การโอนข้อมูลส่วนบุคคลระหว่างประเทศ

จัดทำโดย

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ร่วมกับ

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

การโอนข้อมูลส่วนบุคคลระหว่างประเทศ

โดย กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ
สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ISBN 974-229-724-9

พิมพ์ครั้งที่ 1 (พฤษภาคม 2548)

จำนวน 1,000 เล่ม

เอกสารเผยแพร่

สงวนลิขสิทธิ์ พ.ศ. 2548 ตาม พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
ไม่อนุญาตให้คัดลอก ทำซ้ำ และดัดแปลง ส่วนใดส่วนหนึ่งของหนังสือฉบับนี้
นอกจากจะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของลิขสิทธิ์เท่านั้น

Copyright©2005 by:
Ministry of Information and Communication Technology and
National Electronics and Computer Technology Center
National Science and Technology Development Agency
Ministry of Science and Technology
112 Thailand Science Park, Phahon Yothin Road, Klong 1, Klong Luang,
Pathumthani 12120, THAILAND.
Tel. +66(0)2-564-6900 Fax. +66(0)2-564-6901..2

จัดทำโดย

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ
สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
กระทรวงวิทยาศาสตร์และเทคโนโลยี
73/1 ถนนพระรามที่ 6 เขตราชเทวี กรุงเทพฯ 10400
โทรศัพท์ 02-644-8150-9 โทรสาร 02-644-6653
URL: http://www.nectec.or.th/ e-mail: info@nectec.or.th

คำนำ

หนังสือเล่มนี้จัดทำขึ้นเพื่อให้ผู้ประกอบการและประชาชนทั่วไปตระหนักถึงความสำคัญและความจำเป็นในการให้คุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคลเช่นเดียวกัน โดยเน้นที่การคุ้มครองข้อมูลส่วนบุคคลที่มีการโอนไปยังต่างประเทศและผลกระทบที่อาจได้รับในกรณีที่ประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ในขณะที่บางประเทศกำหนดให้กลไกดังกล่าวเป็นเงื่อนไขห้ามส่งข้อมูลส่วนบุคคลออกจากประเทศตนไปยังประเทศที่ยังไม่มีกลไกการคุ้มครองทางกฎหมายที่เพียงพอดังกล่าว อันอาจส่งผลกระทบต่อการทำ e-Business หรือกลายเป็นมาตรการอย่างหนึ่งในการกีดกันทางการค้าในขณะที่การส่งและโอนข้อมูลข้ามประเทศสามารถกระทำได้โดยง่ายและรวดเร็วขึ้นโดยอาศัยเทคโนโลยีสารสนเทศและการสื่อสารที่ทันสมัย

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ร่วมกับ
สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
พฤษภาคม 2548

บทสรุปสำหรับผู้บริหาร

จากการที่สหภาพยุโรป (European Union) ได้ออกหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในปี ค.ศ. 1995 ที่มีชื่อว่า Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of Such Data ซึ่งมีผลให้ประเทศสมาชิกมีพันธกรณีที่จะต้องบัญญัติกฎหมายภายในให้สอดคล้องกับหลักเกณฑ์ดังกล่าวให้แล้วเสร็จภายในวันที่ 24 ตุลาคม ปี ค.ศ. 1998 ทั้งนี้ ในส่วนที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศนั้นได้กำหนดหลักเกณฑ์สำคัญว่า ห้ามมิให้มีการโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศอื่นซึ่งมิได้เป็นสมาชิกหากประเทศดังกล่าวไม่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ (adequate level of protection) เว้นแต่จะเป็นกรณีเข้าข้อยกเว้นเท่านั้น

ด้วยเหตุนี้เองจึงเป็นเหตุให้ประเทศต่างๆ ซึ่งมิได้เป็นสมาชิกสหภาพยุโรปจำเป็นที่ต้องดำเนินการให้ประเทศของตนมีระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอในมุมมองของสหภาพยุโรปเพื่อให้สามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโปได้โดยปราศจากข้อจำกัดดังกล่าว ตลอดจนหลีกเลี่ยงผลกระทบที่อาจเกิดขึ้นแก่ผู้ประกอบการหรือองค์กรภายในประเทศที่จำเป็นต้องรับโอนข้อมูลส่วนบุคคลจากประเทศซึ่งเป็นสมาชิกสหภาพยุโรป

ประเทศไทยก็เป็นอีกประเทศหนึ่งที่อยู่ระหว่างการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยปัจจุบันได้มีการยกร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เสร็จเรียบร้อยแล้ว และอยู่ในขั้นตอนการเสนอกฎหมายในกระบวนการนิติบัญญัติ ดังนั้น ในหนังสือนี้จึงได้แสดงให้เห็นถึงหลักเกณฑ์ที่ใช้ในการประเมินระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปและประเทศต่าง ๆ ตลอดจนแนวทางในการดำเนินการให้ประเทศไทยหรือผู้ประกอบที่ตั้งอยู่ในประเทศไทยได้รับการยอมรับจากนานาประเทศว่ามีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอในขณะที่ไม่สร้างภาระแก่บุคคลผู้ซึ่งจำเป็นต้องปฏิบัติตามกฎหมาย

ดังกล่าวมากเกินไป ตลอดจนขั้นตอนในทางปฏิบัติที่ผู้ประกอบการหรือองค์กรภายในประเทศควรใช้เพื่อหลีกเลี่ยงปัญหาในการประกอบธุรกิจการค้าระหว่างประเทศอันเนื่องจากมาตรการคุ้มครองข้อมูลส่วนบุคคลที่กำลังดำเนินอยู่หรืออาจเกิดขึ้นในอนาคตอันใกล้นี้

จากการศึกษาพบว่า แนวทางดำเนินการให้ประเทศใดประเทศหนึ่งได้รับการพิจารณาจากสหภาพยุโรปว่ามีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอนั้น จะต้องมีหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลและสามารถบังคับใช้ได้อย่างมีประสิทธิภาพครบทุกประเด็นตามที่คณะทำงาน (Working Party) ซึ่งเป็นองค์กรที่จัดตั้งขึ้นโดย Directive 95/46/EC ให้ความเห็นไว้

ดังนั้น กรณีของประเทศไทยก็จำเป็นต้องมีการปรับปรุงแก้ไขเพิ่มเติมร่างพระราชบัญญัติฯ บางส่วนเพื่อให้สอดคล้องกับความเห็นดังกล่าว ซึ่งนอกจากจะทำให้ประเทศไทยได้รับการพิจารณาว่าการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอแล้ว และสามารถหลีกเลี่ยงปัญหาด้านกฎหมายที่อาจส่งผลกระทบต่อการประกอบธุรกิจการค้าและบริการระหว่างผู้ประกอบในประเทศไทยกับประเทศสมาชิกสหภาพยุโรปและประเทศอื่นๆ ที่ได้อาศัย Directive 95/46/EC เป็นแนวทางในการบัญญัติกฎหมายแล้ว ยังสามารถเพิ่มระดับการให้ความคุ้มครองความเป็นอยู่ส่วนตัวในข้อมูลข่าวสารของคนในประเทศให้ดียิ่งขึ้นด้วย

อย่างไรก็ตาม การปรับปรุงแก้ไขร่างพระราชบัญญัติดังกล่าวจะต้องคำนึงถึงปัญหาในทางปฏิบัติอันเนื่องจากการบังคับใช้กฎหมายด้วย โดยภายหลังจากการศึกษาวิเคราะห์ปัญหาการบังคับใช้กฎหมายเกี่ยวกับข้อจำกัดในการโอนข้อมูลส่วนบุคคลในกฎหมายของต่างประเทศก็ทำให้ทราบว่าในการกำหนดข้อจำกัดเกี่ยวกับการโอนข้อมูลส่วนบุคคลนั้น จะต้องคำนึงถึงความสามารถในการบังคับใช้สิทธิของเจ้าของข้อมูลภาพหลังที่ข้อมูลส่วนบุคคลของตนได้ถูกโอนไปต่างประเทศแล้ว ตลอดจนความยืดหยุ่นในการบัญญัติและบังคับใช้กฎหมายเพื่อมิให้เกิดภาระแก่ผู้ประกอบการมากเกินไป นอกจากนี้ ยังจำเป็นต้องบัญญัติกฎหมายให้เกิดความชัดเจนในบางประเด็นเพื่อหลีกเลี่ยงปัญหาการตีความดังที่ได้เกิดขึ้นแล้วในต่างประเทศ

ในส่วนของการดำเนินการของภาคธุรกิจเพื่อหลีกเลี่ยงปัญหาข้อจำกัดการโอนข้อมูลส่วนบุคคลนั้น วิธีการที่ได้รับความนิยมในปัจจุบันคือการขอความยินยอมจากเจ้าของข้อมูลและการทำสัญญาโอนข้อมูลส่วนบุคคล ซึ่งสามารถทำได้โดยการใช้สัญญาแม่แบบที่จัดทำขึ้นโดย Commission หรือเงื่อนไขข้อสัญญาขั้นต่ำที่กำหนดไว้ในกฎหมายภายในของแต่ละประเทศ โดยสัญญาที่จัดทำขึ้นนั้นจะต้องกำหนดรายละเอียดเกี่ยวกับสิทธิหน้าที่ของผู้โอนข้อมูลและผู้รับโอนข้อมูล กรณีที่คู่กรณีจะต้องรับต่อเจ้าของข้อมูล ข้อสัญญาเพื่อประโยชน์ของเจ้าของข้อมูลซึ่งเป็นบุคคลภายนอกสัญญาเป็นสำคัญ

ดังนั้น แม้ว่าปัจจุบันประเทศไทยจะยังไม่มีการบัญญัติกฎหมายเกี่ยวกับข้อจำกัดการโอนข้อมูลส่วนบุคคลก็ตาม ผู้ประกอบการที่มีสำนักงานใหญ่ หรือสำนักงานสาขาในประเทศไทยก็ควรศึกษาถึงข้อจำกัดและข้อยกเว้นต่างๆ เพื่อเตรียมความพร้อมในการปฏิบัติตามกฎหมาย ตลอดจนแสวงหาวิธีการที่จะทำให้สามารถโอนหรือรับโอนข้อมูลส่วนบุคคลระหว่างประเทศโดยปราศจากข้อจำกัดด้านกฎหมาย

สารบัญ

บทที่ 1 การโอนข้อมูลส่วนบุคคลของผู้ประกอบการ 9

1.1 ข้อมูลส่วนบุคคลมีความจำเป็นอย่างไรในการทำธุรกิจ 9

1.2 การโอนข้อมูลส่วนบุคคลมีกี่ประเภท อะไรบ้าง 10

บทที่ 2 ข้อพิจารณาเมื่อผู้ประกอบการจำเป็นต้องโอนข้อมูลส่วนบุคคล 14

2.1 การคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา 14

2.2 การคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบขององค์การสหประชาชาติ 17

2.3 การคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบของสหภาพยุโรป 18

บทที่ 3 ผลกระทบต่อผู้ประกอบการอันเนื่องมาจากมาตรการจำกัดการโอนข้อมูลส่วนบุคคลของสหภาพยุโรป 22

3.1 กรณีศึกษาของผู้ประกอบการที่ได้รับผลกระทบจากมาตรการของสหภาพยุโรป 22

3.2 ผลกระทบต่อผู้ประกอบการในประเทศไทย 31

3.3 การแก้ปัญหาของรัฐบาลสหรัฐอเมริกาโดยข้อตกลง Safe Harbor 31

บทที่ 4 ผู้ประกอบการจะต้องทำอย่างไรเมื่อจำเป็นต้องโอนข้อมูลส่วนบุคคลไปต่างประเทศ 37

4.1 สิ่งที่ผู้ประกอบการควรรู้เมื่อต้องโอนข้อมูลส่วนบุคคลไปต่างประเทศ 37

4.2 ทางเลือกของผู้ประกอบการเมื่อจำเป็นต้องโอนข้อมูลส่วนบุคคลไปต่างประเทศ 39

- การจัดทำสัญญาโอนข้อมูลส่วนบุคคล 40
- การจัดทำนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคล 45
- การประเมินผลกระทบต่อความเป็นอยู่ส่วนตัว 48

บทที่ 5 สรุป 53

บทที่ 1
การโอนข้อมูลส่วนบุคคลของผู้ประกอบการ

1.1 ข้อมูลส่วนบุคคลมีความจำเป็นอย่างไรในการทำธุรกิจ

ในยุคสังคมสารสนเทศ (Information Society) นั้นข้อมูลข่าวสาร (Information) นับว่ามีบทบาทสำคัญอย่างยิ่งในระบบเศรษฐกิจ ดังจะเห็นได้จากกิจกรรมทางเศรษฐกิจส่วนใหญ่ซึ่งมักจะอาศัยข้อมูลข่าวสารมาเป็นพื้นฐานในการตัดสินใจเพื่อดำเนินการอย่างหนึ่งอย่างใดด้านเศรษฐกิจแทบทั้งสิ้น และจากพัฒนาการทางเทคโนโลยีสารสนเทศและการสื่อสาร (Information and Communication Technology) ที่มีความก้าวหน้าอย่างรวดเร็วในช่วงสิบปีที่ผ่านมา ก็ได้ทำให้มีการนำเอาเทคโนโลยีดังกล่าวมาประยุกต์ใช้เพื่อให้เกิดประโยชน์ทั้งในด้านสังคมและเศรษฐกิจมากมาย โดยเฉพาะอย่างยิ่งการใช้เพื่อประโยชน์ในการประมวลผลการส่งหรือโอนข้อมูลระหว่างกันที่สามารถทำได้สะดวก รวดเร็ว และไม่มีข้อจำกัดด้านเวลาหรือระยะทางอีกต่อไป

หนึ่งในข้อมูลที่มีการประมวลผล การส่งหรือโอนข้อมูลระหว่างกันอย่างแพร่-หลายและมีปริมาณมากคือ “ข้อมูลส่วนบุคคล (Personal Data)” เนื่องจากในการดำเนินการต่าง ๆ ไม่ว่าโดยหน่วยงานของรัฐหรือหน่วยงานภาคเอกชน ต่างมีความ จำเป็นที่จะต้องมีการประมวลผลและส่งข้อมูลส่วนบุคคลอยู่ตลอดเวลา ซึ่งอาจอยู่ในลักษณะการส่งข้อมูลภายในหน่วยงานนั้นเองหรือระหว่างหน่วยงาน ทั้งนี้ การสื่อสารหรือส่งผ่านข้อมูลดังกล่าวมิได้จำกัดเฉพาะแต่มีการส่งข้อมูลภายในประเทศเท่านั้น หากแต่ยังมีลักษณะที่

เป็นการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศด้วย เช่น การโอนข้อมูลพนักงานบริษัทไปยังสำนักงานใหญ่หรือสำนักงานสาขาที่ตั้งอยู่ในต่างประเทศ การโอนข้อมูลของผู้ถือบัตรเครดิตเพื่อการเรียกเก็บเงินอันเนื่องจากการใช้บัตรเครดิตในต่างประเทศ ข้อมูลการเดินทางของผู้โดยสารสายการบินต่างๆ หรือแม้แต่การโอนข้อมูลส่วนบุคคลโดยภาครัฐเพื่อประโยชน์ในการบังคับใช้กฎหมาย การตรวจคนเข้าเมือง การเก็บภาษีศุลกากร เป็นต้น

นอกจากนี้ ผลของการพัฒนาเทคโนโลยีการสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ต (Internet) ก็ได้เป็นปัจจัยหนึ่งที่ทำให้มีการส่งหรือโอนข้อมูลส่วนบุคคลระหว่างประเทศเพิ่มมากขึ้นเป็นลำดับ โดยเฉพาะอย่างยิ่งการส่งหรือโอนข้อมูลส่วนบุคคลอันเนื่องจากการประกอบพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) ซึ่งจำเป็นต้องมีการรวบรวมข้อมูลส่วนบุคคลหลายประเภทเพื่อให้ธุรกิจสามารถดำเนินต่อไปได้อาทิ หมายเลขบัตรเครดิต หมายเลขบัญชีธนาคาร เป็นต้น

1.2 การโอนข้อมูลส่วนบุคคลมีกี่ประเภท อะไรบ้าง

จากพัฒนาการด้านเทคโนโลยีการประมวลผลข้อมูลและการสื่อสารที่มีความก้าวหน้าอย่างรวดเร็ว ก็ได้เป็นเหตุให้องค์กรธุรกิจต่างๆ นำเทคโนโลยีดังกล่าวมาใช้อำนวยความสะดวก เพิ่มศักยภาพหรือเป็นปัจจัยสำคัญการประกอบธุรกิจเพิ่มมากขึ้น โดยเฉพาะในกรณีของการประกอบธุรกิจที่มีลักษณะการดำเนินงานเชื่อมโยงกันในหลายประเทศ (Multinational companies) ซึ่งมีความจำเป็นอย่างยิ่งที่จะต้องมีการโอนข้อมูลจากประเทศหนึ่งไปยังอีกประเทศหนึ่งอยู่ตลอดเวลา โดยการโอนข้อมูลข้อมูลดังกล่าวอาจอยู่ในรูปของการโอนข้อมูลทางการภาพ อาทิ การส่งอุปกรณ์ที่บันทึกข้อมูลส่วนบุคคลไปยังอีกประเทศหนึ่งโดยทางไปรษณีย์[1] หรือการส่งข้อมูลผ่าน

[1] Ian Walden and Nagel Savage, “Transborder Data Flows,” in Information Technology and The Law, ed. Chris Edwards, Nagel Savage, Ian Walden (United Kingdom: Macmillan Publishers, 1990), p.121.

สื่ออิเล็กทรอนิกส์ต่างๆ ไม่ว่าจะเป็นดาวเทียม สายเคเบิ้ล[2] หรือแม้แต่การส่งข้อมูลผ่านทางเครือข่ายคอมพิวเตอร์แบบออนไลน์[3] เป็นต้น ทั้งนี้ สามารถจำแนกลักษณะของการโอนข้อมูลส่วนบุคคลตามลักษณะของข้อมูลและประเภทขององค์กรซึ่งมีความจำเป็นต้องโอนข้อมูลออกเป็น 4 ลักษณะ[4] ได้แก่

1. การโอนข้อมูลภายในองค์กรเดียวกันที่ตั้งอยู่คนละประเทศ

การโอนข้อมูลดังกล่าวมีความจำเป็นเพื่อประโยชน์ในการบริหารจัดการในองค์กร โดยเฉพาะอย่างยิ่งในการบริหารจัดการงานบุคคล (human resource management) อาทิ การโอนข้อมูลพนักงานระหว่างบริษัทสำนักงานสาขาในประเทศหนึ่งไปยังสำนักงานสาขาอื่น หรือสำนักงานใหญ่ที่ตั้งอยู่ในต่างประเทศ เพื่อการจัดทำฐานข้อมูลพนักงานกลางเพื่อให้บริษัทในเครือซึ่งตั้งอยู่ในประเทศต่างๆ สามารถเข้าถึงเพื่อใช้ประโยชน์ในข้อมูลดังกล่าวได้[5] หรือการจ่ายเงินเดือนให้แก่พนักงานที่ทำงานอยู่ในสำนักงานสาขาในต่างประเทศต่าง[6]

2. การโอนข้อมูลไปยังองค์กรอื่นที่ตั้งอยู่ในต่างประเทศ

ตัวอย่างเช่นการโอนข้อมูลระหว่างกลุ่มธุรกิจธนาคารระหว่างประเทศ[7] ธุรกิจประกันภัย ธุรกิจบัตรเครดิต[8] ธุรกิจการบินในกรณีการจองตั๋วเครื่องบิน ธุรกิจท่องเที่ยว การให้บริการทางการแพทย์ ธุรกิจตลาดแบบตรง (Direct Marketing) การ

---

[2] Ibid.

[3] A.C.M. Nugter, Transborder Flow of Personal Data within the EC, (Netherlands: Kluwer Law and Taxation Publishers,1990), p.1.

[4] Ian Walden and Nagel Savage, p.121.

[5] Christopher Kuner, European Data Privacy Law and Online Business (Great Britain: Oxford University Press, 2003), p.117.

[6] Ibid., p.122.

[7] ตัวอย่างเช่น การโอนเงินระหว่างประเทศโดยการใช้ระบบ S.W.I.F.T (the Society for Worldwide Interbank Financial Telecommunications)

[8] Ian Walden and Nagel Savage, p.121.

ประกอบพาณิชย์อิเล็กทรอนิกส์ที่จะต้องมีการโอนข้อมูลของลูกค้าจากประเทศหนึ่งไปยังอีกประเทศหนึ่งอยู่ตลอดเวลา[9]

3. การโอนข้อมูลเพื่อประโยชน์ของหน่วยงานภาครัฐ

ตัวอย่างเช่น การโอนข้อมูลส่วนบุคคลโดยภาครัฐเพื่อประโยชน์ในการบังคับใช้กฎหมาย การตรวจคนเข้าเมือง การเก็บภาษีศุลกากร เป็นต้น[10]

4. การโอนข้อมูลเพื่อประโยชน์ในการประมวลผลหรือการจัดเก็บฐานข้อมูลในต่างประเทศ

การโอนข้อมูลในลักษณะนี้มักเกิดขึ้นในกรณีที่มีการมอบหมายงานด้านสารสนเทศให้กับหน่วยงานภายนอก (Outsourcing) จากผู้ประกอบการในประเทศหนึ่งไปให้ผู้ประกอบการที่อยู่ในประเทศอื่นซึ่งส่วนใหญ่จะมีข้อมูลส่วนบุคคลปะปนไปด้วยเสมอ[11] ทั้งนี้ ก็เพื่อลดต้นทุนในในการประมวลผล หรือการบริหารจัดการต่างๆ เกี่ยวกับข้อมูล อาทิ การจัดตั้งศูนย์ให้บริการลูกค้า (call center) ในราคาที่ถูกกว่า ซึ่งปัจจุบันประเทศซึ่งเป็นผู้รับโอนข้อมูลส่วนใหญ่มักเป็นประเทศที่มีความก้าวหน้าด้านเทคโนโลยีในการประมวลผล หรือบริษัทที่มีสำนักงานสาขาตั้งอยู่ ไม่ว่าจะเป็นสหรัฐ-อเมริกา สิงคโปร์ ฮ่องกง รวมไปถึงอินเดียก็เป็นประเทศหนึ่งที่ได้รับการมอบหมาย

---

[9] European Union.“Application of a Methodoloty Designed to Asses the Adequacy of the level of protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer. ”<http://www.europa.eu.int/comm/internal_market/en/media/dataprot/studies/adequate.pdf>. September 1998.

[10] Elizabeth Longworth, “Transborder Data Flow: EU Directive and Implication for International Business”,Paper presented at E-Privacy in the New Economy Conference, Hong Kong, 26 March 2001.

[11] Christopher Kuner ,supra note 5, p.117.

งานด้านสารสนเทศข้างมากเนื่องจากมีอัตราค่าจ้างงานที่ไม่แพงจนเกินไปและมีบุคลากรที่สามารถใช้ภาษาอังกฤษได้ดี [12]

[12] David Bender, <dbender@whitecase.com>, “Data Protection Law in India : A Change of Direction,” private e-mail message to Patiwat Unruan, 20 January 2004

บทที่ 2
ข้อพิจารณา
เมื่อผู้ประกอบการจำเป็นต้องโอนข้อมูลส่วนบุคคล

เมื่อการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ มิได้จำกัดอยู่แค่เพียงการค้าภายในประเทศเท่านั้น แต่ขยายวงกว้างไปสู่การค้าระหว่างประเทศ ซึ่งประเทศคู่ค้าทั้งหลายคือทุกประเทศทั่วโลก เพราะฉะนั้นแล้ว เมื่อผู้ประกอบการจำเป็นต้องโอนข้อมูลส่วนบุคคลของลูกค้าซึ่งเป็นบุคคลต่างชาติ จึงมีความจำเป็นต้องทราบหลักเกณฑ์ กฎและกติกาต่างๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับการให้ความคุ้มครองข้อมูลส่วนบุคคล ที่ชาวต่างชาติถือว่าเป็นสิทธิขั้นพื้นฐานที่ผู้ประกอบการจะต้องให้ความสำคัญและมิอาจล่วงละเมิดได้ ทั้งนี้ หากผู้ประกอบการไทยตระหนักถึงความสำคัญและความจำเป็นในการให้คุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคลแล้ว ก็จะช่วยเสริมสร้างความเชื่อมั่นในการทำ e-Business กับคู่ค้าชาวต่างชาติได้เป็นอย่างดี

2.1 การคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)

กรอบในการบัญญัติกฎหมายเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลในระดับสากลในระยะเริ่มต้นนั้นได้เกิดขึ้นจากการจัดแนวปฏิบัติด้านการคุ้มครองความเป็นอยู่ส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ” (Guidelines on the protection

of Privacy and Transborder Data Flows of Personal Data) [13] โดยองค์การเพื่อเศรษฐกิจและการพัฒนา (OECD) ในปี ค.ศ. 1980 โดยหลักการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีทั้งสิ้น 8 ประการ ได้แก่

1. หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)

ผู้ประกอบการจะต้องกำหนดหลักเกณฑ์เกี่ยวกับข้อจำกัดในการรวบรวมข้อมูลส่วนบุคคลว่าจะสามารถรวบรวมได้ต่อเมื่อได้ข้อมูลดังกล่าวมาโดยชอบด้วยกฎหมาย (lawful) วิธีการที่เป็นธรรม (fair means) และเหมาะสม (appropriate) ภายใต้การรับรู้หรือความยินยอมจากเจ้าของข้อมูลเท่านั้น

2. หลักคุณภาพของข้อมูล (Data Quality Principle)

ผู้ประกอบการจะต้องใช้ข้อมูลส่วนบุคคลภายในขอบวัตถุประสงค์ในการจัดเก็บ หรืออาจใช้เพื่อวัตถุประสงค์อื่นได้ตามความจำเป็น โดยข้อมูลดังกล่าวจะต้องเป็นข้อมูลที่มีความถูกต้อง และเป็นปัจจุบัน (up-to-date)

3. หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)

ผู้ประกอบการจะต้องแจ้งวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลได้ทราบก่อนการรวบรวมข้อมูล อีกทั้งจะต้องใช้ข้อมูลส่วนบุคคลภายในวัตถุประสงค์ดังกล่าวด้วย

4. หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)

ผู้ประกอบการจะต้องไม่เปิดเผย (disclose) ทำให้แพร่หลาย (made available) หรือใช้เพื่อวัตถุประสงค์อื่นใดนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบก่อนหน้านั้น เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลหรือมีกฎหมายบัญญัติเป็นอย่างอื่น

---

[13] OECD. “Council Recommendations Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.” < http://www.oecd.org/document/20/0,2340,en_2649_201185_15589524_1_1_1_1,00.html >. October 1980.

5. หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)

ผู้ประกอบการจะต้องรักษาความปลอดภัยของข้อมูลโดยใช้มาตรการรักษาความปลอดภัยตามสมควร (reasonable security safeguards) เพื่อป้องกันการเข้าถึงข้อมูลโดยปราศจากอำนาจ (unauthorized access) , การทำลาย (destruction), ใช้ (use), เปลี่ยนแปลง (modification), หรือการเปิดเผยข้อมูล (disclosure)

6. หลักการเปิดเผย (Openess Principle)

ผู้ประกอบการจะต้องประกาศนโยบายเกี่ยวกับการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลให้ทราบโดยทั่วไป วัตถุประสงค์ในการใช้ข้อมูล รายละเอียดเกี่ยวกับผู้ควบคุมข้อมูล (controller) ถิ่นที่อยู่ของผู้ควบคุม เป็นต้น

7. หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

ผู้ประกอบการจะต้องกำหนดให้เจ้าของข้อมูลมีสิทธิในการได้รับการยืนยัน (Confirmation) จากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูล (Controller) มีข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลหรือไม่เพียงใด โดยจะต้องได้รับทราบผลการยืนยันภายในเวลาอันสมควร ทั้งนี้ อาจมีการคิดค่าใช้จ่ายในการดำเนินการได้ในอัตราที่เหมาะสม และในกรณีที่ไม่สามารถดำเนินการตามที่เจ้าของข้อมูลร้องขอข้างต้นก็จะต้องแจ้งเหตุผลให้เจ้าของข้อมูลทราบ อีกทั้งบอกกล่าวให้เจ้าของข้อมูลทราบถึงสิทธิในการโต้แย้งการไม่ปฏิบัติตามคำร้องขอดังกล่าว และหากต่อมาปรากฏว่าข้อโต้แย้งของเจ้าของข้อมูลสามารถรับฟังได้ เจ้าของข้อมูลก็มีสิทธิที่จะขอให้มีการลบ แก้ไข ปรับปรุง หรือทำให้ข้อมูลมีความสมบูรณ์

8. หลักความรับผิดชอบ (Accountability Principle)

ผู้ประกอบการจะต้องมีหน้าที่ในการปฏิบัติการตามหลักการข้างต้นให้ครบถ้วนทุกประการ

2.2 การคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบขององค์การสหประชาชาติ (UN)

นอกจากหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลในระดับนานาชาติที่ได้จัดทำขึ้นโดยองค์การระหว่างประเทศซึ่งมีประเทศสมาชิกส่วนใหญ่อยู่ในภาคพื้นยุโรปดังที่ได้กล่าวข้างต้นแล้ว องค์การสหประชาชาติ (United Nation: UN) โดยคณะมนตรีด้านสังคมและเศรษฐกิจแห่งสหประชาชาติ (United Nations Economic and Social Council) ก็ได้ให้การรับรอง “Guidelines for the Regulation of Computerized Personal Data File”[14] เมื่อวันที่ 14 ธันวาคม ค.ศ. 1990 โดยได้กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขั้นต่ำ 6 ประการที่สมควรกำหนดไว้ในกฎหมายภายในของประเทศสมาชิก อันประกอบด้วย

- หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and fairness)[15]
- หลักความถูกต้อง (Principle of accuracy)[16]
- หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง (Principle of the purpose specification)[17]
- หลักการเข้าถึงข้อมูลโดยบุคคลที่เกี่ยวข้อง (Principle of interested-person access)[18]
- หลักการไม่เลือกปฏิบัติ (Principle of non-discrimination)[19]

---

[14] United Nations, “Guidelines for the Regulation of Computerized Personal Data File,” < http://www.unhchr.ch/html/menu3/b/71.htm >. 1990

[15] Ibid., Article 1

[16] Ibid., Article 2

[17] Ibid., Article 3

[18] Ibid., Article 4

[19] Ibid., Article 5

- หลักการรักษาความปลอดภัย (Principle of security)[20]

ทั้งนี้ เนื้อหาของหลักการต่างๆ ที่ปรากฏอยู่ UN Guidelines มีลักษณะเป็นไปในทิศทางเดียวกันกับ OECD Guidelines แต่แตกต่างกันตรงที่ได้เพิ่มหลักการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษ (sensitive data) ไว้ในหลักการไม่เลือกปฏิบัติ (Principle of non-discrimination) ด้วย กล่าวคือ ห้ามมิให้ทำการรวบรวมข้อมูลซึ่งอาจทำให้เกิดการเลือกปฏิบัติต่อบุคคลที่แตกต่างกัน อาทิ ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง ศาสนา ความเชื่อทางปรัชญาหรือความเชื่ออื่นใด และรวมถึงความเป็นสมาชิกสหภาพการค้า

2.3 การคุ้มครองข้อมูลส่วนบุคคลภายใต้กรอบของสหภาพยุโรป (EU)

กฎเกณฑ์ที่นับได้ว่าเป็นต้นแบบหรือที่มาของการบัญญัติกฎหมายที่กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลถูกจัดทำขึ้นเป็นครั้งแรกโดยสหภาพยุโรป (European Union: EU) ในปี ค.ศ. 1995 โดยการ Directive ที่มีชื่อว่า Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data on the Free Movement of Such Data ซึ่งเอกสารฉบับนี้ได้กำหนดให้ประเทศสมาชิก EU เดิมทั้ง 15 ประเทศมีพันธกรณีที่จะต้องบัญญัติกฎหมายภายในให้สอดคล้องกับหลักเกณฑ์ดังกล่าวให้แล้วเสร็จภายในวันที่ 24 ตุลาคม ค.ศ.1998

EU Directive มีวัตถุประสงค์เพื่อคุ้มครองสิทธิขั้นพื้นฐานและเสรีภาพของบุคคลธรรมดาโดยเฉพาะอย่างยิ่งสิทธิในความเป็นอยู่ส่วนตัวอันเนื่องจากการประมวลผลข้อมูลส่วนบุคคล[21] ซึ่งหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลใน EU Directive ในภาพรวมนั้นมีเนื้อหาที่กว้างขวางกว่าหลักการคุ้มครองข้อมูลส่วนบุคคล

---

[20] Ibid., Article 7

[21] Article 1 “ to protect the fundamental rights and freedom of natural personal , and in particular the right to privacy with respect to the processing of personal data [emphasis added]”

ใน OECD Guidelines ตัวอย่างเช่น ได้มีการเพิ่มเติมหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลชนิดพิเศษ (sensitive data)[22] ว่าห้ามมิให้มีการประมวลผลข้อมูลดังกล่าวเว้นแต่จะเข้ากรณีข้อยกเว้น, หลักเกณฑ์การเปิดเผยรายละเอียดต่างๆ เกี่ยวกับการประมวลผล ข้อมูล[23] หลักเกณฑ์การแจ้งรายละเอียดเกี่ยวกับการประมวลผลต่อองค์กรด้านการ คุ้มครองข้อมูลส่วนบุคคล[24] สิทธิในการขอให้ยุติ (opt-out) การนำข้อมูลส่วนบุคคลไปใช้เพื่อประโยชน์ในการทำการตลาดแบบตรง (direct marketing)[25] และสิทธิในการ ได้รับการชดใช้ค่าเสียหาย[26]

นอกจากนี้ EU Directive ยังมีวัตถุประสงค์เพื่อต้องการให้เกิดการโอนถ่ายข้อมูลส่วนบุคคลภายในกลุ่มประเทศสมาชิกโดยสะดวก แต่หากเป็นการโอนข้อมูลไปยังประเทศนอกสมาชิกแล้วจะต้องอยู่ภายใต้ข้อจำกัด โดยได้กำหนดหลักเกณฑ์สำคัญไว้ว่า *"ห้ามมิให้มีการโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศอื่นซึ่งมิได้เป็นสมาชิก EU หากประเทศดังกล่าวไม่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ (adequate level of protection) เว้นแต่จะเป็นกรณีเข้าข้อยกเว้นเท่านั้น"* ซึ่งข้อยกเว้นดังกล่าว เช่น เจ้าของข้อมูลได้ให้ความยินยอมให้มีการโอนข้อมูลอย่างชัดแจ้ง[27] *การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล หรือการดำเนินการใดๆ ก่อนการเข้าทำสัญญาตามที่เจ้าของข้อมูลร้องขอ*[28] *จำเป็นต้องทำการโอนข้อมูลเพื่อหาข้อสรุปของสัญญาหรือปฏิบัติตามสัญญา ซึ่งทำเพื่อประโยชน์ของเจ้าของข้อมูล และได้จัดทำขึ้น*

---

[22] EU Directive, Article 8

[23] Ibid., Article 10–12

[24] Ibid., Article 18–21

[25] Ibid., Article 14

[26] Ibid., Article 22–24

[27] Ibid., Article 26

[28] ตัวอย่างเช่น การโอนข้อมูลส่วนบุคคลของผู้จองตั๋วโดยสารเครื่องบินไปยังสายการบินหรือโรงแรมในต่างประเทศ

โดยผู้ควบคุมข้อมูลและบุคคลภายนอก[29] *การโอนข้อมูลมีความจำเป็นเพื่อประโยชน์สาธารณะ หรือเพื่อการก่อตั้งสิทธิเรียกร้อง หรือการต่อสู้คดีตามกฎหมาย การโอนข้อมูลมีความจำเป็นคุ้มครองชีวิตของเจ้าของข้อมูล การโอนข้อมูลโดยหน่วยงานทางทะเบียนตามที่กฎหมายบัญญัติ การให้ข้อมูลข่าวสารแก่สาธารณะเพื่อเป็นข้อมูลประกอบการรับฟังความคิดเห็นจากประชาชนหรือผู้มีประโยชน์ได้เสียในข้อมูลส่วนบุคคลนั้น*

นอกจากข้อยกเว้นข้างต้นที่ทำให้ประเทศสมาชิก EU สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศอื่นที่ไม่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอแล้ว ประเทศสมาชิก EU ยังอาจโอนข้อมูลส่วนบุคคลไปยังประเทศดังกล่าวในกรณีที่สามารถแสดงให้เห็นว่าประเทศนั้นให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลที่เพียงพอ โดยการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวอาจอยู่ในรูปของการทำข้อสัญญาที่เหมาะสม (appropriate contractual clauses)[30] อีกด้วย

ทั้งนี้ EU Directive ได้ให้อำนาจแก่คณะกรรมาธิการยุโรป[31] (European Commission) ในการพิจารณาชี้ขาดว่าประเทศนอกสมาชิก EU ประเทศใดที่มีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอด้วย[32] ซึ่งผลของการชี้ขาดโดยคณะกรรมาธิการดังกล่าวก็จะมีผลให้ประเทศนั้นๆ สามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ได้โดยปราศจากข้อจำกัดในทำนองเดียวกับการโอนข้อมูลส่วนบุคคลภายในประเทศสมาชิก EU เนื่องจากคำชี้ขาดดังกล่าวมีผลผูกพันให้ประเทศสมาชิก EU

---

[29] ตัวอย่างเช่น การที่บริษัทที่รับประกันภัยในประเทศได้โอนข้อมูลไปยังผู้รับ ประกันภัยต่อ (reinsurance) ในต่างประเทศ

[30] EU Directive, Article 26 (2)

[31] คณะกรรมาธิการยุโรป (European Commission) เป็นองค์กรด้านบริหารองค์กรหนึ่งของ EU อันประกอบด้วยคณะกรรมาธิการจำนวน 36 คณะ (Directorate General) โดยคณะกรรมาธิการซึ่งมีบทบาทสำคัญด้านการคุ้มครองข้อมูลส่วนบุคคลและมีหน้าที่ปฏิบัติการให้เป็นไปตาม EU Directive คือ DG Internal Market , See Christopher Kuner , supra note 78 , p.6.

[32] EU Directive, Article 25 (6)

ทุกประเทศต้องปฏิบัติให้สอดคล้องกับคำชี้ขาดดังกล่าวด้วย[33]โดยปัจจุบันมีประเทศที่ได้รับการพิจารณาชี้ขาดจากคณะกรรมธิการว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอจำนวน 5 ประเทศ ได้แก่ อาเจนตินา ฮังการี สวิตเซอร์แลนด์ กูนซี (Guernsey) และไอซ์ออฟแมน (Isle of Man) ส่วนประเทศแคนาดาและสหรัฐอเมริกานั้นได้รับการรับรองเฉพาะกรณีการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ภายในบังคับของ Personal Information Protection and Electronic Documents Act 2002 และหน่วยงานที่เข้าร่วมโครงการ Safe Harbor ตามลำดับ[34] นอกจากนี้ Commission ก็ยังมีอำนาจในการประกาศว่าประเทศนอกสมาชิกใดเป็นประเทศที่มีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่เพียงพอได้ด้วย[35] ซึ่งจนถึงปัจจุบัน Commission ก็ยังมิได้ออกประกาศในลักษณะดังกล่าวแต่อย่างใด ซึ่งอาจเป็นเพราะเกรงว่าจะส่งผลกระทบต่อความสัมพันธ์ทางการเมืองระหว่างประเทศนั่นเอง[36]

---

[33] Ibid.

[34] สามารถตรวจสอบรายชื่อประเทศที่ Commission มีคำชี้ขาดว่ามีระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอได้ที่
<http://europa.eu.int/comm/internal_market/privacyadequacy_en.htm.>

[35] EU Directive, Article 25 (3)

[36] Christopher Kuner , supra note 5 , p.133.

บทที่ 3
ผลกระทบต่อผู้ประกอบการ อันเนื่องมาจากมาตรการจำกัด การโอนข้อมูลส่วนบุคคลของสหภาพยุโรป

3.1 กรณีศึกษาของผู้ประกอบการที่ได้รับผลกระทบจากมาตรการของสหภาพยุโรป

ผลจากการที่ประเทศสมาชิกทั้ง 15 ประเทศมีหน้าที่ต้องบัญญัติกฎหมายภายให้สอดคล้องกับ EU Directive ให้แล้วเสร็จภายในวันที่ 24 ตุลาคม ค.ศ. 1998 นี้เอง ซึ่งรวมถึงหลักเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลระหว่างประเทศด้วยนั้น ก็ได้ส่งผลให้ประเทศ EU ต่างบัญญัติกฎหมายหรือแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้มีสาระสำคัญเช่นเดียวกับที่กำหนดไว้ใน EU Directive[37] แม้จะมีความแตกต่างกันในรายละเอียดบางประการก็ตาม ก็ได้ส่งผลกระทบต่อผู้ประกอบการซึ่งอยู่นอกสมาชิก EU เป็นอย่างมาก เนื่องจากไม่สามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ได้ หรือต้องใช้ระยะเวลาและงบประมาณค่อนข้างมากเพื่อทำให้สามารถรับโอนข้อมูลส่วนบุคคลนั้นได้ ซึ่งจะเห็นได้จากตัวอย่างต่างๆ ดังต่อไปนี้

[37] EU Directive, Article 25-26

กรณีของผู้ประกอบการในเยอรมัน[38]

ปัญหาเกี่ยวกับการโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ไปยังประเทศนอกสมาชิก EU ที่ค่อนข้างมีชื่อเสียงและมีการอ้างถึงในหนังสือหรือเอกสารทางวิชาการด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างแพร่หลายคือ กรณีที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งกรุงเบอร์ลิน ประเทศเยอรมัน ได้ชะลอการโอนข้อมูลส่วนบุคคลที่จะมีขึ้นระหว่างการรถไฟแห่งเยอรมัน (German Federal Railway) และธนาคารซิตี้แบงค์ซึ่งมีสำนักงานในสหรัฐอเมริกา[39] เพื่อใช้เป็นข้อมูลในการจัดทำบัตรโดยสารรถไฟซึ่งสามารถใช้เป็นบัตรเครดิตได้ด้วย โดยมีข้อเท็จจริงดังนี้

ภายหลังจากที่การรถไฟแห่งเยอรมัน (German Federal Railway) ซึ่งเป็นหน่วยงานภาครัฐที่ให้บริการขนส่งทางรถไฟในประเทศเยอรมันได้แปรรูปไปเป็นบริษัทมหาชนจำกัดที่มีรัฐบาลเป็นผู้ถือหุ้นใหญ่ในปี ค.ศ.1994 โดยใช้ชื่อว่าบริษัท Deutsche Bahn AG ก็ได้มีแนวคิดที่จะพัฒนาระบบการให้บริการของตนให้ดียิ่งขึ้น โดยหนึ่งในการพัฒนาระบบการให้บริการดังกล่าว คือ การจัดทำระบบลดค่าโดยสารผ่านการใช้บัตรพลาสติกที่เรียกว่า BahnCard ซึ่งผู้ที่ถือบัตรนี้จะได้รับส่วนลดค่าโดยสารรถไฟในประเทศเยอรมัน

ต่อมา Deutsche Bahn AG ก็ได้ตัดสินใจที่จะร่วมมือกับธนาคารซิตี้แบงค์ สาขาเยอรมันในการออกบัตร BahnCard แบบใหม่ที่สามารถใช้เป็นบัตรเครดิตวีซ่าได้ด้วย โดยบัตรแบบนี้จะมีรูปภาพของผู้ถือบัตรไว้

---

[38] Alexander Dix, “Case Study : North America and the European Directive”, Paper Presented at 18th International Privacy and Data Protection Conference, Ottawa, Canada, 18-20 September 1996.

[39] John R. Vacca, “The European Data Protection Directive: A Roadblock to International Trade?,” The Privacy Papers : Managing Technology, Consumer, Employee, and Legislative Action , ed. Rebecca Herole (New York : CRC Press LLC, 2002), p.570.

ด้วย และในปีต่อมาก็ได้มีการริเริ่มออกบัตรดังกล่าวให้แก่ลูกค้าของซิตี้แบงค์ในประเทศเยอรมัน

ประเด็นปัญหาที่เกิดขึ้นตามมาจากการออกบัตรดังกล่าวคือ มีการวิพากษ์วิจารณ์กันอย่างกว้างขวางว่า บริษัท Deutsche Bahn AG ได้ขายข้อมูลของลูกค้าเดิมของบริษัทไปให้แก่ธนาคารซิตี้แบงค์ซึ่งมีสำนักงานใหญ่ในประเทศสหรัฐอเมริกา เพื่อใช้เป็นข้อมูลในการทำธุรกิจตลาดแบบตรง (direct marketing business) ซึ่งเป็นเหตุให้หน่วยงานท้องถิ่นด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศเยอรมันได้ออกมาวิพากษ์วิจารณ์แบบฟอร์มในการขอใช้บัตร BahnCard แบบใหม่ โดยเฉพาะอย่างยิ่งรายละเอียดเกี่ยวกับความน่าเชื่อถือทางด้านการเงิน (creditworthiness) ซึ่งเห็นว่าไม่จำเป็นต้องรวบรวมข้อมูลดังกล่าวเนื่องจากผู้ยื่นใบสมัครมีความประสงค์เพียงแค่บัตรโดยสารรถไฟเท่านั้น

ต่อมาไม่นานหลังจากที่มีการต่อต้านโดยองค์กรด้านคุ้มครองผู้บริโภคและหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลของเยอรมัน Deutsche Bahn AG และธนาคารซิตี้แบงค์ก็ได้มีการเจรจาเพื่อจัดทำข้อตกลงเกี่ยวกับการออกบัตรชนิดใหม่โดยเปิดโอกาสให้ประชาชนสามารถเลือกที่จะใช้บัตร BahnCard แบบปกติซึ่งไม่มีคุณสมบัติเป็นบัตรเครดิต หรือจะเลือกเป็นบัตรชนิดใหม่ที่สามารถเป็นบัตรเครดิตได้ในเวลาเดียวกัน

และภายหลังจากมีการแก้ไขกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศเยอรมันในปี ค.ศ. 1995 ก็เป็นผลเหตุให้กรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งเบอร์-ลิน (Berlin Data Protection Commissioner) มีอำนาจที่จะพิจารณาปัญหาดังกล่าวของบริษัท Deutsche Bahn AG ซึ่งกรรมการมีความเห็นว่าบริษัท Deutsche Bahn AG มีฐานะเป็นผู้รวบรวมข้อมูลส่วนบุคคลของผู้โดยสารในลำดับแรก (primary collector) ดังนั้น จึงไม่ควรอนุญาตให้บริษัทคู่สัญญาอื่นรับโอนไปซึ่งข้อมูลส่วนบุคคลของผู้โดยสารไปทั้งหมด ในกรณีนี้เนื่องจากบริษัทคู่สัญญาเป็นบริษัทที่มีสำนักงานใหญ่ในประเทศสหรัฐอเมริกา จึงเท่ากับว่าการโอนข้อมูลผู้โดยสายของบริษัท Deutsche Bahn AG เป็นการโอนข้อมูลส่วนบุคคลไปยังประเทศอื่นที่มิได้เป็นสมาชิก EU ซึ่งแม้ว่าในขณะนั้นประเทศเยอรมันจะยังมิได้แก้ไข Federal Data Protection Act

ให้สอดคล้องกับ EU Directive ก็ตาม แต่กรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งเบอร์ลินก็เห็นว่า การโอนข้อมูลส่วนบุคคลของผู้โดยสารดังกล่าวจะสามารถทำได้ต่อเมื่อมีเหตุให้โอนข้อมูลส่วนบุคคลไปยังต่างประเทศตามเงื่อนไขที่กำหนดไว้ใน Article 25 และ 26 เท่านั้น

ด้วยเหตุนี้เอง ทางบริษัท Deutsche Bahn AG และซิตี้แบงค์จึงได้พยายามหาวิธีการแก้ไขปัญหาดังกล่าวโดยการทำสัญญาคุ้มครอง ข้อมูลส่วนบุคคล (Data Protection Agreement) ระหว่างกันในเดือนกุมภาพันธ์ ค.ศ. 1996 ซึ่งในข้อสัญญาดังกล่าวก็ได้ระบุหน้าที่ของบริษัท Deutsche Bahn AG ในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวบรวมมาจากผู้โดยสารเพื่อใช้กิจการเดินรถไฟ ในขณะที่ธนาคารซิตี้แบงค์มีหน้าที่ในการให้ความคุ้มครองเกี่ยวกับ ข้อมูลเครดิตของผู้โดยสารด้วย ทั้งนี้ทั้งสองบริษัทมีหน้าที่ร่วมกันในการให้ความคุ้มครองเกี่ยวกับชื่อและที่อยู่ของผู้ถือบัตร

นอกจากนี้ ในระหว่างธนาคารสาขาของซิตี้แบงค์ในเยอรมันและสหรัฐอเมริกาก็ได้ทำสัญญาเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลระหว่างกันที่มีชื่อว่า Agreement on Interterritorial Data Protection โดยมีเนื้อหาดังต่อไปนี้

1) คู่กรณี (สำนักงานสาขาธนาคารซิตี้แบงค์ในเยอรมันและสหรัฐอเมริกา) ตกลงให้นำกฎหมายคุ้มครองข้อมูลส่วนบุคคลมาใช้บังคับแก่การดำเนินการใดๆ เกี่ยวกับข้อมูลของผู้ถือบัตร
2) ข้อมูลส่วนบุคคลของลูกค้าจะถูกประมวลผลในสหรัฐอเมริกาเพื่อประโยชน์ในการจัดทำบัตรเท่านั้น
3) ธนาคารสาขาของซิตี้แบงค์ทั้งที่อยู่ในเยอรมันและสหรัฐอเมริกาไม่อาจโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอกเพื่อวัตถุประสงค์ด้านการตลาดได้ ยกเว้นในสองกรณีดังต่อไปนี้

- ข้อมูลที่กรอกในใบสมัครเพื่อรับบัตรโดยสารรถไฟซึ่งมีคุณสมบัติเป็นบัตรครดิตได้อาจโอนไปยังบริษัทในเครือของซิตี้แบงค์ได้เพื่อวัตถุประสงค์ในการให้บริการด้านการเงิน (market financial services)
- ข้อมูลที่กรอกในใบสมัครเพื่อรับบัตรโดยสารรถไฟแบบปกติ อาจนำไปใช้หรือโอนไปวัตถุประสงค์ในการทำการตลาดของบริษัท Deutsche Bahn AG ตัวอย่างเช่น เพื่อเชิญชวนลูกค้าให้ทำการเปลี่ยนแปลงบัตรโดยสารของตนซึ่งเป็นแบบปกติไปเป็นบัตรที่มีคุณสมบัติเป็นบัตรเครดิตได้ด้วย

4) การกำหนดรายละเอียดเกี่ยวกับวิธีการรักษาความปลอดภัยของข้อมูลที่สอดคล้องกับกฎหมายเยอรมัน
5) สำนักงานสาขาของธนาคารซิตี้แบงค์ในสหรัฐอเมริกามีหน้าที่ต้องแต่งตั้ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (data protection supervisors) เพื่อให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของเยอรมัน
6) ผู้ถือบัตรในประเทศเยอรมันมีสิทธิเรียกร้องเกี่ยวกับข้อมูลส่วนบุคคลของตนต่อธนาคารซิตี้แบงค์ในสหรัฐอเมริกาตามที่บัญญัติไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของเยอรมัน อาทิ การขอตรวจดูข้อมูล การร้องขอลบข้อมูล การแก้ไขข้อมูลให้ถูกต้อง การเรียกค่าเสียหายภายใต้หลักความรับผิดเด็ดขาด (strict liability) ภายใต้กฎหมายเยอรมัน ทั้งนี้สามารถเรียกร้องค่าเสียหายไปยังบริษัท Deutsche Bahn AG , ธนาคารซิตี้แบงค์สาขาเยอรมัน หรือเรียกร้องโดยตรงไปยังธนาคารซิตี้แบงค์ในสหรัฐอเมริกาได้
7) ธนาคารซิตี้แบงค์ในสหรัฐเมริกายินยอมให้หน่วยงานด้านการคุ้มครองข้อมูลส่วน บุคคลประเทศเยอรมัน อาทิ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือตัวแทนที่ได้รับการแต่งตั้งจากกรรมการคุ้มครองข้อมูล

ส่วนบุคคล เข้าทำการตรวจสอบว่าได้ปฏิบัติตามหลักเกณฑ์คุ้มครองข้อมูลส่วนบุคคลหรือไม่

จากข้อเท็จจริงข้างต้น ก็มีปัญหาที่ต้องพิจารณาว่าข้อสัญญาดังกล่าวสามารถให้การความคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ อันเข้าข้อยกเว้นที่สามารถโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสมาชิก EU ได้หรือไม่[40] ซึ่งก็มีผู้เห็นว่าการทำสัญญาที่มีเงื่อนไขดังกล่าวสามารถให้การคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

ประเด็นต่อมาคือ การทำ Agreement on Interterritorial Data Protection ระหว่างสาขาธนาคารซิตี้แบงค์ที่ตั้งอยู่ในประเทศเยอรมันและสหรัฐอเมริกานั้น เจ้าของข้อมูลก็มิได้เป็นคู่กรณีในสัญญาด้วยแต่อย่างใด แต่ก็สามารถใช้สิทธิบางประการได้และยังสามารถบังคับใช้สิทธิของตนโดยตรงต่อศาลในประเทศเยอรมัน จึงย่อมถือได้ว่าสัญญาดังกล่าวเป็นสัญญาเพื่อประโยชน์ของบุคคลภายนอก[41] และเป็นที่ยอมรับตามหลักกฎหมายประเทศเยอรมัน

นอกจากนี้ มีข้อสังเกตว่าการระบุไว้ในสัญญาว่าธนาคารซิตี้แบงค์ในประเทศสหรัฐอเมริกาจะต้องยอมให้กรรมการคุ้มครองข้อมูลส่วนบุคคลของเยอรมันเข้าทำการตรวจสอบว่าได้ปฏิบัติตามหลักเกณฑ์คุ้มครองข้อมูลส่วนบุคคลที่ระบุไว้ในสัญญาหรือ

---

[40] EU Directive, Article 26 (2)

[41] สัญญาเพื่อประโยชน์บุคคลภายนอกเป็นสัญญาที่ก่อให้เกิดหนี้แก่คู่สัญญาฝ่ายใดฝ่ายหนึ่งหรือทั้งสองฝ่ายที่จะต้องชำระหนี้ตามสัญญาให้แก่บุคคลภายนอก บุคคลภายนอกนั้นเป็นบุคคลที่จะได้รับประโยชน์จากสัญญา อย่างไรก็ตามคู่สัญญานั้นนอกจากกำหนดให้บุคคลภายนอกได้รับประโยชน์จากสัญญาแล้ว อาจจะกำหนดให้บุคคลภายนอกต้องชำระหนี้ตอบแทนให้ด้วยก็ได้ แต่จะไปบังคับให้บุคคลภายนอกกระทำการชำระหนี้ให้แก่คู่สัญญาเท่านั้นอย่างเดียวไม่ได้ เพราะเป็นเรื่องของบุคคลภายนอกที่จะเลือกว่าจะรับประโยชน์ตามสัญญาหรือไม่ ถ้าเลือกจะรับประโยชน์ตามสัญญาก็ต้องชำระหนี้ตอบแทนตามที่ได้มีการกำหนดในสัญญา แต่ไม่อยากชำระหนี้ก็ไม่ต้องรับประโยชน์อันนั้น , ดู อัครวิทย์ สุมาวงศ์, คู่มือการศึกษาประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยนิติกรรมและสัญญา (สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา) หน้า 231.

ไม่นั้น แท้จริงแล้วจะสามารถบังคับการให้เป็นไปตามสัญญาได้มากน้อยเพียงใด เนื่องจากในทางปฏิบัติกรรมการคุ้มครองข้อมูลส่วนบุคคลของเยอรมันอาจไม่มีงบประมาณหรือบุคลากรที่เพียงพอในการเข้าไปตรวจสอบด้วยตนเองหรือมอบหมายให้องค์กรอื่นเข้าทำการตรวจสอบในนามกรรมการได้

กรณีการโอนข้อมูลหมายเลขโทรศัพท์บริษัท General Motor[42]

ในปี ค.ศ. 2003 บริษัท General Motors มีแผนการที่จะจัดทำฐานข้อมูลหมายเลขโทรศัพท์ของพนักงานในสำนักงานสาขาต่างๆ ทั่วโลกโดยจะเก็บฐานข้อมูลดังกล่าวไว้ในเครื่องให้บริการ (server) ของสำนักงานใหญ่ซึ่งตั้งอยู่ในประเทศสหรัฐอเมริกา เพื่อให้พนักงานของบริษัทจากทั่วโลกเข้าถึงฐานข้อมูลหมายเลขโทรศัพท์ดังกล่าวได้ แต่ปรากฏว่าแผนการดังกล่าวก็ต้องล่าช้ากว่ากำหนดการเดิมเนื่องจากประสบปัญหาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่เข้มงวด โดย EU ให้ความเห็นว่า หมายเลขโทรศัพท์ของพนักงานเป็นข้อมูลส่วนตัว ดังนั้น การโอนข้อมูลดังกล่าวไปยังประเทศอื่นนอกเหนือจากประเทศสมาชิก EU จึงไม่อาจกระทำได้ในทันที ดังนั้น บริษัท General Motors จึงจำเป็นจะต้องศึกษาข้อกฎหมายพร้อมทั้งจัดทำเอกสารทางกฎหมายที่เกี่ยวข้องกับการโอนข้อมูลข้อมูล เพื่อให้สามารถโอนข้อมูลหมายเลขโทรศัพท์ของพนักงานจากสำนักงานสาขาซึ่งตั้งอยู่ในประเทศสมาชิก EU ไปยังสำนักงานใหญ่ซึ่งตั้งอยู่ในประเทศสหรัฐอเมริกาเป็นไปโดยชอบด้วยกฎหมายภายในของประเทศนั้นๆ ซึ่งจากการดำเนินการดังกล่าวก็เป็นเหตุให้บริษัท General Motors ต้องใช้เวลาเพื่อดำเนินการดังกล่าวข้างต้นเป็นเวลาถึงหกเดือนจึงจะแล้วเสร็จ ซึ่ง Bob Rothman ผู้ปฏิบัติหน้าที่เป็นหัวหน้าเจ้าหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคล (Chief Privacy Officer) ของบริษัท General Motors ก็ได้ให้ความเห็นว่า ผลจากหลักเกณฑ์การคุ้มครองข้อมูลส่วนที่เข้มงวดของ EU

[42] David Sheer. “Europe’s New High-Tech Role: Playing Privacy Cop to World.” <http://cryptome.org/eu-dat-cop.htm>. October 2003.

ก็ได้ส่งผลให้บริษัท General Motors ต้องสูญเสียงบประมาณและเวลามากเกินกว่าที่ควรจะเป็นมาก[43]

เพื่อเป็นการแก้ไขปัญหาในระยะยาวบริษัท General Motors จึงได้จัดให้มีเจ้าหน้าที่เพื่อปฏิบัติหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลในสำนักงานสาขาแต่ละประเทศ เพื่อให้สามารถปฏิบัติได้ครบตามเงื่อนไขของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศซึ่งมีความแตกต่างกัน และต่อมาบริษัท General Motors ก็ได้จัดตั้งสำนักงานคุ้มครองข้อมูลส่วนบุคคลกลาง (global privacy center) เพื่อทำหน้าที่ประสานงานระหว่างเจ้าหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลในประเทศต่างๆ ทั่วโลก[44]

อนึ่ง แม้ต่อมาภายหลังจากประเทศสหรัฐอเมริกาได้จัดทำข้อตกลง Safe Harbor กับ Commission แล้วก็ตาม แต่บริษัท General Motors ก็หาได้เข้าร่วมโครงการดังกล่าวแต่อย่างใดเนื่องจากหากบริษัทจะต้องปฏิบัติตามหลักเกณฑ์ในโครงการ Safe Harbor แล้วก็จะต้องใช้ระยะเวลาหลายเดือนในการสำรวจว่าฐานข้อมูลหมายเลขโทรศัพท์ของพนักงานที่จะจัดทำขึ้นนั้นจะถูกใช้โดยบุคคลใดและในประเทศใด[45]

สำนักงานใหญ่ของ General Motors ในสหรัฐอเมริกาจึงได้แจ้งไปยังพนักงานในสำนักงานที่ตั้งอยู่ในประเทศสมาชิก EU ว่าจะมีการโอนข้อมูลหมายเลขโทรศัพท์ของพนักงานไปยังสำนักงานใหญ่ในสหรัฐอเมริกา โดยสำนักงานใหญ่รับรองว่าจะปฏิบัติตามหลักเกณฑ์กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิก EU ทั้งนี้ หากพนักงานคนใดประสงค์คัดค้านการโอนดังกล่าวก็จะจัดให้มีบุคคลภายนอกทำหน้าที่เป็นผู้ไกล่เกลี่ย (third-party mediator) ให้เพื่อแก้ปัญหาดังกล่าวในที่สุด บริษัท General Motors จึงได้จัดทำสัญญาโอนข้อมูลส่วนบุคคลเพื่อให้สำนักงานสาขาต่างๆ ทั่วโลกกว่า 200 สาขา ลงนามในสัญญาซึ่งมีข้อความว่าสำนักงานสาขาแต่และ

---

[43] Ibid.

[44] Ibid.

[45] Ibid.

แห่งจะไม่ใช้ฐานข้อมูลหมายเลขโทรศัพท์ที่จัดทำขึ้นนั้นในทางมิชอบ อาทิ การขายข้อมูลไปให้ผู้ประกอบธุรกิจโดยใช้การตลาดแบบตรง เป็นต้น

กรณีของผู้ประกอบการสายการบินในสหรัฐอเมริกา[46]

ในปี 1998 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสวีเดน (Datainspektionen Fleminggatan)[47] ได้มีคำสั่งให้บริษัทสายการบินอเมริกัน (American Airlines) ทำการลบข้อมูลด้านสุขภาพ (health) ข้อมูลด้านการรักษาพยาบาล (medical detail)[48] ของผู้โดยสารสัญชาติสวีเดนในทันทีภายหลังจากได้เดินทางถึงที่หมายแล้วในทุกเที่ยวบิน เว้นแต่จะได้รับการยินยอมจากผู้โดยสารโดยชัดแจ้ง (explicit consent) ว่าอนุญาตให้ทำการเก็บข้อมูลนั้นต่อไปนี้ ซึ่งปกติแล้วจะมีการเก็บข้อมูลต่างๆ เหล่านี้ในขณะที่ทำการจองตั๋วเครื่องบิน และจากผลของคำสั่งดังกล่าวนี้เองที่ส่งผลให้บริษัทสายการบินอเมริกันไม่สามารถส่งข้อมูลไปยังศูนย์กลางระบบการจองตั๋วโดยสาร (SABRE central reservation system) ที่ตั้งอยู่ในประเทศสหรัฐอเมริกาได้

ต่อมาบริษัทสายการบินอเมริกันก็ได้ยื่นอุทธรณ์คำสั่งข้างต้นต่อศาลปกครองชั้นต้น (County Administrative Court) ในประเทศสวีเดน โดยให้เหตุผลว่า การขอความยินยอมจากผู้โดยสารโดยชัดแจ้งเพื่อให้มีการโอนข้อมูลส่วนบุคคลไปยังสหรัฐอเมริกานั้นไม่สามารถทำได้ในทางปฏิบัติ (impractical) อีกทั้งก่อให้เกิดความไม่สะดวกแก่ผู้โดยสารเนื่องจากจำเป็นต้องให้ข้อมูลใหม่ทุกครั้งที่จองตั๋วเครื่องบินกับทางบริษัท

อย่างไรก็ตาม ศาลปกครองก็ไม่เห็นด้วยกับข้ออุทธรณ์ดังกล่าว โดยกล่าวว่าเหตุผลเกี่ยวกับความไม่สะดวกของผู้โดยสารไม่อาจนำมาใช้เป็นข้อยกเว้นในการ

---

[46] John R. Vacca, p.572.

[47] สามารถสืบค้นรายละเอียดเพิ่มเติมได้ที่ <http://www.datainspektionen.se/>

[48] ตัวอย่างเช่น อาหารที่ทำให้เกิดอาการแพ้ (allergies), อาการหืดหอบ (asthma), การงดอาหาร (dietary)

บังคับใช้กฎหมายได้ หลังจากนั้นก็ได้มีการยื่นอุทธรณ์ต่อไปยังศาลปกครองสูงสุด ซึ่งศาลปกครองสูงสุดก็ได้ยกคำร้องอุทธรณ์ดังกล่าวเช่นกัน

3.2 ผลกระทบต่อผู้ประกอบการในประเทศไทย

เคยมีปัญหาที่เกิดขึ้นอันเนื่องจากหลักเกณฑ์การโอนข้อมูลส่วนบุคคลของประเทศสมาชิก EU เกิดขึ้นแล้วในประเทศไทยกรณีที่ บริษัท การบินไทย จำกัด (ในขณะนั้น) ได้รับการสอบถามจากสายการบินลุฟทานซาว่าประเทศไทยมีหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลหรือไม่ เนื่องจากจำเป็นต้องมีการโอนข้อมูลผู้โดยสายจากชาติยุโรปมาให้บริษัทการบินไทยในประเทศไทยด้วย ซึ่งบริษัทการบินไทยก็ได้ชี้แจงว่า เนื่องจากประเทศไทยมีพระราชบัญญัติว่าด้วยข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่ให้การคุ้มครองข้อมูลส่วนบุคคลซึ่งการบินไทยก็เป็นหน่วยงานของรัฐซึ่งตกอยู่ภายใต้บังคับของพระราชบัญญัติดังกล่าวด้วย แต่อย่างไรก็ตาม ก็ได้มีการจัดทำสัญญาโอนข้อมูลส่วนบุคคลระหว่างบริษัทการบินไทยกับสายการบินลุฟทานซาในเวลาต่อมา[49]

3.3 การแก้ปัญหาของรัฐบาลสหรัฐอเมริกาโดย Safe Harbor

แม้สหรัฐอเมริกาจะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลหลายฉบับ ได้แก่ Privacy Act 1974, Fair Credit Reporting Act 1970, Health Insurance Portability and Accountability Act 1996, Children's On line Privacy Protection Act 1998, Financial Modernization Act 1999 รวมไปถึงการมีกลไกกำกับดูแลตนเอง (self-regulation)[50] โดยการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) หรือ Code of Conduct ของภาคอุตสาหกรรมต่างๆ

---

[49] สัมภาษณ์ สิทธินัย จันทรานนท์ , นิติกร 6 บริษัทการบินไทย จำกัด (มหาชน), 10 มีนาคม 2547

[50] ในกรณีที่ไม่ปฏิบัติตามกลไกกำกับดูแลตนเองที่ได้ประกาศไว้ FTC ก็มีอำนาจสั่งการให้ปฏิบัติตามกลไกกำกับดูแลตนเองดังกล่าวและกำหนดให้ชำระค่าเสียหายแก่ผู้บริโภคได้

แต่อย่างไรก็ตาม ประเทศสหรัฐอเมริกาก็หาได้รับการพิจารณาจากประเทศสมาชิก EU ว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอแต่อย่างใด โดยปัจจัยสำคัญประการหนึ่งที่ทำให้ประเทศสมาชิก EU มองว่าประเทศสหรัฐอเมริกาไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอคือ การไม่มีองค์กรระดับชาติด้านการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะนั่นเอง[51]

เพื่อหลีกเลี่ยงปัญหาที่จะเกิดขึ้นต่อไปอันเนื่องจากการโอนข้อมูลส่วนบุคคลรัฐบาลประเทศสหรัฐอเมริกาโดยกระทรวงพาณิชย์ (Department of Commerce) จึงได้เริ่มเจรจากับ Commission เพื่อหาทางในการสร้างความเชื่อมั่นว่าประเทศสหรัฐอเมริกามีระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ และสร้างความมั่นใจในการโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ไปยังสหรัฐอเมริกาได้

ผลจากการเจรจาเป็นเวลาสองปีระหว่าง Commission และสหรัฐอเมริกาดังกล่าว ก็ได้ก่อให้เกิดข้อตกลงระหว่าง Commission กับรัฐบาลสหรัฐอเมริกาที่เรียกว่า ข้อตกลง “Safe Harbor Principles” เมื่อวันที่ 26 กรกฎาคม ค.ศ. 2000 โดยข้อตกลงดังกล่าวมีหลักการสำคัญว่า บริษัทหรือองค์กรใดที่เข้าร่วมในโครงการ Safe Harbor จะสามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ได้อย่างปราศจากข้อจำกัดใดๆ ทั้งนี้ บริษัทหรือองค์กรที่เข้าร่วมโครงการ[52]ดังกล่าวจะต้องปฏิบัติตามหลักการ คุ้มครองข้อมูลส่วนบุคคลใน 7 ประการดังต่อไปนี้

โดยอาศัยอำนาจตาม Section 5 ของ Federal Trade Commission Act (15 U.S.C. A. 41) เนื่องจากถือว่าเป็นการกระทำที่เข้าข่ายไม่เป็นธรรมและเป็นการหลอกลวงผู้บริโภค (unfair and deceptive acts or practice)

[51] John R. Vacca, p.571.

[52]องค์กรหรือหน่วยงานที่เข้าร่วมโครงการดังกล่าวได้จะต้องเป็นองค์กรหรือหน่วยงานที่ตกอยู่ภายใต้บังคับของ FTC และกระทรวงการขนส่ง (Department of Transportation: DOT)

- **หลักการแจ้งให้ทราบ (Notice)**

ผู้ประกอบการจะต้องแจ้งให้เจ้าของข้อมูลทราบถึงวัตถุประสงค์ในการรวบรวมและประมวลผลข้อมูลส่วนบุคคล รวมไปถึงจะนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยในกรณีใดบ้าง อีกทั้งวิธีการที่เจ้าของข้อมูลจะใช้สิทธิในการควบคุมหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลของตน

- **หลักการให้สิทธิเลือก (Choice)**

ผู้ประกอบการจะต้องให้สิทธิแก่เจ้าของข้อมูลในการห้ามมิให้มีการใช้และประมวลผลข้อมูลของตนอีกต่อไป (Opt-out) หรือหากเป็นกรณีข้อมูลส่วนบุคคลชนิดพิเศษ (sensitive) อาทิ ข้อมูลด้านสุขภาพ เชื้อชาติ ก็จะต้องได้รับอนุญาตให้เก็บรวบรวมข้อมูล (Opt-in) จากเจ้าของข้อมูลเสียก่อน

- **หลักการห้ามโอนข้อมูลต่อ (Onward Transfer)**

ผู้ประกอบการจะต้องให้การรับรองว่า จะไม่โอนหรือเปิดเผยข้อมูลส่วนบุคคลไปยังบุคคลอื่นต่อไป เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลเสียก่อน ทั้งนี้บุคคลผู้รับโอนข้อมูลส่วนบุคคลต่อไปนั้นจะต้องเป็นองค์กรที่เข้าร่วมโครงการ Safe Harbor หรือเป็นองค์กรที่ตกอยู่ภายใต้ผลการบังคับของ Directive หรือได้ทำสัญญาการโอนข้อมูลส่วนบุคคล (transborder data flow agreement)

- **หลักการรักษาความปลอดภัย (Security)**

ผู้ประกอบการจะต้องมีนโยบายและมาตรการรักษาความปลอดภัยในข้อมูลส่วนบุคคลที่เพียงพอ เพื่อป้องกันการใช้ (use) หรือเปิดเผย (disclose) โดยมิชอบตลอดจนป้องกันการทำให้เสียหาย (loss) หรือทำลายซึ่งข้อมูลส่วนบุคคล

- **หลักความถูกต้องแท้จริงของข้อมูล (Data Integrity)**

ข้อมูลที่บริษัทหรือองค์กรจะนำไปประมวลผลนั้นจะต้องเป็นข้อมูลที่มีความ-ถูกต้องแท้จริง (Integrity) มีความครบถ้วน (complete) และเป็นปัจจุบัน

- **หลักการเข้าถึงข้อมูล (Access)**

ผู้ประกอบการจะต้องเปิดโอกาสให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลของตน ตลอดจนให้สิทธิแก่เจ้าของข้อมูลในการลบ หรือแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องภายใต้เงื่อนไขและวิธีการอันสมเหตุสมผล

- **หลักการบังคับใช้ (Enforcement)**

ผู้ประกอบการจะต้องเผยแพร่วิธีการระงับข้อพิพาทที่เกิดขึ้นอันเนื่องจากข้อมูลส่วนบุคคลและจะต้องปฏิบัติตามวิธีการดังกล่าว ทั้งนี้ วิธีการระงับข้อพิพาทดังกล่าวจะต้องครอบคลุมถึงการให้สิทธิแก่เจ้าของข้อมูลในการร้องเรียน (complain) เพื่อให้มีการสอบสวนและชี้ขาดในกรณีที่มิได้ปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลตาม Safe Harbor ตามข้อร้องเรียนของเจ้าของข้อมูล

การเข้าร่วม Safe Harbor

ผู้ประกอบการที่ต้องการเข้าร่วมโครงการ Safe Harbor ก็จะต้องดำเนินการให้สอดคล้องกับหลักเกณฑ์ทั้ง 7 ประการข้างต้น โดยในการปฏิบัติให้สอดคล้องกับหลักเกณฑ์ดังกล่าวบริษัทหรือองค์กรก็สามารถเลือกที่จะดำเนินการในทางใดทางหนึ่งดังนี้

1) เข้าร่วมโครงการกลไกกำกับดูแลตนเองที่มีหลักการสอดคล้องกับหลักเกณฑ์ของ Safe Harbor
2) จัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของตนเองที่สอดคล้องกับหลักเกณฑ์ของ Safe Harbor[53]

[53] International Trade Administration, Department of Commerce, “Safe Harbor Overvies” The Privacy Papers : Managing Technology, Consumer, Employee, and Legislative Action, ed. Rebecca Herole (New York : CRC Press LLC, 2002), p.620.

หลังจากนั้นก็ยื่นหนังสือไปยังกระทรวงพาณิชย์ (Department of Commerce: DOC) เพื่อแจ้งให้ทราบว่าบริษัทหรือองค์กรของตนจะปฏิบัติตามหลักเกณฑ์ใน Safe Harbor ทั้ง 7 ประการข้างต้น โดยในหนังสือดังกล่าวจะต้องระบุรายละเอียดต่างๆ ตามที่ Safe Harbor กำหนดไว้ด้วย อาทิ รายละเอียดเกี่ยวกับการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลที่ได้รับจากประเทศสมาชิก EU, หน่วยที่ทำหน้าที่รับข้อร้องเรียนหรือร้องขอเพื่อเข้าถึงข้อมูลจากเจ้าของข้อมูล กระบวนการระงับข้อพิพาทในกรณีที่ไม่สามารถปฏิบัติตามคำร้องเรียนจากเจ้าของข้อมูล และเมื่อบริษัทหรือองค์กรดังกล่าวได้ผ่านการตรวจรายละเอียดต่างๆ เกี่ยวในการสมัครเป็นที่เรียบร้อยแล้วก็จะได้รับการประกาศการเป็นสมาชิกโครงการ Safe Harbor ผ่านเว็บไซต์ของกระทรวงการส่งออก (Department of Export)[54]

ประโยชน์จากการเข้าร่วม Safe Harbor ของผู้ประกอบการ

ประโยชน์ที่บริษัทหรือองค์กรจะได้รับจากการเข้าร่วมโครงการ Safe Harbor คือ มีผลผูกพันให้ประเทศสมาชิก EU ยอมรับว่าบริษัทหรือองค์กรนั้นๆ สามารถให้การคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ[55] และสามารถดำเนินการโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ได้ต่อไป และยังสามารถช่วยให้ลดขั้นตอนการ

---

[54] สามารถตรวจสอบรายชื่อบริษัทหรือองค์กรที่เข้าร่วมโครงการ Safe Harbor ได้ที่ <http://www.export.gov/safeharbor/>

[55] EU Directive, Article 25(6)

โอนข้อมูลส่วนบุคคลที่ยุ่งยากได้ด้วย เนื่องจากหากประเทศสมาชิก EU ใดมีบทบัญญัติให้ต้องมีการขออนุญาตโอนข้อมูลส่วนบุคคลก่อน ก็ไม่จำเป็นต้องยื่นคำร้องขอเพื่อโอนข้อมูลส่วนบุคคลอีกต่อไป นอกจากนี้ ยังสามารถทำให้องค์กรหรือหน่วยงานต่างๆ สามารถปฏิบัติตามหลักเกณฑ์ของ EU Directive ได้ง่ายขึ้นและมีต้นทุนที่ต่ำ ซึ่งจะเป็นประโยชน์อย่างยิ่งแก่ประกอบวิสาหกิจขนาดกลางและขนาดย่อม[56]

[56] International Trade Administration, Department of Commerce, p.620.

บทที่ 4
ผู้ประกอบการจะต้องทำอย่างไร เมื่อจำเป็นต้องโอนข้อมูลส่วนบุคคลไปต่างประเทศ

4.1 สิ่งที่ผู้ประกอบการควรรู้เมื่อต้องโอนข้อมูลส่วนบุคคลไปต่างประเทศ

การโอนข้อมูลส่วนบุคคลกับประเทศในกลุ่มสหภาพยุโรป

สำหรับประเทศสมาชิก EU นั้น ส่วนใหญ่ก็ได้บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการโอนข้อมูลส่วนบุคคลตามแนวทางของ EU Directive กล่าวคือห้ามมิให้โอนข้อมูลไปยังประเทศนอกสมาชิก EU เว้นแต่ประเทศที่รับโอนข้อมูลนั้นมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ อย่างไรก็ตาม ประเทศสมาชิก EU ก็ได้กำหนดหลักเกณฑ์ปลีกย่อยในการพิจารณาว่าประเทศใดมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอแตกต่างกันพอสมควร อาทิ

ประเทศฝรั่งเศส โปรตุเกส และสเปน ได้ให้อำนาจแก่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการพิจารณาว่าประเทศนอกสมาชิกใดมีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ นอกเหนือจากประเทศที่ได้รับการพิจารณาชี้ขาดจาก Commission ในขณะที่ประเทศเบลเยี่ยม[57] เนเธอแลนด์ และสวีเดน ได้ให้อำนาจแก่

[57] โดยการประกาศเป็นพระราชกฤษฎีกา

รัฐมนตรีว่าการกระทรวงยุติธรรมหรือรัฐบาลในการพิจารณาดังกล่าว ส่วนประเทศอื่นที่เหลืออีก 9 ประเทศหาได้ให้อำนาจแก่คณะกรรมการหรือหน่วยงานของรัฐในการใช้อำนาจดังกล่าวแต่อย่างใด ทั้งนี้ แนวโน้มในการพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบันจะยึดถือตามคำชี้ขาดของ Commission เป็นสำคัญ ทั้งนี้ หากประเทศใดยังไม่ได้รับการพิจารณาชี้ขาดจาก Commission ดังกล่าว ก็เป็นดุลพินิจของผู้ควบคุมข้อมูลในการประเมินว่าประเทศที่จะรับโอนข้อมูลส่วนบุคคลนั้นมีการคุ้มครองข้อมูลส่วนบุคคลที่ดีพอหรือไม่

การโอนข้อมูลส่วนบุคคลกับประเทศอื่น

โดยทั่วไปแล้วการพิจารณาว่าประเทศใดมีการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอหรือไม่ในประเทศซึ่งมิได้เป็นสมาชิก EU ก็มีลักษณะเช่นเดียวกับที่กำหนดในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิก EU กล่าวคือ เป็นดุลยพินิจของผู้ควบคุมข้อมูลหรือผู้ที่ต้องการโอนข้อมูลส่วนบุคคลในการประเมินว่าการให้ความคุ้มครองข้อมูลส่วนบุคคลในประเทศที่จะรับโอนข้อมูลมีระดับที่เพียงพอหรือไม่โดยไม่จำเป็นต้องขออนุญาตจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเสียก่อน อย่างไรก็ตาม คณะกรรมการก็มีอำนาจที่จะตรวจสอบการโอนข้อมูลดังกล่าวหากพบข้อสงสัยหรือได้รับคำร้องเรียนว่าการโอนข้อมูลส่วนบุคคลโดยฝ่าฝืนบทบัญญัติของกฎหมาย และหากพบว่า ข้อสงสัยหรือคำร้องเรียนดังกล่าวเป็นความจริง คณะกรรมการก็มีอำนาจในการออกคำสั่งให้มีการแก้ไขหรือดำเนินการให้ถูกต้อง หากยังคงฝ่าฝืนคำสั่งดังกล่าวอยู่ต่อไปก็เป็นสาเหตุหนึ่งในการถูกมาตรการบังคับทางกฎหมายได้ โดยประเทศที่ใช้หลักเกณฑ์เช่นว่านี้ได้แก่ ฮ่องกง[58]

อย่างไรก็ตาม ในบางประเทศก็ได้ให้อำนาจแก่คณะกรรมการคุ้มครองข้อมูลในการประกาศว่าประเทศใดเป็นประเทศซึ่งมีให้การคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอตัวอย่างเช่น ฮ่องกงก็ได้บัญญัติกฎหมายโดยให้อำนาจแก่คณะ

---

[58] Office of the Privacy Commissioner for Personal Data, Hong Kong. "Transfer of Personal Data Outside Hong Kong : Some Common Question." <http://www.pco.org.hk/english/publications/fact1_intro_1.html>. April 1997.

กรรมการคุ้มครองข้อมูลส่วนบุคคลในการประกาศรายชื่อประเทศที่ได้พิจารณาเห็นว่ามีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ[59] แต่ปรากฏว่าจนถึงปัจจุบันคณะกรรมการก็ยังไม่ได้มีออกประกาศดังกล่าวแต่อย่างใด[60]

4.2 ทางเลือกของผู้ประกอบการเมื่อจำเป็นต้องโอนข้อมูลส่วนบุคคลไปต่างประเทศ

แม้ว่าปัจจุบันประเทศไทยจะยังไม่มีกฎหมายกำหนดหลักเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลไปต่างประเทศก็ตาม[61] โดยมีแต่เพียงแนวปฏิบัติที่ออกโดยบางหน่วยงานเท่านั้น ดังจะเห็นได้จากการจัดทำแนวปฏิบัติสำหรับการโอนข้อมูลส่วนบุคคลไปต่างประเทศโดยธนาคารแห่งประเทศไทย ซึ่งออกเป็นหนังสือเวียน ที่ ธปท. สนส. (01) ว.1191/2546) เรื่อง แนวปฏิบัติในการใช้บริการ ด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing) เมื่อวันที่ 14 พฤษภาคม 2546 ใน

---

[59] Personal Data (Privacy) Ordinance, Section 34(3)

[60] White & Case LLP, “2003 Data Privacy Survey : Cross-Border Transborder of Personal Data in 22 Major Jurisdictions”, Paper presented at Third Annual Global Privacy Symposium, New York, 14 May 2003.

[61] ร่างกฎหมายที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้มีการกำหนดหลักเกณฑ์ดังกล่าวไว้ว่า

“ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศซึ่งมิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกันในสาระสำคัญเช่นเดียวกับบทบัญญัติแห่งพระราชบัญญัตินี้ เว้นแต่ในกรณีดังต่อไปนี้

(1) ได้รับความยินยอมจากเจ้าของข้อมูล

(2) เป็นความจำเป็นเพื่อชำระหนี้ตามความผูกพันที่เป็นผลของสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเป็นสัญญาระหว่างหน่วยงานกับบุคคลอื่นที่เป็นไปเพื่อประโยชน์ของเจ้าของข้อมูล

(3) กระทำเพื่อประโยชน์ของบุคคลซึ่งไม่สามารถให้ความยินยอมได้

(4) กรณีอื่นใดตามที่คณะกรรมการประกาศกำหนด”

หลักการข้อ 4 วรรคสอง ซึ่งระบุว่า *"สำหรับสถาบันการเงินที่เคยได้รับอนุญาตจากธนาคารแห่งประเทศไทยในเรื่องการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่นหรือการนำข้อมูลไปประมวลผลในต่างประเทศโดยมีเงื่อนไขประกอบ ให้ยกเลิกเงื่อนไขดังกล่าวและให้ถือปฏิบัติตามแนวปฏิบัตินี้แทน อย่างไรก็ดี สถาบันการเงินยังคงสามารถปฏิบัติตามข้อตกลงหรือสัญญาเดิมที่ได้ทำไว้กับผู้ให้บริการได้จนกว่าจะมีการเปลี่ยนแปลง ต่ออายุหรือจัดทำข้อตกลงหรือสัญญาใหม่"* ซึ่งปรากฏว่าในรายละเอียดของแนวปฏิบัติดังกล่าวหาได้กำหนดหลักเกณฑ์เกี่ยวกับการนำข้อมูลไปประมวลผลในต่างประเทศไว้แต่อย่างใด ซึ่งจากเนื้อความดังกล่าวแสดงให้เห็นว่าปัจจุบันการโอนข้อมูลส่วนบุคคลโดยสถาบันการเงินในประเทศไทยไปยังสำนักงานใหญ่หรือสำนักงานสาขาในต่างประเทศ หรือการโอนข้อมูลไปยังผู้ให้บริการด้านงานเทคโนโลยีสารสนเทศซึ่งตั้งอยู่ในต่างประเทศสามารถดำเนินการได้โดยปราศจากเงื่อนไขใดๆ ดังนั้นเพื่อหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นกับประเทศที่มีหลักเกณฑ์ข้อจำกัดการโอนข้อมูลส่วนบุคคลที่เข้มงวดผู้ประกอบการก็สามารถดำเนินการเกี่ยวกับการโอนข้อมูลส่วนบุคคลได้ในหลายรูปแบบ ไม่ว่าจะโดยการทำสัญญาโอนข้อมูลส่วนบุคคล การจัดทำนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองภายในองค์กร (Binding Corporate Rules) หรือการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัว (Privacy Impact Assessment)

การจัดทำสัญญาโอนข้อมูลส่วนบุคคล

ในกรณีที่มีการทำสัญญาโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU ไปยังประเทศนอกสมาชิกโดยใช้สัญญาแม่แบบที่จัดทำขึ้นโดย Commission นั้น ก็จะมีผลว่าทั้งผู้โอนและผู้รับข้อมูลจะต้องรับผิดร่วมกันหากเจ้าของข้อมูลได้รับความเสียหายอันเนื่องจากผลของการโอนข้อมูลส่วนบุคคลนั้น ซึ่งเจ้าของข้อมูลมีสิทธิเลือกวิธีการระงับข้อพิพาทในรูปแบบต่างๆ ได้เอง ไม่ว่าจะเป็นการไกล่เกลี่ยข้อพิพาท อนุญาโตตุลาการหรือแม้แต่การฟ้องร้องต่อศาล โดยกฎหมายที่นำมาปรับใช้บังคับกับสัญญาแม่แบบดังกล่าว ก็ได้มีการกำหนดให้นำเอากฎหมายภายในของประเทศสมาชิก EU ที่ผู้โอนข้อมูลได้จัดตั้งขึ้นมาใช้บังคับกับสัญญาที่ได้จัดทำขึ้น ดังจะเห็นได้

ตัวอย่างในสัญญาแม่แบบในการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลในต่างประเทศนั้น ซึ่งกำหนดรายละเอียดในหัวข้อต่างๆ ดังต่อไปนี้

- **ชื่อ สถานที่ตั้ง ของผู้โอนข้อมูล (Exporter)**
- **ชื่อ สถานที่ตั้ง ของผู้รับโอนข้อมูล (Importer)**
- **คำนิยาม "ข้อมูลส่วนบุคคล", "ผู้โอนข้อมูล", "ผู้รับโอนข้อมูล"**
- **รายละเอียดของการโอนข้อมูล** (กำหนดให้คู่สัญญากรอกรายละเอียดในเอกสารผนวกท้ายข้อสัญญา) ซึ่งได้แก่ ลักษณะการดำเนินการผู้โอนข้อมูลที่เกี่ยวข้องกับการโอนข้อมูล ลักษณะการดำเนินการผู้รับโอนข้อมูลที่เกี่ยวข้องกับการโอนข้อมูล เจ้าของข้อมูลในข้อมูลที่โอน (คู่สัญญาจะต้องระบุถึงประเภทของเจ้าของข้อมูลด้วย) วัตถุประสงค์ของการโอนข้อมูล (คู่กรณีจะต้องระบุเหตุผลความจำเป็นในการโอนข้อมูล) ประเภทของข้อมูลส่วนบุคคลที่มีการโอน (จะต้องระบุประเภทของข้อมูลส่วนบุคคลที่จะมีการโอน) ประเภทของข้อมูลส่วนบุคคลชนิดพิเศษ (sensitive data) ที่มีการโอน (จะต้องระบุประเภทของข้อมูลส่วนบุคคลชนิดพิเศษว่ามีประเภทใดบ้าง) ผู้รับโอนข้อมูลต่อ (recipients) (ข้อมูลส่วนบุคคลที่โอนไปยังผู้รับโอนนั้นอาจถูกโอนต่อไปยังบุคคลอื่นได้ตามที่ระบุไว้เท่านั้น) ระยะเวลาการเก็บรักษาข้อมูล (ข้อมูลส่วนบุคคลจะถูกจัดเก็บไว้ภายหลังการโอนไม่เกินระยะเวลาที่คู่กรณีตกลงกัน) ข้อสัญญาเพื่อประโยชน์ของบุคคลที่สาม (Third-party beneficiary clause) (เจ้าของข้อมูลสามารถบังคับใช้สิทธิของตนแม้มิได้เป็นคู่สัญญา) สิทธิที่จะได้รับแจ้งล่วงหน้าว่าข้อมูลที่จะโอนไปนั้นเป็นข้อมูลส่วนบุคคลชนิดพิเศษ และข้อมูลดังกล่าวจะถูกโอนไปยังประเทศที่มีระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ สิทธิในการร้องขอสำเนาสัญญาโอนข้อมูลส่วนบุคคล การยื่นข้อซักถามหรือข้อสงสัยใดๆ เกี่ยวกับการประมวลผลข้อมูล การเรียกร้องค่าเสียหายอันเนื่องจากการละเมิดข้อสัญญาเพื่อประโยชน์บุคคลภายจากคู่สัญญา สิทธิในการเลือกใช้วิธีการระงับข้อพิพาท เป็นต้น

- **หน้าที่ของผู้โอนข้อมูล (Obligations of the data exporter)**

ผู้โอนข้อมูลมีหน้าที่ต่างๆ ดังต่อไปนี้ การประมวล และการโอนข้อมูลส่วนบุคคลจะต้องปฏิบัติให้สอดคล้องกับบทบัญญัติของกฎหมายภายในของประเทศสมาชิก EU ที่ผู้โอนข้อมูลมีสถานที่ทำการงานตั้งอยู่ ในกรณีที่ข้อมูลที่จะโอนไปนั้นเป็นข้อมูลส่วนบุคคลชนิดพิเศษ จะต้องแจ้งไปยังเจ้าของข้อมูลให้ทราบล่วงหน้าว่าข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะถูกโอนไปยังประเทศที่มีระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอ การจัดทำสำเนาข้อสัญญาโอนข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลเมื่อได้รับการร้องขอ การดำเนินการเพื่อสนองตอบต่อข้อซักถามหรือข้อสงสัยใดๆ เกี่ยวกับการประมวลผลข้อมูลตามที่ได้จากเจ้าของข้อมูลหรือหน่วยงานด้านการโอนข้อมูลส่วนบุคคลภายใต้ระยะเวลาอันควร

- **หน้าที่ของผู้รับโอนข้อมูล (Obligations of the data importer)**

ได้แก่ ผู้รับโอนข้อมูลจะต้องปฏิบัติตามข้อสัญญานี้โดยไม่สามารถอ้างได้ว่าเหตุแห่งการไม่ปฏิบัติตามข้อสัญญาได้ว่าจำเป็นต้องปฏิบัติตามที่กฎหมายบัญญัติไว้ซึ่งมีสำระสำคัญที่แตกต่างจากที่กำหนดไว้ในข้อสัญญา นอกจากนี้ ยังมีหน้าที่ต้องแจ้งไปยังผู้โอนข้อมูลและหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลที่ผู้โอนข้อมูลมีสถานที่ทำการตั้งอยู่ในกรณีที่ผู้โอนข้อมูลมีสิทธิระงับการโอนข้อมูล และ/หรือยุติข้อสัญญา นอกจากนี้ จะต้องปฏิบัติตามหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ในภาคผนวก 2 โดยเคร่งครัด (หลักเกณฑ์เป็นหลักการเดียวกับที่กำหนดไว้ใน EU Directive แต่ได้เพิ่มหลักเกณฑ์เกี่ยวกับข้อจำกัดการโอนข้อมูลส่วนบุคคลต่อ (onward transfer) เอาไว้ด้วย รวมทั้งตอบข้อซักถามหรือสงสัยแก่ผู้โอนข้อมูลหรือเจ้าของข้อูลภายในเวลาอันควร รวมถึงการให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการบังคับการให้เป็นไปตามกฎหมาย รวมไปถึงการปฏิบัติตามคำแนะนำของหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลที่ได้รับโอนมา และให้ข้อมูลเกี่ยวกับการประมวลผลแก่ผู้โอนข้อมูลเพื่อการตรวจสอบหรือผู้ตรวจสอบภายนอกที่คัดเลือกโดยผู้โอนข้อมูล และการจัดทำสำเนาข้อสัญญาโอนข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลเมื่อได้รับการร้องขอ และองค์กรภายในที่ทำหน้าที่รับเรื่องร้องเรียน

- **ความรับผิด (Liability)** ในกรณีที่เจ้าของข้อมูลได้รับความเสียหายอันเนื่องจากการละเมิดข้อสัญญาเพื่อประโยชน์บุคคลภายนอกที่กำหนดไว้ในข้อ 5) ย่อมมีสิทธิได้รับความเสียหายจากคู่สัญญา ทั้งนี้ คู่สัญญาจะปฏิเสธการชำระค่าเสียหายได้ต่อเมื่อสามารถพิสูจน์ได้ว่าตนไม่มีส่วนรับผิดชอบกับการละเมิดข้อสัญญาดังกล่าว ทั้งนี้ คู่สัญญาตกลงที่จะรับผิดชอบในค่าเสียหายแก่เจ้าของข้อมูลร่วมกันในกรณีที่มีการละเมิดข้อสัญญาเกิดขึ้น ไม่ว่าความเสียหายจะเกิดขึ้นอันเนื่องจากการละเมิดข้อสัญญาของอีกฝ่ายหนึ่งก็ตาม และในกรณีที่คู่สัญญาได้ชดใช้ค่าเสียหายให้แก่เจ้าของข้อมูลอันเนื่องจากการละเมิดข้อสัญญาของอีกฝ่ายหนึ่ง คู่กรณีที่ชดใช้ค่าเสียหายไปก็มีสิทธิเรียกร้องค่าเสียหายคืนเอาจากคู่สัญญาอีกฝ่ายหนึ่งได้

- **การไกล่เกลี่ยและเขตอำนาจศาล (Mediation and Jurisdiction)** ในกรณีที่มีข้อพิพาทระหว่างเจ้าของข้อมูลและคู่สัญญาเกี่ยวกับการไม่ปฏิบัติตามข้อสัญญาเพื่อประโยชน์ของบุคคลภายนอก คู่สัญญาตกลงที่จะดำเนินการตามที่เจ้าของข้อมูลใช้สิทธิเลือก ซึ่งได้แก่ การเสนอข้อพิพาทเพื่อการไกล่เกลี่ยโดยบุคคลภายนอก หรือหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล หรือเสนอข้อพิพาทไปยังศาลในประเทศสมาชิก EU ที่ผู้โอนข้อมูลส่วนบุคคลจัดตั้งขึ้น ซึ่งย่อมหมายความว่าหากมีการจัดทำสัญญาโอนข้อมูลส่วนบุคคลตามสัญญาแม่แบบจะต้องใช้กฎหมายภายในของประเทศสมาชิก EU มาปรับใช้ทุกสัญญานั่นเอง นอกจากนี้ เจ้าของข้อมูลอาจทำสัญญาอนุญาโตตุลาการเพื่อให้มีการชี้ขาดข้อพิพาทโดยอนุญาโตตุลาการได้ด้วย หากคู่สัญญาฝ่ายใดฝ่ายหนึ่งในสัญญาอนุญาโตตุลาการจัดตั้งขึ้นในประเทศที่ได้ให้สัตยาบันต่ออนุสัญญาว่าด้วยการบังคับตามคำชี้ขาดของอนุญาโตตุลาการต่างประเทศ (New York Convention) อย่างไรก็ตาม การใช้สิทธิต่างๆ ของเจ้าของข้อมูลที่ได้กล่าวมาแล้วนั้น หาได้เป็นการตัดสิทธิของเจ้าของข้อมูลในการเรียกร้องค่าเสียหายตามที่บัญญัติไว้ในกฎหมายภายในหรือกฎหมายระหว่างประเทศ

- **ความร่วมมือกับหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคล (Cooperation with supervisory authorities)** คู่กรณีตกลงที่จะมอบสำเนาของสัญญาโอนข้อมูลส่วนบุคคลนี้ให้แก่หน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลตามที่ได้รับการร้องขอหรือตามที่กฎหมายภายในบัญญัติไว้
- **ความสิ้นสุดของสัญญา (Termination of the Clauses)** ความสิ้นสุดของสัญญาไม่ว่าด้วยเหตุผลใดก็ตาม หาเป็นเหตุยกเว้นความรับผิดหรือเงื่อนไขที่ต้องปฏิบัติเกี่ยวกับการประมวลผลข้อมูลที่ถูกโอนไปแล้ว
- **กฎหมายที่ใช้บังคับกับสัญญา (Governing Law)**
- **การแก้ไขเปลี่ยนแปลงสัญญา (Variation of the contract)** กล่าวคือ คู่สัญญารับรองว่าจะไม่แก้ไขเปลี่ยนแปลงใดๆ ในสัญญาที่จัดทำขึ้นนี้

ในส่วนของสัญญาแม่แบบในการโอนข้อมูลส่วนบุคคลไปยังผู้ประมวลผลข้อมูลในต่างประเทศ ก็มีเนื้อในทำนองเดียวกับสัญญาแม่แบบในการโอนข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลในต่างประเทศ แต่ก็ได้เพิ่มหลักเกณฑ์ด้านการรักษาความปลอดภัยของข้อมูลส่วนบุคคล กล่าวคือ จะต้องมีให้รายละเอียดเกี่ยวกับเทคนิคหรือวิธีการที่ใช้ในการรักษาความปลอดภัยของข้อมูลของผู้รับโอนข้อมูลไว้ในเอกสารผนวกท้ายข้อสัญญาด้วย

มีข้อสังเกตว่า การทำสัญญาโอนข้อมูลส่วนบุคคลโดยอาศัยสัญญาแม่แบบของ Commission นั้นอาจไม่เหมาะสมสำหรับการใช้ในทางปฏิบัติสำหรับภาคธุรกิจเช่นกัน เนื่องจากขาดความยืดหยุ่น อีกทั้งส่งผลให้ต้องมีการจัดทำสัญญาโอนข้อมูลส่วนบุคคลเป็นจำนวนมากระหว่างสำนักงานสาขาขององค์กรหรือบริษัทต่างๆ มีสำนักงานตั้งอยู่ในหลายประเทศแม้ว่าเป็นองค์กรหรือบริษัทในเครือเดียวกันก็ตาม ซึ่งส่งผลทางกฎหมายต่อมาเป็นว่าการทำสัญญาที่คู่สัญญาเป็นบุคคลเดียวกัน

นอกจากการทำสัญญาโดยใช้สัญญาแม่แบบที่จัดทำขึ้นโดย EU Commission แล้ว ผู้โอนข้อมูลและผู้รับโอนข้อมูลก็อาจทำสัญญาโอนข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล ซึ่งก็มีปัญหาตามมาว่าในกรณีบริษัทหรือองค์กรใดมีสำนักงานสาขาอยู่ในหลายประเทศก็จำเป็นที่จะต้องยื่นเสนอกลไกหรือนโยบายดังกล่าวให้กับองค์กรคุ้มครองข้อมูลส่วนบุคคลในประเทศนั้นๆ ทำการพิจารณาในทุกประเทศที่สำนักงานสาขาของตนตั้งอยู่

ดังนั้น จึงได้มีการเสนอแนะโดยภาคเอกชนว่า สมควรให้มีความร่วมมือกันระหว่างองค์กรด้านการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศ เพื่อที่ว่าหากประเทศใดประเทศหนึ่งให้การรับรองกลไกหรือนโยบายดังกล่าวก็สมควรที่องค์กรในประเทศอื่นจะให้การรับรองเช่นเดียวกัน ทั้งนี้ ได้มีการเสนอแนะว่า เพื่อให้กลไกหรือนโยบายดังกล่าวสามารถบังคับใช้ได้ในทันทีโดยไม่จำต้องผ่านการตรวจสอบจากองค์กรด้านคุ้มครองข้อมูลส่วนบุคคลอีกครั้งหนึ่งโดยการกำหนดว่า หากองค์กรใดไม่สามารถปฏิบัติตามกลไกหรือนโยบายที่ตนประกาศไว้ก็ให้ถือว่าเป็นการกระทำที่เข้าข่ายไม่เป็นธรรมต่อผู้บริโภค ซึ่งหากมีการร้องเรียนโดยเจ้าของข้อมูลหรือตรวจสอบพบโดยองค์กรด้านคุ้มครองข้อมูลส่วนบุคคลว่าองค์กรดังกล่าวดังกล่าวไม่สามารถตามกลไกหรือนโยบายที่ให้ไว้ก็สามารถลงโทษได้ทันที[63] ซึ่งปัจจุบัน EU ก็ได้ตระหนักถึงความจำเป็นของหลักเกณฑ์ดังกล่าวและได้สร้างกรอบในการพิจารณา Biding Corporate Rule ว่าจะต้องมีคุณสมบัติในทำนองเดียวกับหลักเกณฑ์การพิจารณาระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศคือจะต้องมีเนื้อหาการคุ้มครองข้อมูลส่วนบุคคลที่ครบถ้วนและสามารถบังคับใช้ได้อย่างมีประสิทธิภาพ อาทิ การใช้ระบบการตรวจสอบ (audit) จากองค์กรที่ได้รับอนุญาตจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล การประสานความร่วมมือกันระหว่างหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศ เป็นต้น[64] ซึ่งองค์กรเอกชนที่สนับสนุนในเรื่องนี้อย่างจริงจังคือหอการค้านานาชาติ (International Chamber of Commerce)

---

[63] Miriam H. Wugmeister. “Re : Binding Corporate Rules for International Data Transfers.” <http://europa.eu.int/comm/internal_market/privacy/docs/consultations/morrison-foerster_en.pdf.>. September 2003.

[64] Article 29 Working Party.

ซึ่งต่อมาก็ได้จัดทำรายงานที่มีชื่อว่า “ICC report on binding corporate rules for international transfer of personal data” เพื่อให้ข้อมูลทั่วไปเกี่ยวกับการทำ Biding Corporate Rule รวมถึงประเด็นข้อกฎหมายที่เกี่ยวข้องกับการจัดทำ Biding Corporate Rule [65]

เมื่อนำหลักการจัดทำนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองภายในองค์กร (Binding Corporate Rules) ที่ภาคธุรกิจในต่างประเทศให้การสนับสนุนมาพิจารณาควบคู่กับการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลฯ ก็มีความเห็นว่าน่าจะถือว่าการจัดทำนโยบายดังกล่าวเป็น Binding Corporate Rules อย่างหนึ่งที่มีสภาพบังคับโดยการกำหนดกลไกสนับสนุนทางกฎหมายโดยการกำหนดมาตรการลงโทษใดๆ โดยคณะกรรมการ จึงมีความเห็นว่าในการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล หรือ Privacy Policy นั้นก็ควรที่จะระบุรายละเอียดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปต่างประเทศนอกเหนือจากระบุวิธีการให้ความคุ้มครองแบบทั่วไปด้วย หลักเกณฑ์ด้วย ซึ่งเมื่อพิจารณาตัวอย่าง Privacy Policy ของหลายบริษัทที่มีสำนักงานสาขากระจายตั้งอยู่ทั่วโลกได้กำหนดรายละเอียดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังสำนักงานสาขาหรือบริษัทในเครือซึ่งตั้งอยู่ในต่างประเทศเช่นเดียวกัน

นอกจากนี้ ยังมีความเห็นว่า ผู้ประกอบการควรจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของตนเองที่สอดคล้องกับหลักเกณฑ์ของ Safe Harbor ด้วย เนื่องจากเป็นหนึ่งในสองวิธีการที่ทำให้องค์กรหรือบริษัทที่ตั้งอยู่ในสหรัฐอเมริกาสามารถรับโอนข้อมูลจากสำนักงานใหญ่หรือสำนักงานสาขาหรือองค์กรอื่นใดที่ตั้งอยู่ในประเทศสมาชิก EU ได้ ดังนั้น การจัดทำ Privacy Policy ของผู้ประกอบใน

[65] International Chamber of Commerce. “ .”< http://www.iccwbo.org/home/news_archives/2004/data_transfer.asp.>. November 2004.

ระหว่างกันโดยจะกำหนดเงื่อนไขอย่างไรก็ได้ แต่อย่างไรก็ตาม ในบางประเทศก็ได้กำหนดให้ต้องยื่นสัญญาดังกล่าวไปยังหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลในประเทศผู้โอนข้อมูลเพื่อให้ความเห็นชอบหรือต้องนำสำเนาสัญญาดังกล่าวไปมอบให้แก่หน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งย่อมนำมาสู่ปัญหาความล่าช้าในการดำเนินการและเกิดภาระค่าใช้จ่ายแก่ภาคธุรกิจพอสมควร

ดังนั้น ผู้ประการก็อาจพิจารณาเงื่อนไขของสัญญาแม่แบบข้างต้นและปรับเปลี่ยนเงื่อนไขให้มีความเหมาะสมสอดคล้องกับลักษณะการโอนข้อมูลส่วนบุคคลและการดำเนินธุรกิจของตน ซึ่งจะช่วยให้สามารถแก้ไขปัญหาด้านการโอนข้อมูลได้ หากประเทศที่ต้องการโอนข้อมูลมายังประเทศไทยมีข้อยกเว้นให้สามารถโอนไป โดยปราศจากข้อจำกัดหากมีการทำสัญญาโอนข้อมูลส่วนบุคคลแล้ว

การจัดทำนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคล

นอกจาก การทำสัญญาโอนข้อมูลส่วนบุคคลแล้ว ปัจจุบันได้มีการตื่นตัวในกลุ่มผู้ประกอบธุรกิจซึ่งมีสำนักงานสาขาในหลายประเทศว่าในการพิจารณาระดับการคุ้มครองข้อมูลส่วนบุคคลนั้นควรพิจารณาจากนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองที่จัดทำขึ้นภายในองค์กร (Binding Corporate Rules) นั้นเองด้วย[62] เนื่องจากเป็นวิธีการหนึ่งที่จะช่วยให้สามารถลดขั้นตอนและความยุ่งยากในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลขององค์กรเดียวกันในสำนักงานสาขาในแต่ละประเทศที่มีความแตกต่างกัน กล่าวคือ ผู้ที่ต้องการโอนข้อมูลส่วนบุคคลสามารถพิจารณาเพียงแค่ว่าผู้รับโอนข้อมูลมีกลไกการคุ้มครองในระดับที่ได้มาตรฐานหรือไม่ โดยไม่จำต้องพิจารณาถึงระดับการให้ความคุ้มครองในระดับประเทศแต่อย่างใด ทั้งนี้กลไกหรือนโยบายดังกล่าวจะมีประสิทธิภาพได้ต่อเมื่อมีสภาพบังคับได้ในทางกฎหมาย เช่น จะต้องผ่านการพิจารณาให้ความเห็นชอบจากองค์กรด้านการคุ้มครอง

---

[62] Article 29 Working Party. “Transfer of personal data to third countries : Applying Article 26(2) of the E.U. Data Protection Directive to Binding Corporate Rules for International Data Transfers.” < http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf > May 2003.

ประเทศไทยที่มีหลักการคุ้มครองสอดคล้องกับข้อตกลง Safe Harbor ก็น่าที่จะได้รับยอมรับในมุมมองของประเทศสมาชิก EU เช่นเดียวกัน

ในขณะเดียวกันผู้ประกอบการในประเทศไทยอาจขอใช้บริการเครื่องหมายรับรองความน่าเชื่อถือ (Trust Mark) ด้านการคุ้มครองข้อมูลส่วนบุคคลที่มีชื่อเสียงและได้รับการยอมรับเป็นการทั่วไป อาทิ TRUSTe หรือ WEBTrust ได้เนื่องจากเป็นอีกวิธีการหนึ่งที่สหภาพยุโรปให้การยอมรับว่าองค์กรหรือบริษัทใดในสหรัฐอเมริกาที่ใช้เครื่องหมายรับรองความน่าเชื่อถือดังกล่าวสามารถให้การคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอเช่นกัน แต่อย่างไรก็ตาม การขอใช้บริการดังกล่าวก็มีภาระค่าใช้จ่ายในการสมัครเข้าเป็นสมาชิกที่องค์กรหรือบริษัทจะต้องตระหนักในข้อนี้เช่นกัน

การประเมินผลกระทบต่อความเป็นอยู่ส่วนตัว (Privacy Impact Assessment)

ปัจจุบันได้มีกลไกการตรวจสอบระดับการคุ้มครองข้อมูลส่วนบุคคลนอกเหนือจากการตรวจสอบ (audit) ที่เรียกว่า การประเมินผลกระทบต่อความเป็นอยู่ส่วนตัว (Privacy Impact Assessment) ซึ่งเป็นกลไกที่มีการส่งเสริมให้มีการใช้ในหลายประเทศ ได้แก่ แคนาดา ออสเตรเลีย นิวซีแลนด์ และฮ่องกง[66] โดยสมาคมการประเมินผลกระทบนานาชาติ (The International Association for Impact Assessment) ได้ให้คำจำกัดความการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัว ไว้ว่า *"การประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวที่จะเกิดขึ้นอันเนื่องจากการดำเนินการใดๆ ต่อข้อมูลส่วนในปัจจุบันหรือที่จะมีขึ้นในอนาคต (the identification of future consequence of a current or proposed action)* [67] ซึ่งจะมีลักษณะแตกต่างจากกลไก

---

[66] Privacy Commissioner, Privacy Impact Assessment Handbook, (New Zealand: OPC Publication, 2002), p.3.

[67] Ibid., p.9.

การตรวจสอบตรงที่การประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวมุ่งเน้นที่การชี้วัดผลกระทบที่จะเกิดขึ้นเพื่อหาทางหลีกเลี่ยงการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลที่จะส่งผลเสียต่อความเป็นอยู่ส่วนตัวเป็นหลัก ซึ่งผลที่ได้ก็จะเป็นข้อมูลให้แก่ผู้กำหนดนโยบายในองค์กรในการพิจารณาว่าจะยังคงดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลตามแผนการที่วางไว้หรือไม่ ในขณะที่กลไกการตรวจสอบจะมุ่งเน้นไปที่การตรวจสอบว่าการดำเนินการที่เป็นอยู่นั้นสอดคล้องตามหลักเกณฑ์การคุ้มครองความเป็นอยู่ส่วนตัวโดยการคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่หรือไม่เพียงใด[68] นอกจากนี้ การประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวนั้นยังถือได้ว่าเป็นระบบการแจ้งเตือนล่วงหน้า (early warning system) ที่เหมาะสมสำหรับหน่วยงานภาคเอกชนขนาดกลางไปจนถึงขนาดใหญ่และหน่วยงานของรัฐเพื่อช่วยในการวางแผนในการบริหารจัดการข้อมูลส่วนบุคคลภายองค์กรเพื่อหลีกเลี่ยงความเสียหายทั้งต่อเจ้าของข้อมูลและองค์กรหรือหน่วยงานนั้นเองที่อาจตกเป็นข่าวว่ามีการดำเนินการที่กระทบต่อความเป็นอยู่ส่วนตัวของลูกค้าหรือผู้ใช้บริการได้[69]

สำหรับบุคคลที่จะเป็นผู้ทำหน้าที่ในการประเมินดังกล่าวนั้น เนื่องจากปัจจุบันกฎหมายในประเทศส่วนใหญ่ที่ส่งเสริมให้มีการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวมิได้บัญญัติถึงหลักเกณฑ์ดังกล่าวไว้แต่อย่างใด ยกเว้นแต่ในกรณีรัฐ Alberta ของประเทศแคนาดาเท่านั้นที่กำหนดไว้ในกฎหมายว่าหน่วยงานของรัฐจะต้องจัดให้มีการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวก่อนการจัดทำระบบข้อมูลสาธารณสุขสาธารณะ (public health information systems)[70] ขึ้นใหม่ ดังนั้น การประเมินที่เกิดขึ้นจึงเป็นการจัดให้มีการประเมินโดยความสมัครใจขององค์กรนั้นเองไม่ว่าจะเป็นองค์กรของภาครัฐหรือภาคเอกชน ด้วยเหตุนี้เองผู้ที่สามารถทำการประเมินจึงมีได้ทั้งบุคลากรที่มีความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลในองค์กรนั้นเอง หรือเป็นผู้เชี่ยวชาญจากภายนอก ซึ่งก็มีผู้ให้ความเห็นว่า บุคคลที่สมควรทำหน้า

---

[68] Ibid.

[69] Ibid.

[70] Ibid., p.3.

ที่ประเมินดังกล่าวควรเป็นบุคคลในองค์กรนั้นเองที่พัฒนาระบบข้อมูลใดๆ อันอาจส่งผลกระทบต่อข้อมูลส่วนบุคคล เนื่องจากจะทำให้สามารถถึงรายละเอียด ขั้นตอนการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลได้ดี แต่อย่างไรก็ตามปัญหาที่อาจเกิดขึ้นจากแนวคิดดังกล่าวคือเป็นยากที่จะหาบุคลากรที่พัฒนาระบบผู้มีความรู้ความเข้าใจเกี่ยวกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ดีเพียงพอซึ่งจะทำให้พิจารณาได้ว่าระบบใดๆ ที่จะพัฒนาขึ้นนั้นจะส่งผลกระทบต่อความเป็นอยู่ส่วนตัวมากน้อยเพียงใด[71]

ประเด็นที่ต้องพิจารณาต่อมามีว่า ประเทศไทยควรกำหนดหลักเกณฑ์ด้านการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวหรือไม่เพียงใด กล่าวคือ สมควรมีการกำหนดกลไกทางกฎหมายเพื่อกระตุ้นหรือส่งเสริมให้เกิดการประเมินผลกระทบดังกล่าวโดยสมัครใจของหน่วยงานหรือองค์กรต่างๆ โดยมีแนวทางปฏิบัติ (Guideline) อย่างชัดเจนที่ออกโดยหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลซึ่งเป็นแนวทางที่มีการใช้อยู่ในหลายประเทศ หรือสมควรกำหนดให้องค์กรหรือหน่วยงานบางประเภท จำเป็นต้องมีการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวก่อนเสมอ ซึ่งที่ผ่านมาประเทศไทยได้ใช้แนวทางในลักษณะดังกล่าวกับการทำรายงานการวิเคราะห์ผลกระทบสิ่งแวดล้อมภายใต้พระราชบัญญัติส่งเสริมและรักษาคุณภาพสิ่งแวดล้อมแห่งชาติ พ.ศ. 2535 โดยการกำหนดให้รัฐมนตรีโดยความเห็นชอบของคณะกรรมการ สิ่งแวดล้อมแห่งชาติ มีอำนาจประกาศในราชกิจจานุเบกษากำหนดประเภท และขนาดของโครงการหรือกิจการของส่วนราชการ รัฐวิสาหกิจ หรือเอกชนที่มีผลกระทบสิ่งแวดล้อมซึ่งต้องจัดทำรายงานการวิเคราะห์ผลกระทบสิ่งแวดล้อมเสนอต่อคณะกรรมการสิ่งแวดล้อมแห่งชาติ[72] ทั้งนี้ รัฐมนตรีโดยความเห็นชอบของคณะกรรมการสิ่งแวดล้อมแห่งชาติอาจกำหนดให้การรายงานผลกระทบสิ่งแวด-

---

[71] David Flaherty, “Privacy Impact Assessments : an essential tool for data protection”, Paper Presented at 22nd Annual Meeting of Privacy and Data Protection Officials, Venice, Italy, 27-30 September 2000.

[72] พระราชบัญญัติส่งเสริมและรักษาคุณภาพสิ่งแวดล้อมแห่งชาติ พ.ศ. 2535, มาตรา 46-50

ล้อมต้องจัดทำหรือได้รับการรับรองจากบุคคลซึ่งได้รับอนุญาตให้เป็นผู้ชำนาญการศึกษาผลกระทบสิ่งแวดล้อมก็ได้ โดยการขออนุญาต การออกใบอนุญาต ตลอดจนคุณสมบัติของผู้ชำนาญ ดังกล่าวให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดในกฎกระทรวง[73]

มีความเห็นว่าควรกำหนดมาตรการทางกฎหมายเพื่อให้มีการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวโดยความสมัครใจขององค์กรหรือหน่วยงานบางประเภทซึ่งในการดำเนินงานหรือให้บริการต่อประชาชนหรือลูกค้านั้นจำเป็นต้องมีการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลค่อนข้างมาก อาทิ ธนาคาร สถาบันการเงิน สถานพยาบาล ผู้ให้บริการโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการด้านการขนส่งสาธารณะ เป็นต้น สามารถยื่นรายงานผลการประเมินดังกล่าวไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอีกครั้งหนึ่ง โดยประโยชน์ที่องค์กรหรือหน่วยงานที่ได้ทำการประเมินผลกระทบต่อความเป็นอยู่ส่วนตัวจะได้รับนั้นอาจอยู่ในรูปของการประกาศรายชื่อองค์กรหรือหน่วยงานนั้นๆ ไว้ในเอกสารทางทะเบียนหรือเว็บไซต์ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นองค์กรหรือหน่วยงานที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ดีตามที่กฎหมายกำหนด เพื่อให้ประชาชนทั่วไป ลูกค้า หรือผู้ใช้บริการสามารถตรวจสอบได้โดยง่าย ทั้งนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจจัดให้มีเครื่องหมายรับรองความน่าเชื่อถือ (Trust Mark) ด้านการคุ้มครองข้อมูลส่วนบุคคลแก่องค์กรหรือหน่วยงานที่ผ่านความเห็นชอบ ในรายงานผลการประเมินต่อความเป็นอยู่ส่วนตัวติดตั้งในเว็บไซต์ของตน ซึ่งผลของการใช้วิธีการดังกล่าวจะทำให้เกิดทัศนะคติที่ดีแก่ผู้ปฏิบัติเนื่องจากเป็นมาตรการที่สามารถดำเนินการด้วยความสมัครใจขึ้นอยู่กับความพร้อมของหน่วยงานเป็นหลัก และสามารถสร้างความเชื่อมั่นให้แก่ประชาชน ลูกค้า หรือผู้ใช้บริการทั้งในและต่างประเทศว่าข้อมูลส่วนบุคคลของตนที่ถูกเก็บรวบรวม ใช้เปิดเผย หรือแม้แต่โอนไปยังองค์กรหรือหน่วยงานที่ได้รับตราประทับว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ดีพอ

[73] เพิ่งอ้าง, มาตรา 51.

จากเนื้อหาที่ได้กล่าวมาในข้างต้นจะเห็นได้ว่าได้มุ่งเน้นถึงแนวทางในการดำเนินการเพื่อให้ประเทศที่บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลของตนโดยอาศัยแนวทางในการบัญญัติกฎหมายจาก EU Directive พิจารณาว่าประเทศไทยมีการคุ้มครองข้อมูลส่วนบุคคลในระดับเพียงพอ โดยไม่กล่าวถึงประเทศที่มิได้บัญญัติกฎหมายโดยอาศัยแนวทางจาก EU Directive อาทิ ญี่ปุ่น สหรัฐอเมริกา เนื่องจากประเทศเหล่านี้มิได้มีการมีการวางข้อจำกัดเกี่ยวกับการโอนข้อมูลส่วนบุคคลไปต่างประเทศไว้แต่ประการใด ซึ่งย่อมมีผลให้ผู้โอนข้อมูลสามารถโอนข้อมูลส่วนบุคคลไปต่างประเทศโดยปราศจากเงื่อนไขในทำนองเดียวกับที่กำหนดไว้ใน EU Directive Article 25 และ 26 และเป็นเหตุให้ประเทศไทยสามารถรับโอนข้อมูลส่วนบุคคลจากประเทศดังกล่าวได้โดยปราศข้อจำกัด ดังนั้น ปัญหาในการรับโอนข้อมูลส่วนบุคคลจึงย่อมไม่เกิดขึ้น แต่ในทางกลับกัน ก็มีประเด็นที่ต้องพิจารณาว่า จะถือได้หรือไม่ว่าประเทศซึ่งมิได้บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยอาศัยแนวทางตาม EU Directive เป็นประเทศซึ่งมีบทบัญญัติในการคุ้มครองในระดับที่เท่าเทียมกันในสาระสำคัญกับร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... หรือไม่ ซึ่งเห็นว่า หากมีการใช้หลักเกณฑ์การแจ้งให้คณะกรรมการทราบก่อนมีการโอนข้อมูลส่วนบุคคล ก็จะเป็นบทบาทของคณะกรรมการในการพิจารณาว่าบทบัญญัติในกฎหมายประเทศผู้รับโอนข้อมูลสามารถให้การคุ้มครองในระดับที่เท่าเทียมหรือไม่ ซึ่งอาจยากในการพิจารณาชี้ขาดของคณะกรรมการฯ ได้เนื่องจากอาจจำเป็นต้องคำนึงถึงการเมืองและความสัมพันธ์ระหว่างประเทศด้วย ดังนั้น จึงเห็นว่า อาจมีการเพิ่มเติมเงื่อนไขในร่างพระราชบัญญัติว่านอกเหนือจากการพิจารณาถึงบทบัญญัติภายในประเทศผู้รับโอนข้อมูลแล้ว ก็ควรเปิดโอกาสให้คำนึงถึงมาตรการ หรือกลไกการกำกับดูแลตนเอง ซึ่งมีเนื้อหาการคุ้มครองข้อมูลส่วนบุคคลในสาระสำคัญและสามารถบังคับใช้ได้ในประเทศนั้นๆ เท่าเทียมกับที่ระบุไว้ในร่างพระราชบัญญัติ เพื่อให้เกิดความยืดหยุ่นในทางปฏิบัติ

บทที่ 5
บทสรุป

การกำหนดหลักเกณฑ์ข้อจำกัดในการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศเป็นมาตรการสำคัญประการหนึ่งเพื่อให้การคุ้มครองความเป็นอยู่ส่วนตัวในข้อมูลข่าวสารของเจ้าของเจ้าของข้อมูล โดยสามารถป้องกันผลกระทบหรือความเสียหายที่อาจเกิดขึ้นจากการละเมิดความเป็นอยู่ส่วนตัวในข้อมูลส่วนบุคคลที่ถูกโอนไปยังต่างประเทศได้เนื่องจากโดยปกติแล้วหากมีการดำเนินการใดๆ อันเป็นการกระทบสิทธิต่อเจ้าของข้อมูลในต่างประเทศแล้ว ก็เป็นการยากที่เจ้าของข้อมูลจะได้รับการเยียวยาความเสียหายได้ภายในประเทศของตนภายหลังจากที่มีการโอนข้อมูลไปยังต่างประเทศเรียบร้อยแล้ว อีกทั้งยังสามารถสร้างหลักประกันในเบื้องต้นแก่เจ้าของข้อมูลว่า ข้อมูลส่วนบุคคลของตนถูกโอนไปยังประเทศอื่นจะยังคงได้รับการคุ้มครองหรือได้รับการปฏิบัติในระดับที่ดีเช่นเดียวกับมาตรการการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศเจ้าของข้อมูล หากมีการกำหนดเงื่อนไขว่าจะข้อมูลส่วนบุคคลที่จะถูกโอนไปนั้นสามารถกระทำได้ต่อเมื่อประเทศผู้รับโอนมีกฎหมายหรือมาตรการด้านการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ดี กล่าวคือ มีเนื้อหาการคุ้มครองครบถ้วนและสามารถบังคับใช้ได้อย่างมีประสิทธิภาพ

ปัจจุบันหลักเกณฑ์ข้อจำกัดการโอนข้อมูลส่วนบุคคลในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของหลายประเทศไม่ว่าจะเป็นประเทศสมาชิกของสหภาพยุโรปหรือไม่ก็ตามก็ได้รับอิทธิพลมาจาก EU Directive ซึ่งได้วางหลักการสำคัญว่า ห้ามโอนข้อมูลส่วนบุคคลไปยังประเทศนอกสมาชิกที่ไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ ซึ่งการคุ้มครองดังกล่าวอาจอยู่ในรูปแบบของบทบัญญัติหรือมาตรการอื่นใด อาทิ กลไกการกำกับดูแลตนเอง เว้นแต่จะเป็นกรณีเข้าข้อยกเว้นเท่านั้น ซึ่งผลของการกำหนดหลักเกณฑ์ข้อจำกัดดังกล่าวก็ได้ก่อให้เกิดปัญหาและ

อุปสรรคแก่องค์กรหรือหน่วยงานที่มีความจำเป็นต้องโอนข้อมูลซึ่งมีข้อมูลส่วนบุคคลรวมอยู่ด้วยไปยังประเทศนอกสมาชิก EU มากพอสมควร และแม้ว่าจะมีผู้ตั้งข้อสังเกตว่าหลักเกณฑ์ข้อจำกัดการโอนข้อมูลส่วนบุคคลของ EU ที่ปรากฏอยู่ใน EU Directive ดังกล่าวจะขัดต่อหลักการในความตกลงทั่วไปว่าด้วยการค้าบริการ (The General Agreement on Trade in Service (GATS) ก็ตาม แต่ก็ปรากฏว่าการกำหนดเงื่อนไขใดๆ เพื่อประโยชน์ในการคุ้มครองข้อมูลส่วนบุคคลเป็นสิ่งที่สามารถกระทำได้เนื่องจากเป็นกรณีตามข้อยกเว้นใน GATS

ด้วยเหตุนี้เองจึงเป็นเหตุให้หลายประเทศได้พยายามบัญญัติกฎหมายภายในหรือแก้ไขกฎหมายเดิมให้สอดคล้องกับ EU Directive ซึ่งรวมถึงหลักเกณฑ์ข้อจำกัดการโอนข้อมูลส่วนบุคคลไปยังต่างประเทศด้วย เพื่อที่จะให้ประเทศของตนได้รับการพิจารณาว่ามีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอและได้มาตรฐานสากล ซึ่งจะมีผลให้ผู้ประกอบการหรือองค์กรในประเทศของตนสามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิก EU หรือประเทศอื่นๆ โดยปราศจากอุปสรรคด้านกฎหมาย มิฉะนั้นแล้ว ก็จำเป็นที่ต้องใช้มาตรการที่จัดทำขึ้นเองซึ่งก่อให้เกิดภาระและต้นทุนแก่ผู้ประกอบในการดำเนินการเพื่อให้สามารถรับโอนข้อมูลส่วนบุคคลตามข้อยกเว้นที่กำหนดไว้ในกฎหมาย อาทิ การขอความยินยอมจากเจ้าของข้อมูล การจัดทำสัญญาโอนข้อมูลส่วนบุคคล เป็นต้น หรือในบางครั้งอาจจำเป็นต้องมีการแก้ไขปัญหาเฉพาะหน้าโดยการจัดทำข้อตกลงระหว่างประเทศ ดังเช่น การทำข้อตกลง Safe Harbor ระหว่างประเทศสหรัฐอเมริกากับ EU อันเนื่องจากการที่สหรัฐอเมริกาไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลได้ในระดับที่เพียงพอในมุมมองของ EU ในขณะเดียวกันก็จะเป็นการขยายขอบเขตการคุ้มครองแก่เจ้าของข้อมูลให้กว้างขวางมากยิ่งขึ้นด้วย

สำหรับกรณีของประเทศไทยนั้น หากได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยมีเนื้อหาการคุ้มครองและกลไกการบังคับใช้ที่มีประสิทธิภาพ ซึ่งสอดคล้องกับ EU Directive แล้วก็จะมีข้อดีตรงที่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลในประเด็นสำคัญต่างๆ ได้อย่างครบถ้วน โดยเฉพาะอย่างยิ่งการคุ้มครองข้อมูลส่วนบุคคลของประชาชนภายในประเทศหากต้องมีการโอนข้อมูลไปยังต่างประเทศ ซึ่ง

เสี่ยงต่อการถูกละเมิดด้วยวิธีการต่างๆ อยู่ตลอดเวลา ในขณะเดียวกันก็สามารถหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นอันเนื่องจากการรับโอนข้อมูลส่วนบุคคลจากประเทศทั้งที่เป็นสมาชิก EU ซึ่งปัจจุบันได้เพิ่มจำนวนเป็น 25 ประเทศและประเทศอื่นๆ ที่ได้บัญญัติกฎหมายโดยอาศัยแนวทางของ EU Directive ได้ ซึ่งในอนาคตการโอนข้อมูลส่วนบุคคลมายังประเทศไทยจะมีความสำคัญมากยิ่งขึ้นเนื่องจากข้อมูลดังกล่าวเป็นปัจจัยสำคัญประการหนึ่งในตลาดบริการซึ่งมีส่งเสริมและสนับสนุนอย่างจริงจังทั้งจากภาครัฐและภาคเอกชนอย่างต่อเนื่อง อาทิ ธุรกิจการท่องเที่ยว ธุรกิจการบริการด้านสุขภาพ การขนส่งระหว่างประเทศ เป็นต้น รวมไปถึงเพื่อประโยชน์ด้านการรักษาความมั่นคงของประเทศอีกด้วย นอกจากนี้ การมีกฎหมายที่สอดคล้องกับแนวโน้มกับการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศต่างๆ ทั่วโลก ก็จะมีส่วนเสริมสร้างให้ผู้ประกอบการทั้งภายในและต่างประเทศเกิดความเชื่อมั่นในกฎเกณฑ์ด้านการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศนั้นๆ และช่วยให้สามารถปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างครบถ้วนโดยสามารถคาดการณ์ (predictable) ถึงผลกระทบทางกฎหมายที่ตนจะได้รับอันเนื่องจากการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคล และสามารถแก้ไขหรือหลีกเลี่ยงปัญหาที่เกิดขึ้นหรืออาจเกิดขึ้นได้โดยอาศัยวิธีการอย่างเดียวกันอันจะสามารถลดอุปสรรคในการประกอบธุรกิจการค้าระหว่างประเทศที่เกี่ยวข้องกับมาตรการคุ้มครองข้อมูลส่วนบุคคลลงไปได้มาก

นอกจากนี้ การที่ประเทศไทยบัญญัติกฎหมายภายในให้สอดคล้องกับ EU Directive ซึ่งรวมถึงข้อจำกัดการโอนข้อมูลส่วนบุคคลดังกล่าวข้างต้นนั้นก็หาได้ส่งผลกระทบต่อการประกอบธุรกิจการค้าระหว่างประเทศกับประเทศที่มิบัญญัติหรือแก้ไขกฎหมายให้สอดคล้องกับ EU Directive แต่ประการใด เนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศเหล่านั้นมิได้กำหนดหลักเกณฑ์เกี่ยวกับข้อจำกัดการโอนข้อมูลส่วนบุคคลไปต่างประเทศไว้ ดังนั้น ผู้ประกอบการชาวไทยหรือมีสถานประกอบการในประเทศไทยจึงไม่ได้รับผลกระทบหรือประสบอุปสรรคด้านกฎหมายในการรับโอนข้อมูลส่วนบุคคลจากประเทศดังกล่าว

ดังนั้น จึงอาจกล่าวโดยสรุปได้ว่า การบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่ครบถ้วนสมบูรณ์ได้มาตรฐาน

สากล นอกจากจะสามารถให้การคุ้มครองข้อมูลส่วนบุคคลในประเด็นต่างๆ ได้ครบถ้วนแล้ว ก็จะเป็นวิธีการหนึ่งที่จะช่วยลดภาระแก่ผู้ประกอบการหรือหน่วยงานที่จำเป็นต้องรับโอนข้อมูลส่วนบุคคลระหว่างประเทศได้ค่อนข้างมาก เพราะเหตุว่าจะได้รับการพิจารณาจากนานาประเทศว่าประเทศนั้นๆ สามารถให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอหรือทัดเทียมกับประเทศผู้โอนข้อมูล และมีผลให้สามารถทำได้สามารถรับโอนข้อมูลได้โดยปราศจากอุปสรรคโดยไม่จำเป็นต้องไปศึกษาหาวิธีการ หรือลงทุนเพื่อดำเนินให้เป็นไปตามข้อยกเว้นต่างๆ ตามที่กฎหมายของประเทศผู้โอนข้อมูลกำหนด อาทิ มีหนังสือขอความยินยอมไปยังพนักงานหรือลูกค้าทุกรายหรือต้องมีการจัดทำสัญญาโอนข้อมูลส่วนบุคคลกับสำนักงานสาขาในประเทศต่างๆ ซึ่งก่อให้เกิดความยุ่งยากและใช้ระยะเวลาในการดำเนินการค่อนข้างนาน

อย่างไรก็ตาม ในระหว่างที่ยังไม่มีกฎหมายออกใช้บังคับผู้ประกอบการหรือหน่วยงานของรัฐที่จำเป็นต้องรับโอนข้อมูลส่วนบุคคลจากต่างประเทศก็มีความจำเป็นที่จะต้องศึกษาถึงหลักเกณฑ์ข้อเว้นที่ทำให้สามารถรับโอนข้อมูลส่วนบุคคลได้ ไม่ว่าจะเป็นจัดทำ Privacy Policy ที่มีเนื้อหาและสภาพบังคับครบถ้วนเนื่องจากถือว่าเป็น Binding Corporate Rule อย่างหนึ่ง, การขอความยินยอมจากเจ้าของข้อมูล รวมไปถึงการจัดทำสัญญาโอนข้อมูลส่วนบุคคลที่สอดคล้องกับสัญญาแม่แบบที่จัดทำขึ้นโดย Commission ในกรณีที่ต้องการรับโอนข้อมูลจากประเทศสมาชิก EU หรือเงื่อนไขสัญญาที่คณะกรรมการในประเทศนอกสมาชิก EU กำหนดให้บรรจุเป็นเงื่อนไขขั้นต่ำในสัญญาโอนข้อมูลส่วนบุคคล