



ประกาศกลุ่มบริษัท ซีวิลเอนจิเนียริง จำกัด (มหาชน)

ฉบับที่ 1/2565

เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล

ด้วยคณะกรรมการของบริษัท ซีวิลเอนจิเนียริง จำกัด (มหาชน) และบริษัทในเครือ เห็นถึงความสำคัญในการประมวลผลข้อมูลส่วนบุคคลให้เหมาะสมและถูกต้องตามกฎหมาย คณะกรรมการบริษัทจึงอนุมัติรับรองและออกประกาศบริษัท เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ขึ้น เพื่อกำหนดกรอบการประมวลผลข้อมูลส่วนบุคคลในกระบวนการของบริษัท เพื่อไม่ให้กระทบสิทธิภายใต้กรอบกฎหมายของเจ้าของข้อมูลแต่ละกลุ่มมากเกินไป รวมถึงเป็นนโยบายการกำกับดูแล และบริหารจัดการการประมวลผลข้อมูลดังกล่าวให้ถูกต้องตามมาตรฐานที่ระบุไว้โดยหน่วยงานกำกับดูแล โดยมีจุดประสงค์ให้พนักงานและบุคคลที่เกี่ยวข้องของบริษัทยึดถือและปฏิบัติตาม ภายใต้รายละเอียด ดังนี้

ข้อ 1 นโยบายและคู่มือการคุ้มครองข้อมูลส่วนบุคคล

1.1) ประกาศฉบับนี้เรียกว่า “ประกาศกลุ่มบริษัท เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล” โดยให้มีผลบังคับใช้นับแต่วันที่บริษัทประกาศเป็นต้นไป โดยให้มีผลบังคับใช้ กับ บริษัท ซีวิลเอนจิเนียริง จำกัด (มหาชน) และ บริษัทในเครือทั้งหมด ได้แก่ บริษัท ซีวิล คอนสตรัคชั่น เซอร์วิส เซส แอนด์ โปรดัคส์ จำกัด, บริษัท เดอะ ซี.อี.ซี. คอนสตรัคชั่น จำกัด และ บริษัท ซีวิล เอส.ที.ที. จำกัด

1.2) อาศัยอำนาจของประกาศบริษัทฉบับนี้ บริษัทอาจพิจารณากำหนดและประกาศคู่มือการปฏิบัติงานโดยละเอียด เพื่อกำหนดแนวทางการปฏิบัติต่าง ๆ ในการรับประกันความสมบูรณ์ ถูกต้อง และครบถ้วนในการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องเพิ่มเติม โดยให้คู่มือการปฏิบัติงานดังกล่าวมีผลบังคับสมบูรณ์เช่นเดียวกันกับประกาศฉบับนี้

ข้อ 2 โครงสร้างการบริหารจัดการและกำกับการประมวลผลข้อมูลส่วนบุคคล

เพื่อรับประกันการกำกับดูแลและบริหารจัดการด้านการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลให้สมบูรณ์ บริษัทกำหนดจัดตั้งโครงสร้างดังต่อไปนี้

2.1) คณะกรรมการบริษัทมอบหมายให้ คณะกรรมการบริหารมีหน้าที่หลักในการกำหนดทิศทางและการกำกับการประมวลผลข้อมูลส่วนบุคคลในภาพรวมของบริษัท รวมถึงบริหารจัดการความเสี่ยงที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคล โดยให้มีบทบาทหลักในการตรวจสอบและอนุมัติทุกนโยบายย่อย และคู่มือแนวทางการปฏิบัติที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล และรายงานต่อคณะกรรมการบริษัทให้ได้รับทราบ

2.2) เพื่อกำกับดูแลการปฏิบัติงานการประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามนโยบายและสอดคล้องกับกรอบกฎหมาย บริษัทกำหนดกลไกกำกับการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลภายใต้รูปแบบโครงสร้าง 3 Lines of Defence ดังนี้

(1) 1st Line of Defence: Risk Owner ได้แก่ ประธาน หรือหัวหน้าแผนก/หน่วยงานภายใน ซึ่งมีหน้าที่รับผิดชอบโดยตรงในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของพนักงานภายในหน่วยงานของตน ให้ถูกต้องและสอดคล้องกับนโยบายและกฎหมายที่เกี่ยวข้อง

(2) 2nd Line of Defence: Risk Control กำหนดให้มีการแต่งตั้งคณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Working Committee) ซึ่งประกอบด้วยหัวหน้าฝ่ายที่มีการประมวลผลข้อมูลส่วนบุคคลต่างๆ ในบริษัท ทำงานร่วมกับหน่วยงานกำกับดูแลการปฏิบัติงาน โดยการทำงานของคณะทำงานดังกล่าวต้องเป็นไปอย่างอิสระภายใต้หลักการสอบยืนยันการปฏิบัติงาน (Maker – Checker) ซึ่งบริษัทจะได้ออกประกาศในการแต่งตั้งโครงสร้างคณะทำงานดังกล่าว พร้อมทั้งกำหนดบทบาทหน้าที่ของคณะทำงานดังกล่าวเป็นประกาศต่างหาก



(3) 3rd Line of Defence: Risk Assurance ได้แก่ คณะกรรมการหรือหน่วยงานตรวจสอบ ซึ่งมีหน้าที่กำกับดูแล และตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลของทุกหน่วยงานอีกครั้งโดยดำเนินการเป็นปกติ ทั้งนี้อาจเป็นหน่วยงานตรวจสอบกำกับดูแลภายใน หรือภายนอกตามแต่ การพิจารณาตามความเหมาะสมโดยคณะกรรมการบริหาร

2.3) บริษัทกำหนดจัดสรรทรัพยากรอย่างเพียงพอทั้งในแง่ของระบบงาน บุคลากร และงบประมาณ ในการสนับสนุนการปฏิบัติงานของแต่ละหน่วยงานกำกับดูแล ตามนโยบายและมาตรฐานการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลในทูลส่วน

ข้อ 3 การประเมินและบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

3.1) บริษัทกำหนดให้มีการประเมินและทบทวนการประเมินความเสี่ยง การประมวลผลข้อมูลส่วนบุคคล ในภาพรวมขององค์กร (Enterprise Risk Management Level) อย่างน้อยปีละ 1 ครั้งหรือทุกครั้งที่มีการเปลี่ยนแปลงของรูปแบบการประมวลผลข้อมูลส่วนบุคคลอย่างมีสาระสำคัญ

3.2) บริษัทกำหนดให้แต่ละหน่วยงานใน 1st Line of Defence ที่ระบุไว้ในข้อ 2.2 มีหน้าที่และความรับผิดชอบในการประเมิน ทบทวน และบริหารจัดการความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลภายในหน่วยงานของตน รวมถึงการติดตาม และรายงานผลด้านความเสี่ยงให้แก่คณะทำงานคุ้มครองข้อมูลส่วนบุคคล

3.3) บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ในฐานะผู้รับผิดชอบหลักในส่วนที่เกี่ยวข้องกับ การประมวลผลข้อมูลส่วนบุคคลของบริษัทรวบรวม และจัดทำเอกสารการประเมินรวมถึงทบทวนการประมวลผลบริหารจัดการความเสี่ยงของบริษัทในภาพรวม โดยคำนึงถึงกรอบ “ความเสี่ยงที่ยอมรับได้ด้านการประมวลผลข้อมูลส่วนบุคคลของบริษัท” และรายงานต่อคณะกรรมการบริหาร เพื่อพิจารณาและอนุมัติรับรองแผนการบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท

3.4) บนพื้นฐานการประเมินความเสี่ยงในระดับองค์กร สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ซึ่งอาจนำไปสู่การเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญของเจ้าของข้อมูลส่วนบุคคล หรือที่จะทำให้เจ้าของข้อมูลไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ บริษัทกำหนดให้ต้องมีการจัดการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Processing Impact Assessment: DPIA) เฉพาะกิจกรรมการประมวลผลข้อมูลส่วนบุคคลความเสี่ยงสูงดังกล่าวเพิ่มขึ้น ก่อนการตัดสินใจประมวลผลข้อมูลส่วนบุคคลดังกล่าว โดยต้องทำรายงานกระบวนการประเมินความเสี่ยงดังกล่าวเป็นลายลักษณ์อักษร เพื่อการตรวจสอบ

ทั้งนี้ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ต้องดำเนินการภายใต้หลักการ ดังนี้

- (1) ต้องมีการอธิบายรายละเอียดขอบเขตการประเมินผลวัตถุประสงค์ และความจำเป็นในการประมวลผลข้อมูลดังกล่าว
- (2) ต้องมีกระบวนการปรึกษาหารือกับผู้มีส่วนเกี่ยวข้องต่าง ๆ ทั้งภายในและภายนอกองค์กร ซึ่งรวมถึงเจ้าของข้อมูลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- (3) ต้องมีคำอธิบายที่ชัดเจนเกี่ยวกับความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล
- (4) ต้องจัดให้มีการประเมินความเสี่ยงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยคำนึงถึง “ความน่าจะเป็น” (likelihood) และ “ความร้ายแรง” (severity)
- (5) ต้องกำหนดรายละเอียดมาตรการในการลดความเสี่ยงที่ระบุไว้ และคำอธิบายเกี่ยวกับมาตรการที่เหมาะสมในการลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลดังกล่าว ให้อยู่ในเกณฑ์ความเสี่ยงที่ยอมรับได้ที่บริษัทกำหนดไว้ในกรอบการประเมินความเสี่ยงระดับองค์กร



ข้อ 4 การสื่อสารประชาสัมพันธ์นโยบาย

4.1) บริษัทให้ความสำคัญต่อการสื่อสารนโยบายและแนวทางการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลให้แก่พนักงาน รวมถึงผู้ให้บริการภายนอกทั้งหมดของบริษัทที่มีส่วนเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยและในนามบริษัท โดยกำหนดเป็นนโยบายให้มีการสื่อสารผ่านทุกช่องทางการติดต่อกับพนักงานและผู้ให้บริการภายนอก ดังกล่าวอย่างเป็นปกติ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญและกระทบต่อการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท

4.2) บริษัทกำหนดให้เป็นหน้าที่ของแต่ละหน่วยงานที่ดำเนินการประมวลผลข้อมูลส่วนบุคคล ในการสื่อสาร และจัดการฝึกอบรม รวมถึงสร้างความตระหนักรู้ต่าง ๆ ให้พนักงานภายในแผนกหรือฝ่ายของตน รวมถึงผู้ให้บริการภายนอกที่อยู่ภายใต้สังกัดและการดูแลของหน่วยงาน หรือแผนกดังกล่าวรับทราบเพื่อให้มั่นใจว่าบุคคลดังกล่าวตระหนักรู้ถึงความสำคัญของสิทธิของเจ้าของข้อมูล รวมถึงหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งหมดนั้น

ข้อ 5 กลไกการกำกับดูแลและตรวจสอบ

บริษัทกำหนดกลไกการติดตามตรวจสอบการปฏิบัติตามนโยบายการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักการ ดังนี้

5.1) บริษัทกำหนดกลไกการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคล ตาม 3 Lines of Defence ที่ระบุไว้ในข้อ 2.2 โดยให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลทำหน้าที่ติดตามและตรวจสอบการปฏิบัติตามนโยบายของบริษัทที่กำหนดไว้ ทั้งส่วนของพนักงานและผู้ให้บริการภายนอก และรายงานผลต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง หรือกรณีมีภาระเมื่อดังกล่าวมีความสำคัญต่อธุรกิจ หรือชื่อเสียงของบริษัท

5.2) บริษัทกำหนดแผนการว่าจ้างผู้ตรวจสอบอิสระภายนอก มาดำเนินการตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของบริษัท พร้อมทั้งรายงานผลการตรวจสอบต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงอันสำคัญในบริษัท

5.3) กรณีที่ตรวจพบการฝ่าฝืนนโยบายการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคลจะเป็นหน่วยงานรับเรื่องร้องเรียน และทำหน้าที่ตรวจสอบจนทราบข้อเท็จจริง หากพบว่าเกิดการฝ่าฝืนหรือละเมิดนั้นจริง คณะทำงานจะเสนอไปยังคณะกรรมการของบริษัท เพื่อพิจารณากำหนดมาตรการลงโทษทางวินัยตามระเบียบบริหารงานบุคคลต่อไป

ข้อ 6 การจัดทำบันทึกการการประมวลผลข้อมูลส่วนบุคคล (Report of Processing)

6.1) บริษัทกำหนดให้แต่ละหน่วยงานใน 1st Line of Defence ที่ระบุไว้ในข้อ 2.2 เป็นหน่วยงานผู้รับผิดชอบในการจัดทำและปรับปรุงรายการการประมวลผลข้อมูลดังกล่าวอย่างสม่ำเสมอ โดยต้องดำเนินการควบคู่ไปกับการประเมิน และการทบทวนการประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

6.2) บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลเป็นหน่วยงานให้ความรู้คำแนะนำ กำกับดูแลและตรวจสอบการจัดทำบันทึกการการประมวลผลข้อมูลส่วนบุคคลโดยแต่ละหน่วยงานใน 1st Line of Defence เพื่อรับประกันความถูกต้อง ครบถ้วน และสอดคล้องกับมาตรฐานและกฎหมายที่เกี่ยวข้อง

ข้อ 7 นโยบายการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก

7.1) บริษัทกำหนดการบริหารจัดการข้อมูลส่วนบุคคลโดยจัดระดับความลับของข้อมูลดังกล่าว เป็นข้อมูลความลับที่สุด (Strictly Confidential) ภายใต้หลักการในการรักษาความลับของบริษัท โดยเฉพาะกรณีที่จะมีการเปิดเผยส่งต่อข้อมูลส่วนบุคคลไปให้แก่หน่วยงานภายนอกองค์กร



7.2) บริษัทกำหนดให้พนักงานทุกคนมีหน้าที่การบันทึกการการประมวลผลข้อมูลส่วนบุคคลที่มีการส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกองค์กร โดยหากจำเป็นต้องมีการเปิดเผยข้อมูลส่วนบุคคลออกไปให้แก่หน่วยงานภายนอก จะต้องมีการตรวจสอบความจำเป็น รวมถึงความเสี่ยงในการส่งต่อข้อมูลส่วนบุคคลและความน่าเชื่อถือของผู้รับข้อมูลส่วนบุคคลดังกล่าวก่อน ทั้งนี้การส่งต่อหรือเปิดเผยแต่ละครั้งต้องได้รับความยินยอมจากผู้บังคับบัญชาตามอำนาจการอนุมัติ

7.3) ในกรณีการส่งต่อหรือรับข้อมูลส่วนบุคคลจากบุคคลภายนอกองค์กร บริษัทกำหนดนโยบายให้ต้องมีการลงนามในสัญญาหรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัท และบุคคลภายนอกดังกล่าว เพื่อกำหนดเงื่อนไขข้อกำหนดสิทธิและหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลระหว่างคู่สัญญาและรับประกันความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว

7.4) พนักงานผู้เปิดเผยหรือส่งต่อข้อมูลออกไปนอกองค์กร ต้องรับประกันปฏิบัติตามช่องทางและวิธีการส่งต่อหรือเปิดเผยข้อมูลของบริษัทกำหนดเพื่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยน้อยที่สุด รวมถึงหลีกเลี่ยงการส่งผ่านช่องทางส่วนตัวที่ไม่สามารถควบคุมได้

ข้อ 8 นโยบายการกำหนดระยะเวลาการรักษาข้อมูล

8.1) บริษัทกำหนดกรอบการกำหนดระยะเวลา ในการเก็บรักษาข้อมูลส่วนบุคคล ตามหลักการพิจารณาความจำเป็นเป็น ดังนี้

- (1) หากมีระยะเวลาตามกฎหมายระบุชัดเจนให้เก็บรักษาข้อมูลส่วนบุคคลส่วนใดไว้ เป็นระยะเวลานานเท่าใด ให้จัดเก็บตามกำหนดเวลานั้น และในกรณีการเก็บรักษาข้อมูลส่วนบุคคลส่วนใดอยู่ ภายใต้เกณฑ์การเก็บรักษาของกฎหมายที่แตกต่างกัน บริษัทกำหนดกรอบการเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นระยะเวลาตามกรอบเวลาสูงสุดที่กฎหมายทั้งหมดกำหนดไว้
- (2) กรณีเป็นการเก็บข้อมูลส่วนบุคคลเนื่องจากความจำเป็น ที่พิจารณาโดยอาศัยความสัมพันธ์ต่างๆ ที่บริษัทมีกับเจ้าของข้อมูลด้วยฐานสัญญา ให้เก็บข้อมูลไว้เท่าที่จำเป็นเพื่อการปฏิบัติตามหน้าที่ในสัญญาที่บริษัทมีกับเจ้าของข้อมูลดังกล่าว เช่น ตลอดระยะเวลาการให้บริการหรือตราบเท่าที่จะมีการยกเลิกสัญญา หรือความสัมพันธ์ที่เกี่ยวข้องซึ่งอาจมีระยะเวลาแน่นอนหรือไม่ก็เป็นได้ แต่มีกรอบระยะเวลาการเก็บรักษาที่ชัดเจนแน่นอนซึ่งคาดหมายได้โดยเจ้าของข้อมูล
- (3) กรณีเป็นการเก็บข้อมูลเพื่อประโยชน์อันชอบด้วยกฎหมายของบริษัท ให้เก็บข้อมูลดังกล่าวไว้ตามกรอบที่เหมาะสมเพื่อการใช้สิทธิและประโยชน์อันชอบด้วยกฎหมายนั้นในแต่ละกรณี ภายใต้หลักการดังนี้ เช่น ตามระยะเวลาอายุความกรณีการฟ้องร้องต่อผู้สิทธิต่างๆ ทั้งนี้สำหรับการเก็บรักษาข้อมูลส่วนบุคคลด้วยฐานประโยชน์อันชอบด้วยกฎหมาย บริษัทกำหนดหลักการสำคัญที่ต้องพิจารณา คือการเก็บรักษาข้อมูลส่วนบุคคลดังกล่าวต้องไม่กระทบสิทธิของเจ้าของข้อมูลมากเกินไป และบริษัทต้องให้สิทธิเจ้าของข้อมูลในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยฐานดังกล่าวได้ตามสิทธิที่มี
- (4) กรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานความยินยอม ให้เก็บข้อมูลได้ตราบเท่าที่เจ้าของข้อมูลยังไม่ได้ใช้สิทธิในการถอนความยินยอม ซึ่งเป็นสิทธิอิสระที่เจ้าของข้อมูลสามารถดำเนินการได้ ตลอดระยะเวลาและบริษัทเคารพสิทธิในการตัดสินใจดังกล่าว
- (5) กรณีข้อมูลส่วนบุคคลอ่อนไหว เช่น ประวัติอาชญากรรม หรือประวัติสุขภาพการรักษาพยาบาล หรือข้อมูลชีวภาพอื่นๆ ที่บริษัทอาจเก็บรักษาด้วยความยินยอมของเจ้าของข้อมูล บริษัทต้องใช้ความระมัดระวังในการเก็บรักษาข้อมูลส่วนบุคคลด้วยมาตรฐานที่สูงขึ้น โดยต้องลบหรือทำลายในทันทีที่หมดความจำเป็น



8.2) บริษัทกำหนดแจ้งกรอบระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลแต่ละฐาน เพื่อแต่ละจุดประสงค์ ให้เจ้าของข้อมูลแต่ละกลุ่มที่เกี่ยวข้องรับทราบ ในนโยบายข้อมูลส่วนบุคคลที่บริษัทจะจัดทำและแจ้ง เจ้าของข้อมูลเป็นลายลักษณ์อักษร

8.3) เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลตามกรอบที่กำหนดไว้ในข้อ 8.1 แล้ว บริษัทจะลบทำลายข้อมูลส่วนบุคคลดังกล่าว หรือจะดำเนินการทำให้ข้อมูลกลายเป็นข้อมูลนิรนามขึ้นอยู่กับลักษณะของข้อมูล โดยต้องทำลายข้อมูลทั้งที่เป็นกระดาษเอกสาร และข้อมูลในระบบ

8.4) บริษัทกำหนดกระบวนการการตรวจสอบระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล โดยให้ฝ่ายที่เกี่ยวข้อง ซึ่งเป็นฝ่ายที่รับผิดชอบข้อมูลและเอกสารดังกล่าวโดยตรง มีหน้าที่ในการตรวจสอบระยะเวลาการเก็บรักษาข้อมูลตามนโยบายการเก็บรักษาที่ได้ประกาศไว้

8.5) กรณีที่บริษัทว่าจ้างผู้ให้บริการภายนอก เป็นผู้ทำลายข้อมูลส่วนบุคคลที่หมดความจำเป็นดังกล่าว บริษัทกำหนดให้ต้องมีการจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการนั้น เพื่อรับการประกันความสมบูรณ์ในการทำลายข้อมูลด้วยเทคนิคที่เหมาะสม

ข้อ 9 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

9.1) บริษัทกำหนดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ภายใต้หลักการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ภายใต้กรอบการรับประกัน ดังนี้

- (1) ข้อมูลทั้งหมดจะได้รับการเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ (Confidentiality) โดยถือว่า ข้อมูลส่วนบุคคลทั้งหมดโดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหวเป็นข้อมูลความลับสูงสุด
- (2) ข้อมูลทั้งหมดต้องเป็นข้อมูลที่ถูกต้องเชื่อถือได้เป็นไปตามข้อมูลที่ทางผู้เป็นเจ้าของข้อมูลได้ให้ข้อมูลดังกล่าวขึ้นมาโดยไม่เกิดการแก้ไขโดยไม่ได้รับอนุญาต (Integrity) และ
- (3) ข้อมูลต้องมีความพร้อมใช้งานได้ทันทีที่ต้องการ (Availability)

9.2) บริษัทกำหนดจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการผ่านโครงสร้างการจัดตั้งที่กำหนดขึ้น มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพภายใต้หลักการในการควบคุมเงื่อนไขการเข้าถึงและเข้าใช้ข้อมูลส่วนบุคคลในแต่ละระดับข้อมูลผ่านระบบ Authorization Matrix ตาม Role-Based การจัดการระบบ เพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึงการเปลี่ยนแปลง การลบ หรือถ่ายโอนข้อมูลส่วนบุคคลได้ โดยเฉพาะอย่างยิ่งกรณีส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอ่อนไหว

9.3) บริษัทกำหนดจัดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของการเข้าถึง เปลี่ยนแปลง ข้อมูลส่วนบุคคลในส่วนต่างๆ โดยกำหนดให้

- (1) หัวหน้าฝ่ายหรือหน่วยงานที่เกี่ยวข้องรับผิดชอบทำการสอบทานบันทึก Log ของพนักงานภายใต้กำกับดูแลของฝ่ายหรือหน่วยงานของตนตรวจความผิดปกติของ Log อย่างสม่ำเสมอ
- (2) ให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการตรวจสอบ ตรวจสอบ Log ดังกล่าวตามลำดับ Line of Defenses ที่เกี่ยวข้อง

9.4) ในการดำเนินการควบคุมและบริหารจัดการการประมวลผลข้อมูลส่วนบุคคลทั้งหมด บริษัทกำหนดให้ดำเนินการภายใต้กรอบ Maker-Checker และต้องมีการตรวจสอบทดสอบประสิทธิภาพในการทำงาน ของมาตรการและกลไกต่างๆ อย่างสม่ำเสมอ



9.5) บริษัทกำหนดกรอบนโยบายให้หน่วยงานต่างๆ ดำเนินการประมวลผลข้อมูลส่วนบุคคลทั้งหมด ผ่านระบบอิเล็กทรอนิกส์ที่ควบคุมการเข้าถึง และบันทึกการเข้าถึงได้มากกว่าการจัดเก็บข้อมูลเป็นกระดาษ ทั้งนี้ในกรณีจำเป็นต้องใช้ข้อมูลส่วนบุคคลในรูปแบบของกระดาษ ต้องจัดทำบันทึกการใช้ข้อมูลต้องมียุทธศาสตร์ Clean Desk และห้ามนำกระดาษที่มีข้อมูลส่วนบุคคลไปใช้ซ้ำ (Recycled) ต้องจัดเก็บใส่กล่องเรียบร้อยที่ระบุกำหนดระยะเวลาการเก็บข้อมูลดังกล่าว และหากจะมีการเคลื่อนย้ายข้อมูลดังกล่าวต้องดำเนินการตามกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล

9.6) กรณีที่บริษัทใช้เครื่องมืออุปกรณ์หรือทรัพย์สินสารสนเทศใด ในการเก็บและประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูล บริษัทต้องดำเนินการจัดทำทะเบียนทรัพย์สินดังกล่าวให้ครบถ้วน และโดยเฉพาะอย่างยิ่ง ต้องกำหนดจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลโดยผ่านทรัพย์สินสารสนเทศที่เป็นของพนักงานแต่ละคน (BYOD) ให้ชัดเจน เพื่อให้มีมาตรฐานในการรักษาความมั่นคงของข้อมูล ส่วนบุคคลในทุกอุปกรณ์ทรัพย์สินสารสนเทศ โดยควรจำกัดการใช้ BYOD เพื่อการเก็บรักษาหรือประมวลผลข้อมูลส่วนบุคคลให้เหลือน้อยที่สุดเพื่อป้องกันความเสี่ยงของการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล

9.7) บริษัทกำหนดนโยบายการสำรองข้อมูลส่วนบุคคลที่มีความสำคัญทั้งหมด ให้ครบถ้วนเพื่อให้ข้อมูลส่วนบุคคลดังกล่าวพร้อมใช้งานได้ตลอดเวลาโดยไม่หยุดชะงัก ตามขอบระยะเวลาที่เหมาะสมเป็นปกติ ทั้งนี้ บริษัทกำหนดจัดให้มีการทดสอบการสำรองข้อมูลและกระบวนการกู้คืนข้อมูลตามกรอบระยะเวลาที่เหมาะสมตามความเสี่ยงที่ประเมินไว้

9.8) บริษัทกำหนดกระบวนการในการควบคุม และรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคลโดยผู้ให้บริการภายนอกอย่างชัดเจน โดยกำหนดมาตรฐานตั้งแต่กระบวนการคัดเลือกผู้ให้บริการภายนอก การจัดทำสัญญา การกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ผู้ให้บริการภายนอกอาจเข้าถึง โดยจำกัดการเข้าถึงและการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น พร้อมทั้งรับประกันการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของผู้ให้บริการดังกล่าวให้ได้มาตรฐานเดียวกันกับมาตรฐานของบริษัท ทั้งนี้ หน่วยงานที่จ้างผู้ให้บริการดังกล่าวมีหน้าที่ในการติดตาม และตรวจสอบการปฏิบัติหน้าที่ของผู้ให้บริการภายนอกให้เป็นไปตามมาตรฐานที่กำหนดตามกำหนดระยะเวลาเป็นปกติ โดยหากพบความผิดปกติหรือการละเมิดให้ดำเนินการลงโทษผู้ให้บริการดังกล่าวทันที โดยรับประกันไม่ให้เกิดผลกระทบต่อความต่อเนื่องในการให้บริการของบริษัท

9.9) บริษัทต้องทบทวนนโยบายและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามการประเมินความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้ง

ข้อ 10 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

10.1) บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ในการกำหนดนโยบายและมาตรการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลเป็นเหตุละเมิดข้อมูลส่วนบุคคล โดยประสานกับหน่วยงานที่เกี่ยวข้องใน 1st Line of Defence และหน่วยงานตรวจสอบ

10.2) กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคลที่กำหนดนิยามไว้ บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล เป็นผู้ทำหน้าที่รับแจ้งเหตุการณ์และบริหารจัดการเหตุการณ์ดังกล่าวก่อน รวมถึงต้องทำหน้าที่ในการรายงานเหตุการณ์ดังกล่าวให้คณะกรรมการบริหารทราบเพื่อจัดเตรียมเอกสารรายงานจัดส่งให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในกรอบระยะเวลาการรายงาน 72 ชั่วโมงนับแต่ทราบเหตุและให้แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลกรณีได้รับผลกระทบ

10.3) ภายหลังจากสิ้นสุดเหตุละเมิดดังกล่าว คณะทำงานคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการตรวจสอบและ สอบทานเพื่อพิจารณา Root Cause ของเหตุการณ์ดังกล่าว เพื่อจัดทำรายงานเสนอต่อคณะกรรมการบริหารและคณะกรรมการบริหารทราบ และเพื่อเป็นแผนการในการปรับปรุงแก้ไขป้องกันเหตุละเมิดที่อาจเกิดขึ้นในอนาคตต่อไป

10.4) บริษัทต้องทบทวนแผนการดำเนินการเพื่อบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบต่อแผนดังกล่าว

**ข้อ 11 การทบทวนหรือปรับปรุงนโยบาย**

บริษัทกำหนดให้มีการทบทวนหรือปรับปรุงนโยบายฉบับนี้โดยกรรมการของบริษัท โดยพิจารณาจากรายงานการปฏิบัติตามนโยบายการบริหารจัดการคุ้มครองการประมวลผลข้อมูล ที่นำเสนอโดยคณะทำงานคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้งหรือกรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อธุรกิจบริษัท หรือกระบวนการประมวลผลข้อมูลส่วนบุคคลที่บริษัทดำเนินการเพื่อให้นโยบายเป็นปัจจุบันอยู่เสมอ

ประกาศ ณ วันที่ 25 เมษายน 2565

นายชัยวัฒน์ อุทัยวรรณ

ประธานคณะกรรมการบริษัท

บริษัท ซีวิลเอนจิเนียริง จำกัด (มหาชน)