การโอนข้อมูลส่วนบุคคลข้ามประเทศ: ศึกษากรณีการท่องเที่ยวแห่งประเทศไทยสำนักงานต่างประเทศที่ตั้งอยู่ในเขตสหภาพยุโรป

Cross-Border Transfer of Personal Data: A Study of the Tourism Authority of Thailand's Offices Located in the European Union

(Received: January 15, 2025 Revised: May 24, 2025 Accepted: June 20, 2025)

อัญธิกา ณ พิบูลย์[1]

Auntika Na Pibul

บทคัดย่อ

การท่องเที่ยวแห่งประเทศไทย (ททท.) เป็นหน่วยงานรัฐวิสาหกิจที่อยู่ภายใต้กระทรวงการท่องเที่ยวและกีฬา ถูกจัดตั้งขึ้นโดยมีวัตถุประสงค์ในการส่งเสริมการท่องเที่ยวไทย ททท. มีการจัดตั้งสำนักงานที่อยู่ในเขตสหภาพยุโรปซึ่งในแต่ละสำนักงานมีการดำเนินกิจกรรมที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในประเทศในเขตสหภาพยุโรป จึงส่งผลให้สำนักงานดังกล่าวตกอยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation (GDPR)) งานวิจัยนี้จึงมุ่งศึกษาลักษณะของกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ ททท. สำนักงานปารีส ประเทศฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต ประเทศเยอรมนี ททท. สำนักงานโรม ประเทศอิตาลี ททท. สำนักงานสตอกโฮล์ม ประเทศสวีเดน ซึ่งจากผลการศึกษาพบว่า ททท. สำนักงานดังกล่าว มีการดำเนินกิจกรรมที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศไทย ซึ่ง GDPR กำหนดเงื่อนไขของการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามไว้ค่อนข้างเข้มงวด งานวิจัยนี้จึงมุ่งเสนอแนะแนวทางในการพิจารณาว่า อย่างไรคือการโอนข้อมูลข้ามประเทศไปยังประเทศที่สาม รวมทั้งเสนอแนะให้มีการกำหนดแนวปฏิบัติที่เหมาะสมและถูกต้องตามกฎหมายในการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สาม ทั้งนี้ เพื่อเป็นการลดความเสี่ยงที่ ททท. จะมีความรับผิดตาม GDPR

คำสำคัญ: การท่องเที่ยวแห่งประเทศไทย, การโอนข้อมูลส่วนบุคคลข้ามประเทศ

---

[1] อาจารย์ ดร. ประจำคณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์ E-mail: auntika.n@nida.ac.th

Abstract

The Tourism Authority of Thailand (TAT) is a state enterprise under the Ministry of Tourism and Sports, established with the objective of promoting tourism in Thailand. TAT has set up offices within the European Union, and each office engages in activities related to the processing of personal data of data subjects in the EU countries. As a result, these offices are subject to the General Data Protection Regulation (GDPR). This research aims to study the nature of activities relating to personal data processing carried out by TAT offices in Paris (France), Frankfurt (Germany), Rome, (Italy) and Stockholm (Sweden). This research shows that some activities of these offices involve cross-border transfers of personal data to Thailand. Since the GDPR imposes stringent conditions on transfer of personal data to third countries, this research aims to suggest guideline for TAT to determine what constitutes cross-border data transfers to third countries and to propose the appropriate and legally practices for cross-border transferring of personal data to Thailand. This is intended to mitigate the risk of TAT being held liable under the GDPR.

Keywords: Tourism Authority of Thailand, Cross-Border Transfer of Personal Data

บทนำ

การท่องเที่ยวแห่งประเทศไทย (ททท.) เป็นหน่วยงานรัฐวิสาหกิจที่ถูกจัดตั้งขึ้นโดยพระราชบัญญัติการท่องเที่ยวแห่งประเทศไทย พ.ศ. 2522 ซึ่งมาตรา 8 กำหนดวัตถุประสงค์หลักไว้ 5 ประการ คือ 1. ส่งเสริมการท่องเที่ยวและอุตสาหกรรมท่องเที่ยว ตลอดจนการประกอบอาชีพของคนไทยในอุตสาหกรรมท่องเที่ยว; 2. เผยแพร่ประเทศไทยในด้านความงามของธรรมชาติ โบราณสถาน โบราณวัตถุ ประวัติศาสตร์ ศิลปวัฒนธรรม การกีฬา และวิวัฒนาการของเทคโนโลยี ตลอดจนกิจการอย่างอื่นอันจะเป็นการชักจูงให้มีการเดินทางท่องเที่ยว; 3. อำนวยความสะดวกและความปลอดภัยแก่นักท่องเที่ยว; 4. ส่งเสริมความเข้าใจอันดีและความเป็นมิตรไมตรีระหว่างประชาชนและระหว่างประเทศโดยอาศัยการท่องเที่ยว; 5. ริเริ่มให้มีการพัฒนาการท่องเที่ยว และเพื่อพัฒนาปัจจัยพื้นฐานและสิ่งอำนวยความสะดวกให้แก่นักท่องเที่ยว

โดยพระราชบัญญัติการท่องเที่ยวแห่งประเทศไทย พ.ศ. 2522 มาตรา 9 กำหนดให้ททท. มีอำนาจดังนี้

1. ให้คำปรึกษา แนะนำ ร่วมมือ และประสานงานกับส่วนราชการ องค์การ สถาบัน นิติบุคคลและเอกชน ทั้งภายในและภายนอกราชอาณาจักร

2. ส่งเสริม ร่วมมือ หรือดำเนินการในการฝึกอบรมและให้การศึกษาวิชาการต่าง ๆ เพื่อสร้างบุคลากรให้ได้มาตรฐานและเพียงพอในอุตสาหกรรมท่องเที่ยว

3. ส่งเสริมการทัศนศึกษา

4. สำรวจและรวบรวมหลักฐานต่าง ๆ จากส่วนราชการ องค์การสถาบัน นิติบุคคลและเอกชนผู้ประกอบอุตสาหกรรมท่องเที่ยว เพื่อประโยชน์ในการจัดทำสถิติเกี่ยวกับอุตสาหกรรมท่องเที่ยว

5. สำรวจ กำหนดพื้นที่และสถานที่เป็นสถานที่ท่องเที่ยวและทรัพยากรทางการท่องเที่ยวที่ต้องสงวนไว้เป็นของรัฐและให้อยู่ในความควบคุมดูแลของ ททท.

6. สำรวจ วางแผนและดำเนินการ จัดสร้าง ส่งเสริม อนุรักษ์ ฟื้นฟู พัฒนาสถานที่ท่องเที่ยวตลอดจนทรัพยากรทางการท่องเที่ยวและคุณภาพสิ่งแวดล้อม

7.ประกอบอุตสาหกรรมท่องเที่ยวเท่าที่จำเป็นรวมตลอดถึงการลงทุน หรือร่วมทุน เพื่อเป็นการริเริ่มให้มีการพัฒนาการท่องเที่ยวหรือพัฒนาปัจจัยพื้นฐานและสิ่งอำนวยความสะดวกให้แก่นักท่องเที่ยว

8. กู้หรือยืมเงินภายในและภายนอกราชอาณาจักร

9. ให้กู้หรือให้ยืมเงินโดยมีหลักประกันด้วยบุคคลหรือทรัพย์สินเพื่อส่งเสริมอุตสาหกรรมท่องเที่ยว

10. ออกพันธบัตรหรือตราสารอื่นใดเพื่อการลงทุนหรือร่วมทุนในกิจการอุตสาหกรรมท่องเที่ยว

11. ถือกรรมสิทธิ์ หรือมีสิทธิครอบครองหรือมีทรัพยสิทธิต่าง ๆ สร้าง ซื้อ จัดหา ขาย จำหน่าย เช่า ให้เช่า เช่าซื้อ ให้เช่าซื้อ ยืม ให้ยืม รับจำนำ รับจำนอง ทำการแลกเปลี่ยน โอน รับ โอน หรือดำเนินการใดๆ เกี่ยวกับทรัพย์สินทั้งในและนอกราชอาณาจักร ตลอดจนรับทรัพย์สินที่มีผู้อุทิศให้

12. กระทำกิจการอย่างอื่นบรรดาที่เกี่ยวกับหรือเนื่องในการจัดให้สำเร็จตามวัตถุประสงค์ของ ททท.

ทั้งนี้ เพื่อให้การปฏิบัติหน้าที่บรรลุวัตถุประสงค์ดังกล่าวข้างต้น ททท. จึงจัดตั้งสำนักงานทั้งภายในประเทศไทยและต่างประเทศมากมาย ยกตัวอย่างเช่น ททท. มีการจัดตั้งสำนักงานในเขตของสหภาพยุโรปหลายสำนักงาน (ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน) ในกรณีนี้จึงส่งผลให้ททท. มีการดำเนินกิจกรรมที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลเป็นจำนวนมากที่อยู่ในเขตสหภาพยุโรป และในบางกิจกรรมจะต้องมีการโอนข้อมูลส่วนบุคคลไปยังประเทศไทย จึงทำให้ ททท. อยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งก็คือ General Data Protection Regulation (GDPR) ซึ่งกฎหมายฉบับนี้กำหนดภาระหน้าที่ให้กับองค์กรที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลไว้หลายประการ และกำหนดเงื่อนไขที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม(ประเทศที่อยู่นอกเขตประเทศสมาชิกสหภาพยุโรป 27 ประเทศและนอร์เวย์ ไอซ์แลนด์ และลิกเตนสไตน์) ไว้ค่อนข้างเข้มงวด เนื่องจากการโอนข้อมูลส่วนในลักษณะดังกล่าว อาจส่งผลกระทบต่อระดับการคุ้มครองข้อมูลส่วนบุคคลได้ ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ ททท. จะต้องศึกษาหลักกฎหมายที่เกี่ยวข้อง แนวทางการปรับใช้ และกำหนดแนวปฏิบัติสำหรับ ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน ในการโอนข้อมูลข้ามประเทศไปยังประเทศไทย ทั้งนี้เพื่อป้องกันมิให้ ททท. มีความรับผิดและต้องรับโทษตามกฎหมาย อันจะส่งผลต่อภาพลักษณ์ของททท.และประเทศไทยต่อไป

วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของงานวิจัยนี้ คือ เพื่อศึกษาลักษณะของกิจกรรมของ ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน ที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล เพื่อวิเคราะห์ว่ามีการดำเนินกิจกรรมที่เป็นการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สามหรือไม่ รวมทั้งศึกษาหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพ

ยุโรป ซึ่งก็คือ General Data Protection Regulation(GDPR) ที่เกี่ยวข้องกับเงื่อนไขในการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สามหรือองค์การระหว่างประเทศ เพื่อที่จะเสนอแนะแนวปฏิบัติที่เหมาะสมและถูกต้องตามกฎหมายให้กับ ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน

วิธีดำเนินการวิจัย

งานวิจัยนี้ใช้วิธีการวิจัยเชิงเอกสาร (Documentary Research) โดยมุ่งศึกษา

1. เอกสารขั้นปฐมภูมิ (primary document) ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกรณีศึกษาต่างๆ ที่เกี่ยวข้อง

2. เอกสารชั้นทุติยภูมิ (secondary document) ได้แก่ คำแนะนำจากคณะทำงานและหน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น หน่วยงานของสหภาพยุโรป (Article 29 Data Protection Working Party (A29WP), European Data Protection Board (EDPB)) เป็นต้น รวมทั้งข้อมูลจากเว็บไซต์ของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง

ผลการวิจัย

1. แผนผังข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของ ททท.

ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน มีการดำเนินกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่เหมือนกัน ทั้งนี้เพื่อให้บรรลุภารกิจในการส่งเสริมการท่องเที่ยวไทย ซึ่งสามารถสรุปรายละเอียดได้ดังต่อไปนี้

กิจกรรม	วัตถุประสงค์	เจ้าของข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่เก็บรวบรวม	การเปิดเผยข้อมูล
การเชิญผู้ประกอบการเข้าร่วมกิจกรรม Road Show	เพื่อให้ผู้ประกอบการไทยได้พบกับนักท่องเที่ยวและผู้ประกอบการต่างชาติ	นักท่องเที่ยว/ผู้ประกอบการที่เข้าร่วมงาน	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล สำเนาหนังสือเดินทาง	ไม่มี
การจัดกิจกรรม FAM Trip	เพื่อให้ชาวต่างชาติได้รับประสบการณ์การท่องเที่ยวไทยและ	สื่อมวลชน Influencer Blogger	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล สำเนาหนังสือเดินทาง	ผู้ให้บริการสายการบิน/ที่พักในประเทศไทย

	นำกลับไปประชาสัมพันธ์			
การรับลงทะเบียนเพื่อจัดฝึกอบรม	เพื่อจัดฝึกอบรม	ผู้เข้าร่วมฝึกอบรม	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	ไม่มี
การถ่ายภาพและวิดีโอ	เพื่อใช้การประชาสัมพันธ์	ผู้เข้าร่วมกิจกรรมต่างๆ	ภาพถ่าย วิดีโอ	เปิดเผยต่อสาธารณะ
การรับสมัครสมาชิกทางเว็บไซต์และเก็บข้อมูลผู้ใช้งานบนเว็บไซต์	เพื่อใช้ในการจัดกิจกรรมและส่งข่าวสารในการส่งเสริมการท่องเที่ยว/ เพื่อใช้ในการปรับปรุงประสิทธิภาพในการทำงานของเว็บไซต์	ผู้เข้าร่วมกิจกรรมผ่านทางเว็บไซต์	ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ คุกกี้	บริษัทผู้รับจ้างดูแลเว็บไซต์
การรับสมัครงาน	เพื่อรับสมัครงาน	ผู้สมัครงาน	ชื่อ นามสกุล ที่อยู่ อีเมล เบอร์โทรศัพท์ สำเนาหนังสือเดินทาง ข้อมูลสุขภาพ ภาพถ่าย วุฒิการศึกษา ประสบการณ์ทำงาน ข้อมูลผู้ติดต่อ ประวัติอาชญากรรม	ททท. สำนักงานใหญ่
การทำคำสั่งจ้าง/สัญญาจ้าง	เพื่อจ้างงาน	บุคลากร ททท.	ชื่อ นามสกุล อีเมล ที่อยู่ เบอร์โทรศัพท์ ภาพถ่าย สำเนาหนังสือเดินทางประชาชน ข้อมูลสุขภาพ เงินเดือน วุฒิการศึกษา ประสบการณ์ทำงาน ประวัติอาชญากรรม	ททท. สำนักงานใหญ่และหน่วยงานที่เกี่ยวข้องกับการจัดสวัสดิการให้บุคลากร ททท.

2. หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป

กฎหมายที่กำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้ในเขตสหภาพยุโรปในปัจจุบัน คือข้อบังคับทั่วไปเกี่ยวกับการคุ้มครองข้อมูล หรือที่เรียกว่า General Data Protection Regulation (GDPR) มีผลบังคับใช้ตั้งแต่ในวันที่ 25 พฤษภาคม 2561 เป็นต้นมา ซึ่งกฎหมายฉบับนี้มีผลบังคับใช้กับ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม ด้วย แม้ว่าในแต่ละประเทศอันเป็นสถานที่ตั้งของสำนักงานต่างๆ ดังกล่าวจะมีการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายเฉพาะของแต่ละประเทศ ซึ่งก็คือ French Act No. 2018-493 of 20 June 2018 ของสาธารณรัฐฝรั่งเศส, Bundesdatenschutzgesetz (BDSG) ของสหพันธ์สาธารณรัฐเยอรมนี, Personal Data Protection Code (Legislative Decree no. 196 of 30 June 2003) ของสาธารณรัฐอิตาลีและ Lag (2018:218) med kompletterande bestämmelser till EU: sdataskyddsförordning (dataskyddslagen) หรือเรียกว่า Data Protection Act (2019:218) ของราชอาณาจักรสวีเดน แต่อย่างไรก็ตาม กฎหมายของแต่ละประเทศดังกล่าวมีหลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและเงื่อนไขของการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศที่เหมือนกันกับที่ GDPR กำหนดไว้ ในส่วนนี้ ผู้วิจัยจะนำเสนอสาระสำคัญโดยสรุปของ GDPR รวมทั้งหลักเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สามหรือองค์กรระหว่างประเทศตามที่ GDPR กำหนดไว้ ซึ่งมีรายละเอียดดังต่อไปนี้

2.1 ขอบเขตการบังคับใช้

GDPR มาตรา 2 กำหนด<u>ขอบเขตการบังคับใช้เชิงเนื้อหา</u>ไว้ว่า ลักษณะของกิจกรรมที่อยู่ภายใต้บังคับของ GDPR คือ “การประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วนด้วยวิธีการอัตโนมัติและกระบวนการประมวลผลอื่นนอกเหนือจากวิธีอัตโนมัติกับข้อมูลส่วนบุคคลซึ่งประกอบเป็นส่วนหนึ่งของระบบแฟ้มข้อมูลหรือตั้งใจจะประกอบเป็นส่วนหนึ่งของระบบแฟ้มข้อมูล” โดยจะไม่ใช้บังคับกับการประมวลผลข้อมูลในบางกรณี เช่น การประมวลผลข้อมูลส่วนบุคคลโดยพนักงานเจ้าหน้าที่ผู้มีอำนาจเพื่อวัตถุประสงค์ในการป้องกัน สืบสวนสอบสวน ตรวจจับหรือดำเนินคดีต่อความผิดหรือบังคับโทษทางอาญา รวมถึงการคุ้มครองและป้องกันภัยคุกคามต่อความปลอดภัยสาธารณะ โดย GDPR มาตรา 4 (2) กำหนดคำนิยามของคำว่า ‘การประมวลผล’ ไว้ว่าหมายถึง “การกระทำใด ๆ ต่อข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บรวบรวม การบันทึก การจัดระเบียบ การวางโครงสร้าง การจัดเก็บ การปรับเปลี่ยนหรือแก้ไข การดึงข้อมูลมาใช้ การผสมรวม การใช้ การเปิดเผยโดยการโอน การเผยแพร่ หรือกระทำการอื่นใดที่ทำให้ข้อมูลมีการแพร่หลาย การจัดตำแหน่งหรือการรวม การจำกัด การลบหรือการทำลาย”

GDPR มาตรา 3 กำหนดขอบเขตการบังคับใช้เชิงพื้นที่ไว้ว่า บังคับใช้กับ

1. การประมวลผลข้อมูลส่วนบุคคลในบริบทของกิจกรรมของสถานที่ตั้งของผู้ควบคุมหรือผู้ประมวลผลซึ่งอยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลนั้นได้กระทำในหรือนอกสหภาพยุโรปก็ตาม

2. การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในสหภาพยุโรปโดยที่ผู้ควบคุมหรือผู้ประมวลผลมิได้อยู่ในสหภาพยุโรป เมื่อกิจกรรมการประมวลผลนั้นเกี่ยวข้องกับ (a) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลซึ่งอยู่ในสหภาพยุโรป โดยไม่คำนึงว่าจะมีการชำระเงินโดยเจ้าของข้อมูลหรือไม่ (b) การติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในสหภาพยุโรป

2.2 ข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลชนิดพิเศษ

GDPR มาตรา 3 กำหนดบทนิยามศัพท์ของคำว่า ‘ข้อมูลส่วนบุคคล’ ไว้ว่า หมายถึง “ข้อมูลใด ๆ ที่เกี่ยวกับบุคคลธรรมดาที่ถูกระบุหรือสามารถระบุอัตลักษณ์ได้ (‘เจ้าของข้อมูลส่วนบุคคล’) บุคคลธรรมดาที่สามารถถูกระบุอัตลักษณ์ได้ คือ บุคคลที่สามารถถูกระบุอัตลักษณ์ได้ไม่ว่าโดยตรงหรือโดยอ้อมโดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งที่ระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลที่แสดงถึงสถานที่ตั้ง สิ่งที่ระบุอัตลักษณ์ออนไลน์หรือปัจจัยประการหนึ่งหรือหรือหลายประการที่เจาะจงไปยังอัตลักษณ์ทางกายภาพสรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรมหรืออัตลักษณ์ทางสังคมของบุคคลดังกล่าว” GDPR มาตรา 9 อธิบายลักษณะของข้อมูลส่วนบุคคลชนิดพิเศษไว้ว่าคือ “ข้อมูลส่วนบุคคลที่เปิดเผยต้นกำเนิดทางเชื้อชาติและชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา หรือการเป็นสมาชิกสหภาพวิชาชีพ และการประมวลข้อมูลพันธุกรรม ข้อมูลชีวภาพเพื่อวัตถุประสงค์ในการระบุอัตลักษณ์บุคคลธรรมดาอย่างเฉพาะเจาะจง ข้อมูลเกี่ยวข้องกับสุขภาพหรือข้อมูลเกี่ยวกับชีวิตทางเพศหรือพฤติกรรมทางเพศของบุคคลธรรมดา

2.3 ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

GDPR กำหนดสถานะของบุคคลหรือหน่วยงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลไว้ 2 สถานะ คือ ผู้ควบคุม (Controller) และผู้ประมวลผล (Processor) GDPR มาตรา 4(7) ให้ความหมายของคำว่า ‘ผู้ควบคุม’ ไว้ว่า หมายถึง “บุคคลหรือนิติบุคคล หน่วยงานภาครัฐ ตัวแทนหรือองค์กรอื่นใด โดยลำพังหรือร่วมกันกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลดังกล่าวถูกกำหนดโดยกฎหมายของสหภาพยุโรปหรือของประเทศสมาชิก ผู้ควบคุมหรือเกณฑ์เฉพาะสำหรับการแต่งตั้งตัวแทนผู้ควบคุมอาจถูกกำหนดไว้โดยกฎหมายของสหภาพยุโรปหรือกฎหมายของประเทศสมาชิกนั้น” โดย GDPR มาตรา 13 และ 30 กำหนดให้ผู้ควบคุมมีหน้าที่ต่างๆ เช่น แจ้งข้อมูลต่างๆ ให้เจ้าของข้อมูลส่วน

บุคคลทราบเมื่อได้รับข้อมูลส่วนบุคคล เช่น วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลและฐานทางกฎหมายสำหรับการประมวลผลข้อมูล ฯลฯ จัดทำบันทึกกิจกรรมการประมวลผล

DPR มาตรา 4(8) ให้ความหมายของคำว่าคำว่า ‘ผู้ประมวลผล’ ไว้ว่า หมายถึง “บุคคลหรือนิติบุคคล หน่วยงานภาครัฐ ตัวแทนหรือองค์กรอื่นใด ซึ่งประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุม” โดย GDPR มาตรา 28 กำหนดให้ผู้ประมวลมีหน้าที่ต่างๆ เช่น การปรับใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมในลักษณะที่ทำให้การประมวลผลข้อมูลเป็นไปตามเงื่อนไขที่กฎหมายกำหนดและทำให้แน่ใจว่ามีการคุ้มครองสิทธิของเจ้าของข้อมูล ฯลฯ ในส่วนของ ‘ผู้ควบคุมร่วม’ GDPR มาตรา 26 อธิบายลักษณะไว้ว่าคือ “ผู้ควบคุมจำนวนตั้งแต่สองรายขึ้นไปซึ่งร่วมกันกำหนดวัตถุประสงค์และวิธีการในประมวลผล” ซึ่ง GDPR กำหนดให้ผู้ควบคุมร่วมจะต้องกำหนดความผิดชอบในการปฏิบัติตามกฎหมายสำหรับผู้ควบคุมร่วมแต่ละรายโดยเฉพาะอย่างยิ่งในประเด็นที่เกี่ยวข้องกับการใช้สิทธิของเจ้าของข้อมูลและหน้าที่ของผู้ควบคุมแต่ละราย รวมทั้งการระบุที่ติดต่อสำหรับเจ้าของข้อมูล

2.4 ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคล

GDPR มาตรา 5 กำหนดหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลไว้ว่า ควรดำเนินการภายใต้หลักความชอบด้วยกฎหมาย ความเป็นธรรม ความโปร่งใส หลักการกำหนดขอบเขตของวัตถุประสงค์ หลักการใช้ข้อมูลให้น้อยที่สุด หลักความแม่นยำ หลักการกำหนดขอบเขตการเก็บรักษา หลักความสมบูรณ์และเป็นความลับ หลักความรับผิดชอบและสามารถตรวจสอบได้ ซึ่งการประมวลข้อมูลส่วนบุคคลจะชอบด้วยกฎหมายก็ต่อเมื่อดำเนินการภายใต้ฐานทางกฎหมายที่กำหนดไว้ตาม GDPR มาตรา 6 เช่น (1) เจ้าของข้อมูลให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์เฉพาะอย่างหนึ่งหรือมากกว่า (2) การประมวลผลจำเป็นสำหรับการปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อให้เป็นตามขั้นตอนที่เจ้าของข้อมูลร้องขอก่อนทำสัญญาฯลฯ

นอกจากนั้น GDPR มาตรา 9 กำหนดไว้ว่า การประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษจะสามารถดำเนินการได้ในกรณี เช่น (1) เจ้าของข้อมูลให้ความยินยอมอย่างชัดแจ้งในการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์เฉพาะอย่างหนึ่งหรือมากกว่า (2) การประมวลผลจำเป็นต่อวัตถุประสงค์ในการปฏิบัติตามพันธกรณีและใช้สิทธิบางประการของผู้ควบคุมหรือเจ้าของข้อมูลในด้านที่เกี่ยวกับกฎหมายการจ้างงาน

โดย GDPR มาตรา 7 กำหนดไว้ว่าในกรณีที่การประมวลผลอยู่บนฐานความยินยอม ผู้ควบคุมจะต้องสามารถแสดงเห็นได้ว่าเจ้าของข้อมูลให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลของของตน ซึ่งในกรณีที่เจ้าของข้อมูลให้ความยินยอมในรูปแบบของลายลักษณ์อักษร คำร้องขอความ

ยินยอมควรจะอยู่ในลักษณะที่มีความแยกเฉพาะจากเรื่องอื่นๆ ในรูปแบบที่เข้าใจได้และเข้าถึงได้ง่าย ใช้ภาษาที่ชัดเจนและไม่ซับซ้อน และแจ้งให้เจ้าของข้อมูลทราบก่อนการให้ความยินยอมว่ามีสิทธิในการถอนความยินยอมเมื่อใดก็ได้

2.5 การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์กรระหว่างประเทศ

GDPR Chapter 5 (มาตรา 44-50) กำหนดหลักเกณฑ์ที่ค่อนข้างเข้มงวดในการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม (ประเทศนอกเขตเศรษฐกิจยุโรป (European Economic Area(EEA)) ซึ่งก็คือประเทศที่อยู่นอกเขตของประเทศสมาชิกสหภาพยุโรป 27 ประเทศและประเทศไอซ์แลนด์ นอร์เวย์ ลิกเตนสไตน์)) หรือการโอนไปข้อมูลส่วนบุคคลไปยังองค์การระหว่างประเทศ ทั้งนี้ เพื่อเป็นการทำให้แน่ใจว่าระดับการคุ้มครองข้อมูลที่ได้รับการรับรองโดย GDPR จะยังคงมีอยู่ แม้จะมีการโอนข้อมูลไปยังประเทศที่สามหรือไปยังองค์การระหว่างประเทศก็ตาม โดย GDPR กำหนดเงื่อนไขที่ผู้ควบคุมและผู้ประมวลผลสามารถโอนข้อมูลส่วนบุคคลในกรณีดังกล่าวได้ ภายใต้เงื่อนไขดังต่อไปนี้

2.5.1 เป็นการโอนภายใต้คำตัดสินที่รับรองความเพียงพอ (Adequacy Decision)

GDPR มาตรา 45 กำหนดไว้ว่า ภายหลังจากที่คณะกรรมาธิการยุโรปได้ประเมินระดับการคุ้มครองที่เพียงพอจากองค์ประกอบต่างๆ เช่น การมีอยู่และการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพของหน่วยงานกำกับดูแล ฯลฯ แล้ว คณะกรรมาธิการยุโรปอาจออกคำตัดสินรับรองความเพียงพอให้กับประเทศที่สามหรือองค์การระหว่างประเทศที่มีระดับในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเทียบเท่ากับ GDPR จึงส่งผลให้ข้อมูลส่วนบุคคลสามารถถูกโอนยังประเทศเหล่านั้นได้อย่างเสรี แต่จะต้องมีกลไกในการทบทวนระดับความเพียงพออย่างน้อยทุกๆ สี่ปี

2.5.2 เป็นการโอนภายใต้มาตรการป้องกันที่เหมาะสม (Appropriate Safeguards)

GDPR มาตรา 46 กำหนดไว้ว่า ในกรณีที่จะมีการโอนข้อมูลไปยังประเทศที่ไม่มีคำตัดสินรับรองความเพียงพอ การโอนข้อมูลสามารถทำได้หากมีการใช้มาตรการป้องกันที่เหมาะสม และอยู่ภายใต้เงื่อนไขของการมีอยู่ของการบังคับใช้สิทธิของเจ้าของข้อมูลและการเยียวยาทางกฎหมายที่มีประสิทธิภาพให้กับเจ้าของข้อมูล ยกตัวอย่างเช่น เป็นการโอนภายใต้ข้อสัญญามาตรฐาน (Standard Contractual Clauses - SCCs) หรือ นโยบายการคุ้มครองข้อมูลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding Corporate Rules - BCRs) เป็นต้น

2.5.3 เป็นการโอนภายใต้ข้อยกเว้นเฉพาะ (Derogations for Specific Situations)

ในกรณีที่ไม่มีคำตัดสินที่รับรองความเพียงพอตามมาตรา 45 และไม่สามารถใช้มาตรการป้องกันที่เหมาะสมตามมาตรา 46 ได้ GDPR มาตรา 49 กำหนดไว้ว่า การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามหรือองค์การระหว่างประเทศสามารถทำได้หากอยู่ภายใต้ข้อยกเว้นเฉพาะบางประการ

เช่น ได้รับการยินยอมจากเจ้าของข้อมูลอย่างชัดเจนภายหลังจากได้รับแจ้งความเสี่ยงที่อาจเกิดขึ้นจากการโอนดังกล่าว หรือการโอนข้อมูลเป็นสิ่งจำเป็นเพื่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุม เป็นต้น

2.6 การเยียวยา ความรับผิดและโทษ

GDPR มาตรา 82 กำหนดสิทธิในการได้รับการชดเชยและความรับผิดไว้ว่า บุคคลใดก็ตามที่ได้รับความเสียหายทางวัตถุหรือความเสียหายที่ไม่ใช่ทางวัตถุอันเป็นผลจากการละเมิดบทบัญญัติจะต้องมีสิทธิได้รับการชดเชยจหรือผู้ประมวลผลสำหรับมูลค่าความเสียหายที่ได้รับ และ GDPR มาตรา 83 กำหนดค่าปรับทางปกครองไว้สำหรับกรณีมีการละเมิดบทบัญญัติต่างๆ ไว้ดังนี้ (1) กำหนดจำนวนค่าปรับทางปกครองไม่เกิน 10,000,000 ยูโรหรือในกรณีของวิสาหกิจคือไม่เกินร้อยละ 2 ของยอดเงินหมุนเวียนทั่วโลกตลอดปีงบประมาณก่อนหน้า แล้วแต่ว่าสิ่งใดมีมูลค่าสูงกว่า สำหรับการละเมิดบทบัญญัติบางประการ เช่น กรณีที่ผู้ควบคุมไม่ปฏิบัติตามเงื่อนไขการขอความยินยอมเด็กที่เกี่ยวข้องกับบริการสารสนเทศ (GDPR มาตรา 8) ฯลฯ และ (2) กำหนดจำนวนค่าปรับทางปกครองไว้ไม่เกิน 20,000,000 ยูโร หรือในกรณีของวิสาหกิจคือไม่เกินร้อยละ 4 ของยอดเงินหมุนเวียนทั่วโลกตลอดปีงบประมาณก่อนหน้า แล้วแต่ว่าสิ่งใดมีมูลค่าสูงกว่า สำหรับการละเมิดบทบัญญัติบางประการ เช่น การละเมิดหลักการพื้นฐานสำหรับการประมวลผลรวมถึงเงื่อนไขเรื่องความยินยอมตามมาตรา 5,6,7,9 ฯลฯ

3. วิเคราะห์ประเด็นข้อพิจารณากรณีการโอนข้อมูลส่วนบุคคลข้ามประเทศของ ททท. สำนักงานสาขาต่างประเทศที่อยู่ในเขตสหภาพยุโรป

เนื่องจาก ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม มีการดำเนินกิจกรรมที่มีความหลากหลายที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลและในบางกรณีก็มีการดำเนินกิจกรรมที่อาจเข้าข่ายเป็นการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศไทย ดังนั้น เพื่อให้ททท. สามารถกำหนดแนวทางในการปฏิบัติตาม GDPR ได้อย่างถูกต้องและครบถ้วน จึงมีประเด็นที่จะต้องพิจารณาดังต่อไปนี้

3.1 ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม มีการดำเนินกิจกรรมที่เป็นการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สามหรือไม่

GDPR ไม่ได้มีการกำหนดคำนิยามของคำว่าการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สามไว้ แต่ EDPB ซึ่งเป็นหน่วยงานกำกับดูแลในการปฏิบัติตาม GDPR ได้กำหนดหลักเกณฑ์การพิจารณา

ว่าการประมวลผลข้อมูลส่วนบุคคลใดถือว่าเป็นการโอนข้อมูลไปยังไปยังประเทศที่สามที่อยู่ภายใต้บังคับของ GDPR Chapter 5 ไว้ในแนวทางที่ 5/2021 ว่าจะต้องมีองค์ประกอบ 3 ประการ ดังต่อไปนี้

1. ผู้ควบคุมหรือผู้ประมวลผล (ผู้ส่งออกข้อมูล) จะต้องอยู่ภายใต้บังคับของ GDPR สำหรับการประมวลผลข้อมูลนั้นๆ

2. ผู้ส่งออกข้อมูลมีการประมวลผลที่เป็นการเปิดเผยข้อมูลโดยการโอนหรือการทำให้ข้อมูลส่วนบุคคลเปิดเผยต่อผู้ควบคุมอื่นๆ, ผู้ควบคุมร่วม หรือผู้ประมวลผล (ผู้นำเข้าข้อมูล) โดย EDPB ให้ความเห็นไว้ว่า กรณีการให้อำนาจองค์กรที่อยู่ในประเทศที่สามสามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์ที่อยู่ในเขตสหภาพยุโรปจากระยะทางไกล (remote access) ก็ถือว่าเป็นการโอนข้อมูลตามองค์ประกอบนี้เช่นกัน นอกจากนั้น EDPB ให้ความเห็นว่า แม้เป็นการใช้บริการเก็บข้อมูลใน Cloud ซึ่งผู้ให้บริการตั้งอยู่ในเขตของประเทศที่สาม ก็ถือว่าเป็นการโอนข้อมูลเช่นกัน

3. ผู้นำเข้าข้อมูลอยู่ในประเทศที่สาม โดยไม่คำนึงว่าผู้นำเข้าข้อมูลจะอยู่ภายใต้บังคับของ GDPR หรือไม่ก็ตาม

เมื่อพิจารณาจากองค์กรประกอบข้อ 1 แล้วพบว่า ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์มซึ่งมีสถานที่ตั้งอยู่ในเขตสหภาพยุโรปและมีการประมวลผลข้อมูลส่วนบุคคลที่เก็บรวบรวมจากสถานที่ตั้งดังกล่าว จึงมีสถานะเป็นเป็นผู้ควบคุมซึ่งเป็นผู้ส่งออกข้อมูลที่อยู่ภายใต้บังคับของ GDPR

หากพิจารณาองค์ประกอบข้อ 2 และข้อมูลที่ได้จากการเข้าหารือกับองค์กรกำกับดูแลที่เกี่ยวข้อง พบว่า ททท. สำนักงานข้างต้นมีดำเนินกิจกรรมที่เป็นการโอนข้อมูลส่วนบุคคลของลูกจ้างท้องถิ่นของแต่ละสำนักงานไปยัง ททท. สำนักงานใหญ่ ประเทศไทย (ผู้ควบคุมร่วม) ซึ่งมีสถานะทางกฎหมายเป็นนิติบุคคลที่แยกต่างหากจาก ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม (แต่ละสำนักงานมีสถานะเป็นนิติบุคคลที่มีอำนาจในการตัดสินใจในการดำเนินกิจกรรมต่างๆ และอยู่ภายใต้การบริหารจัดการโดยผู้อำนวยการของแต่ละสำนักงาน) เพื่อวัตถุประสงค์ในการบริหารจัดการงานด้านทรัพยากรบุคคล นอกจากนั้น ททท. สำนักงานข้างต้นยังมีการโอนข้อมูลส่วนบุคคลของนักท่องเที่ยวที่เก็บรวบรวมโดยแต่ละสำนักงานไปยังผู้ประกอบการท่องเที่ยวอื่นๆ (ผู้ประมวลผล) ในประเทศไทย เช่น ผู้ประกอบการที่พัก สายการบิน ฯลฯ เพื่อวัตถุประสงค์ในการจัดกิจกรรม FAM Trip (การพานักท่องเที่ยวต่างชาติไปสัมผัสประสบการณ์การท่องเที่ยวในประเทศไทย เพื่อให้นักท่องเที่ยวนำข้อมูลไปประชาสัมพันธ์การท่องเที่ยวไทยต่อไป)

เมื่อพิจารณาองค์ประกอบข้อ 3 แล้ว พบว่า ผู้นำเข้าข้อมูลซึ่งเป็นผู้รับโอนข้อมูลจาก ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม นั้นคือ ททท. สำนักงานใหญ่ และผู้ประกอบธุรกิจท่องเที่ยวที่ตั้งอยู่ในประเทศไทย ดังนั้น จึงสามารถสรุป

ได้ว่า ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม มีการโอนข้อมูลส่วนบุคคลข้ามประเทศไปยังประเทศที่สาม (ประเทศไทย)

3.2 ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม สามารถโอนข้อมูลข้ามประเทศไปยังประเทศไทยได้ภายใต้เงื่อนไขใด

ในกรณีนี้ GDPR กำหนดหลักเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามไว้ว่า สามารถดำเนินการได้หากเป็นการดำเนินการภายใต้เงื่อนไขตามที่ GDPR Chapter 5 (มาตรา 44-50) กำหนดไว้ ทั้งนี้ เพื่อเป็นการทำให้แน่ใจว่าระดับในการให้ความคุ้มครองข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่รับรองโดย GDPR จะยังคงมีอยู่ แม้จะมีการโอนข้อมูลในลักษณะดังกล่าว ดังนั้น เมื่อพิจารณาลักษณะของการประมวลผลข้อมูลส่วนบุคคลในบริบทของททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และหลักเกณฑ์ตามที่ GDPR แล้ว จึงสามารถสรุปได้ว่า เนื่องจากคณะกรรมาธิการยุโรปยังไม่มีคำตัดสินรับรองระดับในการคุ้มครองข้อมูลที่เพียงพอให้กับประเทศไทย ททท. สำนักงานดังกล่าว จึงไม่สามารถโอนข้อมูลไปยังประเทศไทยภายใต้เงื่อนไขของ GDPR มาตรา 45

แต่อย่างไรก็ตาม ททท. สำนักงานข้างต้นยังคงสามารถดำเนินกิจกรรมต่างๆ ที่เป็นการโอนข้อมูลส่วนบุคคลไปยังประเทศไทยได้โดยใช้เครื่องมือต่างๆ ตามที่ GDPR กำหนดไว้ในมาตรา 46 (มีมาตรการป้องกันที่เหมาะสม) หรือมาตรา 47 (มีข้อยกเว้นเฉพาะ) ในกรณีนี้ EDPB แนะนำว่าจะต้องมีการประเมินเป็นรายกิจกรรมให้รอบคอบก่อนว่ามีความจำเป็นที่จะต้องมีการโอนข้อมูลหรือไม่ นอกจากนั้น ททท. ควรพิจารณาประเด็นอื่นๆ ที่อาจส่งผลกระทบต่อระดับในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอตามมาตรฐานของ GDPR เช่น การเข้าถึงข้อมูลของหน่วยงานภาครัฐในประเทศที่สามซึ่งอาจอยู่ภายใต้หลักกฎหมายที่ไม่สอดคล้องกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตาม GDPR หรือความไม่สอดคล้องระหว่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศที่สามและ GDPR หรือกรณีที่ประเทศที่สามไม่มีองค์กรกำกับดูแล ไม่มีกระบวนการที่มีประสิทธิภาพที่เพียงพอในการรับเรื่องร้องเรียน ฯลฯ จากนั้นจึงพิจารณาว่าควรจะต้องใช้เครื่องมือใดในการโอนข้อมูลเพื่อให้เกิดประสิทธิภาพมากที่สุดในการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยพิจารณาจากลักษณะของการโอนอันได้แก่ วัตถุประสงค์ของการโอน ประเภทและรูปแบบของข้อมูลส่วนบุคคลที่ถูกโอน ประเภทขององค์กรที่จะเกี่ยวข้องกับข้อมูลที่ถูกโอนสถานที่ในการจัดเก็บข้อมูล ความเป็นไปได้ในกรณีที่ข้อมูลนั้นจะถูกโอนต่อไปยังประเทศอื่นๆ

เมื่อพิจารณาจากหลักเกณฑ์ข้างต้นประกอบกับลักษณะของการโอนข้อมูลของ ททท. แล้วพบว่า การดำเนินกิจกรรมการโอนข้อมูลส่วนบุคคลไปยังประเทศไทยของททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์มเพื่อวัตถุประสงค์ในการบริหารจัดการงานด้านทรัพยากรบุคคล เพื่อวัตถุประสงค์ในการจัดกิจกรรม FAM Trip นั้นมีความจำเป็นทั้งเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลเองและเพื่อประโยชน์ของททท. และประเทศไทย

ต่อไป นอกจากนั้น หากพิจารณาประเด็นอื่นๆ ที่ เช่น เรื่องความสอดคล้องของบทบัญญัติของ GDPR กับบทบัญญัติของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งพบว่าไม่ได้มีความขัดหรือแย้งกันในสาระสำคัญแต่อย่างใด รวมทั้งประเทศไทยมีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานเฉพาะทำหน้าที่ในการกำกับดูแลให้มีการปฏิบัติตามกฎหมายและรับเรื่องร้องเรียนต่างๆ ที่เกี่ยวข้อง ดังนั้นจึงสามารถสรุปได้ว่าไม่พบความเสี่ยงใดที่จะส่งผลกระทบ

แต่อย่างไรก็ตาม ประเทศไทยถือเป็นประเทศที่สาม ททท. จึงต้องพิจารณาเลือกใช้เครื่องมือที่ใช้ในการโอนข้อมูลมายังประเทศไทยตามหลักเกณฑ์ที่ GDPR กำหนดไว้ ซึ่งเมื่อพิจารณาข้อมูลที่ได้จากการเข้าหารือกับองค์กรกำกับดูแลที่เกี่ยวข้อง (เช่น CNIL) ผู้วิจัยพบว่า การจัดทำข้อสัญญามาตรฐาน (Standard Contractual Clauses - SCCs) ตามมาตรา 46 (2) (c) น่าจะเป็นเครื่องมือที่เหมาะสมและมีประสิทธิภาพสำหรับ ททท. ในการโอนข้อมูลไปยังประเทศไทยเพื่อให้บรรลุวัตถุประสงค์ในการบริหารจัดการงานด้านทรัพยากรบุคคล และเพื่อวัตถุประสงค์ในการจัดกิจกรรม FAM Trip ประชาสัมพันธ์การท่องเที่ยวไทย ซึ่งคณะกรรมาธิการยุโรป (European Commission) ได้รับรองตัวอย่างข้อสัญญามาตรฐานที่สามารถนำไปใช้สำหรับการโอนข้อมูลจากผู้ควบคุมไปยังผู้ควบคุม หรือจากผู้ควบคุมไปยังผู้ประมวลผล หรือจากผู้ประมวลผลไปยังผู้ประมวลผล หรือจากผู้ประมวลผลไปยังผู้ควบคุม ซึ่งในข้อสัญญามีรายละเอียดเกี่ยวกับภาระหน้าที่ของคู่สัญญาที่จะต้องปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลต่างๆ ตามมาตรฐานที่กำหนดไว้ตาม GDPR โดยที่คู่สัญญาสามารถเพิ่มเติมรายละเอียดอื่นๆ ได้ตราบเท่าที่ไม่ขัดหรือแย้งกับข้อสัญญาดังกล่าว และจะต้องไม่ปรากฏข้อสัญญาที่มีความกำกวมซึ่งจะส่งผลกระทบต่อระดับในการให้ความคุ้มครองข้อมูลส่วนบุคคล คู่สัญญาสามารถใช้ข้อสัญญาดังกล่าวเป็นเครื่องมือในการบริหารจัดความเสี่ยงต่างๆ ที่อาจเกิดขึ้นเมื่อข้อมูลถูกโอนไปยังประเทศที่สาม เช่น ประเด็นความขัดกันของบทบัญญัติของกฎหมายของประเทศดังกล่าวและบทบัญญัติของ GDPR ประเด็นการบริหารจัดการเมื่อมีการเข้าถึงโดยรัฐบาลของประเทศที่สาม ประเด็นการฟ้องร้องคดีและการชดใช้ความเสียหายที่เกิดขึ้น ฯลฯ

ดังนั้น จึงสามารถสรุปได้ว่า ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม สามารถนำข้อสัญญามาตรฐานดังกล่าวมาใช้ในการลงนามทำข้อตกลงกับหน่วยงานผู้รับโอนข้อมูลที่ตั้งอยู่ในประเทศไทยได้ ทั้งนี้ เพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลที่โอนไปจะได้รับการคุ้มครองในระดับที่เพียงพอและเหมาะสมในประเทศไทย กล่าวคือ อยู่ในระดับที่เท่าเทียมกับที่ได้รับความคุ้มครองภายใต้ GDPR โดยแต่ละสำนักงานจะต้องแจ้งให้เจ้าของข้อมูลทราบอย่างชัดเจนเกี่ยวกับการโอนข้อมูลไปยังประเทศที่สาม และมาตรการป้องกันที่เหมาะสมเพื่อรักษาความปลอดภัยของข้อมูลดังกล่าว

ข้อเสนอแนะการวิจัย

เมื่อพิจารณาลักษณะของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการโดย ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์มแล้ว พบว่า ททท. สำนักงานดังกล่าวมีการดำเนินกิจกรรมบางประการที่เป็นการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม ซึ่งก็คือ ประเทศไทย ซึ่งในกรณีนี้ GDPR กำหนดเงื่อนไขสำหรับการโอนข้อมูลไว้ค่อนข้างเข้มงวด ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ ททท. จะต้องจัดทำแนวปฏิบัติเกี่ยวกับการโอนข้อมูลส่วนบุคคลข้ามประเทศ เพื่อให้พนักงานและลูกจ้างของ ททท. แต่ละสำนักงานสามารถปฏิบัติตามหลักเกณฑ์ที่ GDPR กำหนดไว้ได้อย่างถูกต้องและครบถ้วน โดยผู้วิจัยจะเสนอแนะแนวปฏิบัติซึ่งสามารถสรุปได้ดังต่อไปนี้

เมื่อ ททท. แต่ละสำนักงานข้างต้นมีการดำเนินกิจกรรมที่เป็นการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามโดยพิจารณาจากองค์ประกอบ 3 ประการตามที่ได้กล่าวไว้ในข้อ 3.1 แล้วนั้น ททท. จะต้องมีการประเมินผลกระทบการโอนข้อมูล (Transfer Impact Assessment) ตามหลักเกณฑ์ที่ EDPB กำหนดไว้ ซึ่งประกอบด้วย 6 ขั้นตอน อันได้แก่

1. พิจารณาลักษณะของกิจกรรมที่เกิดขึ้นเพื่อทำให้แน่ใจว่าจะมีการดำเนินการที่เป็นการโอนข้อมูลไปยังประเทศที่สาม จากนั้นจึงบันทึกรายละเอียดต่างๆ ของการโอนไว้ในแบบบันทึกรายการกิจกรรมการประมวลผลซึ่งเป็นภาระหน้าที่ของผู้ควบคุมและผู้ประมวลผลที่จะต้องจัดทำตาม GDPR มาตรา 30 เช่น วัตถุประสงค์ของการโอน องค์กรทั้งหมดที่เกี่ยวข้องกับการโอน สถานะขององค์กรที่เกี่ยวข้องกับการโอนว่าเป็นผู้ควบคุมหรือผู้ประมวลผล ประเทศปลายทางที่นำเข้าข้อมูล สถานที่ในการจัดเก็บข้อมูล ระยะเวลาในการจัดเก็บข้อมูล และระบุให้ชัดเจนว่าจะมีการโอนข้อมูลต่อไปยังประเทศอื่นๆ หรือไม่ นอกจากนั้นควรมีการประเมินว่าการโอนนั้นเป็นการดำเนินการภายใต้หลักการเท่าที่เพียงพอ เกี่ยวข้องและจำกัดเฉพาะเท่าที่จำเป็นตามวัตถุประสงค์ของการประมวลผลข้อมูลเท่านั้น

2. บ่งชี้เครื่องมือที่จะใช้ในการโอนข้อมูล เช่น เป็นการโอนภายใต้คำตัดสินรับรองระดับในการคุ้มครองข้อมูลที่เพียงพอของคณะกรรมาธิการยุโรปที่ออกให้กับประเทศดังกล่าว หรือเป็นการโอนภายใต้มาตรการป้องกันที่เหมาะสมตามมาตรา 46 แต่หากไม่สามารถโอนโดยใช้มาตรการดังกล่าวได้ จึงจะพิจารณาใช้เครื่องมือในการโอนเป็นกรณีการโอนภายใต้ข้อยกเว้นเฉพาะตามมาตรา 47 ซึ่งจะต้องปรับใช้อย่างจำกัด

3. ในกรณีที่เป็นการโอนภายใต้มาตรการป้องกันที่เหมาะสมตามมาตรา 46 จะต้องมีการประเมินว่าเครื่องมือที่จะใช้ในการโอนข้อมูลนั้นมีประสิทธิภาพสำหรับสถานการณ์ของการโอนนั้น โดยจะต้องพิจารณาจากประเด็นดังต่อไปนี้ 3.1. ความเป็นไปได้ในกรณีที่เจ้าหน้าที่ภาครัฐของประเทศที่สามจะเข้าถึงข้อมูลทั้งในกรณีที่อยู่ในความรับรู้และไม่อยู่ในความรับรู้ของผู้โอนข้อมูล 3.2. ความสอดคล้อง

ของหลักกฎหมายและแนวปฏิบัติเกี่ยวข้องกับการโอนข้อมูลของประเทศที่รับโอนข้อมูล เมื่อเทียบกับบทบัญญัติของ GDPR 3.3 ลักษณะของระบบกฎหมาย หลักพื้นฐานของกฎหมายรวมทั้งองค์กรที่ทำหน้าที่กำกับดูแลของประเทศที่รับโอนข้อมูลที่จะส่งผลกระทบต่อความมีประสิทธิภาพของเครื่องมือสำหรับเจ้าของข้อมูลในการเรียกร้องค่าชดเชยต่างๆ

4. เมื่อพิจารณาข้อเท็จจริงเป็นรายกรณีแล้วอาจพบได้ว่า ควรจะต้องมีการปรับใช้มาตรการเสริมเพิ่มเติมซึ่งเป็นมาตรการอื่นๆ นอกเหนือจากมาตรการป้องกันที่เหมาะสมตามมาตรา 46 เช่น มาตรการทางเทคนิค มาตรการขององค์กร หรือมาตรการเกี่ยวกับข้อตกลงหรือสัญญาต่างๆ เพื่อทำให้แน่ใจได้ว่าข้อมูลที่ถูกโอนไปยังประเทศที่สามจะได้รับความคุ้มครองในระดับที่เพียงพอเทียบเท่ากับระดับตามที่ได้รับการคุ้มครองตามบทบัญญัติของ GDPR หลักในการเลือกใช้มาตรการเสริมที่เหมาะสมให้พิจารณาจาก ประเภทของข้อมูล รูปแบบของข้อมูล จำนวนขององค์กรที่จะเข้ามาเกี่ยวข้องกับข้อมูล หลักกฎหมายหรือแนวปฏิบัติของประเทศที่สาม และความเป็นไปได้ที่ข้อมูลจะถูกโอนต่อไปยังประเทศอื่นๆ

5. เมื่อมีการบ่งชี้มาตรการป้องกันที่เหมาะสมตามมาตรา 46 ที่จะใช้เป็นเครื่องมือในการโอนข้อมูลแล้ว ก็จะต้องมีกระบวนการในการพิจารณาความมีประสิทธิภาพของมาตรการดังกล่าว ยกตัวอย่างเช่น การเลือกใช้ข้อสัญญามาตรฐาน (Standard Contractual Clauses - SCCs) ก็ต้องพิจารณาให้รอบคอบว่าจะไม่มีข้อสัญญาใดๆ ที่จะขัดหรือแย้งกับข้อสัญญามาตรฐานที่ได้รับการรับรองแล้วโดยคณะกรรมาธิการยุโรป และจะต้องไม่มีข้อสัญญาที่กำกวมซึ่งจะส่งผลกระทบต่อระดับในการให้ความคุ้มครองข้อมูลที่เพียงพอ แต่หากมีกรณีที่คู่สัญญาตกลงจะมีข้อสัญญาในลักษณะดังกล่าวก็จะต้องส่งเรื่องให้เจ้าหน้าที่ผู้ควบคุมที่มีอำนาจพิจารณาเพื่ออนุมัติก่อนการนำไปใช้

6. ทบทวนการประเมินตามกำหนดระยะเวลาที่เหมาะสม : ททท. ควรมีกระบวนการในการตรวจสอบและทบทวนการประเมินผลกระทบอย่างสม่ำเสมอ และควรมีเครื่องมือที่มีประสิทธิภาพที่จะใช้ในการระงับหรือการยกเลิกการโอนในกรณีที่ผู้รับโอนในประเทศที่สามไม่สามารถดำเนินการตามข้อตกลงที่ได้จัดทำระหว่างกันตามมาตรา 46 ได้ หรือกรณีที่มาตรการเสริมเพิ่มเติมไม่มีประสิทธิภาพเพียงพอที่จะสามารถใช้ในประเทศที่สามนั้นได้

นอกจากนั้น ททท. ควรจัดให้มีการอบรมพนักงานอย่างสม่ำเสมอ เพื่อให้พนักงานมีความรู้ความเข้าใจเกี่ยวกับแนวปฏิบัติดังกล่าว และยังถือเป็นการเปิดโอกาสให้พนักงานได้แสดงความคิดเห็นแลกเปลี่ยนประสบการณ์ในการดำเนินการตามแนวปฏิบัติดังกล่าว รวมทั้งนำเสนอประเด็นปัญหาต่างๆ ที่เกิดขึ้น และร่วมกันค้นหาแนวทางที่มีประสิทธิภาพในการแก้ไขปัญหาที่เกิดขึ้น ทั้งนี้ เพื่อทำให้แน่ใจว่าการดำเนินการตามแนวปฏิบัติดังกล่าวมีความเหมาะสมกับสถานการณ์ปัจจุบันและเป็นไปตามหลักกฎหมายที่อาจมีการแก้ไขเปลี่ยนแปลง

เอกสารอ้างอิง

ราชกิจจานุเบกษา. (2522). *พระราชบัญญัติการท่องเที่ยวแห่งประเทศไทย พ.ศ. 2522*. เล่ม 96 ตอนที่ 140 ก หน้า 1–11. http://www.ratchakitcha.soc.go.th/DATA/PDF/2522/A/140/1.PDF

_____. (2562). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. เล่ม 136 ตอนที่ 69 ก (27 พฤษภาคม 2562). http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

Article 29 Data Protection Working Party. (2018, April 11). *Recommendation on the standard application form for approval of processor Binding Corporate Rules for the transfer of personal data (17/EN WP265).* European Commission. https://ec.europa.eu/newsroom/article29/items/611236

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Data Protection Board. (2018, May 25). *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

_____. (2021, June 18). *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0).* https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

_____. (2022, February 22). *Guidelines 04/2021 on codes of conduct as tools for transfers – Version 2.0 (adopted after public consultation).* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042021-codes-conduct-tools-transfers-version_en

European Data Protection Board. (2023, February 14). *Guidelines 07/2022 on certification as a tool for transfers – Version 2.0.* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072022-certification-tool-transfers-version-20_en

_____. (2023, February 14). *Guidelines 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR – Version 2.0.* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3-and_en

_____. (2023, June 20). *Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR).* https://edpb.europa.eu/our-work-tools/ourdocuments/recommendations/recommendations-12022-application-approval-and-elements_en

European Data Protection Board & European Data Protection Supervisor. (2021). *EDPB - EDPS Joint Opinion 1/2021 on the European Commission's implementing decision on standard contractual clauses between controllers and processors for the matters referred to in Article 28(7) of Regulation (EU) 2016/679 and Article 29(7) of Regulation (EU) 2018/1725.* https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/edpb-edps-joint-opinion-12021-european-commissions_en

Federal Republic of Germany. (2017). *Bundesdatenschutzgesetz (Federal Data Protection Act – BDSG)*, as amended by the Act of 30 June 2017. Federal Law Gazette I, p. 2097. https://www.gesetze-im-internet.de/englisch_bdsg/

French Republic. (2018). *Act No. 2018-493 of 20 June 2018 on the protection of personal data.* Official Journal of the French Republic. https://www.legifrance.gouv.fr

Italian Republic. (2003). *Legislative Decree No. 196 of 30 June 2003: Personal Data Protection Code, as amended.* Gazzetta Ufficiale della Repubblica Italiana. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248

Kingdom of Sweden. (2018). *Lag (2018:218) med kompletterande bestämmelser till EU:sdataskyddsförordning (Dataskyddslagen).* Svensk författningssamling. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/dataskyddslag-2018218_sfs-2018-218