นโยบายบริหารการคุ้มครองข้อมูลส่วนบุคคล

บริษัท อีซี่ บาย จำกัด (มหาชน)

1. จุดมุ่งหมายและขอบเขตของนโยบาย

บริษัท อีซี่ บาย จำกัด (มหาชน) มีจุดมุ่งหมายให้มีระบบควบคุมภายในที่ดีและมุ่งมั่นในการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และกฎหมายที่เกี่ยวข้องของทุกประเทศ โดยดูแลสิทธิและเสรีภาพของเจ้าของข้อมูล และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่กำหนด รวมถึงจัดให้มีอุปกรณ์ หรือเครื่องมือที่เพียงพอ เพื่อป้องกันการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

2. คำนิยาม

บริษัทฯ	บริษัท อีซี่ บาย จำกัด (มหาชน) นิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562
หน่วยงานกำกับ	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม บุคคลและคณะกรรมการที่ปฏิบัติหน้าที่ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม
ข้อมูลส่วนบุคคลที่อ่อนไหว	ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและมีเงื่อนไขเฉพาะในการดำเนินการ เช่น เชื้อชาติหรือเผ่าพันธุ์ ความเห็นทางการเมือง ศาสนาหรือความเชื่อทางปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ข้อมูลสหภาพแรงงาน ข้อมูลทางพันธุกรรม หรือข้อมูลใดๆ ที่อาจส่งผลกระทบต่อข้อมูลในลักษณะเดียวกันตามที่กำหนดโดย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
เจ้าของข้อมูล	ผู้ที่เป็นเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักรไทย โดยไม่คำนึงถึงสัญชาติ เช่น ลูกค้า กรรมการบริษัท พนักงาน ผู้ถือหุ้น เป็นต้น
ผู้ควบคุมข้อมูล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล สำหรับวัตถุประสงค์ของนโยบายนี้ ผู้ควบคุมข้อมูล หมายถึง บริษัท อีซี่ บาย จำกัด (มหาชน)
ผู้ประมวลผลข้อมูล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล สำหรับวัตถุประสงค์ของนโยบายนี้ ผู้ประมวลผลข้อมูล หมายถึง ผู้ให้บริการภายนอก
ผู้ให้บริการภายนอก	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัทฯ ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล รวมถึงการเข้าถึงข้อมูลข้ามพรมแดน
ข้อตกลงให้ประมวลผลข้อมูลส่วนบุคคล	สัญญาที่ลงนามโดยผู้ประมวลผลข้อมูลทั้งรูปแบบลายลักษณ์อักษรและรูปแบบอิเล็กทรอนิกส์ เพื่อวัตถุประสงค์ในการกำกับข้อตกลงและเงื่อนไขของข้อมูลส่วนบุคคล
CEO	ประธานเจ้าหน้าที่บริหารของบริษัท
DPO	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท

DPC	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของบริษัท
DPC Secretary	เลขานุการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของบริษัท
RoPA	บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล

3. หลักสำคัญในการปฏิบัติ

3.1 บริษัทฯ จะต้องดูแลข้อมูลส่วนบุคคลของเจ้าของข้อมูล ข้อมูลส่วนบุคคลที่อ่อนไหว เลขประจำตัวบุคคล ข้อมูลส่วนบุคคลที่เฉพาะเจาะจง เป็นต้น เพื่อให้เป็นไปตามกฎหมายและกฎระเบียบแห่งราชอาณาจักรไทย รวมถึงมาตรฐานของประเทศปลายทางที่เกี่ยวข้อง โดยพิจารณาถึงนโยบายการกำกับดูแลกิจการ

3.2 บริษัทฯ ต้องให้ความรู้แก่กรรมการ ผู้บริหาร และพนักงานให้เข้าใจถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เพื่อนำไปปฏิบัติได้อย่างถูกต้อง

3.3 บริษัทฯ จะเก็บรวบรวมข้อมูลส่วนบุคคลเท่าที่จำเป็น และแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ของการรวบรวมเพื่อนำข้อมูลส่วนตัวไปใช้หรือเปิดเผย บริษัทฯ จะใช้ข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายเท่านั้นและไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งไว้ เว้นแต่ได้รับอนุญาตตามกฎหมาย

3.4 บริษัทฯ ห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคลแก่บุคคลอื่น โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยได้รับยกเว้นไม่ต้องขอความยินยอมตามกฎหมาย

3.5 บริษัทฯ จัดตั้งมาตรการเพื่อให้มั่นใจได้ว่าเจ้าของข้อมูลมีสิทธิในการใช้สิทธิของตนในการแก้ไขและเปิดเผยข้อมูลส่วนบุคคล รวมถึงภาระผูกพันตามที่กฎหมายกำหนด บริษัทฯ จัดให้มีช่องทางในการรับความคิดเห็นและสอบถามเกี่ยวกับการจัดการข้อมูลส่วนบุคคลตามสิทธิของเจ้าของข้อมูล

3.6 บริษัทฯ จัดให้มีมาตรการที่เหมาะสม เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล เพื่อป้องกันการเข้าถึง เปลี่ยนแปลง แก้ไข สูญหายหรือข้อมูลรั่วไหล รวมถึงจัดทำและเก็บรักษา RoPA ไว้ ตามที่กฎหมายกำหนด

3.7 บริษัทฯ จัดให้มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และ/หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) โดยประธานเจ้าหน้าที่บริหาร (CEO) มีหน้าที่รับผิดชอบเป็นไปตามที่กฎหมายกำหนด บนพื้นฐานของโครงสร้างการควบคุม กำกับ และตรวจสอบเพื่อควบคุมบทบาทและหน้าที่รับผิดชอบเป็นระยะเวลา 4 ปี โดยประธานเจ้าหน้าที่บริหารสามารถพิจารณาแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และ/หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) ขึ้นใหม่ เมื่อพ้นจากตำแหน่งตามวาระนั้น ในกรณีที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือสมาชิกคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) ท่านใดพ้นจากตำแหน่งก่อนวาระที่กำหนด ประธานเจ้าหน้าที่บริหาร (CEO) สามารถแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และ/หรือสมาชิกคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) ขึ้นใหม่เพื่อรับหน้าที่แทน บริษัทฯ ต้องส่งเสริมการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) โดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคล การประชุมหารือ และประโยชน์อื่นๆ เพื่อการปฏิบัติหน้าที่ได้ตามกฎหมายกำหนด บริษัทฯ อาจมีการแต่งตั้งบุคคลที่มีความเชี่ยวชาญและประสบการณ์ที่เป็นประโยชน์ต่อการปฏิบัติหน้าที่ ในฐานะที่ปรึกษาของบริษัทฯ

3.8 การดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคล และ/หรือข้อมูลข้ามพรมแดน ของผู้ให้บริการภายนอก บริษัทฯ จัดให้มีข้อตกลงระหว่างกัน เพื่อควบคุมและติดตามการดำเนินงานตามหน้าที่ของผู้ให้บริการภายนอก เพื่อให้มั่นใจได้ว่ามีการป้องกันข้อมูลส่วนบุคคลในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล รวมถึงมาตรการทางเทคนิคและการจัดการเพิ่มเติม เพื่อรักษาความมั่นคงปลอดภัยตามที่บริษัทฯร้องขอเป็นครั้งคราวโดยทำเป็นลายลักษณ์อักษร และตามที่กฎหมายที่บังคับใช้กำหนด ทั้งนี้ รวมถึงกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

4. บทบาทและความรับผิดชอบ

4.1 ประธานเจ้าหน้าที่บริหาร (CEO) มีหน้าที่รับผิดชอบในการตรวจสอบแผนงานการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯให้ดำเนินการและปฏิบัติการได้อย่างมีประสิทธิภาพ รวมถึงทำหน้าที่ในการพิจารณาการแก้ไขปัญหาข้อมูลส่วนบุคคลอย่างเหมาะสม แต่งตั้งเจ้าหน้าที่ข้อมูลส่วนบุคคล (DPO) และ/หรือสมาชิกคณะกรรมการข้อมูลส่วนบุคคล (DPC) และ/หรือที่ปรึกษาที่มีความรู้ ความเชี่ยวชาญ และประสบการณ์ตามที่กฎหมายกำหนดหรือที่เป็นประโยชน์ต่อการดำเนินงานของบริษัทฯ

4.2 เจ้าหน้าที่คุ้มครองข้อมูล (DPO) มีหน้าที่ให้คำแนะนำเกี่ยวกับการปฏิบัติตามกฎหมาย ตรวจสอบติดตามการดำเนินงานเกี่ยวกับการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามกฎหมาย ประสานงานและให้ความร่วมมือกับหน่วยงานกำกับ เมื่อมีปัญหาเกี่ยวกับข้อมูลส่วนบุคคลของบริษัทฯ และ/หรือของผู้ให้บริการภายนอก รายงานปัญหาต่าง ๆ ที่เกิดขึ้นระหว่างการปฏิบัติงานไปยังประธานเจ้าหน้าที่บริหารโดยตรง (CEO)

กรณีที่เจ้าหน้าที่คุ้มครองส่วนบุคคล (DPO) ไม่สามารถปฏิบัติหน้าที่ได้เป็นการชั่วคราว ให้ประธานเจ้าหน้าที่บริหาร (CEO) หรือบุคคลที่ได้รับมอบหมายจากประธานเจ้าหน้าที่บริหาร (CEO) หรือจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) อย่างเป็นลายลักษณ์อักษร ปฏิบัติหน้าที่ในฐานะเจ้าหน้าที่คุ้มครองส่วนบุคคล (DPO) แทนได้

4.3 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) ประกอบด้วยประธานและสมาชิกคณะกรรมการโดยหัวหน้าฝ่ายและ/หรือสำนักถูกคัดเลือกและแต่งตั้งจากความรู้ ความเชี่ยวชาญ และประสบการณ์ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านสุขภาพ ด้านการเงิน หรือด้านอื่น ทั้งนี้ต้องเกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC)

1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึง สูญหาย ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้เป็นไปตามกฎหมายกำหนด หรือตามมาตรฐานขั้นต่ำที่กำหนดและประกาศโดยคณะกรรมการ
2) ให้คำแนะนำและควบคุมข้อมูลส่วนบุคคลที่จะให้แก่ผู้ให้บริการภายนอกหรือบุคคลที่สามนอกเหนือจากบริษัทฯ เพื่อป้องกันจากการใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวโดยปราศจากอำนาจหรือโดยมิชอบ
3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือเมื่อเจ้าของข้อมูลร้องขอหรือถอนความยินยอม นอกเสียจากว่ามีการเก็บไว้ดังเดิมเพื่อวัตถุประสงค์ตามกฎหมาย
4) ให้คำแนะนำเกี่ยวกับผลการพิจารณาและวิธีการแก้ไขปัญหาที่เหมาะสมเมื่อหน่วยงานกำกับมีคำสั่งให้บริษัทฯดำเนินการส่งเอกสารหรือข้อมูล รวมถึงชี้แจงข้อเท็จจริงเกี่ยวกับเรื่องที่มีผู้ร้องเรียนเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย
5) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใด ๆ เพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯในการปฏิบัติตามกฎหมาย
6) ส่งเสริมและสนับสนุนการปฏิบัติงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ให้เกิดผลสำเร็จเพื่อให้เป็นไปตามกฎหมาย หรืองานใด ๆ ที่ได้รับมอบหมายจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
7) เสนอบุคคลเข้ารับการแต่งตั้งให้เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) และ/หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) และ/หรือที่ปรึกษาผู้มีความรู้หรือความเชี่ยวชาญเรื่องการคุ้มครองข้อมูลส่วนบุคคลและ/หรือบุคคลที่มีคุณสมบัติตามที่กฎหมายกำหนด ตามความเห็นชอบของบุคคลดังกล่าวต่อประธานเจ้าหน้าที่บริหาร (CEO) เพื่อแต่งตั้ง
8) แต่งตั้งคณะอนุกรรมการเพื่อปฏิบัติงานตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (DPC) มอบหมาย

9) เพื่อรับทราบการจัดทำ การแก้ไข หรือการยกเลิก RoPA

4.4 เลขานุการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

หัวหน้าแผนกคุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่เป็นเลขานุการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของบริษัท โดยมีหน้าที่และความรับผิดชอบดังนี้

1) จัดเตรียมการประชุมคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล การจัดเตรียมวาระการประชุมและเอกสารประกอบการประชุม บันทึกรายงานการประชุม รวมถึงติดตามประเด็นอภิปรายจากที่ประชุม
2) สนับสนุนการปฏิบัติงานของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงรับผิดชอบงานที่ได้รับมอบหมายจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
3) ดำเนินการอื่นใดตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลและกฎหมายที่เกี่ยวข้องกำหนด

4.5 กรรมการ ประธานเจ้าหน้าที่บริหาร ผู้บริหาร และพนักงาน

กรรมการ ประธานเจ้าหน้าที่บริหาร ผู้บริหาร และพนักงาน มีหน้าที่ปฏิบัติตามนโยบายบริหารการคุ้มครองข้อมูลส่วนบุคคล ข้อบังคับและกฎระเบียบของบริษัทอย่างเคร่งครัด รวมถึงการรักษาความลับของข้อมูลส่วนบุคคลที่ได้ล่วงรู้จากการปฏิบัติงาน การละเมิดนโยบายบริหารการคุ้มครองข้อมูลส่วนบุคคลจะได้รับการพิจารณาลงโทษตามข้อบังคับเกี่ยวกับการทำงานและ/หรือตามกฎหมายที่บังคับใช้

ภาคผนวก

การแก้ไขและยกเลิกนโยบายฉบับนี้

การแก้ไขหรือการยกเลิกที่มีนัยสำคัญใด ๆ ในนโยบายฉบับนี้ จะต้องถูกนำเสนอโดยสำนักกำกับธุรกิจองค์กร เพื่อให้คณะกรรมการบริษัทฯ พิจารณาอนุมัติ

รอบการทบทวนนโยบายฉบับนี้

นโยบายฉบับนี้กำหนดให้มีการทบทวนเป็นประจำทุกปีนับจากวันที่มีผลบังคับใช้ อย่างไรก็ตาม อาจมีการทบทวนตามระยะเวลาที่เหมาะสม หากมีการแก้ไขหรือยกเลิกเนื้อหาที่มีนัยสำคัญ

วันที่มีผลบังคับใช้

นโยบายฉบับนี้ได้รับการพิจารณาและอนุมัติโดยคณะกรรมการบริษัทฯ วันที่ 25 พฤษภาคม พ.ศ.2566 และนโยบายฉบับนี้มีผลบังคับใช้ตั้งแต่ วันที่ 1 มิถุนายน พ.ศ.2566