แนวทางการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในทวีปยุโรปสำหรับสำนักงานต่างประเทศของการท่องเที่ยวแห่งประเทศไทย[1]

GUIDELINES ON COMPLIANCE WITH EUROPEAN PERSONAL DATA PROTECTION LAWS FOR TOURISM AUTHORITY OF THAILAND (TAT) OVERSEAS OFFICES

อัญธิกา ณ พิบูลย์
Auntika Na Pibul
อาจารย์ประจำคณะ
นิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์: auntika.n@nida.ac.th
Lecturer
Graduate School of Law, National Institute of Development Administration
: auntika.n@nida.ac.th

Received : January 21, 2025
Revised : March 13, 2025
Accepted : March 26, 2024

บทคัดย่อ

การท่องเที่ยวแห่งประเทศไทย (ททท.) จัดตั้งสำนักงานต่างประเทศในทวีปยุโรปหลายสาขาเพื่อให้บรรลุวัตถุประสงค์ในการส่งเสริมการท่องเที่ยวไทย ซึ่ง ททท. แต่ละสำนักงานมีการดำเนินกิจกรรมที่มีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในประเทศในทวีปยุโรป จึงส่งผลให้สำนักงานดังกล่าวตกอยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศ บทความนี้มาจากการศึกษาวิจัยซึ่งมุ่งศึกษาลักษณะของกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดนและ ททท. สำนักงานลอนดอน สหราชอาณาจักร เพื่อจัดทำตารางแผนผังข้อมูลของแต่ละสำนักงาน และศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศส สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐอิตาลี ราชอาณาจักรสวีเดน และสหราชอาณาจักร เพื่อเสนอแนะแนวปฏิบัติที่เหมาะสมและมีประสิทธิภาพสำหรับแต่ละสำนักงานในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างถูกต้องและครบถ้วน ทั้งนี้ เพื่อเป็นการลดความเสี่ยงที่ ททท. จะมีความรับผิดและต้องรับโทษตามกฎหมายอันจะส่งผลให้เกิดความเสียหายต่อองค์กรและประเทศไทยต่อไป

[1] บทความเรียบเรียงขึ้นจากงานวิจัยเรื่อง ‘แนวทางการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในทวีปยุโรปสำหรับสำนักงานต่างประเทศของการท่องเที่ยวแห่งประเทศไทย’ ได้รับทุนสนับสนุนจากวิจัยจากการท่องเที่ยวแห่งประเทศไทย.

คำสำคัญ

การท่องเที่ยวแห่งประเทศไทย, กฎหมายคุ้มครองข้อมูลส่วนบุคคล, แนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล

ABSTRACT

The Tourism Authority of Thailand (TAT) has established several overseas offices across Europe to achieve its objective of promoting Thai tourism. Each TAT office engages in activities involving the processing of personal data of the data subjects residing in European countries, which means these offices are subject to each country's personal data protection laws. This article is based on research study that aims to examines the characteristics of personal data processing activities of the Tourism Authority of Thailand (TAT) in the Paris office (Republic of France), the Frankfurt office (Federal Republic of Germany), the Rome office (Republic of Italy), the Stockholm office (Kingdom of Sweden) and the London office (United Kingdom) with a view to creating data mapping for each office. Then, this research explores the personal data protection laws in France, Germany, Italy, Sweden, and the UK in order to provide the appropriate and effective practices for each office to ensure compliance with personal data protection laws, thereby reducing the risk of legal liability and penalties that could potentially have a negative impact on TAT and Thailand as a whole.

Keywords

The Tourism Authority of Thailand, Personal Data Protection Law, Guidelines on Personal Data Protection

1. บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

พระราชบัญญัติการท่องเที่ยวแห่งประเทศไทย พ.ศ. 2522 กำหนดให้การท่องเที่ยวแห่งประเทศไทย (ททท.) มีสถานะเป็นนิติบุคคลที่มีสำนักงานใหญ่ตั้งอยู่ในกรุงเทพมหานครหรือจังหวัดใกล้เคียง และสามารถจัดตั้งสำนักงานสาขาภายนอกราชอาณาจักรเมื่อได้รับอนุมัติจากรัฐมนตรีแล้ว ททท. จัดตั้งขึ้นโดยมีวัตถุประสงค์เพื่อส่งเสริมการท่องเที่ยวและอุตสาหกรรมท่องเที่ยวตลอดจนการประกอบอาชีพของคนไทยในอุตสาหกรรมท่องเที่ยว[2] ดังนั้น ททท. จึงจัดตั้งสำนักงานหลายแห่งในภูมิภาคเอเชียตะวันออก อาเซียน เอเชียใต้ แปซิฟิกใต้ ยุโรป แอฟริกา ตะวันออกกลาง และอเมริกา ซึ่งในการดำเนินกิจกรรมของแต่ละสำนักงานจะมีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในประเทศนั้นๆ จึงส่งผลให้ ททท. สำนักงานต่างประเทศอยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอันเป็นสถานที่ตั้งของสำนักงานนั้นๆ

ในกรณีสำนักงาน ททท. ที่ตั้งอยู่ในเขตสหภาพยุโรป (European Union (EU)) ซึ่งได้แก่ ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน ที่มีการประมวลผลข้อมูลส่วนบุคคลในบริบทของกิจกรรมของสถานที่ตั้งดังกล่าว ไม่ว่าการประมวลผลนั้นได้กระทำในหรือนอกสหภาพยุโรปก็ตาม สำนักงานดังกล่าวก็จะตกอยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปซึ่งมีชื่อว่า “ข้อกำหนดทั่วไปว่าด้วยการคุ้มครองข้อมูล” (General Data Protection Regulation) (ต่อไปจะเรียกว่า GDPR) มีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม 2561 เป็นต้นมา[3] สาระสำคัญของกฎหมายฉบับนี้ คือ การกำหนดภาระหน้าที่ในการปฏิบัติตามกฎหมายและกำหนดความรับผิดให้กับบุคคลหรือองค์กรที่เกี่ยวข้องกับประมวลผลข้อมูลส่วนบุคคลซึ่งแบ่งออกได้เป็นสองสถานะ คือ (1) ผู้ควบคุม (controller) ซึ่งเป็นผู้กำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูล และ (2) ผู้ประมวลผล (processor) ซึ่งเป็นผู้ประมวลผลข้อมูลในนามของผู้ควบคุมดังกล่าว[4] โดยหากฝ่าฝืนไม่ปฏิบัติตามก็จะต้องรับโทษปรับทางปกครอง และหากการกระทำดังกล่าวก่อให้เกิดความเสียหายก็จะต้องรับผิดทางแพ่งชดใช้ความเสียหายที่เกิดขึ้นให้กับผู้ที่ได้รับเสียหาย[5]

แต่อย่างไรก็ตาม แม้ว่าสำนักงานที่ตั้งอยู่ในประเทศที่อยู่ในสหภาพยุโรปจะอยู่ภายใต้บังคับที่จะต้องปฏิบัติตาม GDPR แต่ประเทศดังกล่าวอาจมีการกำหนดหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในที่มีรายละเอียดเฉพาะที่แตกต่างไปจากหลักเกณฑ์ตามที่ปรากฏในบทบัญญัติของ GDPR ก็ได้ นอกจากนั้น ททท. มีสำนักงานที่ตั้งอยู่ในลอนดอน สหราชอาณาจักร ซึ่งภายหลังจากที่สหราชอาณาจักรถอนตัวออกจากการเป็นสมาชิกของสหภาพยุโรปแล้ว สหราชอาณาจักรจะอยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายภายในที่ชื่อว่า UK General Data Protection Regulation (Regulation (EU) (2016/679) (ต่อไปจะเรียกว่า UK GDPR) และ Data Protection Act 2018 ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ ททท. จะต้องศึกษาเพิ่มเติมกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในของประเทศอันเป็นที่ตั้งของสำนักงาน ททท. ในทวีปยุโรป ซึ่งก็คือกฎหมายของสาธารณรัฐฝรั่งเศส สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐอิตาลี ราชอาณาจักรสวีเดน รวมทั้งกฎหมายของสหราชอาณาจักร โดยมีวัตถุประสงค์เพื่อกำหนดแนวปฏิบัติของแต่ละสำนักงานให้เป็นตามที่

---

[2] พระราชบัญญัติการท่องเที่ยวแห่งประเทศไทย พ.ศ. 2522 มาตรา 7-8.

[3] 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).

[4] GDPR article 4.

[5] GDPR article 82-83.

กฎหมายของแต่ละประเทศกำหนดไว้ได้อย่างถูกต้องและครบถ้วน ทั้งนี้ เพื่อเป็นการลดความเสี่ยงในกรณีที่ ททท. จะต้องรับผิดจากการไม่ปฏิบัติตามกฎหมาย ซึ่งจะส่งผลเสียต่อชื่อเสียงของ ททท. และประเทศไทยต่อไป

1.2 วัตถุประสงค์ของงานวิจัย

วัตถุประสงค์ของงานวิจัยนี้ คือ เพื่อศึกษากิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลของ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และททท. สำนักงานลอนดอน พร้อมทั้งศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศส สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐอิตาลี ราชอาณาจักรสวีเดน และสหราชอาณาจักร ซึ่งแต่ละสำนักงานอยู่ภายใต้บังคับที่จะต้องปฏิบัติตาม ทั้งนี้ เพื่อเสนอแนะแนวทางที่เหมาะสมและเป็นไปได้สำหรับแต่ละสำนักงานในการปฏิบัติตามกฎหมายดังกล่าวได้อย่างถูกต้องและครบถ้วน

1.3 ขอบเขตของงานวิจัย

งานวิจัยนี้มุ่งศึกษาแผนผังข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และททท. สำนักงานลอนดอน และศึกษาหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศส สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐอิตาลี ราชอาณาจักรสวีเดน และสหราชอาณาจักรที่เกี่ยวข้องกับการดำเนินกิจกรรมของ ททท. รวมทั้งศึกษาคำแนะนำและแนวทางปรับใช้กฎหมายดังกล่าวที่กำหนดไว้โดยหน่วยงานกำกับดูแลที่เกี่ยวข้อง

1.4 สมมติฐานของงานวิจัย

ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม ททท. สำนักงานลอนดอนมีการดำเนินกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล จึงอยู่ภายใต้บังคับที่จะต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศ ซึ่งมีการกำหนดหลักเกณฑ์ที่มีความแตกต่างกัน การที่แต่ละสำนักงานไม่มีแนวทางเฉพาะที่ชัดเจนสำหรับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศ อาจส่งผลให้แต่ละสำนักงานไม่สามารถปฏิบัติตามกฎหมายได้อย่างถูกต้องและครบถ้วน อันจะส่งผลให้เกิดความรับผิดและต้องรับโทษตามกฎหมายได้ ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ ททท. แต่ละสำนักงานดังกล่าวจะต้องกำหนดแนวปฏิบัติเฉพาะ เพื่อให้พนักงานและลูกจ้างของแต่ละสำนักงานสามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศได้อย่างถูกต้องและครบถ้วน ซึ่งจะส่งผลดีต่อขององค์กรและประเทศชาติต่อไป

1.5 วิธีการศึกษาวิจัย

งานวิจัยนี้ใช้วิธีการวิจัยเชิงเอกสาร (Documentary Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) ในส่วนของการวิจัยเชิงเอกสาร ผู้วิจัยมุ่งศึกษา 1) เอกสารขั้นปฐมภูมิ (primary document) ได้แก่ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศส สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐอิตาลี ราชอาณาจักรสวีเดน และสหราชอาณาจักร และ 2) เอกสารชั้นทุติยภูมิ (secondary document) ได้แก่ หนังสือ บทความในวารสารต่างประเทศ และคำแนะนำจากคณะทำงานด้านการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง เช่น Article 29 Data Protection Working Party (A29WP) [6], European Data Protection Board (EDPB)[7] และหน่วยงานกำกับดูแลด้านการ

[6] Article 29 Data Protection Working Party (A29WP) เป็นคณะทำงานของยุโรปที่จัดตั้งขึ้นตามความของ Article 29 ของ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ที่มีความเป็นอิสระในการทำหน้าที่ให้คำแนะนำในประเด็นต่างๆ ที่เกี่ยวข้องกับการคุ้มครองสิทธิความเป็นส่วนตัวและข้อมูลส่วนบุคคลให้กับสหภาพยุโรป (European Commission) คณะทำงานนี้ถูกแทนที่โดย European Data Protection BOARD (EDPB) ในวันที่ 25 พฤษภาคม 2561 ที่จัดตั้งขึ้นตามความของ GDPR article 68-76. See 'Legacy : Art. 29 Working Party' (EDPB) :< https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en>สืบค้นเมื่อ 11 พฤษภาคม 2567.

[7] European Data Protection BOARD (EDPB) มีเป้าหมายในการทำให้การปรับใช้และการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในเขตเศรษฐกิจยุโรป European Economic Area (EEA) มีความสอดคล้องกัน ผ่านการดำเนินภารกิจในด้านต่างๆ เช่น การกำหนด

คุ้มครองข้อมูลส่วนบุคคลของประเทศต่างๆ เช่น CNIL[8],BfDI[9], GPDP[10],IMY[11],UK Information Commissioner's Office (ICO)[12] เป็นต้น รวมทั้งข้อมูลจากเว็บไซต์ของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ในส่วนของการวิจัยเชิงคุณภาพ[13] ผู้วิจัยใช้แบบสอบถามและการสัมภาษณ์ บุคลากรของ ททท. แต่ละสำนักงาน เพื่อศึกษาลักษณะและวัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลของแต่ละฝ่ายงานของ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และททท. สำนักงานลอนดอน

1.6 ประโยชน์ที่คาดว่าจะได้รับ

ททท. สำนักงานปารีส สาธารณรัฐฝรั่งเศส ททท. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี ททท. สำนักงานโรม สาธารณรัฐอิตาลี ททท. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน และททท. สำนักงานลอนดอน สหราชอาณาจักร มีแนวทางในการปฏิบัติตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างถูกต้องและเหมาะสม ทั้งนี้ เพื่อเป็นการลดความเสี่ยงที่จะมีความรับผิดและต้องรับโทษตามกฎหมายอันจะส่งผลเสียต่อชื่อเสียงขององค์กรและประเทศไทยต่อไป

2. ตารางแผนผังข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของการท่องเที่ยวแห่งประเทศไทย สำนักงานต่างประเทศที่อยู่ในทวีปยุโรป

จากการศึกษาโครงสร้างขององค์กร หน้าที่ของแต่ละฝ่ายงานในองค์กร รวมทั้งการศึกษาข้อมูลที่ได้รับจากแบบสอบถามและการสัมภาษณ์ตัวแทนของบุคลากร ททท. แล้ว พบว่า ททท.สำนักงานปารีส ททท. สำนักงาน

แนวทาง ข้อเสนอแนะ แนวปฏิบัติที่ดี เพื่อสร้างความชัดเจนและความเข้าใจที่ตรงกันของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล รวมทั้งสนับสนุนการทำงานและร่วมมือกันกับ National Supervisory Authorities. See 'Tasks and Duties' (EDPB)< https://www.edpb.europa.eu/about-edpb/what-we-do/tasks-and-duties_en> สืบค้นเมื่อ 11 พฤษภาคม 2566..

[8] Commission nationale de l'informatique et des libertés (CNIL) คือ หน่วยงานอิสระของประเทศฝรั่งเศสที่จัดตั้งขึ้นในปี ค.ศ. 1978 โดยบทบัญญัติของกฎหมายคุ้มครองข้อมูลของฝรั่งเศส มีหน้าที่หลายประการที่เกี่ยวข้องกับการกำกับดูแลการบังคับใช้กฎหมายและระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูล เช่น GDPR และ the French Data Protection Act (Loi Informatique et Libertes) รวมทั้งกำหนดแนวปฏิบัติต่างๆ ที่เกี่ยวข้อง. See The CNIL's Missions (CNIL) <https://www.cnil.fr/en/cnil/cnils-missions> สืบค้นเมื่อ 11 พฤษภาคม 2566.

[9] The Federal Commission of Data Protection and Freedom of Information (BfDI) คือ หน่วยงานที่มีความเป็นอิสระของประเทศเยอรมนีซึ่งจัดตั้งขึ้นในปี ค.ศ. 1978 มีสถานะเป็นเจ้าหน้าที่สูงสุดของรัฐบาลกลางซึ่งมีหน้าที่หลายประการที่เกี่ยวข้องกับการกำกับดูแลการบังคับใช้กฎหมายและระเบียบที่เกี่ยวข้องกับการคุ้มครองข้อมูล เช่น GDPR และ the BDSG (Federal Data Protection Act) รวมทั้งการจัดการกับข้อร้องเรียนต่างๆ ของเจ้าของข้อมูลส่วนบุคคล. See 'Committee Work' (BfDI) <https://www.bfdi.bund.de/EN/Fachthemen/Gremienarbeit/Gremienarbeit_node.html> สืบค้นเมื่อ 11 พฤษภาคม 2566.

[10] GARANTE PER LA PROTERZIONE DEI DATI PERSONALI (GPDP) คือ องค์กรอิสระของประเทศอิตาลีซึ่งจัดตั้งขึ้นในปี ค.ศ. 1997 เพื่อทำหน้าที่คุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานซึ่งเชื่อมโยงกับการประมวลผลข้อมูลส่วนบุคคล และทำให้แน่ใจว่าศักดิ์ศรีของแต่ละบุคคลจะได้รับการเคารพ และยังมีฐานะเป็นเจ้าหน้าที่คุ้มครองข้อมูลของอิตาลีในการกำกับดูแลการบังคับใช้ GDPR และกฎหมายคุ้มครองข้อมูลของอิตาลี. See 'Contact Information' (GPDP) <https://www.garanteprivacy.it/web/garante-privacy-en>สืบค้นเมื่อ 11 พฤษภาคม 2566.

[11] SWEDISH Authority of Privacy Protection (IMY) คือ องค์กรที่ได้รับการแต่งตั้งจากรัฐบาลสวีเดนให้ทำหน้าที่เป็นเจ้าหน้าที่ผู้ควบคุมตามบทบัญญัติของ GDPR และกฎหมายคุ้มครองข้อมูลของสวีเดน รับผิดชอบในเรื่องของการให้คำแนะนำ ควบคุม ตรวจสอบและดูแลการปฏิบัติตามกฎหมาย. See 'Our Mission' (IMY) < https://www.imy.se/en/about-us/swedish-authority-for-privacy-protections-assignment/ > สืบค้นเมื่อ 11 พฤษภาคม 2566.

[12] Information Commissioner Officer (ICO) คือ หน่วยงานอิสระของสหราชอาณาจักร ทำหน้าที่กำกับดูแลในด้านการคุ้มครองข้อมูลและเสรีภาพทางด้านข้อมูลข่าวสารเพื่อประโยชน์สาธารณะ เป็นหน่วยงานหลักที่รับผิดชอบเกี่ยวกับการบังคับใช้ the Data Protection Act 2018 (DPA) and Freedom of Information Act 2000 (FOIA) และกฎหมายอื่นๆ ที่เกี่ยวข้อง. See 'About the ICO' < https://ico.org.uk/about-the-ico/> สืบค้นเมื่อ 11 พฤษภาคม 2566.

[13] ผ่านกระบวนการพิจารณาและรับรองโดยคณะกรรมการกลางพิจารณาจริยธรรมการวิจัยในมนุษย์ (Central Research Ethics Committee (CREC)) ก่อนดำเนินการเก็บข้อมูลเรียบร้อยแล้ว

แฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และ ททท. สำนักงานลอนดอน มีบุคลากรที่ปฏิบัติงานจำนวน 7-9 คน โดยจะมีผู้อำนวยการและรองผู้อำนวยงานเป็นหลักในการปฏิบัติหน้าที่เพื่อส่งเสริมการท่องเที่ยวไทยและเพื่อให้บรรลุเป้าหมายตามนโยบายและกลยุทธ์ของ ททท. ในแต่ละปี ซึ่งแต่ละสำนักงานจะมีการดำเนินกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่ค่อนข้างคล้ายกัน ดังต่อไปนี้[14]

กิจกรรม	วัตถุประสงค์	เจ้าของข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่เก็บรวบรวม	การเปิดเผยข้อมูลส่วนบุคคล	การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม
1. การเชิญผู้ประกอบการเข้าร่วมกิจกรรม Road Show	เพื่อให้ผู้ประกอบการไทยได้พบกับนักท่องเที่ยวและผู้ประกอบการต่างชาติ	นักท่องเที่ยว/ผู้ประกอบการที่เข้าร่วมงาน	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล สำเนาหนังสือเดินทาง	จัดทำฐานข้อมูลการติดต่อเพื่อเปิดเผยกับผู้เข้าร่วมงานในกิจกรรมเดียวกัน	ไม่มีการโอนข้อมูล
2. การจัดกิจกรรม FAM Trip	เพื่อให้ชาวต่างชาติได้รับประสบการณ์การท่องเที่ยวไทยและนำกลับไปประชาสัมพันธ์	สื่อมวลชน Influencer Blogger	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล สำเนาหนังสือเดินทาง ข้อมูลสุขภาพ	เปิดเผยแก่ผู้ให้บริการสายการบิน	โอนไปยัง ททท. สำนักงานใหญ่ และผู้ประกอบการที่พักในประเทศไทย
3. การรับลงทะเบียนเพื่อจัดฝึกอบรม e - learning	เพื่อจัดฝึกอบรม	ผู้เข้าร่วมฝึกอบรม	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	ไม่มีการเปิดเผยข้อมูล	ไม่มีการโอนข้อมูล
4.การถ่ายภาพและบันทึกวีดิโอ	เพื่อใช้การประชาสัมพันธ์	ผู้เข้าร่วมกิจกรรมต่างๆ	ภาพถ่าย วีดิโอ	เปิดเผยต่อสาธารณะ	ไม่มีการโอนข้อมูล
5.การรับสมัครสมาชิกทางเว็บไซต์และเก็บข้อมูลผู้ใช้งานบนเว็บไซต์	เพื่อใช้ในการจัดกิจกรรมและส่งข่าวสารในการส่งเสริมการท่องเที่ยว/ เพื่อ	ผู้เข้าร่วมกิจกรรมผ่านทางเว็บไซต์	ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ ข้อมูลคุกกี้ (cookie)	เปิดเผยแก่บริษัทผู้รับจ้างดูแลเว็บไซต์	ไม่มีการโอนข้อมูล

[14] การนำเสนอข้อมูลต่างๆในบทความนี้เป็นการนำเสนอข้อมูลในลักษณะภาพรวม เนื่องจากมีข้อจำกัดในเรื่องจำนวนหน้าของบทความและหน่วยงานผู้ให้ทุนสงวนสิทธิในการเปิดเผยข้อมูลบางส่วนเป็นการทั่วไป

กิจกรรม	วัตถุประสงค์	เจ้าของข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่เก็บรวบรวม	การเปิดเผยข้อมูลส่วนบุคคล	การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม
	ใช้ในการปรับปรุงประสิทธิภาพในการทำงานของเว็บไซต์				
6.การรับสมัครงาน	เพื่อรับสมัครงาน	ผู้สมัครงาน	ชื่อ นามสกุล ที่อยู่ อีเมล เบอร์โทรศัพท์ สำเนาหนังสือเดินทาง ภาพถ่าย วุฒิการศึกษา ประสบการณ์ทำงาน ข้อมูลผู้ติดต่อ ประวัติอาชญากรรม	ไม่มีการเปิดเผยข้อมูล	ไม่มีการโอนข้อมูล
7.การทำคำสั่งจ้าง/สัญญาจ้าง	เพื่อจ้างงาน	บุคลากร ททท.	ชื่อ นามสกุล อีเมล ที่อยู่ ภาพถ่าย เบอร์โทรศัพท์ สำเนาหนังสือเดินทาง เงินเดือน วุฒิการศึกษา	เปิดเผยแก่หน่วยงานที่เกี่ยวข้องกับการจัดสวัสดิการให้ลูกจ้าง	โอนไปยัง ททท. สำนักงานใหญ่

3. หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง

ในส่วนนี้ ผู้เขียนจะนำเสนอสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ซึ่งคือข้อกำหนดทั่วไปว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation (GDPR)) ซึ่ง ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม อยู่ภายใต้บังคับที่จะต้องปฏิบัติตาม และสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในของสาธารณรัฐฝรั่งเศส สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐอิตาลี ราชอาณาจักรสวีเดน โดยมุ่งนำเสนอเนื้อหาของกฎหมายที่มีความแตกต่างไปจากหลักเกณฑ์ตามที่ GDPR กำหนดไว้ และสุดท้ายจะนำเสนอสาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร ซึ่งสามารถสรุปได้ดังต่อไปนี้

3.1 ข้อกำหนดทั่วไปว่าด้วยการคุ้มครองข้อมูล (General Data Protection Regulation (GDPR))

GDPR เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ถูกบัญญัติขึ้นมาเพื่อแทนที่กฎหมายฉบับเดิมที่ชื่อว่า Directive 95/46/EC[15] โดยมีวัตถุประสงค์เพื่อทำให้การคุ้มครองสิทธิของเจ้าของข้อมูลส่วน

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the processing of personal data on the free movement of such data.

บุคคลมีความเข้มแข็งมากยิ่งขึ้นโดยการให้สิทธิกับเจ้าของข้อมูลในการควบคุมข้อมูลของตนเองได้มากขึ้น และสร้างมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกให้เป็นมาตรฐานเดียวกัน รวมทั้งทำให้หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลมีความทันสมัยมากขึ้นสอดคล้องกับการพัฒนาของเทคโนโลยี กฎหมายฉบับนี้จะเป็นเครื่องมือในการสนับสนุนให้เกิดการเคลื่อนไหวของข้อมูลส่วนบุคคลได้อย่างอิสระในสหภาพยุโรปเพื่อลดอุปสรรคในการดำเนินธุรกิจ โดย GDPR มีผลบังคับใช้ตั้งแต่ในวันที่ 25 พฤษภาคม 2561 เป็นต้นมา โดยมีคณะกรรมาธิการคุ้มครองข้อมูลส่วนบุคคลของยุโรป (European Data Protection Board (EDPB)) ซึ่งจัดตั้งขึ้นตาม GDPR Article 68 เพื่อทำหน้าที่ควบคุมดูแลการปรับใช้กฎหมาย สาระสำคัญโดยสรุปของ GDPR ในส่วนที่เกี่ยวข้องกับการดำเนินกิจกรรมของททท. มีรายละเอียดดังต่อไปนี้

3.1.1 ขอบเขตในการบังคับใช้กฎหมาย

GDPR กำหนดขอบเขตการบังคับใช้เชิงเนื้อหาไว้ว่า ลักษณะของกิจกรรมที่อยู่ภายใต้บังคับของ GDPR คือ การประมวลผลข้อมูลส่วนบุคคลทั้งหมดหรือบางส่วนด้วยวิธีการอัตโนมัติและกระบวนการประมวลผลอื่นนอกเหนือจากวิธีอัตโนมัติกับข้อมูลส่วนบุคคลซึ่งประกอบเป็นส่วนหนึ่งของระบบแฟ้มข้อมูลหรือตั้งใจจะประกอบเป็นส่วนหนึ่งของระบบแฟ้มข้อมูล[16] โดย GDPR จะไม่ใช้บังคับกับการประมวลผลข้อมูลในบางกรณี เช่น การประมวลผลข้อมูลส่วนบุคคลโดยบุคคลธรรมดาเพื่อกิจกรรมส่วนตัวหรือภายในครัวเรือนเท่านั้น ฯลฯ[17]

GDPR กำหนดขอบเขตการบังคับใช้เชิงพื้นที่ไว้ว่า จะบังคับใช้ในกรณี “1. การประมวลผลข้อมูลส่วนบุคคลในบริบทของกิจกรรมของสถานที่ตั้งของผู้ควบคุมหรือผู้ประมวลผลซึ่งอยู่ในสหภาพยุโรป ไม่ว่าการประมวลผลนั้นได้กระทำในหรือนอกสหภาพยุโรปก็ตาม และ 2. การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่อยู่ในสหภาพยุโรปโดยที่ผู้ควบคุมหรือผู้ประมวลผลมิได้อยู่ในสหภาพยุโรป เมื่อกิจกรรมการประมวลผลนั้นเกี่ยวข้องกับ (a) การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลซึ่งอยู่ในสหภาพยุโรป โดยไม่คำนึงว่าจะมีการชำระเงินโดยเจ้าของข้อมูลหรือไม่ (b) การติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในสหภาพยุโรป[18]

3.1.2 บทนิยามศัพท์

GDPR ให้ความหมายของคำว่า ‘*ข้อมูลส่วนบุคคล*’ ไว้ว่า หมายถึง “ข้อมูลใด ๆ ที่เกี่ยวกับบุคคลธรรมดาที่ถูกระบุหรือสามารถระบุอัตลักษณ์ได้ (‘เจ้าของข้อมูลส่วนบุคคล’) บุคคลธรรมดาที่สามารถถูกระบุอัตลักษณ์ได้ คือ บุคคลที่สามารถถูกระบุอัตลักษณ์ได้ไม่ว่าโดยตรงหรือโดยอ้อมโดยเฉพาะอย่างยิ่งด้วยการอ้างอิงจากสิ่งที่ระบุอัตลักษณ์เป็นการเฉพาะ เช่น ชื่อ หมายเลขประจำตัว ข้อมูลที่แสดงถึงสถานที่ตั้ง สิ่งที่ระบุอัตลักษณ์ออนไลน์หรือปัจจัยประการหนึ่งหรือหรือหลายประการที่เจาะจงไปยังอัตลักษณ์ทางกายภาพสรีรวิทยา พันธุกรรม จิตใจ เศรษฐกิจ วัฒนธรรม หรืออัตลักษณ์ทางสังคมของบุคคลดังกล่าว”[19] และอธิบายลักษณะของ ‘*ข้อมูลส่วนบุคคลชนิดพิเศษ*’ ไว้ว่าคือ “ข้อมูลส่วนบุคคลที่เปิดเผยต้นกำเนิดทางเชื้อชาติและชาติพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนาหรือปรัชญา หรือการเป็นสมาชิกสหภาพวิชาชีพ และการประมวลข้อมูลพันธุกรรม ข้อมูลชีวภาพเพื่อวัตถุประสงค์ในการระบุอัตลักษณ์บุคคลธรรมดาอย่างเฉพาะเจาะจง ข้อมูลเกี่ยวข้องกับสุขภาพหรือข้อมูลเกี่ยวกับชีวิตทางเพศหรือพฤติกรรมทางเพศของบุคคลธรรมดา[20] GDPR ให้ความหมายของคำว่า “*ประมวลผล*” ไว้ว่า หมายถึง “การกระทำใดๆ ต่อข้อมูลส่วนบุคคล ไม่ว่าจะด้วยวิธีการโดยอัติโนมัติ หรือไม่ก็ตาม อาทิเช่น การรวบรวม การบันทึก การจัดระบบ การวางโครงสร้าง การเก็บ การปรับปรุง การเปลี่ยนแปลง การกู้คืน การจัดตำแหน่ง การผสมรวม การใช้ การเปิดเผยโดยการโอน การจ่ายแจก หรือกระทำการอื่นใดที่ทำให้ข้อมูลมีการแพร่หลาย การรวบรวม การจำกัด การลบ หรือการทำลาย”[21] โดยกำหนดสถานะของผู้ที่เกี่ยวข้องกับการ

[16] GDPR article 2.

[17] GDPR article 2 para 2.

[18] GDPR article 3.

[19] GDPR article 4 (1).

[20] GDPR article 9.

[21] GDPR article 4 (2).

ประมวลผล คือ (1) *"ผู้ควบคุม"* หมายถึง"บุคคลหรือนิติบุคคล หน่วยงานภาครัฐ ตัวแทนหรือองค์กรอื่นใด โดยลำพังหรือร่วมกันกำหนดวัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่วัตถุประสงค์และวิธีการประมวลผลข้อมูลส่วนบุคคลดังกล่าวถูกกำหนดโดยกฎหมายของสหภาพยุโรปหรือของประเทศสมาชิก ผู้ควบคุมหรือเกณฑ์เฉพาะสำหรับการแต่งตั้งตัวแทนผู้ควบคุมอาจถูกกำหนดไว้โดยกฎหมายของสหภาพยุโรปหรือกฎหมายของประเทศสมาชิกนั้น"[22] และ (2) "ผู้ประมวลผล" หมายถึง "บุคคลหรือนิติบุคคล หน่วยงานภาครัฐ ตัวแทนหรือองค์กรอื่นใด ซึ่งประมวลผลข้อมูลส่วนบุคคลในนามของผู้ควบคุม"[23] และ (3) "ผู้ควบคุมร่วม" ซึ่ง GDPR อธิบายลักษณะไว้ว่าคือ "ผู้ควบคุมจำนวนตั้งแต่สองรายขึ้นไปซึ่งร่วมกันกำหนดวัตถุประสงค์และวิธีการในประมวลผล"[24]

3.1.3 ภาระหน้าที่ของผู้ควบคุมและผู้ประมวลผล

GDPR กำหนดให้ "ผู้ควบคุม"มีหน้าที่ดำเนินการต่างๆ เช่น การประมวลผลให้เป็นไปตามหลักการประมวลผลข้อมูลส่วนบุคคลตาม Article 5 (เช่น หลักความชอบด้วยกฎหมาย ความเป็นธรรม ความโปร่งใส)และต้องสามารถแสดงให้เห็นได้ว่ามีการปฏิบัติตามหลักการดังกล่าวแล้ว[25] และกำหนดให้ "ผู้ควบคุมร่วม" จะต้องกำหนดหน้าที่ในการปฏิบัติตามกฎหมายสำหรับผู้ควบคุมร่วมแต่ละรายโดยเฉพาะอย่างยิ่งในประเด็นที่เกี่ยวข้องกับการใช้สิทธิของเจ้าของข้อมูลและการแจ้งข้อมูลต่างๆ แก่เจ้าของข้อมูล รวมทั้งการแจ้งช่องทางการติดต่อผู้ควบคุมแต่ละรายให้เจ้าของข้อมูลทราบ[26] GDPR กำหนดให้ผู้ควบคุมมีหน้าที่จะต้องดำเนินการตามคำร้องขอใช้สิทธิของเจ้าของข้อมูลโดยไม่ล่าช้าภายใน 30 วันนับแต่วันที่ได้รับคำร้อง โดย GDPR รับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลไว้หลายประการ เช่น สิทธิในการเข้าถึงข้อมูล สิทธิในการแก้ไขข้อมูล สิทธิในการลบข้อมูล ฯลฯ[27] GDPR กำหนดให้ "ผู้ประมวล" มีหน้าที่ดำเนินการต่างๆ เช่น การปรับใช้มาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมในลักษณะที่ทำให้การประมวลผลข้อมูลเป็นไปตามเงื่อนไขที่กฎหมายกำหนดและทำให้แน่ใจว่ามีการคุ้มครองสิทธิของเจ้าของข้อมูล รวมทั้งการที่จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรเป็นการเฉพาะหรือเป็นการทั่วไปจากผู้ควบคุมก่อนการติดต่อกับผู้ประมวลผลรายอื่นฯลฯ[28]

นอกจากนั้น ผู้ควบคุมและผู้ประมวลผลมีหน้าที่ในการประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment (DPIA)) เมื่อประเภทของการประมวลผลดำเนินการโดยใช้เทคโนโลยีใหม่ และเมื่อพิจารณาร่วมกันกับลักษณะ ขอบเขต บริบทและวัตถุประสงค์ของการประมวลผลแล้วพบว่ามีแนวโน้มที่จะส่งผลให้เกิดความเสี่ยงในระดับสูงต่อสิทธิเสรีภาพของบุคคลธรรมดา โดยเฉพาะในกรณีดังต่อไปนี้ (1) เมื่อมีการประเมินแง่มุมส่วนบุคคลต่างๆ อย่างเป็นระบบและเข้มข้นโดยสัมพันธ์กับบุคคลธรรมดาซึ่งเกิดจากการประมวลผลอัตโนมัติอันรวมถึงการทำโปรไฟล์และมีการตัดสินใจจากการประเมินดังกล่าวซึ่งส่งผลกระทบทางกฎหมายที่เกี่ยวข้องกับบุคคลธรรมดาหรือส่งผลกระทบอย่างมีนัยสำคัญเช่นเดียวกันกับบุคคลธรรมดา หรือ (2) เมื่อมีการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลที่สัมพันธ์กับการตัดสินโทษและความผิดทางอาญาเป็นจำนวนมาก หรือ(3) เมื่อมีการกำกับควบคุมอย่างเป็นระบบขนาดใหญ่กับบริเวณที่สามารถเข้าถึงได้โดยทั่วไป[29] รวมทั้งผู้ควบคุมและผู้ประมวลผลมีหน้าที่กำหนดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หาก (1) การประมวลผลดำเนินการโดยเจ้าหน้าที่หรือหน่วยงานสาธารณะ หรือ (2) กิจกรรมหลักของผู้ควบคุมหรือผู้ประมวลผลประกอบด้วยการประมวลผลที่จำเป็นต้องมีการควบคุมข้อมูลขนาดใหญ่อย่างสม่ำเสมอและเป็นระบบ หรือ (3)

[22] GDPR article 4 (7).

[23] GDPR article 4 (8).

[24] GDPR article 26.

[25] GDPR article 24.

[26] GDPR article 26.

[27] GDPR article 12-23.

[28] GDPR article 28.

[29] GDPR article 35.

กิจกรรมหลักของผู้ควบคุมหรือผู้ประมวลผลประกอบด้วยการประมวลผลขนาดใหญ่ซึ่งข้อมูลส่วนบุคคลชนิดพิเศษ ตาม Article 9 และข้อมูลที่มีความเกี่ยวพันกับการตัดสินและความผิดทางอาญาตาม Article 10[30]

3.1.4 ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลชนิดพิเศษ

GDPR กำหนดหลักเกณฑ์การประมวลผลข้อมูลส่วนบุคคลไว้ว่า ควรดำเนินการภายใต้หลักความชอบด้วยกฎหมาย ความเป็นธรรม ความโปร่งใส หลักการกำหนดขอบเขตของวัตถุประสงค์ หลักการใช้ข้อมูลให้น้อยที่สุด หลักความแม่นยำ หลักการกำหนดขอบเขตการเก็บรักษา หลักความสมบูรณ์และเป็นความลับ หลักความรับผิดชอบและสามารถตรวจสอบได้[31] ซึ่งการประมวลข้อมูลส่วนบุคคลที่ชอบด้วยกฎหมายจะต้องดำเนินการภายใต้ฐานทางกฎหมายที่กำหนดไว้ เช่น เจ้าของข้อมูลให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนเพื่อวัตถุประสงค์เฉพาะอย่างหนึ่งหรือมากกว่า หรือ การประมวลผลจำเป็นสำหรับการปฏิบัติตามสัญญาที่เจ้าของข้อมูลเป็นคู่สัญญาหรือเพื่อให้เป็นตามขั้นตอนที่เจ้าของข้อมูลร้องขอก่อนทำสัญญา ฯลฯ[32]

เมื่อการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษ GDPR กำหนดไว้ว่าสามารถดำเนินการได้ภายใต้ฐานทางกฎหมายที่กำหนดไว้ เช่น เจ้าของข้อมูลให้ความยินยอมอย่างชัดแจ้งในการประมวลผลข้อมูลของตนเพื่อวัตถุประสงค์เฉพาะอย่างหนึ่งหรือมากกว่า หรือ การประมวลผลข้อมูลจำเป็นต่อวัตถุประสงค์ในการปฏิบัติตามพันธกรณีและใช้สิทธิบางประการของผู้ควบคุมหรือเจ้าของข้อมูลในด้านที่เกี่ยวกับกฎหมายการจ้างงาน หรือ การประมวลผลข้อมูลจำเป็นต่อวัตถุประสงค์ด้านเวชศาสตร์ป้องกันหรือเวชศาสตร์โรคจากการทำงาน เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรค การจัดหาบริการสาธารณสุขและสังคมหรือการรักษาหรือจัดการระบบและบริการสาธารณสุขและสังคมตามหลักของกฎหมาย[33]

ในกรณีที่การประมวลผลอยู่บนฐานความยินยอม GDPR กำหนดไว้ว่า ผู้ควบคุมจะต้องสามารถแสดงเห็นได้ว่าเจ้าของข้อมูลให้ความยินยอมสำหรับการประมวลผลข้อมูลส่วนบุคคลของของตน ซึ่งในกรณีที่เจ้าของข้อมูลให้ความยินยอมในรูปแบบของลายลักษณ์อักษร การร้องขอความยินยอมควรจะนำเสนอในลักษณะที่แยกเฉพาะจากเรื่องอื่นๆ ในรูปแบบที่เข้าใจได้และเข้าถึงได้ง่าย ใช้ภาษาที่ชัดเจนและไม่ซับซ้อน และแจ้งให้เจ้าของข้อมูลทราบก่อนการให้ความยินยอมว่า มีสิทธิในการถอนความยินยอมเมื่อใดก็ได้ โดยจะไม่กระทบต่อการประมวลผลข้อมูลที่ชอบด้วยกฎหมายบนฐานของความยินยอมที่เกิดขึ้นก่อนการถอนความยินยอม[34] ในกรณีที่ต้องมีการขอความยินยอมจากผู้เยาว์ เช่น หากเป็นการประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์ที่อายุต่ำกว่า 16 ปี ที่เกี่ยวข้องกับการเสนอบริการสารสนเทศ[35] การประมวลผลข้อมูลดังกล่าวจะชอบด้วยกฎหมายก็ต่อเมื่อได้รับความยินยอมจากผู้แทนโดยชอบธรรมของผู้เยาว์[36]

3.1.5 การโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม

GDPR กำหนดหลักเกณฑ์ที่ค่อนข้างเข้มงวดในการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม (ประเทศนอกเขตเศรษฐกิจยุโรป (European Economic Area(EEA)) ซึ่งก็คือประเทศที่อยู่นอกเขตของประเทศสมาชิกสหภาพยุโรป 27 ประเทศและประเทศไอซ์แลนด์ นอร์เวย์ ลิกเตนสไตน์)) ทั้งนี้ เพื่อเป็นการทำให้แน่ใจว่าระดับ

---

[30] GDPR article 37.

[31] GDPR article 5.

[32] GDPR article 6.

[33] GDPR article 9.

[34] GDPR article 7.

[35] GDPR Article 6 (25) กำหนดบทนิยามศัพท์ของคำว่า “information society service” (บริการสารสนเทศ) ไว้ว่าให้มีความหมายตามที่ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services กำหนดไว้ ซึ่ง Directive (EU) 2015/1535 Article 1(b) ให้ความหมายของ “information society service” ไว้ว่า หมายถึงบริการทั้งหมดที่เสนอด้วยวิธีการทางอิเล็กทรอนิกส์ตามที่ผู้ใช้บริการแต่ละคนร้องขอเพื่อให้ได้รับค่าตอบแทน ซึ่งก็คือบริการที่นำเสนอทางออนไลน์ทั้งหมด

[36] GDPR article 8.

การคุ้มครองข้อมูลที่ได้รับการรับรองโดย GDPR จะยังคงมีอยู่ โดย GDPR กำหนดเงื่อนไขที่ผู้ควบคุมและผู้ประมวลผลสามารถโอนข้อมูลส่วนบุคคลในกรณีดังกล่าวได้ ภายใต้เงื่อนไขดังต่อไปนี้

1 เป็นการโอนภายใต้คำตัดสินที่รับรองความเพียงพอ (Adequacy Decision)

ภายหลังจากที่คณะกรรมาธิการยุโรปได้ประเมินระดับการคุ้มครองที่เพียงพอจากองค์ประกอบต่างๆ เช่น การมีอยู่และการปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพของหน่วยงานกำกับดูแล ฯลฯ แล้ว คณะกรรมาธิการยุโรปอาจออกคำตัดสินรับรองความเพียงพอให้กับประเทศที่สามที่มีระดับในการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอเทียบเท่ากับ GDPR จึงส่งผลให้ข้อมูลส่วนบุคคลสามารถถูกโอนยังประเทศเหล่านั้นได้อย่างเสรี แต่จะต้องมีกลไกในการทบทวนระดับความเพียงพออย่างน้อยทุกๆ สี่ปี[37]

2 เป็นการโอนภายใต้มาตรการป้องกันที่เหมาะสม (Appropriate Safeguards)

ในกรณีที่จะมีการโอนข้อมูลไปยังประเทศที่ไม่มีคำตัดสินรับรองความเพียงพอ การโอนข้อมูลสามารถทำได้หากมีการใช้มาตรการป้องกันที่เหมาะสม และอยู่ภายใต้เงื่อนไขของการมีอยู่ของการบังคับใช้สิทธิของเจ้าของข้อมูลและการเยียวยาทางกฎหมายที่มีประสิทธิภาพให้กับเจ้าของข้อมูล ยกตัวอย่างเช่น เป็นการโอนภายใต้ข้อสัญญามาตรฐาน (Standard Contractual Clauses - SCCs) หรือ นโยบายการคุ้มครองข้อมูลในเครือกิจการหรือเครือธุรกิจเดียวกัน (Binding Corporate Rules - BCRs) เป็นต้น[38]

3 เป็นการโอนภายใต้ข้อยกเว้นเฉพาะ (Derogations for Specific Situations)

ในกรณีที่ไม่มีคำตัดสินที่รับรองความเพียงพอ และไม่มีมาตรการป้องกันที่เหมาะสม GDPR กำหนดไว้ว่าการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สามสามารถทำได้หากอยู่ภายใต้ข้อยกเว้นเฉพาะบางประการ เช่น ได้รับการยินยอมจากเจ้าของข้อมูลอย่างชัดเจนภายหลังจากได้รับแจ้งความเสี่ยงที่อาจเกิดขึ้นจากการโอนดังกล่าว หรือการโอนข้อมูลเป็นสิ่งจำเป็นเพื่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุม เป็นต้น[39]

3.1.6 การเยียวยา ความรับผิดและโทษ

GDPR กำหนดสิทธิในการได้รับการชดเชยและความรับผิดไว้ว่า “บุคคลใดก็ตามที่ได้รับความเสียหายทางวัตถุหรือความเสียหายที่ไม่ใช่ทางวัตถุอันเป็นผลจากการละเมิดบทบัญญัติจะต้องมีสิทธิได้รับการชดเชยจากผู้ควบคุมหรือผู้ประมวลผลจากความเสียหายที่ได้รับ”[40] และกำหนดค่าปรับทางปกครองไว้สำหรับกรณีมีการละเมิดบทบัญญัติต่างๆ ซึ่งแบ่งออกเป็น (1) กำหนดจำนวนค่าปรับทางปกครองไม่เกิน 10,000,000 ยูโรหรือในกรณีของวิสาหกิจคือไม่เกินร้อยละ 2 ของยอดเงินหมุนเวียนทั่วโลกตลอดปีงบประมาณก่อนหน้า แล้วแต่ว่าสิ่งใดมีมูลค่าสูงกว่า สำหรับการละเมิดบทบัญญัติต่างๆ เช่น กรณีที่ผู้ควบคุมและผู้ประมวลผลไม่จัดให้มีมาตรการทางเทคนิคและมาตรการขององค์กรที่เหมาะสมเพื่อทำให้แน่ใจถึงระดับการรักษาความปลอดภัยที่เหมาะสมสำหรับความเสี่ยง ฯลฯ และ (2) กำหนดจำนวนค่าปรับทางปกครองไม่เกิน 20,000,000 ยูโร หรือในกรณีของวิสาหกิจคือไม่เกินร้อยละ 4 ของยอดเงินหมุนเวียนทั่วโลกตลอดปีงบประมาณก่อนหน้า แล้วแต่ว่าสิ่งใดมีมูลค่าสูงกว่า สำหรับกรณีการละเมิดบทบัญญัติ เช่น การไม่ปฏิบัติตามเงื่อนไขในเรื่องความยินยอมตาม Article 7 ฯลฯ[41]

3.2 หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศส

กฎหมายหลักที่เกี่ยวข้องกับการคุ้มครองข้อมูลของสาธารณรัฐฝรั่งเศส คือ Loi n° 2018-493 du 20 juin 2018relative à la protection des données personnelles (ซึ่งมีชื่อภาษาอังกฤษว่า No. 2018-493 of 20 June 2018 on Personal Data Protection (DPA)) มีเนื้อหาในลักษณะที่เป็นการนำเอาบทบัญญัติของ GDPR มาปรับใช้เพิ่มเติมกับกฎหมายที่บังคับใช้อยู่ก่อนแล้วซึ่งก็คือ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ซึ่งมีชื่อภาษาอังกฤษว่า Act No. 78-17 of 6 January 1978

[37] GDPR article 45.

[38] GDPR article 46.

[39] GDPR article 49.

[40] GDPR article 82.

[41] GDPR article 83.

on Information Technology, Data Files and Civil Liberties) และเพื่อให้เกิดความชัดเจนยิ่งขึ้นสาธารณรัฐฝรั่งเศส ได้ออกกฤษฎีกา Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personne (ซึ่งมีชื่อภาษาอังกฤษว่า Ordinance No. 2018-1125 of 12 December 2018) ขึ้นมาเพื่อแก้ไขเพิ่มเติมและยกเลิกบทบัญญัติบางข้อที่ขัดแย้งกับ GDPR ซึ่งมีผลบังคับใช้บังคับตั้งแต่วันที่ 1 มิถุนายน 2019 เป็นต้นมา ในส่วนของการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการทำการโฆษณาและการทำการตลาดแบบตรงนั้นจะอยู่ภายใต้บังคับของ Postal and Electronic Communications Code (*Articles L.34 et seq and Articles R.10 et seq*) นอกจากนั้น CNIL ได้กำหนดข้อแนะนำและแนวทางเกี่ยวกับการใช้งานคุกกี้ไว้เป็นการเฉพาะ[42]

หน่วยงานกำกับดูแลในการปฏิบัติตามกฎหมายในประเทศคุ้มครองข้อมูลของฝรั่งเศส คือ Commission Nationale de l'Informatique et des Libertés (CNIL) เป็นหน่วยงานกำกับดูแลระดับชาติที่เป็นอิสระ ประกอบด้วยกรรมการจำนวน 18 คน ภารกิจหลักของ CNIL คือการควบคุมและตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลและกำหนดบทลงโทษในกรณีที่ไม่สามารถเยียวยาการละเมิดได้ นอกจากนั้น CNIL มีสิทธิในการขอเข้าไปยังสถานที่และตรวจสอบการปฏิบัติตามกฎหมาย เมื่อสิ้นสุดกระบวนการตรวจสอบแล้ว CNIL จะร่างรายงานการตรวจสอบ และเมื่อพบว่ามีการละเมิดอย่างร้ายแรง CNIL สามารถกำหนดบทลงโทษได้ ในส่วนของการพัฒนากฎเกณฑ์ต่าง ๆ นั้น CNIL มีอำนาจในการปรับปรุงหรือส่งเสริมการพัฒนาเครื่องมือในทางกฎหมายใหม่ ๆ เช่น แนวทาง คำแนะนำ จรรยาบรรณ ข้อบังคับต้นแบบ วิธีการอ้างอิงสำหรับการประมวลผลข้อมูลด้านสุขภาพ กลไกการรับรอง ฯลฯ

สาระสำคัญโดยสรุปของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐฝรั่งเศสที่เกี่ยวข้องกับการดำเนินกิจกรรมของ ททท. สำนักงานปารีส ซึ่งมีรายละเอียดเพิ่มเติมหรือแตกต่างไปจากที่ GDPR กำหนดไว้ มีรายละเอียดดังต่อไปนี้

เรื่อง	หลักกฎหมาย
1. การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์	-ในกรณีที่มีการเสนอบริการสารสนเทศ (เสนอสินค้าและบริการโดยใช้อุปกรณ์อิเล็กทรอนิกส์ในการประมวลผลและเก็บข้อมูลของผู้รับบริการ (information society)) แก่ผู้เยาว์ที่อาศัยอยู่ในสหพันธ์สาธารณรัฐฝรั่งเศส ผู้เยาว์สามารถให้ความยินยอมอย่างมีผลสมบูรณ์ตามกฎหมายเมื่อมีอายุอย่างน้อย 15 ปี แต่หากมีอายุน้อยกว่า 15 ปี จะต้องได้รับความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์
2. การประมวลผลข้อมูลส่วนบุคคลของลูกจ้าง	- การประมวลผลข้อมูลของลูกจ้างหรือที่เกี่ยวกับข้อมูลไบโอเมตริกซ์สามารถดำเนินการได้เมื่อมีความจำเป็นอย่างยิ่งในการควบคุมการเข้างานหรือการใช้เครื่องมือโปรแกรมทรัพยากรคอมพิวเตอร์ต่างๆ เท่านั้น (DPA, Article 27)
3. การประมวลผลข้อมูลเลขประจำตัวประชาชน	-การประมวลผลข้อมูลเลขประจำตัวประชาชน (Personal Identification Number (PIN) in the National Register of Individual Identification (RNIPP) สามารถดำเนินการได้เฉพาะเพื่อวัตถุประสงค์ที่กฎหมายกำหนดไว้เท่านั้น ซึ่งส่วนใหญ่จะ

[42] Deliberation No. 2020-091 of September 17, 2020 adopting guidelines on the application of Article 82 of the amended Law of January 6, 1978 to operations of reading and writing on a user's terminal (notably concerning "cookies and other trackers") and repealing Deliberation No. 2019-093 of July 4, 2019.

เรื่อง	หลักกฎหมาย
	เป็นไปเพื่อวัตถุประสงค์ทางด้านการดูแลสุขภาพ และการให้ความดูแลทางด้านสังคมแก่เจ้าของข้อมูล[43] (DPA, Article 22)
4. ข้อยกเว้นภาระหน้าที่ของผู้ควบคุมในการแจ้งเจ้าของข้อมูลในกรณีที่มีการละเมิดข้อมูล	-ข้อยกเว้นสำหรับภาระหน้าที่ของผู้ควบคุมในการแจ้งเจ้าของข้อมูลเมื่อมีการละเมิดข้อมูลในกรณีที่เป็นไปได้ว่าจะส่งผลให้เกิดความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล คือ กรณีที่มีการประมวลผลข้อมูลที่สามารถบ่งชี้ตัวบุคคลได้ไม่ว่าโดยทางตรงหรือทางอ้อมซึ่งบุคคลดังกล่าวได้รับการคุ้มครองตามภายใต้ Article 39 sexies ของ Press Freedom Act of the French Republic (1881, as amended 2014) หรือกรณีที่มีการประมวลผลข้อมูลเกี่ยวกับการบริหารจัดการ ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับสุขภาพซึ่งหากมีการเปิดเผยแล้วจะส่งให้เกิดความเสี่ยงต่อความปลอดภัยของประเทศหรือความปลอดภัยของสาธารณะ เนื่องจากปริมาณของข้อมูลที่ถูกละเมิดหรือเนื้อหาของข้อมูลที่ความเป็นส่วนตัว[44]
5. ภาระหน้าที่ในการใช้ภาษาฝรั่งเศสสำหรับการสื่อสาร	-องค์กรต่างๆ ที่ดำเนินธุรกิจหรือติดต่อกับลูกค้าหรือลูกจ้างที่อยู่ในสาธารณรัฐฝรั่งเศสมีภาระหน้าที่ทั่วไปภายใต้กฎหมายของสาธารณรัฐฝรั่งเศสที่จะต้องใช้ภาษาฝรั่งเศสในการดำเนินการดังกล่าว (law 94-665 of 4 August 1994 relating to usage of the French language (the Toubon Law))
6. การใช้งานคุกกี้	-องค์กรสามารถเก็บข้อมูลคุกกี้ได้เมื่อได้รับความยินยอมจากผู้ใช้งานเรียบร้อยแล้ว โดยจะต้องมีป้ายแจ้งเตือนรายละเอียดเกี่ยวกับคุกกี้ที่ใช้งานรวมทั้งจัดให้มีช่องทางและแจ้งวิธีการในการยกเลิกคุกกี้รวมทั้งผลที่อาจเกิดขึ้นเมื่อมีการยกเลิกไว้ด้วย CNIL กำหนดไว้ว่าการให้ความยินยอมดังกล่าวจะมีผลสมบูรณ์บังคับใช้ได้เพียง 13 เดือนเท่านั้น
7. ความรับผิดและโทษทางอาญา	-การกระทำที่เป็นการฝ่าฝืนหรือไม่กระทำการตามบทบัญญัติต่างๆ ของ DPA ส่งผลให้ผู้กระทำมีความผิดทางอาญาตามประมวลอาญา จะต้องรับโทษปรับสูงสุดถึง 300,000 ยูโร และรับโทษจำคุกสูงสุดถึง 5 ปี เช่น กรณีการประมวลผลข้อมูลเลขประจำตัวประชาชนที่ไม่เป็นไปตามเงื่อนไขของกฎหมาย หรือกรณีที่ไม่มีการแจ้ง CNIL เมื่อมีการละเมิดข้อมูลตามหลักเกณฑ์ที่กฎหมายกำหนดไว้ (DPA Article 40, Criminal Code Article 226-16 to 226-24)

3.3 หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี

สหพันธ์สาธารณรัฐเยอรมนีได้มีการปรับแก้กฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในให้มีความสอดคล้องกับ GDPR และยกร่างกฎหมายที่มีชื่อว่า Bundesdatenschutzgesetz (BDSG) ภายใต้ชื่อภาษาอังกฤษว่า Federal Data Protection Act ซึ่งมีผลบังคับใช้ตั้งแต่ 25 พฤษภาคม 2018 โดยมีวัตถุประสงค์เพื่อกำหนดรายละเอียดให้มีความเฉพาะเจาะจงและเพิ่มเติมข้อจำกัดบางประการ และในส่วน Part 3 ของ BDSG มีเนื้อหาเกี่ยวกับแนวทางการคุ้มครองข้อมูลที่เกี่ยวข้องกับการสืบสวนสอบสวนและกระบวนการพิจารณาคดีทางอาญา ซึ่งเป็นการปรับใช้ Law Enforcement Directive (EU) 2016/680 นอกจากนั้น สหพันธ์สาธารณรัฐ

[43] Decree No. 2019-341 of April 19, 2019 concerning the implementation of data processing involving the use of the personal identification number in the National Register of Individual Identification (RNIPP) or requiring consultation of this register.

[44] Decree No. 2019-536 of May 29, 2019 issued for the application of Law No. 78-17 of January 6, 1978 concerning information technology, data files, and civil liberties.

เยอรมนี ยังมีการกำหนดหลักกฎหมายคุ้มครองข้อมูลของแต่ละภาคส่วน เช่น การเงิน พลังงาน ฯลฯ สำหรับการคุ้มครองข้อมูลกรณีการติดต่อสื่อสารโทรคมนาคม สหพันธ์สาธารณรัฐเยอรมนีนำเอาบทบัญญัติที่เกี่ยวกับการใช้งานคุกกี้ของ EU ePrivacy Directive มาปรับใช้ โดยมีการยกร่างกฎหมายที่ชื่อว่า Telecommunications Telemedia Data Protection Act (TTDSG) ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 1 ธันวาคม 2021 สำหรับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับการโฆษณาและการทำการตลาดแบบตรงจะอยู่ภายใต้บังคับของ Section 7 of the German Act Against Unfair Competition (UWG) ซึ่งกฎหมายฉบับนี้มีการปรับแก้ในหลักการเมื่อ ธันวาคม 2020 ซึ่งต่อมามีการปรับแก้เพิ่มเติมและมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2022 นอกจากนั้น ยังมีกำหนดแนวทางเพิ่มเติมสำหรับการทำการโฆษณาแบบตรงภายใต้หลักเกณฑ์ของ GDPR ไว้ใน Guidance from the supervisory authorities on the processing of personal data for direct advertising purposes under the General Data Protection Regulation (GDPR) เมื่อวันที่18 กุมภาพันธ์ 2022.

หน่วยงานกำกับดูแลในการปฏิบัติตามกฎหมายในระดับรัฐบาลกลางมีชื่อว่า Federal Commissioner for Data Protection and Freedom of Information หรือ BfDI ตั้งอยู่ที่เมืองบอนน์ BfDI มีอำนาจในการควบคุมกำกับดูแลหน่วยงานราชการ ผู้ให้บริการเกี่ยวกับโทรคมนาคมและไปรษณีย์ รวมทั้งเป็นตัวแทนของสหพันธ์สาธารณรัฐเยอรมนีใน European Data Protection Board หรือ EDPB นอกจากนั้นยังมีหน่วยงานคุ้มครองข้อมูลในระดับรัฐบาลกลางซึ่งเป็นเจ้าหน้าที่ผู้ควบคุมที่มีความเป็นอิสระของสหพันธ์สาธารณรัฐเยอรมนี ที่ชื่อว่า The Data Protection Conference (DSK) ซึ่งจะประกอบด้วยเจ้าหน้าที่คุ้มครองข้อมูลจากรัฐบาลกลางและจาก รัฐ (Länder) ทั้ง 16 รัฐ เพื่อทำหน้าที่ในการปกป้องและคุ้มครองสิทธิพื้นฐานในการคุ้มครองข้อมูล รวมทั้งการทำให้แน่ใจว่าจะมีการปรับใช้กฎหมายคุ้มครองข้อมูลซึ่งเป็นกฎหมายภายในของประเทศและ GDPR เพื่อให้เป็นไปตามมาตรฐานเดียวกัน นอกจากนั้นในแต่ละรัฐ จะมีหน่วยงานกำกับดูแลที่รับผิดชอบในการตรวจสอบการปฏิบัติตามกฎหมายคุ้มครองข้อมูลในอาณาเขตของตนอีกด้วย (BDSG Section 40)

สาระสำคัญโดยสรุปของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหพันธ์สาธารณรัฐเยอรมนี ที่เกี่ยวข้องกับการดำเนินกิจกรรมของ ททท. สำนักงานแฟรงก์เฟิร์ต ซึ่งมีรายละเอียดเพิ่มเติมหรือแตกต่างไปจากที่ GDPR กำหนดไว้ มีรายละเอียดดังต่อไปนี้

เรื่อง	หลักกฎหมาย
1. การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์	-ในกรณีที่มีการเสนอบริการสารสนเทศ (เสนอสินค้าและบริการโดยใช้อุปกรณ์อิเล็กทรอนิกส์ในการประมวลผลและเก็บข้อมูลของผู้รับบริการ (information society)) แก่ผู้เยาว์ที่อาศัยอยู่ในสหพันธ์สาธารณรัฐเยอรมนี ผู้เยาว์สามารถให้ความยินยอมอย่างมีผลสมบูรณ์ตามกฎหมายเมื่อมีอายุอย่างน้อย 16 ปี แต่หากมีอายุน้อยกว่า 16 ปี จะต้องได้รับความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์ -TTDPA กำหนดไว้ว่าข้อมูลของผู้เยาว์ที่ได้รับมาโดยใช้วิธีการทางโทรคมนาคมไม่สามารถนำมาใช้ในการประมวลผลเพื่อวัตถุประสงค์ในทางการค้าได้
2. การใช้งานคุกกี้	-TTDSG Section 25 กำหนดให้ต้องมีการขอความยินยอมที่ชัดเจนก่อนการเก็บข้อมูลจากเครื่องมือปลายทาง (โทรศัพท์ คอมพิวเตอร์ เครื่องใช้ไฟฟ้าในบ้าน ยานยนต์อัจฉริยะ) หลักเกณฑ์ดังกล่าวใช้บังคับการการใช้คุกกี้เก็บข้อมูลโดยไม่พิจารณาว่าข้อมูลนั้นสามารถระบุตัวบุคคลได้หรือไม่ ความยินยอมที่ผลสมบูรณ์ตามฎหมายจะต้องเกิดขึ้นจากความสมัครใจ เฉพาะเจาะจง และจะต้องรับทราบข้อมูลครบถ้วนแล้ว โดยจะต้องมีการกระทำที่ชัดเจนที่เป็นการให้ความยินยอม ข้อยกเว้นกรณีไม่ต้องขอความยินยอมคือกรณีการเก็บข้อมูลคุกกี้สำหรับการส่งข้อมูลผ่านระบบเครือข่ายโทรคมนาคมสาธารณะ

เรื่อง	หลักกฎหมาย
	และข้อมูลคุกกี้ที่จำเป็นอย่างยิ่งสำหรับผู้ให้บริการในการให้บริการโทรคมนาคมกับผู้ใช้บริการที่มีการร้องขออย่างชัดเจน
3. การส่งอีเมลเพื่อโฆษณาและทำการตลาดแบบตรง	-UWG Section 7 กำหนดไว้ว่า การทำการตลาดแบบตรงผ่านทางอีเมลจะต้องได้รับความยินยอมอย่างชัดเจนจากผู้รับข้อมูลก่อนเท่านั้น โดยจะต้องเป็นความยินยอมในรูปแบบที่เรียกว่า double opt-in กล่าวคือจะต้องได้รับอีเมลยืนยันความยินยอมจากผู้รับข้อมูลเพื่อแสดงให้เห็นเจตนาของผู้รับข้อมูลว่าได้มีการร้องขอเอง ภายหลังจากที่ผู้รับข้อมูลได้รับอีเมลเพื่อขอความยินยอมในการตอบรับการเป็นสมาชิกโดยจะต้องมีการแสดงเจตนาให้ความยินยอมที่เรียกว่า initial opt-in given โดยการคลิ๊กลิ้งที่ส่งไปทางอีเมลเพื่อขอความยินยอมในการตอบรับการเป็นสมาชิกซึ่งอีเมลนี้จะต้องไม่มี
	เนื้อหาเกี่ยวกับการโฆษณาหรือการตลาด อีเมลนี้จะต้องมีการแจ้งที่อยู่ของอีเมลที่จะให้ผู้รับข้อมูลส่งอีเมลไปเพื่อร้องขอให้มีการส่งข้อมูลเพื่อโฆษณาและทำการตลาดแบบตรง ซึ่งถือเป็นการทำ double opt-in consent โดยจะต้องแจ้งรายละเอียดเกี่ยวกับชื่อองค์กรที่จะส่งอีเมลและข้อมูลเกี่ยวกับสินค้าหรือบริการที่จะทำการโฆษณาหรือการตลาดแบบตรงประกอบด้วย UWG ห้ามมิให้มีการส่งอีเมลที่ปกปิดตัวตนของผู้ส่งหรือการไม่แจ้งสิทธิและช่องทางในการยกเลิกการรับข้อมูล -Section 7 (3) UWG กำหนดข้อยกเว้นไว้ว่า กรณีการส่งอีเมลเพื่อทำการตลาดสำหรับสินค้าหรือบริการที่ผู้รับข้อมูลได้ซื้อไปแล้ว สามารถทำได้หากผู้รับข้อมูลได้รับแจ้งสิทธิในการยกเลิกการรับข้อมูลในอีเมลฉบับแรกแล้ว และผู้รับข้อมูลไม่ได้แสดงเจตนาในการยกเลิก
4. การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล	-องค์กรจะต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากมีจำนวนของลูกจ้างประจำอย่างน้อย 20 คนที่ปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล หรือหากองค์กรใดมีลูกจ้างน้อยว่า 20 คน แต่มีการประมวลผลข้อมูลในลักษณะที่ส่งผลให้เกิดความเสี่ยงสูง เช่น การประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษอยู่เป็นประจำ โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นบุคคลภายในหรือบุคคลภายนอกองค์กรก็ได้ แต่จะต้องสามารถปฏิบัติหน้าที่ได้อย่างอิสระ และมีคุณสมบัติ ความรู้ความสามารถที่จำเป็นในการปฏิบัติหน้าที่
5. การประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment (DPIA))	-เจ้าหน้าที่ผู้ควบคุมในแต่ละรัฐกำหนดรายการของกิจกรรมที่มีความเสี่ยงสูงซึ่งจำเป็นต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูล ซึ่งรายการนี้เรียกว่า "black list" กิจกรรมดังกล่าวมีความเกี่ยวข้องกับกิจกรรมการประมวลผลที่เกี่ยวข้องกับการนำเอาข้อมูลจำนวนมากมาใช้ในการวิเคราะห์ หรือการใช้เทคโนโลยีใหม่ในการประมวลผลข้อมูลซึ่งผลให้เกิดความเสี่ยงต่อเจ้าของข้อมูล (เช่น ระบบ facial recognition) หรือการโอนข้อมูลออกนอกเขตสหภาพยุโรป
6. ความรับผิดและโทษทางอาญา	-BDSG Section 42 กำหนดให้การโอนข้อมูลไปยังบุคคลที่สามหรือการทำให้ข้อมูลเข้าถึงได้เพื่อวัตถุประสงค์ทางการค้า จะต้องรับโทษทางอาญาเป็นโทษปรับหรือจำคุกไม่เกินสามปี ในกรณีที่มีการประมวลผลข้อมูลโดยไม่ได้รับอนุญาตหรือเป็นการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลเพื่อให้ได้รับผลตอบแทนหรือมีเจตนาในการทำอันตรายบุคคลอื่นจะต้องรับโทษทางอาญาเป็นโทษปรับหรือจำคุกสูงสุดถึงสองปี

เรื่อง	หลักกฎหมาย
	-TTDSG Section 27-30 กำหนดความรับผิดทางอาญาไว้กรณีที่ไม่ได้รับความยินยอมก่อนการเก็บข้อมูลคุกกี้จะต้องรับโทษปรับสูงสุดถึง 300,000 ยูโร ในกรณีที่มีการละเมิดเรื่องการรักษาความปลอดภัยของข้อมูลจะต้องรับโทษปรับและจำคุกสูงสุดถึงสองปี

3.4 หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐอิตาลี

สาธารณรัฐอิตาลีนำบทบัญญัติของ GDPR มาใช้ โดยการปรับปรุงบทบัญญัติซึ่งเป็นกฎหมายภายในที่มีชื่อว่า Legislative Decree No. 196 of June 30, 2003 (Personal Data Protection Code) เพื่อให้สอดคล้องกับ GDPR โดยมีการออกบทบัญญัติ the Legislative Decree No. 101 of August 10, 2018 มาเพื่อปรับแก้ Personal Data Protection Code เพื่อให้สอดคล้องกับ GDPR รวมทั้งมีการกำหนดบทบัญญัติใหม่ ๆ ขึ้นมาเพื่อรองรับหลักการที่อยู่ใน GDPR ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 19 กันยายน 2018 เป็นต้นมา โดยมีหน่วยงานกำกับดูแลชื่อว่า Garante ทำหน้าที่กำกับดูแลให้มีการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล บริหารจัดการข้อร้องเรียน สามารถสั่งระงับการประมวลผลข้อมูลที่ส่งกระทบอย่างมากต่อเจ้าของข้อมูลส่วนบุคคล นอกจากนั้น Garante ยังมีอำนาจที่จะดำเนินคดีตามกฎหมายกับผู้ควบคุมหรือผู้ประมวลผลที่ละเมิดข้อกำหนดเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลโดยมีพนักงานอัยการเป็นผู้ฟ้องคดี และมีอำนาจส่งเอกสารและข้อค้นพบต่างๆ ไปยังพนักงานอัยการเมื่อพบว่ามีกิจกรรมที่นำไปสู่การสันนิษฐานได้ว่ามีการละเมิดบทบัญญัติเกิดขึ้น (Personal Data Protection Code, Article 167(5)) นอกจากนั้น สาธารณรัฐอิตาลีมีการกำหนดแนวทางเกี่ยวกับการใช้งานคุกกี้ไว้ใน Guidelines on the Use of Cookies and Other Tracking Tools with Decision No. 231 of June 10, 2021 (Cookie Guidelines) ซึ่งมีผลตั้งแต่วันที่ 10 มกราคม 2022 เป็นต้นมา

สาระสำคัญโดยสรุปของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสาธารณรัฐอิตาลีที่เกี่ยวข้องกับการดำเนินกิจกรรมของ ททท. สำนักงานโรม ซึ่งมีรายละเอียดเพิ่มเติมหรือแตกต่างไปจากที่ GDPR กำหนดไว้ มีรายละเอียดดังต่อไปนี้

เรื่อง	หลักกฎหมาย
1. การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์	-ในกรณีที่มีการเสนอบริการสารสนเทศ (เสนอสินค้าและบริการโดยใช้อุปกรณ์อิเล็กทรอนิกส์ในการประมวลผลและเก็บข้อมูลของผู้รับบริการ (information society)) แก่ผู้เยาว์ที่อาศัยอยู่ในสาธารณรัฐอิตาลี ผู้เยาว์สามารถให้ความยินยอมอย่างมีผลสมบูรณ์ตามกฎหมายเมื่อมีอายุอย่างน้อย 14 ปี แต่หากมีอายุน้อยกว่า 14 ปี จะต้องได้รับความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์ (Personal Data Protection Code, Article 2-quinquies)
2. การประมวลผลข้อมูลในบริบทของการจ้างงาน	- องค์กรในฐานะนายจ้างไม่สามารถดำเนินการตรวจสอบข้อมูลของผู้สมัครงานและลูกจ้างในส่วนที่เกี่ยวกับความคิดเห็นทางการเมือง ความเชื่อทางศาสนา สมาชิกสหภาพแรงงาน หรือเรื่องอื่นๆ ที่ไม่ได้มีความเกี่ยวข้องโดยตรงกับทักษะ ความสามารถประสบการณ์ทางวิชาชีพของลูกจ้างได้ แม้จะเป็นการตรวจสอบโดยใช้บุคคลที่สามเป็นผู้ดำเนินการให้ก็ตาม (Personal Data Protection Code, Article 113) - องค์กรไม่สามารถใช้เทคโนโลยีหรือเครื่องมือต่างๆ เช่น กล้องวิดีโอ เพื่อควบคุมหรือติดตามพฤติกรรมของลูกจ้างในช่วงเวลาระหว่างการทำงานได้ แต่นายจ้างสามารถใช้เทคโนโลยีหรือเครื่องมือดังกล่าวได้เฉพาะกรณีเพื่อรักษาความปลอดภัยในสถานที่ทำงานเท่านั้น โดยจะต้องมีการทำข้อตกลงกับสหภาพแรงงานไว้ก่อนจึงจะสามารถดำเนินการได้ (Personal Data Protection Code, Article 114)

เรื่อง	หลักกฎหมาย
3. การประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรม	- การประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมสามารถดำเนินการได้เฉพาะกรณีที่มีกฎหมายให้อำนาจไว้เท่านั้น เช่น เพื่อปฏิบัติตามกฎหมายป้องกันการฟอกเงิน กฎหมายแรงงาน ฯลฯ ในกรณีที่ไม่มีกฎหมายให้อำนาจไว้ องค์กรสามารถเสนอให้ Garante พิจารณาเพื่อออกพระราชกฤษฎีกาอนุญาตให้ประมวลผลข้อมูลดังกล่าวได้เช่นกัน แต่อย่างไรก็ตามการประมวลผลข้อมูลดังกล่าวองค์กรจะต้องใช้มาตรการในการป้องกันที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล (Personal Data Protection Code, Article 2- *octies*)
4. ข้อจำกัดในการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล	- Personal Data Protection Code Article 2-*undecies* กำหนดข้อจำกัดบางประการสำหรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น เจ้าของข้อมูลไม่สามารถใช้สิทธิในการเข้าถึงข้อมูลได้หากการใช้สิทธินั้นก่อให้เกิดความเสี่ยงต่อผลประโยชน์ที่ได้รับการคุ้มครองโดยกฎหมายป้องกันการฟอกเงิน หรือส่งผลกระทบต่อการใช้สิทธิในศาลหรือทำให้ทราบตัวตนของผู้แจ้งเบาะแสในบริบทของการจ้างงาน
5. การประเมินผลกระทบด้านการคุ้มครองข้อมูล (Data Protection Impact Assessment (DPIA))	- Garante กำหนดตัวอย่างรายการกิจกรรมที่มีความจำเป็นจะต้องประเมินผลกระทบด้านการคุ้มครองข้อมูลไว้ใน Decision No. 467 of October 11, 2018 ยกตัวอย่าง เช่น การประมวลผลข้อมูลขนาดใหญ่ที่เกี่ยวข้องกับการประเมินผล การคาดเดาที่เกี่ยวข้องกับการปฏิบัติงานทางวิชาชีพ เรื่องสุขภาพ ความสนใจส่วนตัว ความน่าเชื่อถือ พฤติกรรม ที่อยู่ของเจ้าของข้อมูลส่วนบุคคล/ การประมวลผลขอมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลที่เกี่ยวข้องกับประวัติอาชญากรรมซึ่งมีความเชื่อมโยงกับข้อมูลส่วนบุคคลอื่นๆที่เก็บไว้สำหรับวัตถุประสงค์ที่แตกต่างกัน/การประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลที่เป็นกลุ่มเปราะบาง/การประมวลผลข้อมูลโดยใช้เทคโนโลยีใหม่ๆ/การประมวลผลข้อมูลไบโอเมตริกซ์
6. การใช้สิทธิของเจ้าของข้อมูลที่ถึงแก่กรรมไปแล้ว	-Personal Data Protection Code Article 2-terdecies กำหนดให้บุคคลที่มีลักษณะดังต่อไปนี้ สามารถใช้สิทธิของเจ้าของข้อมูลที่ถึงแก่กรรมไปแล้วได้ คือ 1. มีผลประโยชน์ส่วนตัวที่เกี่ยวข้อง 2. ทำหน้าที่เพื่อผลประโยชน์ของผู้ที่ถึงแก่กรรมไปแล้วในฐานะตัวแทนที่มีอำนาจ 3. ทำหน้าที่เพื่อรักษาผลประโยชน์ของครอบครัว เว้นแต่จะมีข้อห้ามตามกฎหมายหรือเป็นไปตามเจตนารมณ์ที่เป็นลายลักษณ์อักษรของผู้ตาย
7. การใช้คุกกี้	- Personal Data Protection Code Section 122 และ Cookie Guidelines กำหนดประเภทของคุกกี้ไว้ 3 ประเภท คือ 1. Technical cookies ใช้เฉพาะเพื่อการส่งผ่านการสื่อสารบนระบบการติดต่อทางอิเล็กทรอนิกส์ หรือเป็นการจำเป็นสำหรับผู้ให้บริการสารสนเทศในการให้บริการที่ได้รับการร้องขออย่างชัดเจนจากผู้ใช้บริการ การใช้คุกกี้ประเภทนี้ไม่ต้องขอความยินยอมจากเจ้าของข้อมูล ; 2. Profiling cookies ใช้สำหรับการติดตามการกระทำที่เฉพาะเจาะจงหรือรูปแบบพฤติกรรมที่เกิดขึ้นเป็นประจำที่ใช้สำหรับการนำเสนอบริการที่มีความเฉพาะเจาะจง ซึ่งสามารถบ่งชี้ถึงตัวบุคคลได้เพื่อวัตถุประสงค์ในการจัดกลุ่มตามเนื้อหาหรือแบ่งตามขนาด ทำให้ผู้ควบคุมสามารถให้บริการตามความต้องการของผู้ใช้บริการและสามารถส่งข้อความที่เป็นการโฆษณาแบบกำหนดกลุ่มเป้าหมายได้ตามความต้องการที่ผู้ใช้บริการแสดงเจตนาร้องขอไว้ การใช้คุกกี้ประเภทนี้ต้องขอความยินยอมจากเจ้าของข้อมูลก่อนการใช้งาน 3. Analytics cookies การใช้คุกกี้ประเภทนี้ต้องขอความยินยอมจากเจ้าของข้อมูลก่อนการใช้งาน เว้นแต่เป็นการดำเนินการโดยฝ่ายที่สาม โดยมีการนำเครื่องมือที่เหมาะสมไปใช้สำหรับ

เรื่อง	หลักกฎหมาย
	ลดความสามารถในการบ่งชี้ของคุกกี้ เช่น การใช้วิธีการปิดบังข้อมูลบางส่วนของ IP address และไม่มีการรวมข้อมูลที่ได้รับมาจากคุกกี้ประเภทนี้กับข้อมูลอื่นๆที่ได้รับมาโดยฝ่ายที่สาม
8. ความรับผิดและโทษทางอาญา	-Personal Data Protection Code, Article 167-172 กำหนดความรับผิดและบทลงโทษทางอาญาไว้เป็นการลงโทษจำคุกตั้งแต่ 6 เดือนถึง 6 ปี สำหรับการกระทำบางประการ เช่น การเผยแพร่ข้อมูลส่วนบุคคลที่ผิดกฎหมายเพื่อให้ได้รับผลกำไรจากเจ้าของข้อมูลหรือทำให้เกิดความเสียหายต่อเจ้าของข้อมูล/การหลอกลวงเพื่อเก็บรวบรวมข้อมูลที่มีขนาดใหญ่เพื่อให้ได้รับผลกำไรหรือทำให้เกิดความเสียหายต่อเจ้าของข้อมูล/การจัดทำเอกสารเท็จหรือตั้งใจรบกวนการทำหน้าที่ของ Garante หรือในขั้นตอนการสืบสวนสอบสวน/การไม่ปฏิบัติตามบทบัญญัติที่ออกโดย Garante.

3.5 หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของราชอาณาจักรสวีเดน

กฎหมายคุ้มครองข้อมูลฉบับแรกของราชอาณาจักรสวีเดนบังคับใช้เมื่อปี 1973 โดยใช้ชื่อกฎหมายว่า Datalagen และมีหน่วยงานกำกับดูแล คือ Datainspektionen ที่ก่อตั้งขึ้นในปีเดียวกัน และเมื่อวันที่ 1 มกราคม 2021 หน่วยงานดังกล่าวได้เปลี่ยนชื่อเป็น Integritetsskyddsmyndigheten ("IMY") ต่อมาเมื่อ GDPR มีผลบังคับใช้ ราชอาณาจักรสวีเดนมีการบัญญัติกฎหมายเฉพาะออกมาเพื่อเสริมเนื้อหาใน GDPR ซึ่งก็คือ Lag (2018:218) med kompletterande bestämmelser till EU: sdataskyddsförordning (dataskyddslagen) ภายใต้ชื่อภาษาอังกฤษว่า Data Protection Act (2019:218) ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 25 พฤษภาคม 2018 เป็นต้นมา โดยมี IMY เป็นหน่วยงานกำกับดูแลให้มีการปฏิบัติตาม GDPR และ Data Protection Act รวมทั้งมีอำนาจตรวจสอบการปฏิบัติตามกฎหมายโดยสามารถขอให้ผู้ควบคุมหรือผู้ประมวลผลให้ข้อมูลและเอกสารที่เกี่ยวข้องและมีอำนาจเข้าไปยังสถานที่ของหน่วยงานต่างๆ เพื่อตรวจสอบทางกายภาพได้อีกด้วย ซึ่งหากพบว่ามีการไม่ปฏิบัติตามกฎหมาย IMY สามารถออกคำสั่งลงโทษตามความหนักเบาของการไม่ปฏิบัติตามกฎหมายได้ นอกจากนั้น ราชอาณาจักรสวีเดนใช้บทบัญญัติของ EU e-Privacy Directive มาเป็นแนวทางในการยกร่างกฎหมายภายในที่ชื่อว่า Lag (2003:389) om Elektronisk Kommunikation ภายใต้ชื่อภาษาอังกฤษว่า the Swedish Electronics Communication Act (SEC) มีผลบังคับใช้ตั้งแต่วันที่ 3 มิถุนายน 2022 โดยมุ่งกำหนดหลักเกณฑ์เกี่ยวกับการติดต่อสื่อสารระหว่างกันในรูปแบบที่ไม่ใช้เบอร์ เช่น อีเมล การสนทนาแบบกลุ่ม รวมทั้งกำหนดหลักเกณฑ์เกี่ยวกับการใช้งานคุกกี้ ซึ่งจะมี the Swedish Post and Telecom Authority (PTS) เป็นหน่วยงานเฉพาะในการกำกับดูแลและกำหนดบทลงโทษกรณีที่มีการไม่ปฏิบัติตามกฎหมาย

สาระสำคัญโดยสรุปของหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของราชอาณาจักรสวีเดนที่เกี่ยวข้องกับการดำเนินกิจกรรมของ ททท. สำนักงานสตอกโฮล์ม ซึ่งมีรายละเอียดเพิ่มเติมหรือแตกต่างไปจากที่ GDPR กำหนดไว้ มีรายละเอียดดังต่อไปนี้

เรื่อง	หลักกฎหมาย
1. การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์	-ในกรณีที่มีการเสนอบริการสารสนเทศ (เสนอสินค้าและบริการโดยใช้อุปกรณ์อิเล็กทรอนิกส์ในการประมวลผลและเก็บข้อมูลของผู้รับบริการ (information society)) แก่ผู้เยาว์ที่อาศัยอยู่ในราชอาณาจักรสวีเดน ผู้เยาว์สามารถให้ความยินยอมอย่างมีผลสมบูรณ์ตามกฎหมายเมื่อมีอายุอย่างน้อย 13 ปี แต่หากมีอายุน้อยกว่า 13 ปี จะต้องได้รับความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์ สำหรับผู้เยาว์ที่อายุเกิน 16 ปีสามารถให้ความยินยอมในการประมวลผลข้อมูลส่วนบุคคลของตนได้ แต่ผู้เยาว์ที่อายุ 13-16 ปี จะต้องมีการประเมินประเด็นต่างๆ ประกอบการให้ความยินยอมเป็นรายกรณีไป เช่น อายุของเจ้าของข้อมูล ประเภทของข้อมูลส่วนบุคคล ระยะเวลาในการประมวลผล วัตถุประสงค์ของการประมวลผล ฯลฯ นอกจากนี้ ผู้ควบคุมหรือผู้ประมวลผลจะต้องให้ข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่ชัดเจน เข้าถึงได้ และเข้าใจง่ายจากมุมมองของผู้เยาว์ ทั้งนี้ เพื่อให้ผู้เยาว์เข้าใจได้อย่างถูกต้องว่าการประมวลผลข้อมูลส่วนบุคคลของตนเป็นไปเพื่อวัตถุประสงค์ใด และเพื่อให้ผู้เยาว์ได้รับข้อมูลที่ถูกต้องครบถ้วนก่อนตัดสินใจให้ความยินยอม (Data Protection Act, Chapter 2 Section 4)
2. การประมวลผลข้อมูลส่วนบุคคลในบริบทของการจ้างงาน	-การประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษในบริบทของการจ้างงานสามารถดำเนินการได้ หากเป็นการดำเนินการเพื่อการประเมินความสามารถในการทำงาน ทั้งนี้เพื่อเป็นการปฏิบัติตามหน้าที่ตามกฎหมายแรงงานหรือกฎหมายอื่นๆ ที่เกี่ยวข้อง (Data Protection Act, Chapter 3 Section 2)
3. การประมวลผลข้อมูลเลขประจำตัวประชาชนและเลขประจำตัวผู้เสียภาษี	-แม้ข้อมูลเกี่ยวกับเลขประจำตัวประชาชนและเลขประจำตัวผู้เสียภาษี (Personal Identity Number and Coordination Numbers) จะไม่ใช่ข้อมูลส่วนบุคคลชนิดพิเศษ แต่ Data Protection Act, Chapter 3 Section 10,11 กำหนดรายละเอียดไว้โดยเฉพาะว่า การประมวลผลข้อมูลเลขประจำตัวประชาชนและเลขประจำตัวผู้เสียภาษีโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลอาจทำได้เฉพาะเพื่อให้บรรลุวัตถุประสงค์บางประการเท่านั้น เช่น เพื่อรักษาความปลอดภัยของข้อมูล ฯลฯ
4. การประเมินผลกระทบด้านการคุ้มครองข้อมูลข้อมูล (Data Protection Impact Assessment (DPIA))	- Data Protection Act กำหนดหลักเกณฑ์เฉพาะสำหรับการจัดทำ DPIA โดยหน่วยงานกำกับดูแล (IMY) ให้รายละเอียดไว้ว่า กิจกรรมที่จะต้องทำ DPIA นั้น คือ กิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีลักษณะเข้าเกณฑ์ดังต่อไปนี้ อย่างน้อยสองประการ 1. การประเมินหรือการให้คะแนน 2. การตัดสินใจโดยระบบอัตโนมัติโดยมีผลทางกฎหมายหรือมีผลสำคัญที่คล้ายคลึงกัน 3. การติดตามควบคุมอย่างเป็นระบบ 4. เป็นข้อมูลชนิดพิเศษหรือข้อมูลที่มีลักษณะที่เป็นส่วนตัวสูง 5. ข้อมูลที่ถูกประมวลผลมีจำนวนมาก 6. การจับคู่หรือการรวมชุดข้อมูลในรูปแบบที่เจ้าของข้อมูลไม่สามารถคาดหมายได้ 7. ข้อมูลที่เกี่ยวกับกับเจ้าของข้อมูลที่เป็นกลุ่มเปราะบาง (เช่น ผู้เยาว์, ลูกจ้าง) 8. การใช้วิธีการทางเทคนิคหรือวิธีการขององค์กรในรูปแบบใหม่ๆ ในการประมวลผลข้อมูล 9. การประมวลผลนั้นทำให้เจ้าของข้อมูลไม่สามารถใช้บริการหรือเข้าทำสัญญาได้ - นอกจากนั้น IMY ได้ยกตัวอย่างกิจกรรมการประมวลผลข้อมูลส่วนบุคคลซึ่งต้องทำ DPIA ไว้ด้วย เช่น กรณีนายจ้างควบคุมกำกับดูแลอย่างเป็นระบบในเรื่องการใช้งาน

เรื่อง	หลักกฎหมาย
	อินเตอร์เน็ตและอีเมลของลูกจ้าง, กรณีที่นายจ้างใช้ระบบการเก็บข้อมูลไบโอเมติกของลูกจ้างเพื่อใช้ในการยืนยันตัวตนของลูกจ้าง, กรณีนายจ้างค้นหาและตรวจสอบข้อมูลประวัติผู้สมัครงานเพื่อวัตถุประสงค์ในการสรรหาบุคลากร, การเก็บรวบรวมข้อมูลส่วนบุคคลจากโซเชียลมีเดียหรือจากผู้ใช้บริการแอพพลิเคชั่นเพื่อใช้ในการวิเคราะห์การตลาด, การที่หน่วยงานของรัฐให้บริการต่างๆ โดยใช้ดิจิทัลแพลตฟอร์ม ฯลฯ[45]
5. สิทธิในการแสดงความเห็น (the right to give an opinion)	- Data Protection Act, Chapter 6 Section 4 กำหนดให้สิทธิกับองค์กรที่อาจโดนปรับเนื่องจากถูกกล่าวหาว่าไม่ปฏิบัติตามกฎหมาย โดยกำหนดไว้ว่า “ค่าปรับทางปกครองไม่อาจกำหนดได้ เว้นแต่องค์กรที่อาจถูกปรับมีโอกาสในการให้ความเห็นภายในห้าปีนับจากวันที่มีการฝ่าฝืนกฎหมาย”
6. การใช้คุกกี้	- ECA Chapter 6, Section 18 กำหนดไว้ว่า หากมีการใช้งานคุกกี้บนเว็บไซต์หรือแอพพลิเคชั่น องค์กรจะต้องจัดทำป้ายแจ้งเตือนเสมอเกี่ยวกับรายละเอียดของคุกกี้ที่ใช้ วัตถุประสงค์ที่ใช้ ระยะเวลาในการเก็บ วิธีการในการปฏิเสธการใช้คุกกี้ และมีการแจ้งนโยบายการใช้งานคุกกี้ด้วย องค์กรจะสามารถติดตั้งคุกกี้บนเครื่องมือของเจ้าของข้อมูลผู้ใช้งานเว็บไซต์หรือแอพพลิเคชั่นได้ก็ต่อเมื่อมีการแจ้งรายละเอียดดังกล่าวและได้รับความยินยอมก่อนแล้วเท่านั้น รวมทั้งต้องกำหนดช่องทางที่สะดวกและเห็นได้ชัด (first layer of cookie consent pop-up) สำหรับการปฏิเสธการใช้งานคุกกี้ ECA กำหนดข้อยกเว้นกรณีที่ไม่ต้องขอความยินยอมไว้ เช่น คุกกี้ที่มีความจำเป็นอย่างยิ่งสำหรับการส่งข้อความระหว่างกันในระบบอิเล็กทรอนิกส์ และคุกกี้ที่ใช้สำหรับการให้บริการที่เกิดขึ้นจากการร้องขออย่างชัดแจ้งของเจ้าของข้อมูลเอง
7. ความรับผิดและโทษทางอาญา	- Data Protection Act ไม่ได้กำหนดความรับผิดทางอาญาไว้ แต่การละเมิดข้อมูลส่วนบุคคลถือเป็นการกระทำความผิดทางอาญาที่ต้องรับโทษตามประมวลกฎหมายอาญาของราชอาณาจักรสวีเดน (Swedish Penal Code (Sw. *brottsbalken*, SFS 1962:700) Chapter 4, Section 9c)

3.6 หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหราชอาณาจักร

สหราชอาณาจักรกำหนดหลักกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลไว้ใน UK General Data Protection Regulation (Regulation (EU) (2016/679)) (UK GDPR) และ Data Protection Act 2018 ในส่วนที่เกี่ยวกับการสื่อสารทางอิเล็กทรอนิกส์ โดยเฉพาะกิจกรรมทางการตลาด จะอยู่ภายใต้บังคับของ Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) ซึ่งใช้บังคับควบคู่กันไปกับ UK GDPR และ Data Protection Act 2018

Data Protection Act 2018 มีผลใช้บังคับตั้งแต่เมื่อวันที่ 25 พฤษภาคม ค.ศ. 2018 แต่ต่อมาได้รับการแก้ไขหลังจากเหตุการณ์ Brexit จึงส่งผลให้ Data Protection Act 2018 ฉบับปัจจุบันมีผลบังคับใช้ในสหราชอาณาจักรตั้งแต่วันที่ 1 มกราคม 2021 เป็นต้นมา บทบัญญัติของ UK GDPR ปรากฏอยู่ใน Part 2 ของ Data Protection Act 2018 มีเนื้อหาที่มีความคล้ายคลึงกับ EU GDPR โดย Data Protection Act 2018 จะทำหน้าที่เป็นส่วนเสริมระบอบของการคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ใน UK GDPR ซึ่ง Data Protection Act 2018

[45] IMY, List Regarding Data Protection Impact Assessments According to Article 35.4 of the Data Protection Regulation 2019 <https://www.imy.se/globalassets/dokument/ovrigt/list-regarding-data-protection-impact-assessments.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.

และ UK GDPR ซึ่งมีรายละเอียดโดยสรุปที่เกี่ยวข้องกับการดำเนินกิจกรรมของ ททท. สำนักงานลอนดอน ดังต่อไปนี้

เรื่อง	หลักกฎหมาย
1.การประมวลผลข้อมูลส่วนบุคคลของผู้เยาว์	- ในกรณีที่มีการเสนอบริการสารสนเทศ (เสนอสินค้าและบริการโดยใช้อุปกรณ์อิเล็กทรอนิกส์ในการประมวลผลและเก็บข้อมูลของผู้รับบริการ (information society)) แก่ผู้เยาว์ที่อาศัยอยู่ในสหราชอาณาจักร ผู้เยาว์สามารถให้ความยินยอมอย่างมีผลสมบูรณ์ตามกฎหมายเมื่อมีอายุอย่างน้อย 13 ปี แต่หากมีอายุน้อยกว่า 13 ปี จะต้องได้รับความยินยอมจากผู้แทนโดยชอบธรรม (UK GDPR Art 9) โดยบริการสารสนเทศในกรณีนี้ จะไม่รวมถึงบริการที่นำเสนอออนไลน์ในรูปแบบของเว็ปไซต์หรือแอพพลิเคชั่นในลักษณะของการให้คำปรึกษาหรือบริการอื่นที่เป็นการป้องกันในกรณีต่างๆ เช่น บริการคัดกรองโรคหรือเช็คสุขภาพ แต่หากเป็นการให้บริการทั่วไปเกี่ยวกับสุขภาพ การออกกำลังกาย ก็ยังคงอยู่ภายใต้บังคับของ UK GDPR (UK GDPR Art 9(b))
2.การประมวลผลข้อมูลอาชญากรรม	- ผู้ควบคุมสามารถประมวลผลข้อมูลอาชญากรรมได้หากเป็นไปเพื่อวัตถุประสงค์ในการปฏิบัติหน้าที่ตามกฎหมายเกี่ยวกับการจ้างงาน (UK GDPR Art 10 (1)(a))
3.คำนิยามของคำว่า “ลูกจ้าง” (employee)	- UK GDPR Art 33 (2) ให้ความหมายของคำว่า “ลูกจ้าง” ไว้ว่า หมายถึง “บุคคลรวมถึงปัจเจกชนซึ่งได้รับและไม่ได้รับค่าจ้างที่มีตำแหน่งอยู่ภายใต้การควบคุมของบุคคลดังกล่าวด้วย”
4. ค่าธรรมเนียมการคุ้มครองข้อมูล (Data Protection Fee	- ผู้ควบคุมที่มีการประมวลผลข้อมูลส่วนบุคคลบางส่วนหรือทั้งหมดด้วยวิธีการทางอิเล็กทรอนิกส์มีหน้าที่ชำระ “ค่าธรรมเนียมการคุ้มครองข้อมูล” เป็นรายปีและให้ข้อมูลบางประเภทเช่น ชื่อและที่อยู่ขององค์กร จำนวนพนักงานในองค์กรแก่หน่วยการกำกับดูแล (ICO) ค่าธรรมเนียมการคุ้มครองข้อมูลมีสามระดับตั้งแต่ 40 ปอนด์จนถึง 2,900 ปอนด์ต่อปี ขึ้นอยู่กับประเภทขององค์กร จำนวนพนักงาน และมูลค่าการซื้อขาย หากไม่ชำระค่าธรรมเนียมให้ถูกต้องจะมีโทษปรับสูงสุด 4,000 ปอนด์[46](เป็นไปตามที่ the Data Protection (Charges and Information) Regulations 2018 ซึ่งมีผลบังคับใช้เมื่อวันที่ 25 พฤษภาคม 2018 ได้กำหนดไว้)
5.การจัดทำเอกสารนโยบายที่เหมาะสม (Appropriate Policy Documents (APD))	-ในกรณีที่มีการประมวลผลข้อมูลชนิดพิเศษ ข้อมูลอาชญากรรม และกรณีการประมวลผลข้อมูลในบริบทของการจ้างงาน องค์กรมีหน้าที่จะต้องจัดทำเอกสารนโยบายที่เหมาะสมสำหรับการประมวลผลดังกล่าว ซึ่งมีรายละเอียดเกี่ยวกับการปฏิบัติตามหลักเกณฑ์ของกฎหมาย เช่น รายละเอียดเกี่ยวกับการประมวลผลข้อมูล ฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูล ระยะเวลาในการเก็บและแนวทางการลบทำลายข้อมูล ฯลฯ โดย Data Protection Act 2018(Schedule 1 paragraphs 1 and 5) กำหนดไว้ว่าเอกสารนี้จำเป็นต้องมีอยู่ตลอดระยะเวลาที่มีการประมวลผลข้อมูลและอย่างน้อยอีก 6 เดือนนับแต่การประมวลผลข้อมูลสิ้นสุดลง รวมทั้งจะต้องมีการทบทวนรายละเอียดในเอกสารนี้ทุกปีหรือมีการแก้ไขได้เสมอเมื่อมีความจำเป็น

[46] The Data Protection (Charges and Information) Regulations 2018. And ‘Data Protection Fee’ (ICO) <https://ico.org.uk/for-organisations/data-protection-fee/> สืบค้นเมื่อ 11 พฤษภาคม 2567.

เรื่อง	หลักกฎหมาย
6.การประเมินผลกระทบด้านการคุ้มครองข้อมูลข้อมูล (Data Protection Impact Assessment)	- UK GDPR Art 64 กำหนดไว้ว่าการประมวลผลข้อมูลที่มีความเป็นไปได้ที่จะส่งผลให้เกิดความเสี่ยงสูง จำเป็นที่ต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA) ซึ่ง ICO ได้ยกตัวอย่างไว้ในกรณีการประมวลผลข้อมูลของบุคคลที่เป็นกลุ่มเปราะบาง เช่น การประมวลผลข้อมูลของผู้เยาว์ในกรณีที่มีการนำเสนอบริการสารสนเทศ และการประมวลผลข้อมูลของลูกจ้างเนื่องจากลูกจ้างมีอำนาจที่ไม่เท่าเทียมกันกับนายจ้าง ทั้งสองกรณีถือเป็นการประมวลผลที่มีความเป็นไปได้ที่จะส่งผลให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูล จึงต้องจัดทำ DPIA[47]
7. การใช้คุกกี้	- PECR กำหนดหลักเกณฑ์สำหรับบังคับใช้กับการใช้คุกกี้ในทุกรูปแบบ แม้จะเป็นการใช้คุกกี้เก็บข้อมูลที่ไม่สามารถระบุตัวตนได้ก็ตาม (anonymous data) องค์กรจะต้องขอความยินยอมก่อนเสมอ โดยจะต้องแจ้งรายละเอียดที่ชัดเจน ครอบคลุม และเข้าถึงได้ง่าย เกี่ยวกับวัตถุประสงค์ที่จะนำไปใช้ ผลกระทบที่จะเกิดขึ้นจากการให้ความยินยอม ความยินยอมที่ผลสมบูรณ์ตามกฎหมายจะต้องเกิดขึ้นจากความสมัครใจเฉพาะเจาะจง และจะต้องรับทราบข้อมูลครบถ้วนแล้ว โดยจะต้องมีการกระทำที่ชัดเจนที่เป็นการให้ความยินยอม เช่น การกดลิ้งหรือใส่เครื่องหมายถูกในกล่องข้อความ รวมทั้งต้องจัดให้มีช่องทางในการยกเลิกที่ง่ายและยกเลิกเมื่อใดก็ได้ PECR กำหนดข้อยกเว้นกรณีที่ไม่ต้องได้รับความยินยอมไว้ด้วย เช่น การใช้ session cookie ในการรักษาความปลอดภัยของข้อมูล หรือ load-balancing cookie สำหรับการทำให้แน่ใจว่าหน้าเว็ปสามารถแสดงผลได้อย่างรวดเร็ว (PECR Regulation ข้อ 6)
8. การทำการโฆษณาและการตลาด	- PECR บังคับใช้กับการทำโฆษณาและการตลาดแบบไม่พึงประสงค์เท่านั้น (ในลักษณะที่ไม่ได้เป็นการร้องขอเองโดยเฉพาะเจาะจงจากเจ้าของข้อมูล ซึ่ง ICO ให้ความเห็นว่าแม้องค์กรจะใช้ opt-in consent ก็ยังไม่ถือว่าเป็นการร้องขอเองโดยเฉพาะเจาะจงจากเจ้าของข้อมูล[48]) ทั้งทางโทรศัพท์ ข้อความ อีเมล และแฟกซ์ โดยองค์กรจะต้องได้รับความยินยอมก่อนจึงจะส่งสามารถส่งข้อความไปโฆษณาหรือทำการตลาดได้ และข้อความขอความยินยอมจะต้องแยกส่วนต่างหากจากนโยบายความเป็นส่วนตัวและระบุให้ชัดเจนเกี่ยวกับองค์กรที่จะส่งข้อความไปและช่องทางที่จะส่งและจะต้องจัดให้มีระบบในการแสดงเจตนาที่ชัดเจนผ่านการกระทำ เช่น การกดลิงก์หรือใส่เครื่องหมายถูกในกล่องข้อความ และหากมีการจ้างให้องค์กรอื่นดำเนินการจะต้องระบุภาระหน้าที่ในการปฏิบัติตาม PECR ในสัญญาจ้างให้ชัดเจน (PECR Regulation ข้อ 22-23)

[47] ICO,‘Data Protection Impact Assessments (DPIAs)’ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/> สืบค้นเมื่อ 11 พฤษภาคม 2567.

[48] Opt-in consent คือ การให้ความยินยอมที่จะต้องมีการกระทำที่เฉพาะเจาะจงแสดงให้เห็นเจตนาของผู้ให้ความยินยอม ตัวอย่างของกระทำดังกล่าวคือ การลงนามกำกับข้อความให้ความยินยอม. See ICO,‘What is valid consent?’ <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/>สืบค้นเมื่อ 11 พฤษภาคม 2567. And ICO,‘When is Marketing ‘Solicited’ and When is it ‘Unsolicited’?’<https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/electronic-and-telephone-marketing/#solicited>
สืบค้นเมื่อ 11 พฤษภาคม 2567.

เรื่อง	หลักกฎหมาย
9 .การประเมินผลกระทบด้านการคุ้มครองข้อมูลข้อมูล (Data Protection Impact Assessment)	- UK GDPR Art 64 กำหนดไว้ว่าการประมวลผลข้อมูลที่มีความเป็นไปได้ที่จะส่งผลให้เกิดความเสี่ยงสูง จำเป็นที่ต้องมีการประเมินผลกระทบด้านการคุ้มครองข้อมูล (DPIA) ซึ่ง ICO ได้ยกตัวอย่างไว้ในกรณีการประมวลผลข้อมูลของบุคคลที่เป็นกลุ่มเปราะบาง เช่น การประมวลผลข้อมูลของผู้เยาว์ในกรณีที่มีการนำเสนอบริการสารสนเทศ และการประมวลผลข้อมูลของลูกจ้างเนื่องจากลูกจ้างมีอำนาจที่ไม่เท่าเทียมกันกับนายจ้าง ทั้งสองกรณีถือเป็นการประมวลผลที่มีความเป็นไปได้ที่จะส่งผลให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูล จึงต้องจัดทำ DPIA[49]
10. การแจ้งรายละเอียดและข้อมูลการติดต่อDPO	- องค์กรจะต้องแจ้งรายละเอียดและช่องทางการติดต่อของ DPO เมื่อ 1) ติดต่อปรึกษา ICO ในเรื่อง DPIA ; 2) ทำหน้าที่ในฐานะเป็นผู้ควบคุมแจ้งข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยระบุไว้ใน Privacy Policy ; 3) ติดต่อ ICO ในเรื่องการจ่ายค่าธรรมเนียมการคุ้มครองข้อมูล (UK GDPR Art 64)

4. แนวทางการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในทวีปยุโรปสำหรับสำนักงานต่างประเทศของการท่องเที่ยวแห่งประเทศไทย

ภายหลังจากการศึกษาลักษณะของการดำเนินกิจกรรมต่างๆ ของ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และ ททท. สำนักงานลอนดอน และศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (GDPR) และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอันเป็นสถานที่ตั้งของสำนักงาน ททท. ดังกล่าวข้างต้นแล้ว ผู้เขียนพบว่าประเทศดังกล่าวนำบทบัญญัติของ GDPR มาเป็นต้นแบบในการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในของแต่ละประเทศ ดังนั้น กฎหมายภายในของแต่ละประเทศจึงมีหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เหมือนกัน ดังนั้น ททท. แต่ละสำนักงานสามารถนำความเห็นและคำแนะนำต่างๆ ของหน่วยงานกำกับดูแลให้มีการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (A29WP และ EDPB) มาเป็นแนวทางในการปรับใช้หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศนอกเหนือไปจากคำแนะนำของหน่วยงานกำกับดูแลเฉพาะของแต่ละประเทศได้ เช่น เรื่องข้อมูลส่วนบุคคล[50] เรื่องสถานะของผู้ควบคุมและผู้ประมวลผล[51] เรื่องขอบเขตการบังคับใช้

[49] ICO, 'Data Protection Impact Assessments (DPIAs)'<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/> สืบค้นเมื่อ 11 พฤษภาคม 2567.

[50] See A29WP, Opinion 4/2007 on The Concept of Personal Data (01248/07/EN WP 136 Adopted 20 June 2007). <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>สืบค้นเมื่อ 11 พฤษภาคม 2567.

[51] See EDPB, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR (Version 2.1 Adopted on 07 July 2021). < https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007 _controllerprocessor_ final_en.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.

กฎหมาย[52] เรื่องการแจ้งเตือนกรณีละเมิดข้อมูลส่วนบุคคล[53] เรื่องสิทธิของเจ้าของข้อมูลส่วนบุคคล[54] เรื่องความยินยอม[55] เรื่องการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม[56]แต่อย่างไรก็ตาม ผู้เขียนพบว่ากฎหมายภายในของแต่ละประเทศจะมีรายละเอียดบางประการที่มีความแตกต่างกันไป เช่น เกณฑ์อายุของผู้เยาว์ เกณฑ์การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ฯลฯ ดังนั้น ผู้เขียนจึงได้จัดทำคู่มือการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละสำนักงาน ซึ่งประกอบด้วยรายละเอียด 3 ส่วน กล่าวคือ ส่วนแรกจะเป็นการให้ความรู้เกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานดังกล่าวอยู่ภายใต้บังคับที่จะต้องปฏิบัติตาม (GDPR สำหรับ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และ UK GDPR สำหรับ ททท. สำนักงานลอนดอน และกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศอันเป็นสถานที่ตั้งของสำนักงานดังกล่าว) ส่วนที่สองจะเป็นแนวปฏิบัติทั่วไปสำหรับ ททท. ทั้ง 5 สำนักงาน ที่จะต้องยึดถือปฏิบัติตามให้เป็นไปตามแนวทางเดียวกัน ทั้งนี้เพื่อให้เกิดความสะดวกและเป็นการลดค่าใช้จ่ายให้กับ ททท. ในการบริหารจัดการข้อมูลให้เป็นไปตามนโยบายภายใต้หลักธรรมาภิบาลข้อมูล (data governance) ขององค์กร[57] ส่วนที่สามจะเป็นแนวปฏิบัติเฉพาะของแต่ละสำนักงาน แนวปฏิบัติดังกล่าวจะเป็นไปตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในของแต่ละประเทศอันเป็นสถานที่ตั้งของแต่ละสำนักงาน ซึ่งจะมีรายละเอียดเพิ่มเติมจากแนวปฏิบัติทั่วไปในส่วนที่สองและมีความแตกต่างกันไปในแต่ละสำนักงาน

ในส่วนนี้ ผู้เขียนจะนำเสนอข้อมูลบางส่วนในลักษณะเป็นตารางสรุปสาระสำคัญในส่วนของแนวปฏิบัติทั่วไปสำหรับการดำเนินกิจกรรมต่างๆ ที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม ททท. สำนักงานลอนดอน และตารางสรุปสาระสำคัญในส่วนของแนวปฏิบัติเฉพาะสำหรับแต่ละสำนักงาน ซึ่งมีรายละเอียดดังต่อไปนี้[58]

---

[52] See A29WP, Opinion 8/2010 on Applicable Law (0836-02/10/EN WP 179 Adopted 16 December 2010).< https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

[53] See EDPB, Guidelines 9/2022 on Personal Data Breach Notification under GDPR Version 2.0 Adopted 28 March 2023).<https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

[54] See EDPB, Guidelines 01/2022 on Data Subject Rights - Right of Access (Version 2.1 Adopted on 28 March 2023). < https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.

[55] See A29WP, Opinion 15/2011 on the Definition of Consent (01197/11/EN WP187 Adopted 13 July 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf > accessed 11 May 2024. and EDPB, Guidelines 05/2020 on Consent under Regulation 2016/679 (Version 1.1 Adopted on 4 May 2020). < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

[56] See EDPB, 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 Adopted on 14 February 2023) <https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567

[57] หลักธรรมาภิบาลข้อมูล (data governance) คือ หลักการกำกับดูแลข้อมูลเพื่อให้เกิดความปลอดภัย ความถูกต้องสมบูรณ์ และความพร้อมใช้งาน ททท. มีการกำหนดนโยบายและแนวทางในการบริหารจัดการข้อมูลของทั้งองค์กรเพื่อให้เป็นไปตามหลักดังกล่าว งานวิจัยนี้จะไม่ได้กล่าวถึงรายละเอียดในส่วนนี้เนื่องจากอยู่นอกขอบเขตของงานวิจัย

[58] การนำเสนอข้อมูลในส่วนนี้เป็นการนำเสนอข้อมูลในลักษณะภาพรวม เนื่องจากมีข้อจำกัดในเรื่องจำนวนหน้าของบทความและหน่วยงานสงวนสิทธิในการเปิดเผยข้อมูลบางส่วนเป็นการทั่วไป ซึ่งแนวทางในการปฏิบัติตามกฎหมายดังกล่าวเกิดขึ้นจากการศึกษาลักษณะของการประมวลผลข้อมูลในบริบทการทำงานของ ททท. กฎหมายคุ้มครองข้อมูลที่เกี่ยวข้อง คำแนะนำของหน่วยงานกำกับดูแลในแต่ละประเทศ และแนวทางการปรับใช้กฎหมายของ ททท. ซึ่งมุ่งสนับสนุนให้เกิดความเป็นมาตรฐานเดียวกันของแนวปฏิบัติของแต่ละสำนักงาน

กิจกรรม	แนวปฏิบัติทั่วไป
1. การเชิญผู้ประกอบการเข้าร่วมกิจกรรม Road Show	จัดทำแบบฟอร์มลงทะเบียน(ในรูปแบบ google form) ส่งไปโดยใช้อีเมลของสำนักงานพร้อมกับหนังสือเชิญเข้าร่วมงาน โดยระบุข้อความขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลชนิดพิเศษ แจ้งวัตถุประสงค์ของการประมวลผล และระบุข้อความขอความยินยอมแยกส่วนในการเปิดเผยข้อมูลการติดต่อให้กับผู้เข้าร่วมงานอื่นๆ แจ้งสิทธิและช่องทางในการถอนความยินยอม รวมทั้งใส่ลิ้งก์ของนโยบายความเป็นส่วนตัวซึ่งปรากฏหน้า website หลักของ ททท. / เก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงานและส่งรหัสการเข้าถึงให้แก่ผู้ที่มีสิทธิเข้าถึงฐานข้อมูลเท่านั้นรวมทั้งแจ้งกำหนดระยะเวลาที่สามารถเข้าถึงฐานข้อมูลดังกล่าวได้
2. การจัดกิจกรรม FAM Trip	จัดทำแบบฟอร์มลงทะเบียน(ในรูปแบบ google form) ระบุข้อความขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลและข้อมูลส่วนบุคคลชนิดพิเศษ ส่งไปโดยใช้อีเมลของสำนักงานพร้อมกับหนังสือเชิญเข้าร่วมงาน แจ้งวัตถุประสงค์ของการประมวลผลข้อมูล และระบุข้อความขอความยินยอมแยกส่วนในกรณีการเปิดเผยข้อมูลกับสายการบินและกรณีการโอนข้อมูลไปยังผู้ประกอบธุรกิจท่องเที่ยวในประเทศไทย แจ้งสิทธิและช่องทางในการถอนความยินยอม รวมทั้งใส่ลิ้งก์ของนโยบายความเป็นส่วนตัวซึ่งปรากฏที่หน้า website หลักของ ททท. / เก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงาน
3. การรับลงทะเบียนเพื่อจัดฝึกอบรม e -learning	จัดทำแบบฟอร์มลงทะเบียน(ในรูปแบบ google form) เข้าร่วมการฝึกอบรม ระบุข้อความขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคล แจ้งวัตถุประสงค์ของการประมวลผลข้อมูล แจ้งสิทธิและช่องทางในการถอนความยินยอม และระบุข้อความขอความยินยอมแยกส่วนในกรณีการส่งข่าวสารประชาสัมพันธ์ต่างๆ รวมทั้งใส่ลิ้งก์ของนโยบายความเป็นส่วนตัวซึ่งปรากฏหน้า website หลักของ ททท. / เก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงาน
4. การถ่ายภาพและบันทึกวีดิโอ	ในกรณีที่มีการส่งหนังสือเชิญเข้าร่วมงาน ให้ใช้อีเมลของสำนักงานและแจ้งรายละเอียดเกี่ยวกับการถ่ายภาพและ/หรือบันทึกวีดิโอในงานด้วย และในวันงานให้จัดทำป้ายแจ้งผู้เข้าร่วมงานว่าจะมีการถ่ายภาพและ/หรือบันทึกวิดีโอ และนำไปเผยแพร่เพื่อวัตถุประสงค์ใด โดยขอให้ผู้เข้าร่วมงานแจ้งเจ้าหน้าที่หากไม่ยินยอมให้ถ่ายภาพและ/หรือบันทึกวิดีโอ พร้อมทั้งแจ้งรายละเอียดช่องทางการติดต่อเจ้าหน้าที่ผู้รับผิดชอบ และใส่ QR Code ของนโยบายความเป็นส่วนตัวซึ่งปรากฏหน้า website หลักของ ททท. ไว้ที่ป้ายดังกล่าวด้วย / เก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงาน

กิจกรรม	แนวปฏิบัติทั่วไป
5. การรับสมัครสมาชิกทางเว็บไซต์และเก็บข้อมูลผู้ใช้งานบนเว็บไซต์	ระบุข้อความขอความยินยอมในการประมวลผลข้อมูลส่วนบุคคลในหน้ารับสมัครสมาชิกและระบุข้อความขอความยินยอมแยกส่วนในกรณีการส่งข่าวสารประชาสัมพันธ์ต่างๆ แจ้งวัตถุประสงค์ของการประมวลผลข้อมูล แจ้งสิทธิและช่องทางในการถอนความยินยอม รวมทั้งใส่ลิ้งก์ของนโยบายความเป็นส่วนตัวซึ่งปรากฏที่หน้า website หลักของ ททท. / เก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงาน/ จัดทำข้อความขอความยินยอมกรณีการเก็บข้อมูลคุกกี้ประเภทต่างๆ แจ้งวัตถุประสงค์ของการเก็บข้อมูล พร้อมใส่ลิ้งก์ของนโยบายการใช้งานคุ้กกี้ซึ่งปรากฏที่หน้า website หลักของ ททท./ หากมีการจ้างบริษัทให้เข้ามาดูแลเว็บไซต์หรือระบบ server ซึ่งทำให้บริษัทผู้รับจ้างสามารถเข้าถึงข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของ ททท. ได้ จะต้องมีการทำสัญญาประมวลผลข้อมูล (Data Processing Agreement) เพื่อกำหนดสถานะ หน้าที่และความรับผิดระหว่างกัน
6.การรับสมัครงาน	จัดทำแบบฟอร์มใบสมัครงาน(ในรูปแบบ google form) แจ้งวัตถุประสงค์ของการประมวลผลข้อมูล พร้อมใส่ลิ้งก์ของนโยบายความเป็นส่วนตัวซึ่งปรากฏที่หน้า website หลักของ ททท. / ใส่รหัสการเข้าถึงข้อมูลและเก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงาน
7.การทำคำสั่งจ้าง/สัญญาจ้าง	จัดทำสัญญาจ้างระหว่างททท.และลูกจ้าง ระบุรายละเอียดเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของฝ่ายทรัพยากรบุคคล และระบุรายละเอียดเกี่ยวกับการโอนข้อมูลไปยังททท. สำนักงานใหญ่ ประเทศไทย เพื่อทำคำสั่งจ้างและเพื่อจัดสวัสดิการต่างๆ ที่เกี่ยวข้อง/ ใส่รหัสการเข้าถึงข้อมูลและเก็บรักษาข้อมูลไว้ในระบบ server ของสำนักงาน

สำนักงาน ททท.	แนวปฏิบัติเฉพาะ
1.สำนักงานปารีส สาธารณรัฐฝรั่งเศส	- กรณีที่มีการเสนอบริการสารสนเทศแก่ผู้เยาว์ที่มีอายุน้อยกว่า 15 ปี จะต้องจัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์ - จะต้องมีการจัดทำเอกสารต่างๆ เป็นภาษาฝรั่งเศส เช่น นโยบายความเป็นส่วนตัว แบบขอความยินยอม สัญญาจ้างงาน สัญญาประมวลผลข้อมูล รวมทั้งภาษาที่ใช้บนหน้าเว็บไซต์ - จัดทำแบบขอความยินยอม เพื่อขอความยินยอมจากเจ้าของข้อมูลผู้ใช้งานเว็ปไซต์สำหรับการใช้งาน cookies ทุกประเภทก่อนการเก็บข้อมูลทุกครั้ง โดยจะต้องมีการขอความยินยอมใหม่ทุกปี
2. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี	- กรณีที่มีการเสนอบริการสารสนเทศแก่ผู้เยาว์ที่มีอายุน้อยกว่า 16 ปี จะต้องจัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์

สำนักงาน ททท.	แนวปฏิบัติเฉพาะ
2. สำนักงานแฟรงก์เฟิร์ต สหพันธ์สาธารณรัฐเยอรมนี (ต่อ)	- ติดต่อหน่วยงานกำกับดูแลเกี่ยวกับการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลประจำสำนักงาน - จัดทำ DPIA ในกรณีที่มีการโอนข้อมูลส่วนบุคคลของลูกจ้างและนักท่องเที่ยวมายังประเทศไทย - จัดทำแบบขอความยินยอม เพื่อขอความยินยอมจากเจ้าของข้อมูลผู้ใช้งานเว็ปไซต์สำหรับการใช้งาน cookies ประเภทที่มีการเก็บสถิติเพื่อนำข้อมูลไปวิเคราะห์ก่อนการเก็บข้อมูลทุกครั้ง - ก่อนการส่งอีเมลเพื่อการโฆษณาและการตลาดแบบตรง จะต้องได้รับอีเมลยืนยันการแจ้งขอรับข้อมูลจากผู้ขอรับข้อมูลก่อนทุกครั้ง ดังนั้นองค์กรจะต้องส่งอีเมลเพื่อขอความยินยอมในการบอกรับเป็นสมาชิกก่อนโดยให้มีการคลิกลิ้งก์เพื่อให้ความยินยอมในการเข้าเป็นสมาชิกในการรับข้อมูล และในอีเมลดังกล่าวจะต้องแจ้งที่อยู่ของอีเมลที่จะให้ผู้รับข้อมูลส่งอีเมลมาเพื่อแจ้งยืนยันการรับข้อมูลผ่านทางอีเมลซึ่งมีจะเนื้อหาเกี่ยวกับการโฆษณาและการตลาดแบบตรง โดยจะต้องแจ้งรายละเอียดต่างๆเกี่ยวกับสินค้าด้วยว่าเป็นสินค้าและบริการใดบ้าง
3.สำนักงานโรม สาธารณรัฐอิตาลี	- กรณีที่มีการเสนอบริการสารสนเทศแก่ผู้เยาว์ที่มีอายุน้อยกว่า 14 ปี จะต้องจัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์ - จัดทำ DPIA ในกรณีที่มีการประมวลผลข้อมูลของผู้เยาว์ในกรณีที่มีการนำเสนอบริการสารสนเทศ การประมวลผลข้อมูลไบโอเมตริกซ์ของลูกจ้าง การประมวลผลขอมูลส่วนบุคคลชนิดพิเศษหรือข้อมูลที่เกี่ยวข้องกับประวัติอาชญากรรมของลูกจ้างซึ่งมีความเชื่อมโยงกับข้อมูลส่วนบุคคลอื่นๆที่เก็บไว้สำหรับวัตถุประสงค์อื่น - จัดทำแบบขอความยินยอม เพื่อขอความยินยอมจากเจ้าของข้อมูลผู้ใช้งานเว็ปไซต์สำหรับการใช้งาน cookies ประเภทที่มีการเก็บสถิติเพื่อนำข้อมูลไปวิเคราะห์ก่อนการเก็บข้อมูลทุกครั้ง
4. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน	- กรณีที่มีการเสนอบริการสารสนเทศแก่ผู้เยาว์ที่มีอายุน้อยกว่า 13 ปี จะต้องจัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์ กรณีผู้เยาว์ที่อายุ 13-16 ปี แม้กฎหมายจะให้ประเมินเป็นรายกรณีแต่ผู้เขียนแนะนำให้จัดทำแบบขอความยินยอมเพื่อขอความความยินยอมจากบุคคลที่มีความรับผิดชอบในการใช้อำนาจปกครองผู้เยาว์เช่นเดียวกัน - จัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากเจ้าของข้อมูลเมื่อมีการประมวลผลเลขประจำตัวประชาชนและเลขประจำตัวผู้เสียภาษี เมื่อมีการจัดทำกิจกรรมที่ต้องมีการเก็บรวบรวมข้อมูลดังกล่าว เช่น การจัดกิจกรรม Fam trip

สำนักงาน ททท.	แนวปฏิบัติเฉพาะ
4. สำนักงานสตอกโฮล์ม ราชอาณาจักรสวีเดน (ต่อ)	- จัดทำแบบขอความยินยอม เพื่อขอความยินยอมจากเจ้าของข้อมูลผู้ใช้งานเว็ปไซต์สำหรับการใช้งาน cookies ประเภทที่มีการเก็บสถิติเพื่อนำข้อมูลไปวิเคราะห์ก่อนการเก็บข้อมูลทุกครั้ง - จัดทำ DPIA ในกรณีที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกจ้าง เนื่องจากเป็นข้อมูลของกลุ่มเปราะบาง ซึ่งใช้ในการประเมินผลการปฏิบัติงานและเป็นข้อมูลที่มีลักษณะส่วนตัวสูง มีการควบคุมกำกับดูแลอย่างเป็นระบบในเรื่องการใช้งานอินเตอร์เน็ตและอีเมลของลูกจ้าง รวมทั้งมีการเก็บข้อมูลไบโอเมติกของลูกจ้างเพื่อใช้ในการยืนยันตัวตนของลูกจ้าง
5. สำนักงานลอนดอน สหราชอาณาจักร	- กรณีที่มีการเสนอบริการสารสนเทศแก่ผู้เยาว์ที่มีอายุน้อยกว่า 13 ปี จะต้องจัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากผู้แทนโดยชอบธรรมของผู้เยาว์ - จัดทำ DPIA สำหรับการประมวลผลข้อมูลของผู้เยาว์ในกรณีที่มีการนำเสนอบริการสารสนเทศ และการประมวลผลข้อมูลของลูกจ้าง - จัดทำ APD สำหรับการประมวลผลข้อมูลชนิดพิเศษ ข้อมูลอาชญากรรม และการประมวลผลข้อมูลในบริบทของการจ้างงาน - ติดต่อหน่วยงาน ICO เพื่อหารือและดำเนินการเกี่ยวกับการจ่ายค่าธรรมเนียมการคุ้มครองข้อมูล รวมทั้งแจ้งรายละเอียดเกี่ยวกับ DPO แก่ ICO เพื่อลงทะเบียนสำหรับการจ่ายธรรมเนียมการคุ้มครองข้อมูล - จัดทำแบบขอความยินยอม เพื่อขอความยินยอมจากเจ้าของข้อมูลผู้ใช้งานเว็ปไซต์สำหรับการใช้งาน cookies ทุกประเภทก่อนการเก็บข้อมูลทุกครั้ง - จัดทำแบบขอความยินยอมเพื่อขอความยินยอมจากเจ้าของข้อมูลก่อนการส่งอีเมลเพื่อโฆษณาหรือทำการตลาดแบบตรงในทุกกรณีที่เจ้าของข้อมูลไม่ได้มีการร้องขอโดยเฉพาะเจาะจงให้มีการส่ง ซึ่งจะต้องทำแยกส่วนจากการขอความยินยอมเรื่องอื่นๆ และจะต้องให้มีการกดลิ้งหรือใส่เครื่องหมายถูกในกล่องข้อความในการให้ความยินยอม

5. บทสรุป

ททท. เป็นหน่วยงานรัฐวิสาหกิจภายใต้สังกัดกระทรวงการท่องเที่ยวและกีฬาที่มีบทบาทสำคัญในการส่งเสริมอุตสาหกรรมการท่องเที่ยวไทย ซึ่งเมื่อพิจารณาลักษณะของการดำเนินกิจกรรมต่างๆ ของ ททท. สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และททท. สำนักงานลอนดอนแล้วพบว่ามีความเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในหลายหลากกิจกรรม จึงทำให้ ททท. แต่ละสำนักงานตกอยู่ภายใต้บังคับที่จะต้องปฏิบัติตาม GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นกฎหมายภายในของประเทศอันเป็นสถานที่ตั้งของแต่ละสำนักงาน 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) ของสาธารณรัฐอิตาลี และ Lag (2018:218) med kompletterande bestämmelser till EU: sdataskyddsförordning (dataskyddslagen) หรือเรียกว่า Data Protection Act (2019:218) ของราชอาณาจักรสวีเดน รวมทั้ง ททท.

สำนักงานลอนดอน สหราชอาณาจักร จะอยู่ภายใต้บังคับที่จะต้องปฏิบัติตาม UK GDPR และ Data Protection Act 2018

จากการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้ว พบว่าแม้ว่ากฎหมายภายในของแต่ประเทศจะใช้หลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ GDPR เป็นแม่แบบในการยกร่างก็ตาม แต่ในบางกรณีก็จะมีการกำหนดรายละเอียดเพิ่มเติมที่มีความแตกต่างกันไปในแต่ละประเทศ ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ ททท. แต่ละสำนักงานจำเป็นจะต้องมีแนวปฏิบัติเฉพาะในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้ เพื่อเป็นการกำหนดแนวทางในการดำเนินกิจกรรมต่างๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตามหลักเกณฑ์ตามที่กฎหมายของแต่ละประเทศกำหนดไว้ ซึ่งผู้เขียนแนะนำให้ ททท สำนักงานปารีส ททท. สำนักงานแฟรงก์เฟิร์ต ททท. สำนักงานโรม ททท. สำนักงานสตอกโฮล์ม และททท. สำนักงานลอนดอน จัดทำคู่มือซึ่งกำหนดแนวปฏิบัติเฉพาะสำหรับแต่ละสำนักงาน ทั้งนี้ เพื่อสนับสนุนให้พนักงานและลูกจ้างของแต่ละสำนักงานมีความรู้ ความเข้าใจหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องและสามารถปฏิบัติตามกฎหมายได้อย่างถูกต้องและครบถ้วน ซึ่งการดำเนินการเหล่านี้จะสามารถลดความเสี่ยงจากการที่ททท.จะมีความรับผิดและต้องรับโทษตามกฎหมาย อันจะส่งผลกระทบทางลบต่อความน่าเชื่อถือ ชื่อเสียงของททท. และประเทศไทยต่อไป

บรรณานุกรม

กฎหมาย
ภาษาไทย

พระราชบัญญัติการท่องเที่ยวแห่งประเทศไทย พ.ศ. 2522.
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.

ภาษาต่างประเทศ

Bundesdatenschutzgesetz (BDSG).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services.

Decree No. 2019-341 of April 19, 2019 concerning the implementation of data processing involving the use of the personal identification number in the National Register of Individual Identification (RNIPP) or requiring consultation of this register.

Decree No. 2019-536 of May 29, 2019 issued for the application of Law No. 78-17 of January 6, 1978 concerning information technology, data files, and civil liberties.

French Act No. 2018-493 of 20 June 2018.

Lag (2018:218) med kompletterande bestämmelser till EU: sdataskyddsförordning (dataskyddslagen) .

Personal Data Protection Code (Legislative Decree no. 196 of 30 June 2003).

Privacy and Electronic Communications (EC Directive) Regulations 2003.

UK Data Protection Act 2018.

UK General Data Protection Regulation (Regulation (EU) (2016/679)).

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).

เอกสารอื่นๆ
ภาษาต่างประเทศ

A29WP, Opinion 4/2007 on The Concept of Personal Data (01248/07/EN WP 136 Adopted 20 June 2007)<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, Opinion 8/2010 on Applicable Law (0836-02/10/EN WP 179 Adopted 16 December 2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, Opinion 15/2011 on the Definition of Consent (01197/11/EN WP187 Adopted 13 July 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, Guidelines 05/2020 on Consent under Regulation 2016/679 (Version 1.1 Adopted on 4 May 2020)<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

EDPB, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR (Version 2.1 Adopted on 07 July 2021) <https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, 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 Adopted on 14 February 2023) <https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, Guidelines 01/2022 on Data Subject Rights - Right of Access (Version 2.1 Adopted on 28 March 2023) 2023 < https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, Guidelines 9/2022 on Personal Data Breach Notification under GDPR (Version 2.0 Adopted 28 March 2023) <https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf> สืบค้นเมื่อ 11 พฤษภาคม 2567.

ICO, 'Data Protection Impact Assessments (DPIAs)'<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/> สืบค้นเมื่อ 11 พฤษภาคม 2567.

--, 'What is valid consent?' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/> สืบค้นเมื่อ 11 พฤษภาคม 2567.

--,'When is Marketing 'Solicited' and When is it Unsolicited?' (ICO) <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/electronic-and-telephone-marketing/#solicited> สืบค้นเมื่อ 11 พฤษภาคม 2567.

IMY, List Regarding Data Protection Impact Assessments According to Article 35.4 of the Data Protection Regulation 2019 <https://www.imy.se/globalassets/dokument/ovrigt/list-regarding-data-protection-impact-assessments.pdf > สืบค้นเมื่อ 11 พฤษภาคม 2567.