AIRA Asset Management Company Limited 319 Chamchuri Square Building, 12th Floor, Phayathai Road, Pathumwan, Bangkok 10330
บริษัทหลักทรัพย์จัดการกองทุน ไอร่า จำกัด เลขที่ 319 อาคารจัตุรัสจามจุรี ชั้น 12 ถนนพญาไท แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330
Tel. 0-2038-4499 ทะเบียนเลขที่ 0105560035008

นโยบายคุ้มครองข้อมูลส่วนบุคคล

(Personal Data Protection Policy)

(ฉบับทบทวน ปี 2567)

สารบัญ

หน้า

ส่วนที่ 1 วัตถุประสงค์และขอบเขตการบังคับใช้

1.1 วัตถุประสงค์

เพื่อเป็นแนวทางในการคุ้มครองข้อมูลส่วนบุคคล ที่บริษัทได้มีการเก็บรวบรวม ใช้หรือเปิดเผยให้สอดคล้องกับกฎเกณฑ์ ระเบียบของทางราชการและหน่วยงานกำกับดูแล ดังรายการต่อไปนี้

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตามแนวสมาคมบริษัทจัดการกองทุน

1.2 ขอบเขตการบังคับใช้

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท ครอบคลุมถึงข้อมูลส่วนบุคคลในส่วนที่บริษัทได้มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคลนั้น ได้กระทำในหรือนอกราชอาณาจักรก็ตาม

ส่วนที่ 2 นิยามและคำจำกัดความ

ข้อมูลส่วนบุคคล (Personal Data)	หมายถึง	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม โดยเฉพาะ เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ฯลฯ
ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Personal Data)	หมายถึง	ข้อมูลที่ต้องระมัดระวังเป็นพิเศษในการเก็บรวบรวม หรือประมวลผล เช่น เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา รสนิยมทางเพศ ข้อมูลทางชีวภาพ ทั้งนี้ กฎหมายให้การคุ้มครองข้อมูลที่อ่อนไหวเข้มงวดกว่าข้อมูลส่วนบุคคลธรรมดา
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	หมายถึง	พนักงาน ผู้สมัครงาน บุคคลที่มาติดต่อและตกลงทำธุรกรรมกับบริษัท
บริษัท	หมายถึง	บริษัทหลักทรัพย์จัดการกองทุน ไอร่า จำกัด
ผู้ใช้บริการ	หมายถึง	บุคคลหรือนิติบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล ที่เข้ามาติดต่อยังระบบสารสนเทศของบริษัท
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	หมายถึง	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)	หมายถึง	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
สำนักงาน	หมายถึง	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
คณะกรรมการ	หมายถึง	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
ข้อมูลชีวภาพ	หมายถึง	ข้อมูลส่วนบุคคลที่เกิดจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเด่นทางกายภาพหรือทางพฤติกรรมของบุคคลมาใช้ ทำให้สามารถยืนยันตัวตน ของบุคคลนั้นที่ไม่เหมือนกับบุคคลอื่นได้ เช่น ข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองม่านตา หรือ ข้อมูลจำลองลายนิ้วมือ

ส่วนที่ 3 บุคคล หน่วยงาน บทบาทหน้าที่และความรับผิดชอบของผู้เกี่ยวข้อง

3.1 บริษัทในฐานะ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controllers) และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processors)

3.1.1 บทบาทในฐานะการเป็นผู้ควบคุมข้อมูลส่วนบุคคล (Data Controllers) โดยการเก็บ รวบรวม ใช้ และเปิดเผย ทั้งในส่วนของข้อมูลพนักงาน ผู้สมัครงาน ลูกค้า และอื่นๆ เพื่อประโยชน์ในการดำเนินธุรกิจ บริษัทจึงมีนโยบายจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลดังนี้

(1) การรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล และทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีมีการเปลี่ยนแปลงไปเพื่อให้การทำงานมีประสิทธิภาพยิ่งขึ้น

(2) บริษัทจะไม่เปิดเผยข้อมูลส่วนบุคคลให้กับบุคคลอื่นที่ไม่เกี่ยวข้องทราบ เว้นแต่จะมีเหตุจำเป็นที่ต้องเปิดเผยข้อมูลให้บุคคลอื่นรับรู้

(3) มีการบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ มีรายละเอียดอย่างน้อย ดังนี้

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูลส่วนบุคคล
- การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล

3.1.2 บทบาทในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processors) ตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controllers) หรือในกรณีที่บริษัทดำเนินการให้ผู้อื่นเป็นผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทจัดให้มีนโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

(1) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นไม่เป็นไปตามที่กฎหมายกำหนด

(2) มีระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ การแก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคล และแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบเมื่อมีการละเมิดข้อมูลส่วนบุคคลเกิดขึ้น

(3) จัดทำและเก็บรักษาบันทึกรายการของการประมวลผลข้อมูลส่วนบุคคล

(4) มีข้อตกลงร่วมกันระหว่างผู้ควบคุมข้อมูลส่วนบุคคล กับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อควบคุมการดำเนินงานตามหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล

3.2 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

บริษัทจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ซึ่งต้องมีความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามพรบ.คุ้มครองข้อมูลส่วนบุคคล หรือเกณฑ์ที่บริษัท กำหนด โดยมีหน้าที่ดังนี้

(1) ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

(2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(3) ประสานงานและให้ความร่วมมือกับสำนักงาน เมื่อเกิดปัญหาเกี่ยวกับการเก็บรวบรวมใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลขณะปฏิบัติงาน

(4) รักษาความลับข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

บริษัทมีนโยบายสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยการจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐาน

3.3 คณะทำงานเตรียมความพร้อมระดับองค์กรเพื่อรองรับ พรบ. คุ้มครองข้อมูลส่วนบุคคล

เพื่อเป็นการเตรียมความพร้อม และยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล บริษัทมีนโยบายที่จะตั้งคณะทำงานเตรียมความพร้อมระดับองค์กรเพื่อรองรับ พรบ.คุ้มครองข้อมูลส่วนบุคคล โดยให้มีบทบาทหน้าที่ ดังนี้

(1) ทำความเข้าใจกฎหมาย พรบ.คุ้มครองข้อมูลส่วนบุคคล กฎระเบียบต่างๆ ที่ออกโดยสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2) วิเคราะห์และประเมินผลกระทบจากกฎหมาย ระเบียบต่างๆ ที่เกี่ยวข้องกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

(3) เสนอฝ่ายบริหารเพื่อพิจารณาปรับปรุงแนวปฏิบัติและขั้นตอนการดำเนินงานขององค์กร (Procedures and Operation workflow) เพื่อให้สอดคล้องกับกฎหมาย ประกาศ และระเบียบต่างๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

ส่วนที่ 4 การคุ้มครองข้อมูลส่วนบุคคล

บริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล มีนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ทั้งในส่วนของข้อมูลพนักงาน ผู้สมัครงาน ลูกค้า และอื่นๆ ดังนี้

4.1 หน้าที่และแนวปฏิบัติที่มีต่อเจ้าของข้อมูลส่วนบุคคล

4.1.1 การแจ้งวัตถุประสงค์การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

บริษัทมีนโยบายในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย (Collection limitation) และมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล ถึงรายละเอียด ดังต่อไปนี้

(1) วัตถุประสงค์ของการเก็บรวบรวม ใช้ หรือเปิดเผย และความจำเป็นที่เจ้าของข้อมูลต้องให้ข้อมูลส่วนบุคคลเพื่อเข้าปฏิบัติตามสัญญาหรือเพื่อปฏิบัติตามกฎหมาย รวมทั้ง ผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคล

(2) ระยะเวลาในการเก็บรวบรวม หากไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

(3) ข้อมูลเกี่ยวกับบริษัท สถานที่ติดต่อ วิธีการติดต่อ ตัวแทน หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

(4) การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงประเภทของบุคคลหรือหน่วยงาน ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

(5) การแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล

4.1.2 การขอและถอนความยินยอม

ในการเก็บรวบรวมข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Personal Data) หรือ การเก็บข้อมูลที่มีวัตถุประสงค์อื่นที่ไม่เป็นไปตามวัตถุประสงค์การปฏิบัติตามสัญญา เช่น การใช้ข้อมูลส่วนบุคคลเพื่อทำการวิเคราะห์เพื่อนำเสนอสินค้าและบริการที่เหมาะสม ตามข้อ 4.1.3

4.1.3 การทำการตลาดแบบตรง (Direct marketing)

บริษัทต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น โดยมีแนวปฏิบัติ ดังนี้

(1) การขอความยินยอมต้องทำเป็นหนังสือหรือทำโดยผ่านระบบอิเล็กทรอนิกส์ เว้นแต่ไม่สามารถขอความยินยอมด้วยวิธีการดังกล่าวได้ และมีแบบหรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ต้องไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ของบริษัท

(2) การถอนความยินยอม เจ้าของข้อมูลส่วนบุคคลจะถอนความยินยอมเมื่อใดก็ได้ และต้องไม่มีขั้นตอนที่ยุ่งยากยกเว้นมีเหตุทำให้ไม่สามารถให้ถอนความยินยอมได้ หากการถอนความยินยอมส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลในเรื่องใด จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ถึงผลกระทบจากการถอนความยินยอมนั้น กรณีเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ข้อมูลส่วนบุคคลโดยลำพังได้ การขอ หรือถอนความยินยอมจากเจ้าของข้อมูลส่วนบุคคลดังกล่าวให้ดำเนินการ ดังต่อไปนี้

- เจ้าของข้อมูลส่วนบุคคลที่เป็นผู้เยาว์ซึ่งยังไม่บรรลุนิติภาวะ ต้องได้รับความยินยอมจากผู้ใช้อำนาจปกครองที่มีอำนาจกระทำการแทนผู้เยาว์

- เจ้าของข้อมูลส่วนบุคคลเป็นคนไร้ความสามารถ ให้ขอความยินยอมจากผู้อนุบาลที่มีอำนาจกระทำการแทนคนไร้ความสามารถ
- เจ้าของข้อมูลส่วนบุคคลเป็นคนเสมือนไร้ความสามารถ ให้ขอความยินยอมจากผู้พิทักษ์ที่มีอำนาจกระทำการแทนคนเสมือนไร้ความสามารถ

4.1.4 การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น (ถ้ามี)

ในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น บริษัทต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า ซึ่งอยู่ภายใต้กรอบระยะเวลาไม่เกิน 30 วัน นับแต่วันที่เก็บ รวบรวม โดยที่หากมีข้อมูลใดเข้าข่ายต้องขอความยินยอม ต้องดำเนินขอความยินยอมตามข้อ 4.1.2

4.2 หน้าที่และแนวปฏิบัติภายในบริษัทเพื่อการคุ้มครองข้อมูลส่วนบุคคล

4.2.1 การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment)

เพื่อให้กระบวนการจัดเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล มีความปลอดภัยในทุกวงจรชีวิตของข้อมูล (Data lifecycle) บริษัทต้องจัดให้มีการวิเคราะห์ และประเมินเพื่อบริหารจัดการข้อมูลส่วนบุคคลให้มีความปลอดภัย ตามขั้นตอนต่างๆ ดังนี้

(1) จัดทำกระบวนการกำหนดและแยกแยะข้อมูลส่วนบุคคล (Data mapping) ตามความเสี่ยงและความร้ายแรงที่อาจกระทบต่อสิทธิและเสรีภาพของบุคคลเพื่อระบุและจัดการข้อมูลบนพื้นฐานความเสี่ยง รวมถึงกำหนดฐานการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม (Lawfulness of processing) ทั้งในส่วนของข้อมูลส่วนบุคคลแบบทั่วไป (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)

(2) จัดทำกระบวนการ (Process integration) บันทึกกิจกรรมที่เกิดขึ้นตลอดวงจรชีวิตของข้อมูล (รวบรวมจัดเก็บ ใช้ เปิดเผย และการทำลาย) ควบคู่ไปกับการจัดทำแผนผัง การจัดเก็บข้อมูล (Storage/Location map) ทั้งในส่วนของข้อมูลอิเล็คทรอนิคส์ และข้อมูลที่จัดเก็บแบบดั้งเดิม เช่น ในกระดาษ เพื่อการบริการจัดการข้อมูลส่วนบุคคลให้สอดคล้องกับข้อกำหนดของกฎหมาย

(3) จัดทำการประเมินความเสี่ยง (Risk Assessment) ในทุกกระบวนการที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(4) เสนอแนะแนวทางการลดหรือกำจัดความเสี่ยง (Risk mitigation) ในการคุ้มครองข้อมูลส่วนบุคคล

4.2.2 การจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

เพื่อให้บริษัทสามารถป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็น หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม โดยต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

4.2.3 การเปิดเผยข้อมูลให้แก่บุคคล หรือนิติบุคคลอื่น เพื่อการประมวลผล

ในกรณีที่บริษัทมีความจำเป็นต้องให้ข้อมูลส่วนบุคคลแก่บุคคล หรือนิติบุคคลอื่น เพื่อการประมวลผล บริษัทมีหน้าที่ดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยอาจจัดให้มีการประเมินคุณสมบัติผู้ให้บริการ (Vendor Due Diligence Checklist) ว่าผู้ให้บริการนั้นมีมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคลที่ได้มาตรฐานที่ยอมรับกันทั่วไปตามหลักสากลหรือไม่ และจัดให้มีการทบทวนการทำสัญญาให้ครอบคลุมกฎหมายคุ้มครองข้อมูลส่วนบุคคล และมาตรการต่างๆ ที่สำนักงานออกประกาศ

4.2.4 การส่งหรือโอนข้อมูลไปต่างประเทศ (Cross Border Data Transfer)

บริษัทมีนโยบายส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอและต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด เว้นแต่

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และได้แจ้งถึงมาตรฐานการคุ้มครองที่ไม่เพียงพอเรียบร้อยแล้ว

(3) เป็นการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

(4) ดำเนินการตามสัญญาผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ข้อมูลในขณะนั้น

(6) ดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญ

4.2.5 การลบ ทำลายข้อมูลส่วนบุคคล

บริษัทจัดให้มีมาตรฐานอายุการจัดเก็บข้อมูล (Retention policy) และมาตรการการลบทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ โดยจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลในกรณีต่อไปนี้

(1) เมื่อพ้นกำหนดระยะเวลาการเก็บรักษา

(2) เมื่อเป็นข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

(3) เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอให้ลบหรือถอนความยินยอม

4.2.6 การจัดให้มีการบันทึก (Record of Processing Activities)

บริษัทมีนโยบายที่จะทำการบันทึกข้อมูลกิจกรรมที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล และการดำเนินการกรณีใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล โดยมีข้อมูลต่างๆ เพื่อใช้ในการตรวจสอบ ดังนี้

(1) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

(3) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(4) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(5) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล และเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม (ข้อมูลส่วนบุคคลที่ได้รับยกเว้น ไม่ต้องขอความยินยอม)

(7) การปฏิเสธคำขอ หรือการคัดค้านสิทธิในการเข้าถึง และขอรับสำเนาข้อมูล สิทธิขอรับข้อมูลโดยอัตโนมัติ หรือขอใช้หรือเปิดเผยโดยวิธีการอัตโนมัติ สิทธิคัดค้านการเก็บรวบรวมใช้หรือเปิดเผยข้อมูลและสิทธิขอให้ทำข้อมูลให้ถูกต้อง เป็นปัจจุบัน สมบูรณ์และไม่ก่อให้เกิดความเข้าใจผิด

ส่วนที่ 5 สิทธิของเจ้าของข้อมูลส่วนบุคคล

5.1 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตนซึ่งอยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

5.2 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอรับข้อมูลส่วนบุคคลที่เกี่ยวกับตนจากผู้ควบคุมข้อมูลส่วนบุคคลได้ ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่านหรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ

5.3 เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้

5.4 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้

5.5 เจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการใช้ข้อมูลส่วนบุคคลได้

5.6 ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

5.7 ในกรณีที่เจ้าของข้อมูลส่วนบุคคลร้องขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามข้อ 5.6 หากผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามคำร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องบันทึกคำร้องขอของเจ้าของข้อมูลส่วนบุคคลพร้อมด้วยเหตุผลให้ชัดเจน

ส่วนที่ 6 มาตรการรองรับการรั่วไหลของข้อมูล (Data Breaches)

แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะกระทำได้ เว้นแต่การละเมิดนั้นไม่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล และหากมีการละเมิดที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคลให้แจ้งเหตุการละเมิดนั้นให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย

6.1 หน้าที่แจ้งต่อสำนักงาน

ข้อมูลที่ต้องแจ้ง มีรายละเอียดอย่างน้อยดังต่อไปนี้

(1) คำอธิบายลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง

(2) ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม

(3) คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว เช่น ข้อมูลส่วนบุคคลของลูกค้าอาจถูกนำไปใช้โดยมิชอบหรือถูกปลอมแปลงตัวตนได้ เป็นต้น

(4) คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

6.2 หน้าที่แจ้งต่อเจ้าของข้อมูลส่วนบุคคล

บริษัทแจ้งไปยังเจ้าของข้อมูลส่วนบุคคลให้เร็วที่สุดเท่าที่จะกระทำได้ เมื่อการรั่วไหลของข้อมูลนั้นอาจเกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยการส่งข้อความทางโทรศัพท์ (SMS) ส่งอีเมล์ ประกาศทางหน้าการแจ้งเตือนหรือแบนเนอร์ (banner) ของเว็บไซต์ หรือส่งจดหมายทางไปรษณีย์ ตามที่เจ้าของข้อมูลส่วนบุคคลระบุช่องทางการติดต่อเพื่อให้เจ้าของข้อมูลส่วนบุคคลที่อาจได้รับผลกระทบทั้งหมดมีโอกาสทราบการแจ้งเตือนนั้นได้โดยเร็วที่สุด เพราะเจ้าของข้อมูลส่วนบุคคลแต่ละคนอาจมีช่องทางในการติดต่อที่สะดวกต่างกัน

6.3 แนวทางเยียวยา

ให้เป็นไปตามประกาศกำหนดหลักเกณฑ์และวิธีการของสำนักงาน

ส่วนที่ 7 การดำเนินการกับข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้ก่อนกฎหมาย พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้

ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลนั้นต่อไปได้ตามวัตถุประสงค์เดิม ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องกำหนดวิธีการยกเลิกความยินยอม และเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวมและใช้ข้อมูลส่วนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้

ส่วนที่ 8 การกำกับดูแลและตรวจสอบและประเมินความเสี่ยง

บริษัทในฐานะผู้ควบคุมข้อมูลมอบหมายให้ฝ่ายกำกับดูแลการปฏิบัติงานทำหน้าที่ในการกำกับดูแล และตรวจสอบการดำเนินงานของบุคลากรและผู้เกี่ยวข้องเพื่อให้เกิดการปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนดไว้ เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลที่หน่วยงานทำการรวบรวม จัดเก็บ และเผยแพร่ ถูกควบคุมภายใต้มาตรการที่กำหนดไว้ รวมถึงมีการตรวจสอบและประเมินความเสี่ยงเป็นประจำอย่างสม่ำเสมอ

ส่วนที่ 9 การทบทวนนโยบาย กระบวนงานที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานที่เกี่ยวข้องต้องทบทวนหรือปรับปรุงกระบวนทำงานและมาตรการที่เกี่ยวข้องกับการ รวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล เมื่อพบว่ามีความเสี่ยง หรือพบว่ามีกระบวนการทำงานที่ไม่สอดคล้องกับข้อกำหนดของกฎหมาย โดยทบทวนตามวงจรชีวิตของข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้ เปิดเผย จนถึงการลบหรือทำลายข้อมูล การทบทวนนโยบายให้เป็นความรับผิดชอบของฝ่ายกำกับดูแลการปฏิบัติงาน

ส่วนที่ 10 การสื่อสาร สร้างความตระหนักรู้ การฝึกอบรม

หน่วยงานต้องสร้างความตระหนักรู้ สำนึกรับผิดชอบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคล และหน้าที่ความรับผิดชอบของหน่วยงาน รวมถึงการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล และผลกระทบที่เกิดขึ้น จากการละเมิดนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ให้แก่บุคลากรของหน่วยงาน โดยการเผยแพร่ข้อมูลข่าวสาร และการฝึกอบรมให้ความรู้ที่เกี่ยวข้องเป็นประจำสม่ำเสมอ

นโยบายคุ้มครองข้อมูลส่วนบุคคล (ฉบับทบทวนปี 2567) ฉบับนี้ ได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 2/2567 เมื่อวันที่ 28 พฤษภาคม 2567 โดยมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2567

.....

(นางเสาวนีย์ กมลบุตร)

ประธานกรรมการบริษัท

บริษัท หลักทรัพย์จัดการกองทุน ไอร่า จำกัด