การโอนข้อมูลส่วนบุคคลระหว่างประเทศ

International Data Transfer

ณัชพงษ์ สำราญ[1]

126/1 คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย ถนนวิภาวดีรังสิต แขวงสามเสนใน เขตดินแดง กรุงเทพมหานคร 10400 เมล์ติดต่อ: Nutchapong_sam@utcc.ac.th

Nutchapong Samran[2]

126/1, School of Law, University of the Thai Chamber of Commerce, Vibhavadi Rangsit Rd, Samsen Nai, Din Daeng, Bangkok, 10400, E-mail: Nutchapong_sam@utcc.ac.th

บทคัดย่อ

บทความวิจัยฉบับนี้ มีวัตถุประสงค์สำคัญเพื่อศึกษามาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมสำหรับประเทศไทย โดยเฉพาะในกรณีที่ต้องมีการโอนข้อมูลส่วนบุคคลระหว่างประเทศเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล โดยมุ่งศึกษาแนวทางการโอนข้อมูลส่วนบุคคลระหว่างประเทศตามกรอบความตกลงระหว่างประเทศที่มีลักษณะเป็น Soft Law คือ OECD Privacy Framework และ APEC Privacy Framework รวมทั้งความตกลงระหว่างประเทศที่มีลักษณะเป็น Hard Law ทั้งความตกลงระดับพหุพาคีและทวิภาคี ซึ่งได้แก่ The EU General Data Protection Regulation (GDPR) และ The EU-U.S. Privacy Shield รวมทั้งตัวอย่างมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของประเทศในอาเซียน คือ สิงคโปร์ เพื่อให้เห็นแนวปฏิบัติที่แตกต่างกัน ซึ่งจะเป็นประโยชน์ต่อการจัดทำข้อเสนอแนะสำหรับประเทศไทยในการจัดทำมาตรการทางกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลให้ได้มาตรฐานทัดเทียมนานาอารยประเทศต่อไป

คำสำคัญ: การโอนข้อมูลส่วนบุคคล ความเป็นส่วนตัว การคุ้มครองข้อมูลส่วนบุคคล

---

[1] รองศาสตราจารย์, อาจารย์ประจำ

[2] Associate professor, Lecturer.

Abstract

This research aims to find the proper legal measures for personal data protection in Thailand, especially in case of data transfer outside territory. By doing so, this paper studies the practice of data transferring in several legal frameworks. Some are International legal frameworks which are usually called soft Law, which are The OECD Privacy Framework and The APEC Privacy Framework. On the other hand, the examples of hard law are The EU General Data Protection Regulation (GDPR), The EU-U.S. Privacy Shield Framework and Singapore Personal Data Protection Act. In addition, the comparison of data transfer measures under several legal frameworks will be provided in order to find some recommendations for Thailand, where The Personal Data Protection Act is not available. Then, this study will introduce an updated, proper and standardized legal tool to protect personal data of Thais while data transfer is happening in the society.

Keywords: Data transfer, Privacy, Personal Data Protection

1. บทนำ

ในยุคเศรษฐกิจดิจิทัล (Digital Economy) ซึ่งเป็นยุคแห่งการขับเคลื่อนเศรษฐกิจของประเทศโดยการนำเอาไอทีหรือเทคโนโลยีดิจิทัลเข้ามาใช้เพื่อเพิ่มผลผลิต เพิ่มผลงาน โดยใช้เวลาน้อยลงและสร้างมูลค่าเพิ่มให้แก่สินค้าและบริการต่าง ๆ[3] ถือเป็นโอกาสที่ดีในการสร้างมูลค่าและโอกาสเติบโตให้กับธุรกิจ เนื่องจากเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วส่งผลให้พฤติกรรมของผู้บริโภคเปลี่ยนไป โดยเฉพาะเทคโนโลยีซึ่งก่อให้เกิดการเชื่อมต่อ (Connectivity) และเข้าถึง (Accessibility) ที่สะดวกรวดเร็ว[4] ส่งผลให้ผู้บริโภคสามารถเข้าถึงสินค้าและบริการต่าง ๆ ได้ง่ายขึ้นผ่านช่องทางออนไลน์โดยอาศัยอุปกรณ์อิเล็กทรอนิกส์ในรูปแบบต่าง ๆ ไม่ว่าจะเป็นคอมพิวเตอร์หรือโทรศัพท์มือถือ โดยกิจกรรมในโลกดิจิทัลหลายประเภทส่งผลให้ผู้บริโภคต้องมีการให้ข้อมูลส่วนบุคคลของตนแก่ผู้ที่ทำหน้าที่เก็บรวบรวมข้อมูล อีกทั้งยังก่อให้เกิดการเก็บรวบรวม การใช้ การประมวลผล และการโอนข้อมูลส่วนบุคคลไปยังหน่วยงานอื่นหรือต่างประเทศมากขึ้น โดยในปี พ.ศ. 2557 มีการโอนสินค้า บริการ และเงินข้ามพรมแดนคิดเป็นมูลค่าประมาณ 30 ล้านล้านดอล์ลาร์สหรัฐ โดย 12% ของการค้าสินค้าระหว่างประเทศนี้เกิดขึ้นจากช่องทางพาณิชย์อิเล็กทรอนิกส์ หรือ e-commerce เช่น Alibaba หรือ Amazon ซึ่งส่งผลให้ GDP ของสหรัฐอเมริกาเพิ่มสูงขึ้น ประมาณ 10% หรือคิดเป็นมูลค่า 7.8 ล้านล้านดอล์ลาร์สหรัฐ โดยการโอนข้อมูลคิดเป็นสัดส่วน ประมาณ 2.8 ล้านล้านดอล์ลาร์สหรัฐ[5]

ในขณะเดียวกันโลกดิจิทัลยังก่อให้เกิดกิจกรรมที่ไม่พึงประสงค์หลายประเภทโดยเฉพาะอาชญากรรมทางคอมพิวเตอร์ ทั้งนี้ จากข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พบว่า ในปี พ.ศ. 2560 ประเทศไทยเกิดภัยคุกคามทางคอมพิวเตอร์ รวมทั้งสิ้น 3,237 ครั้ง โดยเป็นภัยคุกคามประเภท Intrusion Attempts หรือการพยายามเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจำนวนมากที่สุด 939 ครั้ง ตามมาด้วยการฉ้อโกงและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจำนวน 841 และ 570 ครั้ง ตามลำดับ

---

[3] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), "เศรษฐกิจดิจิทัล Digital Economy," แก้ไขครั้งล่าสุด ม.ป.ป., สืบค้นเมื่อ 1 พฤศจิกายน 2560, https://www.etda.or.th/digital-economy.html

[4] สรัญญา จันทร์สว่าง, "รีเทลสู่ยุค'Digital Revolution' เชื่อมการค้าทั่วโลก," *กรุงเทพธุรกิจ*, 17 ตุลาคม 2560, สืบค้นเมื่อ 1 พฤศจิกายน 2560, http://www.bangkokbiznews.com/news/detail/777249

[5] UNCTAD, United Nations, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (Switzerland: United Nation Publication, 2016), 4, accessed November 1, 2017, http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

ตาราง 1 แสดงสถิติภัยคุกคามปี พ.ศ. 2560[6]

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Availability	100	218	212	0	0	9	1	0	0	0	0	0	**540**
Fraud	60	60	71	55	60	70	103	81	80	50	63	88	**841**
Information gathering	1	4	3	0	0	0	0	0	0	0	0	0	**8**
Information security	0	1	19	0	0	0	0	14	15	7	4	8	**68**
Intrusion Attempts	85	65	89	106	84	88	74	62	52	78	79	77	939
Intrusions	157	35	84	47	18	42	40	29	19	23	51	25	**570**
Malicious code	25	31	29	26	32	29	14	19	6	20	7	33	**271**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**428**	**414**	**507**	**234**	**194**	**238**	**232**	**205**	**172**	**178**	**204**	**231**	**3,237**

การเปลี่ยนแปลงและภัยคุกคามที่เกิดขึ้นส่งผลให้เจ้าของข้อมูลส่วนบุคคลเกิดความกังวลในความเป็นส่วนตัวและความปลอดภัยของข้อมูลส่วนบุคคลมากขึ้น ดังนั้นการยอมรับมาตรการบางประการเพื่อป้องกันอันตรายหรือผลกระทบจากเทคโนโลยีจึงเป็นสิ่งจำเป็นเพื่อคุ้มครองสิทธิในความเป็นส่วนตัว ซึ่งเป็นสิทธิของบุคคลตามหลักขั้นพื้นฐานของกฎหมายที่จะอยู่ตามลำพังโดยปราศจากการรบกวนหรือสอดแทรกจากผู้อื่นที่ทำให้เกิดความเดือดร้อนรำคาญใจ เสียหาย อับอาย หรือการแสวงหาประโยชน์โดยมิชอบ[7] โดยสิทธิในความเป็นส่วนตัวนี้เป็นสิทธิขั้นพื้นฐานที่ได้รับการรับรองไว้ในข้อ 12 แห่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) ที่กำหนดให้ “บุคคลใดจะถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองของกฎหมายต่อการแทรกแซงสิทธิหรือการลบหลู่ดังกล่าวนั้น”[8] โดยประเทศไทยได้รับหลักการดังกล่าวมาบัญญัติไว้ในมาตรา 32 แห่งรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 ด้วย นอกจากนี้ ในส่วนของการคุ้มครองข้อมูลส่วนบุคคลฝ่ายกฎหมายระหว่างประเทศขององค์การรัฐอเมริกัน (The Organization of American State)

[6] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), “สถิติภัยคุกคาม,” แก้ไขครั้งล่าสุด ม.ป.ป., สืบค้นเมื่อ 1 พฤศจิกายน 2560, https://www.thaicert.or.th/statistics/statistics2017.html

[7] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), “สิทธิในความเป็นส่วนตัว (Right of privacy),” แก้ไขครั้งล่าสุด ม.ป.ป., สืบค้นเมื่อ 1 พฤศจิกายน 2560, https://www.etda.or.th/terminology-detail/1208.html

[8] กรมองค์การระหว่างประเทศ, กระทรวงการต่างประเทศ, *ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน* (กรุงเทพฯ: กรมองค์การระหว่างประเทศ กระทรวงการต่างประเทศ, 2551), 23, สืบค้นเมื่อ 2 พฤศจิกายน 2560, http://humanrights.mfa.go.th/upload/pdf/udhr-th-en.pdf

ได้อธิบายการคุ้มครองข้อมูลส่วนบุคคลไว้ว่าเป็นการคุ้มครองบุคคลจากการใช้ข้อมูลส่วนบุคคลโดยมิชอบของผู้ประมวลผลข้อมูลส่วนบุคคล[9] ซึ่งถือเป็นการคุ้มครองสิทธิในความเป็นส่วนตัวของปัจเจกชนรูปแบบหนึ่ง อีกทั้งสหภาพยุโรปยังได้กำหนดให้การคุ้มครองข้อมูลส่วนบุคคลเป็นส่วนหนึ่งของการคุ้มครองสิทธิในความเป็นส่วนตัว ซึ่งได้รับการรับรองไว้ในมาตรา 8 แห่งอนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights: EUCHR)[10] ทั้งนี้ ในส่วนของประเทศไทย รัฐธรรมนูญของประเทศไทยได้กำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลไว้อย่างชัดเจน กล่าวคือ กำหนดให้การนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ จะกระทำมิได้ เว้นแต่โดยอาศัยอำนาจตามกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ[11]

อย่างไรก็ดี หากพิจารณาในบริบทของต่างประเทศ จะพบว่า กฎหมายคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศต่างก็กำหนดระดับในการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันไป บางประเทศมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เคร่งครัด บางประเทศมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่ยังไม่เคร่งครัดมากนัก และหลายประเทศยังไม่มีมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคล การที่ระดับการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศมีความแตกต่างกันก่อให้เกิดความไม่เท่าเทียมในการบริหารจัดการกับข้อมูลส่วนบุคคล อีกทั้งมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในระดับที่ไม่เหมาะสมหรือเพียงพออาจส่งผลกระทบต่อการค้าระหว่างประเทศ โดยเฉพาะการลดความเชื่อมั่นของผู้บริโภค ในขณะที่การคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวดเกินไปย่อมเป็นอุปสรรคในการประกอบธุรกิจซึ่งส่งผลกระทบโดยตรงต่อการพัฒนาเศรษฐกิจของประเทศ นอกจากนี้หากพิจารณาสถานการณ์ในปัจจุบันจะพบว่าประเทศไทยยังคงไม่มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปเนื่องจากยังอยู่ระหว่างการพิจารณาจัดทำกฎหมายฉบับดังกล่าว อันส่งผลให้ในปัจจุบันประเทศไทยยังคงไม่มีมาตรการทางกฎหมายในการกำกับดูแลการโอนข้อมูลส่วนบุคคลระหว่างประเทศ และเนื่องจากเมื่อวันที่ 16 เมษายน พ.ศ. 2559 รัฐสภาสหภาพยุโรปได้มีมติเห็นชอบมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่เรียกว่า The EU General Data Protection Regulation (GDPR) ซึ่งจะมีผลใช้บังคับในวันที่ 25 พฤษภาคม พ.ศ. 2561[12] อันจะส่งผลกระทบโดยตรงกับการประกอบธุรกิจการค้าระหว่างประเทศ ไม่ว่า

[9] The Organization of American State, "Data Protection," last modified n.d., accessed April 27, 2018, http://www.oas.org/dil/data_protection_privacy_habeas_data.htm

[10] Joint Committee on Human Rights, *Data Protection and Human Rights* (United Kingdom: The Stationery OYce Limited, 2008), 7.

[11] รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560, *ราชกิจจานุเบกษา* เล่มที่ 134 ตอนที่ 40 ก (6 เมษายน 2560): 9.

[12] Trunomi, "GDPR Portal: Site Overview," last modified n.d., accessed November 2, 2017, https://www.eugdpr.org/

จะเป็นการโอนข้อมูลภายในองค์กรเดียวกันที่ไม่ได้ตั้งอยู่ในประเทศเดียวกัน การโอนข้อมูลไปยังองค์กรอื่นที่ตั้งอยู่ในต่างประเทศ หรือการโอนข้อมูลเพื่อประโยชน์ในการประมวลผลหรือการจัดเก็บฐานข้อมูลในต่างประเทศ เช่น ธุรกิจข้ามชาติซึ่งจะต้องโอนข้อมูลระหว่างบริษัทลูกหรือพันธมิตรทางธุรกิจ (business partner) ที่ให้บริการจัดเก็บหรือประมวลผลข้อมูลเพื่อสร้างมูลค่าเพิ่มให้กับธุรกิจอื่น ๆ ในห่วงโซ่อุปทาน[13] ส่งผลให้ผู้ประกอบการที่มีความจำเป็นต้องโอนข้อมูลส่วนบุคคลจากสหภาพยุโรปมายังประเทศไทยจะต้องให้ความสำคัญกับกฎหมายฉบับนี้ โดยเฉพาะในตลาดการค้าบริการที่ข้อมูลส่วนบุคคลเป็นปัจจัยสำคัญในการดำเนินธุรกิจ เช่น ธุรกิจการท่องเที่ยว ซึ่งรวมไปถึงธุรกิจโรงแรม สายการบิน และไกด์นำเที่ยว ที่จะต้องเก็บ บันทึก หรือโอนข้อมูลส่วนบุคคลของผู้ที่มาใช้บริการ ไม่ว่าจะเป็น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ หมายเลขบัตรเครดิต ซึ่งถือว่าเป็นข้อมูลส่วนบุคคลชนิดพิเศษ (sensitive data) ที่จะต้องได้รับการคุ้มครองตามหลักเกณฑ์ของสหภาพยุโรปหากมีการโอนข้อมูลระหว่างประเทศ นอกจากนี้ธุรกิจการบริการด้านสุขภาพโดยเฉพาะการให้บริการที่นำเทคโนโลยีสารสนเทศมาประยุกต์ใช้กับงานสาธารณสุข หรือ e-health ซึ่งมีการบันทึกข้อมูลด้านสุขภาพประวัติการรักษาพยาบาลของผู้ป่วย[14] และธุรกิจเทคโนโลยีสารสนเทศที่ให้บริการผ่านเครือข่ายสังคมออนไลน์ แอพพลิเคชั่นบนอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ และการให้บริการ cloud computing ที่ให้บริการการเชื่อมโยง ประมวลผลและจัดเก็บข้อมูลแก่บุคคลที่มีถิ่นพำนักในสหภาพยุโรป ย่อมได้รับผลกระทบจากมาตรการทางกฎหมายฉบับดังกล่าวด้วย โดยผู้ประกอบการและผู้มีส่วนเกี่ยวข้องควรศึกษาหลักเกณฑ์ต่าง ๆ ในการคุ้มครองข้อมูลส่วนบุคคลที่ปรากฏใน GDPR เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับการประกอบธุรกิจของตน ในขณะที่รัฐบาลเองก็มีหน้าที่สร้างความมั่นใจให้กับผู้ประกอบการและอารยประเทศด้วยการกำหนดมาตรฐานการโอนข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอ ดังนั้น การศึกษาแนวทางการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะการกำหนดมาตรการเพื่อคุ้มครองการโอนข้อมูลส่วนบุคคลระหว่างประเทศจึงเป็นสิ่งจำเป็น เพื่อจัดทำเป็นข้อเสนอแนะสำหรับประเทศไทยในการกำหนดมาตรการทางกฎหมายที่เหมาะสมสำหรับให้ภาคเอกชนนำไปปฏิบัติตาม เพื่อไม่ให้ต่างชาติใช้ข้ออ้างของการไม่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอของประเทศไทยในการจำกัดการโอนข้อมูลและกีดกันทางการค้ากับประเทศไทยในอนาคต

---

[13] ทีมงาน ThaiEurope.net, “กฎใหม่โอนข้อมูลส่วนบุคคลระหว่างประเทศ กระทบห่วงโซ่อุปทานโลก,” *กรุงเทพธุรกิจ*, 21 มีนาคม 2559, สืบค้นเมื่อ 1 พฤศจิกายน 2560, http://www.bangkokbiznews.com/blog/detail/637251

[14] ทีมงาน ThaiEurope.net, “กฎใหม่โอนข้อมูลส่วนบุคคลระหว่างประเทศ กระทบห่วงโซ่อุปทานโลก.”

2. หลักการคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาวิจัยพบว่าในปัจจุบันกรอบความตกลงระหว่างประเทศในเรื่องการคุ้มครองข้อมูลส่วนบุคคลไม่ว่าจะเป็น The OECD Privacy Framework[15] หรือ The APEC Privacy Framework[16] ต่างกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญร่วมกันไว้ ดังต่อไปนี้

2.1 หลักข้อจำกัดในการเก็บรวบรวมข้อมูล (Collection Limitation Principle)

การเก็บรวบรวมข้อมูลส่วนบุคคลควรมีข้อจำกัดและต้องเป็นไปอย่างเหมาะสม โดยใช้วิธีที่ชอบด้วยกฎหมายและสมเหตุสมผล ซึ่งเจ้าของข้อมูลส่วนบุคคลต้องรับรู้หรือให้ความยินยอมด้วย

2.2 หลักคุณภาพของข้อมูล (Data Quality Principle)

ข้อมูลส่วนบุคคลที่ถูกจัดเก็บจะต้องเกี่ยวข้องกับวัตถุประสงค์ในการใช้ข้อมูลนั้นตามความจำเป็น ทั้งยังต้องเป็นข้อมูลที่ถูกต้อง สมบูรณ์ และทันสมัย

2.3 หลักวัตถุประสงค์ที่เฉพาะเจาะจง (Purpose Specification Principle)

ในการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องแจ้งวัตถุประสงค์ที่มีความเฉพาะเจาะจงให้เจ้าของข้อมูลส่วนบุคคลรับทราบไม่ช้าไปกว่าขณะเก็บรวบรวมข้อมูลนั้น และการใช้ข้อมูลต้องเป็นไปตามวัตถุประสงค์หรือเป็นกรณีอื่นใดที่ไม่ขัดกับวัตถุประสงค์ดังกล่าวตามที่ได้มีการแจ้งเปลี่ยนแปลงวัตถุประสงค์

2.4 หลักข้อจำกัดในการใช้ข้อมูล (Use Limitation Principle)

ข้อมูลส่วนบุคคลจะต้องไม่ถูกเปิดเผยหรือต้องไม่ถูกใช้เพื่อวัตถุประสงค์อื่นใดนอกจากที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคล เว้นแต่ (1) เจ้าของข้อมูลส่วนบุคคลให้ความยินยอม หรือ (2) เป็นไปตามกฎหมาย

2.5 หลักการรักษาความปลอดภัย (Security Safeguards Principle)

ข้อมูลส่วนบุคคลควรได้รับการเก็บรักษาโดยใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันความเสี่ยง ความเสียหาย การเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งการทำลาย การใช้ การแก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

---

[15] OECD, *The OECD Privacy Framework* (n.p.: OECD Publishing, 2013), 14-15, accessed November 2, 2017, http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf

[16] APEC, *APEC Privacy Framework (2015)* (Singapore: APEC Secretarial, 2017), 10-22, accessed November 2, 2017, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

2.6 หลักการมีส่วนร่วมของบุคคล (Individual Participation Principle)

เจ้าของข้อมูลควรมีสิทธิ

2.6.1 ได้รับข้อมูลจากผู้ควบคุมข้อมูลส่วนบุคคล หรือได้รับการยืนยันว่าผู้ควบคุมข้อมูลส่วนบุคคลมีข้อมูลที่เกี่ยวข้องกับตนหรือไม่

2.6.2 ได้รับการติดต่อภายในเวลาที่เหมาะสม โดยเสียค่าธรรมเนียมที่ไม่มากเกินสมควร ด้วยวิธีการที่เหมาะสม และในรูปแบบที่เข้าใจง่าย

2.6.3 ได้รับทราบเหตุผลหากถูกปฏิเสธคำขอตามข้อ 2.6.1 และ ข้อ 2.6.2 ทั้งยังมีสิทธิโต้แย้งการปฏิเสธดังกล่าว

2.6.4 สิทธิโต้แย้งข้อมูลที่เกี่ยวข้องกับตน และในกรณีที่การโต้แย้งเป็นผล เจ้าของข้อมูลส่วนบุคคลมีสิทธิได้รับการแก้ไขข้อมูลให้ถูกต้อง สมบูรณ์ หรือปรับปรุงข้อมูล

2.7 หลักความรับผิดชอบ (Accountability Principle)

ผู้ควบคุมข้อมูลส่วนบุคคลควรมีความรับผิดชอบในการปฏิบัติตามมาตรการที่จะส่งผลกระทบต่อหลักการคุ้มครองข้อมูลส่วนบุคคลข้างต้น ซึ่งรวมถึงการแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงวัตถุประสงค์ในการเก็บรวบรวมข้อมูล บุคคลหรือองค์กรที่ข้อมูลส่วนบุคคลดังกล่าวจะถูกเปิดเผยให้ได้รับทราบ ตัวตนและที่อยู่ของผู้ควบคุมข้อมูล รวมถึงข้อมูลสำหรับการติดต่อ ตัวเลือก วิธีการในการจำกัดการใช้และการเปิดเผยข้อมูลส่วนบุคคล รวมทั้งการเข้าถึงและแก้ไขข้อมูลส่วนบุคคลและการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลด้วย

โดยหลักการดังกล่าวข้างต้นยังปรากฏอยู่ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป คือ The EU General Data Protection Regulation (GDPR)[17] และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Act, 2012)[18] ด้วย อย่างไรก็ดี เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ GDPR และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์เป็นกฎหมายภายในที่มีสภาพบังคับที่ชัดเจน คือ มีลักษณะเป็น Hard Law จึงส่งผลให้กฎหมายทั้งสองฉบับมีการกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลที่เคร่งครัดมากกว่า The OECD Privacy Framework และ The APEC Privacy Framework ซึ่งเป็นความตกลงระหว่างประเทศที่มีลักษณะเป็น Soft Law โดยเฉพาะใน GDPR

[17] 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) 2016, Official Journal of the European Union (April 27, 2016): 35-66.

[18] Personal Data Protection Act 2012, Republic of Singapore Government gazette No.26 of 2012 (December 7, 2012): 17-26

ที่มีการกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลไว้อย่างละเอียด โดยทั้งในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ต่างกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญเพิ่มเติม ดังนี้

2.7.1 หลักการเก็บข้อมูลที่จำกัด (Storage limitations)

ข้อมูลส่วนบุคคลควรเก็บรักษาในรูปแบบที่สามารถระบุเจ้าของข้อมูลส่วนบุคคลได้โดยต้องไม่เก็บไว้นานเกินความจำเป็นตามวัตถุประสงค์ในการประมวลผลข้อมูลนั้น เว้นแต่เป็นไปตามที่กฎหมายกำหนด และต้องทำลายข้อมูลส่วนบุคคลด้วยความระมัดระวังเมื่อไม่จำเป็นต้องใช้ข้อมูลดังกล่าวอีกต่อไป

2.7.2 การกำหนดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data protection officer)

โดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะทำหน้าที่ควบคุมดูแลให้หน่วยงานดำเนินการตามแนวทางการคุ้มครองข้อมูลส่วนบุคคลใน GDPR

2.7.3 การกำหนดโทษสำหรับการฝ่าฝืนไม่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Penalty)

โดยหากผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้ใน GDPR อาจได้รับโทษปรับสูงสุดถึง 4% ของผลประกอบการทั่วโลกหรือ 20 ล้านยูโร แล้วแต่จำนวนใดจะสูงกว่ากัน[19] ในขณะที่โทษสำหรับผู้ควบคุมข้อมูลส่วนบุคคลที่ฝ่าฝืนไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์อาจเป็นไปได้ทั้งโทษปรับหรือจำคุก โดยอาจถูกจำคุกไม่เกินสามปี หรือปรับไม่เกิน 10,000 ดอลลาร์สิงคโปร์ หรือทั้งจำทั้งปรับ[20] เป็นต้น

2.7.4 การรับรองหลัก Binding Corporate Rules (BCRs)

การรับรองหลัก Binding Corporate Rules เป็นการยอมรับมาตรการสำหรับการโอนข้อมูลส่วนบุคคลระหว่างกลุ่มองค์กรธุรกิจ โดยหลัก BCRs จะมีผลผูกพันทางกฎหมายและใช้บังคับได้ในประเทศสมาชิกของกลุ่มผู้ประกอบการ โดยแต่ละกลุ่มองค์กรธุรกิจจะต้องยอมรับหลักการคุ้มครองข้อมูลส่วนบุคคลและต้องยึดถือหลักการดังกล่าวเป็นมาตรฐานเพื่อใช้บังคับโดยทั่วกัน

---

[19] 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) 2016, Official Journal of the European Union (27 April, 2016): 83.

[20] Personal Data Protection Act 2012, Republic of Singapore Government gazette No.26 of 2012 (December 7, 2012): 49.

นอกจากนี้ GDPR ยังได้กำหนดหลักการคุ้มครองข้อมูลส่วนบุคคลเพิ่มเติมจากกรอบความตกลงระหว่างประเทศทั้งสองฉบับข้างต้นและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ เช่น

1) หลักการออกแบบเพื่อคุ้มครองข้อมูลส่วนบุคคล (Privacy by design) ซึ่งเป็นการยอมรับแนวปฏิบัติที่ดีในการคุ้มครองข้อมูลส่วนบุคคล โดยสนับสนุนให้ผู้ควบคุมข้อมูลส่วนบุคคลนำวิธีการทางเทคนิคหรือมาตรการต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลมาใช้ เพื่อแสดงว่าตนเองให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลในขณะที่ทำการประมวลผลข้อมูลส่วนบุคคล

2) หลักหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคล (Role of data processor) โดยกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับผิดชอบในการประมวลผลข้อมูล ซึ่งรวมถึงการบันทึกขั้นตอนการประมวลผลข้อมูลไว้เป็นลายลักษณ์อักษร การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือการแจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงการละเมิดข้อมูลส่วนบุคคลโดยไม่ชักช้า เป็นต้น

3) หลักการแจ้งการละเมิดข้อมูลส่วนบุคคล (Data breach notification) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าและหากเป็นไปได้ควรดำเนินการภายใน 72 ชั่วโมง นับจากทราบการละเมิดข้อมูลนั้น และอาจต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้าด้วยหากเข้าเงื่อนไขตามที่กฎหมายกำหนด

ในขณะที่ Personal Data Protection Act, 2012 ของสิงคโปร์ ได้กำหนดหลักการห้ามโทร (Do-Not-Call: DNC) ไว้ด้วย ซึ่งถือเป็นหลักการที่แตกต่างจากกรอบการคุ้มครองข้อมูลส่วนบุคคลฉบับอื่น ๆ โดยหลักการนี้จะห้ามการส่งข้อความทางการตลาดให้แก่บุคคลทั่วไปที่ได้ลงทะเบียนไว้ไม่ว่าจะเป็นข้อความเสียง ข้อความตัวอักษร หรือโทรสาร เว้นแต่ได้รับความยินยอมที่ชัดแจ้งและไม่คลุมเครือจากบุคคลนั้น

3. หลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

จากการศึกษาวิจัยพบว่ากรอบความตกลงระหว่างประเทศในเรื่องการคุ้มครองข้อมูลส่วนบุคคลไม่ว่าจะเป็น The OECD Privacy Framework หรือ The APEC Privacy Framework ต่างเสนอแนะให้ประเทศสมาชิกความตกลงฉบับนั้น ๆ งดเว้นการกำหนดข้อจำกัดในการโอนข้อมูลส่วนบุคคลจากประเทศตนเองไปยังประเทศอื่น หากประเทศอื่นนั้นยอมรับและนำหลักการคุ้มครองข้อมูลส่วนบุคคลตามกรอบความตกลงฉบับนั้น ๆ ไปใช้เช่นเดียวกันหรือประเทศอื่นนั้นมีมาตรการรักษาความปลอดภัยที่เพียงพอ แต่ประเทศสมาชิกอาจกำหนดข้อยกเว้นในการโอนข้อมูลส่วนบุคคลได้ แต่ข้อยกเว้นดังกล่าวต้องเหมาะสมกับความเสี่ยงที่มีอยู่ในปัจจุบันโดยคำนึงถึงความอ่อนไหวของข้อมูล วัตถุประสงค์และบริบทในการประมวลผลข้อมูลนั้น ในขณะที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป คือ The EU General Data Protection Regulation (GDPR) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Act, 2012) ต่างกำหนดหลักการไว้คล้ายคลึงกันว่าองค์กรหรือหน่วยงานในสหภาพยุโรปหรือในประเทศสิงคโปร์ไม่ควรโอนข้อมูลส่วนบุคคลไปยังประเทศอื่นหรือบริเวณอื่นใด เว้นแต่เป็นการดำเนินการตามเงื่อนไขที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ หากเป็น GDPR การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะทำได้ก็ต่อเมื่อ (1) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้มีคำวินิจฉัยว่าประเทศนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ หรือ (2) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม โดยมาตรการรักษาความปลอดภัยที่เหมาะสมนั้นอาจเกิดขึ้นตามกฎหมาย หรือหลักการ Binding Corporate Rules หรือเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนำมาใช้ หรือเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานนำมาใช้และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้การรับรอง หรือเป็นมาตรการตาม Code of conduct ของหน่วยงาน หรืออาจเป็นเครื่องมืออื่นที่ใช้รับรองการคุ้มครองข้อมูลส่วนบุคคล เช่น เครื่องหมายรับรอง เป็นต้น หรือ (3) ในกรณีที่ไม่ปรากฏทั้งระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือมาตรการรักษาความปลอดภัยที่เหมาะสม การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะสามารถเกิดขึ้นได้เฉพาะในกรณีต่อไปนี้

1) เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างชัดแจ้งภายหลังจากที่ได้รับทราบความเสี่ยงที่อาจเกิดขึ้นจากการโอนข้อมูลส่วนบุคคลนั้น

2) การโอนข้อมูลส่วนบุคคลมีความจำเป็น เพื่อเป็นการดำเนินการตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล

3) การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการสิ้นสุดหรือดำเนินการตามสัญญา

4) การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการดำเนินคดีตามกฎหมาย

5) การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นใด

6) เมื่อเป็นการโอนข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลทางทะเบียน เพื่อให้ข้อมูลแก่สาธารณะและได้รับการเปิดเผยเพื่อการประชุมปรึกษาหารือ

อีกทั้ง GDPR ยังกำหนดเพิ่มเติมแนวทางการบังคับตามคำพิพากษาของศาลต่างประเทศไว้ด้วย กล่าวคือในกรณีที่ศาลของต่างประเทศได้มีคำพิพากษาให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในสหภาพยุโรปโอนหรือเปิดเผยข้อมูลส่วนบุคคลใด ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจำเป็นต้องดำเนินการตามคำพิพากษาดังกล่าวเฉพาะในกรณีที่การบังคับการตามคำพิพากษานี้อยู่บนพื้นฐานของสัญญาระหว่างประเทศที่มีผลบังคับใช้ระหว่างประเทศนั้นกับประเทศสมาชิกสหภาพยุโรปเท่านั้น เช่น สนธิสัญญาการให้ความช่วยเหลือทางกฎหมายระหว่างกัน[21]

ในขณะที่ Personal Data Protection Act, 2012 ของสิงคโปร์ กำหนดให้องค์กรที่อยู่ในต่างประเทศซึ่งข้อมูลส่วนบุคคลได้ถูกโอนไปนั้นมีหน้าที่ตามกฎหมายที่จะต้องจัดให้มีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลเทียบเท่ากับกฎหมายฉบับนี้ โดยหน้าที่ตามกฎหมายนั้นอาจเป็นหน้าที่ที่เกิดจากบทบัญญัติแห่งกฎหมาย หรือสัญญา หรือตามหลัก Binding Corporate Rules หรือหลักการอื่น ๆ และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจแจ้งเป็นลายลักษณ์อักษรให้องค์กรใด ๆ ทราบว่าองค์กรนั้นอาจได้รับยกเว้นไม่ต้องดำเนินการตามที่พระราชบัญญัติฉบับนี้กำหนดไว้ โดยอาจมีการกำหนดเงื่อนไขสำหรับข้อยกเว้นดังกล่าวเป็นลายลักษณ์อักษรโดยไม่จำเป็นต้องตราเป็นพระราชกิจจานุเบกษา และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจเพิกถอนข้อยกเว้นนั้นเมื่อใดก็ได้ นอกจากนี้ ทั้ง GDPR และ Personal Data Protection Act, 2012 ของสิงคโปร์ยังกำหนดโทษปรับสำหรับกรณีที่มีการโอนข้อมูลส่วนบุคคลฝ่าฝืนหลักการที่ปรากฏในกฎหมายทั้งสองฉบับด้วย

นอกจากนี้ หากพิจารณาความตกลงระหว่างประเทศระหว่างสหภาพยุโรปและสหรัฐอเมริกาที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศ จะพบว่าทั้งสองภูมิภาคเคยมีความตกลงร่วมกันในเรื่องดังกล่าวตั้งแต่ปี พ.ศ. 2543 เรียกว่าความตกลง Safe Harbour อย่างไรก็ดีในปี พ.ศ. 2558 ศาลยุติธรรมแห่งสหภาพยุโรปได้มีคำพิพากษาในคดี

[21] Leonie Power, "Getting to Know the GDPR, Part 9 – Data transfer restrictions are here to stay, but so are BCR," last modified February 24, 2016, accessed November 2, 2017, http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/

C-362/14 ระหว่าง Maximillian Schrems และ Data Protection Commissioner ให้ความตกลง Safe Habour เป็นโมฆะ เนื่องจากความตกลง Safe Habour ไม่ได้ใช้บังคับกับการดำเนินการของหน่วยงานภาครัฐของสหรัฐฯ เพราะหน่วยงานภาครัฐของสหรัฐฯ ยังสามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยการอ้างเหตุผลเรื่องความมั่นคงและประโยชน์สาธารณะ ซึ่งเป็นการแทรกแซงสิทธิขั้นพื้นฐานของประชาชนอันขัดกับหลักการใน Safe Habour

ภายหลังจากที่ศาลยุติธรรมแห่งสหภาพยุโรปได้มีคำพิพากษาดังกล่าว รัฐบาลของสหรัฐฯ และผู้แทนจากสหภาพยุโรปได้ร่วมกันจัดทำความตกลงที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เหมาะสมฉบับใหม่ เรียกว่า The EU-U.S. Privacy Shield ซึ่งมีผลใช้บังคับตั้งแต่วันที่ 1 สิงหาคม พ.ศ. 2559 โดยการเข้าร่วมความตกลง The EU-U.S. Privacy Shield นี้จะเป็นไปโดยความสมัครใจของผู้ประกอบการในสหรัฐฯ โดยผู้ประกอบการที่สมัครใจดำเนินการตามความตกลงดังกล่าวจะต้องได้รับการรับรองจากกระทรวงพาณิชย์ของสหรัฐฯ ทั้งยังต้องยอมรับการดำเนินการตามความตกลงฉบับนี้อย่างชัดแจ้งต่อสาธารณะชน[22] ซึ่งรวมถึงการจัดทำแนวนโยบายขององค์กรในการรักษาความปลอดภัยในข้อมูลส่วนบุคคลหรือ Privacy policy ด้วย โดยความตกลง The EU-U.S. Privacy Shield จะให้ความสำคัญกับหลักการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ 7 ประการ ได้แก่ หลักการแจ้งให้ทราบ (Notice) หลักทางเลือก (Choice) หลักความรับผิดชอบ (Accountability) หลักความปลอดภัย (Security) หลักความถูกต้องของข้อมูลและวัตถุประสงค์ที่จำกัด (Data Integrity and Purpose Limitation) หลักการเข้าถึงข้อมูล (Access) หลักการชดใช้ค่าสินไหมทดแทน หลักการบังคับการตามกฎหมาย และหลักความรับผิด (Recourse, Enforcement, and Liability) โดยเฉพาะในการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่สาม ผู้ประกอบการจะต้องตกลงกับบุคคลที่สามโดยระบุให้การโอนข้อมูลส่วนบุคคลไปเพื่อการประมวลผลข้อมูลนั้น จะต้องเป็นการประมวลผลข้อมูลตามวัตถุประสงค์ที่จำกัดและเฉพาะเจาะจงตามที่เจ้าของข้อมูลส่วนบุคคลได้เคยให้ความยินยอมไว้ และบุคคลที่สามนั้นจะต้องจัดให้มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่ากับหลักการใน The EU-U.S. Privacy Shield นี้ รวมทั้งต้องดำเนินการใด ๆ ที่จำเป็นเพื่อทำให้แน่ใจว่าบุคคลที่สามนั้นได้ดำเนินการประมวลผลข้อมูลสอดคล้องกับหน้าที่ของผู้ประกอบการตามที่กำหนดไว้ในความตกลง The EU-U.S. Privacy Shield และต้องกำหนดให้บุคคลที่สามแจ้งผู้ประกอบการให้ทราบหากไม่สามารถดำเนินรักษาความปลอดภัยในข้อมูลส่วนบุคคลในระดับเดียวกันกับความตกลงฉบับนี้ได้ รวมทั้งการดำเนินการอย่างเหมาะสมในการยับยั้งและเยียวยาการประมวลผลข้อมูลที่ไม่ได้รับอนุญาต[23]ด้วย

---

[22] U.S. Department of Commerce, “Privacy Shield Framework: Overview,” last modified n.d., accessed November 2, 2017, https://www.privacyshield.gov/article?id=OVERVIEW

[23] U.S. Department of Commerce, “Privacy Shield Framework: Accountability for onward transfer,” last modified n.d., accessed November 2, 2017, https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER

ทั้งนี้ กระทรวงพาณิชย์ของสหรัฐอเมริกาจะดำเนินการปรับปรุงแก้ไขข้อมูลและทบทวนรายชื่อผู้ประกอบการที่ได้รับการรับรองตามความตกลงฉบับนี้ และหากผู้ประกอบการไม่ปฏิบัติตามความตกลงฉบับนี้ก็จะได้รับโทษและอาจถูกถอนรายชื่อจากการรับรองของกระทรวงพาณิชย์ได้ นอกจากนี้หากเจ้าของข้อมูลส่วนบุคคลเห็นว่าข้อมูลส่วนบุคคลของตนถูกนำไปใช้โดยมิชอบตามหลักการใน Privacy Shield แล้ว เจ้าของข้อมูลส่วนบุคคลสามารถร้องเรียนได้ โดยคำร้องนี้อาจจะได้รับการแก้ไขโดยผู้ประกอบการที่เกี่ยวข้องโดยตรง หรือเจ้าของข้อมูลส่วนบุคคลอาจใช้ช่องทางการระงับข้อพิพาททางเลือก (Alternative Dispute resolution: ADR) หรือเจ้าของข้อมูลส่วนบุคคลอาจใช้ช่องทางร้องเรียนผ่านหน่วยงานคุ้มครองข้อมูลส่วนบุคคลในประเทศของตนก็ได้ และหากข้อร้องเรียนไม่ได้รับการแก้ไข เจ้าของข้อมูลส่วนบุคคลสามารถใช้อนุญาโตตุลาการเพื่อระงับข้อพิพาทที่เกิดขึ้นได้[24]

ในส่วนของประเทศไทยนั้น หากพิจารณาการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายไทยจะพบว่าในปัจจุบันประเทศไทยยังไม่มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลสำหรับข้อมูลที่อยู่ในความครอบครองของภาคเอกชนที่มีลักษณะเป็นหลักกฎหมายทั่วไป ทำให้การดำเนินการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลโดยภาคเอกชนของประเทศไทยยังไม่มีมาตรการทางกฎหมายที่ชัดเจนมากำกับดูแล อย่างไรก็ดีการที่ประเทศไทยยังไม่ได้มีการประกาศใช้กฎหมายฉบับดังกล่าวก็ไม่ได้หมายความว่าประเทศไทยไม่มีมาตรการทางกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนเลย เนื่องจากในปัจจุบันรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 มีบทบัญญัติที่รับรองสิทธิในความเป็นส่วนตัวไว้โดยเฉพาะ กล่าวคือ ในมาตรา 32 รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2560 กำหนดให้บุคคลย่อมมีสิทธิในความเป็นอยู่ส่วนตัว เกียรติยศ ชื่อเสียง และครอบครัว อีกทั้งมาตราดังกล่าวยังกำหนดหลักการเพื่อการคุ้มครองข้อมูลส่วนบุคคล โดยการบัญญัติห้ามนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ไม่ว่าในทางใด ๆ เว้นแต่จะอาศัยอำนาจตามกฎหมายที่ตราขึ้นเพียงเท่าที่จำเป็นเพื่อประโยชน์สาธารณะ นอกจากนี้ในการดำเนินงานของภาครัฐที่เกี่ยวข้องกับข้อมูลส่วนบุคคลนั้น ประเทศไทยมีการประกาศใช้ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540[25] ที่มีการบัญญัติแนวทางการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาครัฐไว้ในหมวด 3 ข้อมูลข่าวสารส่วนบุคคล อันแสดงให้เห็นถึงความพยายามในการกำหนดแนวทางการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาครัฐ อย่างไรก็ดีกฎหมายฉบับนี้ยังขาดรายละเอียด

---

[24] European Commission, “European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows,” last modified July 12, 2016, accessed November 2, 2017, http://europa.eu/rapid/press-release_IP-16-2461_en.htm

[25] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540, *ราชกิจจานุเบกษา* เล่มที่ 114 ตอนที่ 46 ก (10 กันยายน 2540): 8-10.

ในการคุ้มครองข้อมูลส่วนบุคคลหลายประการ รวมทั้งหลักเกณฑ์ที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศด้วย

อย่างไรก็ดี ได้มีความพยายามจากหลายหน่วยงานที่เกี่ยวข้องในการผลักดันร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพื่อสร้างหลักเกณฑ์ในการคุ้มครองสิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลที่เป็นรูปธรรม โดยเฉพาะการคุ้มครองสิทธิดังกล่าวจากการดำเนินงานของภาคเอกชน ซึ่งในการดำเนินการทางธุรกิจมักมีการเก็บรวบรวม ประมวลผลใช้โอน และเปิดเผยข้อมูลส่วนบุคคลของลูกค้าอยู่เสมอ ซึ่งหากไม่มีกฎหมายเพื่อกำหนดกรอบการดำเนินการดังกล่าวอาจส่งผลให้สิทธิในความเป็นส่วนตัวและข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลถูกละเมิดได้ โดยเฉพาะการเข้าถึงข้อมูลโดยไม่อนุญาต ซึ่งอาจกลายเป็นการนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้เพื่อก่ออาชญากรรมอื่น ๆ ได้เช่นกัน โดยเฉพาะในกรณีที่มีการโอนข้อมูลส่วนบุคคลไปยังผู้ประกอบการหรือผู้ประมวลผลข้อมูลในต่างประเทศ ดังนั้น การมีกฎหมายคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลที่กำหนดหลักการรักษาความปลอดภัยที่เหมาะสมในกรณีที่มีการโอนข้อมูลส่วนบุคคลจากประเทศหนึ่งไปยังอีกประเทศหนึ่งย่อมช่วยลดความเสี่ยงต่อความปลอดภัยในข้อมูลส่วนบุคคลของประชาชนได้

ทั้งนี้ หากพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับที่สำนักงานคณะกรรมการกฤษฎีกาได้มีการพิจารณาเป็นเรื่องเสร็จที่ 1135/2558 จะพบว่าแนวทางการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามร่างฯ ดังกล่าวยังขาดความชัดเจน เนื่องจากร่างฯ ดังกล่าวกำหนดให้การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศต้องเป็นไปตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด โดยไม่มีการกำหนดหลักการพื้นฐานใด ๆ ไว้เพื่อเป็นกรอบในการประกาศหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล อันส่งผลให้ไม่มีหลักประกันพื้นฐานในการกำหนดแนวทางการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

ในขณะที่ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ....ฉบับที่เคยมีการเสนอต่อสภานิติบัญญัติแห่งชาติและคณะรัฐมนตรีได้เสนอขอถอนเรื่องดังกล่าวต่อประธานสภานิติบัญญัติเมื่อวันที่ 8 กันยาน พ.ศ. 2558 นั้น ได้มีการกำหนดหลักการเบื้องต้นสำหรับการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศไว้ โดยในมาตรา 29 แห่งร่างฯ ฉบับนี้ได้กำหนดห้ามผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลไปนอกราชอาณาจักรโดยไม่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล ยกเว้นกรณีต่อไปนี้

1) เป็นการปฏิบัติตามกฎหมาย หรือเป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลซึ่งการขอความยินยอมไม่สามารถดำเนินการได้ในเวลานั้น หรือเป็นไปเพื่อประโยชน์ที่เกี่ยวกับชีวิต สุขภาพ หรือความปลอดภัยของเจ้าของข้อมูลส่วนบุคคล

2) เพื่อการดำเนินคดีนอกราชอาณาจักร

3) เป็นการปฏิบัติตามสัญญาที่ทำกับเจ้าของข้อมูลส่วนบุคคลหรือตามมาตรการที่เจ้าของข้อมูลส่วนบุคคลร้องขอเพื่อให้เป็นไปตามสัญญาที่จะทำขึ้น

4) เป็นผลหรือการปฏิบัติตามสัญญาที่ทำกับผู้อื่น เพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

5) เพื่อการป้องกันหรือปราบปรามการฟอกเงินหรือการก่อการร้าย

6) มีความจำเป็นอื่นตามที่คณะกรรมการประกาศกำหนด

อีกทั้งในมาตรา 30 แห่งร่างฯ ฉบับดังกล่าวยังกำหนดห้ามผู้ควบคุมข้อมูลส่วนบุคคลเปิดเผยข้อมูลส่วนบุคคลไปยังประเทศที่มิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคล หรือมีแต่บทบัญญัติของกฎหมายในประเทศนั้นมีมาตรการคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญต่ำกว่าบทบัญญัติแห่งร่างพระราชบัญญัตินี้โดยไม่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่เป็นกรณีต่อไปนี้

1) เป็นการปฏิบัติตามกฎหมาย หรือเป็นไปเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ซึ่งการขอความยินยอมไม่สามารถดำเนินการได้ในเวลานั้น หรือเป็นไปเพื่อประโยชน์ที่เกี่ยวกับชีวิต สุขภาพ หรือความปลอดภัยของเจ้าของข้อมูลส่วนบุคคล

2) มีความจำเป็นอื่นตามที่คณะกรรมการประกาศกำหนด

โดยการขอความยินยอมและการกำหนดว่าบทบัญญัติของกฎหมายในประเทศใดมีมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญต่ำกว่าบทบัญญัติแห่งร่างพระราชบัญญัตินี้ ให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

ดังนั้น จึงอาจสรุปได้ว่าการโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักรไทยตามร่างฯ ฉบับนี้จะสามารถดำเนินการได้ หากเป็นไปตามเงื่อนไขต่อไปนี้

1) ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเป็นหนังสือก่อน นั่นหมายความว่าความยินยอมเป็นเงื่อนไขสำคัญที่จะทำให้การโอนข้อมูลส่วนบุคคลสามารถดำเนินการได้หรือไม่ได้ อย่างไรก็ดีร่างพระราชบัญญัตินี้ได้กำหนดข้อยกเว้นสำหรับกรณีที่ไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลไว้ด้วยเช่นกัน เช่น กรณีเป็นการปฏิบัติตามกฎหมาย หรือการโอนข้อมูลส่วนบุคคลเป็นไปเพื่อการป้องกันหรือปราบปรามการฟอกเงินหรือการก่อการร้าย เป็นต้น

2) ประเทศที่รับโอนข้อมูลส่วนบุคคลไปจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญไม่ต่ำกว่าร่างพระราชบัญญัติฉบับนี้

ถึงแม้ว่าร่างฯ ฉบับนี้จะมีการกำหนดแนวทางการโอนข้อมูลส่วนบุคคลไปต่างประเทศไว้ แต่ก็ยังถือว่าขาดหลักการโอนข้อมูลส่วนบุคคลที่สำคัญหลายประการ เช่น ยังไม่มีการกำหนดแน่ชัดว่าร่างฯ ฉบับนี้รับรองแนวทางการคุ้มครองข้อมูลส่วนบุคคลตามหลัก Binding Corporate Rules หรือไม่ อีกทั้งยังไม่ชัดเจนว่ามาตรการคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญที่ต่ำกว่าบทบัญญัติแห่งร่างพระราชบัญญัตินี้มีลักษณะอย่างไร เป็นต้น และเนื่องจากคณะรัฐมนตรีได้เสนอขอถอนร่างฯ ดังกล่าวต่อประธานสภานิติบัญญัติไปแล้ว จึงยังไม่มีความแน่ชัดว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ที่จะเสนอต่อรัฐสภาจะกำหนดหลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศไว้ด้วยหรือไม่

4. แนวทางในการกำหนดหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศสำหรับประเทศไทย

เนื่องจากประเทศไทยยังอยู่ระหว่างการพิจารณาจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ผู้วิจัยจึงขอเสนอแนวทางในการกำหนดหลักเกณฑ์การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเพื่อปรับปรุงร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยให้มีความชัดเจนมากขึ้นโดยอาศัยการศึกษาความตกลงระหว่างประเทศและแนวปฏิบัติของต่างประเทศดังนี้

4.1 กฎหมายคุ้มครองข้อมูลส่วนบุคคลควรงดเว้นการกำหนดข้อจำกัดในการโอนข้อมูลส่วนบุคคลระหว่างประเทศไทยและประเทศอื่น หากประเทศอื่นนั้นมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพสอดคล้องกับหลักการหรือความตกลงระหว่างประเทศ หรือผู้ควบคุมข้อมูลส่วนบุคคลในประเทศอื่นนั้นมีมาตรการรักษาความปลอดภัยที่เหมาะสม ซึ่งมาตรการรักษาความปลอดภัยที่เหมาะสมนั้นอาจอ้างอิงจากหลักการใน GDPR กล่าวคือ มาตรการรักษาความปลอดภัยที่เหมาะสมนั้นอาจเกิดขึ้นตามกฎหมาย หรือตามหลักการ Binding Corporate Rules หรือเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนำมาใช้ หรือเป็นมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานนำมาใช้และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้การรับรอง หรือเป็นมาตรการตาม Code of conduct ของหน่วยงาน หรืออาจเป็นเครื่องมืออื่นที่ใช้รับรองการคุ้มครองข้อมูลส่วนบุคคล เช่น เครื่องหมายรับรอง เป็นต้น

4.2 ในกรณีที่ไม่ปรากฏมาตรการรักษาความปลอดภัยที่เหมาะสม การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศจะสามารถเกิดขึ้นได้เฉพาะในกรณีต่อไปนี้

4.2.1 เจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมอย่างชัดแจ้งภายหลังจากที่ได้รับทราบความเสี่ยงที่อาจเกิดขึ้นจากการโอนข้อมูลส่วนบุคคล

4.2.2 การโอนข้อมูลส่วนบุคคลมีความจำเป็น เพื่อเป็นการดำเนินการตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคล

4.2.3 การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการสิ้นสุดหรือดำเนินการตามสัญญา

4.2.4 การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการดำเนินคดีตามกฎหมาย

4.2.5 การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นใด

4.2.6 เมื่อเป็นการโอนข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลทางทะเบียน อันมีวัตถุประสงค์เป็นการให้ข้อมูลแก่สาธารณะและได้รับการเปิดเผยเพื่อการประชุมปรึกษาหารือ

4.3 ควรกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องรับผิดชอบต่อข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมของตนโดยไม่คำนึงว่าข้อมูลนั้นจะอยู่ที่ใด

4.4 ควรกำหนดให้ในกรณีที่ศาลของต่างประเทศได้มีคำพิพากษาให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโอนหรือเปิดเผยข้อมูลส่วนบุคคลใด ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจำเป็นต้องดำเนินการตามคำพิพากษาดังกล่าวเฉพาะในกรณีที่การบังคับการตามคำพิพากษานี้อยู่บนพื้นฐานของสัญญา หรือความตกลงระหว่างประเทศที่มีผลบังคับใช้ระหว่างประเทศไทยกับประเทศดังกล่าว

4.5 ควรกำหนดโทษปรับสำหรับผู้ฝ่าฝืน ไม่ปฏิบัติตามหลักการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศที่กำหนดไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5. บทสรุป

การกำหนดแนวทางการโอนข้อมูลส่วนบุคคลระหว่างประเทศไว้อย่างชัดเจนในกฎหมายถือเป็นสิ่งจำเป็นในการคุ้มครองสิทธิในความเป็นส่วนตัวในข้อมูลส่วนบุคคลของประชาชนชาวไทย โดยการกำหนดมาตการทางกฎหมายในกรณีดังกล่าวควรคำนึงถึงสภาวการณ์ที่เกิดขึ้นในปัจจุบันและแนวทางการดำเนินการตามความตกลงระหว่างประเทศที่เกี่ยวข้อง รวมถึงแนวปฏิบัติของประเทศอื่น ๆ ด้วย ซึ่งหากมีการปรับปรุงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยโดยอ้างอิงถึงหลักการทั้ง 5 ข้อ ตามที่ผู้เขียนได้เสนอแนะไปข้างต้นย่อมส่งผลให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยสอดคล้องกับมาตรฐานของสหภาพยุโรปและกฎหมายของประเทศสิงคโปร์มากขึ้น ซึ่งจะเป็นผลดีต่อภาคเอกชนของไทยในกรณีที่ต้องดำเนินการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมทั้งรับโอนข้อมูลส่วนบุคคลจากประเทศอื่นมาประมวลผลที่ประเทศไทยเนื่องจากมีมาตรการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลส่วนบุคคลระหว่างประเทศเทียบเท่ากับภูมิภาคและประเทศที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ก้าวหน้าและทันสมัยมากที่สุดของโลก ในขณะเดียวกันก็เป็นการรับรองการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้ปลอดภัยเนื่องจากเป็นการดำเนินการตามมาตรฐานทางกฎหมายที่ได้รับการยอมรับในระดับนานาอารยประเทศ

References

APEC. *APEC Privacy Framework (2015).* Singapore: APEC Secretarial, 2017. Accessed November 2, 2017. https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

Electronic Transactions Development Agency (Public Organization). Thailand Computer Emergency Response Team. "Cyber Security Statistics." Last modified n.d., Accessed November 1, 2017. https://www.thaicert.or.th/statistics/statistics2017.html [In Thai]

Electronic Transactions Development Agency (Public Organization). "Digital Economy." Last modified n.d., Accessed November 1, 2017. https://www.etda.or.th/digital-economy.html [In Thai]

Electronic Transactions Development Agency (Public Organization). "Right to privacy." Last modified n.d. Accessed November 1, 2017. https://www.etda.or.th/terminology-detail/1208.html [In Thai]

European Commission. "European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows." Last modified July 12, 2016, Accessed November 2, 2017. http://europa.eu/rapid/press-release_IP-16-2461_en.htm

Joint Committee on Human Rights. *Data Protection and Human Rights*. United Kingdom: The Stationery OYce Limited, 2008.

Minister of Foreign Affairs of Thailand. *Universal Declaration of Human Rights.* Bangkok: Minister of Foreign Affairs of Thailand, 2008. Last modified n.d., Accessed November 2, 2017. http://humanrights.mfa.go.th/upload/pdf/udhr-th-en.pdf [In Thai]

Ministry of Foreign Affairs, Department of International Organizations. *Universal Declaration of Human Rights.* Bangkok: Department of International Organizations, Ministry of Foreign Affairs, 2008. [In Thai]

OECD. *The OECD Privacy Framework.* n.p.: OECD Publishing, 2013. Accessed November 2, 2017. http://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf

Power, Leonie. "Getting to Know the GDPR, Part 9 – Data transfer restrictions are here to stay, but so are BCR." Last modified February 24, 2016. Accessed November 2, 2017. http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/

Saranya Jansawang. "Retailing to Digital Revolution Connected to World Trade." *Bangkokbiznews*, October 17, 2017. Accessed November 1, 2017. http://www.bangkokbiznews.com/news/detail/777249 [In Thai]

Thaieurope.net team. "New Rule for International Personal Data Transfer, Affecting the Global Supply Chain." *Bangkokbiznews.* Last modified March 21, 2016. Accessed November 1, 2017. http://www.bangkokbiznews.com/blog/detail/637251 [In Thai]

The Organization of American State. "Data Protection." Last modified n.d. Acessed April 27, 2018. http://www.oas.org/dil/data_protection_privacy_habeas_data.htm

Trunomi. "GDPR Portal: Site Overview." Last modified n.d. Accessed November 2, 2017. https://www.eugdpr.org/

U.S. Department of Commerce. "Privacy Shield Framework: Accountability for onward transfer." Last modified n.d. Accessed November 2, 2017. https://www.privacyshield.gov/article?id=3-ACCOUNTABILITY-FOR-ONWARD-TRANSFER

U.S. Department of Commerce. "Privacy Shield Framework: Overview." Last modified n.d. Accessed November 2, 2017. https://www.privacyshield.gov/article?id=OVERVIEW

UNCTAD, United Nations. *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. Switzerland: United Nation Publication, 2016. Accessed November 1, 2017. http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf