นโยบายคุ้มครองข้อมูลส่วนบุคคล

บริษัท สินมั่นคงประกันภัย จำกัด (มหาชน)

นโยบายคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการของบริษัท เห็นถึงความสำคัญ ในการประมวลผลข้อมูลส่วนบุคคลให้เหมาะสมและถูกต้องตามกฎหมาย คณะกรรมการบริษัท จึงได้มีมติอนุมัติรับรองและออกประกาศบริษัทเรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล ฉบับนี้ขึ้น เพื่อกำหนดกรอบการประมวลผลข้อมูลส่วนบุคคลในกระบวนการต่างๆ ของบริษัท ไม่ให้กระทบสิทธิของเจ้าของข้อมูลมากเกินไป โดยรับประกันให้ เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการการประมวลผลข้อมูลดังกล่าว ให้ถูกต้องตามมาตรฐานที่ระบุไว้โดยหน่วยงานกำกับดูแล และเพื่อให้พนักงานและบุคคลที่เกี่ยวข้องของบริษัทยึดถือและปฏิบัติ ตามให้เป็นไปตามพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) และมาตรฐานที่กำหนดไว้

ข้อ 1 ประกาศและผลบังคับใช้ของประกาศ

ประกาศฉบับนี้เรียกว่า“นโยบายคุ้มครองข้อมูลส่วนบุคคล” โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 9 พฤษภาคม 2566 เป็นต้นไป

ข้อ 2 คู่มือและคำแนะนำในการปฏิบัติตามประกาศ

โดยอาศัยอำนาจของนโยบายฉบับนี้ บริษัทอาจพิจารณากำหนดและประกาศคู่มือการปฏิบัติงานโดยละเอียด เพื่อกำหนดแนวทางการปฏิบัติต่างๆ ด้วยจุดประสงค์รับประกันความสมบูรณ์ ถูกต้อง และครบถ้วนในการคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้องเพิ่มเติม โดยให้คู่มือการปฏิบัติงานดังกล่าวมีผลบังคับสมบูรณ์เช่นเดียวกันกับประกาศฉบับนี้

ข้อ 3 โครงสร้างการบริหารจัดการและกำกับการประมวลผลข้อมูลส่วนบุคคล

เพื่อให้การกำกับดูแลและบริหารจัดการด้านการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล ให้สมบูรณ์ถูกต้องสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัทกำหนดจัดตั้งโครงสร้างดังนี้

3.1. คณะกรรมการบริษัท มีหน้าที่รับผิดชอบในการกำหนดทิศทางและการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในภาพรวมของบริษัทและบริหารจัดการความเสี่ยงต่างๆ ที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคล โดยมีบทบาทหลักในการตรวจสอบและอนุมัติทุกนโยบายย่อยและคู่มือแนวทางการปฏิบัติที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

3.2. ประธานเจ้าหน้าที่ฝ่ายบริหาร (CEO) รับผิดชอบโดยตรงในการกำกับดูแลการปฏิบัติงานการประมวลผลข้อมูลส่วนบุคคลโดยรวมของบริษัทผ่านการกำกับดูแลและการรายงานของหัวหน้าหน่วยงานหรือผู้จัดการฝ่ายที่เกี่ยวข้องภายใต้การมอบหมายและการชี้นำของคณะกรรมการบริษัท

3.3. เพื่อการกำกับดูแลการปฏิบัติงานประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามนโยบายและกฎหมาย บริษัทได้กำหนดการประมวลผลข้อมูลส่วนบุคคลภายใต้รูปแบบโครงสร้าง 3 Lines of Defense ดังนี้

- 1st Line of Defense: Risk Owner ได้แก่ ประธาน หรือหัวหน้าฝ่าย/หน่วยงาน ซึ่งมีหน้าที่รับผิดชอบ โดยตรงในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของพนักงานภายในหน่วยงานของตน ให้ถูกต้องและสอดคล้องกับนโยบายและกฎหมายที่เกี่ยวข้อง โดยเฉพาะ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- 2nd Line of Defense: Risk Control กำหนดให้มีการแต่งตั้งคณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Working Committee) ซึ่งประกอบด้วยหัวหน้าฝ่ายที่มีการประมวลผลข้อมูลส่วนบุคคลต่างๆ ในบริษัท ทำงานร่วมกับหน่วยงานกำกับดูแลการปฏิบัติงาน (Compliance) โดยการทำงานของคณะกรรมการ มีความเป็นไปอิสระภายใต้หลักการ maker-checker ดังนั้น กรณีการตรวจสอบการทำงานฝ่ายงานใด หัวหน้าฝ่ายงานดังกล่าวย่อมไม่มีสิทธิในการแทรกแซงหรือให้คำแนะนำใด โดยให้ดำเนินการรายงานโดยตรงไปยังประธานเจ้าหน้าที่ฝ่ายบริหาร
- 3rd Line of Defense: Risk Assurance ได้แก่ คณะกรรมการตรวจสอบ (Audit Committee) ซึ่งมีหน้าที่กำกับ ดูแลและตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลของทุกหน่วยงานอีก

3.4. บริษัทกำหนดให้มีการจัดสรรทรัพยากรอย่างเพียงพอ ในการสนับสนุนการปฏิบัติงานของแต่ละหน่วยงานให้เป็นไปตามนโยบายและมาตรฐานการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลในทุกส่วน โดยจัดให้มีทรัพยากรที่จำเป็นทั้งในแง่ของระบบงานบุคลากร และงบประมาณ

ข้อ 4 การประเมินและบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

4.1. บริษัทกำหนดให้มีการประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล เพื่อตรวจสอบความพร้อมและความถูกต้อง ในการประมวลผลข้อมูลตามกฎหมายในภาพรวมขององค์กร (Enterprise Risk Management) อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่เพิ่มเติมรูปแบบการประมวลผลข้อมูลส่วนบุคคลจากที่ได้ประเมินไว้ภายใต้หลักการที่กำหนดให้แต่ละหน่วยงานที่เกี่ยวข้องในโครงสร้างการกำกับดูแล มีหน้าที่และความรับผิดชอบในกระบวนการประเมินการบริหารจัดการความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลภายในหน่วยงานของตน รวมถึง การติดตามและรายงานผลด้านความเสี่ยงให้แก่หน่วยงานกำกับดูแลตามที่กำหนดไว้และรายงานต่อคณะกรรมการบริษัท

4.2. บนพื้นฐานการประเมินความเสี่ยงในระดับองค์กร สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบถึงสิทธิเสรีภาพของบุคคล ซึ่งอาจนำไปสู่การเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญของเจ้าของข้อมูลส่วนบุคคล หรือที่จะทำให้เจ้าของข้อมูลไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ บริษัทกำหนดให้มีการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ Data Processing Impact Assessment เพิ่มขึ้น ก่อนการตัดสินใจดำเนินการประมวลผลข้อมูลส่วนบุคคลกรณีดังกล่าว

4.3. ในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล บริษัทดำเนินการภายใต้หลักการ ดังนี้

1) มีการอธิบายรายละเอียดการประมวลผลข้อมูลดังกล่าว ซึ่งระบุถึงขอบเขตการประเมินผล วัตถุประสงค์ความจำเป็นในการประมวลผลข้อมูลดังกล่าว

2) มีกระบวนการปรึกษาหารือกับผู้มีส่วนเกี่ยวข้องต่างๆ ได้แก่ เจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง โดยจัดทำกระบวนการปรึกษาหารือทั้งภายในและภายนอกองค์กร
3) มีคำอธิบายที่ชัดเจนเกี่ยวกับความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล
4) จัดให้มีการประเมินความเสี่ยงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยคำนึงถึง “ความน่าจะเป็น” (likelihood) และ “ความรุนแรงของผลกระทบ” (severity)
5) รายละเอียดมาตรการในการลดความเสี่ยงที่ระบุไว้ ทั้งนี้ มีการจดบันทึกและจัดทำรายงานการประเมินอย่างเป็นขั้นตอน

ข้อ 5 การสื่อสารประชาสัมพันธ์นโยบาย

บริษัทให้ความสำคัญต่อการสื่อสารนโยบายและแนวทางการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลให้แก่พนักงานของบริษัท โดยได้มีการสื่อสารผ่านทุกช่องทางการติดต่อกับพนักงาน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญและกระทบต่อการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท

ข้อ 6 การกำกับดูแลและตรวจสอบ

บริษัทได้กำหนดให้มีการติดตามและตรวจสอบการปฏิบัติตามนโยบายการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักการดังนี้

6.1. กำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่หลักในการติดตามและตรวจสอบการปฏิบัติตามนโยบายและมาตรการการประมวลผลข้อมูลส่วนบุคคล และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่บริษัทกำหนด และการรายงานผลการติดตามและตรวจสอบต่อประธานเจ้าหน้าที่ฝ่ายบริหาร และรายงานต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือกรณีมีการละเมิดอย่างมีนัยสำคัญต่อธุรกิจ หรือชื่อเสียงของบริษัท

6.2. กำหนดให้มีแผนการตรวจสอบด้านการประมวลผลข้อมูลส่วนบุคคลของบริษัท พร้อมทั้งรายงานผลการตรวจสอบด้านความเสี่ยงต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอันสำคัญในบริษัท

6.3. กรณีที่ตรวจพบการฝ่าฝืนนโยบายและมาตรการการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคลจะเป็นหน่วยงานรับเรื่องร้องเรียน กำกับดูแลหลัก รวมถึงทำหน้าที่ตรวจสอบจนทราบข้อเท็จจริง หากพบว่าเกิดการฝ่าฝืนหรือละเมิดนั้นจริง คณะทำงานจะเสนอไปยังประธานเจ้าหน้าที่ฝ่ายบริหาร (CEO) หรือกรรมการ แล้วแต่ความรุนแรงของการละเมิด และตำแหน่งของผู้ที่กระทำผิดเพื่อพิจารณากำหนดมาตรการลงโทษตามข้อกำหนดที่ระบุไว้ ตามการลงโทษทางวินัยตามระเบียบบริหารงานบุคคลต่อไป

ข้อ 7 การจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล (Report of Processing) และนโยบายการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก (Information Disclosure Policy)

บริษัทกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการข้อมูลส่วนบุคคล โดยจัดระดับความลับของข้อมูลดังกล่าวเป็น "ข้อมูลความลับที่สุด (Strictly Confidential)" ภายใต้หลักการในการรักษาความลับของบริษัท โดยดำเนินการบริหารจัดการข้อมูลดังกล่าวภายใต้หลักการ ดังนี้

7.1. กำหนดให้แต่ละฝ่ายงานหรือหน่วยงานที่มีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล และปรับปรุงรายการการประมวลผลข้อมูลดังกล่าวอย่างสม่ำเสมอ รวมทั้งระบุข้อกำหนดในการประมวลผลข้อมูลส่วนบุคคลให้พนักงานภายในฝ่ายงานของตนรับทราบ เพื่อให้มั่นใจว่า พนักงานดังกล่าวตระหนักรู้ถึงความสำคัญของสิทธิของเจ้าของข้อมูล รวมถึงหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งหมดนั้น

7.2. บริษัทกำหนดนโยบายให้การประมวลผลข้อมูลส่วนบุคคลทั้งหมดดำเนินการผ่านระบบอิเล็กทรอนิกส์ ที่ควบคุมการเข้าถึงและบันทึกการเข้าถึงได้มากกว่าการจัดเก็บข้อมูลเป็นกระดาษ ในกรณีใช้ข้อมูลส่วนบุคคลในรูปแบบของกระดาษ ได้มีการจัดทำบันทึกการใช้ข้อมูลและมีนโยบาย Clean Desk โดยห้ามนำกระดาษที่มีข้อมูลส่วนบุคคลไปใช้ซ้ำ (Recycled) และกำหนดให้มีการจัดเก็บใส่กล่องให้เรียบร้อยและกำหนดระยะเวลาการเก็บข้อมูลดังกล่าว และหากมีการเคลื่อนย้ายข้อมูลดังกล่าว ได้กำหนดให้มีการดำเนินการตามกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล

7.3. ในกรณีที่มีความจำเป็นต้องส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกองค์กร บริษัทได้กำหนดให้มีการดำเนินการ ดังนี้

- มีการตรวจสอบความจำเป็น รวมถึงความเสี่ยงในการส่งต่อข้อมูลส่วนบุคคลและความน่าเชื่อถือของผู้รับข้อมูลส่วนบุคคลดังกล่าวก่อน
- การส่งต่อหรือเปิดเผยแต่ละครั้งต้องได้รับความยินยอมจากผู้บังคับบัญชาตามอำนาจการอนุมัติ
- กำหนดให้พนักงานทุกคน และทุกหน่วยงานมีหน้าที่การบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล การส่งต่อเปิดเผยข้อมูลออกไปนอกองค์กรดังกล่าว
- พนักงานผู้เปิดเผยหรือส่งต่อข้อมูล ต้องปฏิบัติตามช่องทางและวิธีการส่งต่อหรือเปิดเผยข้อมูลที่บริษัทกำหนดเพื่อให้มีความเสี่ยงด้านความมั่นคงปลอดภัยน้อยที่สุด รวมถึงหลีกเลี่ยงการส่งผ่านช่องทางส่วนตัวที่ไม่สามารถควบคุมได้
- กำหนดให้มีการลงนามในสัญญา หรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทและบุคคลภายนอกดังกล่าว เพื่อกำหนดเงื่อนไขข้อกำหนดสิทธิและหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลระหว่างคู่สัญญา และรับประกัน ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว

ข้อ 8 การกำหนดระยะเวลาการรักษาข้อมูล (Data Retention Guideline)

8.1. บริษัทได้กำหนดกรอบการพิจารณาระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Data Retention Guideline) โดย พิจารณาตามหลักการความจำเป็นเป็นสำคัญภายใต้กรอบการพิจารณาความจำเป็น ดังนี้

- หากมีระยะเวลาตามกฎหมาย ระบุชัดเจนให้เก็บรักษาข้อมูลส่วนบุคคลส่วนใดไว้เป็นระยะเวลานานเท่าใด บริษัทกำหนดให้มีการจัดเก็บตามกำหนดเวลานั้น และในกรณีการเก็บรักษาข้อมูลส่วนบุคคลส่วนใดอยู่ภายใต้เกณฑ์การเก็บรักษาของกฎหมายที่แตกต่างกัน บริษัทกำหนดกรอบการเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นระยะเวลาตามกรอบเวลาสูงสุดที่กฎหมายทั้งหมดกำหนดไว้
- กรณีเป็นการเก็บข้อมูลส่วนบุคคล เนื่องจากความจำเป็นที่พิจารณาโดยอาศัยความสัมพันธ์ต่างๆ ที่บริษัทมีกับเจ้าของข้อมูล เช่น ด้วยฐานสัญญาให้เก็บข้อมูลไว้เท่าที่จำเป็นเพื่อการปฏิบัติตามหน้าที่ในสัญญา กำหนดระยะเวลา ในการเก็บรักษาข้อมูลดังกล่าวตลอดระยะเวลาการให้บริการ หรือตราบเท่าที่จะมีการยกเลิกสัญญา หรือความสัมพันธ์ที่เกี่ยวข้อง ซึ่งอาจมีระยะเวลาแน่นอนหรือไม่ก็เป็นได้ แต่ต้องมีการกำหนดกรอบระยะเวลาการเก็บรักษาที่ชัดเจนแน่นอนซึ่งคาดหมายได้โดยเจ้าของข้อมูล
- กรณีเป็นการเก็บข้อมูลเพื่อประโยชน์อันชอบธรรม ได้ดำเนินการเก็บข้อมูลดังกล่าวไว้ตามกรอบที่เหมาะสมเพื่อการใช้สิทธิในแต่ละกรณีดังกล่าว เช่น ตามระยะเวลาอายุความ กรณีการฟ้องร้องต่อสู้สิทธิต่างๆ ทั้งนี้หลักการสำคัญที่ได้พิจารณาคือ การประมวลผลข้อมูลส่วนบุคคลดังกล่าวต้องไม่กระทบสิทธิของเจ้าของข้อมูลมากเกินสมควร และบริษัทได้กำหนดให้สิทธิเจ้าของข้อมูลในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยฐานดังกล่าวได้ตามสิทธิที่มี
- กรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานความยินยอมให้เก็บข้อมูลได้ ตราบเท่าที่เจ้าของข้อมูลยังไม่ได้ใช้สิทธิในการถอนความยินยอม ซึ่งเป็นสิทธิอิสระที่เจ้าของข้อมูลสามารถดำเนินการได้ ตลอดระยะเวลาตามสิทธิที่ตนเองมี และบริษัทเคารพสิทธิในการตัดสินใจดังกล่าว
- กรณีข้อมูลส่วนบุคคลที่บริษัทประมวลผลเป็นข้อมูลส่วนบุคคลอ่อนไหว เช่น ประวัติอาชญากรรม หรือประวัติ สุขภาพการรักษาพยาบาล หรือข้อมูลชีวภาพอื่นๆ บริษัทได้ใช้ความระมัดระวังในการบริหารจัดการและประมวลผลข้อมูลส่วนบุคคลด้วยมาตรฐานที่สูงขึ้น โดยเฉพาะระยะเวลาในการทำลายข้อมูลดังกล่าวและจำกัดเวลาให้มีการลบหรือทำลายในทันทีที่หมดความจำเป็น

8.2. เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลตามกรอบที่กำหนดไว้แล้ว บริษัทจะลบทำลายข้อมูลส่วนบุคคลดังกล่าว หรือดำเนินการทำให้ข้อมูลกลายเป็นข้อมูลนิรนามขึ้นอยู่กับลักษณะของข้อมูล ซึ่งบริษัทกำหนดรอบในการทำลายเอกสารที่ครบกำหนดความจำเป็นเป็นรายปีปฏิทิน ทั้งนี้ สำหรับการทำลายข้อมูลที่อยู่ในรูปแบบกระดาษ บริษัทกำหนดให้ผู้ให้บริการภายนอกเป็นผู้ดำเนินการดังกล่าว โดยงรับประกันการจัดทำข้อตกลงและเงื่อนไขการประมวลผลข้อมูลส่วนบุคคล และได้รับการประกันความสมบูรณ์ในการทำลายเอกสารดังกล่าว นอกจากนี้ สำหรับข้อมูล

อิเล็กทรอนิกส์ได้ดำเนินการทำลายทางเทคนิคอย่างเหมาะสม และหากมีการบันทึกข้อมูลดังกล่าวในอุปกรณ์หรือเครื่องมืออื่น เช่น USB หรือคอมพิวเตอร์ใดๆ ได้ใช้ความพยายามอย่างที่สุดในการทำลายข้อมูลดังกล่าวทั้งหมด ตามบันทึกรายการการประมวลผลข้อมูลที่มีการจัดเก็บไว้

8.3. สำหรับกระบวนการในการบริหารจัดการเอกสาร บริษัทกำหนดกระบวนการ ดังนี้

- ฝ่ายงานที่รับผิดชอบข้อมูลและเอกสารดังกล่าว มีหน้าที่ในการตรวจสอบเอกสารที่ถึงกำหนดเคลื่อนย้ายหรือทำลายตามนโยบายการเก็บรักษาที่ได้ประกาศไว้
- เมื่อถึงกำหนดระยะเวลาการเคลื่อนย้ายหรือทำลาย ฝ่ายนั้นต้องปิดกล่องผนึกพร้อมลงวันที่ และแจ้งส่งกล่องเอกสารดังกล่าวเพื่อให้ฝ่ายบริหารสำนักงาน ซึ่งจะทำหน้าที่เพียงการบริหารจัดการการเข้า-ออกของเอกสาร
- กรณีการเคลื่อนย้ายเอกสารไปโกดัง หรือการทำลายเอกสารได้กำหนดให้มีตัวแทนของฝ่ายงานที่เกี่ยวข้อง ซึ่งเป็นเจ้าของข้อมูล และฝ่ายบริหารสำนักงานไปร่วมในการดำเนินการดังกล่าว โดยรับผิดชอบจัดทำบันทึกและสารบัญระบบ เอกสารร่วมกัน เพื่อประโยชน์ในการติดตามเอกสารดังกล่าว
- การทำลายเอกสารโดยผู้ให้บริการภายนอก ได้กำหนดให้มีการดำเนินการโดยรับประกันความสมบูรณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมีการจัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทและผู้ให้บริการภายนอก

ข้อ 9 ข้อมูลส่วนบุคคลใดบ้างที่เราจะเก็บรวบรวม

กรณีทั่วไป

โดยทั่วไป บริษัทจะเก็บรวมรวบข้อมูลส่วนบุคคลทั่วไป รวมถึงข้อมูลการติดต่อจากท่าน เช่น ชื่อ นามสกุล วันเดือนปีเกิด อายุ อาชีพ เพศ หมายเลขโทรศัพท์ ที่อยู่ อีเมล และรายละเอียดข้อมูลที่ใช้ในการติดต่ออื่นๆ เท่าที่จำเป็น เพื่อวัตถุประสงค์ในการปฏิบัติตามสิทธิหน้าที่ที่บริษัทมีสัญญาไว้กับท่าน หรือ ใช้ในการพิจารณาในกระบวนการอนุมัติค่าสินไหมทดแทน ใช้ในการติดต่อโรงพยาบาล สถานพยาบาล คลินิก และวัตถุประสงค์อื่นที่เป็นประโยชน์อันชอบธรรมของบริษัท ในการประมวลผลข้อมูลส่วนบุคคลของท่าน

กรณีการเข้าใช้งาน เว็บไซต์ แอปพลิเคชัน รวมถึงแพลตฟอร์มสื่อสังคมออนไลน์

กรณีท่านเข้าใช้เว็บไซต์ แอปพลิเคชัน และอาจจะรวมถึงแพลตฟอร์มสื่อสังคมออนไลน์ของบริษัท หรือ ผู้ให้บริการภายนอกอื่น บริษัทอาจจะเก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับกิจกรรมส่วนบุคคล ลักษณะการใช้งานที่ท่านชอบ เช่น ชื่อเรียกตัวตนเฉพาะของท่านที่ใช้บนแพลตฟอร์มสื่อสังคมออนไลน์ ที่อยู่ไอพี ประเภทและเวอร์ชั่นของเบราว์เซอร์ การตั้งค่าเขตเวลา ประเภทของปลั๊กอินในเบราว์เซอร์ ระบบปฏิบัติการและแพลตฟอร์ม ข้อมูลผู้ใช้ ข้อมูลเกี่ยวกับอุปกรณ์ ซึ่งรวมถึงข้อมูลเกี่ยวกับอุปกรณ์เคลื่อนที่ ข้อมูลเครือข่ายไร้สายและข้อมูลเครือข่ายทั่วไป

ข้อ 10 วิธีการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน บริษัทอาจเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน โดยวิธีดังต่อไปนี้

10.1. เมื่อท่านติดต่อสื่อสารกับบริษัท หมายถึง ไม่ว่าจะเป็นการสื่อสารเป็นหนังสือ หรือวาจา โดยไม่คำนึงว่าฝ่ายใดจะเป็นผู้ติดต่อฝ่ายนั้นก่อนหรือไม่ก็ตาม และให้รวมถึง การเปิด เข้าดูเอกสารในระบบ หรือ ลิงค์ที่บริษัทได้จัดทำหรือนำส่งแก่ท่าน

10.2. เมื่อท่านติดต่อบุคลากร และคู่ค้าของบริษัท หมายถึง พนักงาน และหรือบุคลากร เจ้าหน้าที่บริการลูกค้า พนักงานขาย ตัวแทน นายหน้า คนกลางประกันภัย ผู้รับจ้าง คู่ค้า ผู้ให้บริการ ผู้รับมอบอำนาจ ผู้กระทำการแทน และหรือบุคคลอื่น และหรือหน่วยงานอื่นที่เกี่ยวข้องของบริษัท ได้มีการติดต่อผ่านทางเว็บไซต์ แอปพลิเคชัน สื่อสังคมออนไลน์ โทรศัพท์ อีเมล์ การพบปะกันโดยตรง การสัมภาษณ์ ข้อความสั้น (SMS) โทรสาร ไปรษณีย์ หรือโดยวิธีการอื่นใด

10.3. เมื่อบริษัทได้รับข้อมูลส่วนบุคคลจากบุคคลภายนอกเกี่ยวกับท่าน หมายถึง การได้รับข้อมูลจากบุคคล และหรือนิติบุคคล หรือ หน่วยงานภายนอกที่ท่านมีภาระผูกพันอยู่ การพบแหล่งข้อมูลที่เป็นสาธารณะ จากแหล่งข้อมูลส่วนตัว หรือแหล่งข้อมูลเชิงพาณิชย์ จากเว็บไซต์ แหล่งข้อมูลสื่อสังคมออนไลน์ ผู้ให้บริการข้อมูล (data providers) แหล่งข้อมูลทางการแพทย์ จากสถานบริการสาธารณสุข โรงพยาบาล สถานพยาบาล คลินิกแพทย์ บุคลากรผู้ประกอบวิชาชีพสาธารณสุขอื่น

10.4. เมื่อท่านให้ข้อมูลส่วนบุคคลใด ๆ ที่เกี่ยวข้องกับบุคคลภายนอกอื่นแก่บริษัท หมายถึง กรณีที่ท่านให้ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลภายนอกอื่นใด สมาชิกในครอบครัว ผู้ชำระเงินตามกรมธรรม์ประกันภัย ผู้รับประโยชน์ หรือบุคคลอ้างอิง ที่ท่านได้รับรองและรับประกันความถูกต้องของข้อมูลส่วนบุคคลนั้น พร้อมทั้งรับรองและรับประกันว่าท่านได้แจ้งให้บุคคลเหล่านั้นทราบอย่างครบถ้วนแล้ว

ข้อ 11 วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของท่าน บริษัทจะประมวลผลข้อมูลส่วนบุคคลของท่าน เพื่อวัตถุประสงค์ ดังต่อไปนี้

11.1. ปฏิบัติตามสิทธิหน้าที่ตามสัญญาของบริษัทกับท่าน และหรือ บุคคลภายนอกที่ต้องเสียหาย และหรือสถานพยาบาลที่เป็นคู่สัญญา เกี่ยวกับการประกันภัย

11.2. ดำเนินการใดๆ ที่เกี่ยวข้องกับการประกันภัย ซึ่งหมายรวมถึงการดำเนินการใด ที่ไม่จำกัดเฉพาะการรับประกันภัย และการเรียกร้องค่าสินไหมทดแทนก็ได้

11.3. การติดต่อสื่อสารระหว่างบริษัทกับท่าน หมายรวมถึง การสื่อสารข้อมูลเกี่ยวกับ การจัดการ และข้อมูลอื่น ๆ เกี่ยวกับผลิตภัณฑ์ประกันภัย หรือ ด้านหนึ่งด้านใดๆ ที่ท่านอาจมีกับบริษัทก็ได้

11.4. การทำวิจัยทางการตลาด การวิเคราะห์ข้อมูล และการทำวิจัยเชิงสถิติ หรือคณิตศาสตร์ประกันภัย การรายงานหรือการประเมินผลต่าง ๆ ตามที่หน่วยงานกำกับดูแลที่เกี่ยวข้องกับบริษัท ขอให้จัดทำขึ้น

11.5. การสืบสวน หรือป้องกันการกระทำที่เกี่ยวกับการฉ้อโกง การปกปิดข้อความจริง และการกระทำผิดอื่น ๆ ไม่ว่าจะเป็นเพียงสงสัยว่าจะเป็นการกระทำผิด ทั้ง ใช้ในการติดต่อสื่อสารกับบริษัทต่าง ๆ ในธุรกิจบริการทางการเงิน และการประกันภัย ตลอดจนเพื่อการติดต่อสื่อสารกับหน่วยงานกำกับดูแลที่เกี่ยวข้องกับบริษัท

11.6. ให้ท่านสามารถเข้าถึงเนื้อหาในเว็บไซต์ แอปพลิเคชัน หรือ การเข้าถึงแพลตฟอร์มสื่อสังคมออนไลน์ หรือบริการอย่างใดอย่างหนึ่งเป็นการเฉพาะของบริษัท หรือ คู่ค้า

11.7. บริษัทอาจประมวลผลพฤติกรรมการใช้เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ เพื่อการวิเคราะห์การใช้งานเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์ของท่าน และการทำความเข้าใจลักษณะการใช้งานที่ท่านชอบ เพื่อจัดทำให้เว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์เหล่านั้นตอบสนองอย่างเหมาะสมกับท่านโดยเฉพาะ เพื่อการประเมิน หรือดำเนินการ และการปรับปรุงเว็บไซต์ แอปพลิเคชัน หรือแพลตฟอร์มสื่อสังคมออนไลน์เหล่านั้น หรือผลิตภัณฑ์และ/ หรือบริการของบริษัท การแก้ไขปัญหาต่างๆ การแนะนำผลิตภัณฑ์ และหรือบริการที่เกี่ยวข้อง และการจัดโฆษณาบนเว็บไซต์ แอปพลิเคชัน และช่องทางอื่นๆ ตามกลุ่มเป้าหมาย

11.8. การปฏิบัติให้เป็นไปตามกฎหมาย และการเข้าไปตรวจสอบธุรกิจของบริษัท ไม่ว่าจะเป็นการตรวจสอบภายในหรือการตรวจสอบจากบุคคลภายนอกก็ตาม

11.9. การดำเนินการให้เป็นไปตามข้อกำหนดภายใต้นโยบายภายในต่าง ๆ ของบริษัทที่ยึดกำหนดให้ต้องถือปฏิบัติ

11.10. การนำไปใช้ในการบริหารจัดการ การจัดเก็บ การบันทึก การสำรอง หรือการทำลายข้อมูลส่วนบุคคล

11.11. ดำเนินการให้เป็นไปตามข้อกำหนดของกฎหมาย กฎระเบียบ คำสั่ง ข้อตกลง หรือ นโยบายใด ๆ ที่ใช้บังคับกับบริษัท ซึ่งกำหนดขึ้นโดยหน่วยงานกำกับดูแลของรัฐ หน่วยงานรัฐใด ๆ ที่มีหน้าที่บังคับใช้กฎหมาย หน่วยงานที่มีหน้าที่ระงับข้อพิพาท หรือหน่วยงานที่ดูแลธุรกิจประกันภัย ไม่ว่าหน่วยงานใดก็ตาม

11.12. การบังคับใช้กฎหมาย หรือการให้ความช่วยเหลือ ให้ความร่วมมือ การสืบสวนโดย บริษัทหรือในนามของ บริษัท โดยเจ้าหน้าที่ตำรวจ หรือโดยหน่วยงานรัฐหรือหน่วยงานกำกับดูแลอื่น ๆ ในประเทศ

11.13. การตรวจสอบและเพิ่มคุณภาพ รวมทั้งการฝึกอบรม เมื่อมีการบันทึกการติดต่อสื่อสารของบริษัท

11.14. ดำเนินการอื่น ๆ ที่จำเป็น และมีความเกี่ยวข้องโดยตรงกับวัตถุประสงค์ข้อหนึ่งข้อใดตามที่กล่าวมา ข้างต้น

ข้อ 12 การโอนข้อมูลส่วนบุคคล

บริษัทอาจถ่ายโอนข้อมูลส่วนบุคคลของท่าน จัดเก็บไว้ หรือ ประมวลผล หรือ ส่งให้แก่บุคคลหรือหน่วยงานใดๆ ซึ่งอาจมีที่ตั้งหรือให้บริการอยู่ในประเทศไทย หรือนอกประเทศไทย ทั้งนี้ ข้อมูลส่วนบุคคลของท่าน จะถูกโอนไปยังสถานที่อื่น ๆ ตามเงื่อนไขเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ตามที่พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลกำหนด

ข้อ 13 สิทธิของท่านในฐานะเจ้าของข้อมูลส่วนบุคคล ท่านมีสิทธิดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่าน ดังต่อไปนี้

13.1. ตรวจสอบว่า บริษัทมีข้อมูลส่วนบุคคลใดๆ เกี่ยวกับท่าน หรือไม่ ตลอดจนสิทธิในการเข้าถึง หรือขอรับสำเนาของข้อมูลใด ๆ ดังกล่าว และหรือเข้าถึงข้อมูลว่าบริษัท ประมวลผลข้อมูลส่วนบุคคลของท่านอย่างไร

13.2. ขอให้บริษัททำการแก้ไขข้อมูลส่วนบุคคลใดๆ ที่เกี่ยวข้องกับท่าน ให้ถูกต้อง

13.3. ขอให้ลบหรือทำลายข้อมูลส่วนบุคคลของท่าน ในกรณีที่ไม่จำเป็นต้องใช้อีกต่อไปเพื่อวัตถุประสงค์ที่กำหนดในนโยบายฉบับนี้ หรือ ในกรณีที่ไม่มีหลักการพื้นฐานทางกฎหมายในการดำเนินการเกี่ยวกับข้อมูลนั้นๆ หรือตามที่กฎหมายกำหนด

13.4. ขอให้จำกัดการดำเนินการประมวลผลข้อมูลส่วนบุคคลของท่านในบางสถานการณ์

13.5. ขอให้บริษัทฯ โอนย้ายข้อมูลส่วนบุคคลของท่านในบางสถานการณ์ให้กับผู้ควบคุมข้อมูลรายอื่น ในกรณีที่ข้อมูลอยู่ในรูปแบบหรือโครงสร้างที่ใช้กันโดยทั่วไป

13.6. ขอให้ระงับการประมวลผลข้อมูลส่วนบุคคลของท่านเป็นการชั่วคราวในบางสถานการณ์

13.7. ขอเพิกถอน หรือ ร้องขอให้เปลี่ยนแปลงขอบเขตความยินยอมของท่าน ที่ท่านได้ให้ไว้ในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของท่าน

ทั้งนี้ บริษัทจะดำเนินการตามสิทธิของท่าน เมื่อมีการร้องขอตามช่องทางการขอใช้สิทธิที่บริษัทกำหนด โดยบริษัท อาจขอสงวนสิทธิไม่ปฏิบัติตามคำร้องขอใช้สิทธิของท่าน ตามความเหมาะสมและเท่าที่กฎหมายที่ใช้บังคับจะอนุญาต

ช่องทางการติดต่อบริษัทเพื่อสอบถาม หรือ การขอใช้สิทธิของท่านเกี่ยวกับข้อมูลส่วนบุคคล

ท่านสามารถติดต่อบริษัท หรือ ส่งคำร้องขอใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของท่านได้ผ่านหน้าเว็บไซต์ https://www.smk.co.th/consent หรือ อีเมล DPO@smk.co.th โดยตั้งชื่อหัวข้อว่า “ขอใช้สิทธิข้อมูลส่วนบุคคล” และทำการแจ้งรายละเอียดที่ต้องการร้องขอ ทั้งนี้ท่านสามารถจะใช้สิทธิเหล่านั้นได้นับแต่วันที่ 1 มิถุนายน 2565 เป็นต้นไป หรือ ตามวันที่ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลประกาศเปลี่ยนแปลง

14. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

14.1. บริษัทกำหนดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ภายใต้หลักการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ภายใต้กรอบการรับประกัน ดังนี้

- ข้อมูลทั้งหมดจะได้รับการเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ (Confidentiality) โดยถือว่าข้อมูลส่วนบุคคลทั้งหมดโดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหวเป็นข้อมูลความลับสูงสุด
- ข้อมูลทั้งหมดต้องเป็นข้อมูลที่ถูกต้องเชื่อถือได้เป็นไปตามข้อมูลที่ทางผู้เป็นเจ้าของข้อมูลได้ให้ข้อมูลดังกล่าวขึ้นมา โดยไม่เกิดการแก้ไขโดยไม่ได้รับอนุญาต (Integrity)
- ข้อมูลต้องมีความพร้อมใช้งานได้ทันทีที่ต้องการ (Availability)

14.2. บริษัทกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการผ่านโครงสร้างการจัดตั้งที่กำหนดขึ้น มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพ ภายใต้หลักการในการควบคุมเงื่อนไขการเข้าถึงและเข้าใช้ข้อมูลส่วนบุคคลในแต่ละระดับข้อมูลผ่านระบบ Authorization Matrix ตาม Role-Based การจัดการระบบ เพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึงการเปลี่ยนแปลง การลบ หรือถ่ายโอนข้อมูลส่วนบุคคลได้ โดยเฉพาะอย่างยิ่งกรณีส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอ่อนไหว

14.3. บริษัทกำหนดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของการเข้าถึง เปลี่ยนแปลง ข้อมูลส่วนบุคคลในส่วนต่างๆ โดยกำหนดให้ (1) หัวหน้าฝ่ายหรือหน่วยงานที่เกี่ยวข้องรับผิดชอบทำการสอบทานบันทึก Log ของพนักงานภายใต้กำกับดูแลของฝ่ายหรือหน่วยงานของตนตรวจความผิดปกติของ Log อย่างสม่ำเสมอ และ (2) ให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ Log ดังกล่าวตามลำดับ Line of Defenses ที่เกี่ยวข้อง

14.4. ในการดำเนินการควบคุมและบริหารจัดการการประมวลผลข้อมูลส่วนบุคคลทั้งหมด บริษัทกำหนดให้ทุกหน่วยงานต้องดำเนินการภายใต้กรอบ Maker-Checker และมีการตรวจสอบ ทดสอบประสิทธิภาพในการทำงานของมาตรการและกลไกต่างๆ อย่างสม่ำเสมอ

14.5. กรณีที่บริษัทใช้เครื่องมืออุปกรณ์ หรือทรัพย์สินสารสนเทศในการเก็บและประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลไม่ว่ากลุ่มใดก็ตาม บริษัทได้ดำเนินการจัดทำทะเบียนทรัพย์สินดังกล่าวให้ครบถ้วน และกำหนดจำกัดสิทธิหรือเงื่อนไขในการใช้ทรัพย์สินสารสนเทศที่เป็นของพนักงานแต่ละคน (BYOD) ไว้อย่างชัดเจน เพื่อให้มีมาตรฐานในการรักษาความมั่นคงของข้อมูลส่วนบุคคลในทุกอุปกรณ์ทรัพย์สินสารสนเทศ ทั้งนี้ได้จำกัดการใช้ BYOD เพื่อการเก็บรักษาหรือประมวลผลข้อมูลส่วนบุคคลให้เหลือน้อยที่สุด เพื่อป้องกันความเสี่ยงของการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล

14.6. กำหนดนโยบายการสำรองข้อมูลส่วนบุคคลที่มีความสำคัญทั้งหมด ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง เพื่อรับประกันให้ข้อมูลส่วนบุคคลดังกล่าวพร้อมใช้งานได้ตลอดเวลาโดยไม่หยุดชะงัก ทั้งนี้ ได้จัดให้มีการทดสอบข้อมูลสำรอง และกระบวนการกู้คืนข้อมูล (Data Recovery) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลทั้งหมด ที่มีการประมวลผลมีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด ทั้งนี้ สำหรับการใช้ Data Recovery Site บริษัทจะพิจารณาใช้บริการผู้ให้บริการภายในประเทศไทยเป็นหลักก่อน เพื่อรับประกันความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

14.7. บริษัทกำหนดกระบวนการในการควบคุม และรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล โดยผู้ให้บริการภายนอกอย่างชัดเจน และได้กำหนดมาตรฐานตั้งแต่กระบวนการคัดเลือกผู้ให้บริการภายนอก การจัดทำสัญญา การกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่ผู้ให้บริการภายนอกอาจเข้าถึง โดยจำกัดการเข้าถึงและการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น และรับประกันการรักษามาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ผู้ให้บริการดังกล่าวอาจเข้าถึงให้ได้มาตรฐานเดียวกันกับมาตรฐานของ

บริษัท ทั้งนี้ได้กำหนดให้มีหน่วยงานเพื่อทำหน้าที่ในการติดตามและตรวจสอบการปฏิบัติหน้าที่ของผู้ให้บริการภายนอกให้เป็นไปตามมาตรฐานที่กำหนดตามกำหนดระยะเวลาเป็นปกติ โดยหากพบความผิดปกติ หรือการละเมิดให้ดำเนินการลงโทษผู้ให้บริการ ดังกล่าวทันที โดยรับประกันไม่ให้เกิดผลกระทบต่อความต่อเนื่องในการให้บริการของบริษัท

14.8. บริษัทกำหนดให้มีการทบทวนนโยบายและมาตรการจัดการและจัดเก็บข้อมูลเพื่อรักษาความมั่นคงปลอดภัยดังกล่าว เป็นประจำอย่างน้อยปีละ 1 ครั้ง

ข้อ 15 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

15.1. บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ในการกำหนดนโยบายและมาตรการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หรือเกิดเป็นเหตุละเมิดข้อมูลส่วนบุคคล โดยประสานกับหน่วยงานที่เกี่ยวข้อง ทั้งนี้ คณะทำงานคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ทำหน้าที่รับแจ้งและบริหารจัดการเหตุการณ์ดังกล่าวก่อน และกำหนดให้มีการทบทวนแผนการดำเนินการดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนดังกล่าว

15.2. กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่ในการรายงานเหตุการณ์ดังกล่าว ให้คณะกรรมการบริษัท ทราบเพื่อจัดเตรียมเอกสารรายงานจัดส่ง ให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายในกรอบระยะเวลาการรายงาน 72 ชั่วโมงนับแต่ทราบเหตุ และให้แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล กรณีได้รับผลกระทบ

15.3. ภายหลังสิ้นสุดเหตุละเมิดดังกล่าว คณะทำงานคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการตรวจสอบ และสอบทานเพื่อพิจารณา Root Cause ของเหตุการณ์ดังกล่าวเพื่อจัดทำรายงานเสนอต่อคณะกรรมการบริษัททราบ และเพื่อเป็นแผนการในการปรับปรุงแก้ไขป้องกันเหตุละเมิดที่อาจเกิดขึ้นในอนาคตต่อไป

ข้อ 16 การทบทวนหรือปรับปรุงนโยบาย

บริษัทกำหนดให้มีการทบทวนหรือปรับปรุงนโยบายฉบับนี้ โดย ประธานกรรมการบริหารและกรรมการผู้จัดการ ด้วยการ พิจารณาจากรายงานการปฏิบัติตามนโยบายการบริหารจัดการคุ้มครองการประมวลผลข้อมูลที่นำเสนอ โดยคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้งหรือกรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อธุรกิจบริษัท หรือกระบวนการ ประมวลผลข้อมูลส่วนบุคคลที่บริษัทดำเนินการเพื่อให้นโยบายเป็นปัจจุบันอยู่เสมอ โดยจะมีการเสนอให้คณะกรรมการ บริษัทพิจารณารับรองทุกครั้งที่มีการทบทวนและแก้ไขเปลี่ยนแปลง

ทั้งนี้ ให้มีผลบังคับ ตั้งแต่วันที่ 9 พฤษภาคม 2566 เป็นต้นไป

(นายเรืองเดช ดุษฎีสุรพจน์)

ประธานกรรมการบริหารและกรรมการผู้จัดการ