่า Configuration และข้อมูลที่จัดเก็บบนอุปกรณ์เป็นค่า Factory Default		

ประเภทข้อมูล	ทั่วไป (Public)	ใช้ภายใน (Internal Use)	ความลับ (Confidential)	ความลับที่สุด (Secret)
การทำลายสื่อบันทึกข้อมูลชนิด CD/DVD	ไม่มีข้อบังคับพิเศษ	ทุบทำลาย หรือใช้เครื่องทำลายแผ่นบันทึกข้อมูลแบบ Strip-cut		
การทำลายสื่อบันทึกข้อมูลชนิด USB Flash Drive, Hard disk และ Tape	ไม่มีข้อบังคับพิเศษ	ทุบทำลาย หรือ วิธีการที่กลุ่มเทคโนโลยีสารสนเทศพิจารณาว่ามีความมั่นคงปลอดภัย		

ทั้งนี้หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

2. แนวทางการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

2.1 ในกรณีที่ไม่สามารถลบหรือทำลายข้อมูลส่วนบุคคลได้โดยตรง เนื่องจากอาจส่งผลกระทบต่อความถูกต้องในการปฏิบัติงาน เช่น อาจส่งผลให้การทำงานของฐานข้อมูลไม่ถูกต้อง หรือเป็นข้อจำกัดของระบบ บริษัทจะใช้วิธีการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของข้อมูลส่วนบุคคลได้ ดังนี้

1) การเปลี่ยนแปลงส่วนใดส่วนหนึ่งของข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม หรือการทำให้เป็นข้อมูลอื่น ๆ หรือการใช้กระบวนการอื่นใดที่ได้รับการรับรองเป็นมาตรฐานในปัจจุบัน เช่น การใช้ Hash Function เพื่อเปลี่ยนข้อมูลเดิมให้ไม่สามารถที่จะให้ข้อมูลย้อนกลับมาระบุตัวตนของเจ้าของข้อมูลได้

2) การลดความชัดเจนของข้อมูล (Blurring or Noising) โดยการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลเดิมเพื่อลดความเฉพาะเจาะจงของข้อมูลลง

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวตนได้เพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

2.2 บริษัทจะดำเนินการลบข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ตามประเภทของข้อมูลส่วนบุคคลเมื่อมีกรณีดังต่อไปนี้

1) ครบกำหนดระยะเวลาการจัดเก็บตามที่กำหนดไว้**นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)**

2) ข้อมูลส่วนบุคคลนั้นไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

3) ข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย

4) เจ้าของข้อมูลส่วนบุคคลร้องขอการใช้สิทธิตามสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคลที่มีการระบุไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

2.3 หากมีการขอให้ลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ บริษัทจะดำเนินการตามกระบวนการดังนี้

1) เมื่อได้รับแบบคำร้องขอใช้สิทธิในการลบหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ข้อมูลจะถูกส่งต่อไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและทำการบันทึกเอาไว้

2) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการตรวจสอบข้อมูลส่วนบุคคลทั้งหมดที่เกี่ยวข้อง เพื่อหาความจำเป็นขั้นพื้นฐานทางกฎหมายและวัตถุประสงค์เดิม

3) ตรวจสอบแบบคำร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ เพื่อให้แน่ใจว่าการขอลบข้อมูลนั้นจะไม่เกี่ยวกับวัตถุประสงค์ในการเก็บรวบรวม หรือการประมวลผลอย่างอื่น

4) ดำเนินการลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงตรวจสอบเพื่อให้แน่ใจว่ามีการลบ/ทำลายข้อมูลส่วนบุคคลออกจากระบบหรือเอกสารที่ใช้งานอยู่ รวมถึงในระบบสำรอง หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้

5) หากมีการปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบันทึกการปฏิเสธดังกล่าวพร้อมเหตุผลในการปฏิเสธ และแจ้งเจ้าของข้อมูลส่วนบุคคลให้รับทราบ

2.4 บริษัทสามารถปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคลที่ขอให้ลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ ตามมาตรา 33 วรรคสอง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

1) มีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล

2) เป็นการจำเป็นในการปฏิบัติตามกฎหมายของบริษัทเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตราย หรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

3) การเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

4.5 นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing)

นโยบายนี้มีวัตถุประสงค์เพื่อกำหนดแนวทางการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่บริษัทมีการเก็บรวบรวม ใช้ และเปิดเผยไปยังบุคคลอื่น ครอบคลุมทั้งข้อมูลส่วนบุคคลของลูกค้า พนักงาน ลูกจ้าง และพันธมิตรของบริษัทให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1. แนวปฏิบัติ

แนวปฏิบัติการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

1.1 หน่วยงานที่มีการเปิดเผยข้อมูลส่วนบุคคลให้กับ คู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือผู้ให้บริการภายนอก จะต้องมีการทำข้อตกลงหรือสัญญาในการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement) ระหว่างบริษัทซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล และคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือผู้ให้บริการภายนอกรายนั้นซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล โดยข้อตกลงหรือสัญญาจะต้องเป็นไปตามรูปแบบที่บริษัทกำหนดไว้

1.2 เนื้อหาของข้อตกลงหรือสัญญาระหว่างบริษัท และคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอกดังกล่าวจะต้องมีการกำหนดมาตรการเกี่ยวกับ

1.2.1 หน้าที่ในการประมวลผลข้อมูล โดยต้องมีข้อความเกี่ยวกับ

1) คำสั่งในการประมวลผลข้อมูลส่วนบุคคล และไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งเป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคล และการให้การรับรองจากผู้ประมวลผลข้อมูลส่วนบุคคลว่าคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลเป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2) การให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีการจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้กับบุคคลที่ได้รับมอบหมาย โดยให้เข้าถึงข้อมูลส่วนบุคคลได้เท่าที่จำเป็นภายในวัตถุประสงค์ที่กำหนด

3) ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ประมวลผล รวมถึงมีมาตรการที่ทำให้มั่นใจว่าบุคคลที่ได้รับสิทธิเข้าถึงข้อมูลส่วนบุคคลได้ให้คำมั่นสัญญาหรือมีหน้าที่ตามสัญญาในการรักษาความลับของข้อมูลส่วนบุคคล

4) ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็นต่อการปฏิบัติตามหน้าที่ตามสัญญาหรือตามที่ตกลงกัน รวมถึงยินยอมและให้ความร่วมมือในการตรวจสอบและสอบสวนโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ตรวจสอบซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย

1.2.2 มาตรการในการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อความเกี่ยวกับ

ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดหามาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อเป็นการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลส่วนบุคคล โดยต้องมีมาตรการป้องกันด้านการบริหารจัดการ (Administrative safeguard) มาตรการป้องกันด้านเทคนิค (Technical safeguard) และมาตรการป้องกันทางกายภาพ (Physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (Access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการดังนี้

1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

2) การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล

3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

4) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล

5) การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

1.2.3 หน้าที่ในการดำเนินกิจกรรมที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล

6) หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการสนับสนุนผู้ควบคุมข้อมูลส่วนบุคคลในเรื่องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

7) การแจ้งต่อผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

1.2.4 การแจ้งเตือนหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ

การแจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า หากทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

1.2.5 การเก็บรักษาข้อมูลส่วนบุคคล และการลบข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ

8) หน้าที่และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็น เพื่อการปฏิบัติหน้าที่ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
9) วิธีในการลบ ทำลาย ส่งคืน หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
10) การเก็บข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

1.2.6 การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยต้องมีข้อความเกี่ยวกับ

1) การไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เว้นแต่จะได้รับอนุญาตจากบริษัท
2) การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ จะต้องเป็นไปตามเงื่อนไขที่กำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคลและประกาศที่เกี่ยวข้อง

4.6 นโยบายการส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก หรือการส่งข้อมูลส่วนบุคคลไปยังประเทศอื่น (Third Parties / Cross Border Data Transfer Policy)

บริษัทได้มีการกำหนดนโยบายในการเปิดเผยข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก หรือการส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศ โดยมีวัตถุประสงค์เพื่อชี้แจงข้อตกลงในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก (หน่วยงานภายนอก) หรือการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ และกำหนดหลักเกณฑ์และมาตรการคุ้มครองในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอก (หน่วยงานภายนอก) หรือการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ

1. การส่งหรือโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก

บริษัทจะเปิดเผยข้อมูลส่วนบุคคลให้แก่องค์กรหรือหน่วยงานภายนอกโดยมีแนวปฏิบัติดังนี้

1.1 หากจะมีการเปิดเผยข้อมูลส่วนบุคคลให้กับ บริษัทคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก ควรมีการระบุรายชื่อของ บริษัทคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก ในบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรให้คำปรึกษาและจะต้องพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลและเงื่อนไขให้สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

1.2 กรณีส่งหรือโอนข้อมูลส่วนบุคคลไปยังนิติบุคคล จะต้องพิจารณาว่าในการส่งหรือโอนข้อมูลส่วนบุคคลนั้นมีมาตรการการรักษาความมั่นคงปลอดภัย และมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน

1.3 กรณีที่หน่วยงานรัฐ หรือองค์กรผู้ถืออำนาจรัฐ ร้องขอเข้าถึงข้อมูลส่วนบุคคลโดยการอ้างถึงกฎหมาย ระเบียบ หรือคำสั่งใด ๆ ที่บริษัทจะต้องปฏิบัติตาม ผู้รับผิดชอบควรพิจารณาให้หน่วยงานเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่มีบทบัญญัติกฎหมาย หรือคำสั่ง หรือหนังสือแจ้งอย่างเป็นทางการ อย่างใดอย่างหนึ่งเป็นอย่างน้อยตามอำนาจทางกฎหมายเท่านั้น มิเช่นนั้นบริษัทจะมีความผิดตามกฎหมายจากการให้หน่วยงานดังกล่าวเข้าถึงหรือเปิดเผยข้อมูลโดยไม่มีหน้าที่ตามกฎหมาย ยกเว้นกรณีที่เป็นการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation) ของบริษัทที่แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่บริษัทจะต้องกระทำตามหน้าที่อยู่แล้ว

2. การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Cross Border data Transfer Policy)

เพื่อให้การส่งหรือโอนข้อมูลส่วนบุคคลอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล การดำเนินการส่งหรือโอนข้อมูลส่วนบุคคลไปประเทศปลายทาง หรือองค์กรระหว่างประเทศจะต้องมีความมั่นคงปลอดภัย โดยบริษัทสามารถพิจารณาทางเลือกดังต่อไปนี้

2.1 การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์กรระหว่างประเทศ บริษัทจะดำเนินการส่งข้อมูลส่วนบุคคลไปยังประเทศที่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่ง

หรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

2.2 มีการจัดทำข้อตกลงระหว่างกันในรูปแบบใดรูปแบบหนึ่งดังต่อไปนี้

- นโยบายการคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules) ที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองส่วนบุคคลแล้ว
- มีการจัดทำข้อตกลงเป็นไปตามข้อสัญญามาตรฐาน (Standard Data Protection Clauses)
- จรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ (Code of Conduct)

2.3 ในกรณีที่ไม่สามารถใช้ทางเลือกการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในข้อ 1) และ 2) สามารถดำเนินการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ หากเป็นกรณีดังนี้

- เป็นการปฏิบัติตามกฎหมายของบริษัท
- บริษัทได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
- บริษัทมีความจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
- เป็นการกระทำตามสัญญาระหว่างบริษัทกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- บริษัทมีความจำเป็นต้องป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
- บริษัทมีความจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

2.4 ในกรณีที่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้นไม่มีมาตรฐานเพียงพอ ให้เสนอต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยเสียก่อน

3. การคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

บริษัทสามารถโอนข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกันได้ หากการส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวเป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน (“สมาชิกเครือกิจการ”) ที่ได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว โดยนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หรือ Binding Corporate Rules (“BCR”) จะต้องมีลักษณะ ดังนี้

3.1 มีผลผูกพันตามกฎหมายและบังคับใช้กับสมาชิกเครือกิจการทุกราย รวมถึงลูกจ้างและพนักงานของสมาชิกเครือกิจการ

3.2 รับรองสิทธิอันสามารถบังคับใช้ได้ของเจ้าของข้อมูลส่วนบุคคลที่ถูกนำข้อมูลส่วนบุคคลมาประมวลผล

3.3 BCR ควรประกอบด้วยองค์ประกอบอย่างน้อยดังต่อไปนี้

1) รายละเอียดโครงสร้างและช่องทางการติดต่อของสมาชิกเครือกิจการ
2) ข้อมูลส่วนบุคคลที่จะถูกเปิดเผยหรือชุดข้อมูลส่วนบุคคลที่จะถูกเปิดเผย รวมถึงรายละเอียดประเภทของข้อมูลส่วนบุคคล, วิธีการและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล, ประเภทของเจ้าของข้อมูลส่วนบุคคล, ประเทศหรือองค์การระหว่างประเทศปลายทางซึ่งรับข้อมูลส่วนบุคคล
3) ความมีผลผูกพันทางกฎหมายทั้งภายในและภายนอกกลุ่มสมาชิกเครือกิจการ
4) การนำหลักการคุ้มครองข้อมูลทั่วไปมาปรับใช้ เช่น การจำกัดวัตถุประสงค์ (Purpose Limitation), การใช้ข้อมูลอย่างน้อยที่สุด (Data Minimization), การจำกัดระยะเวลาในการจัดเก็บข้อมูล (Limited Storage Periods), คุณภาพของข้อมูล (Data Quality), การคุ้มครองข้อมูลผ่านการออกแบบและโดยปริยาย (Data Protection by Design and by Default), ฐานกฎหมายในการประมวลผลข้อมูลส่วนบุคคล (Lawful Basis for Processing), การประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 ของกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Processing of Special Categories of Personal Data), มาตรการในการรับประกันความปลอดภัยของข้อมูล และเงื่อนไขในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอกที่ไม่ใช่สมาชิกเครือกิจการ (Requirements in Respect of Onward Transfers to Bodies not Bound by the Binding Corporate Rules)
5) สิทธิของเจ้าของข้อมูลส่วนบุคคลอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล และช่องทางในการใช้สิทธินั้น รวมถึงสิทธิที่จะร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการฟ้องร้องคดีต่อศาลที่มีอำนาจ สิทธิในการได้รับการเยียวยา และสิทธิในการได้รับค่าเสียหายอันเกิดจากการละเมิด BCR
6) ความยินยอมรับผิดโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นสมาชิกเครือกิจการซึ่งตั้งอยู่ในประเทศไทย ในกรณีที่เกิดเหตุละเมิด BCR โดยสมาชิกเครือกิจการซึ่งไม่ได้ตั้งอยู่ในประเทศไทย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ต้องรับผิดบางส่วนหรือทั้งหมด หากพิสูจน์ได้ว่าสมาชิกเครือกิจการมิได้มีส่วนรับผิดชอบกับเหตุการณ์ที่ก่อให้เกิดความเสียหาย
7) การแจ้งเนื้อหาของ BCR (โดยเฉพาะข้อ 4) - ข้อ 6)) ให้แก่เจ้าของข้อมูลส่วนบุคคลรับทราบเพิ่มเติมจากการแจ้งรายละเอียดตามมาตรา 23 และมาตรา 25 ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
8) หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer (DPO) ที่ได้รับมอบหมายตามมาตรา 41 ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือบุคคลหรือนิติบุคคลที่ได้รับมอบหมายให้ตรวจสอบการดำเนินการตาม BCR ของสมาชิกเครือกิจการ, การฝึกอบรม หรือการรับเรื่องร้องเรียน
9) กระบวนการรับเรื่องร้องเรียน

10) กลไกภายในกลุ่มสมาชิกเครือกิจการสำหรับการรับประกันการดำเนินการตาม BCR ซึ่งต้องมีองค์ประกอบอย่างน้อยดังนี้ การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Audit) และวิธีการในการรับประกันการดำเนินการเชิงแก้ไขเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยบุคคลที่ได้รับมอบหมายตามข้อ 8) (DPO) และคณะกรรมการกลุ่มสมาชิกเครือกิจการจะต้องรับทราบผลการตรวจสอบข้างต้น รวมถึงจัดเตรียมให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบผลการตรวจสอบข้างต้นได้
11) กลไกการรายงานและบันทึกการเปลี่ยนแปลงเนื้อหาของ BCR และการรายงานการเปลี่ยนแปลงดังกล่าวไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
12) กลไกการให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการรับประกันการดำเนินการตาม BCR ของสมาชิกเครือกิจการ เช่น การจัดเตรียมผลการตรวจสอบให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้
13) กลไกในการรายงานไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งข้อบังคับทางกฎหมายที่สมาชิกเครือกิจการที่ตั้งอยู่ในประเทศปลายทางต้องปฏิบัติตามอันอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อหลักประกันที่ได้ให้ไว้ตาม BCR
14) จัดการฝึกอบรมการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมให้แก่พนักงานหรือบุคคลที่เข้าถึงข้อมูลส่วนบุคคลเป็นประจำหรือตลอดเวลา

นอกเหนือจาก BCR แล้ว บริษัทอาจยอมรับให้มาตรการคุ้มครองที่เหมาะสมอื่น ๆ ที่สามารถบังคับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจมีการกำหนดขึ้น ได้แก่ ข้อสัญญามาตรฐาน หรือจรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ หรือคำรับรอง ซึ่งเป็นเงื่อนไขที่ทำให้บริษัท สามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางได้ แม้ว่าประเทศปลายทางนั้นจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยอาจเลือกใช้แนวทางตามข้อ 4 ดังต่อไปนี้

4. ข้อสัญญามาตรฐาน (Standard Data Protection Clauses)

บริษัทสามารถนำข้อสัญญามาตรฐาน (Standard Contractual Clauses) มาใช้เพื่อให้ข้อมูลส่วนบุคคลถูกส่งหรือโอนอย่างที่ควรจะเป็น เพื่อให้การให้บริการ รวมถึงการรักษามาตรฐานและการปรับปรุงบริการให้เป็นไปโดยถูกต้องตามกฎหมาย อย่างไรก็ตามข้อสัญญาคุ้มครองข้อมูลส่วนบุคคลจะต้องมีการกำหนดหน้าที่ทางสัญญาเกี่ยวกับการส่งข้อมูลส่วนบุคคลไปยังต่างประเทศตลอดจนการโอนย้ายข้อมูลส่วนบุคคล ซึ่งเจ้าข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนเองในการส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศได้ โดยต้องมีมาตรการคุ้มครองที่เหมาะสม ดังนี้

4.1 ในการตกลงส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศจะต้องมีรายละเอียดเกี่ยวกับ

4.1.1 บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1) รับรองว่าการเก็บรวบรวม ประมวล ส่งหรือโอนข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2) พิจารณาว่าผู้รับโอนข้อมูลส่วนบุคคลสามารถปฏิบัติตามข้อกำหนดตามที่ระบุในนโยบายนี้ได้
3) ให้ข้อมูลเกี่ยวกับกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลซึ่งใช้บังคับอยู่ในประเทศปลายทางหรือบังคับแก่องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล
4) ตอบคำถามของเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้รับการส่งหรือโอนข้อมูลส่วนบุคคล
5) ให้ข้อมูลเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสิทธิเกี่ยวกับความรับผิดและสิทธิของบุคคลที่สามแก่เจ้าของข้อมูลส่วนบุคคล
6) ร่วมรับผิดกับผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการฝ่าฝืนข้อกำหนด
7) ร่วมกับผู้รับการส่งหรือผู้รับโอนในการระงับข้อพิพาทที่เกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผข้อมูลส่วนบุคคล โดยใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ยซึ่งไม่ได้มีผลบังคับผูกพันทางกฎหมาย
8) ในกรณีที่ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลฝ่าฝืนหน้าที่ตามที่ได้กำหนด บริษัทมีสิทธิที่จะพักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจนกว่าการฝ่าฝืนจะได้รับการแก้ไขหรือข้อกำหนดถูกยกเลิก

4.1.2 บุคคลผู้รับส่งหรือรับโอนข้อมูลส่วนบุคคลที่มีฐานะเป็นผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1) กำหนดว่ามีการจัดมาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) กฎหมายคุ้มครองข้อมูลส่วนบุคคล
2) ดำเนินการให้บุคคลภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลนั้น รักษาความลับของข้อมูลส่วนบุคคล

3) รับรองว่าตนไม่มีเหตุอันควรจะเชื่อได้ว่ามีกฎหมายใดที่ขัดขวางมิให้สามารถปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามข้อกำหนดนี้ได้
4) ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่กำหนดเท่านั้น
5) แจ้งให้บริษัทได้ทราบถึงส่วนงานภายในองค์กรซึ่งมีหน้าที่ในการตอบสนองต่อคำร้องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและจะให้ความร่วมมือกับบริษัทโดยสุจริต
6) ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบ ในกรณีที่ได้รับการร้องขอจากบริษัท
7) ประมวลผลข้อมูลส่วนบุคคลโดยสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
8) ร่วมรับผิดกับบริษัทในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการฝ่าฝืนข้อกำหนด
9) ร่วมกับบริษัทในการระงับข้อพิพาทที่เกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ยซึ่งไม่ได้มีผลบังคับผูกพันทางกฎหมาย

4.2 ในการตกลงส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศ จะต้องมีรายละเอียดเกี่ยวกับข้อสัญญาที่กำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถบังคับสิทธิของตนต่อบริษัท ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลช่วง และ

4.2.1 บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1) รับรองว่าการประมวลผลข้อมูลส่วนบุคคลซึ่งหมายรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นไปโดยสอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
2) รับรองว่าผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลจะประมวลผลข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนตามคำสั่งของบริษัทในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายที่บังคับใช้แก่กรณีและข้อกำหนดนี้
3) รับรองว่าผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะจัดหามาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
4) รับรองว่าจะมีการจัดหามาตรการด้านความปลอดภัยเพื่อป้องกันคุ้มครองมิให้ข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนสูญหายโดยอุบัติเหตุหรือโดยการกระทำโดยมิชอบ หรือการถูกทำลายโดยอุบัติเหตุหรือการกระทำโดยมิชอบ การเปลี่ยนแปลงแก้ไข การถูกเปิดเผย หรือการเข้าถึงโดยมิชอบ โดยเฉพาะอย่างยิ่งในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลผ่านระบบโครงข่าย (Transmission of Data over a Network) และการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายใด ๆ
5) รับรองว่าจะมีการปฏิบัติตามมาตรการคุ้มครองความปลอดภัยของข้อมูล
6) รับรองว่าเจ้าของข้อมูลส่วนบุคคลจะได้รับการแจ้งว่ามีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลในกรณีที่เป็นการ

ส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมารตรา 26 กฎหมายคุ้มครองข้อมูลส่วนบุคคล

7) ดำเนินการส่งการแจ้งเตือนที่ได้รับจากผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่บริษัทตัดสินใจว่าจะส่งหรือโอนข้อมูลส่วนบุคคลต่อไป หรือยกเลิกพักการส่งหรือโอนข้อมูลส่วนบุคคล
8) ส่งบทสรุปรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลช่วง
9) ร่วมกับบริษัทรับผิดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นการกระทำของบริษัทหรือผู้รับสิทธิการส่งหรือรับโอน
10) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถเรียกร้องค่าเสียหายจากบริษัทตามข้อกำหนดได้เนื่องจากบริษัทไม่สามารถถูกติดตามตัวได้หรือล้มละลาย เจ้าของข้อมูลส่วนบุคคลสามารถเรียกค่าเสียหายได้จากการผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล
11) บริษัทจะส่งสำเนาของข้อกำหนดนี้ให้สำนักงานคณะกรรมคุ้มครองข้อมูลส่วนบุคคลเก็บรักษาไว้

4.2.2 บุคคลผู้รับส่งหรือรับโอนข้อมูลส่วนบุคคลที่มีฐานะเป็นผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1) รับรองว่าจะประมวลผลข้อมูลส่วนบุคคลเฉพาะในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลและตามคำสั่งของบริษัทเท่านั้น ในกรณีที่ไม่สามารถปฏิบัติการตามหน้าที่ดังกล่าวได้จะแจ้งบริษัททราบโดยไม่ชักช้า ในกรณีนี้บริษัทสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้
2) รับรองว่าตนไม่มีเหตุอันควรจะเชื่อได้ว่ามีกฎหมายใดที่ขัดขวางมิให้สามารถประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของบริษัท และในกรณีที่มีการเปลี่ยนแปลงทางกฎหมายซึ่งจะส่งผลต่อการปฏิบัติหน้าที่ตามข้อกำหนดนี้ ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะแจ้งให้บริษัททราบถึงการเปลี่ยนแปลงดังกล่าวโดยไม่ชักช้า ในกรณีนี้บริษัทสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้
3) รับรองว่าตนได้จัดหามาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) กฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว
4) แจ้งให้บริษัททราบโดยไม่ชักช้าเกี่ยวกับคำร้องให้เปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมาย เว้นแต่ กรณีไม่สามารถแจ้งได้เนื่องจากมีกำหมายห้าม เช่น เป็นข้อห้ามตามกฎหมายอาญาเพื่อรักษาความลับของการดำเนินกระบวนการสืบสวนสอบสวน การเข้าถึงข้อมูลหรือโดยการกระทำที่มิชอบ และคำร้องที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรงโดยไม่มีการตอบสนองต่อคำร้องดังกล่าว
5) สอบถามบริษัทถึงการประมวลผลข้อมูลส่วนบุคคลซึ่งถูกส่งหรือโอน

6) ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบในกรณีที่ได้รับคำร้องขอจากบริษัท
7) ส่งบทสรุปรายละเอียดเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลตลอดจนสำเนาสัญญาให้บริการประมวลผลข้อมูลส่วนบุคคลช่วงโดยลบส่วนที่เป็นข้อมูลเชิงพาณิชย์ออก แต่มีการเติมรายละเอียดเกี่ยวกับมาตรการรักษาความปลอดภัยเข้าไปแทนในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถดำเนินการให้ได้รับรายละเอียดดังกล่าวจากบริษัทได้
8) แจ้งบริษัทให้ทราบถึงการประมวลผลข้อมูลส่วนบุคคลช่วงและได้รับความยินยอม
9) ร่วมกับบริษัทรับผิดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นการกระทำของบริษัทหรือผู้รับการส่งหรือรับโอน
10) การประมวลผลข้อมูลส่วนบุคคลช่วงจะเป็นไปตามข้อกำหนดนี้
11) ส่งสำเนาสัญญาประมวลผลข้อมูลส่วนบุคคลช่วงให้กับบริษัท
12) ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนเพื่อเรียกร้องค่าสินไหมทดแทนหรือค่าเสียหายจากผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลตกลงว่าจะระงับข้อพิพาทดังกล่าวโดยการไกล่เกลี่ยซึ่งมีความเป็นอิสระหรือโดยองค์กรคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

4.3 จรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ (Code of Conduct)

บริษัทจะนำส่งหรือโอนข้อมูลส่วนบุคคลเมื่อผู้รับโอนได้ลงนามในข้อปฏิบัติซึ่งได้รับการอนุมัติจากเจ้าพนักงาน โดยข้อปฏิบัติที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศจะต้องมีรายละเอียดของมาตรการที่เหมาะสมในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งถูกนำไปประมวลผล ตลอดจนโอนข้อมูลส่วนบุคคล ทั้งนี้ข้อปฏิบัติดังกล่าวจะต้องมีผลบังคับได้ต่อเจ้าข้อมูลส่วนบุคคลโดยตรง บริษัทจะนำจรรยาบรรณและจริยธรรมในการดำเนินธุรกิจที่ยึดมั่นในเจตนารมณ์ของการดำเนินธุรกิจอันตั้งอยู่บนพื้นฐานของการบริหารจัดการตามหลักการกำกับดูแลกิจการที่ดี โดยยึดมั่นต่อคุณธรรมและจริยธรรมในการดำเนินธุรกิจ มีความโปร่งใสตรวจสอบได้ และตระหนักถึงความรับผิดชอบต่อผู้มีส่วนได้เสียทุกฝ่าย เพื่อให้เกิดการป้องกันข้อมูลส่วนบุคคลอย่างเหมาะสมและเป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

4.4 คำรับรอง (Certification Mechanism)

บริษัทจะใช้คำรับรองที่ได้รับการยอมรับโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งประกอบกับคำมั่นสัญญาที่มีผลบังคับผูกพันผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศที่จะปรับใช้มาตรการที่เหมาะสมเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อแสดงให้เห็นว่ามีการป้องกันที่เหมาะสมในการส่งหรือโอนข้อมูลส่วนบุคคลในระดับสากล