ประกาศ บริษัท เจมาร์ท กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน)

ฉบับที่ [2]/2566

เรื่อง นโยบายคุ้มครองการประมวลผลข้อมูลส่วนบุคคลของกลุ่ม บริษัท เจมาร์ท กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน)

ด้วยคณะกรรมการบริษัท เจมาร์ท กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) (“บริษัท”) เห็นถึงความสำคัญในการประมวลผลข้อมูลส่วนบุคคลให้เหมาะสมและถูกต้องตามกฎหมาย โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้อง คณะกรรมการบริษัทจึงอนุมัติรับรองและออกประกาศบริษัท เรื่อง นโยบายคุ้มครองการประมวลผลข้อมูลส่วนบุคคลของกลุ่มบริษัท เจมาร์ท กรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) ฉบับนี้ขึ้น เพื่อกำหนดกรอบการประมวลผลข้อมูลส่วนบุคคลในกระบวนการดำเนินงานต่าง ๆ ของบริษัท และบริษัทในเครือ เพื่อไม่ให้กระทบสิทธิภายใต้กรอบกฎหมายของเจ้าของข้อมูลแต่กลุ่มมากสมควร รวมถึงเป็นนโยบายการกำกับดูแล และบริหารจัดการการประมวลผลข้อมูลดังกล่าวให้ถูกต้องตามมาตรฐานที่ระบุไว้โดยหน่วยงานกำกับดูแล โดยมีจุดประสงค์ให้พนักงานและบุคคลที่เกี่ยวข้องของบริษัทยึดถือและปฏิบัติตาม ภายใต้รายละเอียด ดังนี้

ข้อ 1 ประกาศและผลบังคับใช้ของประกาศ

1.1 ประกาศฉบับนี้เรียกว่า “ประกาศบริษัท เรื่อง นโยบายคุ้มครองการประมวลผลข้อมูลส่วนบุคคลของกลุ่มบริษัท เจมาร์ท” โดยให้มีผลบังคับใช้นับแต่วันที่บริษัทประกาศเป็นต้นไป

1.2 ประกาศฉบับนี้ให้ใช้ครอบคลุมการประมวลผลข้อมูลส่วนบุคคลทั้งหมดของทุกกลุ่มเจ้าของข้อมูลที่ดำเนินการโดยตรงกับบริษัท รวมถึงบริษัทในเครือ บริษัทที่เกี่ยวข้อง ซึ่งบริษัทมีขอบเขตความรับผิดชอบในการบริหารจัดการควบคุมดูแลความถูกต้องและสอดคล้องในการประมวลผลข้อมูลส่วนบุคคลของบริษัทดังกล่าว ซึ่งได้แก่

(1)บริษัท เจมาร์ท โมบาย จำกัด

(2)บริษัท เจ เอ็ม ที เน็ทเวอร์คเซอร์วิสเซ็ส จำกัด (มหาชน)

(3)บริษัท เจมาร์ท ประกันภัย จำกัด (มหาชน)

(4)บริษัท บริหารสินทรัพย์ เจ จำกัด

(5)บริษัท บริหารสินทรัพย์ เจเค จำกัด

(6)บริษัท เจเอเอส แอสเซ็ท จำกัด (มหาชน)

(7)บริษัท ซิงเกอร์ ประเทศไทย จำกัด (มหาชน)

(8)บริษัท เอสจี แคปปิตอล จำกัด (มหาชน)

(9)บริษัท เจ เวนเจอร์ส จำกัด

(10)บริษัท บีนส์แอนด์บราวน์ จำกัด

(11)บริษัท เจ อีลิท จำกัด

(12)บริษัท เจจีเอส ซินเนอร์จี พาวเวอร์ จำกัด

(13) บริษัท เคบี เจ แคปปิตอล จำกัด

(“บริษัทในเครือ”)

ข้อ 2 นิยามศัพท์ และหลักการสำคัญในการประมวลผลข้อมูลส่วนบุคคล

2.1 คำนิยามสำคัญภายใต้นโยบายคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ ให้มีความหมายโดยสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ดังนี้

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลส่วนบุคคลอ่อนไหว” หมายถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนและอาจสุ่มเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคล ในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

2.2 หลักการสำคัญในการประมวลผลข้อมูลส่วนบุคคล

บริษัทและบริษัทในเครือจะประมวลผลข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ และฐานอันชอบด้วยกฎหมายในการประมวลผล ทั้งนี้ จะยึดถือตามกรอบการประมวลผลข้อมูลส่วนบุคคลที่ระบุไว้ภายใต้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยเฉพาะต้องรับประกันประมวลผลข้อมูลส่วนบุคคล เพียงเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ที่บริษัทและบริษัทในเครือมีกับแต่ละกลุ่มเจ้าของข้อมูลเป็นหลักเท่านั้น ทั้งนี้ ก่อนที่บริษัทหรือบริษัทในเครือจะดำเนินการเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคล บริษัทและบริษัทในเครือต้องแจ้งให้เจ้าของข้อมูลแต่ละกลุ่มรับทราบ และ/หรือให้ความยินยอมในรูปแบบต่าง ๆ อย่างเหมาะสม สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

ข้อ 3 คู่มือและคำแนะนำในการปฏิบัติตามประกาศ

โดยอาศัยอำนาจของประกาศบริษัทฉบับนี้ บริษัทและ/หรือบริษัทในเครืออาจพิจารณากำหนด และประกาศคู่มือการปฏิบัติงานโดยละเอียดเพื่อกำหนดแนวทางการปฏิบัติต่าง ๆ ด้วยจุดประสงค์รับประกันความสมบูรณ์ ถูกต้อง และครบถ้วนในการคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้องเพิ่มเติม โดยให้คู่มือการปฏิบัติงานดังกล่าวมีผลบังคับสมบูรณ์เช่นเดียวกันกับประกาศฉบับนี้

ข้อ 4 โครงสร้างการบริหารจัดการและกำกับการประมวลผลข้อมูลส่วนบุคคล

เพื่อรับประกันการกำกับดูแล และบริหารจัดการด้านการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลให้สมบูรณ์ถูกต้องสอดคล้องกับพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัทกำหนดจัดตั้งโครงสร้างดังต่อไปนี้

4.1 บริษัทกำหนดให้ดำเนินการบริหารจัดการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลทั้งหมดของบริษัท และบริษัทในเครือ ภายใต้รูปแบบโครงสร้าง 3 Lines of Defense ดังนี้

- 1st Line of Defense: Risk Owner ได้แก่ หัวหน้าฝ่าย/หน่วยงานภายในของแต่ละบริษัทและบริษัทในเครือ ซึ่งมีหน้าที่รับผิดชอบโดยตรง ในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลภายในหน่วยงานของตน ให้ถูกต้องและสอดคล้อง

- 2nd Line of Defense: Risk Control กำหนดให้มีการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัท (Group Data Protection Committee) เพื่อทำหน้าที่เป็นหน่วยงานหลักใจกลางในการติดตามและตรวจสอบการปฏิบัติหน้าที่ของ Risk Owner และการประมวลผลข้อมูลส่วนบุคคลทั้งหมดของบริษัทและบริษัทในเครือ ทั้งนี้ คณะกรรมการบริษัทจะกำหนดประกาศการแต่งตั้งโครงสร้าง อำนาจหน้าที่และกลไกการประสานงานเพื่อการดำเนินงานของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว เป็นการเฉพาะแต่ต้องดำเนินการโดยสอดคล้องกับนโยบายฉบับนี้

- 3rd Line of Defense: Risk Assurance ได้แก่ คณะกรรมการตรวจสอบ (Audit Committee) ซึ่งมีหน้าที่กำกับดูแลและตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลของทุกหน่วยงานในบริษัทและบริษัทในเครือ ให้ถูกต้องสอดคล้องอีกครั้ง

4.2 บริษัทและบริษัทในเครือรับปะกันต้องจัดสรรทรัพยากรทั้งในแง่ของระบบงาน บุคลากร และงบประมาณอย่างเพียงพอในการสนับสนุนการปฏิบัติงานของแต่ละหน่วยงานให้เป็นไปตามนโยบายการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลฉบับนี้

ข้อ 5 การประเมินและบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

5.1 บริษัทและบริษัทในเครือกำหนดให้แต่ละหน่วยงานใน 1st Line of Defense ทำหน้าที่ประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคลภายในการทำงานของฝ่ายงานของตน เป็นส่วนหนึ่งของการประเมินความเสี่ยงภาพรวมขององค์กร (Enterprise Risk Management Level) เป็นประจำหรือทุกครั้งที่มีการเปลี่ยนแปลงเพิ่มเติมรูปแบบการประมวลผลข้อมูลส่วนบุคคลจากที่ได้ประเมินไว้ ภายใต้หลักการที่หน่วยงานใน 1st Line of Defense ต้องส่งผลการประเมินความเสี่ยงของตนให้แก่

2nd Line of Defense (คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของกลุ่มบริษัท) ประเมิน ตรวจสอบ และรวบรวมเป็นการประเมินความเสี่ยง ด้านการประมวลผลข้อมูลส่วนบุคคลภาพรวมของบริษัท บริษัทในเครือ และกลุ่มบริษัทอีกครั้ง

5.2 บนพื้นฐานการประเมินความเสี่ยงที่จัดทำขึ้น สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง ที่จะมีผลกระทบถึงสิทธิเสรีภาพของบุคคล ซึ่งอาจนำไปสู่ความเสี่ยงการเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัยสำคัญของเจ้าของข้อมูลส่วนบุคคล หรือที่จะทำให้เจ้าของข้อมูลไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ บริษัทและบริษัทในเครือกำหนดให้หน่วยงานที่เกี่ยวข้อง ต้องจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ Data Processing Impact Assessment เพิ่มขึ้นก่อนการตัดสินใจดำเนินการประมวลผลข้อมูลส่วนบุคคลกรณีดังกล่าว

5.3 ในการดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Processing Impact Assessment) หน่วยงานที่เกี่ยวข้องต้องดำเนินการภายใต้หลักการ ดังนี้ (1) ต้องมีการอธิบายรายละเอียดการประมวลผลข้อมูลดังกล่าวซึ่งระบุถึงขอบเขตการประเมินผลวัตถุประสงค์ความจำเป็นในการประมวลผลข้อมูลดังกล่าว (2) ต้องมีกระบวนการปรึกษา หารือกับผู้มีส่วนเกี่ยวข้องต่าง ๆ ได้แก่ เจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง โดยต้องจัดทำกระบวนการปรึกษาหารือทั้งภายในและภายนอกองค์กร (3) ต้องมีคำอธิบายที่ชัดเจนเกี่ยวกับความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล (4) การจัดให้มีการประเมินความเสี่ยงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยคำนึงถึง “ความน่าจะเป็น” (likelihood) และ “ความรุนแรงของผลกระทบ” (severity) (5) ระบุรายละเอียดมาตรการในการลดความเสี่ยงในทะเบียนความเสี่ยง

ข้อ 6 การสื่อสารประชาสัมพันธ์นโยบาย

บริษัทและบริษัทในเครือให้ความสำคัญต่อการสื่อสารนโยบายเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ให้แก่พนักงานทั้งหมด รวมถึงบุคคลภายนอกอาจมีส่วนเกี่ยวข้อง หรือได้รับว่าจ้างให้ดำเนินการประมวลผลข้อมูลส่วนบุคคลของบริษัทและบริษัทในเครือรับทราบ และตระหนักถึงความสำคัญ โดยบริษัทและบริษัทในเครือกำหนดนโยบายให้มีการสื่อสารผ่านทุกช่องทางการติดต่อกับพนักงาน และบุคคลดังกล่าวอย่างเป็นปกติ โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญ และกระทบต่อการประมวลผลข้อมูลส่วนบุคคลของบริษัทหรือบริษัทในเครือ หรือการ เปลี่ยนแปลงในนโยบายฉบับนี้

ข้อ 7 กลไกการกำกับดูแลและตรวจสอบ

บริษัทและบริษัทในเครือ กำหนดกลไกการติดตามตรวจสอบการปฏิบัติตามนโยบายการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักการ ดังนี้

7.1 บริษัทและบริษัทในเครือกำหนดให้หน่วยงานภายใต้โครงสร้าง 3 Lines of Defense ทำหน้าที่ในการกำกับดูแล โดยให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัท ทำหน้าที่เป็นศูนย์กลางและหน่วยงานหลักในการติดตามและตรวจสอบการประมวลผลข้อมูลส่วนบุคคลของทั้งองค์กรให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล และสอด คล้องกับนโยบายฉบับนี้ โดยให้มีการวางแผนในการตรวจสอบเป็นปกติ และให้คณะกรรมการดังกล่าวทำหน้าที่ในการรายงานผลการติดตามและตรวจสอบต่อคณะกรรมการของบริษัท หรือคณะกรรมการอื่นที่คระกรรมการบริษัทอาจพิจารณามอบหมายให้ทำหน้าที่โดยเฉพาะเกี่ยวกับ

การประมวลผลข้อมูลส่วนบุคคลอย่างน้อยปีละ 1 ครั้ง หรือ ทันทีทุกครั้งกรณีมีการเหตุการณ์ละเมิดข้อมูลส่วนบุคคลอย่างมีนัยสำคัญต่อธุรกิจหรือชื่อเสียงของบริษัท

7.2 เพื่อรับประกันกลไกการตรวจสอบ และกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของบริษัทและบริษัทในเครือเพิ่มเติม บริษัทหรือบริษัทในเครืออาจพิจารณาว่าจ้างผู้ตรวจสอบอิสระจากภายนอก เพื่อทำหน้าที่ดังกล่าว พร้อมทั้งรายงานผลการตรวจสอบต่อคณะกรรมการบริษัท หรือคณะกรรมการอื่นที่อาจได้รับการมอบหมายให้ทำหน้าที่คุ้มครองการประมวลผลข้อมูลส่วนบุคคล ตามแต่ละระยะเวลาที่บริษัทอาจเห็นสมควร

7.3 กรณีที่ตรวจพบการฝ่าฝืนนโยบาย หรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัทจะเป็นหน่วยงานรับเรื่องร้องเรียน กำกับดูแล รวมถึงทำหน้าที่ตรวจสอบจนทราบข้อเท็จจริง หากพบว่าเกิดการฝ่าฝืนหรือละเมิดนั้นจริง และเป็นกรณีเหตุการณ์ดังกล่าวเกิดจากความผิด หรือความบกพร่องของพนักงานใด คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัทจะเสนอไปยังคณะกรรมการของบริษัทหรือบริษัทในเครือของแต่ละบริษัท เพื่อพิจารณากำหนดมาตรการลงโทษตามมาตรการลงโทษทางวินัยตามระเบียบบริหารงานบุคคลต่อไป

ข้อ 8 การจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล (Record of Processing)

บริษัทและบริษัทในเครือกำหนดให้แต่ละแผนกหรือฝ่ายใน 1st Line of Defense เป็นหน่วยงานผู้รับผิดชอบในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) และปรับปรุงรายการการประมวลผลข้อมูลดังกล่าวอย่างสม่ำเสมอ โดยให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัทเป็นผู้ตรวจสอบ และให้คำแนะนำในการจัดทำ รวมถึงปรับปรุงบันทึกรายการดังกล่าว ทั้งนี้บันทึกดังกล่าวจะถูกใช้ เพื่อเป็นพื้นฐานในการประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคลของหน่วยงาน และใช้เป็นพื้นฐานหลักในการจัดทำนโยบายความเป็นส่วนตัว และนโยบายข้อมูลส่วนบุคคลของแต่ละกลุ่มเจ้าของข้อมูล

ข้อ 9. นโยบายการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก (Information Disclosure Policy)

9.1 บริษัทและบริษัทในเครือกำหนดนโยบายหลักที่จะไม่แบ่งปัน ขาย ส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลด้วยวิธีการอื่นใดต่อบุคคลภายนอก โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล เว้นแต่มีกฎหมายอนุญาต หรือเป็นกรณีการเปิดเผยที่บริษัทมีความจำเป็นในการดำเนินการดังกล่าว เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามสัญญาที่บริษัทหรือบริษัทในเครืออาจมีกับเจ้าของข้อมูลส่วนบุคคล หรือเพื่อการปกป้องสิทธิอันชอบด้วยกฎหมายของบริษัท โดยบริษัทรับประกันดำเนินการตามข้อกำหนดข้อ 9.2 นี้อย่างเคร่งครัด

9.2 ในกรณีที่มีความจำเป็นต้องส่งต่อ หรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกองค์กร ภายใต้กรอบการพิจารณาตามที่กำหนดไว้ในข้อ 9.1 บริษัทและบริษัทในเครือกำหนดนโยบายดำเนินการ ดังนี้

- จะต้องมีการตรวจสอบความจำเป็น รวมถึงความเสี่ยงในการส่งต่อข้อมูลส่วนบุคคล และความน่าเชื่อถือของผู้รับข้อมูลส่วนบุคคลดังกล่าวก่อน

- การส่งต่อหรือเปิดเผยแต่ละครั้งต้องได้รับความยินยอมจากผู้บังคับบัญชาตามอำนาจการอนุมัติ

- หน่วยงานที่ส่งต่อเปิดเผยข้อมูลส่วนบุคคลออกไปภายนอก มีหน้าที่บันทึกรายการการประมวลผลข้อมูลส่วนบุคคลการส่งต่อเปิดเผยข้อมูลออกไปนอกองค์กรดังกล่าว และต้องทำหน้าที่ในการติดตามตรวจสอบการทำงาน โดยเฉพาะการประมวลผลข้อมูลส่วนบุคคลโดยบุคคลภายนอกนั้นอย่างใกล้ชิด

- พนักงานผู้เปิดเผยหรือส่งต่อข้อมูล ต้องปฏิบัติการส่งต่อเปิดเผยข้อมูลผ่านช่องทางและวิธีการที่บริษัทกำหนดเพื่อให้มีความเสี่ยงด้านความมั่นคงปลอดภัยหรือการเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคลให้น้อยที่สุด รวมถึงหลีกเลี่ยงการส่งผ่านช่องทางส่วนตัวที่ไม่สามารถควบคุมได้

- ต้องมีการลงนามในสัญญา หรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัท/บริษัทในเครือ และบุคคลภายนอกดังกล่าวเพื่อกำหนดเงื่อนไขข้อกำหนดสิทธิ และหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลระหว่างคู่สัญญา และรับประกันความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว

ข้อ 10 นโยบายการกำหนดระยะเวลาการรักษาข้อมูล (Data Retention Guideline)

10.1 บริษัทและบริษัทในเครือกำหนดกรอบการพิจารณาระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Data Retention Guideline) โดยพิจารณาตามหลักการความจำเป็น ดังนี้ โดยบริษัทและบริษัทในเครือต้องทำหน้าที่ในการแจ้งระยะเวลาการรักษาข้อมูลดังกล่าวให้เจ้าของข้อมูลแต่ละกลุ่มทราบ

- หากมีระยะเวลาตามกฎหมายระบุชัดเจน ให้เก็บรักษาข้อมูลส่วนบุคคลส่วนใดไว้เป็นระยะเวลานานเท่าใด ให้จัดเก็บตามกำหนดเวลานั้น และหากมีหลายกฎหมายที่กำหนดให้มีการเก็บรักษาข้อมูล ให้เก็บไว้เป็นระยะเวลานานที่สุด

- กรณีการเก็บข้อมูลส่วนบุคคลจากความจำเป็นโดยอาศัยความสัมพันธ์ต่าง ๆ ที่บริษัทหรือบริษัทในเครือมีกับเจ้าของข้อมูล กล่าวคือ การประมวลผลข้อมูลส่วนบุคคลด้วยฐานสัญญา ให้เก็บข้อมูลไว้เท่าที่จำเป็น เพื่อการปฏิบัติตามหน้าที่ในสัญญา หรือตราบเท่าที่จะมีการยกเลิกสัญญา หรือความสัมพันธ์ที่เกี่ยวข้องนั้น

- กรณีเป็นการเก็บข้อมูลเพื่อประโยชน์อันชอบด้วยกฎหมาย ให้เก็บข้อมูลดังกล่าวไว้ตามกรอบที่เหมาะสมเพื่อการใช้สิทธิในแต่ละกรณีดังกล่าว เช่น ตามระยะเวลาอายุความกรณีการฟ้องร้องต่อสู้สิทธิต่าง ๆ หรือเท่าที่จำเป็นในการดำเนินจุดประสงค์ทางธุรกิจ ทั้งนี้ หลักการสำคัญที่ต้องพิจารณาคือการประมวลผลข้อมูลส่วนบุคคลดังกล่าวต้องไม่กระทบสิทธิของเจ้าของข้อมูลมากเกินสมควร และบริษัทหรือบริษัทในเครือดังกล่าวต้องให้สิทธิเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยฐานดังกล่าวได้ตามสิทธิที่มีได้

- กรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานความยินยอม ให้เก็บข้อมูลได้เฉพาะกรณีเจ้าของข้อมูลให้ความยินยอมและตราบเท่าที่เจ้าของข้อมูลยังไม่ได้ใช้สิทธิในการถอนความยินยอม ซึ่งเป็นสิทธิอิสระที่เจ้าของข้อมูลสามารถดำเนินการได้ตลอดระยะเวลา

- กรณีข้อมูลส่วนบุคคลที่บริษัทและ/หรือบริษัทในเครือประมวลผล เป็นข้อมูลส่วนบุคคลอ่อนไหว เช่น ประวัติอาชญากรรม หรือประวัติสุขภาพการรักษาพยาบาล หรือข้อมูลชีวภาพอื่น ๆ บริษัทและบริษัทในเครือต้องใช้ความระมัดระวังในการบริหารจัดการ และประมวลผลข้อมูลส่วนบุคคลด้วยมาตรฐานที่สูงขึ้น โดยเฉพาะระยะเวลาในการทำลายข้อมูลดังกล่าว ควรจำกัดให้มีการลบหรือทำลายในทันทีที่หมดความจำเป็น

10.2 เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลตามกรอบระยะเวลาที่กำหนดไว้แล้ว หน่วยงานที่เกี่ยวข้องต้องลบทำลายหรือดำเนินการทำให้ข้อมูลกลายเป็นข้อมูลนิรนาม โดยต้องทำลายข้อมูลทั้งที่อยู่ในรูปแบบกระดาษ และข้อมูลอิเล็กทรอนิกส์ซึ่งต้องดำเนินการทำลายทางเทคนิคอย่างเหมาะสม รวมถึงหากมีการบันทึกข้อมูลดังกล่าวในอุปกรณ์หรือเครื่องมือใด เช่น USB หรือคอมพิวเตอร์ ต้องใช้ความพยายามอย่างดีที่สุดในการทำลายข้อมูลดังกล่าวทั้งหมดอย่างเหมาะสม

ข้อ 11 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

11.1 โดยหลัก บริษัทและบริษัทในเครือกำหนดนโยบายการประมวลผลข้อมูลส่วนบุคคลทั้งหมด ให้ดำเนินการผ่านระบบอิเล็กทรอนิกส์ที่สามารถควบคุมและบันทึกการเข้าถึงได้มากกว่าการจัดเก็บข้อมูลเป็นกระดาษ แต่ทั้งนี้ ในกรณีใช้ข้อมูลส่วนบุคคลในรูปแบบของกระดาษ หน่วยงานที่เกี่ยวข้องต้องจัดทำบันทึกการใช้ข้อมูลและดำเนินมาตรการรักษาความปลอดภัยข้อมูลดังกล่าวภายใต้แนวปฏิบัติ Clean Desk โดยห้ามนำกระดาษที่มีข้อมูลส่วนบุคคลไปใช้ซ้ำ (Recycled) ต้องจัดเก็บใส่กล่องเรียบร้อยที่ระบุกำหนดระยะเวลาการเก็บข้อมูลดังกล่าว และหากจะมีการเคลื่อนย้ายข้อมูลดังกล่าวต้องดำเนินการตามกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล

11.2 บริษัทและบริษัทในเครือกำหนดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ภายใต้หลักการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยน แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ภายใต้กรอบการรับประกัน ดังนี้

- ข้อมูลทั้งหมดจะได้รับการเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ (Confidentiality) โดยถือว่าข้อมูลส่วนบุคคลทั้งหมดโดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหวเป็นข้อมูลความลับสูงสุด

- ข้อมูลทั้งหมดต้องเป็นข้อมูลที่ถูกต้องเชื่อถือได้เป็นไปตามข้อมูลที่ทางผู้เป็นเจ้าของข้อมูลได้ให้ข้อมูลดังกล่าวขึ้นมาโดยไม่เกิดการแก้ไขโดยไม่ได้รับอนุญาต (Integrity) และ

- ข้อมูลต้องมีความพร้อมใช้งานได้ทันทีที่ต้องการ (Availability)

11.3 บริษัทและบริษัทในเครือกำหนดจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการด้านโครงสร้างการบริหารจัดการ มาตรการด้านเทคนิค และมาตรการทางด้านกายภาพ ซึ่งถึงแต่ไม่จำกัดเพียงมาตรการภายใต้หลักการในการควบคุมเงื่อนไขการเข้าถึงข้อมูลส่วนบุคคล ผ่านระบบ Role-Based Authorization Matrix

11.4 บริษัทและบริษัทในเครือกำหนดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของการเข้าถึง เปลี่ยนแปลง ข้อมูลส่วนบุคคลในส่วนต่าง ๆ โดยหัวหน้าฝ่ายหรือหน่วยงานที่เกี่ยวข้องรับผิดชอบสอบทานบันทึก Log ของพนักงานภายใต้กำกับดูแลของตนอย่างสม่ำเสมอ และเจ้าหน้าที่หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ Log ดังกล่าวตามที่เกี่ยวข้องและเหมาะสม

11.5 ในการดำเนินการควบคุมและบริหารจัดการการประมวลผลข้อมูลส่วนบุคคลทั้งหมด บริษัทและบริษัทในเครือกำหนดให้ทุกหน่วยงานต้องดำเนินการภายใต้กรอบ Maker-Checker และต้องมีการตรวจสอบทดสอบประสิทธิภาพในการทำงานของมาตรการและกลไกต่าง ๆ อย่างสม่ำเสมอ

11.6 กรณีที่บริษัทและบริษัทในเครือใช้เครื่องมืออุปกรณ์หรือทรัพย์สินสารสนเทศใดในการเก็บ และประมวลผลข้อมูลส่วนบุคคลของพนักงาน บริษัทและบริษัทในเครือต้องดำเนินการจัดทำทะเบียนทรัพย์สินดังกล่าวให้ครบถ้วน และโดยเฉพาะต้องกำหนดจำกัดสิทธิหรือเงื่อนไขในการใช้ทรัพย์สินสารสนเทศที่เป็นของพนักงานแต่ละคน (BYOD) ให้ชัดเจน เพื่อให้มีมาตรฐานในการรักษาความมั่นคงของข้อมูลส่วนบุคคลในทุกอุปกรณ์ทรัพย์สินสารสนเทศ ทั้งนี้ควรจำกัดการใช้อุปกรณ์ของพนักงาน เพื่อการเก็บรักษาหรือประมวลผลข้อมูลส่วนบุคคลให้น้อยที่สุด เพื่อป้องกันความเสี่ยงของการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล

11.7 บริษัทและบริษัทในเครือกำหนดนโยบายการสำรองข้อมูลส่วนบุคล ที่มีความสำคัญทั้งหมดให้พร้อมใช้งานได้อย่างต่อเนื่อง โดยไม่หยุดชะงัก ทั้งนี้ ต้องจัดให้มีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูล (Data Recovery) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลทั้งหมด ที่มีการประมวลผลมีความถูกต้อง ครบถ้วน และสามารถใช้งานได้ภายในระยะเวลาที่กำหนด

11.8 บริษัทและบริษัทในเครือกำหนดกระบวนการในการควบคุม และรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล โดยผู้ให้บริการภายนอกอย่างชัดเจน โดยกำหนดมาตรฐานตั้งแต่กระบวนการคัดเลือก การจัดทำสัญญาจำกัดการเข้าถึงและการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น และรับประกันการรักษามาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ผู้ให้บริการดังกล่าวต้องรักษาให้ได้มาตรฐานเดียวกันกับมาตรฐานของบริษัท ทั้งนี้หน่วยงานที่ว่าจ้างผู้ให้บริการดังกล่าวมีหน้าที่ในการติดตาม และตรวจสอบการปฏิบัติหน้าที่ของผู้ให้บริการภายนอก ให้เป็นไปตามข้อกำหนดอย่างเป็นปกติ โดยหากพบความผิดปกติหรือการละเมิด ให้ดำเนินการลงโทษผู้ให้บริการดังกล่าวทันที โดยรับประกันไม่ให้เกิดผลกระทบต่อความต่อเนื่องในการดำเนินธุรกิจของบริษัทหรือบริษัทในเครือที่เกี่ยวข้อง

ข้อ 12 สิทธิเจ้าของข้อมูล

บริษัทและบริษัทในเครือยอมรับและเคารพสิทธิตามกฎหมายของเจ้าของข้อมูลทั้งหมด ในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่อยู่ในการควบคุมของบริษัทและบริษัทในเครือ โดยบริษัทต้องรับประกันว่า เจ้าของข้อมูลทั้งหมดสามารถใช้สิทธิต่าง ๆ ที่มีภายใต้

กฎหมายได้ โดยบริษัทและบริษัทในเครือรับประกันที่จะพิจารณาและดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูล ภายใต้กรอบระยะเวลาที่ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ ทั้งนี้สิทธิของเจ้าของข้อมูลดังกล่าว ได้แก่

- สิทธิขอเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคล รวมถึงสิทธิในการขอแก้ไขข้อมูลส่วนบุคคลให้เป็นปัจจุบัน และถูกต้อง
- สิทธิขอรับข้อมูลส่วนบุคคล ในกรณีที่บริษัททำให้ข้อมูลส่วนบุคคลนั้น อยู่ในรูปแบบที่สามารถอ่านหรือใช้งาน โดยทั่วไปด้วยเครื่องมือหรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติ รวมถึงสิทธิขอให้ส่ง หรือโอนข้อมูลรูปแบบดังกล่าวไปยังผู้ควบ คุมข้อมูลส่วนบุคคลอื่น
- สิทธิคัดค้านการประมวลผลข้อมูลส่วนบุคคล
- สิทธิขอให้ลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เมื่อข้อมูลนั้นหมดความจำเป็นหรือเมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม
- สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคลได้ ในกรณีเมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบหรือเมื่อข้อมูลดังกล่าวหมดความจำเป็น
- สิทธิถอนความยินยอม

ข้อ 13 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

13.1 บริษัท และบริษัทในเครือกำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัท มีหน้าที่ในการกำหนดนโยบายและมาตรการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หรือเกิดเป็นเหตุละเมิดข้อมูลส่วนบุคคล โดยประสานกับหน่วยงานที่เกี่ยวข้อง โดยตัวแทนของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในแต่ละบริษัทในเครือ เป็นผู้ทำหน้าที่รับแจ้งและบริหารจัดการเหตุการณ์ดังกล่าวในลำดับแรก

13.2 กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัทต้องทำหน้าที่จัดทำรายงานเหตุการณ์ดังกล่าวให้คณะกรรมการบริษัท หรือคณะกรรมการอื่น หรือผู้ให้บริการระดับสูงที่ได้รับการมอบหมายให้รับผิดชอบเกี่ยวกับการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลเพื่อทราบ และจัดเตรียมเอกสารรายงานจัดส่งให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายในกรอบระยะเวลาการรายงาน 72 ชั่วโมงนับแต่ทราบเหตุ และให้แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคลกรณีได้รับผลกระทบ

13.3 ภายหลังสิ้นสุดเหตุละเมิดดังกล่าว คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัทมีหน้าที่ในการตรวจสอบและสอบทาน เพื่อพิจารณาสาเหตุที่แท้จริงของเหตุการณ์ดังกล่าวเพื่อจัดทำรายงานเสนอต่อคณะกรรมการบริษัท หรือคณะกรรมการอื่นที่รับผิดชอบคุ้มครองการประมวลผลข้อมูลส่วนบุคคลทราบ และเพื่อการปรับปรุงแก้ไขป้องกันเหตุละเมิดที่อาจเกิดขึ้นในอนาคตต่อไป

ข้อ 14 การทบทวนหรือปรับปรุงนโยบาย

บริษัทกำหนดให้มีการทบทวน หรือปรับปรุงนโยบายฉบับนี้โดยคณะกรรมการบริษัท หรือคณะกรรมการอื่นที่ได้รับการมอบหมายการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล ด้วยการพิจารณาจากรายงานการปฏิบัติตามนโยบายที่นำเสนอโดยคณะกรรมการตรวจสอบ หรือคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกลุ่มบริษัทอย่างน้อยปีละ 1 ครั้งหรือกรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อธุรกิจบริษัทหรือบริษัทในเครือ โดยเฉพาะการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในกระบวนการประมวลผลข้อมูลส่วนบุคคลที่บริษัทหรือบริษัทในเครือดำเนินการ เพื่อให้นโยบายเป็นปัจจุบันอยู่เสมอ