

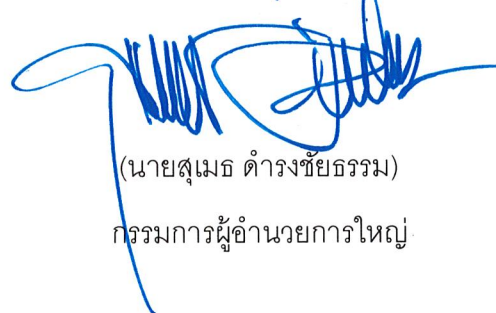
ประกาศบริษัท การบินไทย จำกัด (มหาชน) ที่ 005 /2562

เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล

ตามอนุมัติของฝ่ายบริหารงานนโยบายฯ ในคราวประชุม ครั้งที่ 32/2561 เมื่อวันที่ 21 สิงหาคม 2561 บริษัท การบินไทย จำกัด (มหาชน) ได้กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับวิธีปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ทั้งนี้ บริษัทฯ ให้ความสำคัญเป็นอย่างยิ่งในการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปอย่างมีประสิทธิภาพและอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าข้อมูลของผู้โดยสาร พนักงาน และบุคคลที่เกี่ยวข้องจะได้รับการคุ้มครองให้เป็นไปตามกฎหมายตามรายละเอียดที่ปรากฏในเอกสารแนบท้ายประกาศนี้

จึงประกาศมาให้ทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 24 เมษายน 2562



(นายสุเมธ ดำรงชัยธรรม)
กรรมการผู้อำนวยการใหญ่

นโยบายการคุ้มครองข้อมูลส่วนบุคคล

บริษัท การบินไทยจำกัด มหาชน

คณะทำงาน GDPR – กลุ่มงาน Data Privacy Policy

(คำแปลจากนโยบายที่ได้รับอนุมัติจาก EMM
21 ส.ค. 2561)

1. บทนำ

บริษัท การบินไทย จำกัด (มหาชน) (บริษัท) ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล รวมถึง ความจำเป็นที่จะทำให้งานได้ดำเนินไปอย่างมีประสิทธิภาพ และระเบียบที่เกี่ยวข้อง เพื่อเป็นการลดความเสี่ยงของการละเมิดข้อมูลส่วนบุคคล และการไม่ปฏิบัติตามกฎหมายดังกล่าวที่อาจเกิดขึ้น นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้จัดทำขึ้น เพื่อแจ้งแก่พนักงาน ในการบริหารจัดการข้อมูลส่วนบุคคลอย่างระมัดระวังด้วยความปลอดภัย และปฏิบัติตามกฎหมาย และระเบียบที่เกี่ยวข้อง

นโยบายนี้ ใช้บังคับกับข้อมูลส่วนบุคคลทั้งหลายที่มีการประมวลผลโดยพนักงานเต็มเวลา และพนักงานทำงานเป็นกะ คู่สัญญา และหุ้นส่วนที่ทำธุรกิจชื่อนามของบริษัทฯ รวมถึงหน่วยงานทางกฎหมาย และฝ่ายปฏิบัติทั้งหมดในประเทศต่าง ๆ และหน่วยธุรกิจที่กระทำโดยบริษัท ที่อยู่ภายใต้บังคับการปฏิบัติตามเนื้อหาของนโยบายนี้

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ บังคับใช้กับข้อมูลส่วนบุคคลทั้งปวงที่มีการประมวลผลโดยพนักงานเต็มเวลา และพนักงานส่วเวลา พนักงานตามสัญญา และคู่สัญญาที่ทำงานชื่อนามของการบินไทย รวมถึงหน่วยงานทางกฎหมาย หน่วยปฏิบัติในประเทศต่าง ๆ และหน่วยธุรกิจที่ดำเนินการโดยการการบินไทยที่อยู่ภายใต้ขอบเขตของนโยบายนี้

กฎหมายท้องถิ่น ของทุกประเทศ และเขตปกครองทางกฎหมายซึ่งมีการเก็บและประมวลผลซึ่งใช้บังคับอยู่ในประเทศนั้น ๆ ข้อกำหนดต่าง ๆ เกี่ยวกับการจดทะเบียนที่กำหนดให้ต้องปฏิบัติตามข้อกำหนดจะต้องได้รับการปฏิบัติตาม หน่วยงานทางกฎหมายอิสระใด ๆ ภายใต้การกำกับของการบินไทย มีหน้าที่รับผิดชอบในการประเมินว่าข้อกำหนดของการจดทะเบียนดังกล่าวกำหนดไว้ให้ดำเนินการเพียงใดต่อหน่วยงานแห่งชาติหรือหน่วยงานบังคับใช้กฎหมาย ในกรณีที่ไม่มีแจ้งผู้เกี่ยวข้องต้องปรึกษาหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือฝ่ายกฎหมาย

การเก็บรวบรวมข้อมูลส่วนบุคคลโดย และการเปิดเผยข้อมูลส่วนบุคคลให้กับหน่วยงานและเจ้าหน้าที่ของรัฐบาลจะต้องดำเนินการโดยอาศัยพื้นฐานตามที่กฎหมายกำหนดไว้โดยเฉพาะ นโยบายการคุ้มครองข้อมูลส่วนบุคคลฉบับนี้กำหนดข้อปฏิบัติที่จำเป็นเพื่อให้เป็นไปตามข้อกำหนดของกฎหมายที่เกี่ยวข้อง

2. บทบาทและหน้าที่ความรับผิดชอบ

การปกป้องความเป็นส่วนบุคคลของพนักงานและลูกค้าถือเป็นความรับผิดชอบของพนักงานของการบินไทย และบริษัทในเครือทุกคน

ความรับผิดชอบในการปฏิบัติตามนโยบายฉบับนี้โดยรวมอยู่ที่ฝ่ายบริหารงานนโยบายซึ่งสนับสนุนและมอบหมายการจัดทำแผนบริหารงานคุ้มครองข้อมูลส่วนบุคคล โดยฝ่ายบริหารงานนโยบายถือเป็นผู้รับผิดชอบในภาพรวมทั้งหมด

แผนบริหารงานคุ้มครองข้อมูลส่วนบุคคลมุ่งที่จะควบคุมและลดความเสี่ยงเกี่ยวกับการละเมิดความเป็นส่วนบุคคล ประกอบไปด้วยกระบวนการ มาตรฐานและข้อแนะนำที่พัฒนาและรักษาไว้โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เพื่อแนะนำสั่งการเจ้าของหน่วยธุรกิจ รวมถึงพนักงานแต่ละคนของการบินไทยในการบริหารจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยเพื่อให้เป็นไปตามกฎหมายและข้อบังคับเกี่ยวกับข้อมูลส่วนบุคคล

3. การคุ้มครองข้อมูลส่วนบุคคลตั้งแต่กระบวนการออกแบบ

ในการใช้แอปพลิเคชัน บริการ และผลิตภัณฑ์ใหม่ โดยอยู่บนพื้นฐานของ “ความเป็นส่วนบุคคลตั้งแต่กระบวนการออกแบบ” ถือเป็นเป้าหมายที่ชัดเจนของการบินไทยเพื่อประกันว่าการคุ้มครองข้อมูลส่วนบุคคลถือเป็นข้อพิจารณาอันสำคัญตั้งแต่ขั้นตอนของการพัฒนาหน่วยธุรกิจ และตลอดช่วงอายุของการปฏิบัติ อันประกอบด้วยหลักการหกประการดังนี้:

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

4. หลักการประมวลผลด้วยความชอบด้วยกฎหมาย เป็นธรรม และโปร่งใส

การประมวลผลข้อมูลส่วนบุคคลจะต้องชอบด้วยกฎหมายและเป็นธรรม และโปร่งใสต่อเจ้าของข้อมูลที่มีการเก็บ ใช้ รวบรวมข้อมูลส่วนบุคคลตรงเท่าที่ข้อมูลของบุคคลดังกล่าวได้ถูก หรือจะถูกประมวลผล

เจ้าของหน่วยธุรกิจจะต้องประกันว่าการประมวลผลข้อมูลส่วนบุคคลจะกระทำเฉพาะเมื่อเจ้าของข้อมูลได้ให้ความยินยอม หรือยอมให้กระทำได้ภายใต้บทบัญญัติของกฎหมาย การยอมให้กระทำได้ในการประมวลผลข้อมูลส่วนบุคคลจะต้องมีอยู่ก่อนการโอนข้อมูลใดๆ ทั้งสิ้น

ความยินยอมจะต้องมีการแสดงความชัดเจนโดยเป็นลายลักษณ์อักษร หรือโดยวิธีการอย่างอื่นที่กระทำได้ตามกฎหมาย ซึ่งเจ้าของข้อมูลส่วนบุคคลจะต้องได้รับการแจ้งล่วงหน้าเกี่ยวกับวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลและการโอนข้อมูลส่วนบุคคลดังกล่าวหากมี หากว่าข้อความในการแสดงความยินยอมอยู่รวมกับข้อความอื่นๆ การแสดงความยินยอมจะต้องมีการเน้นข้อความอันจะทำให้เจ้าของข้อมูลสังเกตได้ เจ้าของหน่วยธุรกิจ จะต้องนำคู่มือการรักษาข้อมูลส่วนบุคคล และข้อความมาตรฐานในการขอความยินยอมไปใส่ไว้ในหน่วยธุรกิจตั้งแต่เริ่มต้น

หน่วยธุรกิจที่มีการประมวลผลข้อมูลทุกหน่วยงานอยู่ภายใต้หน้าที่ความรับผิดชอบที่ได้รับมอบหมาย นอกจากนั้น จะต้องมีการที่ชัดเจนของกระบวนการของวงจรชีวิตของข้อมูลเพื่อให้มีการวิเคราะห์ความเสี่ยงอย่างเหมาะสม และมีการควบคุมความมั่นคงปลอดภัยที่เพียงพอ การจัดเก็บข้อมูลการประมวลผลเป็นสิ่งจำเป็นสำหรับเจ้าของหน่วยธุรกิจทุกกระบวนการ

5. หลักจำกัดตามวัตถุประสงค์

ข้อมูลส่วนบุคคลต้องเก็บเพื่อวัตถุประสงค์เฉพาะ หรือที่ชัดเจน และไม่อาจประมวลต่อสำหรับวัตถุประสงค์ที่ไม่ได้เจตนาให้ไว้แต่แรก เจ้าของหน่วยธุรกิจจะต้องจำกัดค่านิยาม และบันทึกวัตถุประสงค์ในการประมวลผลไว้ด้วย ทั้งนี้โดยการหารือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากจำเป็น การเปลี่ยนวัตถุประสงค์สามารถกระทำได้ด้วยความยินยอมของเจ้าของข้อมูลหรือตามที่กฎหมายกำหนดให้กระทำได้นั้น

เจ้าของหน่วยธุรกิจจะต้องควบคุมการเก็บ บันทึก และลงรายการข้อมูลส่วนบุคคลที่จำเป็นเพื่อสนองต่อวัตถุประสงค์ในการจัดเก็บเท่านั้น

6. หลักการลดปริมาณข้อมูล

เพื่อเป็นการลดความเสี่ยงต่อการรั่วไหลของข้อมูลโดยการลดความอ่อนไหวของข้อมูลที่จัดเก็บ เมื่อเป็นไปได้

- วิธีการหนึ่งคือการลดความชัดเจนของข้อมูลที่เก็บไว้หลังจากที่ได้ทำการเก็บรวบรวม เช่น ข้อมูลหมายเลขโทรศัพท์ของลูกค้าที่จะใช้เพื่อการวิเคราะห์ทางสถิติ ควรจะเป็นข้อมูลบางกลุ่มที่คัดแยกแล้ว เช่นข้อมูลหมายเลขพื้นที่ให้บริการ
- อีกวิธีการหนึ่งคือการแปลงข้อมูลส่วนบุคคลให้มีความอ่อนไหวน้อยลง เช่น การใช้ ไอพีแอดเดรสเพื่อหาที่ตั้งเพื่อวัตถุประสงค์ในการวิเคราะห์ทางสถิติ ควรจะมีการลด ไอพีแอดเดรสทิ้งไปหลังจากได้มีการค้นหาเมืองหรือประเทศได้แล้ว

- อีกวิธีการหนึ่งคือการจำกัดการเข้าถึงข้อมูลส่วนบุคคลขนาดใหญ่ เช่น พนักงานที่มีความจำเป็นจะต้องเข้าถึงระเบียบข้อมูลส่วนบุคคลชนิดใดไม่ควรมีสิทธิในการเข้าถึงกลุ่มของข้อมูลทั้งหมดโดยอัตโนมัติ

7. หลักความถูกต้องของข้อมูล

เจ้าของหน่วยธุรกิจจะต้องดำเนินการที่จำเป็นทั้งหมดเพื่อประกันว่ามีการเก็บข้อมูลที่รวบรวมมาอย่างถูกต้องและทันสมัย ความไม่ถูกต้องและทันสมัยของข้อมูลจะต้องมีการลบหรือแก้ไข เจ้าของธุรกิจควรจะต้องเลือกใช้กระบวนการหรือวิธีการให้เจ้าของข้อมูลสามารถปรับปรุงข้อมูลของตนได้ หากเป็นไปได้ควรจัดให้มีเครื่องมือในการแก้ไขข้อมูลส่วนบุคคลได้ด้วยตนเอง (self-service system)

8. หลักการจำกัดการเก็บ

ยิ่งเก็บนานยิ่งมีความเสี่ยงต่อการถูกเปิดเผย สูญหาย หรือถูกโจรกรรม หรือกระบวนการหยุดชะงัก หรืออีกนัยหนึ่ง เวลาคือองค์ประกอบแห่งความสำเร็จสำหรับการละเมิดข้อมูลส่วนบุคคล ดังนั้น ข้อมูลส่วนบุคคลจะต้องมีการจัดเก็บเป็นเวลาเท่าที่จะใช้เพื่อสนับสนุนวัตถุประสงค์ทางธุรกิจหรือเพื่อวัตถุประสงค์ทางกฎหมาย

ให้เจ้าของหน่วยธุรกิจจำกัดระยะเวลาของการจัดเก็บข้อมูลโดยระบุว่าจะต้องมีการจัดเก็บนานเท่าไร และด้วยเหตุผลใด และกระบวนการในการย้ายข้อมูลออกจากแหล่งที่เก็บ ระยะเวลาในการจัดเก็บดังกล่าวจะต้องใช้บังคับกับทุกระบบที่มีการเก็บข้อมูลส่วนบุคคลอยู่ รวมถึงแหล่งสำรองข้อมูลและแหล่งของบุคคลที่สามด้วย

9. ความสมบูรณ์ของข้อมูลและหลักการรักษาความลับ

เจ้าของหน่วยธุรกิจจะต้องควบคุมการเข้าถึงข้อมูลส่วนบุคคลโดยให้สิทธิสำหรับพนักงานที่ได้รับอนุญาตซึ่งมีหน้าที่ในการปฏิบัติเกี่ยวกับการรักษาความลับ และได้รับอนุญาตให้เข้ามีส่วนร่วมในการประมวลผลข้อมูลส่วนบุคคลเท่านั้น พนักงานเหล่านั้นจะต้องไม่ใช้ข้อมูลส่วนบุคคลดังกล่าวเพื่อวัตถุประสงค์ส่วนตัว หรือโอนข้อมูลส่วนบุคคลดังกล่าวไปยังผู้ที่ไม่ได้รับอนุญาตหรือไม่ทำให้สามารถเข้าถึงข้อมูลได้โดยวิธีการที่ไม่เหมาะสมแก่บุคคลที่ไม่ได้รับอนุญาต คำว่า “ไม่ได้รับอนุญาต” ในที่นี้ หมายความว่ารวมถึง เช่น การใช้ข้อมูลส่วนบุคคลของพนักงานโดยที่ตนไม่จำเป็นต้องเข้าถึงข้อมูลส่วนบุคคลในการปฏิบัติหน้าที่ของพนักงานนั้น ๆ นอกจากนี้ การควบคุมความมั่นคงปลอดภัยเพื่อประกันความสมบูรณ์และความลับของข้อมูลส่วนบุคคลให้เป็นไปตาม “คู่มือการปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ” THAI Privacy handbook: Technical and Organizational Measure

10. ข้อมูลชนิดพิเศษและข้อมูลอ่อนไหว

ข้อมูลส่วนบุคคลชนิดพิเศษรวมถึงข้อมูลเชื้อชาติ ชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา หรือการเป็นสมาชิกในองค์กรการค้า และการประมวลผลข้อมูลพันธุกรรม ข้อมูลชีวภาพ เพื่อวัตถุประสงค์ในการระบุอัตลักษณ์ของบุคคลธรรมดา ข้อมูลเกี่ยวกับสุขภาพหรือข้อมูลเกี่ยวกับความต้องการหรือรสนิยมทางเพศ ข้อมูลดังกล่าวโดยคำนิยามถือเป็นข้อมูลอ่อนไหว และต้องห้ามในการออกคำสั่งใด ๆ ทางกฎหมาย การบินไทยต้องไม่ประมวลผลข้อมูลดังกล่าวเว้นแต่เป็นข้อกำหนดตามสัญญาจ้างงาน กฎหมาย และข้อกำหนด หรือโดยความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

การประมวลผลข้อมูลส่วนบุคคลอื่น ๆ อาจถือเป็นข้อมูลอ่อนไหวเช่นกัน เมื่อคำนึงถึงเนื้อหาแหล่งที่มาปริมาณ และการใช้ตามวัตถุประสงค์ และเมื่อได้มีการประเมินความเสี่ยงของการประมวลผลแล้ว เช่น ข้อมูลการเงินในการบริหารจัดการค่าตอบแทน อาจถือเป็นข้อมูลอ่อนไหว จำเป็นต้องมีมาตรการในปกป้องและควบคุมเพิ่มเติม

11. การติดตามพฤติกรรม

การบินไทยสงวนสิทธิในการติดตามอีเมล การจราจรทางไซเบอร์ และสื่อสังคมออนไลน์ ของพนักงานของการบินไทยทราบเท่าที่กฎหมายอนุญาตให้ทำได้ แต่จะพยายามปกป้องความเป็นส่วนตัวส่วนตัวของพนักงานเท่าที่สามารถกระทำได้

12. การใช้อุปกรณ์เคลื่อนที่

การบินไทยจะพยายามปกป้องข้อมูลส่วนบุคคลของพนักงานที่อยู่ในอุปกรณ์เคลื่อนที่ เท่าที่สามารถกระทำได้ และเท่าที่การใช้อุปกรณ์ดังกล่าวเพื่อวัตถุประสงค์ส่วนตัว สามารถกระทำได้ รายละเอียดสามารถดูได้จาก นโยบายการใช้อุปกรณ์เคลื่อนที่ THAI Mobile Device Usage Policy

13. การละเมิดข้อมูลส่วนบุคคล

การละเมิดข้อมูลส่วนบุคคล หมายถึง ความสูญเสียการควบคุมโดยไม่เจตนา หรือการสูญหายของข้อมูลส่วนบุคคลภายใต้การบินไทย การป้องกันมิให้เกิดการละเมิดข้อมูลส่วนบุคคลถือเป็นความรับผิดชอบของพนักงาน และลูกจ้าง และคู่สัญญาของการบินไทยทั้งหมด ในกรณีที่เกิดความไม่ปกติของกระบวนการในการประมวลผลข้อมูลส่วนบุคคลขอให้ทุกคนแจ้งไปที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในทันที การถูกลักลอบในเวลาที่ การตอบกลับ การปฏิบัติ และการแจ้ง (ทั้งในกรณีหน่วยงานคุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลที่ได้รับผลกระทบ) เป็นไปตาม THAI Privacy Handbook: Personal Data Breach Management Process

14. การฝึกอบรมและความตระหนักรู้

พนักงานการบินไทยจะต้องประกันว่าหลักการทั่วไปที่ระบไว้ในนโยบายฉบับนี้จะได้รับการปฏิบัติ เพื่อการนี้ พนักงานระดับบริหาร อำนวยการ และจัดการ ทุกๆ ระดับจะต้องนำนโยบายนี้ไปปฏิบัติอย่างทั่วถึง รวมถึงการส่งมอบนโยบายนี้ให้กับพนักงานทุก ๆ คน

หากต้องการให้มีการฝึกอบรมใด ๆ ที่จำเป็น ขอให้ติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือผู้แทนท้องถิ่นของท่าน

15. ผลของสัญญาว่าจ้าง

หน้าที่และมาตรการต่าง ๆ ที่ต้องปฏิบัติเพิ่มเติมจากสัญญาการจ้างงานของพนักงานและคำสั่งและข้อบังคับต่าง ๆ พนักงานการบินไทยจะต้องศึกษาและทำความเข้าใจด้วยตนเองเป็นปกติอย่างสม่ำเสมอ การไม่ปฏิบัติตามข้อปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลถือเป็นการปฏิบัติผิดสัญญาว่าจ้างกับบริษัท ซึ่งอาจจะส่งผลถึงการจ้างบังคับตามกฎหมายแรงงานที่เกี่ยวข้อง

16. การให้บริการของบุคคลที่สาม และการช่วงงาน

เจ้าของหน่วยธุรกิจอาจมีการติดต่อบุคคลที่สามให้ทำการเก็บ รวบรวม หรือประมวลผลข้อมูล และข้อมูลส่วนบุคคล บุคคลที่สามดังกล่าวอาจเสนอบริการในการเป็นผู้ดูแล (hosting) หรือบริการงานช่วง (outsourcing) หรือการให้บริการสังคมข้อมูล (public cloud computing service)

หากว่าเจ้าของหน่วยธุรกิจตัดสินใจที่จะทำสัญญาให้บุคคลที่สามในการประมวลผลข้อมูล จะต้องกระทำภายใต้สัญญาซึ่งระบุสิทธิและหน้าที่ของการบินไทย และของคู่สัญญาไว้ ผู้รับงานช่วงที่เลือกจะต้องเลือกจากผู้ให้คำรับรองเกี่ยวกับการปฏิบัติตามมาตรการเทคนิค และมาตรการทางองค์กรที่การบินไทยกำหนด และการให้คำรับรองอันเพียงพอเกี่ยวกับการปกป้องรักษาสิทธิส่วนบุคคลและการใช้สิทธิต่าง ๆ เกี่ยวกับเรื่องดังกล่าว

ผู้ให้บริการช่วงมีหน้าที่ตามสัญญาในการประมวลผลข้อมูลส่วนบุคคลภายใต้ขอบเขตที่ระบุในสัญญา และตามคำสั่งของการบินไทยเท่านั้น การประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นไม่อาจกระทำได้ อย่างไรก็ตาม การบินไทยยังคงมีหน้าที่และต้องรับผิดชอบต่อการประมวลผลนั้นโดยคู่สัญญาที่จ้าง

ในกรณีที่มีความจำเป็นที่จะต้องส่งออก หรือโอนข้อมูลส่วนบุคคลจากสหภาพยุโรป (EU) หรือเขตเศรษฐกิจยุโรป (EEA) ไปยังประเทศที่ไม่มีมาตรการในการปกป้องข้อมูลส่วนบุคคลที่เพียงพอ เจ้าของหน่วยธุรกิจ โดยการหรือกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) จะต้องระบุกลไกการปกป้องที่เพียงพอตามที่กำหนดใน THAI Privacy Handbook: Cross Border Management Guidelines ทั้งนี้จะต้องมีการลงนามสัญญาการประมวลผลและการถ่ายโอนข้อมูล และข้อสัญญามาตรฐานเพื่อเป็นส่วนหนึ่งของสัญญาระหว่างผู้ส่งออก และผู้รับโอนข้อมูล

17. สิทธิของเจ้าของข้อมูล

เจ้าของข้อมูลสามารถใช้สิทธิของตนได้ตามกฎหมาย ซึ่งรวมถึงสิทธิในการเข้าถึง สิทธิในการแก้ไข สิทธิในการลบ สิทธิในการจำกัดการประมวลผล สิทธิในการถ่ายโอนข้อมูล สิทธิในการคัดค้านการประมวลผล ค่าขอดังกล่าวจะถูกส่งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือตัวแทนท้องถิ่น และได้รับการตอบกลับโดยไม่ชักช้า ภายในเวลา 30 วัน หลังจากได้รับคำร้องขอและอาจจะขยายออกไปได้เป็นเวลาอีกหนึ่งเดือน

เจ้าของหน่วยธุรกิจจะต้องสั่งการให้ผู้ประมวลผลข้อมูลเพื่อให้ความช่วยเหลือในการตอบคำร้องขอเกี่ยวกับการใช้สิทธิดังกล่าวภายใต้กฎหมายและจะต้องให้ข้อมูลที่จำเป็นเพื่อการดังกล่าวภายในเวลาอันสมควรหลังจากได้รับการแจ้งขอดังกล่าว

18. คำนิยาม

“ข้อมูลส่วนบุคคล” หมายถึงข้อมูลใด ๆ เกี่ยวกับการระบุตัวตน หรือที่สามารถระบุตัวตนบุคคลธรรมดาได้ คำว่าบุคคลที่สามารถระบุตัวตนได้ คือบุคคลที่สามารถระบุตัวตนได้ ไม่ว่าทางตรงหรือทางอ้อม โดยการอ้างอิงถึงหมายเลข หรือองค์ประกอบอย่างใดอย่างหนึ่ง หรือหลายอย่างรวมกัน ที่เจาะจงถึงตัวบุคคลทางกายภาพ ทางปรัชญา ทางจิตใจ ทางเศรษฐกิจ ทางวัฒนธรรม หรือทางสังคม

“ข้อมูลส่วนบุคคลชนิดพิเศษ” หมายถึงข้อมูลที่แสดงถึง เชื้อชาติ ชาติพันธุ์ ความเห็นทางการเมือง ความเชื่อทางศาสนา หรือปรัชญา ความเป็นสมาชิกสมาคมการค้า และการประมวลผลข้อมูลทางพันธุกรรม ข้อมูลชีวภาพ เพื่อวัตถุประสงค์ของการระบุตัวตนของบุคคลธรรมดา ข้อมูลเกี่ยวกับสุขภาพ หรือเกี่ยวกับความชอบหรือรสนิยมทางเพศ

“ข้อมูลส่วนบุคคลอ่อนไหว” ไม่ว่าเป็นการระบุถึง “ข้อมูลชนิดพิเศษ” (ดูคำนิยามข้างบน) หรือคือข้อมูลส่วนบุคคลซึ่งได้มีการประเมินและจัดระดับของความอ่อนไหวแล้ว อาจส่งผลกระทบอย่างแรงต่อเจ้าของข้อมูลหากมีการละเมิดข้อมูลส่วนบุคคลดังกล่าว

“ความยินยอม” ของเจ้าของข้อมูล หมายถึง ข้อบ่งชี้ ซึ่งให้โดยอิสระ เฉพาะเจาะจง ชัดแจ้ง ไม่คลุมเครือ ของเจ้าของข้อมูล ซึ่งแสดงถึงความตกลงให้ประมวลผลข้อมูลส่วนบุคคลของตนอย่างชัดเจน



Management Circular No. 005 /2019

Subject: Privacy Policy

According to the Management Meeting No. 32/2561 on 21 August 2018, Thai Airways International Public Company Limited (THAI) has established the Personal Data Privacy Policy in accordance with the procedures laid down by the European Union General Data Protection Regulation. THAI commits to take privacy as an issue of high importance to ensure the effective and continued data privacy practice and the protection of personal data of passengers, employees and related persons as required by law. The policy is attached herewith.

Your attention and cooperation will be much appreciated.

Bangkok, April 24 , 2019

THAI AIRWAYS INTERNATIONAL
PUBLIC COMPANY LIMITED

A handwritten signature in blue ink, appearing to read "Sumeth Damrongchaitham".

Sumeth Damrongchaitham
President

Approved by EMM
21 August 2018

Privacy Policy

THAI AIRWAYS INTERNATIONAL PUBLIC COMPANY LIMITED

GDPR Working Group - Data Privacy Policy Work Stream

[Last update date]
21 August 2018

1. Introduction

Thai Airways International Public Company Ltd. (THAI) realizes the importance of personal data, as well as, the needs to ensure the compliance with laws and regulations. In order to minimize the risks of personal data breach and non-compliance issues we may face. The privacy policy is established to instruct THAI employee to manage personal data securely and comply with the applicable laws and regulations.

This privacy policy applies to all personal data processed by full-time and part-time employees, contractors and partners doing business on behalf of THAI, as well as all legal entities, all operating locations in all countries, and all business processes conducted by THAI that are subject to comply with the contents of the policy.

The national and local laws of every country and legal jurisdiction in which personal data is collected and processed apply. Any mandatory registration provisions that may exist according to legal requirements must be observed. Every legally independent entity within THAI is responsible for assessing whether and to what extent such registration obligations exist toward national and/or regulatory authorities. In case of uncertainty, stakeholders must consult the Chief Privacy Officer/Data Protection Officer and/or legal department.

Collection of personal data by – and the disclosure to – governmental institutions and authorities will be carried out only on the basis of specific legal provisions. In all cases, this privacy policy imposes those restrictions that are necessary to meet the legal requirements of the respective laws.

2. Roles and Responsibilities

Protecting employee and customer privacy is a responsibility of every individual employee of THAI, including all its subsidiaries.

The general responsibility for adherence to this policy lies with the THAI management, who support and commissioned the execution of Privacy Management program in which all the relevant roles and responsibilities are enumerated.

Privacy Management program aims to control and mitigate privacy risk. It consists of process, standard and guidelines developed and maintained by Chief Privacy Officer/Data Protection Officer to instruct business process owner, as well as, every individual employee of THAI to manage personal data securely in order to align with the privacy laws and regulations.

3. Privacy by Design

It is THAI's explicit goal to implement new applications, services and products based on “privacy by design” to ensure that data privacy is a key consideration in the early stages of any development of business process and then throughout its life cycle. It consists of six privacy principles as follows:

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality

4. Lawfulness, Fairness and Transparency Processing

Processing of personal data shall be lawful and fair. It shall be transparent to data subject that their personal data are collected, used, and to what extent their personal data are or will be processed.

Business process owner shall ensure that processing of personal data is permitted only if the data subject has consented to it or if legal permissibility follows from applicable law. The permissibility of processing of personal data is a prerequisite for any transfer.

The consent shall be explicit declared in writing or with other legally permissible means, whereby the data subject has to be informed in advance about the purpose of such processing of personal data and any possible transfer. The declaration of consent has to be highlighted when included as part of other statements so as to be clear to the data subject. Business process owner shall incorporate "THAI Privacy Handbook: *Standard Consent Management and Template*" during the design of the business process.

Every business process in which personal data is processed falls under the delegated responsibility of the relevant mandated business process owner. In addition, it is imperative to have a clear overview of the data life cycle to enable proper risk analysis and adequate security control. An inventory of personal data processing is necessary for every business process owner.

5. Purpose Limitation

Personal data may be collected only for specific, explicit and legitimate purposes and may not be further processed contrary to such intended purpose. Business process owners (in consultation where necessary with the Chief Privacy Officer/Data Protection Officer) define and document processing purposes. Changes of purpose are permissible only with the consent of the data subject or if permitted by law.

Based on the defined and documented purposes, business process owners motivate the personal data records/items necessarily processed to serve those purposes.

6. Data Minimization

To minimize the risk of data exposure by reducing the sensitivity of stored information, wherever possible:

- One approach is to reduce the precision of the data retained after it has been collected. For example, if a customer phone number is to be used for statistical analysis, only a subset of the digits will be retained, such as the area code.
- Another approach is to convert personal data to a less sensitive form. For example, when using the customer's IP address to determine location for statistical analysis, the IP address will be discarded after mapping it to a city or town
- Another approach is to restrict access to large amounts of personal data. For example, employees who have a need to access individual records of personal data do not automatically have access to batches of personal data.

7. Accuracy

Business process owner shall take every reasonable step to ensure accuracy of personal data obtained and kept up-to-date. Inaccurate or outdated data shall be deleted or amended. Business owner should implement process or application for data subject to update his/her personal data. If applicable, provide self-service system for data subject to update by themselves.

8. Storage Limitation

The longer that personal data is retained, the higher the likelihood is of accidental disclosure, loss, theft and/or information growing stale. In other words, time is a critical success factor for a data breach. Therefore, personal data is retained only for the minimum amount of time necessary to support the business purpose or to meet legal requirements.

Business process owner shall define data retention period which states how long the data is being kept and why, and the manner in which it will be removed from all data stores. This retention period shall be applied in all systems where personal data exists, including backups and third-party environments.

9. Integrity & Confidentiality

Business process owner shall control the access of personal data by giving privilege to only the authorized staffs that are obligated to observe the requirements regarding data confidentiality, and are allowed to be involved in the processing of personal data. It is prohibited for them to use such data for their own private purposes, to transfer personal data to unauthorized parties or to make it accessible in any other improper way to unauthorized people. "Unauthorized" also means within this context, for instance, the use of personal data by employees in so far as it is not required for them to have access to the respective personal data to fulfill their employee duties. In addition, other security control to ensure integrity and confidentiality of personal data shall refer to *THAI Information Security Handbook* and *THAI Privacy Handbook: Technical and Organizational Measure*.

10. Special Categories and Sensitive Personal Data

Special categories of personal data include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Such information by definition is sensitive, and barring legal instructions, THAI will not process this information unless it is required by obligations under employment, laws and regulations or by the explicit consent of the data subject.

Taking into account context and attribution, volume and intended usage, other processing activities of personal data may be considered sensitive as well, following the privacy risk assessed. Financial information in the context of salary administration, for example, requires additional protection and security controls.

11. Monitoring

THAI reserves the right to monitor email, web traffic and social media activities of THAI employees to the extent permitted by law, but it will also strive to protect employees' privacy where possible.

12. Mobile Device Usage

THAI will strive to protect personal data in THAI employee mobile devices where possible and where the use of these devices for personal reasons is permitted. Details can be found in the respective to *THAI Mobile Device Usage policy*.

13. Data Breach

A data breach is any (potential) unintended loss of control over or loss of personal data within THAI's environment. Preventing a data breach is the responsibility of all THAI employees and contracted workforce. In addition, everyone is encouraged to notify the Chief Privacy Officer/Data Protection Officer in case of an irregularity in relation to personal data processing activities. A timely discovery,

response, treatment and notification (of both regulatory authorities and potentially the data subject's impacted) process is outlined in *THAI Privacy Handbook: Personal Data Breach Management Process*.

14. Training and Awareness

THAI will ensure that the general principles set forth in this privacy policy are observed. In this respect, managerial staff of THAI shall ensure that this policy is implemented, which includes, in particular, providing policy information to employees.

If additional training is required, the Chief Privacy Officer/Data Protection Officer, or the local representative, should be approached.

15. Employment law consequence

Further obligations and measures result from your employment contract and corresponding instructions, with which all THAI employees must familiarize themselves regularly and independently. Failure to exercise due diligence in the handling of personal data generally constitutes a breach of obligations arising from the employment relationship, which may lead to consequences under applicable labour law.

16. Third parties services/ subcontracting

Business process owner may decide to contract a third party for the collection, storage or processing of data, including personal data. The third party may offer services such as hosting, outsourcing, or private or public cloud computing services.

If business process owner decides to contract a third party for the processing of personal data, this must be regulated in a written agreement in which the rights and duties of THAI and of the subcontractor are specified. A subcontractor shall be selected that will guarantee the technological and organizational security measures required by THAI, and provide sufficient guarantees with respect to the protection of the personal rights and the exercise of rights related thereto.

The subcontractor is contractually obligated to process personal data only within the scope of the contract and the directions issued by THAI. Processing of personal data may not be undertaken for any other purpose. THAI remains responsible and accountable for the personal data processed by the contract partner.

In case there are needs to export or transfer personal data from European Union (EU) or European Economic Area (EEA) to the country without adequate level of data protection, business process owner (in consultation where necessary with Chief Privacy Officer and legal department) shall determine the appropriate safeguard mechanism according to "*THAI Privacy Handbook: Cross Border Management Guidelines*". "Data Processing and Transfer Agreement" and "Standard Contractual Clause" may have to be added as part of the contract between the data exporter and data importer.

17. Data Subject Right

Data subject may exercise their rights according to the applicable laws. This includes the right of access, right to rectification, right to erasure, right to restrict of processing, right to data portability, right to object. The requests shall pass to the Chief Privacy Officer, or the local representative and response without delay within 30 days after receiving of the request and may be prolonged for a further month.

Business process owner shall instruct the processor to assist them in responding to any requests relating to the exercise of a Data Subject's Rights under the applicable law and shall provide any information necessary therefore within timely manner after receiving the notification of such request.

18. Definition

"Personal data" (or "personal information") means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly – in particular, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

"Special Categories of Personal Data" pertains to personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Sensitive personal data" either indicates "special categories" (see above), or is personal data of which the sensitivity level has been assessed and classified, indicating potential severe impact on data subject when confidentiality of such data is breached.

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"Controller" means the natural person or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" means a natural or legal person, public authority, agency or other body which processes personal information on behalf of the controller.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Technological and organizational security measures" mean the operational measures to protect personal information from loss, destruct, and misuse, correct or disclose to unauthorized person during transfer and transit.

"Employee" means a person who is hired as a permanent worker for a salary to perform work for THAI.