

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

บริษัท ดุไฮม จำกัด (มหาชน)

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

ด้วยคณะกรรมการของบริษัทเห็นถึงความสำคัญในการประมวลผลข้อมูลส่วนบุคคลให้เหมาะสมและถูกต้องตามกฎหมาย คณะกรรมการบริษัทจึงอนุมัติรับรองและออกประกาศบริษัท เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้นเพื่อกำหนดกรอบการประมวลผลข้อมูลส่วนบุคคลในกระบวนการต่างๆ ของบริษัทเพื่อไม่ให้กระทบสิทธิภายใต้กรอบกฎหมายของเจ้าของข้อมูลแต่กลุ่มมากเกินไป รวมถึงเป็นนโยบายการกำกับดูแลและบริหารจัดการการประมวลผลข้อมูลดังกล่าวให้ถูกต้องตามมาตรฐานที่ระบุไว้โดยหน่วยงานกำกับดูแล โดยมีจุดประสงค์ให้พนักงานและบุคคลที่เกี่ยวข้องของบริษัทยึดถือและปฏิบัติตามภายใต้รายละเอียด ดังนี้

ข้อ 1 นโยบายและคู่มือการคุ้มครองข้อมูลส่วนบุคคล

1.1 ประกาศฉบับนี้เรียกว่า “ประกาศกลุ่มบริษัท เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล” โดยให้มีผลบังคับใช้ นับแต่วันที่บริษัทประกาศเป็นต้นไป

1.2 โดยอาศัยอำนาจของประกาศบริษัทฉบับนี้ บริษัทอาจพิจารณากำหนดและประกาศคู่มือการปฏิบัติงานโดยละเอียดเพื่อกำหนดแนวทางการปฏิบัติต่างๆ ในการรับประกันความสมบูรณ์ ถูกต้องและครบถ้วนในการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องเพิ่มเติม โดยให้คู่มือการปฏิบัติงานดังกล่าวมีผลบังคับสมบูรณ์เช่นเดียวกันกับประกาศฉบับนี้

ข้อ 2 โครงสร้างการบริหารจัดการและกำกับการประมวลผลข้อมูลส่วนบุคคล

เพื่อรับประกันการกำกับดูแลและบริหารจัดการด้านการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลให้สมบูรณ์ บริษัทกำหนดจัดตั้งโครงสร้างดังต่อไปนี้

2.1 คณะกรรมการบริษัทมีหน้าที่หลักในการกำหนดทิศทางและการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในภาพรวมของบริษัท รวมถึงบริหารจัดการความเสี่ยงต่างๆ ที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคลโดยมีบทบาทหลักในการตรวจสอบและอนุมัติทุกนโยบายย่อยและคู่มือแนวทางการปฏิบัติที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

2.2 เพื่อกำกับดูแลการปฏิบัติงานการประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามนโยบายและสอดคล้องกับกรอบกฎหมาย บริษัทกำหนดกลไกกำกับการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลภายใต้รูปแบบโครงสร้าง 3 Lines of Defence ดังนี้

- 1st Line of Defence: Risk Owner ได้แก่ ประธานหรือหัวหน้าฝ่าย/หน่วยงานภายในซึ่งมีหน้าที่รับผิดชอบโดยตรงในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของพนักงานภายในหน่วยงานของตนให้ถูกต้องและสอดคล้องกับนโยบายและกฎหมายที่เกี่ยวข้อง
- 2nd Line of Defence: Risk Control กำหนดให้มีการแต่งตั้งคณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Working Committee) ซึ่งประกอบด้วยหัวหน้าฝ่ายที่มีการประมวลผลข้อมูลส่วนบุคคลต่างๆ ในบริษัททำงานร่วมกับหน่วยงานกำกับดูแลการปฏิบัติงาน โดยการทำงานของคณะทำงานดังกล่าวต้องเป็นไปอย่างอิสระภายใต้หลักการ maker-checker ซึ่งบริษัทจะได้ออกประกาศในการแต่งตั้งโครงสร้างคณะทำงานดังกล่าวพร้อมกับกำหนดบทบาทหน้าที่ของคณะทำงานดังกล่าวเป็นประกาศต่างหาก

- 3rd Line of Defence: Risk Assurance ได้แก่ คณะกรรมการหรือหน่วยงานตรวจสอบซึ่งมีหน้าที่กำกับดูแลและตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลของทุกหน่วยงานอีกครั้งโดยดำเนินการเป็นปกติ ทั้งนี้ อาจเป็นหน่วยงานตรวจสอบกำกับดูแลภายในหรือภายนอกตามแต่การพิจารณาตามความเหมาะสมโดยคณะกรรมการบริษัท

2.3 บริษัทกำหนดจัดสรรทรัพยากรอย่างเพียงพอทั้งในแง่ของระบบงาน บุคลากร และงบประมาณในการสนับสนุนการปฏิบัติงานของแต่ละหน่วยงานกำกับดูแลตามนโยบายและมาตรฐานการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลในทุกส่วน

ข้อ 3 การประเมินและบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

3.1 บริษัทกำหนดให้มีการประเมินและทบทวนการประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคลใน

ภาพรวมขององค์กร (Enterprise Risk Management Level) อย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงของรูปแบบการประมวลผลข้อมูลส่วนบุคคลอย่างมีสาระสำคัญ

3.2 บริษัทกำหนดให้แต่ละหน่วยงานใน 1st Line of Defence ที่ระบุไว้ในข้อ 2.2 มีหน้าที่และความรับผิดชอบในการประเมิน ทบทวน และบริหารจัดการความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลภายในหน่วยงานของตน รวมถึงการติดตามและรายงานผลด้านความเสี่ยงให้แก่คณะทำงานคุ้มครองข้อมูลส่วนบุคคลพิจารณา

3.3 บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลในฐานะผู้รับผิดชอบหลักในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของบริษัทมีหน้าที่รวบรวมและจัดทำเอกสารการประเมิน รวมถึงทบทวนการบริหารจัดการความเสี่ยงของบริษัทในภาพรวมโดยคำนึงถึงกรอบ “ความเสี่ยงที่ยอมรับได้ในด้านการประมวลผลข้อมูลส่วนบุคคลของบริษัท” และรายงานต่อคณะกรรมการบริษัทเพื่อพิจารณาและอนุมัติรับรองแผนการบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท

3.4 บนพื้นฐานการประเมินความเสี่ยงในระดับองค์กร สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบถึงสิทธิเสรีภาพของบุคคลซึ่งอาจนำไปสู่การเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญของเจ้าของข้อมูลส่วนบุคคลหรือที่จะทำให้เจ้าของข้อมูลไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ บริษัทกำหนดให้ต้องมีการจัดทำประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Processing Impact Assessment: DPIA) เฉพาะกิจกรรมการประมวลผลข้อมูลส่วนบุคคลความเสี่ยงสูงดังกล่าวเพิ่มขึ้นก่อนการตัดสินใจประมวลผลข้อมูลส่วนบุคคลดังกล่าวโดยต้องทำรายงานกระบวนการประเมินความเสี่ยงดังกล่าวเป็นลายลักษณ์อักษรเพื่อตรวจสอบ

ทั้งนี้ การประเมิน DPIA ต้องดำเนินการภายใต้หลักการดังนี้ (1) ต้องมีการอธิบายรายละเอียดขอบเขตการประเมินผลวัตถุประสงค์และความจำเป็นในการประมวลผลข้อมูลดังกล่าว (2) ต้องมีกระบวนการปรึกษาหารือกับผู้มีส่วนเกี่ยวข้องต่างๆ ทั้งภายในและภายนอกองค์กรซึ่งรวมถึงเจ้าของข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง (3) ต้องมีคำอธิบายที่ชัดเจนเกี่ยวกับความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล (4) ต้องจัดให้มีการประเมินความเสี่ยงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยคำนึงถึง “ความน่าจะเป็น” (likelihood) และ “ความร้ายแรง” (severity) (5) ต้องกำหนดรายละเอียดมาตรการในการลดความเสี่ยงที่ระบุไว้และคำอธิบายเกี่ยวกับมาตรการที่เหมาะสมในการลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลดังกล่าวให้อยู่ในเกณฑ์ความเสี่ยงที่ยอมรับได้ที่บริษัทกำหนดไว้ในกรอบการประเมินความเสี่ยงระดับองค์กร

ข้อ 4 การสื่อสารประชาสัมพันธ์นโยบาย

4.1 บริษัทให้ความสำคัญต่อการสื่อสารนโยบายและแนวทางการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผล

ข้อมูลส่วนบุคคลให้แก่พนักงานรวมถึงผู้ให้บริการภายนอกทั้งหมดของบริษัทที่มีส่วนเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลโดยและในนามบริษัท โดยกำหนดเป็นนโยบายให้มีการสื่อสารผ่านทุกช่องทางการติดต่อกับพนักงานและผู้ให้บริการภายนอกดังกล่าวอย่างเป็นปกติ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญและกระทบต่อการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท

4.2 บริษัทกำหนดให้เป็นหน้าที่ของแต่ละหน่วยงานที่ดำเนินการประมวลผลข้อมูลส่วนบุคคลในการสื่อสารและจัดการฝึกอบรม รวมถึงสร้างความตระหนักรู้ต่างๆ ให้พนักงานภายในแผนกหรือฝ่ายของตน รวมถึงผู้ให้บริการภายนอกที่อยู่ภายใต้สังกัดและการดูแลของหน่วยงานหรือแผนกดังกล่าวรับทราบเพื่อให้มั่นใจว่าบุคคลดังกล่าวตระหนักรู้ถึงความสำคัญของสิทธิของเจ้าของข้อมูล รวมถึงหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งหมดนั้น

ข้อ 5 กลไกการกำกับดูแลและตรวจสอบ

บริษัทกำหนดกลไกการติดตามตรวจสอบการปฏิบัติตามนโยบายการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักการ ดังนี้

5.1 บริษัทกำหนดกลไกการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลตาม 3 Lines of Defence ที่ระบุไว้ในข้อ 2.2 โดยให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลทำหน้าที่ติดตามและตรวจสอบการปฏิบัติตามนโยบายของบริษัทที่กำหนดไว้ ทั้งส่วนของพนักงานและผู้ให้บริการภายนอก และรายงานผลต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง หรือกรณีที่มีการละเมิดอย่างมีนัยสำคัญต่อธุรกิจหรือชื่อเสียงของบริษัท

5.2 บริษัทกำหนดแผนการว่าจ้างผู้ตรวจสอบอิสระภายนอกให้ดำเนินการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของบริษัท พร้อมทั้งรายงานผลการตรวจสอบต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงอันสำคัญในบริษัท

5.3 กรณีที่ตรวจพบการฝ่าฝืนนโยบายการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคลจะเป็นหน่วยงานรับเรื่องร้องเรียนและทำหน้าที่ตรวจสอบจนทราบข้อเท็จจริง หากพบว่าเกิดการฝ่าฝืนหรือละเมิดนั้นจริง คณะทำงานจะเสนอไปยังคณะกรรมการของบริษัทเพื่อพิจารณากำหนดมาตรการลงโทษทางวินัยตามระเบียบบริหารงานบุคคลต่อไป

ข้อ 6 การจัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคล (Report of Processing)

6.1 บริษัทกำหนดให้แต่ละหน่วยงานใน 1st Line of Defence ดังที่ระบุไว้ในข้อ 2.2 เป็นหน่วยงานผู้รับผิดชอบในการจัดทำและปรับปรุงรายการการประมวลผลข้อมูลดังกล่าวอย่างสม่ำเสมอ โดยต้องดำเนินการควบคู่ไปกับการประเมินและการทบทวนการประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

6.2 บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลเป็นหน่วยงานให้ความรู้คำแนะนำ กำกับดูแลและตรวจสอบการจัดทำบันทึกการประมวลผลข้อมูลส่วนบุคคลโดยแต่ละหน่วยงานใน 1st Line of Defence เพื่อรับประกันความถูกต้อง ครบถ้วน และสอดคล้องกับมาตรฐานและกฎหมายที่เกี่ยวข้อง

ข้อ 7 นโยบายการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก

7.1 บริษัทกำหนดการบริหารจัดการข้อมูลส่วนบุคคลโดยจัดระดับความลับของข้อมูลดังกล่าวเป็นข้อมูลความลับที่สุด (Strictly Confidential) ภายใต้หลักการในการรักษาความลับของบริษัท โดยเฉพาะกรณีที่จะมีการเปิดเผยส่งต่อข้อมูลส่วนบุคคลไปให้แก่หน่วยงานภายนอกองค์กร

7.2 บริษัทกำหนดให้พนักงานทุกคนมีหน้าที่การบันทึกการการประมวลผลข้อมูลส่วนบุคคลที่มีการส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกองค์กร โดยหากจำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลออกไปให้แก่หน่วยงานภายนอกจะต้องมีการตรวจสอบความจำเป็น รวมถึงความเสี่ยงในการส่งต่อข้อมูลส่วนบุคคลและความน่าเชื่อถือของผู้รับข้อมูลส่วนบุคคลดังกล่าวก่อน ทั้งนี้ การส่งต่อหรือเปิดเผยแต่ละครั้งต้องได้รับความยินยอมจากผู้บังคับบัญชาตามอำนาจการอนุมัติ

7.3 ในกรณีการส่งต่อหรือรับข้อมูลส่วนบุคคลจากบุคคลภายนอกองค์กร บริษัทกำหนดนโยบายให้ต้องมีการลงนามในสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทและบุคคลภายนอกเพื่อกำหนดเงื่อนไขข้อกำหนดสิทธิและหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลระหว่างคู่สัญญาและรับประกันความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว

7.4 พนักงานผู้เปิดเผยหรือส่งต่อข้อมูลออกไปนอกองค์กรต้องรับประกันปฏิบัติตามช่องทางและวิธีการส่งต่อหรือเปิดเผยข้อมูลที่บริษัทกำหนดเพื่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยน้อยที่สุดรวมถึงหลีกเลี่ยงการส่งผ่านช่องทางส่วนตัวที่ไม่สามารถควบคุมได้

ข้อ 8 นโยบายการกำหนดระยะเวลาการรักษาข้อมูล

8.1 บริษัทกำหนดกรอบการกำหนดระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลตามหลักการพิจารณาความจำเป็นเป็น ดังนี้

- หากมีระยะเวลาตามกฎหมายระบุชัดเจนให้เก็บรักษาข้อมูลส่วนบุคคลส่วนใดไว้เป็นระยะเวลานานเท่าใดให้จัดเก็บตามกำหนดเวลานั้น และในกรณีการเก็บรักษาข้อมูลส่วนบุคคลส่วนใดอยู่ภายใต้เกณฑ์การเก็บรักษาของกฎหมายที่แตกต่างกัน บริษัทกำหนดกรอบการเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นระยะเวลาตามกรอบเวลาสูงสุดที่กฎหมายทั้งหมดกำหนดไว้
- กรณีเป็นการเก็บข้อมูลส่วนบุคคลเนื่องจากความจำเป็นที่พิจารณาโดยอาศัยความสัมพันธ์ต่างๆ ที่บริษัทมีกับเจ้าของข้อมูลด้วยฐานสัญญาให้เก็บข้อมูลไว้เท่าที่จำเป็นเพื่อการปฏิบัติตามหน้าที่ในสัญญาที่บริษัทมีกับเจ้าของข้อมูลดังกล่าว เช่น ตลอดระยะเวลาการให้บริการหรือตราบเท่าที่จะมีการยกเลิกสัญญาหรือความสัมพันธ์ที่เกี่ยวข้อง ซึ่งอาจมีระยะเวลาแน่นอนหรือไม่ก็ได้แต่มีกรอบระยะเวลาการเก็บรักษาที่ชัดเจนแน่นอนซึ่งคาดหมายได้โดยเจ้าของข้อมูล
- กรณีเป็นการเก็บข้อมูลเพื่อประโยชน์อันชอบด้วยกฎหมายของบริษัทให้เก็บข้อมูลดังกล่าวไว้ตามกรอบที่เหมาะสมเพื่อการใช้สิทธิและประโยชน์อันชอบด้วยกฎหมายนั้น ในแต่ละกรณีภายใต้หลักการดังนี้ เช่น ตามระยะเวลาอายุความกรณีการฟ้องร้องต่อผู้สิทธิต่างๆ ทั้งนี้ สำหรับการเก็บรักษาข้อมูลส่วนบุคคลด้วยฐานประโยชน์อันชอบด้วยกฎหมาย บริษัทกำหนดหลักการสำคัญที่ต้องพิจารณา คือ การเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวต้องไม่กระทบสิทธิของเจ้าของข้อมูลมากเกินไปและบริษัทต้องให้สิทธิเจ้าของข้อมูลในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยฐานดังกล่าวได้ตามสิทธิที่มี

- กรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานความยินยอมให้เก็บข้อมูลได้ทราบเท่าที่เจ้าของข้อมูลยังไม่ได้ใช้สิทธิในการถอนความยินยอมซึ่งเป็นสิทธิอิสระที่เจ้าของข้อมูลสามารถดำเนินการได้ตลอดระยะเวลาและบริษัทเคารพสิทธิในการตัดสินใจดังกล่าว

- กรณีข้อมูลส่วนบุคคลอ่อนไหว เช่น ประวัติอาชญากรรม หรือประวัติสุขภาพการรักษาพยาบาล หรือข้อมูลชีวภาพอื่นๆ ที่บริษัทอาจเก็บรักษาด้วยความยินยอมของเจ้าของข้อมูล บริษัทต้องใช้ความระมัดระวังในการเก็บรักษาข้อมูลส่วนบุคคลด้วยมาตรฐานที่สูงขึ้นโดยต้องลบหรือทำลายในทันทีที่หมดความจำเป็น

8.2 บริษัทกำหนดแจ้งกรอบระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลแต่ละฐานเพื่อแต่ละจุดประสงค์ให้เจ้าของข้อมูลแต่ละกลุ่มที่เกี่ยวข้องรับทราบในนโยบายข้อมูลส่วนบุคคลที่บริษัทจะจัดทำและแจ้งเจ้าของข้อมูลเป็นลายลักษณ์อักษร

8.3 เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลตามกรอบที่กำหนดไว้ในข้อ 8.1 แล้ว บริษัทจะลบทำลายข้อมูลส่วนบุคคลดังกล่าว หรือจะดำเนินการทำให้ข้อมูลกลายเป็นข้อมูลนิรนามขึ้นอยู่กับลักษณะของข้อมูล โดยต้องทำลายข้อมูลทั้งที่เป็นกระดาษเอกสารและข้อมูลในระบบ

8.4 บริษัทกำหนดกระบวนการการตรวจสอบระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลโดยให้ฝ่ายที่เกี่ยวข้อง ซึ่งเป็นฝ่ายที่รับผิดชอบข้อมูลและเอกสารดังกล่าวโดยตรงมีหน้าที่ในการตรวจสอบระยะเวลาการเก็บรักษาข้อมูลตามนโยบายการเก็บรักษาที่ได้ประกาศไว้

8.5 กรณีที่บริษัทว่าจ้างผู้ให้บริการภายนอกเป็นผู้ทำลายข้อมูลส่วนบุคคลที่หมดความจำเป็นดังกล่าว บริษัทกำหนดให้ต้องมีการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการนั้นเพื่อรับประกันความสมบูรณ์ในการทำลายข้อมูลด้วยเทคนิคที่เหมาะสม

ข้อ 9 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

9.1 บริษัทกำหนดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลภายใต้หลักการป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบภายใต้กรอบการรับประกัน ดังนี้

- ข้อมูลทั้งหมดจะได้รับการเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ (Confidentiality) โดยถือว่าข้อมูลส่วนบุคคลทั้งหมดโดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหวเป็นข้อมูลความลับสูงสุด

- ข้อมูลทั้งหมดต้องเป็นข้อมูลที่ถูกต้องเชื่อถือได้เป็นไปตามข้อมูลที่ทางผู้เป็นเจ้าของข้อมูลได้ให้ข้อมูลดังกล่าวขึ้นมาโดยไม่เกิดการแก้ไขโดยไม่ได้รับอนุญาต (Integrity) และ

- ข้อมูลต้องมีความพร้อมใช้งานได้ทันทีที่ต้องการ (Availability)

9.2 บริษัทกำหนดจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการผ่านโครงสร้างการจัดตั้งที่กำหนดขึ้น มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพภายใต้หลักการในการควบคุมเงื่อนไขการเข้าถึงและเข้าใช้ข้อมูลส่วนบุคคลในแต่ละระดับข้อมูลผ่านระบบ Authorization Matrix ตาม Role-Based การจัดการระบบเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึงการเปลี่ยนแปลง การลบ หรือถ่ายโอนข้อมูลส่วนบุคคลได้ โดยเฉพาะอย่างยิ่งกรณีส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอ่อนไหว

9.3 บริษัทกำหนดจัดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของการเข้าถึง เปลี่ยนแปลงข้อมูลส่วนบุคคลในส่วนต่างๆ โดยกำหนดให้ (1) หัวหน้าฝ่ายหรือหน่วยงานที่เกี่ยวข้องรับผิดชอบทำการสอบทานบันทึก Log ของพนักงานภายใต้กำกับดูแลของฝ่ายหรือหน่วยงานของตนตรวจความผิดปกติของ Log อย่างสม่ำเสมอ และ (2) ให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการตรวจสอบตรวจสอบ Log ดังกล่าวตามลำดับ Line of Defences ที่เกี่ยวข้อง

9.4 ในการดำเนินการควบคุมและบริหารจัดการการประมวลผลข้อมูลส่วนบุคคลทั้งหมด บริษัทกำหนดให้ดำเนินการภายใต้กรอบ Maker-Checker และต้องมีการตรวจสอบทดสอบประสิทธิภาพในการทำงาน ของมาตรการและกลไกต่างๆ อย่างสม่ำเสมอ

9.5 บริษัทกำหนดกรอบนโยบายให้หน่วยงานต่างๆ ดำเนินการประมวลผลข้อมูลส่วนบุคคลทั้งหมดผ่านระบบอิเล็กทรอนิกส์ที่ควบคุมการเข้าถึงและบันทึกการเข้าถึงได้มากกว่าการจัดเก็บข้อมูลในรูปแบบกระดาษ ทั้งนี้ ในกรณีจำเป็นต้องใช้ข้อมูลส่วนบุคคลในรูปแบบของกระดาษต้องจัดทำบันทึกการใช้ข้อมูลต้องมีนโยบาย Clean Desk และห้ามนำกระดาษที่มีข้อมูลส่วนบุคคลไปใช้ซ้ำ (Recycled) ต้องจัดเก็บใส่กล่องเรียบร้อยแล้วระบุกำหนดระยะเวลาการเก็บข้อมูลดังกล่าว และหากจะมีการเคลื่อนย้ายข้อมูลดังกล่าวต้องดำเนินการตามกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล

9.6 กรณีที่บริษัทใช้เครื่องมืออุปกรณ์หรือทรัพย์สินสารสนเทศใดในการเก็บและประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล บริษัทต้องดำเนินการจัดทำทะเบียนทรัพย์สินดังกล่าวให้ครบถ้วนและโดยเฉพาะอย่างยิ่งต้องกำหนดจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลโดยผ่านทรัพย์สินสารสนเทศที่เป็นของพนักงานแต่ละคน (BYOD) ให้ชัดเจนเพื่อให้มีมาตรฐานในการรักษาความมั่นคงของข้อมูลส่วนบุคคลในทุกอุปกรณ์ทรัพย์สินสารสนเทศ โดยควรจำกัดการใช้ BYOD เพื่อการเก็บรักษาหรือประมวลผลข้อมูลส่วนบุคคลให้เหลือน้อยที่สุดเพื่อป้องกันความเสี่ยงของการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล

9.7 บริษัทกำหนดนโยบายการสำรองข้อมูลส่วนบุคคลที่มีความสำคัญทั้งหมดให้ครบถ้วนเพื่อให้ข้อมูลส่วนบุคคลดังกล่าวพร้อมใช้งานได้ตลอดเวลาโดยไม่หยุดชะงักตามขอบระยะเวลาที่เหมาะสมเป็นปกติ ทั้งนี้ บริษัทกำหนดจัดให้มีการทดสอบการสำรองข้อมูลและกระบวนการกู้คืนข้อมูลตามกรอบระยะเวลาที่เหมาะสมตามความเสี่ยงที่ประเมินไว้

9.8 บริษัทกำหนดกระบวนการในการควบคุมและรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคลโดยผู้ให้บริการภายนอกอย่างชัดเจน โดยกำหนดมาตรฐานตั้งแต่กระบวนการคัดเลือกผู้ให้บริการภายนอก การจัดทำสัญญาการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ผู้ให้บริการภายนอกอาจเข้าถึงโดยจำกัดการเข้าถึงและการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น พร้อมทั้งรับประกันการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ให้บริการดังกล่าวให้ได้มาตรฐานเดียวกันกับมาตรฐานของบริษัท ทั้งนี้ หน่วยงานที่จ้างผู้ให้บริการดังกล่าวมีหน้าที่ในการติดตามและตรวจสอบการปฏิบัติหน้าที่ของผู้ให้บริการภายนอกให้เป็นไปตามมาตรฐานที่กำหนดตามกำหนดระยะเวลาเป็นปกติ โดยหากพบความผิดปกติหรือการละเมิดให้ดำเนินการลงโทษผู้ให้บริการดังกล่าวทันทีโดยรับประกันไม่ให้เกิดผลกระทบต่อความต่อเนื่องในการให้บริการของบริษัท

9.9 บริษัทต้องทบทวนนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามการประเมินความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้ง

ข้อ 10 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

10.1 บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการกำหนดนโยบายและมาตรการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลเป็นเหตุละเมิดข้อมูลส่วนบุคคล โดยประสานกับหน่วยงานที่เกี่ยวข้องใน 1st Line of Defence และหน่วยงานตรวจสอบ

10.2 กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคลที่กำหนดนิยามไว้ บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ทำหน้าที่รับแจ้งเหตุการณ์และบริหารจัดการเหตุการณ์ดังกล่าวก่อน รวมถึงต้องทำหน้าที่ในการรายงานเหตุการณ์ดังกล่าวให้คณะกรรมการบริษัททราบเพื่อจัดเตรียมเอกสารรายงานจัดส่งให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในกรอบระยะเวลาการรายงาน 72 ชั่วโมงนับแต่ทราบเหตุและให้แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลกรณีได้รับผลกระทบ

10.3 ภายหลังสิ้นสุดเหตุละเมิดดังกล่าว คณะทำงานคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการตรวจสอบและ สอบทาน เพื่อพิจารณา Root Cause ของเหตุการณ์ดังกล่าวเพื่อจัดทำรายงานเสนอต่อคณะกรรมการ บริษัททราบและเพื่อเป็นแผนการในการปรับปรุงแก้ไขป้องกันเหตุละเมิดที่อาจเกิดขึ้นในอนาคตต่อไป

10.4 บริษัทต้องทบทวนแผนการดำเนินการเพื่อบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนดังกล่าว

ข้อ 11 การทบทวนหรือปรับปรุงนโยบาย

บริษัทกำหนดให้มีการทบทวนหรือปรับปรุงนโยบายฉบับนี้โดยกรรมการของบริษัทซึ่งพิจารณาจากรายงานการปฏิบัติตามนโยบายการบริหารจัดการคุ้มครองการประมวลผลข้อมูลที่น่าเสนอโดยคณะทำงานคุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้ง หรือกรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อธุรกิจบริษัทหรือกระบวนการประมวลผลข้อมูลส่วนบุคคลที่บริษัทดำเนินการเพื่อให้เป็นนโยบายเป็นปัจจุบันอยู่เสมอ

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ มีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2565 เป็นต้นไป

นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ได้ผ่านการพิจารณา โดยที่ประชุมคณะกรรมการตรวจสอบ ครั้งที่ 4/2564 เมื่อวันที่ 10 พฤศจิกายน 2564 และได้รับการอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 4/2564 เมื่อวันที่ 10 พฤศจิกายน 2564

-นายฉัตรชัย ดวงรัตนพันธ์-
(นายฉัตรชัย ดวงรัตนพันธ์)
ประธานกรรมการบริษัท
บริษัท ดูโฮม จำกัด (มหาชน)