



คำสั่งบริษัท วิงสแปน เซอร์วิสเชส จำกัด ที่ 01/2565

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท วิงสแปน เซอร์วิสเชส จำกัด

บริษัท บริษัท วิงสแปน เซอร์วิสเชส จำกัด ให้ความสำคัญเป็นอย่างยิ่งในการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ เพื่อให้มั่นใจได้ว่าข้อมูลของผู้สมัครงาน พนักงาน และบุคคลที่เกี่ยวข้องจะได้รับการคุ้มครองให้เป็นไปตามกฎหมาย

ที่ประชุมฝ่ายบริหารบริษัท วิงสแปน เซอร์วิสเชส จำกัด ในการประชุมเมื่อวันที่ 01 มิถุนายน 2565 ได้มีมติเห็นชอบให้ใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท การบินไทย จำกัด (มหาชน) ให้เป็นไป ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับการดำเนินงานของบริษัทฯ และมีคำสั่งให้ใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท การบินไทย จำกัด (มหาชน) ลงวันที่ 27 พฤษภาคม 2565 รายละเอียดปรากฏตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท การบินไทย จำกัด (มหาชน) ท้ายคำสั่งนี้

ขอให้พนักงานและลูกจ้างของบริษัท วิงสแปน เซอร์วิสเชส จำกัด ศึกษาและถือปฏิบัติโดยเคร่งครัด

สั่ง ณ วันที่ 01 มิถุนายน 2565

(นายโอม พลธานีชัย)



รองประธานกรรมการบริษัท วิงสแปน เซอร์วิสเชส จำกัด

และ กรรมการผู้จัดการ บริษัท วิงสแปน เซอร์วิสเชส จำกัด

นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท การบินไทย จำกัด (มหาชน)

1. บทนำ

บริษัท การบินไทย จำกัด (มหาชน) (“บริษัท”) ซึ่งหมายความรวมถึง บริษัทย่อย ได้แก่ บริษัท ไทยสมายล์แอร์เวย์ จำกัด บริษัท ไทยไฟลท์เทรนนิ่ง จำกัด บริษัท ไทย-อะมาดิอุส เซาท์อีสต์เอเชีย จำกัด บริษัท ทัวร์เอ็องหลวง จำกัด และ บริษัท วิงสแปน เซอร์วิสเซส จำกัด ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล รวมถึงความจำเป็น ที่จะทำให้มั่นใจได้ว่าบริษัทปฏิบัติตามกฎหมาย และระเบียบที่เกี่ยวข้อง เพื่อเป็นการลดความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล และการไม่ปฏิบัติตามกฎหมายดังกล่าวที่อาจจะเกิดขึ้น นโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท การบินไทย จำกัด (มหาชน) นี้ได้จัดทำขึ้น เพื่อแจ้งแก่พนักงานในการบริหารจัดการข้อมูลส่วนบุคคลอย่างระมัดระวังเพื่อความปลอดภัย

นโยบายการคุ้มครองข้อมูลส่วนบุคคล ของบริษัท การบินไทย จำกัด (มหาชน) ใช้บังคับกับข้อมูลส่วนบุคคลทั้งปวงที่มีการประมวลผลโดยพนักงานประจำ พนักงานชั่วคราว พนักงานตามสัญญาจ้าง แรงงานภายนอกของบริษัท พนักงานฝึกงาน นักศึกษาฝึกงาน และพันธมิตรคู่สัญญาหรือคู่ค้า รวมถึงหน่วยงานทางกฎหมาย หน่วยงานที่ปฏิบัติงานในประเทศต่าง ๆ และหน่วยธุรกิจที่ดำเนินการโดยบริษัทที่อยู่ภายใต้ขอบเขตของนโยบายนี้

กฎหมายท้องถิ่นของทุกประเทศ และเขตปกครองตามกฎหมายที่บริษัทมีการเก็บและประมวลผล รวมถึงข้อกำหนดต่าง ๆ เกี่ยวกับการจดทะเบียน จะต้องได้รับการปฏิบัติตามอย่างเคร่งครัด หน่วยงานภายใต้การกำกับของบริษัทมีหน้าที่รับผิดชอบในการประเมินว่าข้อกำหนดดังกล่าว กำหนดไว้ให้ดำเนินการเพียงใด ในกรณีที่ไม่มีแจ้งผู้เกี่ยวข้องต้องปรึกษาเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือฝ่ายกฎหมาย

การเก็บรวบรวมข้อมูลส่วนบุคคล และการเปิดเผยข้อมูลส่วนบุคคลให้กับหน่วยงาน และเจ้าหน้าที่ของรัฐบาล จะต้องดำเนินการโดยอาศัยฐานตามที่กฎหมายกำหนดไว้โดยเฉพาะนโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ กำหนดข้อปฏิบัติที่จำเป็นเพื่อให้เป็นไปตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง

2. บทบาทและหน้าที่ความรับผิดชอบ

การปกป้องความเป็นส่วนตัวส่วนตัวของพนักงานและลูกค้า ถือเป็นความรับผิดชอบของพนักงานบริษัท และพนักงานบริษัทในเครือทุกคน

ความรับผิดชอบในการปฏิบัติตามนโยบายฉบับนี้ รวมอยู่ที่ฝ่ายบริหารซึ่งสนับสนุน และมอบหมายการจัดทำแผนบริหารงานคุ้มครองข้อมูลส่วนบุคคล โดยฝ่ายบริหารถือเป็นผู้รับผิดชอบในภาพรวมทั้งหมด

การบริหารงานการคุ้มครองข้อมูลส่วนบุคคลมุ่งที่จะควบคุม และลดความเสี่ยงเกี่ยวกับการละเมิดความเป็นส่วนตัวส่วนตัว ประกอบไปด้วยกระบวนการ มาตรฐาน และข้อแนะนำที่พัฒนาและรักษาไว้โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อแนะนำให้คำปรึกษาแก่หน่วยงานผู้รับผิดชอบ รวมถึงพนักงานทุกคนของบริษัทในการบริหารจัดการข้อมูลส่วนบุคคลอย่างปลอดภัย เพื่อให้เป็นไปตามกฎหมายและข้อบังคับเกี่ยวกับข้อมูลส่วนบุคคล

3. การคุ้มครองข้อมูลส่วนบุคคลตั้งแต่กระบวนการออกแบบ

ในการใช้แอปพลิเคชัน บริการ และผลิตภัณฑ์ใหม่ โดยอยู่บนพื้นฐานของ “ความเป็นส่วนตัวตั้งแต่กระบวนการออกแบบ” ถือเป็นเป้าหมายที่ชัดเจนของบริษัท เพื่อประกันว่าการคุ้มครองข้อมูลส่วนบุคคล ถือเป็นข้อพิจารณาอันสำคัญตั้งแต่ขั้นต้นของการพัฒนาธุรกิจ และตลอดเวลาของการปฏิบัติ อันประกอบด้วยหลักการ 7 ประการ ดังนี้

- หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส
- หลักจำกัดตามวัตถุประสงค์
- หลักการลดปริมาณข้อมูล
- หลักความถูกต้องของข้อมูล
- หลักการจำกัดการเก็บ
- ความสมบูรณ์ของข้อมูลและหลักการรักษาความลับ
- หลักความรับผิดชอบ

3.1 หลักความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส

การประมวลผลข้อมูลส่วนบุคคล จะต้องชอบด้วยกฎหมาย เป็นธรรม และโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล และมีการเก็บรวบรวมข้อมูลส่วนบุคคลเพียงพอที่จำเป็นต่อการประมวลผล

ผู้บริหารหน่วยงานผู้รับผิดชอบ จะต้องทำให้มั่นใจว่าการประมวลผลข้อมูลส่วนบุคคลจะกระทำเฉพาะเมื่อเจ้าของข้อมูลได้ให้ความยินยอม หรือเมื่อมีฐานทางกฎหมายอื่นภายใต้บทบัญญัติของกฎหมายที่ใช้บังคับในการประมวลผล

การขอความยินยอม จะต้องทำโดยชัดแจ้ง เป็นหนังสือหรือผ่านระบบอิเล็กทรอนิกส์ เว้นแต่โดยสภาพไม่อาจขอความยินยอมด้วยวิธีดังกล่าวได้ ซึ่งเจ้าของข้อมูลส่วนบุคคลจะต้องได้รับการแจ้งล่วงหน้า เกี่ยวกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคล การขอความยินยมนั้นต้องแยกส่วนออกจากข้อความอื่นอย่างชัดเจน หากมีข้อความขอความยินยอมอยู่ร่วมกับข้อความอื่นๆ ข้อความขอความยินยมนั้นจะต้องมีการเน้นข้อความและมีการแยกส่วนออกมาอย่างชัดเจน อันจะทำให้เจ้าของข้อมูลส่วนบุคคลสังเกตได้ง่าย นอกจากนี้ ข้อความขอความยินยอมจะต้องเข้าถึงได้ง่าย และเข้าใจได้ รวมทั้งใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์ในการประมวลผลดังกล่าว ผู้บริหารหน่วยงานผู้รับผิดชอบจะต้องนำคู่มือการรักษาข้อมูลส่วนบุคคล และข้อมูลมาตรฐานในการขอความยินยอมใส่ไว้ในกระบวนการตั้งแต่เริ่มต้น

หน่วยงานผู้รับผิดชอบที่มีการประมวลผลข้อมูลส่วนบุคคลทุกหน่วยงานอยู่ภายใต้หน้าที่ความรับผิดชอบที่ได้รับมอบหมาย นอกจากนั้น จะต้องมีการบันทึกที่ชัดเจนของการเก็บ รวบรวม ใช้ และลบข้อมูลส่วนบุคคล รวมทั้ง ให้มีการวิเคราะห์ความเสี่ยงอย่างเหมาะสม เพื่อให้มีการควบคุมความมั่นคงปลอดภัยที่เพียงพอในการจัดเก็บข้อมูล การประมวลผล ซึ่งเป็นสิ่งจำเป็นสำหรับผู้บริหารหน่วยงานผู้รับผิดชอบทุกกระบวนการ

3.2 หลักจำกัดตามวัตถุประสงค์

ข้อมูลส่วนบุคคลต้องเก็บเพื่อวัตถุประสงค์เฉพาะ และชัดเจน และไม่อาจประมวลผลสำหรับวัตถุประสงค์ที่ไม่ได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบไว้แต่แรก ผู้บริหารหน่วยงานผู้รับผิดชอบจะต้องระบุ และบันทึกวัตถุประสงค์ในการประมวลผลไว้ด้วย ทั้งนี้โดยการหารือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากจำเป็นการเปลี่ยนวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลสามารถกระทำได้ โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ใหม่และขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือตามที่กฎหมายที่ใช้บังคับกำหนดให้กระทำได้นั้น

ผู้บริหารหน่วยงานผู้รับผิดชอบต้องควบคุมการเก็บ บันทึก และลงรายการข้อมูลส่วนบุคคลที่จำเป็นเพื่อสนองต่อวัตถุประสงค์ในการจัดเก็บเท่านั้น



3.3 หลักการลดปริมาณข้อมูล

เพื่อเป็นการลดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล บริษัทต้องพิจารณาดำเนินการ ดังนี้

- การลดความชัดเจนของข้อมูลที่เก็บไว้หลังจากที่ได้ทำการเก็บรวบรวม เช่น ข้อมูลหมายเลขโทรศัพท์ของลูกค้าที่จะใช้เพื่อการวิเคราะห์ทางสถิติควรเก็บเป็นข้อมูลบางส่วนของหมายเลขโทรศัพท์ หรือข้อมูลหมายเลขพื้นที่ให้บริการ
- การแปลงข้อมูลส่วนบุคคลให้มีความอ่อนไหวน้อยลงเพื่อลดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล เช่น กรณีการใช้ไอพีแอดเดรสหาที่ตั้งเพื่อวัตถุประสงค์ในการวิเคราะห์ทางสถิติ ควรจะมีการลบไอพีแอดเดรสทิ้งไปหลังจากได้มีการค้นหาเมืองหรือประเทศได้แล้ว
- การจำกัดการเข้าถึงข้อมูลส่วนบุคคลขนาดใหญ่ เช่น พนักงานที่มีความจำเป็นจะต้องเข้าถึงข้อมูลส่วนบุคคลเฉพาะกลุ่ม ไม่ควรมีสิทธิในการเข้าถึงกลุ่มของข้อมูลทั้งหมดโดยอัตโนมัติ

3.4 หลักความถูกต้องของข้อมูล

หน่วยงานผู้รับผิดชอบจะต้องดำเนินการที่จำเป็นทั้งหมดเพื่อให้มั่นใจว่าการเก็บข้อมูลส่วนบุคคลที่รวบรวมมาถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด ข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ไม่เป็นปัจจุบัน ไม่สมบูรณ์ หรือ ก่อให้เกิดความเข้าใจผิดจะต้องมีการลบ หรือแก้ไข หน่วยงานผู้รับผิดชอบควรจะต้องเลือกใช้กระบวนการหรือวิธีการให้เจ้าของข้อมูลส่วนบุคคลสามารถปรับปรุงข้อมูลของตนได้ หากเป็นไปได้ควรจัดให้มีเครื่องมือในการแก้ไขข้อมูลส่วนบุคคลได้ด้วยตนเอง (self-service system)

3.5 หลักการจำกัดการเก็บ

การเก็บข้อมูลไว้เป็นระยะเวลานานจะทำให้เกิดความเสี่ยงต่อการละเมิดข้อมูลส่วนบุคคล ดังนั้นควรจัดเก็บข้อมูลส่วนบุคคลเป็นระยะเวลาเท่าที่จำเป็นสำหรับการใช้งาน เพื่อสนับสนุนวัตถุประสงค์ทางธุรกิจหรือเพื่อวัตถุประสงค์ทางกฎหมาย

ให้ผู้บริหารหน่วยงานผู้รับผิดชอบจำกัดระยะเวลาของการจัดเก็บข้อมูลส่วนบุคคล โดยระบุว่าจะต้องมีการจัดเก็บไว้ นานเท่าใด และด้วยเหตุผลใดและกระบวนการในการย้ายข้อมูลส่วนบุคคลออกจากแหล่งที่เก็บ ระยะเวลาในการ จัดเก็บดังกล่าวควรใช้บังคับกับทุกระบบที่มีการเก็บข้อมูลส่วนบุคคลอยู่ รวมถึงแหล่งจัดเก็บข้อมูลสำรองและแหล่ง จัดเก็บข้อมูลของบุคคลที่สามด้วย

3.6 ความสมบูรณ์ของข้อมูลและหลักการรักษาความลับ

ผู้บริหารหน่วยงานผู้รับผิดชอบจะต้องควบคุมการเข้าถึงข้อมูลส่วนบุคคลโดยให้สิทธิสำหรับพนักงานที่ได้รับอนุญาตซึ่ง มีหน้าที่ในการปฏิบัติเกี่ยวกับการรักษาความลับ และได้รับอนุญาตให้เข้ามีส่วนร่วมในการประมวลผลข้อมูลส่วนบุคคล เท่านั้น พนักงานจะต้องไม่ใช่ข้อมูลส่วนบุคคลดังกล่าวเพื่อวัตถุประสงค์ส่วนตัว หรือโอนข้อมูลส่วนบุคคลดังกล่าวไปยัง ผู้ที่ไม่ได้รับอนุญาต หรือไม่ทำให้สามารถเข้าถึงข้อมูลได้โดยวิธีการที่ไม่เหมาะสมแก่บุคคลที่ไม่ได้รับอนุญาต คำว่า “ไม่ได้รับอนุญาต” ในที่นี้หมายความรวมถึงการใช้ข้อมูลส่วนบุคคลของพนักงาน โดยที่ตนไม่จำเป็นต้องเข้าถึงข้อมูล ส่วนบุคคลในการปฏิบัติหน้าที่ของพนักงานนั้นๆ นอกจากนี้การควบคุมความมั่นคงปลอดภัยเพื่อประกันความสมบูรณ์ และความลับของข้อมูลส่วนบุคคลให้เป็นไปตามคู่มือการปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และ คู่มือการรักษาข้อมูลส่วนบุคคล: การปฏิบัติด้านเทคนิค และด้านองค์กร (THAI Information Security Handbook and THAI Privacy Handbook: Technical and Organizational Measure)

3.7 หลักความรับผิดชอบ

หน่วยงานผู้รับผิดชอบต้องดำเนินการเพื่อให้เป็นไปตามหลักความรับผิดชอบต่อเจ้าของข้อมูลส่วนบุคคล ดังนี้

- จัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- จัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคลกับผู้ให้บริการ
- วิเคราะห์ความเสี่ยงการประมวลผลในกรณีที่ข้อมูลส่วนบุคคลที่อ่อนไหวหรือเป็นข้อมูลที่มีความเสี่ยงสูง

4. ข้อมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลส่วนบุคคลที่อ่อนไหว

หน่วยงานผู้รับผิดชอบต้องไม่ประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลส่วนบุคคลที่อ่อนไหว นอกจากจะได้รับ ความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่กรณีที่ต้องด้วยข้อยกเว้นตามกฎหมาย เช่น เป็นข้อกำหนด ตามสัญญาจ้างงาน กฎหมายที่ใช้บังคับ และข้อกำหนดของบริษัท

การประมวลผลข้อมูลส่วนบุคคลอื่น ๆ อาจถือเป็นข้อมูลส่วนบุคคลที่อ่อนไหว เมื่อคำนึงถึงเนื้อหา แหล่งที่มา ปริมาณ และการใช้ตามวัตถุประสงค์ และเมื่อได้มีการประเมินความเสี่ยงของการประมวลผลแล้ว เช่น ข้อมูลการเงินในการบริหารจัดการ ค่าจ้าง ค่าตอบแทน อาจถือเป็นข้อมูลส่วนบุคคลที่อ่อนไหว จำเป็นต้องมีมาตรการในการปกป้อง และควบคุม เพิ่มเติม

5. การติดตามพฤติกรรม

บริษัทสงวนสิทธิในการติดตาม อีเมล การจราจรทางไซเบอร์ และสื่อสังคมออนไลน์ ของพนักงานตรงเท่าที่กฎหมายที่ ใช้บังคับอนุญาตให้ทำได้ แต่จะพยายามปกป้องความเป็นส่วนตัวส่วนตัวของพนักงานเท่าที่สามารถกระทำได้

6. การใช้อุปกรณ์พกพา

บริษัทจะคุ้มครองข้อมูลส่วนบุคคลของพนักงานที่อยู่ในอุปกรณ์พกพา และการใช้อุปกรณ์ดังกล่าวเพื่อวัตถุประสงค์ ส่วนตัวเท่าที่สามารถกระทำได้ รายละเอียดขอบเขต เงื่อนไข และข้อกำหนดการให้บริการอุปกรณ์พกพา สามารถ ศึกษาข้อมูลเพิ่มเติมได้ที่ <http://thaisphere.thairways.co.th/ThaiVZ/Pages/Mobile/>

7. การละเมิดข้อมูลส่วนบุคคล

การป้องกันมิให้เกิดการละเมิดข้อมูลส่วนบุคคลถือเป็นความรับผิดชอบของพนักงาน และ ลูกจ้าง และคู่สัญญาของ บริษัททั้งหมด ในกรณีที่เกิดความไม่ปกติของกระบวนการในการประมวลผลข้อมูลส่วนบุคคล ขอให้ทุกคนแจ้งไปยัง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ในทันที การกักกลับภายในเวลา การตอบกลับ การปฏิบัติ และการแจ้ง (ทั้งในกรณีหน่วยงานคุ้มครองข้อมูลส่วนบุคคล และเจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบ) เป็นไปตาม คู่มือการ รักษาข้อมูลส่วนบุคคล: การบริหารจัดการเมื่อเกิดข้อมูลรั่วไหล (THAI Privacy Handbook: Data Breach Management)

8. การฝึกอบรม และความตระหนักรู้

พนักงานจะต้องมั่นใจว่าหลักการทั่วไปที่ระบุไว้ในนโยบายฉบับนี้ จะได้รับการนำไปปฏิบัติ ทั้งนี้ พนักงานในระดับ บริหาร และหัวหน้าหน่วยงานทุกๆ ระดับจะต้องนำนโยบายนี้ไปปฏิบัติอย่างทั่วถึง รวมถึงการส่งมอบนโยบายนี้ ให้กับ พนักงานในสังกัดทุกๆ คนหากต้องการให้มีการฝึกอบรมใดๆ ที่จำเป็น ขอให้ติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

9. ผลของสัญญาว่าจ้าง

พนักงานจะต้องศึกษาและทำความเข้าใจหน้าที่และมาตรการต่างๆ ที่ต้องปฏิบัติเพิ่มเติมจากสัญญาการจ้างงานของพนักงานและคำสั่งและข้อบังคับต่างๆด้วยตนเองเป็นปกติอย่างสม่ำเสมอ การไม่ปฏิบัติตามข้อปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลถือเป็นการปฏิบัติผิดสัญญาว่าจ้างกับบริษัท ซึ่งอาจจะส่งผลถึงการใช้บังคับตามกฎหมายแรงงานที่เกี่ยวข้อง นอกจากนี้ยังถือเป็นการกระทำความผิดทางวินัย

10. การให้บริการของบุคคลที่สาม และการชวงงาน

ผู้บริหารหน่วยงานผู้รับผิดชอบอาจมีการติดต่อบุคคลที่สามให้ทำการประมวลผลข้อมูลส่วนบุคคลในนามหรือตามคำสั่งของบริษัท บุคคลที่สามดังกล่าว อาจเสนอบริการในการเป็นผู้ดูแล (hosting) หรือจ้างบริการ (outsourcing) หรือการให้บริการคราวด์คอมพิวติง เฉพาะบริษัท หรือสาธารณะ (private or public cloud computing service)

ในกรณีที่ผู้บริหารหน่วยงานผู้รับผิดชอบตัดสินใจที่จะทำสัญญากับบุคคลที่สามในการประมวลผลข้อมูลส่วนบุคคลในนามหรือตามคำสั่งของบริษัท จะต้องมีการเข้าทำสัญญาซึ่งระบุสิทธิและหน้าที่ของบริษัท และของคู่สัญญาไว้เพื่อควบคุมการดำเนินงานตามหน้าที่ของคู่สัญญาให้เป็นไปตามกฎหมายที่ใช้บังคับ ผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทเลือกจะต้องเลือกจากผู้ที่ทำให้คำรับรองเกี่ยวกับการปฏิบัติตามมาตรการรักษาความปลอดภัยทางด้านเทคนิคและองค์กรที่บริษัทกำหนด และให้คำรับรองอย่างครบถ้วนเกี่ยวกับการปกป้องรักษาสิทธิส่วนบุคคลและการจัดการกับคำร้องขอใช้สิทธิต่างๆของเจ้าของข้อมูลส่วนบุคคล รวมถึงผูกพันในข้อสัญญาและหน้าที่ไม่น้อยไปกว่าที่กำหนดไว้ในสัญญาประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทและบุคคลที่สามดังกล่าว

บุคคลที่สามในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลของบริษัทที่มีหน้าที่ตามสัญญาในการประมวลผลข้อมูลส่วนบุคคลภายใต้ขอบเขตที่ระบุในสัญญา และตามคำสั่งของบริษัทเท่านั้น การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นไม่อาจกระทำได้อีกต่อไป ภายใต้อาณัติของบริษัทยังคงมีหน้าที่และต้องรับผิดชอบต่อการประมวลผลนั้นที่เกิดจากคู่สัญญา

ในกรณีที่มีความจำเป็นที่จะต้องส่งออก หรือโอนข้อมูลส่วนบุคคลจากประเทศไทย หรือจากสหภาพยุโรป (EU) หรือเขตเศรษฐกิจยุโรป (EEA) ไปยังประเทศที่ไม่มีมาตรการในการปกป้องข้อมูลส่วนบุคคลที่เพียงพอ ผู้บริหาร หน่วยงานผู้รับผิดชอบจะต้องหารือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อระบุมมาตรการการคุ้มครองที่เพียงพอตามที่กำหนดในคู่มือการรักษาข้อมูลส่วนบุคคล: ข้อปฏิบัติในการจัดการโอนข้อมูลข้ามประเทศ (THAI Privacy Handbook: Cross Border Management Guidelines) เพื่อให้การโอนข้อมูลส่วนบุคคลเป็นไปโดยสอดคล้องกับข้อกำหนดตามกฎหมายที่ใช้บังคับ ทั้งนี้ อาจต้องมีการลงนามสัญญาการประมวลผลและการถ่ายโอนข้อมูลและข้อสัญญามาตรฐาน เพื่อเป็นส่วนหนึ่งของสัญญาระหว่างผู้ส่งออกและผู้รับโอนข้อมูล

11. สิทธิของเจ้าของข้อมูลส่วนบุคคล

เจ้าของข้อมูลส่วนบุคคลสามารถใช้สิทธิของตนได้ตามกฎหมาย ซึ่งรวมถึงสิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล สิทธิขอรับหรือส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น สิทธิขอคัดค้าน สิทธิขอไหลบหรือทำลายข้อมูลส่วนบุคคล สิทธิขอให้ระงับการใช้ข้อมูลส่วนบุคคล สิทธิขอแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง สิทธิในการถอนความยินยอม สิทธิแจ้งยกเลิกความยินยอม คำขอตกลงว่าจะถูกส่งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือตัวแทนท้องถิ่น และได้รับการตอบกลับโดยไม่ชักช้าภายในเวลา 30 วัน หลังจากได้รับคำร้องขอและอาจจะขยายออกไปได้ 30 วัน

ผู้บริหารหน่วยงานผู้รับผิดชอบจะต้องสั่งการให้ผู้ประมวลผลข้อมูลส่วนบุคคลให้ความช่วยเหลือในการตอบคำร้องขอเกี่ยวกับการใช้สิทธิดังกล่าวภายใต้กฎหมาย และจะต้องให้ข้อมูลที่จำเป็นเพื่อการดังกล่าวภายในเวลาอันสมควร หลังจากได้รับการแจ้งขอใช้สิทธิ

12. คำนิยาม

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใดๆ เกี่ยวกับการระบุตัวตน หรือที่สามารถระบุตัวตนบุคคลธรรมดาได้ คำว่าบุคคลที่สามารถระบุตัวตนได้ คือบุคคลที่สามารถระบุตัวตนได้ไม่ว่าทางตรง หรือทางอ้อม โดยการอ้างอิงถึง หมายเลข หรือองค์ประกอบอย่างใดอย่างหนึ่ง หรือหลายอย่างรวมกัน แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“ข้อมูลส่วนบุคคลชนิดพิเศษ” หมายถึง ข้อมูลที่แสดงถึง เชื้อชาติ ชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อ ทางศาสนา หรือปรัชญา ข้อมูลสุขภาพแรงงาน ประวัติอาชญากรรม ข้อมูลทางพันธุกรรม ข้อมูลชีวภาพ ข้อมูล เกี่ยวกับสุขภาพ ความพิการ หรือพฤติกรรมทางเพศ หรือข้อมูลอื่นใดที่กระทบเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“ข้อมูลส่วนบุคคลที่อ่อนไหว” ไม่ว่าจะเป็นการระบุถึง “ข้อมูลส่วนบุคคลชนิดพิเศษ” (ดูคำนิยามด้านบน) หรือคือ ข้อมูลส่วนบุคคลซึ่งได้มีการประเมิน และจัดระดับของความอ่อนไหวแล้ว อาจส่งผลกระทบอย่างร้ายแรงต่อเจ้าของข้อมูล หากมีการละเมิดข้อมูลส่วนบุคคลดังกล่าว

“ความยินยอม” ของเจ้าของข้อมูลส่วนบุคคล หมายถึง ข้อบ่งชี้ซึ่งให้โดยอิสระเฉพาะเจาะจง ชัดแจ้ง ไม่คลุมเครือ ของเจ้าของข้อมูลส่วนบุคคล ซึ่งแสดงถึงความยินยอมให้ประมวลผลข้อมูลส่วนบุคคลของตนอย่างชัดเจน

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง บุคคล หรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง บุคคล หรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

“การประมวลผล” หมายถึง กระบวนการ หรือการดำเนินการใดๆ กับข้อมูลส่วนบุคคล ไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ ได้แก่ การเก็บ การบันทึก การจัดการ การจัดโครงสร้าง การจัดเก็บ การปรับเปลี่ยน การเรียกคืน การสืบค้น ข้อมูลเพิ่มเติม การนำมาใช้ การเข้า หรือ การเปิดเผยโดยการส่งผ่าน การเผยแพร่ หรือวิธีการอื่นใดที่ทำให้ได้ข้อมูลส่วนบุคคล การโอนไปต่างประเทศ การจัดเรียง การรวบรวม การจำกัด การลบ หรือการทำลาย

“การจำกัดการประมวลผล” หมายถึง การกระทำต่อข้อมูลส่วนบุคคลเพื่อความมุ่งประสงค์ในการจำกัดการประมวลผลข้อมูลส่วนบุคคลในอนาคต

“การละเมิดข้อมูลส่วนบุคคล” หมายถึง การละเมิดต่อความมั่นคงปลอดภัยซึ่งนำไปสู่การสูญเสีย การทำลาย การเปลี่ยนแปลง การเปิดเผย การเข้าถึงข้อมูลส่วนบุคคลของบริษัท โดยอุบัติเหตุ โดยปราศจากอำนาจ หรือโดยมิชอบ ทั้งที่เกิดขึ้นจริง หรือที่สงสัยว่าอาจเกิดขึ้น

“มาตรการในการรักษาความปลอดภัยทางด้านเทคนิค และองค์กร” หมายถึง การดำเนินการตามมาตรการในการป้องกันข้อมูลส่วนบุคคลจากการสูญหาย ถูกทำลาย การใช้ผิดวัตถุประสงค์ หรือการแก้ไขหรือเปิดเผย กับผู้ที่ไม่มิสิทธิ ในระหว่างการส่งผ่าน และการโอนย้าย

“พนักงาน” หมายถึง พนักงานตามข้อบังคับเกี่ยวกับการทำงานของบริษัท การบินไทย จำกัด (มหาชน) ฉบับลงวันที่ 11 มีนาคม 2564