

นโยบายและระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

บริษัท ฟรอนท์ไลน์ เอ็นจิเนียริ่ง จำกัด (มหาชน) (“บริษัทฯ”) ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) ที่ควรได้รับการคุ้มครองทั้งของ กรรมการ ลูกค้า คู่ค้า ผู้มาติดต่องาน พนักงาน หรือผู้เกี่ยวข้องในธุรกิจของบริษัทฯ โดยบริษัทฯ จะปฏิบัติตามข้อมูลส่วนบุคคลของท่านในการเก็บรวบรวม ใช้ หรือเปิดเผย ด้วยความเคารพในสิทธิของเจ้าของข้อมูลภายใต้สัญญาข้อตกลงและกฎหมายที่เกี่ยวข้อง

บริษัทฯ จึงได้กำหนดนโยบายและแนวทางในการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล โดยยึดแนวทางการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นหลัก รวมถึงประกาศต่อสาธารณชนเพื่อให้เจ้าของข้อมูลส่วนบุคคลทุกท่านเชื่อมั่นว่าบริษัทฯ จะดูแลรักษาข้อมูลส่วนบุคคลของเจ้าของข้อมูล และจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ บริษัทฯ ถือว่าข้อมูลส่วนบุคคลที่เก็บรวบรวมไว้เป็นทรัพย์สิน ผู้ละเมิดจะต้องได้รับโทษตามกฎหมายที่กำหนดโทษที่ระบุไว้

วัตถุประสงค์

ด้วยความก้าวหน้าของเทคโนโลยีสารสนเทศ รวมถึงระบบการสื่อสารได้พัฒนาไปอย่างรวดเร็ว ทำให้การเข้าถึง การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล สามารถทำได้โดยง่าย สะดวก และรวดเร็ว อันอาจนำมาซึ่งความเสียหายต่อเจ้าของข้อมูล

บริษัทฯ ได้ตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) จึงได้กำหนดนโยบายและแนวทางในการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นหลักในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ข้อมูลส่วนบุคคลของลูกค้า คู่ค้า ผู้มาติดต่อ พนักงาน หรือผู้เกี่ยวข้องในธุรกิจของบริษัทฯ ได้รับการเก็บรวบรวม ใช้ รักษาอย่างปลอดภัย และใช้งานตามวัตถุประสงค์ ตามนโยบายที่บริษัทฯ กำหนด และเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นิยาม

“บริษัทฯ” หมายถึง บริษัท ฟรอนท์ไลน์ เอ็นจิเนียริ่ง จำกัด (มหาชน)

“บุคคล” หมายถึง บุคคลธรรมดา

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น

- (1) ชื่อ-นามสกุล
- (2) ชื่อเล่น
- (3) หมายเลขต่าง ๆ ที่ระบุตัวบุคคล ได้แก่ เลขบัตรประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร เลขบัตรเครดิต
- (4) ที่อยู่ อีเมล และเบอร์โทรศัพท์
- (5) ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP Address, Mac Address, Cookie ID เป็นต้น
- (6) ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน เป็นต้น
- (7) ข้อมูลที่สามารถเชื่อมโยงไปถึงตัวบุคคลได้ เช่น วันเกิดและสถานที่เกิด เชื้อชาติ สัญชาติ น้าหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ ข้อมูลทางการเงิน ข้อมูลทางการแพทย์ ข้อมูลการศึกษา ข้อมูลการจ้างงาน ประวัติประสบการณ์การทำงานกับองค์กรต่าง ๆ เป็นต้น
- (8) ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ พัลมเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง ข้อมูลพันธุกรรม เป็นต้น
- (9) ข้อมูลการประเมินผลการปฏิบัติงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง
- (10) ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น ข้อมูลจราจรคอมพิวเตอร์ (Log file) เป็นต้น
- (11) ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลอื่น ๆ ในอินเทอร์เน็ต

“ข้อมูลส่วนบุคคลอ่อนไหว” หมายถึง ข้อมูลที่เป็นเรื่องส่วนบุคคล แต่มีความละเอียดอ่อนและอาจจะส่อเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เช่น

- (1) เชื้อชาติ เผ่าพันธุ์
- (2) ความคิดเห็นทางการเมือง
- (3) ความเชื่อในลัทธิ ศาสนา หรือปรัชญา
- (4) พฤติกรรมทางเพศ
- (5) ประวัติอาชญากรรม
- (6) ข้อมูลสุขภาพหรือความพิการ
- (7) ข้อมูลสุขภาพแรงงาน
- (8) ข้อมูลพันธุกรรม
- (9) ข้อมูลชีวภาพ
- (10) ข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“เจ้าของข้อมูลส่วนบุคคล” หมายถึง บุคคลซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลนั้น โดยเจ้าของข้อมูลส่วนบุคคลนี้จะหมายถึง “บุคคลธรรมดา” เท่านั้น และไม่รวมถึง “นิติบุคคล” ที่จัดตั้งขึ้นตามกฎหมาย เช่น บริษัทฯ สมาคม มูลนิธิ หรือองค์กรอื่นใด

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง บริษัทฯ หรือประธานกรรมการบริหาร หรือประธานเจ้าหน้าที่บริหาร หรือผู้ได้รับมอบอำนาจ หรือผู้ได้รับมอบหมายให้มีอำนาจหน้าที่ตัดสินใจเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง พนักงานระดับบริหาร หรือผู้ได้รับมอบอำนาจ หรือผู้ได้รับมอบหมายให้เป็นผู้เก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูล ตามคำสั่งหรือในนามของบริษัทฯ ทั้งนี้ ผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งดำเนินการดังกล่าวต้องไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“ผู้ประมวลผลภายใน” หมายถึง พนักงานที่บริษัทฯ มอบหมายให้เป็นผู้ เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลในการทำงานตามหน้าที่ที่ได้รับมอบหมาย

“ผู้ประมวลผลภายนอก” หมายถึง บุคคลหรือบริษัทฯ ภายนอก ที่ทำการเก็บรวบรวม ใช้ เปิดเผยข้อมูลตามคำสั่งหรือข้อตกลงกับบริษัทฯ

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” (Data Protection Officer: DPO) หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่ให้คำแนะนำและตรวจสอบการดำเนินงาน ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล รวมถึงหน่วยงานอื่นที่เกี่ยวข้อง

“คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” หมายถึง ผู้ที่บริษัทฯ แต่งตั้งให้เป็นคณะกรรมการเพื่อเก็บรวบรวม ใช้ เปิดเผยข้อมูลให้เป็นระบบเดียวกัน เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลจากทุกหน่วยงานได้รับการคุ้มครองตามนโยบายของบริษัทฯ และ/หรือ ตามที่กฎหมายกำหนด

“ผู้เก็บ รวบรวม ใช้ รักษาข้อมูลส่วนบุคคล” หมายถึง พนักงานทุกคนที่นำข้อมูลส่วนบุคคลมาใช้งานตามหน้าที่ของตนเองเกี่ยวข้อง

“กรรมการ” (Directors) หมายถึง กรรมการของบริษัทฯ

“ลูกค้า” (Customer) หมายถึง บุคคลภายนอกที่มาซื้อสินค้าหรือใช้บริการของบริษัทฯ

“คู่ค้า” (Supplier) หมายถึง บุคคลภายนอกที่ทำธุรกิจซื้อ ขายสินค้าหรือบริการให้กับบริษัทฯ ทั้งในนามบุคคลหรือนิติบุคคล

“ผู้มาติดต่องาน” (Visitor) หมายถึง ผู้ที่เข้ามาติดต่องานใด ๆ ในธุรกิจของบริษัทฯ

“พนักงาน” (Employee) หมายถึง ผู้ที่บริษัทฯ ว่าจ้างเข้าทำงานประจำหรือชั่วคราวในธุรกิจของบริษัทฯ

หมายเหตุ เพื่อความสะดวกในการเรียกชื่อเจ้าของข้อมูล ในเอกสารนี้จะเรียก “กรรมการ ลูกค้า คู่ค้า ผู้มาติดต่องาน พนักงาน” ว่า “เจ้าของข้อมูล”

ข้อมูลที่ได้รับการคุ้มครอง

ข้อมูลของ กรรมการ ลูกค้า คู่ค้า หรือผู้มาติดต่องาน ที่ได้รับการคุ้มครองให้เป็นไปตามรายการและวัตถุประสงค์ที่ผู้ประมวลผลและคณะทำงานคุ้มครองข้อมูลส่วนบุคคลกำหนดและได้รับอนุมัติจากประธานเจ้าหน้าที่บริหาร

ข้อมูลของพนักงาน ที่ได้รับการคุ้มครองให้เป็นไปตามรายการและวัตถุประสงค์ที่ผู้ประมวลผลข้อมูลส่วนบุคคลของพนักงานกำหนดและได้รับอนุมัติจากประธานเจ้าหน้าที่บริหาร

การเก็บรวบรวม การใช้ การเปิดเผย การคุ้มครองข้อมูลส่วนบุคคล

- (1) บริษัทฯ จะขอเก็บข้อมูลส่วนบุคคลใด ๆ เฉพาะที่จำเป็นในการบริหารงาน หรือเพื่อประโยชน์ในการทำงานร่วมกัน หรือตามที่กฎหมายกำหนด และจะขอจากเจ้าของข้อมูลโดยตรง
- (2) บริษัทฯ จะแจ้งวัตถุประสงค์การขอข้อมูล การใช้ และการเก็บรักษาให้เจ้าของข้อมูลทราบโดยชัดแจ้ง และได้รับความยินยอมจากเจ้าของข้อมูลตั้งแต่แรก เว้นแต่เป็นข้อมูลส่วนบุคคลที่ได้รับข้อยกเว้นไม่ต้องขอความยินยอมตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนดไว้
- (3) บริษัทฯ จะใช้ข้อมูลตามวัตถุประสงค์ที่ได้รับการยินยอม โดยสุจริต เป็นความลับ จะไม่นำไปหาประโยชน์เกินจากความยินยอม และไม่ทำให้เจ้าของข้อมูลเสียหาย
- (4) รายการข้อมูลของบริษัทฯ ร้องขอจากเจ้าของข้อมูล บริษัทฯ จะคุ้มครองตามนโยบายนี้อย่างเคร่งครัดและเสมือนหนึ่งเป็นข้อมูลหรือทรัพย์สินของบริษัทฯ เอง
- (5) สถานที่เก็บและวิธีการคุ้มครองข้อมูล
 - 5.1 การเก็บเป็นเอกสาร ตู้เก็บเอกสารจะจัดให้มีกุญแจเปิด-ปิด เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
 - 5.2 การเก็บในคอมพิวเตอร์หรือระบบสารสนเทศ จะจัดให้มีรหัส (Password) เฉพาะบุคคลที่เก็บรักษาเท่านั้น
 - 5.3 หากข้อมูลใดเก็บไว้ในคอมพิวเตอร์ครบถ้วน ถูกต้อง ตรงตามเอกสาร สามารถตรวจสอบได้แล้ว อาจทำลายเอกสารนั้นก็ได้ เพื่อไม่ให้เป็นการระงับในการจัดเก็บ
- (6) ระยะเวลาในการเก็บ
 - 6.1 เอกสารที่ไม่มีการทำธุรกรรมต่อกัน เช่น ใบสมัครงานที่ไม่รับเข้าทำงาน ใบเสนอราคา ข้อเสนอ ที่ไม่ได้มีการซื้อขาย ไม่ได้ติดต่อธุรกิจกัน จะเก็บเอกสารไว้ไม่เกิน 1 ปี
 - 6.2 เอกสารที่ใช้ในการทำงาน ทำธุรกิจร่วมกัน เช่น ข้อมูลของกรรมการ ข้อมูลของพนักงานที่จ้างทำงาน ข้อมูลของลูกค้าที่ทำธุรกิจร่วมกัน จะเก็บไว้ตลอดเวลาที่ทำงาน และหลังจากสิ้นสุดการทำงานแล้วไม่เกิน 10 ปี
- (7) การเปลี่ยนแปลง การลบ และการทำลายข้อมูลที่เก็บรวบรวมไว้ บริษัทฯ จะจัดให้มีการทบทวนอนุมัติจากผู้ควบคุมข้อมูลก่อนตามเอกสารการมอบอำนาจอนุมัติให้ทำลายเอกสาร
- (8) การส่งข้อมูลไปประมวลผลภายนอก หรือการส่งให้หน่วยงานภายนอกจัดทำข้อมูลให้ เช่น สำนักงานตรวจสอบบัญชี ผู้รับจ้างทำการวิเคราะห์การตลาด การส่งข้อมูลค่าจ้างไปให้ผู้รับจ้างภายนอก การส่งข้อมูลที่ปรึกษาภายนอก หรือการส่งข้อมูลไปต่างประเทศ (ถ้ามี) บริษัทฯ จะกำกับ ควบคุมให้หน่วยงานภายนอกหรือต่างประเทศนั้นมีการคุ้มครองที่ปลอดภัย เหมาะสมเพียงพอ เพื่อให้มั่นใจว่า มีการใช้หรือการคุ้มครองเป็นไปตามนโยบายนี้ และถูกต้องตามที่กฎหมายกำหนด
- (9) การเปลี่ยนแปลง เพิ่มเติม ลบ ทำลายข้อมูลจะบันทึกไว้เพื่อตรวจสอบได้ง่ายและเชื่อถือได้

หน้าที่และความรับผิดชอบของผู้เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

- (1) ประธานเจ้าหน้าที่บริหาร มีหน้าที่ดังต่อไปนี้
 - 1.1 แต่งตั้งผู้แทนฝ่ายบริหาร หรือผู้ได้รับมอบอำนาจ หรือผู้ได้รับมอบหมายในระบบการคุ้มครองข้อมูลส่วนบุคคล
 - 1.2 แต่งตั้งผู้ประมวลผลข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องกับนโยบายและกฎหมายที่กำหนด
 - 1.3 แต่งตั้งคณะทำงานคุ้มครองข้อมูลส่วนบุคคลของลูกค้า คู่ค้า หรือผู้มาติดต่องาน ประกอบด้วยผู้จัดการฝ่าย/หัวหน้าหน่วยงานทุกหน่วยงาน เพื่อร่วมกันกำหนดข้อมูลที่จะเก็บรวบรวม ใช้ รักษาข้อมูล ตรวจสอบการใช้ข้อมูลส่วนบุคคลให้ครบ เป็นระบบเดียวกัน และสอดคล้องกับตามกฎหมาย
 - 1.4 เป็นผู้ทบทวนและอนุมัติการใช้การคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกินจากอำนาจของผู้ประมวลผลข้อมูล หรือการส่งข้อมูลไปให้หน่วยงานภายนอกหรือต่างประเทศที่เกี่ยวข้อง

- 1.5 จัดให้มีการประชุมทบทวนระบบการคุ้มครองข้อมูลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่า การคุ้มครองเป็นไปตามนโยบายนี้ หรือตามกฎหมายกำหนด
- 1.6 หากพบว่า มีการฝ่าฝืนมาตรการรักษาความปลอดภัยของบริษัทฯ จนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลรั่วไหลสู่สาธารณะ และมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล จะต้องดำเนินการแจ้งแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง และแจ้งแก่เจ้าของข้อมูลให้ทราบโดยเร็ว

(2) ผู้ตรวจสอบภายใน มีหน้าที่ดังต่อไปนี้

- 2.1 เป็นผู้แทนฝ่ายบริหารในระบบคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่บริหารจัดการระบบการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามนโยบายและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- 2.2 ปฏิบัติตามมาตรา 89/15 แห่งพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ในการจัดทำ และเก็บรักษาเอกสารดังต่อไปนี้
 - ก. ทะเบียนกรรมการ
 - ข. รายงานการมีส่วนได้เสียที่รายงานโดยกรรมการหรือผู้บริหาร
- 2.3 ร่วมกับผู้ประมวลผลข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคล เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจัดทำรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลที่จะเก็บ รวบรวม ใช้ รักษาตามความจำเป็น พร้อมเหตุผลความจำเป็นในการใช้รายงานให้ประธานเจ้าหน้าที่บริหาร พิจารณาทบทวนอนุมัติ
- 2.4 เป็นผู้พิจารณาอนุมัติการเก็บรวบรวม ใช้ รักษาข้อมูลส่วนบุคคลที่ต้องคุ้มครองพิเศษ (ตามมาตรา 26)
- 2.5 เป็นผู้พิจารณาอนุมัติการออกเอกสารรับรองข้อมูลตามที่เจ้าของข้อมูลร้องขอเพื่อประโยชน์ต่อเจ้าของข้อมูล
- 2.6 ให้คำปรึกษา แนะนำผู้จัดการ พนักงานแต่ละหน่วยงานให้ใช้ข้อมูลด้วยความระมัดระวัง เป็นความลับ ไม่ล่วงละเมิดข้อมูลส่วนบุคคลเกินกว่าที่เจ้าของข้อมูลยินยอม
- 2.7 หากพบเหตุผิดปกติในการเก็บรวบรวม ใช้ รักษาข้อมูลผิดไปจากนโยบายหรือผิดไปจากที่กฎหมายกำหนด ให้ระงับ ยับยั้งเหตุผิดปกติทันที และรายงานให้ประธานเจ้าหน้าที่บริหาร ทราบเพื่อแก้ไข ป้องกันได้ทันเหตุการณ์
- 2.8 บันทึก จัดทำรายงานการเก็บรวบรวม ใช้ รักษาข้อมูลส่วนบุคคลพร้อมรับการตรวจสอบ และ/หรือ ส่งให้หน่วยงานที่กฎหมายกำหนด
- 2.9 ทบทวน ตรวจสอบระบบการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการคุ้มครองข้อมูลส่วนบุคคลตรงตามนโยบาย หรือกฎหมายกำหนด รายงานให้ประธานเจ้าหน้าที่บริหารทราบ

(3) ผู้บังคับบัญชาของทุกหน่วยงาน มีหน้าที่ดังต่อไปนี้

- 3.1 เป็นคณะทำงานคุ้มครองข้อมูลส่วนบุคคล จัดทำรายการข้อมูล การขอ การเก็บรวบรวม ใช้ รักษาข้อมูล การตรวจสอบ และการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับนโยบาย และตามที่กฎหมายกำหนด
- 3.2 รวบรวมข้อมูลส่วนบุคคล ที่หน่วยงานของตนติดต่อกับด้วย ส่งให้ประธานเจ้าหน้าที่บริหารทบทวน/อนุมัติ
- 3.3 กำกับ ตรวจสอบ ให้พนักงานในหน่วยงานเก็บรวบรวม ใช้ รักษาข้อมูลส่วนบุคคลที่หน่วยงานตนเองเกี่ยวข้องให้เป็นไปตามนโยบายนี้ และตามที่กฎหมายกำหนด
- 3.4 อนุมัติให้มีการเพิ่มเติม เปลี่ยนแปลง ข้อมูลส่วนบุคคลตามที่ได้รับมอบอำนาจ
- 3.5 สื่อสาร ประสานงานกับเจ้าของข้อมูลให้เข้าใจนโยบายและกฎหมายนี้ และแจ้งการเปลี่ยนแปลงที่เกิดขึ้นอันอาจส่งผลกระทบต่อเจ้าของข้อมูล เพื่อร่วมกันป้องกัน แก้ไขให้ทันเหตุการณ์
- 3.6 หากพบเหตุผิดปกติให้ระงับ ยับยั้งทันที และแจ้งผู้แทนฝ่ายบริหารหรือประธานเจ้าหน้าที่บริหาร ทราบเพื่อป้องกัน แก้ไขได้ทันเหตุการณ์
- 3.7 ร่วมกันทบทวน การเก็บรวบรวม การใช้ การรักษาข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่า การคุ้มครองเป็นไปตามนโยบายนี้ หรือตามกฎหมายกำหนด และเป็นปัจจุบัน รายงานให้ประธานเจ้าหน้าที่บริหารทราบ

- (4) พนักงานที่เกี่ยวข้องกับลูกค้า คู่ค้า หรือผู้มาติดต่องาน มีหน้าที่ดังต่อไปนี้
- 4.1 เก็บรวบรวม ใช้ รักษาข้อมูลของเจ้าของข้อมูลตามวัตถุประสงค์ ตามหน้าที่โดยสุจริต ตามที่ได้รับมอบหมาย
 - 4.2 ไม่ใช้ข้อมูลเกินจากที่เจ้าของข้อมูลยินยอมไว้แต่แรก ไม่นำไปหาประโยชน์ส่วนตน ไม่ทำให้เจ้าของข้อมูลเสียหาย
 - 4.3 หากจะเปลี่ยนแปลง แก้ไขข้อมูลที่คุ้มครองไว้ ต้องได้รับการทบทวน/อนุมัติจากผู้จัดการต้นสังกัดหรือประธานเจ้าหน้าที่บริหาร ตามลำดับการมอบอำนาจ ห้ามไม่ให้แก้ไข เปลี่ยนแปลงโดยพลการ
 - 4.4 หากพบเหตุการณ์ผิดปกติในการใช้ การคุ้มครองข้อมูลให้ระงับ ยับยั้งทันที และแจ้งให้ผู้จัดการต้นสังกัดหรือประธานเจ้าหน้าที่บริหาร ทราบโดยเร็ว
 - 4.5 บันทึกการใช้ การเปลี่ยนแปลงข้อมูลไว้เพื่อการตรวจสอบ

(5) แผนกเทคโนโลยีดิจิทัล มีหน้าที่ดังต่อไปนี้

- 5.1 เป็นผู้ประมวลผลข้อมูลส่วนบุคคลของลูกค้า คู่ค้า ผู้มาติดต่องาน
- 5.2 ร่วมกับคณะทำงาน ดำเนินการหรือให้คำแนะนำวิธีการเก็บข้อมูลส่วนบุคคลทั้งข้อมูลของกรรมการ ลูกค้า คู่ค้า ผู้มาติดต่องาน หรือข้อมูลของพนักงาน ลงในระบบสารสนเทศอย่างเป็นความลับ และมีการดำเนินการสำรองข้อมูลตามที่ระบุไว้ในคู่มือการปฏิบัติงาน แผนกศูนย์ระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่า ข้อมูลอยู่ครบ ไม่ถูกลบ ไม่ถูกละเมิด ไม่ถูกทำลาย สามารถตรวจสอบข้อมูล วัน เวลา ที่มีการใช้ได้ทันเหตุการณ์
- 5.3 มอบหมายและกำกับ ตรวจสอบ ให้เจ้าหน้าที่แผนกเทคโนโลยีดิจิทัล กำหนดรหัสผ่านหรือรหัสลับเฉพาะ เช่น Bar Code, Finger Scan เป็นต้น รวมถึงช่วยเหลือผู้ควบคุมข้อมูลส่วนบุคคล คณะทำงาน และ/หรือ พนักงานที่เกี่ยวข้องในการเก็บ ใช้ การประมวลผลข้อมูลส่วนบุคคล ลงในระบบสารสนเทศ อย่างเป็นความลับ
- 5.4 กำหนดรหัสผ่านให้ผู้ที่ใช้คอมพิวเตอร์หรือสื่ออิเล็กทรอนิกส์อื่น ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเฉพาะคนอย่างเป็นความลับ
- 5.5 บันทึก ตรวจสอบ การใช้ข้อมูลส่วนบุคคลประจำวัน
- 5.6 ให้คำแนะนำ ช่วยเหลือผู้แทนฝ่ายบริหาร ผู้ประมวลผลข้อมูลส่วนบุคคล และพนักงานที่เกี่ยวข้องทุกคน เก็บ ใช้ รักษาข้อมูลให้ตรงตามนโยบายและกฎหมายที่กำหนด
- 5.7 หากพบเหตุผิดปกติในการเก็บรักษา การใช้ข้อมูลผิดไปจากนโยบายหรือผิดไปจากที่กฎหมายกำหนดให้ระงับยับยั้งเหตุผิดปกติทันที และรายงานผู้จัดการต้นสังกัดทราบทันที เพื่อแก้ไข ป้องกันได้ทันเหตุการณ์

(6) ผู้จัดการแผนกทรัพยากรบุคคล มีหน้าที่ดังต่อไปนี้

- 6.1 เป็นผู้ประมวลผลข้อมูลส่วนบุคคลของพนักงาน ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ภายในขอบเขต และตามความจำเป็นในการบริหารงานบุคคล
- 6.2 กำหนดรายการ วัตถุประสงค์ วิธีการขอข้อมูลให้พนักงานทราบและยินยอมแต่แรกจ้าง หรือขอเพิ่มระหว่างการทำงาน ยกเว้นการขอเพื่อทดแทนฉบับเดิมที่หมดอายุ หรือเป็นการเปลี่ยนแปลงข้อมูลโดยเจ้าของข้อมูล เช่น สถานะสมรส ย้ายทะเบียนบ้าน เป็นต้น
- 6.3 กำหนดผู้เก็บ ใช้ ผู้รักษาข้อมูลในงานบุคคล รายละเอียดตามหนังสือมอบหมายงานพนักงานแผนกทรัพยากรบุคคล
- 6.4 ควบคุม กำกับการส่งเอกสารไปให้หน่วยงานราชการหรือหน่วยงานภายนอก เช่น ส่งเงินสมทบประกันสังคม ส่งรายการหักภาษี ณ ที่จ่ายให้สรรพากร ส่งเอกสารพนักงานให้กระทรวงแรงงาน ส่งเงินพนักงานให้กรมบังคับคดี หรือให้หน่วยงานอื่นตามที่กฎหมายกำหนด
- 6.5 เป็นผู้ควบคุมการเก็บ การใช้ข้อมูลส่วนบุคคลอ่อนไหวที่ต้องคุ้มครองพิเศษ เช่น ข้อมูลด้านสุขภาพการเจ็บป่วยของพนักงาน ประวัติอาชญากรรม ลัทธิความเชื่อทางศาสนา หรือข้อมูลอื่น ๆ ตามที่กฎหมายกำหนด ไว้เป็นการเฉพาะ เพื่อให้มีการใช้เท่าที่จำเป็น เป็นความลับและได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง
- 6.6 เป็นผู้เก็บดูแลสำรองหรือรับรู้รหัสผ่านเข้าระบบคอมพิวเตอร์ของผู้เก็บ ผู้ใช้ข้อมูล เพื่อใช้ในกรณีเร่งด่วนฉุกเฉิน
- 6.7 เป็นผู้พิจารณาอนุมัติการเปลี่ยน การเพิ่มเติม การขอใช้ข้อมูลส่วนบุคคลของพนักงานที่จำเป็นในงานของบริษัทฯ หรือที่เป็นประโยชน์ต่อเจ้าของข้อมูล
- 6.8 บันทึก จัดทำรายงานการคุ้มครองข้อมูลส่วนบุคคลของพนักงานไว้เพื่อการตรวจสอบ หรือส่งให้หน่วยงานราชการที่เกี่ยวข้อง

- 6.9 ทบทวน ตรวจสอบ และสรุปการคุ้มครองข้อมูลส่วนบุคคลของพนักงานให้ประธานเจ้าหน้าที่บริหารพิจารณาอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของพนักงานได้รับการเก็บรักษา ใช้ตรงตามนโยบายหรือกฎหมายกำหนด
- 6.10 หากพบเหตุผิดปกติในการเก็บรักษา การใช้ข้อมูลผิดไปจากนโยบายหรือผิดไปจากที่กฎหมายกำหนดให้ระงับยับยั้งเหตุผิดปกติทันที และรายงานผู้จัดการต้นสังกัดทราบทันที เพื่อแก้ไข ป้องกันได้ทันเหตุการณ์
- 6.11 เป็นผู้ประมวลผลข้อมูล ใช้ เก็บรักษาข้อมูลส่วนบุคคลเกี่ยวกับค่าจ้าง สวัสดิการ ประกันสังคม ภาษีเงินได้ของพนักงานแต่ละคน
- 6.12 เป็นผู้มีสิทธิขอเอกสารข้อมูลส่วนบุคคลเพิ่มเติม เพื่อคำนวณภาษีประจำปี หรือเพื่อจัดสวัสดิการเพิ่มเติมระหว่างปี
- 6.13 เป็นผู้ออกหนังสือรับรองค่าจ้างหรือข้อมูลอื่นที่เจ้าของข้อมูลร้องขอ
- 6.14 เก็บรักษาข้อมูลเกี่ยวกับค่าจ้างไว้ตลอดเวลาตามที่สรรพากรกำหนด
- 6.15 บันทึกการใช้ การเปลี่ยนแปลง การเก็บ และการรักษาข้อมูลไว้เพื่อการตรวจสอบเพื่อให้มั่นใจว่าปฏิบัติตามนโยบายนี้

(7) พนักงานแผนกทรัพยากรบุคคลที่ทำหน้าที่รับสมัครพนักงาน มีหน้าที่ดังต่อไปนี้

- 7.1 เป็นผู้เก็บ ประมวลผลข้อมูล บันทึก รักษา และใช้ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการสมัครงาน
- 7.2 เก็บประวัติของผู้สมัครงาน ที่รับเข้าทำงาน โดยให้เก็บไว้ตลอดเวลาและไม่เกิน 10 ปีหลังจากที่พ้นสภาพการเป็นพนักงาน หรือจนกว่าคดีจะสิ้นสุด (ถ้ามี)
- 7.3 ข้อมูลของผู้สมัครงานที่ไม่รับเข้าทำงาน ให้เก็บรักษาไม่เกิน 6 เดือน
- 7.4 วิธีการทำลายข้อมูล ให้ใช้วิธีย่อย หรือเผาทำลาย หรือวิธีการอื่น ที่มั่นใจว่าไม่มีบุคคลอื่นล่วงรู้ในข้อมูลนั้น
- 7.5 เก็บกุญแจหรือรหัสผ่าน ที่เกี่ยวข้องกับการเก็บข้อมูล
- 7.6 บันทึกการใช้ การเปลี่ยนแปลง การเก็บ และการรักษาข้อมูลไว้เพื่อการตรวจสอบเพื่อให้มั่นใจว่าปฏิบัติตามนโยบายนี้

(8) เจ้าหน้าที่ความปลอดภัยวิชาชีพ มีหน้าที่ดังต่อไปนี้

- 8.1 เก็บข้อมูลการเจ็บป่วยของพนักงานไว้เป็นความลับ
- 8.2 ประสานงานกับแพทย์หรือหน่วยงานที่เกี่ยวข้องเพื่อการรักษาหรือทำตามกฎหมายกำหนด

สิทธิการเข้าถึงข้อมูลของเจ้าของข้อมูลส่วนบุคคล

- (1) สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access) เจ้าของข้อมูลมีสิทธิในการขอเข้าถึงและขอให้บริษัทฯ ทำสำเนาข้อมูลส่วนบุคคลดังกล่าวให้กับเจ้าของข้อมูลได้ รวมถึงขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอมต่อบริษัทฯ ได้
- (2) สิทธิในการโอนย้ายข้อมูลส่วนบุคคล (right to data portability) เจ้าของข้อมูลมีสิทธิในการขอ รับ ส่ง หรือโอนข้อมูลส่วนบุคคลที่ได้ให้ไว้กับบริษัทฯ ไปยังผู้ควบคุมข้อมูลส่วนบุคคลรายอื่น หรือเจ้าของข้อมูลเอง ด้วยเหตุผลบางประการได้
- (3) สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object) เจ้าของข้อมูลมีสิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล ด้วยเหตุผลบางประการได้
- (4) สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure) เจ้าของข้อมูลมีสิทธิในการขอให้บริษัทฯ ดำเนินการลบหรือทำลายด้วยเหตุผลบางประการได้
- (5) สิทธิในการระงับการใช้ข้อมูลส่วนบุคคล (right to restriction of processing) เจ้าของข้อมูลมีสิทธิระงับการใช้ข้อมูลส่วนบุคคล ด้วยเหตุผลบางประการได้
- (6) สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification) เจ้าของข้อมูลมีสิทธิในการขอให้บริษัทฯ แก้ไขข้อมูลส่วนบุคคลที่ไม่ถูกต้อง หรือเพิ่มเติมข้อมูลส่วนบุคคลที่ไม่สมบูรณ์ได้
- (7) สิทธิในการเพิกถอนความยินยอม (right to withdraw consent) เจ้าของข้อมูลส่วนบุคคลมีสิทธิเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมได้ตลอดระยะเวลาที่ข้อมูลส่วนบุคคลของตนอยู่กับบริษัทฯ

การร้องขอสิทธิตามรายการข้างต้นนั้น เจ้าของข้อมูลจะต้องกระทำการยื่นคำร้องขอในเรื่องต่าง ๆ เป็นลายลักษณ์อักษรตามหลักเกณฑ์และวิธีการที่บริษัทฯ กำหนด และเมื่อได้รับคำร้องแล้ว บริษัทฯ จะดำเนินการบันทึกคำร้องต่าง ๆ ไว้เป็นหลักฐาน ทั้งนี้ บริษัทฯ จะดำเนินการภายในระยะเวลาที่สมเหตุสมผล แต่ไม่เกินระยะเวลาตามที่กฎหมายกำหนด

ทั้งนี้ ข้อจำกัดในการให้บริการหรือประมวลผลข้อมูลส่วนบุคคลด้านต่าง ๆ ในกรณีที่เจ้าของข้อมูลขอให้บริษัทฯ ลบ ทำลาย ระบุ ปิดกั้น ขอให้โอน หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้ หรือถอนความยินยอม อาจทำให้เกิดข้อจำกัดกับบริษัทฯ ในการทำธุรกรรม หรือการให้บริการกับเจ้าของข้อมูลในบางกรณีได้ ทั้งนี้ ภายใต้ข้อกำหนด เงื่อนไขของการยินยอมด้านต่าง ๆ และตามที่กฎหมายกำหนด

อย่างไรก็ตาม บริษัทฯ จะปฏิบัติตามที่กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ เว้นแต่เป็นการขัดหรือแย้งกับบทบัญญัติแห่งกฎหมาย หรือกระทบต่อความมั่นคงแห่งราชอาณาจักร หรือกระทบต่อเศรษฐกิจและการพาณิชย์ของประเทศ หรือมีผลต่อการสืบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย หรือการพิจารณาพิพากษาคดีของศาล หรือกระทบต่อสิทธิและเสรีภาพของบุคคลอื่น

บทกำหนดโทษ

เมื่อผู้มีหน้าที่รับผิดชอบในการดำเนินงานเรื่องใดเรื่องหนึ่งตามหน้าที่ของตน หากละเลย หรือละเว้นไม่สั่งการ หรือไม่ดำเนินการ หรือดำเนินการอย่างใดอย่างหนึ่งในหน้าที่ของตน อันเป็นการฝ่าฝืนนโยบายและแนวปฏิบัติเกี่ยวกับเรื่องการคุ้มครองข้อมูลส่วนบุคคล จนเป็นเหตุให้เกิดความผิดตามกฎหมาย และ/หรือ ความเสียหายขึ้น ผู้นั้นจะได้รับโทษ ดังต่อไปนี้

- (1) ผู้ใดทำการใช้ เปิดเผย ละเมิดข้อมูลส่วนบุคคลของผู้อื่น หรือนำไปใช้ประโยชน์ส่วนตัวโดยไม่ได้รับอนุมัติจากผู้ควบคุมข้อมูลส่วนบุคคล หรือจากเจ้าของข้อมูลส่วนบุคคล บริษัทฯ ถือว่า ผู้นั้นทุจริตต่อหน้าที่ จึงใจทำให้บริษัทฯ ได้รับความเสียหาย ละเมิดสิทธิส่วนบุคคลทำให้บุคคลอื่นเสียหาย ถือเป็นความผิดร้ายแรง อาจลงโทษถึงขั้นเลิกจ้างโดยไม่จ่ายค่าชดเชยใด ๆ
- (2) ผู้ใดที่บริษัทฯ มอบหมายให้มีหน้าที่ควบคุมข้อมูล เก็บรักษา ประมวลผล ใช้ข้อมูล ถือเป็นพนักงานเจ้าหน้าที่ หากกระทำความผิดเสียเองจะถูกพิจารณาลงโทษในอัตราสูงกว่าพนักงานทั่วไป
- (3) ผู้ใดที่ไม่นำส่งข้อมูลส่วนบุคคลที่บริษัทฯ ร้องขอ หรือให้ข้อมูลเท็จ ถือว่าเป็นการทุจริตต่อหน้าที่ จึงใจทำให้บริษัทฯ ได้รับความเสียหาย บริษัทฯ จะลงโทษทางวินัยหรืออาจลงโทษถึงขั้นเลิกจ้างโดยไม่จ่ายค่าชดเชยใด ๆ ตามเห็นสมควร
- (4) ผู้ใดละเมิด ไม่ปฏิบัติตามนโยบายและแนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนี้ หากเกิดความเสียหายใด ๆ ผู้นั้นจะต้องชดใช้ความเสียหายด้วยตนเองเต็มจำนวนตามที่กฎหมายกำหนด ทั้งนี้หากความผิดดังกล่าวก่อให้เกิดความเสียหายแก่บริษัทฯ และ/หรือ บุคคลอื่นใด บริษัทฯ อาจพิจารณาดำเนินคดีตามกฎหมายเพิ่มเติมต่อไป

การทบทวนนโยบายการคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ จะทำการพิจารณาทบทวนข้อมูลส่วนบุคคลที่เก็บไว้อย่างน้อยปีละ 1 ครั้ง หรือกรณีที่กฎหมายมีการเปลี่ยนแปลงแก้ไข เพื่อให้สอดคล้องกับแนวปฏิบัติ ข้อบังคับ และกฎหมายอื่นที่เกี่ยวข้อง

กรณีมีการเปลี่ยนแปลงนโยบายการคุ้มครองข้อมูลส่วนบุคคล บริษัทฯ จะแจ้งให้ทราบผ่านอีเมลและผ่านเว็บไซต์ของบริษัทฯ โดยเร็วที่สุด

ช่องทางการติดต่อ

หากต้องการสอบถามข้อมูลเพิ่มเติมหรือมีเหตุร้องเรียนเกี่ยวกับข้อมูลส่วนบุคคล สามารถติดต่อได้ที่ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ผู้ตรวจสอบภายใน บริษัทฯ ฟรอนท์ไลน์ เอ็นจิเนียริ่ง จำกัด (มหาชน) เลขที่ 409 ถนนบอนด์สตรีท ตำบลบางพูด อำเภอปากเกร็ด จังหวัดนนทบุรี 11120 โทรศัพท์ (662) 960 1145 โทรสาร (662) 960 1147 Email : contact@front-line.co.th

นโยบายและระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลนี้ มีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2568 เป็นต้นไป



(นายปัญญา บุญญาภิวัฒน์)
ประธานกรรมการบริษัท