บริษัท เอเอสเอ็น โบรกเกอร์ จำกัด (มหาชน)

และบริษัทย่อย

นโยบายคุ้มครองข้อมูลส่วนบุคคล

(Data Protection Policy)

สารบัญ

หน้า

1. คำนิยาม

ในนโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ คำหรือข้อความสามารถนิยามได้ดังนี้

เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลซึ่งสามารถถูกระบุตัวตนได้โดยข้อมูลส่วนบุคคลนั้น ๆ ไม่ว่าโดยทางตรงหรือทางอ้อม
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
การประมวลผลข้อมูลส่วนบุคคล (Processing)	การดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อม ใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	ผู้ที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	ผู้ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล
ข้อมูลบริษัท	ข้อมูลในรูปแบบใดก็ตามทั้งในแบบอิเล็กทรอนิกส์และไม่ใช่อิเล็กทรอนิกส์ เช่น ข้อมูลในสิ่งพิมพ์ซึ่งอยู่ในระบบภายในหรือระบบภายนอกที่นอกเหนือการควบคุมของบริษัท และปรากฏเงื่อนไขดังต่อไปนี้ ▪ ข้อมูลที่พนักงานของบริษัทหรือบุคคลที่ได้รับมอบหมายได้มา ประมวลผล จัดการ และ/หรือ ดูแล (เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษา) เพื่อปฏิบัติหน้าที่ ▪ ข้อมูลที่เกี่ยวเนื่องกับการจัดการ การปฏิบัติงาน วางแผน รายงาน หรือการตรวจสอบการดำเนินงานของบริษัท ▪ ข้อมูลที่ใช้อ้างอิงหรือจำเป็นต่อการทำงานของหน่วยงานอย่างน้อยหนึ่งหน่วย

การเข้าถึงข้อมูล (Access)	หมายถึง สิทธิในการอ่าน/ดู บันทึก คัดลอก เก็บสำรอง จัดเก็บ สืบค้น ดาวน์โหลด หรือแก้ไข (อัพเดท แทรก/เพิ่ม ลบ) ข้อมูล รวมถึงการจัดการสิทธิการเข้าถึงนั้น ๆ
ผู้ใช้ หรือ ผู้ใช้ข้อมูล (Data Users)	หมายถึง บุคคลดังต่อไปนี้ ▪ พนักงานบริษัท เอเอสเอ็น โบรกเกอร์ จำกัด (มหาชน) ▪ บุคลากรที่บริษัทกำหนดให้เข้าถึงข้อมูล เพื่อปฏิบัติงานตามที่ได้รับมอบหมาย เช่น ผู้รับเหมา หน่วยงานภายนอก ที่ปรึกษาฯ ▪ บุคลากรของพันธมิตรของบริษัทซึ่งได้รับความยินยอม/อนุญาตจากบริษัทให้เข้าถึงข้อมูลอย่างเฉพาะเจาะจงและจำกัด เพื่อปฏิบัติงานตามที่ได้รับมอบหมาย ซึ่งเป็นไปเพื่อสนับสนุนการดำเนินงานของบริษัท
หน่วยงาน	สายงาน ฝ่ายงาน หรือหน่วยปฏิบัติงานภายใต้ความรับผิดชอบของบริษัทเพื่อกิจกรรมเฉพาะขององค์กร
การบันทึก (Record)	ข้อมูลหรือสารสนเทศในรูปแบบเฉพาะ ซึ่งถูกสร้างขึ้นหรือได้มาจากกิจกรรมบุคคลหรือกิจกรรมองค์กร และได้สำรอง (เก็บรักษา) ไว้เป็นหลักฐานของกิจกรรมนั้น ๆ เพื่อใช้อ้างอิงในอนาคต
บริษัท	บริษัท เอเอสเอ็น โบรกเกอร์ จำกัด (มหาชน) บริษัท เอเอสเอ็น ไลฟ์ โบรกเกอร์ จำกัด และ บริษัทได้เงิน ดอทคอม จำกัด
กฎหมายคุ้มครองข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และที่จะมีการแก้ไขเพิ่มเติม รวมถึงกฎ ระเบียบ และคำสั่งที่เกี่ยวข้อง

2. วัตถุประสงค์

บริษัท เอเอสเอ็น โบรกเกอร์ จำกัด (มหาชน) (“บริษัท”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการรับผิดชอบต่อสังคมและเป็นรากฐานในการสร้างความสัมพันธ์ที่น่าเชื่อถือกับประชาชน บริษัทจึงยึดมั่นในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎเกณฑ์ทางการอื่น ๆ ที่เกี่ยวข้อง

เอกสารฉบับนี้ได้รับการจัดทำขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

- เพื่อชี้แจงความรับผิดชอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- เพื่อกำหนดมาตรฐานและแนวทางบริหารข้อมูลส่วนบุคคล โดยครอบคลุมถึงการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล

3. ขอบเขต

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

4. คำแถลงนโยบาย

4.1 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy)

- นโยบายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Policy) ดูแลโดย ฝ่ายกฎหมายและบริหารความเสี่ยง และต้องจัดให้มีการประกาศและสื่อสารไปยังพนักงานและหน่วยงานที่เกี่ยวข้อง และกำหนดให้มีการทบทวนและปรับปรุงนโยบายฉบับนี้ให้เป็นปัจจุบันอย่างสม่ำเสมอ
- การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลจะต้องเป็นไปตามกฎหมาย มีความเป็นธรรม และมีความโปร่งใส
- การเก็บรวบรวมข้อมูลส่วนบุคคล จะต้องพอเหมาะเป็นไปตามวัตถุประสงค์ที่กำหนด เป็นไปตามฐานในการประมวลผลข้อมูลส่วนบุคคล
- การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการประมวลผลข้อมูลส่วนบุคคลอย่างจำกัด และสอดคล้องตามวัตถุประสงค์ที่กำหนด
- การประมวลผลข้อมูลส่วนบุคคลจะต้องมีการปรับปรุงอยู่เสมอ รวมทั้งจะต้องมีการกำหนดขั้นตอนในการตรวจสอบ เพื่อให้ข้อมูลส่วนบุคคลมีความถูกต้องเป็นไปตามกฎหมายหรือหน่วยงานกำกับดูแลที่เกี่ยวข้องกำหนด

- บริษัทอนุญาตให้จัดเก็บข้อมูลส่วนบุคคลภายในระยะเวลาที่บริษัทกำหนดเท่านั้น ข้อมูลส่วนบุคคลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด ผู้รับผิดชอบจะต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
- การประมวลผลข้อมูลส่วนบุคคลจะต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการป้องกันการประมวลผลข้อมูลส่วนบุคคลโดยผู้ที่ไม่มีสิทธิ การลบหรือทำลายข้อมูลทั้งโดยความตั้งใจและไม่ตั้งใจ และรวมถึงการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศให้อยู่ในระดับที่องค์กรยอมรับได้

4.2 การปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคล (Rights of Data Subject)

- สายงานที่เกี่ยวข้องจะต้องพิจารณาถึงสิทธิของเจ้าของข้อมูลส่วนบุคคล ดังต่อไปนี้
    - สิทธิในการเพิกถอนความยินยอม
    - สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
    - สิทธิในการขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอม
    - สิทธิในการขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น
    - สิทธิในการคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
    - สิทธิในการขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้
    - สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล
    - สิทธิในการขอให้แก้ไขข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์
- สายงานที่เกี่ยวข้องและ DPO จะต้องร่วมจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล โดยรายละเอียดของบันทึกรายการการประมวลผลข้อมูลส่วนบุคคลจะต้องมีความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และหลักเกณฑ์ที่เกี่ยวข้อง
- จัดให้มีการระบุช่องทางในการใช้สิทธิให้กับเจ้าของข้อมูลส่วนบุคคลทราบ
- สายงานที่เกี่ยวข้องและ DPO จะต้องบันทึกรายละเอียดเกี่ยวกับการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยต้องประกอบด้วยข้อมูลดังต่อไปนี้
    - รายละเอียดของเจ้าของข้อมูลส่วนบุคคล
    - รายละเอียดการขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
    - รายละเอียดของการดำเนินการ ซึ่งรวมถึงเหตุผลในกรณีที่มีการปฏิเสธการขอตามสิทธิของเจ้าของข้อมูลส่วนบุคคล
- เมื่อมีการขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคล หน่วยงานจะต้องปฏิบัติตามกระบวนการการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลของบริษัทโดยเคร่งครัด

4.3 การประมวลผลข้อมูลส่วนบุคคลให้สอดคล้องตามกฎหมาย (Lawfulness of Processing)

- สายงานที่เกี่ยวข้องและ DPO จะต้องร่วมกันทบทวนให้การประมวลผลข้อมูลส่วนบุคคลมีความสอดคล้องกับกฎหมาย โดยจะต้องระบุฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยการในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลจะต้องเป็นไปตามวัตถุประสงค์อันชอบด้วยกฎหมาย และมีความสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยในการระบุฐานในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถพิจารณาได้ดังนี้
    - ข้อมูลส่วนบุคคล
        - การขอความยินยอม
        - ความจำเป็นเพื่อการปฏิบัติตามสัญญา
        - ความจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล
        - ความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย
        - ความจำเป็นเพื่อปฏิบัติตามกฎหมาย
        - เพื่อการวิจัยและสถิติ
        - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
    - ข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว
        - การขอความยินยอมโดยชัดแจ้ง
        - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล
        - เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิ สมาคม หรือองค์กรไม่แสวงหากำไรนั้น
        - เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล
        - ความจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
        - ความจำเป็นเพื่อปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์ตามที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลระบุไว้

- หากหน่วยงานเลือกใช้วิธีการขอความยินยอม จะต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น และจะต้องขอความยินยอมก่อนที่จะมีการประมวลผลเกิดขึ้น
- หากมีการเปลี่ยนแปลงวัตถุประสงค์ที่ใช้ฐานการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องขอความยินยอมใหม่ทุกครั้ง
- หน่วยงานจะต้องมีการคำนึงถึงการเก็บหลักฐานของการขอความยินยอมไว้อย่างเหมาะสม
- การเปิดเผยข้อมูลจะต้องเป็นไปตามแนวทางและกระบวนการเปิดเผยข้อมูลที่บริษัทกำหนดไว้

4.4 การโอนข้อมูลส่วนบุคคล (Personal Data Transfer)

- การถ่ายโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะต้องคำนึงถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ และเป็นไปตามหลักเกณฑ์ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- ห้ามโอนถ่ายข้อมูลส่วนบุคคลให้กับผู้นำเข้าข้อมูลที่อยู่นอกประเทศ เว้นแต่
    - บริษัทและผู้นำเข้าข้อมูลได้ตกลงกันเป็นลายลักษณ์อักษรเพื่อให้สัญญาเกี่ยวกับเจ้าของข้อมูลสมบูรณ์
    - เป็นการกระทำตามสัญญาเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
    - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล
    - เมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลทราบในกรณีที่มาตรการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางไม่เพียงพอ
- การโอนถ่ายและการประมวลผลข้อมูลต้องดำเนินการด้วยวิธีที่ปลอดภัย และเป็นไปตามมาตรฐานความปลอดภัยขั้นต่ำของบริษัทพร้อมทั้งสอดคล้องกับนโยบายและกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ

4.5 การควบคุมหน่วยงานภายนอกที่มีการประมวลผลข้อมูลส่วนบุคคล (Controlling Other Parties Involving the Processing of Personal Data)

- สายงานที่เกี่ยวข้องจะต้องมีการระบุรายละเอียดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในสัญญาระหว่างบริษัทและหน่วยงานภายนอก โดยจะต้องครอบคลุมเนื้อหาดังต่อไปนี้
    - ข้อตกลงการไม่เปิดเผยความลับของข้อมูล
    - รายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
    - สิทธิของบริษัทในการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานภายนอก
    - มาตรการการลบ ทำลาย หรือส่งคืนข้อมูลเมื่อสิ้นสุดระยะเวลาการประมวลผลข้อมูล
    - การแจ้งต่อบริษัทเมื่อเกิดเหตุการละเมิดข้อมูลส่วนบุคคล

4.6 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO)

- บริษัทจะต้องมีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเป็นทางการ โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่
    - ให้คำแนะนำแก่ผู้ที่เกี่ยวข้องทั้งภายในบริษัทและภายนอกบริษัทในการประมวลผลข้อมูลส่วนบุคคล
    - ตรวจสอบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องทั้งภายในบริษัทและภายนอกบริษัท
    - ประสานงานและให้ความร่วมมือกับบริษัทคุ้มครองข้อมูลส่วนบุคคล
    - ให้คำแนะนำในการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล
    - รายงานผลการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้กับผู้บริหารสูงสุดของบริษัท
- แจ้งรายชื่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้หน่วยงานกำกับดูแลเรื่องคุ้มครองข้อมูลส่วนบุคคลทราบตามที่กฎหมายกำหนด หรือเมื่อมีการเปลี่ยนแปลง

4.7 การออกแบบโดยคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล (Privacy by Design)

- บริษัทจะต้องคำนึงถึงการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนของการออกแบบผลิตภัณฑ์หรือบริการ โดยคำนึงถึงหลักการดังต่อไปนี้
    - การจัดเก็บข้อมูลอย่างจำกัด
    - การประมวลผลข้อมูลอย่างจำกัด
    - ความถูกต้อง และคุณภาพของข้อมูลส่วนบุคคล
    - การระบุวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลขั้นต่ำ
    - การลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
    - การจัดการทำข้อมูลที่ถูกจัดเก็บไว้ชั่วคราวในระหว่างการประมวลผล
    - ระยะเวลาการจัดเก็บข้อมูล
    - มาตรการในการแลกเปลี่ยนข้อมูล

4.8 การวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

- สายงานที่เกี่ยวข้องจะต้องเป็นผู้จัดทำขั้นตอนปฏิบัติในการวิเคราะห์ผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment Procedure) และมีการทบทวนขั้นตอนปฏิบัติอย่างสม่ำเสมอ
- สายงานที่เกี่ยวข้องจะต้องเป็นผู้จัดทำและทบทวนการประเมินผลกระทบของข้อมูลส่วนบุคคล (Data Protection Impact Assessment) ร่วมกับ DPO ก่อนริเริ่มดำเนินกิจกรรม โครงการ หรือการกระทำอื่น ๆ ที่อาจก่อให้เกิดผลกระทบต่อการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

4.9 ความปลอดภัยของข้อมูล (Data Security)

- ควรเก็บข้อมูลเป็นความลับและเปิดเผยต่อบุคลากรที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมายและกฎเกณฑ์ที่บังคับใช้เท่านั้น
- มีการกำหนดหลักเกณฑ์ดูแลและเก็บรักษาข้อมูล ทั้งที่อยู่ในรูปแบบเอกสารกระดาษ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ และสื่อบันทึกข้อมูลไว้อย่างปลอดภัย ป้องกันการสูญหาย และพร้อมใช้งาน
- มีการจัดชั้นความลับของข้อมูล เก็บรักษาและทำลายข้อมูลให้เหมาะสมกับชั้นความลับ และมีการบริหารจัดการการเข้ารหัสข้อมูลที่เชื่อถือได้และเป็นมาตรฐานสากล
- มีการกำหนดหลักเกณฑ์เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข และเปิดเผยข้อมูล โดยผู้ที่มีอำนาจและได้รับมอบหมาย รวมทั้งสายงานที่เกี่ยวข้องต้องร่วมดำเนินการให้มีการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น
- การขอสิทธิเพื่อเข้าถึงข้อมูลนอกเหนือจากที่กำหนดไว้จะต้องผ่านการพิจารณาจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือเจ้าของข้อมูล
- การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศและกระบวนการความมั่นคงปลอดภัยด้านสารสนเทศ
- กำหนดหลักเกณฑ์ให้มีการทบทวนสิทธิแก่พนักงานที่มีหน้าที่เกี่ยวข้องเข้าถึงข้อมูลเท่าที่จำเป็นและควบคุมการเข้าถึงระบบงาน และบริหารจัดการสิทธิของพนักงานให้เป็นปัจจุบัน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งหรือการจ้างงาน
- หากมีการจ้างผู้ให้บริการภายนอกหรือพันธมิตรซึ่งต้องมีการจัดเก็บและรวบรวมข้อมูลส่วนบุคคลจะต้องมีการกำหนดหลักเกณฑ์เพื่อควบคุมและบริหารจัดการ การเข้าถึง การใช้ และการดูแลรักษาข้อมูล รวมถึงกระบวนการทำลาย หรือลบข้อมูล ตามมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ
- มีการออกแบบ พัฒนา และทดสอบระบบงานให้มีความมั่นคงปลอดภัย มีความยืดหยุ่น และมีการบำรุงรักษาสม่ำเสมอ)

4.10 การละเมิดข้อมูลส่วนบุคคล (Personal Data Breaches)

- บริษัทจะต้องกำหนดแนวทางปฏิบัติเกี่ยวกับการจัดการกับเหตุการละเมิดข้อมูลส่วนบุคคล หลักเกณฑ์ในการแยกประเภทเหตุการณ์ ระดับความเสี่ยงและผลกระทบ ตลอดจนการดำเนินการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- หากบุคคลใดทราบถึงการละเมิดข้อมูลส่วนบุคคลของบริษัทบุคคลนั้นจะต้องรายงานเหตุการณ์ที่เกิดขึ้นแก่ DPO โดยทันที ทั้งนี้ การรายงานดังกล่าวจะถูกเก็บเป็นความลับ เมื่อมีการแจ้งการละเมิดความปลอดภัย ทีมตอบสนองต่อเหตุการณ์และสายงานที่เกี่ยวข้องจะดำเนินการตรวจสอบข้อเท็จจริงที่เกี่ยวข้องกับเหตุการณ์ร่วมกับ DPO พร้อมเสนอแนวทางแก้ไขที่เหมาะสมแก่คณะบริหารของบริษัท

4.11 มาตรการความมั่นคงปลอดภัยในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทให้ความสำคัญกับความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้าอย่างเคร่งครัด และบริษัทมีมาตรการรักษาความปลอดภัย รวมถึงมีระบบเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ปลอดภัยและเหมาะสม เพื่อป้องกันไม่ให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลสูญหาย ถูกใช้ เข้าถึง เปลี่ยนแปลง หรือเปิดเผย โดยไม่ได้รับอนุญาต บริษัทจำกัดการเข้าถึงข้อมูลส่วนบุคคลสำหรับพนักงาน ตัวแทน ผู้รับจ้างและบุคคลภายนอกที่มีความจำเป็นต้องได้รับข้อมูลและพวกเขาจะประมวลผลข้อมูลส่วนบุคคลของลูกค้าภายใต้เงื่อนไขที่บริษัทกำหนดเท่านั้น

บริษัทจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการ มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล เพื่อธำรงไว้ซึ่งความลับ, ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล อันประกอบไปด้วยการดำเนินการดังต่อไปนี้ เป็นอย่างน้อย

1. การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
2. การกำหนดเกี่ยวกับการอนุญาตหรือกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
3. การบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
5. การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

อนึ่ง บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งแก่ผู้เป็นเจ้าของข้อมูลส่วนบุคคลและให้เป็นไปตามที่กฎหมายกำหนด และในกรณีที่บริษัทจะว่าจ้างบริษัทบุคคลภายนอก ให้ดำเนินการเกี่ยวกับข้อมูล

ส่วนบุคคลของลูกค้า บริษัทจะคัดเลือกบริษัทที่มีระบบการคุ้มครองข้อมูลที่ได้มาตรฐานและจัดทำข้อตกลงที่เกี่ยวกับการเก็บรักษาข้อมูลส่วนบุคคลให้เป็นไปตามนโยบายเช่นเดียวกัน

4.12 นโยบายการจัดเก็บข้อมูลส่วนบุคคล

วัตถุประสงค์ของนโยบายนี้คือเพื่อกำหนดวิธีการจัดเก็บเอกสารที่มีข้อมูลส่วนบุคคล เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลภายในบริษัท เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงการกำหนดระยะเวลาจัดเก็บเอกสารที่มีข้อมูลส่วนบุคคล โดยคำว่า "เอกสาร" ที่ใช้ในนโยบายนี้รวมถึงสำเนาของเอกสาร (เช่น กระดาษ) สำเนาของเอกสารในรูปแบบไฟล์อิเล็กทรอนิกส์ (เช่น รูปภาพ รายละเอียดเอกสารที่สแกนจากกระดาษ) ข้อมูลที่ได้รับจากการเข้าเว็บไซต์ของบริษัทและข้อมูลที่ได้รับจากบุคคลที่สาม (เช่น ผลการตรวจสอบ)

1.สถานที่จัดเก็บข้อมูล

เอกสารในรูปแบบอิเล็กทรอนิกส์, จดหมายอิเล็กทรอนิกส์ (อีเมล) และ บันทึกมัลติมีเดีย (Multimedia)

เอกสารในรูปแบบอิเล็กทรอนิกส์ อีเมล และบันทึกมัลติมีเดียทั้งหมดจะต้องจัดเก็บภายในสถานที่ที่เหมาะสม เพื่อให้แน่ใจว่าสามารถใช้มาตรการรักษาความปลอดภัยที่เป็นไปตามมาตรฐานที่กำหนดโดยกฎหมาย

เอกสารในรูปแบบกระดาษ

การจัดเก็บเอกสารในรูปแบบกระดาษที่จำเป็นสำหรับการดำเนินธุรกิจในแต่ละวัน ต้องเก็บไว้ในตู้เก็บเอกสารและลิ้นชักโต๊ะทำงานเมื่อไม่ได้ใช้งาน และพนักงานจะต้องล็อคกุญแจตู้เก็บเอกสารและลิ้นชักที่จัดเก็บเอกสารที่มีข้อมูลส่วนบุคคลเมื่อสิ้นวันทำการ

2. การปกป้องเอกสาร

บริษัทมุ่งมั่นที่จะป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยเอกสารที่มีข้อมูลส่วนบุคคลซึ่งอยู่ในการควบคุมของบริษัทโดยมิชอบหรือโดยปราศจากอำนาจ เอกสารทั้งในรูปแบบกระดาษและรูปแบบอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลจะถูกเก็บไว้ในที่ปลอดภัยจนกว่าจะถูกทำลาย บริษัทจะใช้เทคโนโลยีและกระบวนการต่าง ๆ ที่ได้รับการตรวจสอบอย่างสม่ำเสมอเพื่อรักษาความปลอดภัยของข้อมูลส่วนบุคคล

3. การทำลายเอกสาร

เมื่อพ้นกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลหรือหมดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลแล้ว เอกสารในรูปแบบประเภทกระดาษที่มีข้อมูลส่วนบุคคลจะถูกทำลายโดยการย่อยเอกสาร โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว ส่วนข้อมูลส่วนบุคคลที่จัดเก็บทางอิเล็กทรอนิกส์จะถูกลบออกจากสื่อที่ใช้เก็บข้อมูล เช่น ฮาร์ดดิสก์จะถูกทำลาย หรือ ถูกลบข้อมูลโดยวิธีที่ไม่สามารถกู้คืนข้อมูลได้ โดยผู้ที่ได้รับมอบหมายให้ดำเนินการดังกล่าว

4. การเก็บรักษาและระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทต้องมีการกำหนดระยะเวลาการจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้เป็นไปตามวัตถุประสงค์ในการเก็บรวบรวมสำหรับการประมวลผลข้อมูลส่วนบุคคลอย่างชัดเจน โดยอาจเป็นไปตามระยะเวลาที่กำหนดตามกฎหมาย แนวปฏิบัติของธุรกิจ หรือมาตรฐานของการประมวลผล <u>สำหรับระยะเวลาในการเก็บรักษาข้อมูลทั้งหมดสามารถตรวจสอบได้จากเอกสารแนบ</u>

บริษัทต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ตามนโยบายในการลบหรือทำลายข้อมูลส่วนบุคคล (Personal Data Disposal Policy)

4.13 นโยบายในการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนด (Personal Data Disposal Policy)

บริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล จึงกำหนดให้มีการลบ ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของเจ้าของข้อมูลส่วนบุคคลได้ เมื่อพ้นกำหนดระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคลตามนโยบายในการจัดเก็บข้อมูลส่วนบุคคล หรือเมื่อมีการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อมีเหตุอื่นตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม และสอดคล้องกับการรักษาความลับของข้อมูลส่วนบุคคล ทั้งนี้เพื่อป้องกันการสูญหาย การเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีสิทธิหรือโดยไม่ชอบด้วยกฎหมาย รวมถึงควบคุมให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการตามที่กำหนดในนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของบริษัทโดยอ้างอิงตามการแบ่งระดับชั้นความลับของข้อมูล

1. การแบ่งชั้นความลับของข้อมูล

1. ทั่วไป (Public) คือ ข้อมูลสารสนเทศที่ไม่ได้กระทบอย่างมีนัยสำคัญต่อการดำเนินงาน และผู้บริหารอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดีข้อมูลสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้กับลูกค้ารวมทั้งรักษาภาพลักษณ์และชื่อเสียง ตัวอย่างข้อมูลทั่วไป เช่น แผ่นพับประชาสัมพันธ์ด้านการตลาด ข่าวประชาสัมพันธ์ ข่าวประกาศผู้ถือหุ้น
2. ใช้ภายใน (Internal Use Only) คือ ข้อมูลที่เปิดเผยได้เฉพาะภายในบริษัทและบุคคลภายนอกที่มีความสัมพันธ์ทางการค้าซึ่งได้รับสิทธิเท่านั้น ไม่เหมาะที่จะเปิดเผยต่อสาธารณชนเป็นการทั่วไป ตัวอย่างข้อมูลใช้ภายใน เช่น เอกสารภายใน E-mail ภายในบริษัทนโยบาย และมาตรฐาน ของบริษัทสมุดรายชื่อโทรศัพท์ ข้อมูลส่วนบุคคลทั่วไป
3. ความลับ (Confidential) คือ ข้อมูลซึ่งหากเปิดเผยโดยไม่ได้รับอนุญาต จะเป็นการฝ่าฝืนกฎ ข้อบังคับของบริษัท ก่อให้เกิดผลกระทบด้านชื่อเสียง การเงิน เสียเปรียบในการแข่งขันทางการค้าต่อบริษัทผู้ที่สามารถเข้าถึงข้อมูลประเภทนี้ได้จึงถูกจำกัดเพียงพนักงานเป็นรายบุคคล กลุ่มพนักงานหรือบุคคลที่ 3 ที่มีความสัมพันธ์กันตามสัญญา โดยกลุ่มคนที่ระบุจำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) ในนามรายบุคคล หรือบริษัทต้นสังกัด หรือในกรณีที่เป็นบริษัทในเครือ อาจจัดทำเป็นข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือ ข้อตกลงในการรักษาความลับระหว่างหน่วยงาน ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย ตัวอย่างข้อมูลความลับ เช่น รหัสผ่าน คีย์การเข้ารหัส ข้อมูลทางการเงิน ข้อมูลงบประมาณ ข้อมูลลูกค้า

ข้อมูลที่เกี่ยวข้องกับระบบความปลอดภัย ข้อมูลจำลองลายนิ้วมือ ข้อมูลเงินเดือน ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ข้อมูลพันธุกรรม ข้อมูลสุขภาพ เป็นต้น

4. ความลับที่สุด (Top Secret) คือ เป็นข้อมูลที่มีการประเมินแล้วว่า หากมีการเปิดเผยโดยไม่ได้รับอนุญาตจะสามารถสร้างความเสียหายทั้งในรูปการเงินและที่ไม่ใช่การเงินต่อบริษัทอย่างร้ายแรง ข้อมูลที่จัดอยู่ในกลุ่มนี้จะต้องได้รับการดูแลเป็นพิเศษ ทั้งจากผู้เป็นเจ้าของ และผู้ที่จำเป็นต้องใช้ตามหน้าที่ของงานที่รับผิดชอบ ทุกคนที่สามารถเข้าถึงข้อมูลเหล่านี้จำเป็นต้องลงนามข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือในกรณีที่เป็นบริษัทในเครือ อาจจัดทำเป็นข้อตกลงไม่เปิดเผยข้อมูล (NDA) หรือ ข้อตกลงในการรักษาความลับระหว่างหน่วยงาน ซึ่งต้องได้รับการอนุมัติจากผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายทั้งสองฝ่าย ตัวอย่างข้อมูลความลับที่สุด เช่น แผนกลยุทธ์ทางธุรกิจ (ก่อนประกาศอย่างเป็นทางการ)

2. วิธีการลบ/ทำลายเอกสาร

บริษัทมีการเก็บรักษาข้อมูลส่วนบุคคลที่เป็นกระดาษซึ่งต้องมีการตรวจสอบแนวทางการทำลายด้วยวิธีที่มีความมั่นคงปลอดภัย เพื่อให้เป็นไปตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับ การทำป้ายแสดงระดับชั้นความลับและการจัดการข้อมูลส่วนบุคคล โดยมีรายละเอียดดังนี้

1. ทั่วไป (Public) ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร
2. ใช้ภายใน (Internal Use Only) ฉีกทำลาย หรือใช้เครื่องย่อยเอกสาร หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร
3. ความลับ (Confidential) ต้องใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) หรือส่งให้หน่วยงานภายนอกที่มีสัญญาในการทำลายเอกสาร
4. ความลับที่สุด (Top Secret) ต้องส่งเอกสารคืนกลับให้เจ้าของเอกสารเพื่อทำการทำลาย หรือใช้เครื่องย่อยเอกสารที่ไม่สามารถนำกลับมาใช้ใหม่ได้ (Cross-cut Shredder) เท่านั้น

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

3. วิธีการลบ/ทำลายด้วยวิธีอิเล็กทรอนิกส์

บริษัทมีการเก็บรักษาข้อมูลส่วนบุคคลที่เป็นอิเล็กทรอนิกส์ซึ่งต้องมีการตรวจสอบแนวทางการทำลายด้วยวิธีที่มีความมั่นคงปลอดภัย เพื่อให้เป็นไปตามขั้นตอนปฏิบัติการจัดระดับชั้นความลับ การทำป้ายแสดงระดับชั้นความลับและการจัดการข้อมูล โดยมีรายละเอียดดังนี้

1. ทั่วไป (Public) ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser
2. ใช้ภายใน (Internal Use Only) ต้องดำเนินการลบข้อมูลด้วยการลบข้อมูลและ Clear ข้อมูลใน Recycle Bin หรือใช้โปรแกรมในการลบข้อมูล เช่น Eraser

3. ความลับ (Confidential) ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes
4. ความลับที่สุด (Top Secret) ต้องดำเนินการลบข้อมูลด้วยการ Format แบบ Low Level หรือใช้โปรแกรมในการลบข้อมูลที่ไม่สามารถกู้คืนกลับมาได้ เช่น Eraser แบบ 3 Passes

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการลบหรือทำลายข้อมูลส่วนบุคคลเพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

4. วิธีการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

ในกรณีที่ไม่สามารถลบ/ทำลายข้อมูลส่วนบุคคลได้โดยตรง เนื่องจากอาจส่งผลกระทบต่อความถูกต้องในการปฏิบัติงาน เช่น อาจส่งผลให้การทำงานของฐานข้อมูลไม่ถูกต้อง หรือเป็นข้อจำกัดของระบบ บริษัทอาจใช้วิธีการจัดทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลเจ้าของข้อมูลส่วนบุคคลได้ ดังนี้

1. การเปลี่ยนแปลงส่วนใดส่วนหนึ่งของข้อมูลโดยการใช้กลุ่มของตัวอักษรที่ได้จากการสุ่ม หรือการทำให้เป็นข้อมูลอื่น ๆ หรือการใช้กระบวนการอื่นใดที่ได้รับการรับรองเป็นมาตรฐานในปัจจุบัน เช่น การใช้ Hash Function เพื่อเปลี่ยนข้อมูลเดิมให้ไม่สามารถที่จะให้ข้อมูลย้อนกลับมาระบุตัวตนของเจ้าของข้อมูลได้
2. การลดความชัดเจนของข้อมูล (Blurring or Noising) โดยการใช้ข้อมูลโดยประมาณแทนที่ข้อมูลเดิมเพื่อลดความเฉพาะเจาะจงของข้อมูลลง

ทั้งนี้ หลักเกณฑ์ดังกล่าวอาจมีการเปลี่ยนแปลงเมื่อมีกฎเกณฑ์เกี่ยวกับการทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลส่วนบุคคลที่ไม่สามารถระบุตัวตนได้ เพิ่มเติมตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภายหลัง

5. กระบวนการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

บริษัทจะดำเนินการลบข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ตามประเภทของข้อมูลส่วนบุคคลเมื่อมีกรณีดังต่อไปนี้

1. ครบกำหนดระยะเวลาการจัดเก็บตามที่กำหนดไว้นโยบายในการจัดเก็บข้อมูลส่วนบุคคล (Data Retention Policy)
2. ข้อมูลส่วนบุคคลนั้นไม่มีความเกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น
3. ข้อมูลส่วนบุคคลได้ถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบด้วยกฎหมาย
4. เจ้าของข้อมูลส่วนบุคคลร้องขอการใช้สิทธิตามสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคลที่มีการระบุไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล หรือเมื่อเจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

ทั้งนี้ บริษัทสามารถปฏิเสธคำร้องขอของเจ้าของข้อมูลส่วนบุคคลได้ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ดังนี้

1. มีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล

2. การประมวลผลเป็นไปตามวัตถุประสงค์ในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย ซึ่งในกรณีดังกล่าว บริษัทจะจัดให้มีมาตรการป้องกันที่เหมาะสม เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
3. เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของบริษัทหรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่บริษัท
4. เป็นการจำเป็นในการปฏิบัติตามกฎหมายของบริษัทเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
    (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์
    (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ
5. การเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

ทั้งนี้ หากมีการขอให้ลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลที่เป็นเจ้าของข้อมูลได้ บริษัทจะดำเนินการตามกระบวนการ ดังนี้

1. เมื่อได้รับแบบคำร้องขอใช้สิทธิในการลบหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ข้อมูลจะถูกส่งต่อไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและทำการบันทึกไว้ในระบบ
2. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกับฝ่ายกฎหมายและบริหารความเสี่ยงดำเนินการตรวจสอบข้อมูลส่วนบุคคลทั้งหมดที่เกี่ยวข้อง เพื่อหาความจำเป็นขั้นพื้นฐานทางกฎหมายและวัตถุประสงค์เดิม
3. ตรวจสอบแบบคำร้องขอใช้สิทธิในการลบข้อมูลส่วนบุคคลหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ เพื่อให้แน่ใจว่าการขอลบข้อมูลนั้นจะไม่เกี่ยวกับวัตถุประสงค์ในการเก็บรวบรวม หรือการประมวลผลอย่างอื่น
4. ดำเนินการลบ/ทำลายข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ รวมถึงตรวจสอบเพื่อให้แน่ใจว่ามีการลบ/ทำลายข้อมูลส่วนบุคคลออกจากระบบหรือเอกสารที่ใช้งานอยู่ รวมถึงในระบบสำรอง หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตน

เจ้าของข้อมูลส่วนบุคคลได้ หากมีการปฏิเสธสิทธิของเจ้าของข้อมูลส่วนบุคคลในการลบข้อมูลส่วนบุคคล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวตนเจ้าของข้อมูลส่วนบุคคลได้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและทำการบันทึกไว้ในระบบ และแจ้งเจ้าของข้อมูลส่วนบุคคล

4.14 นโยบายหรือแนวทางในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

วัตถุประสงค์ของนโยบายนี้เพื่อการกำหนดแนวทางการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล ที่บริษัทมีการเก็บรวบรวม ใช้ และเปิดเผยไปยังบุคคลอื่น ครอบคลุมทั้งข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ พนักงาน เจ้าหน้าที่ และพันธมิตรของบริษัทให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. **แนวปฏิบัติ**

แนวปฏิบัติการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

1) หน่วยงานของบริษัทที่มีการเปิดเผยข้อมูลส่วนบุคคลให้กับ คู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก จะต้องมีการทำสัญญาระหว่างบริษัท และคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก รายนั้น โดยสัญญาจะต้องเป็นไปตามรูปแบบที่ฝ่ายกฎหมายและบริหารความเสี่ยงกำหนดไว้
2) เนื้อหาของสัญญาระหว่างบริษัท และคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอกจะต้องมีการกำหนดมาตรการเกี่ยวกับ
    - หน้าที่ในการประมวลผลข้อมูล โดยต้องมีข้อความเกี่ยวกับ
        - คำสั่งในการประมวลผลข้อมูลส่วนบุคคล และไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลนอกเหนือไปจากคำสั่งเป็นลายลักษณ์อักษรของผู้ควบคุมข้อมูลส่วนบุคคล
        - การให้การรับรองจากผู้ประมวลผลข้อมูลส่วนบุคคลว่าคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล เป็นคำสั่งที่ไม่เกินวัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
        - ผู้ประมวลผลข้อมูลส่วนบุคคลมีการจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลให้กับบุคคลที่ได้รับมอบหมาย โดยมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายในวัตถุประสงค์ของสัญญา
        - ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ในการรักษาความลับของข้อมูลส่วนบุคคลที่ประมวลผล รวมถึงมีมาตรการที่ทำให้มั่นใจว่าบุคคลที่ได้รับสิทธิเข้าถึงข้อมูลส่วนบุคคลได้ให้คำมั่นสัญญาหรือมีหน้าที่ตามสัญญาในการรักษาความลับของข้อมูลส่วนบุคคล
        - ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องจัดข้อมูลที่จำเป็นต่อการแสดงให้เป็นที่พอใจถึงการปฏิบัติตามหน้าที่ตามสัญญารวมถึงยินยอมและให้ความร่วมมือในการตรวจสอบและสอบสวนโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ตรวจสอบซึ่งผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย
    - มาตรการในการรักษาความมั่นคงปลอดภัย โดยต้องมีข้อความเกี่ยวกับ

- ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลในการจัดหามาตรการการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อเป็นการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูลส่วนบุคคล โดยต้องมีมาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard) มาตรการป้องกันด้านเทคนิค (technical safeguard) และมาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องเข้าถึงควบคุมการใช้งานข้อมูลส่วนบุคคล (access control) โดยอย่างน้อยต้องประกอบด้วยการดำเนินการดังนี้
    - การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
    - การกำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
    - การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว
    - การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
    - การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

- หน้าที่ในการดำเนินกิจกรรมที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล
    - หน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลในการสนับสนุนการผู้ควบคุมข้อมูลส่วนบุคคลในเรื่องการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
    - การแจ้งต่อผู้ควบคุมข้อมูลส่วนบุคคลในกรณีที่มีคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- การแจ้งเตือนหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ
    - การแจ้งผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้า หากทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การเก็บรักษาข้อมูลส่วนบุคคล และการลบข้อมูลส่วนบุคคล โดยต้องมีข้อความเกี่ยวกับ
    - หน้าที่และระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเท่าที่จำเป็น เพื่อการปฏิบัติหน้าที่ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล
    - วิธีในการลบ ทำลาย ส่งคืน หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้
    - การเก็บข้อมูลส่วนบุคคลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย
- การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยต้องมีข้อความเกี่ยวกับ
    - การไม่อนุญาตให้ผู้ประมวลผลข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ เว้นแต่จะได้รับอนุมัติจากบริษัท

- การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ จะต้องเป็นไปตามเงื่อนไขที่กำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคล และประกาศที่เกี่ยวข้อง

4.15 นโยบายการแยกประเภทของข้อมูลส่วนบุคคล

1. นโยบายการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล (Personal Data Classification Policy)

1.1 บริษัทมีการกำหนดชั้นความลับของสารสนเทศไว้ 4 ระดับ ได้แก่ ข้อมูลทั่วไป (Public Data) ข้อมูลใช้ภายใน (Internal Use Only Data) ข้อมูลความลับ (Confidential Data) ข้อมูลความลับที่สุด (Top Secret Data) โดยมีการกำหนดนิยาม รวมทั้งแนวทางในการดำเนินการในเอกสารขั้นตอนการปฏิบัติงานสำหรับการแบ่งชั้นของข้อมูลส่วนบุคคล (Personal Data Classification Procedure) ผู้ที่เกี่ยวข้องจะต้องปฏิบัติตามโดยเคร่งครัด หากกลุ่มของสารสนเทศประกอบไปด้วยสารสนเทศหลายระดับชั้นความลับ ให้เจ้าของสารสนเทศกำหนดระดับชั้นความลับของสารสนเทศนั้นตามระดับชั้นความลับของสารสนเทศระดับสูงสุดของกลุ่มสารสนเทศ

1.2 การจัดระดับชั้นความลับของข้อมูลส่วนบุคคลต้องมีการจัดระดับชั้นของข้อมูลและการกำหนดความเสี่ยงของข้อมูลส่วนบุคคลเพื่อกำหนดชั้นความลับของข้อมูลตามขั้นตอนการปฏิบัติงานสำหรับการจัดระดับชั้นของข้อมูลส่วนบุคคล (Personal Data Classification Procedure)

1.3 เจ้าของสารสนเทศมีหน้าที่กำหนดและทบทวนระดับชั้นความลับของข้อมูลส่วนบุคคล ที่อยู่ภายใต้ความรับผิดชอบในของตนอย่างสม่ำเสมอ รวมทั้งจัดให้มีการควบคุมที่เหมาะสมกับระดับชั้นความลับของข้อมูล

1.4 เจ้าของสารสนเทศควรเก็บข้อมูลส่วนบุคคลเป็นความลับและเปิดเผยต่อบุคคลที่ได้รับอนุญาตตามข้อกำหนดทางกฎหมายและกฎเกณฑ์ที่บังคับใช้เท่านั้น

1.5 หน่วยงานที่เกี่ยวข้อง ต้องร่วมดำเนินการให้มีมาตรการควบคุมการเข้าถึงข้อมูลอย่างเหมาะสม เพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลเท่าที่จำเป็น และได้รับอนุญาตให้เข้าถึงข้อมูลที่ถูกต้องในเวลาที่เหมาะสมเท่านั้น

1.6 การขอสิทธิเพื่อเข้าถึงข้อมูลส่วนบุคคลนอกเหนือจากสิทธิที่กำหนดไว้จะต้องผ่านการพิจารณาจากเจ้าของสารสนเทศ

1.7 การดำเนินการทางเทคนิคในการให้สิทธิเข้าถึงข้อมูลต้องเป็นไปตามมาตรการการรักษาความมั่นคงปลอดภัยสารสนเทศที่บริษัทกำหนด

1.8 ในการเก็บรักษาข้อมูลส่วนบุคคลต้องเก็บรักษาตามระยะเวลาเท่าที่จำเป็นเท่านั้น เพื่อให้เป็นไปตามวัตถุประสงค์ในการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และต้องมีการลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้เมื่อไม่ได้ใช้ข้อมูลส่วนบุคคลนั้นตามวัตถุประสงค์

1.9 หากมีการว่าจ้างผู้ให้บริการภายนอกที่ต้องมีการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล จะต้องมีการปฏิบัติตามนโยบายในการทำข้อตกลงหรือสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Outsourcing Policy for Personal Data Processing) ซึ่งต้องมีการจัดระดับชั้นความลับของข้อมูลส่วนบุคคลโดยเจ้าของสารสนเทศที่ได้ทำการว่าจ้างผู้ให้บริการภายนอกนั้น ๆ

ภาคผนวก ก. ตัวอย่างการจัดระดับชั้นความลับของข้อมูลส่วนบุคคล

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use Only)
ข้อมูลที่ใช้ในการ	รหัสผ่าน	✓	
พิสูจน์หรือยืนยัน	คีย์การเข้ารหัสข้อมูล (Encryption keys)	✓	
ตัวตน	ข้อมูลชีวภาพ เช่น ข้อมูลภาพจำลองใบหน้า (Face recognition) ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ	✓	
	บันทึกกิจกรรมการเข้าถึงระบบ (Authentication logs)	✓	
ข้อมูลบัตร	ชื่อผู้ถือบัตรอิเล็กทรอนิกส์	✓	
อิเล็กทรอนิกส์ (เช่น	เลขบัตรอิเล็กทรอนิกส์	✓	
บัตรเดบิต บัตร	PIN, PIN block	✓	
เครดิต เป็นต้น)	CVV, CVV2, CVC2, CID	✓	
	ข้อมูลบัตรบนแถบแม่เหล็ก	✓	
ข้อมูลที่สามารถระบุ	ชื่อ นามสกุล		✓
ตัวบุคคลได้	เลขบัตรประชาชน		✓
(Personally	เลขหนังสือเดินทาง		✓
Identifiable	เลขบัตรประกันสังคม		✓
Information (PII))	เลขใบอนุญาตขับขี่		✓
	เลขประจำตัวผู้เสียภาษี		✓
	รหัสพนักงาน		✓
	เลขบัญชีธนาคาร		✓
	เลขที่กรมธรรม์		✓
	วันเดือนปีเกิด		✓
	อายุ		✓
	เพศ		✓
	ที่อยู่		✓
	เบอร์โทรศัพท์		✓
	อีเมล		✓
	ข้อมูลเงินเดือน	✓	

ประเภทของข้อมูล	รายละเอียด	ความลับ (Confidential)	ใช้ภายใน (Internal Use Only)
	ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID		✓
	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	✓	

4.16 นโยบายการส่งหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก หรือการส่งข้อมูลส่วนบุคคลไปยังประเทศอื่น

1. นโยบายการส่งหรือโอนข้อมูลส่วนบุคคลไปยังหน่วยงานภายนอก (Third Parties Policy)

บริษัท จะเปิดเผยข้อมูลส่วนบุคคลให้แก่องค์กรหรือหน่วยงานภายนอก หลังจากวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มีผลใช้บังคับ โดยมีแนวปฏิบัติดังนี้

1) หากจะมีการเปิดเผยข้อมูลส่วนบุคคลให้กับ บริษัทคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก จะสามารถดำเนินการได้เฉพาะในกรณีที่มีการระบุรายชื่อของ บริษัทคู่ค้า พันธมิตรทางธุรกิจ บริษัทย่อย และ/หรือ ผู้ให้บริการภายนอก ในบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Data Inventory) เท่านั้น หากไม่มีการระบุในบันทึกรายการประมวลผลข้อมูลส่วนบุคคล จะต้องขออนุมัติจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก่อนที่จะเปิดเผยข้อมูลส่วนบุคคล โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องพิจารณาฐานในการประมวลผลข้อมูลส่วนบุคคลและเงื่อนไขให้สอดคล้องตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2) สัญญาระหว่างบริษัทและบริษัทคู่ค้า พันธมิตรทางธุรกิจ บริษัทในเครือ และ/หรือ ผู้ให้บริการภายนอก จะต้องมีการกำหนดมาตรการเกี่ยวกับ
    - หน้าที่ในการประมวลผลข้อมูลส่วนบุคคล
    - มาตรการในการรักษาความมั่นคงปลอดภัย
    - การดำเนินกิจกรรมที่เกี่ยวข้องกับสิทธิของเจ้าของข้อมูลส่วนบุคคล
    - การแจ้งเตือนหากมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
    - การเก็บรักษาข้อมูลส่วนบุคคลและการลบข้อมูลส่วนบุคคล
    - การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ
3) กรณีส่งหรือโอนข้อมูลส่วนบุคคลไปยังนิติบุคคล จะต้องพิจารณาว่าในการส่งหรือโอนข้อมูลส่วนบุคคลนั้นมีมาตรการการรักษาความมั่นคงปลอดภัย และมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐาน
4) กรณีที่หน่วยงานรัฐ หรือองค์กรผู้ถืออำนาจรัฐ ร้องขอเข้าถึงข้อมูลส่วนบุคคลโดยการอ้างถึงกฎหมาย ระเบียบ หรือคำสั่งใด ๆ ที่บริษัท จะต้องปฏิบัติตาม ผู้รับผิดชอบจะสามารถให้หน่วยงานเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่มีบทบัญญัติกฎหมาย หรือคำสั่ง หรือหนังสือแจ้งอย่างเป็นทางการ อย่างใดอย่างหนึ่ง เป็นอย่างน้อยตามอำนาจทางกฎหมายเท่านั้น มิเช่นนั้นบริษัท จะมีความผิดตามกฎหมายจากการให้หน่วยงานดังกล่าวเข้าถึงหรือเปิดเผยข้อมูลโดยไม่มีหน้าที่ตามกฎหมาย ยกเว้นกรณีที่เป็นการปฏิบัติหน้าที่ตามกฎหมาย (Legal Obligation) ของบริษัท ที่แม้ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่บริษัท จะต้องกระทำตามหน้าที่อยู่แล้ว

2. นโยบายการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ (Cross Border data Transfer Policy)

เพื่อให้การถ่ายโอนข้อมูลส่วนบุคคลอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล การดำเนินการถ่ายโอนข้อมูลส่วนบุคคลไปประเทศปลายทาง หรือองค์กรระหว่างประเทศจะต้องมีความมั่นคงปลอดภัย โดยบริษัทสามารถพิจารณาทางเลือกดังต่อไปนี้

1) การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทาง หรือองค์กรระหว่างประเทศ โดยบริษัท จะดำเนินการส่งข้อมูลส่วนบุคคลไปยังประเทศที่มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลที่ได้รับการตรวจสอบและรับรองจากบริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
2) มีการจัดทำข้อตกลงระหว่างกันในรูปแบบใดรูปแบบหนึ่งดังต่อไปนี้

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

3) ในกรณีที่ไม่สามารถใช้ทางเลือกการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศในข้อ 1 และ 2 สามารถดำเนินการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศได้ หากเป็นกรณีดังนี้
   - เป็นการปฏิบัติตามกฎหมาย
   - ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว
   - เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น
   - เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
   - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
   - เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล หรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้
4) ในกรณีที่มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางหรือองค์กรระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้นไม่มีมาตรฐานเพียงพอ ให้เสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยเสียก่อน

3. การคุ้มครองข้อมูลส่วนบุคคลของเครือกิจการ (Binding Corporate Rules)

บริษัท สามารถโอนข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน เพื่อการประกอบกิจการหรือธุรกิจร่วมกันได้ หากการส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวเป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน (“สมาชิกเครือกิจการ”) ที่ได้รับการตรวจสอบและรับรองจากหน่วยงานกำกับดูแลที่เกี่ยวข้องแล้ว โดยนโยบายในการคุ้มครองข้อมูลส่วนบุคคลเพื่อการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน หรือ Binding Corporate Rules (BCR) จะต้อง

1) มีผลผูกพันตามกฎหมายและบังคับใช้กับและถูกบังคับใช้โดยสมาชิกเครือกิจการทุกราย รวมถึงลูกจ้างและพนักงานของเครือกิจการ (“สมาชิกเครือกิจการ”)
2) รับรองสิทธิอันสามารถบังคับใช้ได้ของเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลถูกนำมาประมวลผล

3) BCR ประกอบด้วยองค์ประกอบอย่างน้อย ดังต่อไปนี้

3.1 รายละเอียดโครงสร้างและช่องทางการติดต่อของสมาชิกเครือกิจการ

3.2 ข้อมูลส่วนบุคคลที่จะถูกเปิดเผยหรือชุดข้อมูลส่วนบุคคลที่จะถูกเปิดเผย รวมถึงรายละเอียด ประเภทของข้อมูลส่วนบุคคล, วิธีการและวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล, ประเภทของเจ้าของข้อมูลส่วนบุคคล, ประเทศหรือองค์การระหว่างประเทศปลายทางซึ่งรับข้อมูลส่วนบุคคล

3.3 ความมีผลผูกพันทางกฎหมายทั้งภายในและภายนอกกลุ่มสมาชิกเครือกิจการของ BCR

3.4 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 ของพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Processing of Special Categories of Personal Data), มาตรการในการรับประกันความปลอดภัยของข้อมูล และเงื่อนไขในการเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลภายนอกที่ไม่ใช่สมาชิกเครือกิจการ (Requirements in Respect of Onward Transfers to Bodies not Bound by the Binding Corporate Rules)

3.5 สิทธิของเจ้าของข้อมูลส่วนบุคคลอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล และช่องทางในการใช้สิทธินั้น รวมถึงสิทธิที่จะร้องเรียนต่อบริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการฟ้องร้องคดีต่อศาลที่มีอำนาจ สิทธิในการได้รับการเยียวยา และสิทธิในการได้รับค่าเสียหายอันเกิดจากการละเมิด BCR

3.6 ความยินยอมรับผิดโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นสมาชิกเครือกิจการซึ่งตั้งอยู่ในประเทศไทย ในกรณีที่เกิดเหตุละเมิด BCR โดยสมาชิกเครือกิจการซึ่งไม่ได้ตั้งอยู่ในประเทศไทย ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะไม่ต้องรับผิดบางส่วนหรือทั้งหมด หากพิสูจน์ได้ว่าสมาชิกเครือกิจการมิได้มีส่วนรับผิดชอบกับเหตุการณ์ที่ก่อให้เกิดความเสียหาย

3.7 การแจ้งเนื้อหาของ BCR (โดยเฉพาะข้อ 3.4 - ข้อ 3.6) ให้แก่เจ้าของข้อมูลส่วนบุคคลรับทราบเพิ่มเติมจากการแจ้งรายละเอียดตามมาตรา 23 และมาตรา 25 ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

3.8 หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือ Data Protection Officer (DPO) ที่ได้รับมอบหมายตามมาตรา 41 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือบุคคล/นิติบุคคลที่ได้รับมอบหมายให้ตรวจสอบการดำเนินการตาม BCR ของสมาชิกเครือกิจการ, การฝึกอบรม, การรับเรื่องร้องเรียน

3.9 กระบวนการรับเรื่องร้องเรียน

3.10กลไกภายในกลุ่มสมาชิกเครือกิจการสำหรับการรับประกันการดำเนินการตาม BCR ซึ่งต้องมีองค์ประกอบอย่างน้อยดังนี้ การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Audit) และ

วิธีการในการรับประกันการดำเนินการเชิงแก้ไขเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยบุคคลที่ได้รับมอบหมายตามข้อ 3.8 (DPO) และคณะกรรมการกลุ่มสมาชิกเครือกิจการจะต้องรับทราบผลการตรวจสอบข้างต้น รวมถึงจัดเตรียมให้บริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบผลการตรวจสอบข้างต้นได้

3.11กลไกการรายงานและบันทึกการเปลี่ยนแปลงเนื้อหาของ BCR และการรายงานการเปลี่ยนแปลงดังกล่าวไปยังบริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3.12กลไกการให้ความร่วมมือกับบริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการรับประกันการดำเนินการตาม BCR ของสมาชิกเครือกิจการ เช่น การจัดเตรียมผลการตรวจสอบให้บริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้

3.13กลไกในการรายงานไปยังบริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลซึ่งข้อบังคับทางกฎหมายที่สมาชิกเครือกิจการที่ตั้งอยู่ในประเทศปลายทางต้องปฏิบัติตามอันอาจก่อให้เกิดผลกระทบอย่างมีนัยสำคัญต่อหลักประกันที่ได้ให้ไว้ตาม BCR

3.14จัดการฝึกอบรมการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสม ให้แก่พนักงานหรือบุคคลที่เข้าถึงข้อมูลส่วนบุคคลเป็นประจำหรือตลอดเวลา

4) นอกเหนือจาก BRC แล้ว บริษัทอาจยอมรับให้มาตรการคุ้มครองที่เหมาะสมอื่น ๆ ที่สามารถบังคับสิทธิของเจ้าของข้อมูลส่วนบุคคลได้ตามที่บริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจมีการกำหนดขึ้น ได้แก่ ข้อสัญญามาตรฐาน หรือจรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ หรือคำรับรอง ซึ่งเป็นเงื่อนไขที่ทำให้บริษัท สามารถส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางได้ แม้ว่าประเทศปลายทางนั้นจะไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ โดยอาจเลือกใช้แนวทางตามข้อ 4.1 ถึงข้อ 4.3 ดังต่อไปนี้

4 ข้อสัญญามาตรฐาน (Standard Data Protection Clauses)

บริษัท นำข้อสัญญามาตรฐาน (Standard Contractual Clauses) มาใช้เพื่อให้ข้อมูลส่วนบุคคลถูกถ่ายโอนอย่างที่ควรจะเป็น เพื่อให้การให้บริการ รวมถึงการรักษามาตรฐานและการปรับปรุงบริการให้เป็นไปโดยถูกต้องตามกฎหมาย อย่างไรก็ตาม ข้อสัญญาคุ้มครองข้อมูลส่วนบุคคลจะต้องมีการกำหนดหน้าที่ทางสัญญาเกี่ยวกับการส่งข้อมูลส่วนบุคคลไปยังต่างประเทศตลอดจนการโอนย้ายข้อมูลส่วนบุคคล ซึ่งเจ้าข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนเองในการส่งหรือโอนข้อมูลส่วนบุคคลไปหน่วยงานในต่างประเทศได้ โดยต้องมีมาตรการคุ้มครองที่เหมาะสม ดังนี้

4.1. ในการตกลงส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศ จะต้องมีรายละเอียดเกี่ยวกับ

4.1.1 บริษัท ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1. รับรองว่าการเก็บรวบรวม ประมวล ส่งหรือโอนข้อมูลส่วนบุคคลเป็นไปโดยชอบด้วยพรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. พิจารณาว่าผู้รับโอนข้อมูลส่วนบุคคลสามารถปฏิบัติตามข้อกำหนดตามที่ระบุในนโยบายนี้ได้

3. ให้ข้อมูลเกี่ยวกับกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลซึ่งใช้บังคับอยู่ในประเทศปลายทางหรือบังคับแก่องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล

4. ตอบคำถามของเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้รับการส่งหรือโอนข้อมูลส่วนบุคคล

5. ให้ข้อมูลเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสิทธิเกี่ยวกับความรับผิดและสิทธิของบุคคลที่สามแก่เจ้าของข้อมูลส่วนบุคคล

6. ร่วมรับผิดกับผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการฝ่าฝืนข้อกำหนด

7. ร่วมกับผู้รับการส่งหรือผู้รับโอนในการระงับข้อพิพาทที่เกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผข้อมูลส่วนบุคคล โดยใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ยซึ่งไม่ได้มีผลบังคับผูกพันทางกฎหมาย

8. ในกรณีที่ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลฝ่าฝืนหน้าที่ตามที่ได้กำหนดในข้อ 6.2 บริษัทมีสิทธิที่จะพักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจนกว่าการฝ่าฝืนจะได้รับการแก้ไขหรือข้อกำหนดดังกล่าวถูกยกเลิก

4.1.2 บุคคลผู้รับส่งหรือรับโอนข้อมูลส่วนบุคคล ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1. กำหนดว่ามีการจัดมาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

2. ดำเนินการให้บุคคลภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลนั้น รักษาความลับของข้อมูลส่วนบุคคล

3. รับรองว่าตนไม่มีเหตุอันควรจะเชื่อได้ว่ามีกฎหมายใดที่ขัดขวางมิให้สามารถปฏิบัติหน้าที่เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามข้อกำหนดนี้ได้

4. ประมวลผลข้อมูลส่วนบุคคลตมวัตถุประสงค์ที่กำหนดเท่านั้น

5. แจ้งให้บริษัทได้ทราบถึงส่วนงานภายในองค์กรซึ่งมีหน้าที่ในการตอบสนองต่อคำร้องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและจะให้ความร่วมมือกับบริษัทโดยสุจริต

6. ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบ ในกรณีที่ได้รับการร้องขอจากบริษัท

7. ประมวลผลข้อมูลส่วนบุคคลโดยสอดคล้องกับ พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

8. ร่วมรับผิดกับบริษัทในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้รับความเสียหายจากการฝ่าฝืนข้อกำหนด

9. ร่วมกับบริษัทในการระงับข้อพิพาทที่เกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล โดยใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ยซึ่งไม่ได้มีผลบังคับผูกพันทางกฎหมาย

4.2 ในการตกลงส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศ จะต้องมีรายละเอียดเกี่ยวกับ ข้อสัญญาที่กำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถบังคับ

สิทธิของตนต่อบริษัท ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลช่วง และ

4.2.1 บริษัท ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1. รับรองว่าการประมวลผลข้อมูลส่วนบุคคลซึ่งหมายรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นไปโดยสอดคล้องกับพรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. รับรองว่าผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลจะประมวลผลข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนตามคำสั่งของบริษัทในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายที่บังคับใช้แก่กรณีและข้อกำหนดนี้

3. รับรองว่าผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะจัดหามาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

4. รับรองว่าจะมีการจัดหามาตรการด้านความปลอดภัยเพื่อป้องกันคุ้มครองมิให้ข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนสูญหายโดยอุบัติเหตุหรือโดยการกระทำโดยมิชอบ หรือการถูกทำลายโดยอุบัติเหตุหรือการกระทำโดยมิชอบ การเปลี่ยนแปลงแก้ไข การถูกเปิดเผย หรือการเข้าถึงโดยมิชอบ โดยเฉพาะอย่างยิ่งในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลผ่านระบบโครงข่าย (Transmission of Data over a Network) และการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายใด ๆ

5. รับรองว่าจะมีการปฏิบัติตามมาตรการคุ้มครองความปลอดภัยของข้อมูล

6. รับรองว่าเจ้าของข้อมูลส่วนบุคคลจะได้รับการแจ้งว่ามีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลที่มีความอ่อนไหวตามมารตรา 26 พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

7. ดำเนินการส่งการแจ้งเตือนที่ได้รับจากผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบริษัท คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในกรณีที่บริษัทตัดสินใจว่าจะส่งหรือโอนข้อมูลส่วนบุคคลต่อไป หรือยกเลิกพักการส่งหรือโอนข้อมูลส่วนบุคคล

8. ส่งบทสรุปรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลช่วง

9. ร่วมกับบริษัทรับผิดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นการกระทำของบริษัทหรือผู้รับสิทธิการส่งหรือรับโอน

10. ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถเรียกร้องค่าเสียหายจากบริษัทตามข้อกำหนดได้เนื่องจากบริษัทไม่สามารถถูกติดตามตัวได้หรือล้มละลาย เจ้าของข้อมูลส่วนบุคคลสามารถเรียกค่าเสียหายได้จากการผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล

11. บริษัทจะส่งสำเนาของข้อกำหนดนี้ให้บริษัทคณะกรรมคุ้มครองข้อมูลส่วนบุคคลเก็บรักษาไว้

4.2.2 บุคคลผู้รับส่งหรือรับโอนข้อมูลส่วนบุคคล ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จะต้องดำเนินการดังต่อไปนี้

1. รับรองว่าจะประมวลผลข้อมูลส่วนบุคคลเฉพาะในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลและตามคำสั่งของบริษัทเท่านั้น ในกรณีที่ไม่สามารถปฏิบัติการตามหน้าที่ดังกล่าวได้ จะแจ้งบริษัททราบโดยไม่ชักช้า ในกรณีนี้ บริษัทสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้

2. รับรองว่าตนไม่มีเหตุอันควรจะเชื่อได้ว่ามีกฎหมายใดที่ขัดขวางมิให้สามารถประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของบริษัท และในกรณีที่มีการเปลี่ยนแปลงทางกฎหมายซึ่งจะส่งผลต่อการปฏิบัติหน้าที่ตามข้อกำหนดนี้ ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะแจ้งให้บริษัททราบถึงการเปลี่ยนแปลงดังกล่าวโดยไม่ชักช้า ในกรณีนี้ บริษัทสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้

3. รับรองว่าตนได้จัดหามาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) ของพรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว

4. แจ้งให้บริษัททราบโดยไม่ชักช้าเกี่ยวกับคำร้องให้เปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมาย เว้นแต่ กรณีไม่สามารถแจ้งได้เนื่องจากมีกฎหมายห้าม เช่น เป็นข้อห้ามตามกฎหมายอาญาเพื่อรักษาความลับของการดำเนินกระบวนการสืบสวนสอบสวน การเข้าถึงข้อมูลหรือโดยการกระทำที่มิชอบ และคำร้องที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรงโดยไม่มีการตอบสนองต่อคำร้องดังกล่าว

5. สอบถามบริษัทถึงการประมวลผลข้อมูลส่วนบุคคลซึ่งถูกส่งหรือโอน

6. ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบ ในกรณีที่ได้รับคำร้องขอจากบริษัท

7. ส่งบทสรุปรายละเอียดเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลตลอดจนสำเนาสัญญาให้บริการประมวลผลข้อมูลส่วนบุคคลช่วงโดยลบส่วนที่เป็นข้อมูลเชิงพาณิชย์ออก แต่มีการเติมรายละเอียดเกี่ยวกับมาตรการรักษาความปลอดภัยเข้าไปแทนในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถดำเนินการให้ได้รับรายละเอียดดังกล่าวจากบริษัทได้

8. แจ้งบริษัทให้ทราบถึงการประมวลผลข้อมูลส่วนบุคคลช่วงและได้รับความยินยอม

9. ร่วมกับบริษัทรับผิดต่อเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นการกระทำของบริษัทหรือผู้รับการส่งหรือรับโอน

10. การประมวลผลข้อมูลส่วนบุคคลช่วงจะเป็นไปตามข้อกำหนดนี้

11. ส่งสำเนาสัญญาประมวลผลข้อมูลส่วนบุคคลช่วงให้กับบริษัท

12. ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนเพื่อเรียกร้องค่าสินไหมทดแทนหรือค่าเสียหายจากผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลตกลงว่าจะระงับข้อพิพาทดังกล่าวโดยการไกล่เกลี่ยซึ่งมีความเป็นอิสระหรือโดยองค์กรคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

5. จรรยาบรรณและจริยธรรมในการดำเนินธุรกิจ (Code of Conduct)

บริษัท จะนำส่งหรือโอนข้อมูลส่วนบุคคลเมื่อผู้รับโอนได้ลงนามในข้อปฏิบัติซึ่งได้รับการอนุมัติจากเจ้าพนักงานโดยข้อปฏิบัติที่กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศจะต้องมีรายละเอียดของมาตรการที่เหมาะสมในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งถูกนำไปประมวลผล ตลอดจนโอนข้อมูลส่วนบุคคล ทั้งนี้ข้อปฏิบัติดังกล่าวจะต้องมีผลบังคับได้ต่อเจ้าข้อมูลส่วนบุคคลโดยตรง บริษัท จะนำจรรยาบรรณ

และจริยธรรมในการดำเนินธุรกิจ ที่ยึดมั่นในเจตนารมณ์ของการดำเนินธุรกิจอันตั้งอยู่บนพื้นฐานของการบริหารจัดการตามหลักการกำกับดูแลกิจการที่ดี โดยยึดมั่นต่อคุณธรรมและจริยธรรมในการดำเนินธุรกิจ มีความโปร่งใส ตรวจสอบได้ และตระหนักถึงความรับผิดชอบต่อผู้มีส่วนได้เสียทุกฝ่าย เพื่อให้เกิดการป้องกันข้อมูลส่วนบุคคลอย่างเหมาะสมและเป็นไปตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

6 คำรับรอง (Certification Mechanism)

บริษัท จะใช้คำรับรองที่ได้รับการยอมรับโดยบริษัทคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งประกอบกับคำมั่นสัญญาที่มีผลบังคับผูกพันผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในต่างประเทศ ที่จะปรับใช้มาตรการที่เหมาะสมเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคล เพื่อแสดงให้เห็นว่ามีการป้องกันที่เหมาะสมในการถ่ายโอนข้อมูลส่วนบุคคลในระดับสากล

7. วันที่มีผลบังคับใช้

นโยบายฉบับนี้ได้รับอนุมัติจากคณะกรรมการบริษัทในวันที่ 13 มกราคม 2565 และมีผลบังคับใช้ในวันที่ 13 เดือน มกราคม พ.ศ. 2565 เป็นต้นไป ผู้ใดฝ่าฝืนจะถูกดำเนินการลงโทษตามข้อบังคับการทำงานของบริษัท