ปัญหาทางกฎหมายเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

กรณีศึกษา : การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

Legal problems on privacy protection in electronic transaction

Case Study : the making of privacy policy of banks, financial institutions and credit card operators

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

ปัญหาทางกฎหมายเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กรณีศึกษา : การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

Legal problems on privacy protection in electronic transaction Case Study : the making of privacy policy of banks, financial institutions and credit card operators

โดย

นายธนัท สุวรรณปริญญา

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

BANGKOK UNIVERSITY
FOUNDED 1962

บัณฑิตวิทยาลัย
มหาวิทยาลัยกรุงเทพ

สารนิพนธ์

โดย

นายธนัท สุวรรณปริญญา

เรื่อง

ปัญหาทางกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์
กรณีศึกษา : การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา _____
(ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ)

อาจารย์ที่ปรึกษาร่วม _____
(รองศาสตราจารย์อุดมศักดิ์ สินธิพงษ์)

กรรมการผู้ทรงคุณวุฒิ _____
(รองศาสตราจารย์ ดร.พันธุ์ทิพย์ กาญจนะจิตรา สายสุนทร)

ชื่องานวิจัยภาษาไทย : ปัญหาทางกฎหมายเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ กรณีศึกษา : การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

ชื่องานวิจัยภาษาอังกฤษ : Legal problems on privacy protection in electronic transaction. Case Study : the making of privacy policy of banks, financial institutions, and credit card operators

ชื่อผู้วิจัยภาษาไทย : นายธนัท สุวรรณปริญญา

ชื่อผู้วิจัยภาษาอังกฤษ : Mr.Thanut Suwanprinya

ชื่อคณะ : คณะนิติศาสตร์

สาขา : กฎหมายธุรกิจระหว่างประเทศและธุรกรรมทางอิเล็กทรอนิกส์

ชื่อสถาบัน : มหาวิทยาลัยกรุงเทพ

รายชื่อที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร.อรรยา สิงห์สงบ

ปีการศึกษา : 2550

บทคัดย่อ

ปัจจุบันเทคโนโลยีการติดต่อสื่อสารผ่าน ระบบอินเทอร์เน็ต ถูกนำไปใช้ในการประกอบธุรกิจกันอย่างแพร่หลาย ไม่เว้นแม้แต่ ในธุรกิจประเภทธนาคาร สถาบันการเงินหรือผู้ประกอบธุรกิจบัตรเครดิต ซึ่งส่วนมากจะมีการเปิดให้บริการธนาคารออนไลน์ หรือ Internet Banking ทั้งนี้ เนื่องจากการให้บริการออนไลน์ ทำให้ลูกค้าสาม ารถเข้าถึงการให้บริการของผู้ประกอบธุรกิจได้มากยิ่งขึ้น และช่วยให้การดำเนินธุรกิจในขั้นตอนต่าง ๆ ทำได้โดยง่ายและมีความสะดวกรวดเร็วยิ่งขึ้น ซึ่งสามารถช่วยลดต้นทุนทางธุรกิจได้มากยิ่งขึ้นด้วย ประกอบกับความสามารถ ต่าง ๆ ของระบบอินเทอร์เน็ตและเทคโนโลยีคอมพิวเตอร์ที่ เอื้ออำนวยให้เกิดการใช้มากขึ้น เช่น ความสามารถในการบันทึกข้อมูล การสำรองข้อมูล การประมวลผลข้อมูล รวมไปถึงการถ่ายโอนข้อมูล โดยทั่วไปแล้ว ผู้ประกอบธุรกิจบนอินเทอร์เน็ตส่วนใหญ่จะ สามารถเก็บรวบรวมข้อมูลของลูกค้า และเฝ้าติดตามพฤติกรรมในการใช้บริการของลูกค้าได้ ซึ่งจัดเป็นการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของลูกค้า โดย ลูกค้าหรือผู้ใช้บริการอาจไม่ทราบหรืออาจไม่ได้ให้ความยินยอมแก่การกระทำดังกล่าว หรือแม้จะมีกา รให้ความยินยอมแล้วก็อาจจะมี การนำข้อมูลส่วนบุคคลไปใช้เกินขอบเขตที่ได้ให้ความยินยอมไว้ได้ อันเป็นการละเมิดข้ อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้ ดังนั้น เพื่อสร้างความเชื่อมั่นในการทำธุรกรรมออนไลน์ จึงมีความจำเป็นต้อง ให้ความคุ้มครองความปลอดภัยใน ข้อมูลส่วนบุคคลด้วย โดย วิธีการให้ความคุ้มครองที่ได้รับความนิยม ที่ผู้ประกอบ ธุรกิจสามารถดำเนินการ ได้เอง ก็คือ การจัดทำนโยบายความเป็นส่วนตัว หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลนั่นเอง

การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) เป็นรูปแบบหนึ่งตามแนวทาง การกำกับดูแลตนเอง โดยนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็คือ นโยบายที่ผู้ประกอบธุรกิจประกาศให้แก่ลูกค้าหรือผู้ใช้บริการของตนทราบว่า ตน มีนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลอย่างไร เพื่อให้ลูกค้าหรือผู้ใช้บริการทราบและสามารถใช้พิจารณาตัดสินใจได้ว่าตนจะให้ข้อมูลส่วนบุคคลของตนหรือไม่ แต่เนื่องจากการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลไม่ได้ถูกควบคุม โดยกฎหมายหรือองค์กรใดๆ จึงอาจทำให้การกำหนดนโยบายของผู้ประกอบธุรกิจ ไม่ได้มาตรฐาน ไม่อาจคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริง หรืออาจกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลให้ดูน่าเชื่อถือโดยไม่ได้คำนึงว่าจะสามารถปฏิบัติได้ตามที่ตนได้ประกาศไว้จริ งหรือไม่เพียงใด ดังนั้น ในกรณีที่ผู้ประกอบธุรกิจ ไม่สามารถคุ้มครองข้อมูลส่วนบุค คลได้ตามนโยบายที่ตนประกาศไว้จึงก่อให้เกิดปัญหาว่า ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้เสียหายจะสามารถฟ้องร้องหรือดำเนินการทางกฎหมายอย่างไรต่อผู้ประกอบธุรกิจ โดยที่ปัญหาดังกล่าวสามารถแก้ไขได้โดยการ ตีความว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลมีสถานะทางกฎหมายอย่างไร และกฎหมายที่มีผลบังคับใช้อยู่จะเพียงพอหรือไม่ ซึ่งจากการตีความ นั้น ย่อมแสดงให้เห็นว่านโยบายการคุ้มครองข้อมูลส่วนบุคคล มีสถานะทางกฎหมายเป็น “คำมั่น” ดังนั้น ผู้ประกอบธุรกิจ จึงต้องผูกพันตนที่จะต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ตนได้ประกาศไว้นั่นเอง และในกรณีที่ ผู้ประกอบธุรกิจ ไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคค ลได้ตามนโยบายที่ตนประกาศไว้ ผู้ประกอบการย่อมอยู่ในฐานะที่เป็นฝ่ายผิดคำมั่น ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้ เสียหายจากการที่ข้อมูลส่วนบุคคลของตนถูกนำไปใช้ผิดวัตถุประสงค์ หรือถูกนำไปใช้โดยไม่มีอำนาจ ย่อมสามารถฟ้องร้องหรือดำเนินการทางกฎหมายต่อผู้ประกอบการได้ โดยอาศัยบทบัญญัติแห่งกฎหมายว่าด้วยเรื่องการแสดงเจตนาประกอบกับบทบัญญัติว่าด้วยเรื่องละเมิด

อย่างไรก็ตาม เพื่อเป็นการสร้างความเชื่อมั่นให้แก่ ผู้บริโภค ภาครัฐจะต้องกำหนดมาตรการบังคับ (enforcing) โดยการออกกฎเกณฑ์เพื่อควบคุมการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลขึ้น ประกอบกับต้องแก้ไขกฎเกณฑ์ที่ใช้ควบคุมธุรกิจประเภทต่างๆ ที่ใช้บังคับอยู่ให้มีความสอดคล้องกับกฎเกณ ฑ์ใหม่ด้วย ในการนี้อาจมีการจัดตั้งองค์กรที่ทำหน้าที่กำกับดูแล ซึ่งทำหน้าที่ ควบคุมทางทะเบียน ออกใบอนุญาต ประชาสัมพันธ์ ระงับข้อพิพาท รวมทั้งให้คำปรึกษาแก่ผู้ประกอบธุรกิจและผู้บริโภค โดยรัฐควรจะทำหน้าที่ควบคุมดูแลกิจการเท่าที่จำเป็นเท่านั้น และจะต้องให้การสนับสนุนแก่ภาคเอกชนซึ่งมีขีดความสามารถในการพัฒนาทางเทคโนโลยีสูงกว่าเป็นผู้มีบทบาทนำ ทั้งนี้ เพื่อให้เอกชนมีบทบาทในการพัฒนาด้านเทคโนโลยีอย่างต่อเนื่องโดยไม่ถูกจำกัดโดยกฎเกณฑ์ภาครัฐมากนักนั่นเอง อีกทั้ง ผู้ประกอบธุรกิจประเภท ธนาคาร สถาบันการเงินและผู้ประกอบธุ รกิจบัตรเครดิต ก็ควรจะต้องตระหนักถึงปัญหาการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนให้มีความสอดคล้องกับ แนวทางปฏิบัติที่มีความเป็นสากล ซึ่งหากทุกหน่วยงาน

สามารถความเชื่อมั่นให้แก่ผู้บริโภคได้แล้ว ก็ย่อมส่งผลดีต่อการพาณิ ชย์อิเล็กทรอนิกส์โดยรวมของประเทศได้ และทำให้การพาณิชย์อิเล็กทรอนิกส์มีอัตราการเติบโตตามที่ควรจะเป็นด้วย

Abstract

Nowadays, the technology of telecommunication via the internet is being used widely in operating the business including in certain business as banks, financial institutions, and credit card business most of which provide the online banking services or the so-called internet banking services. This is because of the online services help their clients reach more of their services provided and help make every process of doing business easier, faster, and more convenient, which can reduce the cost of doing business much better. Moreover, the internet system and the computer technology have the abilities such as data storage ability, data backup ability, data processing ability, and data transferring ability which help increase the use of the services. Generally, most of the E-Commerce business operators can collect their clients' information and track the clients' records of services-accessing behaviors which are considered clients' private information processing. The clients may not know nor have given permission in doing so. Or even the clients have given such permission, there might be the uses of private information which are off-limits. Such uses are considered the violation of privacy of the clients. Therefore, to make trustworthiness to the clients in doing the online transaction there is a need in giving security protection for private information. The popular method of giving protection which can be conducted by the business operators on their own is the provision of private information protection policy or the so-called privacy policy.

The provision of privacy policy is a means of the self-regulation policy, that is to say, the privacy policy is the statement which is proclaimed to their customers or clients. Therefore, the customers and the clients acknowledge how the business operators will manage and administer their private information so that they could take into account whether they will give away their private information or not. But as the determination of the privacy policy is not governed by any laws or any organizations, this might cause the non-standard determination and make the policy cannot in reality protect the private information of their clients and customers. Or else, the business operators may determine the privacy policy which sounds credible but may be impracticable. Hence, in the case that business operators are unable to meet the privacy policy proclaimed, it

raises the problem of how the clients or the customers can take legal action against the business operators. Such problem can be solved by construing the legal status of the privacy policy and examining whether the laws currently enforced are sufficient for this issue or not. The construction of the policy indicates that the privacy policy has its own legal status as “promise”, that is, the business operators are obliged to comply with such policy they have proclaimed. While in the case that the business operators are unable to protect private information as proclaimed, they will be deemed to have breached the promise. The clients or the customers who are the sufferers of the misuses or overuses of private information can take legal action against those business operators under the provisions of expression of intention and the provisions of tort.

Nevertheless, to build up confidence in consumers the government shall provide enforceable measure by issuing the provisions to regulate the making of privacy policy and together with making the revisions to any rules which currently regulate certain businesses in conformity with the latest provisions. In doing so, there might be the establishment of the regulating organization whose functions concern registration control, license granting, public relations, settlement of disputes, and also business operators and consumers consultancy. The government functions should be limited only when needed. But they shall support the private sectors that have higher capability in developing technology to lead the tasks because the private sectors should be given opportunities to play the continuous role in developing technology without being restricted by the government rules. Furthermore, certain business operators as banks, financial institutions, and credit card business should take the private information protection problems into account by making their own private information protection policy conform to the universal practice. If every organization can build up confidence in consumers, it will result in a satisfactory benefit over the entire E-Commerce of the country and help raise the growth of the E-Commerce to the rate where it should be.

กิตติกรรมประกาศ

ข้าพเจ้าหวังว่าสารนิพนธ์ฉบับนี้จะสามารถนำไปใช้ประโยชน์ทั้งต่อตนเองและผู้ที่สนใจได้ ความสำเร็จของสารนิพนธ์ฉบับนี้ มีเหตุปัจจัยอยู่หลายอย่างที่ทำให้ข้าพเจ้ามุ่งมั่น ตั้งใจที่จะจัดทำให้สำเร็จ สมบูรณ์ เนื่องด้วยข้าพเจ้าคิดว่าสิ่งที่รอคอยข้าพเจ้าภายหลังจากที่ข้าพเจ้าได้สำเร็จการศึกษาในระดับมหาบัณฑิต จากมหาวิทยาลัยกรุงเทพแล้ว ก็คือ ความก้าวหน้าในวิชาชีพนักกฎหมายของข้าพเจ้า และความสบายใจของคนที่ให้การสนับสนุนและช่วยเหลือข้าพเจ้าเสมอมา ข้าพเจ้าขอกราบขอบพระคุณท่าน ผู้ช่วยศาสตราจารย์ ดร . อรรยา สิงห์สงบ อาจารย์ที่ปรึกษาสารนิพนธ์ ผู้ซึ่งให้คำแนะนำและความช่วยเหลือแก่ข้าพเจ้าในการจัดทำสารนิพนธ์ฉบับนี้ด้วยดีเสมอมา ขอขอบคุณผู้บังคับบัญชาและผู้ร่วมงานทุกท่านที่ บริษัท บัตรกรุงไทย จำกัด (มหาชน) ที่ได้มอบโอกาสและสิ่งดีๆ ให้แก่ข้าพเจ้า ขอบคุณเพื่อนๆ ทุกท่านที่มหาวิทยาลัยกรุงเทพ และมหาวิท ยาลัยธรรมศาสตร์ สำหรับคำแนะนำและคำปรึกษาที่ดี ขอบคุณฟ้าที่ส่งนาตยามาให้พบเจอกัน ขอบคุณที่ช่วยสานฝันและขอบคุณวันแห่งกำลังใจ

สุดท้ายและท้ายสุด ต้องขอบคุณอุ่นไอรักและกำลังใจจากป๊าและม้า ที่ช่วยนำพาให้ฉันก้าวไป ขอบคุณในความห่วงใย ขอบคุณหัวใจที่ให้กัน จะรักและอยู่คอยดูแลตลอดไป ฉันรักบ้านของฉัน

ธนัท สุวรรณปริญญา
มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

BANGKOK UNIVERSITY
FOUNDED 1962

กิตติกรรมประกาศ

ข้าพเจ้าหวังว่าสารนิพนธ์ฉบับนี้จะสามารถนำไปใช้ประโยชน์ทั้งต่อตนเองและผู้ที่สนใจได้ ความสำเร็จของสารนิพนธ์ฉบับนี้ มีเหตุปัจจัยอยู่หลายอย่างที่ทำให้ข้าพเจ้ามุ่งมั่น ตั้งใจที่จะจัดทำให้สำเร็จ สมบูรณ์ เนื่องด้วยข้าพเจ้าคิดว่าสิ่งที่รอคอยข้าพเจ้าภายหลังจากที่ข้าพเจ้าได้สำเร็จการศึกษาในระดับมหาบัณฑิต จากมหาวิทยาลัยกรุงเทพแล้ว ก็คือ ความก้าวหน้าในวิชาชีพนักกฎหมายของข้าพเจ้า และความสบายใจของคนที่ให้การสนับสนุนและช่วยเหลือข้าพเจ้าเสมอมา ข้าพเจ้าขอกราบขอบพระคุณ ท่าน ผู้ช่วยศาสตราจารย์ ดร. อรรยา สิงห์สงบ อาจารย์ที่ปรึกษาสารนิพนธ์ ผู้ซึ่งให้คำแนะนำและความช่วยเหลือแก่ข้าพเจ้าในการจัดทำสารนิพนธ์ฉบับนี้ด้วยดีเสมอมา ขอขอบคุณผู้บังคับบัญชาและผู้ร่วมงานทุกท่านที่ บริษัท บัตรกรุงไทย จำกัด (มหาชน) ที่ได้มอบโอกาสและสิ่งดีๆ ให้แก่ข้าพเจ้า ขอบคุณเพื่อน ๆ ทุกท่านที่มหาวิทยาลัยกรุงเทพ และมหาวิทยาลัยธรรมศาสตร์ สำหรับคำแนะนำและคำปรึกษาที่ดี ขอบคุณฟ้าที่ส่งนาตยามาให้พบเจอกัน ขอบคุณที่ช่วยสานฝันและขอบคุณวันแห่งกำลังใจ

สุดท้ายและท้ายสุด ต้องขอบคุณอุ่นไอรักและกำลังใจจากป๊าและม้า ที่ช่วยนำพาให้ฉันก้าวไป ขอบคุณในความห่วงใย ขอบคุณหัวใจที่ให้กัน จะรักและอยู่คอยดูแลตลอดไป ฉันรักบ้านของฉัน

ธนัท สุวรรณปริญญา
มหาวิทยาลัยกรุงเทพ
พ.ศ. 2550

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง (ต่อ)

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เป็นที่ยอมรับกันโดยทั่วไปว่า เทคโนโลยีสารสนเทศและการติดต่อสื่อสารทางสื่ออิเล็กทรอนิกส์ โดยเฉพาะการติดต่อสื่อสารผ่านระบบอินเทอร์เน็ต เป็นที่แพร่หลายและได้รับความนิยมเป็นอย่างมาก ต่อประชาคมโลก ทั้งนี้ เนื่องจากระบบการติดต่อสื่อสารผ่านระบบอินเทอร์เน็ต เป็นระบบที่มีลักษณะไร้พรมแดน ปราศจากข้อจำกัดทางด้านเวลาและสถานที่ ทำให้ผู้ใช้สามารถเข้าถึงข้อมูลข่าวสารได้ง่ายขึ้น และมีความสะดวกรวดเร็วในการติดต่อสื่อสารยิ่งขึ้น ส่งผลให้การติดต่อสื่อสาร การถ่ายโอนข้อมูล รวมไปถึงการเผยแพร่ข้อมูลต่างๆ สามารถทำได้โดยง่าย ทำให้การประมวลผล จัดเก็บ หรือเปิดเผยข้อมูลข่าวสารสามารถทำได้อย่างสะดวก และรวดเร็ว ซึ่งจากลักษณะทั่วไปของเทคโนโลยีการติดต่อสื่อสารผ่านระบบอินเทอร์เน็ตดังกล่าว ทำให้มีการนำเอาเทคโนโลยีการติดต่อสื่อสารผ่านระบบอินเทอร์เน็ตไปใช้ในการประกอบธุรกิจกันอย่างแพร่หลายปัจจุบันผู้ประกอบธุรกิจมากมายเริ่มที่จะเปลี่ยนวิธีการในการจัดเก็บข้อมูลต่างๆ ให้อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ แทนที่การจัดเก็บข้อมูลในรูปกระดาษ ซึ่งเหตุผลและปัจจัยสำคัญที่ทำให้ข้อมูลต่างๆ ถูกทำให้อยู่ในรูปดิจิทัล (digital format) มีดังต่อไปนี้[1]

1. การสร้าง ส่งหรือเก็บข้อมูลสามารถทำได้ง่ายและสะดวกกว่าการทำให้อยู่ในรูปแบบปกติ
2. การเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ทำให้เกิดการลดต้นทุนทางธุรกิจในการสร้าง ส่ง หรือเก็บข้อมูล โดยเฉพาะอย่างยิ่ง เมื่อกระทำการผ่านระบบอินเทอร์เน็ต
3. เมื่อสังคมก้าวเข้าสู่ยุคสังคมสารสนเทศทำให้ข้อมูลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์มีมูลค่าในตัวเอง สามารถซื้อขายได้ หรือนำไปทำธุรกรรมอื่นๆ ได้
4. คุณสมบัติและความสามารถของระบบคอมพิวเตอร์และเครือข่าย ที่เอื้ออำนวยให้เกิดการใช้มากขึ้น เช่น ความสามารถในการ สำรองข้อมูล (back-up) เพื่อป้องกับการสูญหายของข้อมูล
5. การประมวลผลข้อมูลสามารถได้โดยง่ายโดยการใช้โปรแกรมคอมพิวเตอร์ (software) มาช่วยในการประมวลผลข้อมูล

---

[1] กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข ”, (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2549), หน้า 379.

จากเหตุผลที่กล่าวมาจึงส่งผลทำให้การส่งเอกสารและข้อมูลต่างๆ ทำได้โดยสะดวกมากขึ้น และเมื่อมีการนำเทคโนโลยีดังกล่าวเข้ามาใช้ในการประกอบธุรกิจ จึงมีความจำเป็นต้องหามาตรการมาป้องกันความปลอดภัยให้กับข้อมูลต่างๆ ที่มีการถ่ายโอนไปมา เพื่อสร้างความเชื่อน่าเชื่อถือ (Trust) และสร้างความเชื่อมั่น (Confidence) ในการทำธุรกรรมต่างๆ ทางอิเล็กทรอนิกส์ ทั้งนี้ เพื่อป้องกันการนำ ประโยชน์ของเทคโนโลยีเหล่านี้ไปใช้โดยมิชอบ ซึ่งอาจเป็นการละเมิดสิทธิส่วนบุคคลหรือความเป็นส่วนตัวของบุคคลอื่นได้

คำว่า "สิทธิส่วนบุคคล" หมายถึง สิทธิของบุคคลที่ประกอบไปด้วย สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง รวมทั้งความเป็นอยู่ส่วนตัว โดยสิทธิส่วนบุคคลเป็นสิทธิที่แต่ละบุคคลจะต้องได้รับการคุ้มครองและการเคารพ โดยทั่วไปแล้วข้อมูลส่วนบุคคลก็เป็นสิทธิส่วนบุคคลที่จะต้องได้รับการคุ้มครองเช่นกัน ดังนั้น การกระทำการอันเป็น การละเมิดข้อมูลส่วนบุคคลของบุคคลอื่น ย่อมไม่อาจกระทำได้ และรัฐจะกระทำการละเมิดหรือจำกัดสิทธิส่วนบุคคลไม่ได้ เว้นแต่ มีกฎหมายให้ทำได้เพื่อรักษาความมั่นคง เพื่อรักษาความสงบเรียบร้อยและศีลธรรมอันดีของประชาชนด้วย[2]

แต่เนื่องด้วยการพัฒนาทางเทคโนโลยีทำให้ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ทั้งหลายสามารถเก็บรวบรวมข้อมูลส่วนบุคคล และสามารถเฝ้าติดตาม พฤติกรรมในการใช้บริการเว็บไซต์ของลูกค้าได้ โดยลูกค้าหรือผู้ใช้บริการไม่ทราบและไม่ได้ให้ความยินยอมแก่การกระทำดังกล่าว หรือแม้จะมีการให้ความยินยอมแล้วก็อาจจะมีปัญหาการนำข้อมูลส่วนบุคคลไปใช้เกินขอบเขตที่ได้ให้ความยินยอมไว้ได้ ซึ่งปัญหาดังกล่าวก็ส่งผลกระทบโดยตรงต่อสิทธิส่วนบุคคล ซึ่งเป็นการกระทบต่อข้อมูลส่วนบุคคลของ ผู้บริโภค อันทำให้ผู้บริโภคขาดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบต่อเนื่องทำให้การพาณิชย์อิเล็กทรอนิกส์ของประเทศไม่เติบโตเท่าที่ควร ดังนั้น สิ่งที่ผู้ประกอบการทางพาณิชย์อิเล็ก ทรอนิกส์จำเป็นจะต้องทำให้เกิดขึ้นก็คือ การสร้างความเชื่อมั่นให้กับผู้บริโภคในเรื่องการให้ความคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล โดยวิธีการที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์สามารถดำเนินการ หรือจัดทำได้เอง และเป็นวิธีการที่ได้รับความนิยมวิธีการหนึ่ง ก็คือ การจัดทำนโยบายความเป็นส่วนตัว หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) นั่นเอง

โดยที่คำว่า “ความเป็นส่วนตัว” หรือ “privacy” เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่ได้มีการบัญญัติรับรองคุ้มครองตามกฎหมาย ซึ่งตามปฏิญญาสากลว่าด้วยสิทธิมนุษยช น ค.ศ. 1948 (Universal Declaration of Human Right 1948) มาตรา 12[3] ซึ่งบัญญัติว่า “บุคคลใดๆ

---

[2] Samual Warren & Louis D.Brandeis, The Right to Privacy, Harvard Law Review, 1980, P 1-3.

[3] Article 12 of Universal Declaration of Human Right 1948 “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence’ nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

จะถูกสอดแทรกโดยพลการในชีวิตส่วนบุคคลในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกดูหมิ่นในเกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการสอดแทรกหรือการดูหมิ่นดังกล่าวนั้น " จากบทบัญญัติดังกล่าวจะเห็นได้ว่า ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค .ศ. 1948 ได้บัญญัติรับรองสิทธิความเป็นส่วนตัวไว้อย่างชัดเจน และนานาประเทศต่างก็ให้ความสำคัญต่อการคุ้มครองความเป็นส่วนตัว ดังจะเห็นได้จากการที่ประเทศต่าง ๆ ได้บัญญัติกฎหมายภายในของตนที่ให้ความคุ้มครองความเป็นส่วนตัวเอาไว้ในกฎหมายของตน ประเทศไทยก็เป็นประเทศหนึ่งได้เล็งเห็นถึงความสำคัญของการให้ความคุ้มครองความเป็นส่วนตัวเช่นกัน ดังจะเป็นได้จากร่างรัฐธรรมนูญฉบับใหม่ที่กำลังอยู่ระหว่างการยกร่าง ได้บัญญัติรับรอง สิทธิความเป็นส่วนตัวว่า "สิทธิของบุคคลในครอบครัวเกียรติยศ ชื่อเสียง และความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง " และตามมาตรา 28 และมาตรา 34 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พ .ศ. 2540 ได้ให้ความคุ้มครองสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณชน จึงจำเป็นต้องมีการกำหนดกลไกในการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งสามารถประมวลผล และเผยแพร่ถึงบุคคลจำนวนมากได้โดยง่าย สะดวก รวดเร็วโดยอาศัยเทคโนโลยีสารสนเทศอันทันสมัย ทั้งนี้ โดยกำหนดให้มี คณะกรรมการข้อมูลส่วนบุคคลเพื่อวางนโยบาย และกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล และจากบทนิยามของคำว่า "ข้อมูลส่วนบุคคล " ที่ปรากฏในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... มาตรา 4 ได้ให้ความหมายว่า "ข้อเท็จจริงที่เกี่ยวกับบุคคล ซึ่งสำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม" จากบทนิยามดังกล่าวทำให้สามารถตีความได้ว่าข้อมูลส่วนบุคคล หมายถึง ข้อมูลบุคคล, ข้อมูลที่เป็นเรื่องส่วนตัว, ข้อมูลเกี่ยวกับบุคคล และรวมไปถึงข้อมูลต่างๆ ที่ทำให้ระบุตัวบุคคลนั้นได้ เช่น หมายเลขประจำตัว รหัส ลายนิ้วมือ เป็นต้น โดยที่ตัวอย่างของข้อมูลบุคคลนั้น ก็เช่น ชื่อ อายุ เพศ ส่วนสูง น้ำหนัก หรือสีผิว เป็นต้น, ข้อมูลที่เป็นเรื่องส่วนตัว เช่น การศึกษา ฐานะทางการเงิน การนับถือศาสนา ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน เป็นต้น , ข้อมูลเกี่ยวกับบุคคล ซึ่งจะเป็นข้อมูลใดๆ ก็ได้ที่เกี่ยวกับบุคคลนั้น เช่น พฤติกรรมการบริโภค การใช้ชีวิตประจำวัน[4]

โดยทั่วไปแล้ว ข้อมูลส่วนบุคคลจะสามารถแบ่งออกได้สองประเภทคือ ข้อมูลส่วนบุคคลที่มีลักษณะทั่วไป และข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว โดยที่ข้อมูลที่มีลักษณะทั่วไปหมายถึงข้อมูลทั่วไปของบุคคล เช่น ชื่อ อายุ เพศ ส่วนสูง น้ำหนัก สีผิว การศึกษา เป็นต้น และ

---

[4] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ , แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล , (กรุงเทพมหานคร : สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2546), หน้า 25.

ข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว หรือ Sensitive Data หมายถึง ข้อมูลสำคัญที่ถือว่าเป็นความลับอย่างมากไม่สามารถแพร่งพรายออกสู่ภายนอกได้ เป็นข้อมูลที่อ่อนไหวได้ง่าย เสียหายได้ง่ายและสร้างความ เสียหายได้ง่าย [5] เป็นข้อมูลที่กระทบต่อความเป็นอยู่ส่วนตัวของเจ้าของข้อมูลมาก เช่น ฐานะทางการเงิน การนับถือศาสนา ประวัติสุขภาพ ประวัติอาชญากรรม เป็นต้น

สำหรับปัญหาการละเมิดความเป็นส่วนตัวเกี่ยวกับข้อมูลส่วนบุคคลนั้น นานาประเทศรวมทั้งองค์การระหว่างประเทศต่างก็ให้ความสำคัญเป็นอย่างมาก โดยหลายประเทศทั่วโลกให้ความสำคัญต่อการความคุ้มครองข้อมูลส่วนบุคคลอย่างจริงจัง โดยที่ The Organization for Economic Cooperation and Development หรือ OECD ซึ่งเป็นองค์การระหว่างประเทศที่ให้ความสำคัญกับปัญหาดังกล่าว ได้กำหนดแนวทางหรือกฎเกณฑ์ขั้นพื้นฐาน (Guidelines) ในการคุ้มครองข้อมูลส่ วนบุคคล เพื่อให้นานาประเทศได้มีแนวทางในการบัญญัติกฎหมายของตนเอง ได้ออก Guidelines Governing the Protection of Privacy and Tranborder Data Flows of Personal Data ขึ้นในปี ค.ศ. 1980 เพื่อวางหลักการสำคัญว่า ข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองที่เหมาะสมในทุกขั้ นตอน ตั้งแต่การเก็บรวบรวม การใช้ การเก็บรักษา และการเปิดเผย และใน ค .ศ. 1999 ได้ออก Guidelines for Consumer Protection in the context of Electronic Commerce ขึ้นเพื่อคุ้มครองผู้บริโภคในการทำธุรกรรมทางอิเล็กทรอนิกส์ร่วมกับผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ ซึ่งได้กำหนดสาระสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคด้วย และองค์การระหว่างประเทศอื่นที่ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลก็คือ สหประชาชาติ หรือ United Nation (UN) ได้กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขั้นต่ำไว้ใน Guidelines for the Regulation of Computerized Personal Data File ที่ออกเมื่อปี ค .ศ. 1990 และสหภาพยุโรป หรือ European Union (EU) ก็ได้ออกกฎเกณฑ์หลายฉบับที่มีสาระสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วย เช่น Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ซึ่งกฎเกณฑ์นี้มีวัตถุประสงค์ในการ ป้องกันความเป็นส่วนตัวของข้อมูลส่วนบุคคลและให้ความสำคัญกับการโอนถ่ายข้อมู ลส่วนบุคคลด้วย ซึ่งข้อตกลงนี้จะมีการให้ความคุ้มครองข้อมูลที่อ่อนไหว หรือ Sensitive Data เป็นพิเศษด้วย ข้อตกลงอีกฉบับที่ EU กำหนดขึ้นก็คือ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ซึ่งกฎเกณฑ์นี้มีวัตถุประสงค์ในการ ป้องกันทุกกระบวนการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และมีการคุ้มครองความเป็นส่วนตัวในการติดต่ อสื่อสารทางอิเล็กทรอนิกส์ด้วย นอกจากนี้ประเทศ

---

[5] Internet Security ศัพท์ต่าง ๆ ที่เกี่ยวข้องกับการเข้ารหัสและถอดรหัส <http://coursewares.mju.ac.th/bt454/Chapter5/C1T5_01.htm>

ต่างๆ ทั่วโลก ต่างก็ได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลโดยการออกกฎหมายภายในประเทศของตนให้สอดคล้องกับหลักเกณฑ์ที่องค์การระหว่างประเทศได้กำหนดขึ้นด้วย เช่น ประเทศอังกฤษ ได้ออก The Data Protection Act หรือ DPA ขึ้นในปี 1998, ประเทศสหรัฐอเมริกา ได้ออก Privacy Act ในปี 1974, Children's On line Privacy Protection Act ในปี 1998, ประเทศออสเตรเลียได้ออก Privacy Act ขึ้นในปี 1993, ประเทศเบลเยี่ยมได้ออก Belgium Law on Privacy Protection in relation to the Processing of Personal Data ในปี 1992, ประเทศอิตาลี ได้ออก Protection of individuals and other subjects with regard to the processing of personal data Act ในปี 1996, ประเทศเดนมาร์ค Act on Processing of Personal Data ในปี 2000, ประเทศนิวซีแลนด์ ได้ออก The Privacy Act ในปี 1993, ประเทศฮ่องกง ได้ออก Personal Data (Privacy) Ordinance ในปี 1996 เป็นต้น สำหรับประเทศไทยนั้น ก็ได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลเช่นกัน โดยขณะนี้ ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ. ... กำลังอยู่ในระหว่างการพิจา รณากลั่นกรองในกระบวนการนิติบัญญัติ ซึ่งร่างพระราชบัญญัติดังกล่าวได้ร่างขึ้นโดยอาศัย EU Directive และกฎหมายของออสเตรเลีย ฮ่องกงและนิวซีแลนด์[6] เป็นต้นแบบด้วย

อย่างไรก็ตาม นอกจากวิธีการคุ้มครองข้อมูลส่วนบุคคล จะทำได้โดยการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีลักษณะให้ความคุ้มครองเป็นการทั่วไป หรือบัญญัติกฎหมายที่ให้ความคุ้มครองแต่ละเรื่องไว้โดยเฉพาะแล้ว การคุ้มครองข้อมูลส่วนบุคคลอาจทำได้โดยวิธีการอื่นๆ เช่น การกำหนดกลไกการกำกับดูแลตนเอง (self-regulation) โดยให้ผู้ประกอบการภาคธุรกิจจัดทำนโยบายความเป็นส่วนตัว หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) และมีการกำหนดประมวลจริยธรรม (Codes of practice) ของตนเองขึ้น รวมไปถึงการใช้เครื่องหมายรับรองความน่าเชื่อถือ (Trustmark) ซึ่งออกโดยองค์กรกลางที่ทำหน้าที่ ออกเครื่องหมายรับรองความน่าเชื่อถือ เพื่อสร้างความมั่นใจให้แก่ผู้บริโภคว่าผู้ประกอบการรายนั้นๆ มีมาตรฐานเป็นไปตามที่องค์กรกลางกำหนด และรวมไปถึงการพัฒนาเทคโนโลยีให้มีความทันสมัยและสามารถใช้ป้องกันการละเมิดข้อมูลส่วนบุคคลด้วย เป็นต้น ทั้งนี้ การกำหนดรูปแบ บการคุ้มครองข้อมูลส่วนบุคคลจะขึ้นอยู่กับระบบกฎหมาย รูปแบบการปกครอง นโยบายรัฐ ความก้าวหน้าทางเทคโนโลยี รวมทั้งสภาพสังคม วัฒนธรรม และพฤติการณ์แวดล้อมต่างๆ ของประเทศนั้นๆ

สำหรับการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ในหมวดที่ 2 ว่าด้วย จริยธรรมในการคุ้มครองข้อมูลส่วนบุคคล มาตรา 18 กำหนดว่า "...บุคคลหรือหน่วยงานอาจจัดทำประมวลจริยธรรมเพื่อกำหนดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลก็ได้ ..." จากบทบัญญั ติดังกล่าวจะเห็ นได้ว่ากฎหมายไม่ได้บังคับให้ผู้ปร ะกอบการต้องจัดทำประมวลจริยธรรม เพียงแต่ผู้ประกอบการจะ

---

[6] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ , *อ้างแ ล้ว เชิงอรรถที่ 3*, หน้า12-14.

จัดทำหรือไม่ขึ้นอยู่การให้ความสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการของผู้ประกอบการเอง และขึ้นอยู่กับนโยบายในการบริหารกิจการของผู้ประกอบการด้วย อย่างไรก็ตาม แม้ว่าร่างพระราชบัญญัติว่าด้วย การคุ้มครองข้อมูลส่วนบุคคล พ .ศ. .... จะไม่ได้บังคับให้ผู้ประกอบการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลก็ตาม แต่เนื่องจากกิจการบางประเภทกิจการ เช่น ธนาคาร ผู้ประกอบการบัตรเครดิตและ /หรือสินเชื่อส่วนบุคคล เป็นต้น ซึ่งเป็นกิจการที่เกี่ยวข้องกับการให้บริการทาง การเงินขนาดใหญ่ และกระทบต่อผู้บริโภคจำนวนมาก จะมีความเกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลของผู้ใช้บริการ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่มีลักษณะทั่วไป และ /หรือข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว เพราะการสมัครเข้ารับบริการ หรือการทำธุรกรรมกับผู้ประกอบการรายนั้นๆ ผู้ใช้บริการจะต้องให้ข้อมูลส่วนบุคคลของตนแก่ผู้ประกอบการนั้นๆ เพื่อใช้ประกอบในการสมัครเข้ารับบริการหรือทำธุรกรรมกับผู้ประกอบการรายนั้นๆ ดังนั้น ผู้ประกอบการก็ควรจะต้องมีการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานในระดับสูงด้วย ทั้งนี้ เพื่อสร้างค วามน่าเชื่อถือให้เกิดขึ้นต่อผู้ใช้บริการ และสร้างภาพลักษณ์ที่ดีต่อภาพรวมของธุรกิจการเงินการธนาคารของประเทศไทย ซึ่งส่งผลดีต่อสภาพเศรษฐกิจของประเทศด้วย

ปัจจุบันกรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ ได้ให้ความสำคัญกับปัญหาที่เกี่ยวข้องกับการให้ความคุ้มครองข้อมู ลส่วนบุคคล โดยจัดให้บริการจดทะเบียนพาณิชย์อิเล็กทรอนิกส์ จัดตั้งศูนย์จัดการข้อร้องเรียนด้านพาณิชย์อิเล็กทรอนิกส์ และทำหน้าที่ออกเครื่องหมายรับรองความน่าเชื่อถือหรือ Trustmark สำหรับผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ที่มีคุณสมบัติตามที่กำหนด ซึ่งคุณสมบัติที่สำคัญข้อหนึ่งก็คือ การมีมาตรฐานการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับสูง นอกจากนี้ ในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ. ... ก็ได้มีการกำหนดบทเฉพาะกาล ให้มีการแต่งตั้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นด้วย ซึ่งแสดงให้เห็นว่าประเทศ ไทยก็ได้ให้ความสำคัญกับการให้ความคุ้มครองข้อมูลส่วนบุคคลด้วยเช่นกัน

โดยทั่วไปแล้ว กลไกการกำกับดูแลตนเอง ถือเป็นแนวทางหนึ่ง ที่ช่วยผ่อนคลายความเคร่งครัด หรือความเข้มงวดของกฎเกณฑ์หรือกฎหมายที่ออกโดยรัฐ เนื่องจากผู้ประกอบการสามารถที่จะวางหลักเกณฑ์ในทางปฏิบัติส อดคล้องกับการดำเนินงานภายในองค์กรของตนเองมากที่สุด [7] ทั้งนี้ เพื่อให้การประกอบธุรกิจของผู้ประกอบการเป็นไปอย่างราบรื่น และส่งผลกระทบในทางธุรกิจกับผู้ประกอบการน้อยที่สุด โดยไม่ถือว่าปฏิบัติผิดกฎเกณฑ์ของรัฐ ซึ่งการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ก็เป็นรูปแบบตามแนวทาง การกำกับดูแลตนเองที่ผู้ประกอบการสามารถกำหนดขึ้นได้ เนื่องจาก นโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ประกาศให้แก่ลูกค้าหรือผู้ใช้บริการของตนทราบว่า ผู้ประกอบการมีนโยบายหรือแนวทางในการ บริหารจัดการข้อมูลส่วนบุคคลอย่างไร เพื่อให้ลูกค้าหรือผู้ใช้บริการทราบและสามารถใช้พิจารณาตัดสินใจได้ว่าตน

---

[7] *เพิ่งอ้าง*, หน้า 53-54.

จะให้ข้อมูลส่วนบุคคลของตนหรือไม่ อย่างไรก็ตาม เนื่องจากการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการไม่ได้ถูกควบคุมโดยกฎหมายหรือองค์กรใดๆ จึงอ าจทำให้การกำหนดนโยบายของผู้ประกอบการต่างๆ ไม่ได้มาตรฐานและไม่อาจคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริง และเนื่องจาก นโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ได้จัดทำขึ้นเอง โดยมีวัตถุประสงค์เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบถึงนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของตน ดังนั้น เพื่อสร้างความน่าเชื่อถือต่อลูกค้าหรือผู้ใช้บริการ ผู้ประกอบการจึงอาจกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ดูน่าเชื่อถือ โดยไม่ได้คำนึงว่าจะสามารถปฏิบัติได้ตามที่ตนได้ประกาศไว้จริงหรือไม่เพียงใด ซึ่งอาจก่อให้เกิดปัญหาในทางปฏิบัติมากมาย อีกทั้งการตีความว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลมีสถานะทางกฎหมายอย่างไร ก็ถือเป็นเรื่องสำคัญ เพราะในกรณีที่ผู้ประกอบการไม่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ตามนโยบายที่ตนประกาศไว้ นั้น ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้เสียหายจะสามารถฟ้องร้องหรือดำเนินการทางกฎหมายอย่างไรต่อผู้ประกอบการได้ และกฎหมายที่มีผลบังคับใช้อยู่จะเพียงพอหรือไม่ที่จะดำเนินการเอาผิดกับผู้ประกอบการนั้นๆ นอกจากนี้ ในกรณีที่ผู้ประกอบการได้กำหนดนโยบายการคุ้มครองข้อมู ลส่วนบุคคลของตนไว้ แต่ได้มีการกำหนดข้อยกเว้นหรือข้อจำกัดความรับผิดของตนไว้ด้วยนั้น จะถือได้หรือไม่ว่าลูกค้าหรือผู้ใช้บริการได้ยอมรับด้วยกับข้อยกเว้นหรือข้อจำกัดความรับผิดนั้น และจะถือว่าเป็นธรรมต่อลูกค้าหรือผู้ประกอบการซึ่งเป็นผู้บริโภคหรือไม่

1.2 วัตถุประสงค์ของการศึกษา

งานวิจัยฉบับนี้มีวัตถุประสงค์ในการศึกษาดังต่อไปนี้

1.2.1 เพื่อศึกษาถึงความหมายของข้อมูลส่วนบุคคลบนอินเทอร์เน็ต รวมทั้งรูปแบบและประเภทของข้อมูลส่วนบุคคลบนอินเทอร์เน็ต

1.2.2 เพื่อให้ทราบถึงความหมาย รูปแบบและวิธีการให้คุ้มครองข้อมูลส่วนบุค คลบนอินเทอร์เน็ต

1.2.3 เพื่อให้ทราบถึงแนวทางการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในต่างประเทศ

1.2.4 เพื่อให้ทราบถึงแนวทางการให้ความคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยอาศัยกลไกการกำกับดูแลตนเอง โดยวิธีการจัดทำนโยบายการคุ้มคร องข้อมูลส่วนบุคคล

1.2.5 เพื่อศึกษาความหมาย ความจำเป็น และสถานะทางกฎหมายของนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงการใช้บังคับของนโยบายการคุ้มครองข้อมูลส่วนบุคคลและบทลงโทษของผู้ที่ฝ่าฝืนนโยบายการคุ้มครองข้อมูลส่วนบุคคล ทั้งในต่างประเทศและประเทศไทย

1.2.6 เพื่อวิเคราะห์เปรียบเทียบลักษณะและแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต ของประเทศไทยกับต่างประเทศ

1.2.7 เพื่อเสนอแนะแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

1.3 ขอบเขตของการศึกษา

งานวิจัยฉบับนี้จะทำการศึกษาวิเคราะห์กฎหมายและแนวทางปฏิบัติที่เกี่ยวข้องกับการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลทั้งของประเทศไทยและต่างประเทศ และจะศึกษาถึงสถานการณ์ปัจจุบัน และศึกษาเปรียบเทียบการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจประเภทธนาคาร ผู้ประกอบการบัตรเครดิตและ /หรือสินเชื่อส่วนบุคคล พร้อมทั้งจะทำการศึกษานโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจประเภทธนาคาร ผู้ประกอบการบัตรเครดิตและ/หรือสินเชื่อส่วนบุคคลทั้งในต่างประเทศและประเทศไทยด้วย โดยที่งานวิจัยฉบับนี้จะมุ่งศึกษาปัญหาในทางปฏิบัติที่เกิดขึ้นกับธุรกิจประเภทธนาคารและผู้ประกอบธุรกิจบัตรเครดิตและ /หรือสินเชื่อส่วนบุคคล เนื่องจากธุรกิจดังกล่าวเป็นธุรกิจขนาดใหญ่ที่กระทบต่อผู้บริโภคจำนวนม ากและมีความเกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลโดยเฉพาะด้วย

1.4 วิธีการศึกษา

การศึกษาวิจัยในครั้งนี้ ผู้เขียนใช้วิธีการวิจัยจากเอกสาร โดยค้นคว้าจากหนังสือ และบทความ ทั้งภาษาไทยและภาษาต่างประเทศ รวมทั้งข้อมูลทางอินเทอร์เน็ต โดยจะเข้าไปเยี่ยมชมเว็บไซต์ของผู้ประกอบธุรกิจประเภทธนาคาร ผู้ประกอบการบัตรเครดิตและ /หรือสินเชื่อส่วนบุคคล เพื่อศึกษาข้อเท็จจริงต่างๆ ที่เกี่ยวข้องกับการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการนั้นๆ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ทราบถึงความหมายของข้อมูลส่วนบุคคลบนอินเทอร์เน็ต รวมทั้งรูปแบบและประเภทของข้อมูลส่วนบุคคลบนอินเทอร์เน็ต

1.5.2 ได้ทราบถึงความหมาย รูปแบบและวิธีการให้คุ้มครองข้อมูลส่วนบุคคลบนอินเทอร์เน็ต

1.5.3 ได้ทราบถึงแนวทางการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิ กส์ในต่างประเทศ

1.5.4 ได้ทราบถึงแนวทางการให้ความคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดยอาศัยกลไกการกำกับดูแลตนเอง โดยวิธีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล

1.5.5 ได้ทราบถึงความหมาย ความจำเป็น และสถานะทางกฎหมายของนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมไปถึงการใช้บังคับของนโยบายการคุ้มครองข้อมูลส่วนบุคคลและบทลงโทษของผู้ที่ฝ่าฝืนนโยบายการคุ้มครองข้อมูลส่วนบุคคล ทั้งในต่างประเทศและประเทศไทย

1.5.6 ได้ทราบความแตกต่างของ ลักษณะและแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจประเ ภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต ของประเทศไทยกับต่างประเทศ

1.5.7 ได้เสนอแนะแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

บทที่ 2

ความทั่วไปเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.1 ความทั่วไปเกี่ยวกับ “ข้อมูลส่วนบุคคล”

ข้อมูลส่วนบุคคล มาจากคำว่า “ข้อมูล” และคำว่า “ส่วนบุคคล” รวมกัน โดยที่คำว่า “ข้อมูล” นั้น ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทร อนิกส์ พ.ศ. 2544 สามารถตีความได้ว่าหมายถึง ข้อความ เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ ส่วนคำว่า “ส่วนบุคคล” จะหมายถึง ความเป็นส่วนตัว โดยคำ ว่า “ความเป็นส่วนตัว” นั้นมีการให้คำนิยามความหมายไว้มากมาย ซึ่งจะได้มีการกล่าวต่อไปในงานวิจัยฉบับนี้ ดังนั้น การกล่าวถึงคำว่า “ข้อมูลส่วนบุคคล” ก็จะหมายถึงความเกี่ยวโยงระหว่าง ข้อเท็จจริงและความเป็นส่วนตัว ดังนั้น ในการพิจารณาถึงการคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นที่จะต้องทราบถึงความสัมพันธ์ระหว่าง ความเป็นส่วนตัว (Privacy) กับข้อมูลส่วนบุคคล ดังนี้

2.1.1 ความเป็นส่วนตัว (Privacy) กับข้อมูลส่วนบุคคล

คำว่า “ความเป็นส่วนตัว” หรือ “privacy” เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ที่ได้มีการบัญญัติรับรองคุ้มครองตามกฎหมาย ซึ่งตามปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค .ศ. 1948 (Universal Declaration of Human Right 1948) มาตรา 12 บัญญัติว่า “บุคคลใดๆ จะถูกสอดแทรกโดยพลการในชีวิตส่วนบุคคลในครอบครัว ในเคหสถาน หรือในการสื่อสาร หรือจะถูกดูหมิ่นในเกียรติยศและชื่อเสียงไม่ได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการสอดแทรกหรือการดูหมิ่นดังกล่าวนั้น” ได้บัญญัติรับรองไว้อย่างชัดเจน และต่อมาได้มีการนิยามความหมายของคำว่า “ความเป็นส่วนตัว” หรือ “สิทธิความเป็นส่วนตัว” ไว้อย่างมากมาย เช่น

Black’s Law Dictionary ได้ให้ความหมายของสิทธิในชีวิตส่วนตัวไว้ว่า หมายถึงสิทธิของบุคคลที่จะอยู่โดยลำพัง เสรี ปราศจากการรบกวนจากบุคคลภายนอก เป็นสิทธิที่ปลอดจากการแทรกแซงโดยรัฐในกิจกรรมส่วนตัว เป็นเสรีภาพขั้นพื้นฐานของบุคคลที่จะเลือกในการดำเนินชีวิตของตนไม่ว่าในเรื่องครอบครัว หรือเรื่องค วามสัมพันธ์กับบุคคลอื่นหรือเป็นสิทธิเสรีภาพส่วนบุคคลที่จะถอนตนเองจากการที่จะถูกพิจารณาโดยสังคม[1]

---

[1] กิตติพงศ์ กมลธรรมวงศ์ , “การคุ้มครองข้อมูลข่าว สารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข ”, (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ , 2549, หน้า 17-18.

Alan F. Westin ให้ความหมายว่า สิทธิของแต่ละบุคคล กลุ่มหรือองค์กรในการตัดสินใจว่าข้อมูลข่าวสารของตนเองนั้นจะถูกเปิดเผยต่อบุคคลอื่น เมื่อใด อย่างไร และมีขอบเขตมากน้อยเพียงใด[2]

Richard A. Spinello ได้ให้ความหมายของว่า หมายถึงการจำกัดการเข้าถึงตัวปัจเจกชนโดยบุคคลอื่น (the limitation of other's access to an individual) ซึ่งประกอบไปด้วยปัจจัยที่สำคัญ 3 ประการคือ

1) การเก็บรักษาความลับ (Secrecy) ซึ่งหมายถึงการจำกัดไม่ให้บุ คคลอื่นทราบข้อมูลที่เกี่ยวข้องกับตนเอง (limiting the dissemination of knowledge about oneself)
2) การปิดบังชื่อหรือไม่เปิดเผยตัว (Anonymity) ซึ่งหมายถึงการป้องกันมิให้คนอื่นทราบว่าตนเองเป็นใคร (protection from undesired attention)
3) การอยู่ตามลำพัง (Solitude) ซึ่งหมายถึงการไม่มีบุคคลอื่นเข้ามาอยู่ใกล้ชิดในทางกายภาพ (lack of physical proximity of others)

Samuel D. Warren และ Louis D. Brandeis ได้ให้ความหมายของสิทธิความเป็นอยู่ส่วนตัวว่าหมายถึง สิทธิที่จะอยู่โดยลำพัง (The Right to be let alone) โดยที่ทั้งสองท่านนี้ได้มองสิทธิในความเป็นอยู่ส่วนตัวออกเป็นสองแง่มุมคือ

1) ความเป็นส่วนตัวในแง่นามธรรม ได้แก่ การที่บุคคลมีสิทธิและเสรีภาพในการแสดงอารมณ์ ความรู้สึกนึกคิด ตลอดจน ความเชื่อถือศรัทธาในลัทธิศาสนา
2) ความเป็นส่วนตัวในทางรูปธรรม ได้แก่ สิทธิที่จะอยู่โดยลำพังปราศจากกา รการรบกวนและปราศจากการแทรกแซงจากสังคม การอยู่อย่างสันโดษไม่ติดต่อสัมพันธ์กับสังคม

ซึ่งความหมายของคำว่าความเป็นส่วนตัวที่สอดคล้องกับสภาพสังคมและการพัฒนาทางเทคโนโลยีในปัจจุบันมากที่สุดที่เกี่ยวข้องกับข้อมูลข่าวสารส่วนบุคคล ก็คือ ความหมายของ Alan F. Westin ที่ได้ให้ความหมายว่า สิทธิของแต่ละบุคคล กลุ่มหรือองค์กรในการตัดสินใจว่าข้อมูลข่าวสารของตนเองนั้นจะถูกเปิดเผยต่อบุคคลอื่น เมื่อใด อย่างไร และมีขอบเขตมากน้อยเพียงใด

จากความหมายของคำว่า "ความเป็นส่วนตัว " หรือ "สิทธิความเป็นส่วนตัว " ที่ยกมากล่าวข้างต้น สามารถแสดงให้เห็นได้ว่าความเป็นส่วนตัวสามารถแบ่งออกได้ 4 ประเภทคือ

1. ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)

เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่ อสารอื่นใดที่ผู้อื่นจะล่วงรู้ไม่ได้

---

[2] "Privacy" means the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others.

ทั้งนี้ บทบัญญัติที่สะท้อนการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารในกฎหมายไทยปรากฏเห็นได้ในกฎหมายหลายฉบับ อาทิ

- ประมวลกฎหมายอาญา มาตรา 322 บัญญัติว่า “ผู้ใดเปิดผนึก หรือเอาจดหมาย โทรเลข หรือเอกสารใดๆ ซึ่งปิดผนึกของผู้อื่นไป เพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อความในจดหมาย โทรเลข หรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษ...”

- พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ .ศ. 2544 มาตรา 74 บัญญัติว่า “ผู้ใดกระทำการด้วยประการใดๆ เพื่อดักรับไว้ ใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสาร หรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย ต้องระวางโทษ ...”

2. ความเป็นส่วนตัวในดินแดนหรืออาณาเขต (Territorial Privacy)

เป็นการกำหนดขอบเขตหรือข้อจำกัดที่ บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวีดิโอ และการตรวจสอบรหัสประจำตัวบุคคล (ID checks)

โดยบทบัญญัติที่สะท้อนการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในดินแดนหรืออาณาเขตตามกฎหมายไทยปรากฏให้เห็นได้ใน ประมวลกฎหมายอาญา มาตรา 362 ซึ่งบัญญัติว่า “ผู้ใดเข้าไปในอสังหาริมทรัพย์ของผู้อื่นเพื่อถือการครอบครองอสังหาริมทรัพย์นั้นทั้งหมดหรือแต่บางส่วน หรือเข้าไปกระทำการใดๆ อันเป็นการรบกวนการครอบครองอสังหาริมทรัพย์ของเขาโดยปกติสุข ต้องระวางโทษ ...” เป็นต้น

3. ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy)

เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใดๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม หรือการทดลองยา เป็นต้น

ทั้งนี้ บทบัญญัติที่สะท้อนให้เห็นถึงการคุ้มครองสิทธิความเป็นส่วนตัวในชีวิตร่างการ อาทิ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 ซึ่งบัญญัติว่า “ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิด จำต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้น”

4. ความเป็นส่วนตัวเกี่ยวกับข้อมูลข่าวสาร (Information Privacy)

เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล หรือเป็นที่รู้จักกันภายใต้คำว่า “data protection”

ทั้งนี้ บทบัญญัติตามกฎหมายไทยที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ปรากฏให้เห็นได้ในกฎหมายหลายฉบับ อาทิ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ .ศ. 2540 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 และร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... เป็นต้น

จะเห็นได้ว่า ความเป็นส่วนตัว ที่ได้รับการคุ้มครองมีอยู่มากมายหลายประการ แต่ความเป็นส่วนตัวที่จะต้องให้ความสำคัญอย่างมากอันเนื่องจากพัฒนาการทางเทคโนโลยีสารสนเทศที่ก้าวหน้าไปอย่างรวดเร็ว คือ “ความเป็นส่วนตัวในข้อมูลส่วนบุคคล ” ทั้งนี้ เพราะพัฒนาการล้ำยุคของคอมพิวเตอร์ส่งผลให้การติดต่อสื่อสารและการเผยแพร่ข้อมูลต่างๆ สามารถเคลื่อนย้ายและเชื่อมโยงกันได้โดยไม่จำกัดเวลาและสถานที่อีกต่อไป ทำให้การประมวลผล จัดเก็บ หรือเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวกและรวดเร็ว ในทางกลับกันจึงอาจมีการนำประโยชน์ของเทคโนโลยีเหล่านี้ไปใช้โดยละเมิดต่อบุคคลอื่นนั่นเอง

2.1.2 ความหมายของข้อมูลส่วนบุคคล

คำว่า “ข้อมูลส่วนบุคคล” เป็นคำที่มีความสำคัญกับการจัดทำนโยบายส่วนบุคคลเพราะบุคคลจะได้รับข้อมูลส่วนตัวของตนเพียงใด ย่อมขึ้นอยู่กับการนิยามความหมายของคำว่า “ข้อมูลส่วนบุคคล ” ด้วย ซึ่งคำว่า “ข้อมูลส่วนบุคคล ” นั้น มีความหมายกว้างซึ่งอาจทำให้เกิดปัญหาในการตีความได้ จึงต้องมีการกำหนดขอบเขตไว้อย่างชัดเจน โดยที่กฎหมายของแต่ละประเทศก็ได้นิยามความหมายของคำว่า “ข้อมูลส่วนบุคคล” ไว้แตกต่างกัน ดังนี้

1. ตาม Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ของสหภาพยุโรป คำว่า ข้อมูลส่วนบุคคล หรือ 'personal data' หมายถึง ข้อมูลข่าวสารใดๆ ที่สามารถระบุตัวหรืออาจระบุตัวบุคคลนั้นได้ ซึ่งบุคคลที่อาจระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมนี้ อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะตัวของบุคคล หรือจากปัจจัยอื่นๆ ที่มีลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรม และสภาพสังคมของบุคคลนั้น เป็นต้น[3]

---

[3] 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2. ตาม OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 ของ OECD คำว่า ข้อมูลส่วนบุคคล หรือ 'personal data' หมายถึง ข้อมูลข่าวสารใดๆ ที่สามารถระบุตัวหรืออาจระบุตัวบุคคลได้[4]

3. ตาม The Data Protection Act 1998 (DPA) ของประเทศอังกฤษ คำว่า ข้อมูลส่วนบุคคล หรือ 'personal data' หมายถึง ข้อมูลที่ความเกี่ยวพันกับบุคคลแต่ละคนที่อาจจะระบุตัวได้โดยอาศัยข้อมูลนั้น และหมายความรวมถึงความคิดเห็นและจุดมุ่งหมายของบุคคลด้วย[5]

4. ตาม Privacy Act 1993 ของประเทศออสเตรเลีย คำว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลหรือความเห็นไม่ว่าจะจริงหรือเท็จ และไม่ว่าจะบันทึกไว้ในสื่อประเภทใด โดยข้อมูลดังกล่าวเกี่ยวข้องกับปัจเจกบุคคล อันปรากฏลักษณะเฉพาะตัวอย่างชัดแจ้งหรืออาจสืบหาตัวบุคคลได้จากข้อมูลหรือความเห็นดังกล่าว[6]

5. ตาม Protection of individuals and other subjects with regard to the processing of personal data Act 1996 ของประเทศอิตาลี คำว่า ข้อมูลส่วนบุคคล หมายถึง ข้อความใดๆ ที่เกี่ยวกับบุคคลธรรมดา หรือนิติบุคคล ที่สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม[7]

---

[4] "personal data" means any information relating to an identified or identifiable individual (data subject);

[5] "personal data" means data which relate to a living individual who can be identified-

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

[6] “Personal information” means information or an opinion [including information or an opinion forming part a database], whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion

[7] “Personal data” shall means any information relating to natural or legal person, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number;

6. ตาม The Privacy Act 1993 ของประเทศนิวซีแลนด์ คำว่า ข้อมูลส่วนบุคคล หมายถึง ข้อความที่อาจระบุตัวบุคคลได้ และให้หมายความรวมถึงข้อมูลของบุคคลที่ตายไปแล้วที่ได้เก็บไว้ในทะเบียนตามกฎหมาย[8]

7. ตาม Personal Data (Privacy) Ordinance 1996 ของประเทศฮ่องกง คำว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลใดๆ ที่เกี่ยวกับบุคคลไม่ว่าทางตรงหรือโดยอ้อม หรือข้อมูลดังกล่าวในทางปฏิบัติทำให้อาจสืบหาตัวบุคคลได้ไม่ว่าทางตรงหรือโดยอ้อม และอยู่ในรูปแบบที่สามารถเข้าถึง หรือสามารถนำไปประมวลผลได้[9]

8. ตามร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วน บุคคล พ.ศ. ... คำว่า “ข้อมูลส่วนบุคคล” หมายถึง ข้อเท็จจริงเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงทางอ้อม จากบทนิยามดังกล่าวทำให้สามารถตีความได้ว่าข้อมูลส่วนบุคคล หมายถึงข้อมูลดังต่อไปนี้

- ข้อมูลบุคคล เช่น ชื่อ อายุ เพศ ส่วนสูง น้ำหนัก หรือสีผิว เป็นต้น
- ข้อมูลที่เป็นเรื่องส่วนตัว เช่น การศึกษา ฐานะทางการเงิน การนับถือศาสนา ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน เป็นต้น
- ข้อมูลเกี่ยวกับบุคคล ซึ่งจะเป็นข้อมูลใดๆ ก็ได้ที่เกี่ยวกับบุคคลนั้น เช่น พฤติกรรมการบริโภค การใช้ชีวิตประจำวัน เป็นต้น

ซึ่งความหมายของคำว่า “ข้อมูลส่วนบุคคล” ตามที่กำหนดในร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... นี้ มีความหมายกว้างกว่าคำว่าข้อมูลข่าวสารส่วนบุคคล ตามที่กำหนดในมาตรา 4 ของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งกำหนดว่า “ข้อมูลข่าวสารส่วนบุคคล หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย” จากความหมายดังกล่าวจะเห็นได้ว่า ข้อมูลข่าวสารส่วนบุคคลที่ได้รับความคุ้มครองตามกฎหมายจึงมีนัยค่อนข้างแคบ คือเน้นเฉพาะ “ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวบุคคล” ซึ่ง

---

[8] “Personal information” means information about an identifiable individual; and includes information contained in any register of deaths kept under a Births and Deaths Registration Act 1951:

[9] “Personal data” means any data -

(a) relating directly or indirectly to a living individual

(b) from which it is practicable for the identify of the individual to be directly or indirectly ascertained; and in a form in which access to or processing of the data is practicable

หมายถึง เรื่องส่วนตัวเท่านั้น [10] ซึ่งแตกต่างจากคำว่า “ข้อมูลส่วนบุคคล ” ตามความหมายของร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหมายความครอบคลุมถึง ข้อมูลบุคคล, ข้อมูลเรื่องส่วนตัว และข้อมูลเกี่ยวกับบุคคลด้วย

2.1.3 รูปแบบของข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

ข้อมูลข่าวสารส่วนบุคคลโดยทั่วไปสามารถแบ่งออกได้เป็นสองลักษณะ คือ ข้อมูลส่วนบุคคลทั่วไป หรือ Non – Sensitive Data และข้อมูลส่วนบุคคลที่อ่อนไหว หรือ Sensitive Data ซึ่งลักษณะของข้อมูลส่วนบุคคลทั้งสองประเภทมีลักษณะดังนี้[11]

2.1.3.1 ข้อมูลส่วนบุคคลทั่วไป (Non – Sensitive Data)

ข้อมูลส่วนบุคคลทั่วไป (Non – Sensitive Data) เป็นข้อมูลข่าวสารใดๆ ที่เกี่ยวข้องกับบุคคลซึ่งสามารถบ่งชี้เฉพาะตัวบุคคล อันได้แก่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ที่อยู่ทางอิเล็ กทรอนิกส์ อายุ วุฒิการศึกษา ตำแหน่งหน้าที่การงาน สถานะและลักษณะทางกายภาพของบุคคล หรือข้อมูลใดๆ ที่สามารถนำมาประมวลกันเป็นลักษณะบ่งชี้ตัวบุคคลได้ ซึ่งโดยสภาพของข้อมูลเหล่านี้สามารถเปิดเผยต่อสาธารณะได้เพราะเป็นเรื่องปกติ และไม่กระทบต่อความเป็นส่วนตัวกับเจ้าของข้อมูลมาก

2.1.3.2 ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data)

ข้อมูลส่วนบุคคลที่อ่อนไหว (Sensitive Data) ได้แก่ ข้อมูลที่ถือเป็นเรื่องเฉพาะตัว (Intimate) ของบุคคลโดยเฉพาะ เป็นข้อมูลที่เป็นความลับหรือไม่พึงประสงค์ที่จะให้มีการเปิดเผย ข้อมูลประเภทนี้ได้แก่ การนับถือลัทธิความเชื่อทางศาสนา ปรัชญาชีวิต การดำเนินชีวิตส่วนตัว ลัทธิทางการเมือง เพศสัมพันธ์ ข้อมูลสุขภาพ ข้อมูลที่เกี่ยวกับการดำเนินคดีทางอาญา เป็นต้น

ตาม The Data Protection Act 1998 (DPA) ได้ให้ความหมายของคำว่า ข้อมูลส่วนบุคคลที่อ่อนไหว หรือ Sensitive data ไว้ว่า หมายถึง [12] ข้อมูลส่วนบุคคลที่ประกอบไปด้วยข้อมูลดังต่อไปนี้

---

[10] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล, (กรุงเทพมหานคร : สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, 2546), หน้า 24-25.

[11] ศิริกุล ภู่พันธ์, “ข้อความคิดว่าด้วย ข้อมูลข่าวสารส่วนบุคคล ”, (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2548, หน้า 83.

[12] "sensitive personal data" means personal data consisting of information as to-

(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

1. เชื้อชาติ หรือการเป็นชนกลุ่มน้อยของเจ้าของข้อมูล
2. ความคิดเห็นทางการเมืองของบุคคล
3. ความเชื่อทางศาสนาหรือลัทธิ
4. การเป็นสมาชิกสหภาพแรงงาน
5. สภาพทางการ หรือสภาพทางจิตของบุคคล
6. ชีวิตทางเพศสัมพันธ์
7. การฟ้องร้องของบุคคลที่กระทำหรือถูกกล่าวหาว่ากระทำ
8. การให้การแก้ที่กระทำหรือที่ถูกกล่าวหาว่ากระทำโดยบุคคล การถอนฟ้อง หรือคำพิพากษาของศาล

โดยที่ Reymond Wacks ได้แบ่งระดับข้อมูลส่วนบุคคลที่อ่อนไหวไว้ 3 ระดับ ในหนังสือ Personal Information : Privacy and The Law โดยจะพิจารณาจากผลกระทบต่อเจ้าของข้อมูลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้น ดังนี้[13]

1) ข้อมูลที่มีความอ่อนไหวระดับสูง (High Sensitivity) ข้อมูลประเภทนี้ได้แก่ ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับประวัติทางการแพทย์ ผลการตรวจเลือด ผลการตรวจสุขภาพ ผลการทดสอบทางจิตวิทยา พฤติกรรมทางเพศ ประวัติอาชญากรรม หรือข้อเท็จจริงในชีวิตประจำวันที่ถือเป็นเรื่องลับเฉพาะ เป็นต้น

2) ข้อมูลที่มีความอ่อนไหวระดับปานกลาง (Moderate Sensitivity) ข้อมูลประเภทนี้ มีความเสี่ยงในแง่ที่อาจจะทำให้บุคคลอื่นนำไปใช้ในทางที่ผิดได้ เช่น รายได้ ทรัพย์สิน หนี้สิน เชื้อชาติ ข้อพิพาทของสามีภรรยา ประวัติการหย่าร้าง พินัยกรรม การชำระภาษี กรมธรรม์ประกันชีวิต ประวัติการใช้ยา ข้อมูลที่เกี่ยวกับความคิดเห็นของบุคคล ข้อมูลที่เกี่ยวกับพฤติกรรมส่วนตัว เป็นต้น

3) ข้อมูลที่มีความอ่อนไหวระดับต่ำ (Low Sensitivity) ข้อมูลประเภทนี้เป็นข้อมูลที่เกี่ยวข้องกับบุคคลที่สามารถทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูง เช่น

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labor Relations (Consolidation) Act 1992,

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

[13] Reymond Wacks, Personal Information : Privacy and The Law. (London : Oxford, 1993.), p229-238.

สถานภาพการแต่งงาน ประวัติการทำงาน การถือหุ้น การถือครองที่ดิน สวัสดิการ การใช้อุปกรณ์ทางการแพทย์ เป็นต้น

นอกจากการแบ่งประเภทข้อมูลส่วนบุคคลออกเป็นส องประเภท คือ ข้อมูลส่วนบุคคลทั่วไป หรือ Non – Sensitive Data และข้อมูลส่วนบุคคลที่อ่อนไหว หรือ Sensitive Data ดังกล่าวข้างต้นแล้ว ข้อมูลส่วนบุคคลยังสามารถแบ่งออกโดยลักษณะทางกายภาพของข้อมูลนั้นได้อีก กล่าวคือ สามารถแบ่งเป็น ข้อมูลที่สามารถมองเห็นได้ (Visibly collected Data) และข้อมูลที่ไม่สามรถมองเห็นได้ (Invisibly collected Data) โดยที่ข้อมูลที่สามารถมองเห็นได้นั้น หมายถึง ข้อมูลที่ลูกค้าหรือผู้ใช้บริการเป็นผู้กรอกข้อมูลต่างๆ ด้วยตนเองลงในหน้าเว็บเพจของผู้ให้บริการ เช่น ชื่อ อายุ เพศ การประกอบอาชีพ ที่อยู่ ไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น และสำหรับข้อมูลที่ไม่สามารถมองเป็นได้นั้น หมายถึง ข้อมูลต่างๆ ที่ผู้ประกอบการได้รับจากได้รับจากการใช้คุกกี้[14] โดยที่ผู้ใช้บริการไม่ได้ให้ความยินยอมและไม่อาจรู้ได้ว่าข้อมูลของตนได้ถูกเก็บรวบรวมไว้แล้ว เช่น ข้อมูลวัน เวลา จำนวนครั้ง ของการเข้าเยี่ยมชมเว็บไซต์ เป็นต้น[15]

2.2 การให้ความคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

2.2.1 ความหมายและความจำเป็นของการให้คุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

การให้ความคุ้มครองข้อมูลส่วนบุคคล ก็คือ การดำเนินการใดๆ ก็ตา มกับข้อมูลส่วนบุคคลที่ได้รับมาจากลูกค้าหรือผู้ใช้บริการ ให้มีความปลอดภัยจากการ ใช้ เก็บรักษา รวบรวม การส่ง การโอน หรือการดำเนินการใดๆ ก็ตามเกี่ยวกับข้อมูลส่วนบุคคล ทั้งนี้เพื่อเป็นการสร้างหลักประกันในเรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคลให้แก่ผู้บริโภค

การทำธุรกิจในโลกปัจจุบันนั้นมีการเปลี่ยนแปลงไปอย่างมากโดยเฉพาะมีการนำเทคโนโลยีเข้ามาช่วยในการประกอบกิจการ โดยเฉพาะเทคโนโลยีสื่อสารผ่านอินเทอร์เน็ต ซึ่งมี

---

[14] คุกกี้ในที่นี้คือแฟ้มข้อมูลที่เว็บไซต์ส่งมาที่โปรแกรมค้นผ่าน (Browser) เมื่อผู้ใช้บริการเว็บไซต์เข้าเยี่ยมชมเว็บไซต์นั้นๆ โดยโปรแกรมค้นผ่านของผู้ใช้บริการจะเก็ บคุกกี้ไว้ที่ Hard Drive และทุกครั้งที่ผู้ใช้บริการกลับเข้าไปเยี่ยมชมเว็บไซต์เดิมคุกกี้ของเว็บไซต์ดังกล่าวก็จะถูกส่งกลับไปยังเว็บไซต์นั้นโดยโปรแกรมค้นผ่านของผู้ใช้บริการเองโดยอัตโนมัติ การที่เว็บไซต์ต่างๆ มีการติดตั้งคุกกี้ก็เนื่องจากคุกกี้ช่วยให้เว็บไซต์จ ดจำผู้ใช้บริการได้ว่าผู้ใช้บริการเคยเข้ามาเยี่ยมชมเว็บไซต์นี้หรือเปล่า นอกจากนี้คุกกี้ยังสามารถบันทึกข้อมูลเกี่ยวกับการเยี่ยมชมส่วนต่างๆ บนเว็บไซต์ของผู้ใช้บริการเอาไว้ด้วย

[15] Aunya Singsangob, “Consumer Online Privacy : Right of Individuals in the E-Business Environment”, p. 3.

บทบาทอย่างมากในการช่วยเพิ่มประสิทธิภาพในการแลกเปลี่ยนสินค้า บริการ และข้อมูลข่าวสารได้อย่างรวดเร็ว ครอบค ลุมทุกมุมโลกตลอดเวลา อีกทั้งสามารถช่วยลดต้นทุนในการดำเนินกิจการของผู้ประกอบการได้มาก แต่เนื่องจากการพัฒนาเทคโนโลยีในการติดต่อสื่อสารนั้นมีอยู่ต่อเนื่อง แต่กฎหมายหรือกฎเกณฑ์ที่มีอยู่นั้นไม่อาจที่จะรองรับต่อการพัฒนาของเทคโนโลยีได้อย่างสมบูรณ์ ดังนั้น เมื่อมี การนำเทคโนโลยีเข้ามาใช้ในการทำธุรกิจ ก็จำเป็นที่จะต้องมีกฎเกณฑ์หรือกฎหมายที่เกี่ยวข้องมารองรับการนำเทคโนโลยีมาใช้

เนื่องด้วยปัจจุบัน การสมัครขอรับบริการต่างๆ จากผู้ประกอบการหลายๆ ประเภทนั้น ผู้สมัครรับบริการจะต้องมีการให้ข้อมูลส่วนบุคคลของตน เช่น ชื่อ ที่อ ยู่ เบอร์โทรศัพท์ ที่อยู่อิเล็กทรอนิกส์ อายุ สถานที่ทำงาน อัตราเงินเดือน เป็นต้น เพื่อใช้ประกอบในการพิจารณาให้บริการ ซึ่งโดยส่วนมากในการประกอบธุรกิจประเภทต่างๆ มักจะมีการนำข้อมูลส่วนบุคคลบางประเภทที่เกี่ยวกับการพิจารณาสภาพคล่องทางการเงิน ไปใช้ประโยชน์ในการบริหารจัดการกิจการของผู้ประกอบการ ซึ่งข้อมูลดังกล่าวมีความจำเป็นที่จะต้องเก็บรวบรวมเพื่อให้ธุรกิจสามารถดำเนินได้ต่อไป อาทิเช่น หมายเลขบัตรเครดิต หมายเลขบัญชีธนาคาร เป็นต้น

นอกจากนี้ข้อมูลส่วนบุคคลยังมีมูลค่าทางเศรษฐกิจ กล่าวคือ ข้อมูลส่วนบุคคลสามารถนำใช้ในการทำแผนการตลาด กำหนดกลยุทธ์ โดยการนำฐานลูกค้าของผู้ประกอบการรายหนึ่งไปใช้เป็นฐานลูกค้าของผู้ประกอบการอีกรายหนึ่งซึ่งเป็นการขยายฐานลูกค้าให้แก่ผู้ประกอบการที่ได้รับฐานข้อมูลไป อันเป็นการก่อให้เกิดประโยชน์ในทางเศรษฐกิจได้อย่างมากมาย ดังนั้น ข้อมูลส่วนบุคคลจึงมีความสำคัญ และจำเป็นที่จะต้องได้รับการคุ้มครองเพื่อทำให้ผู้บริโภคเกิดความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์

2.2.2 รูปแบบและวิธีการให้คุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์

เพื่อรองรับกระแสการพัฒนาและการเปลี่ยนแปลง เทคโนโลยีในการติดต่อสื่อ สาร และเพื่อป้องกันมิให้เกิดการละเมิดข้อมูลส่วนบุคคลหรือนำข้อมูลส่วนบุคคลไปใช้โดยมิชอบ หลายประเทศจึงได้ให้ความสำคัญกับการกำหนดรูปแบบและวิธีการในการให้ความคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งการกำหนดรูปแบบการคุ้มครองข้อมูลส่วนบุคคลจะขึ้นอยู่กับระบบกฎหมาย รูปแบบการปกครอง นโยบายรัฐ ความก้าวหน้าทางเทคโนโลยี รวมทั้งสภาพสังคม วัฒนธรรม และพฤติการณ์แวดล้อมต่างๆ ของประเทศนั้นๆ โดยทั่วไปแล้ว รูปแบบและวิธีการในการให้ความคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ จะสามารถแบ่งออกได้ 4 วิธี[16]หลักๆ ดังต่อไปนี้

---

[16] *เพิ่งอ้าง*, p. 5.

2.2.2.1 การบัญญัติกฎหมายที่ให้ความคุ้มครองเป็นการทั่วไป

สำหรับแนวทางการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยวิธีการบัญญัติกฎหมายเป็นการทั่วไป (Comprehensive Law) นั้น เป็นการที่รัฐได้ออกกฎหมายหลักที่มีลักษณะทั่วไป ที่ครอบคลุมกรณีการคุ้มครองข้ อมูลข่าวสารในลักษณะต่างๆ โดยที่การตรากฎหมายในลักษณะนี้มักจะมีการจัดตั้งองค์กรกลางที่ทำหน้าที่ดูแลวินิจฉัยกรณีปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคลที่เกิดขึ้นโดยเฉพาะ ในลักษณะของคณะกรรมการ โดยที่องค์กรที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะมีหน้าที่ดำเนินการในสองลักษณะคือ[17]

1) องค์กรที่ทำหน้าที่กำกับดูแล (Regulatory)

โดยที่องค์กรดังกล่าวจะมีหน้าที่ค่อนข้างกว้างในการกำกับดูแลการประมวลข้อมูลภายในประเทศ อาทิเช่น อำนาจในการอนุญาตหรือไม่อนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลทั้งโดยหน่วยงานภาครัฐ และหน่วยงานภาคเอกชน การดำเนินการทางทะเบียน การวินิจฉัยข้อร้องเรียน รวมทั้ง การ ประชาสัมพันธ์ให้ประชาชนทราบถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งประเทศที่มีองค์กรกำกับดูแลก็เช่น ประเทศฝรั่งเศสที่มี Commission Nationale Informatique Liberte's (CNIL) หรือ ประเทศสวีเดนที่มี Data Inspection Board and National Commission on Informatics and Liberties เป็นต้น

2) องค์กรที่ทำหน้าที่ให้คำปรึกษา (Advisory)

โดยองค์กรดังกล่าวจะมีหน้าที่ในการให้คำปรึกษา และให้ความช่วยเหลือหน่วยงานต่างๆ ในกิจกรรมต่างๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล โดยองค์กรดังกล่าวมีอำนาจที่จะยื่นข้อร้องเรียนไปยังกระทร วง หรือหน่วยงานของรัฐที่รับผิดชอบเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลนั้นๆ ได้ด้วย แต่ทั้งนี้องค์กรดังกล่าวจะไม่มีอำนาจในการออกคำสั่งให้บุคคลหรือหน่วยงานกระทำการ หรืองดเว้นกระทำการใดๆ ได้ ซึ่งประเทศที่มีองค์กรที่ทำหน้าที่ให้คำปรึกษาในลักษณะนี้ได้แก่ ประเทศเ ยอรมัน ซึ่งได้มีการจัดตั้งกรรมการคุ้มครองข้อมูลส่วนบุคคล (Federal Data Protection Commissioner) ซึ่งอยู่ภายใต้สังกัดกระทรวงมหาดไทย เป็นต้น

2.2.2.2 การบัญญัติกฎหมายที่ให้ความคุ้มครองเป็นการเฉพาะ

สำหรับแนวทางการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยวิธีการบัญญั ติกฎหมายที่ให้การคุ้มครองเป็นการเฉพาะ เป็นการที่รัฐได้ออกกฎหมายเพื่อแก้ปัญหาที่เกิดขึ้นเฉพาะหน้า เพื่อแก้ปัญหาและเยียวยาปัญหาที่เกิดขึ้นในปัจจุบัน ซึ่งหากจะรอให้มีการบัญญัติกฎหมายที่มีลักษณะทั่วไปอาจจะไม่ทันต่อเหตุการณ์

โดยที่ประเทศที่สามารถนำมายกเป็นตัว อย่างของการออกกฎหมายที่ให้ความคุ้มครองเป็นการเฉพาะนั้น เช่น กฎหมายของประเทศสหรัฐอเมริกา ทั้งนี้ แม้ว่าประเทศสหรัฐอเมริกาจะมีกฎหมายคุ้มครองสิทธิส่วนบุคคล หรือ Privacy Act 1974 ซึ่งเป็นกฎหมาย

---

[17] ปฏิวัติ อุ่นเรือน, "ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ", หน้า 16-17.

หลักที่ให้ความคุ้มครองสิทธิส่วนบุคคลเป็นการทั่วไปอยู่แล้วก็ตาม แต่เ นื่องจากการพัฒนาทางเทคโนโลยี ร่วมทั้งสภาพแวดล้อมทางสังคมที่เปลี่ยนแปลงไป จึงมีความจำเป็นต้องออกกฎหมายเฉพาะหรือกฎหมายพิเศษมาเพื่อรองรับ เช่น การตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับข้อมูลทางการเงิน หรือ Gamm-Leach Bliley Financial Modernization Act 1970 ซึ่งเป็นกฎหมายที่ใช้บังคับเพื่อควบคุมการใช้ข้อมูลเครดิตของภาคธุรกิจ โดยการกำหนดหลักเกณฑ์ที่สำคัญ อาทิเช่น เรื่องผู้มีสิทธิที่จะใช้ข้อมูลเครดิต การจำกัดการเปิดเผยข้อมูลเครดิต ตลอดจนการให้สิทธิแก่ผู้บริโภคในการเข้าถึงหรือแก้ไขข้อมูลเครดิตของตนให้ถูกต้อง กฎหมาย Children's On line Privacy Protection Act 1998 ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์ห้ามไม่ให้ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ และบริการออนไลน์ต่างๆ ทำการเก็บรวบรวมข้อมูลจากผู้เยี่ยมชมเว็ปไซต์หรือผู้ใช้บริการที่เป็นเด็กอายุต่ำกว่า 13 ปี เว้นแต่ผู้ประกอบก ารจะได้ใช้กลไกการกำกับดูแลตนเอง ซึ่งได้ผ่านการเห็นชอบจากคณะกรรมาธิการการค้า หรือ FTC กฎหมาย Financial Modernization Act 1999 ซึ่งได้ตราขึ้นเพื่อให้สถาบันการเงินต่างๆ เพิ่มระดับความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคในกิจกรรมที่เกี่ยวข้องทางการเงินเพิ่มมากขึ้ น อาทิเช่น การประกาศนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้ลูกค้าหรือผู้ใช้บริการทราบและหน้าที่ในการปฏิบัติตามข้อเรียกร้องของผู้บริโภคที่เกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น ดังนี้ แม้ว่าประเทศสหรัฐอเมริกาจะมีกฎหมายเฉพาะอย่างชัดเจน แต่โดยนโยบายในการกำหนดกฎหมายที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวัตถุประสงค์เพื่อให้เกิดการควบคุมตนเอง โดยการให้ภาคเอกชนกำหนดกลไกการกำกับดูแลตนเอง หรือ Self-Regulation ขึ้น โดยรัฐจะอาศัยกฎหมายในการควบคุมเท่านั้น ทั้งนี้ การให้ภาคเอกชนกำกับดูแลตนเองนั้นมีข้อดีคือมีความ ยืดหยุ่นในการแก้ปัญหาให้ทันท่วงที สอดคล้องกับเหตุการณ์ และความเปลี่ยนแปลงทางด้านเทคโนโลยีด้วย

รูปแบบของการตรากฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกันนี้ มีเหตุผลที่สามารถวิเคราะห์ได้ว่ามีที่มาจาก แนวความคิดในนิติวิธีที่แตกต่างกัน โดยประเทศที่ใช้การต รากฎหมายที่มีลักษณะเป็นการคุ้มครองเป็นการทั่วไปนั้น คือว่ากฎหมายทั่วไปย่อมสามารถคุ้มครองหรือปกป้องสิทธิและเสรีภาพของประชาชนได้ดีกว่า ในขณะที่ประเทศที่ตรากฎหมายที่ให้การคุ้มครองเป็นการเฉพาะนั้น มีความคิดว่ากฎหมายเฉพาะย่อมทันต่อเหตุการณ์ความเปลี่ยนแปลงมากกว่า และมีความยืดหยุ่นกว่าซึ่งสอดคล้องกับสภาพเศรษฐกิจ สังคม การเมืองและการพัฒนาทางเทคโนโลยีต่างๆ อย่างไรก็ตาม เนื่องจากภายหลังที่องค์กรเพื่อเศรษฐกิจและพัฒนา หรือ OECD ได้กำหนดแนวทางปฏิบัติในการคุ้มครองความเป็นอยู่ส่วนตัว และการโอนข้อมูลส่วนบุคคลระหว่างประเทศ ในปี 1980 (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data) ประเทศต่างๆ ในภาคพื้นยุโรปจึงได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับแนวทางที่ OECD กำหนด และเป็นไปในแนวทางเดียวกันกับประเทศสมาชิกอื่นๆ โดยที่ สำหรับรูปแบบของการตรากฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยนั้น ผู้เขียนเห็นว่าน่าจะเหมาะสมกับการตรากฎหมาย

ที่มีลักษณะทั่วไปมากกว่า เนื่องจากประเทศไทยเป็นประเทศที่ใช้กฎหมายในระบบ Civil Law ซึ่งการตีความกฎหมายจะใช้การตีความตามเจตนารมณ์ และจะก่อให้เกิ ดเอกภาพและประสิทธิภาพในการบังคับใช้ได้มากกว่า

2.2.2.3 กลไกการกำกับดูแลตนเอง (Self – Regulation)

กลไกการกำกับดูแลตนเอง หรือ Self – Regulation ถือเป็นรูปแบบและวิธีการให้คุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ ที่สามารถช่วยผ่อนคลายความเคร่งครัด หรือความเข้มงวดของกฎเกณฑ์หรือกฎหมายที่ออกโดยรัฐได้ เนื่องจากผู้ประกอบการสามารถที่จะวางหลักเกณฑ์ในทางปฏิบัติสอดคล้องกับการดำเนินงานภายในองค์กรของตนเองมากที่สุด และเป็นการประหยัดต้นทุนในการผลิตหรือการให้บริการที่เกิดขึ้นอันเนื่องมาจากการเปลี่ยนแปลงกฎเกณฑ์หรือกฎ หมายที่ออกโดยรัฐได้ด้วย ทั้งนี้ เพื่อให้การประกอบธุรกิจของผู้ประกอบการเป็นไปอย่างราบรื่น และส่งผลกระทบในทางธุรกิจกับผู้ประกอบการน้อยที่สุด โดยไม่ถือว่าปฏิบัติผิดกฎเกณฑ์หรือกฎหมายที่ออกโดยรัฐ ซึ่งการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) หรือการจัดทำประมวลจริยธรรม ก็เป็นรูปแบบตามแนวทาง การกำกับดูแลตนเองที่ผู้ประกอบการสามารถกำหนดขึ้นได้ เนื่องจาก นโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ประกาศให้แก่ลูกค้าหรือผู้ใช้บริการของตนทราบว่า ผู้ประกอบการมีนโยบาย หรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลอย่างไร เพื่อให้ลูกค้าหรือผู้ใช้บริการทราบและสามารถใช้พิจารณาตัดสินใจได้ว่าตนจะให้ข้อมูลส่วนบุคคลของตนหรือไม่

อย่างไรก็ตาม เนื่องจากการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการไม่ได้ถูกควบคุมโดยกฎหมายหรื อองค์กรใดๆ จึงอาจทำให้การกำหนดนโยบายของผู้ประกอบการต่างๆ ไม่ได้มาตรฐานและไม่อาจคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริง และเนื่องจาก นโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ได้จัดทำขึ้นเอง โดยมีวัตถุ ประสงค์เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบถึงนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของตน ดังนั้น เพื่อเป็นการสร้างความน่าเชื่อถือต่อลูกค้าหรือผู้ใช้บริการ ผู้ประกอบการจึงอาจกำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ดูน่าเชื่อถือ โดยไม่ได้คำนึงว่ าตนจะปฏิบัติได้ตามที่ตนได้ประกาศไว้จริงหรือไม่เพียงใด ซึ่งอาจก่อให้เกิดปัญหาในทางปฏิบัติมากมาย อีกทั้งการตีความว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลมีสถานะทางกฎหมายอย่างไร ก็ถือเป็นเรื่องสำคัญ เพราะในกรณีที่ผู้ประกอบการไม่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ตามน โยบายที่ตนประกาศไว้นั้น ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้เสียหายจะสามารถฟ้องร้องหรือดำเนินการทางกฎหมายอย่างไรต่อผู้ประกอบการได้ และกฎหมายที่มีผลบังคับใช้อยู่จะเพียงพอหรือไม่ที่จะดำเนินการเอาผิดกับผู้ประกอบการนั้นๆ นอกจากนี้ ในกรณีที่ผู้ประกอบการได้กำหนดนโย บายการคุ้มครองข้อมูลส่วนบุคคลของตนไว้ แต่ได้มีการกำหนดข้อยกเว้นหรือข้อจำกัดความรับผิดของ

ตนไว้ด้วยนั้น จะถือได้หรือไม่ว่าลูกค้าหรือผู้ใช้บริการได้ยอมรับด้วยกับข้อยกเว้นหรือข้อจำกัดความรับผิดนั้น และจะถือว่าเป็นธรรมต่อลูกค้าหรือผู้ประกอบการซึ่งเป็นผู้บริโภคหรือไม่

สำหรับการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ. .... นั้น ในหมวดที่ 2 ว่าด้วยจริยธรรมในการคุ้มครองข้อมูลส่วนบุคคล กำหนดว่า “...บุคคลหรือหน่วยงานอาจจัดทำประมวลจริยธรรมเพื่อกำหนดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลก็ได้...” จากบทบัญญัติดังกล่าวจะเป็นได้ว่า กฎหมายไม่ได้บังคับให้ผู้ประกอบการต้องจัดทำประมวลจริยธรรม เพียงแต่ผู้ประกอบการจะจัดทำหรือไม่ขึ้นอยู่การให้ความสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการของผู้ประกอบการเอง และขึ้นอยู่ กับนโยบายในการบริหารกิจการของผู้ประกอบการด้วย อย่างไรก็ตาม แม้ว่าร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ. .... จะไม่ได้บังคับให้ผู้ประกอบการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลก็ตาม แต่เนื่องจากกิจการบางประเภทกิจการ เช่น ธนาคาร ผู้ประกอบก ารบัตรเครดิตและ /หรือสินเชื่อส่วนบุคคล เป็นต้น ซึ่งเป็นกิจการขนาดใหญ่ และกระทบต่อผู้บริโภคจำนวนมาก จะมีความเกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลของผู้ใช้บริการ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลที่มีลักษณะทั่วไป และ /หรือข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว เพราะการสมัคร เข้ารับบริการ หรือการทำธุรกรรมกับผู้ประกอบการรายนั้นๆ ผู้ใช้บริการจะต้องให้ข้อมูลส่วนบุคคลของตนแก่ผู้ประกอบการนั้นๆ เพื่อใช้ประกอบในการสมัครเข้ารับบริการหรือทำธุรกรรมกับผู้ประกอบการรายนั้นๆ ดังนั้น ผู้ประกอบการก็ควรจะต้องมีการกำหนดนโยบายการคุ้มครองข้อมูลส่ วนบุคคลที่มีมาตรฐานในระดับสูงด้วย ทั้งนี้ เพื่อสร้างความน่าเชื่อถือให้เกิดขึ้นต่อผู้ใช้บริการ และสร้างภาพลักษณ์ที่ดีต่อภาพรวมของเศรษฐกิจด้วย

สำหรับประโยชน์ที่ผู้ประกอบธุรกิจจะได้รับจากการจัดให้มีกลไกการกำกับดูแลตนเองโดยการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุ คคลนั้น เนื่องด้วยนโยบายการคุ้มครองข้อมูลส่วนบุคคลนั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ได้จัดทำขึ้นเอง โดยมีวัตถุประสงค์เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบถึงนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของตน ดังนั้น การที่ผู้ประกอบธุ รกิจจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์ของตนก็ย่อมแสดงให้เห็นว่า ผู้ประกอบธุรกิจให้ความสำคัญกับการให้ความคุ้มครองข้อมูลส่วนบุคคล อันเป็นการสร้างความเชื่อมั่นให้แก่ลูกค้าหรือผู้ใช้บริการที่เข้าไปใช้บริการในเว็บไซต์ของผู้ประกอบการนั้นเอง

2.2.2.4 การพัฒนาเทคโนโลยี

การพัฒนาเทคโนโลยีก็เป็นอีกวิธีการหนึ่งหรือแนวทางหนึ่งที่สามารถช่วยคุ้มครองข้อมูลส่วนบุคคลได้ โดยการปกป้องหรือป้องกันข้อมูลส่วนบุคคลไม่ให้ถูกคุกคามหรือล่วงละเมิด หรือถูกนำไปใช้ในทางที่มิชอบ หรือใช้ป้องกันการเจาะเข้าระบบเพื่อนำข้อมูลส่วนบุคคลไปใช้หาประโยชน์ในทางมิชอบได้ โดยตัวอย่างของการพัฒนาเทคโนโลยีที่ช่วยคุ้มครองข้อมูลส่วนบุคคล เช่น

1. เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) ในการสร้างลายมือชื่อดิจิทัล โดยที่เทคโนโลยีดังกล่าวมีความสามารถดังนี้

- สามารถใช้ในกา ระบุและตรวจสอบตัวบุคคล (Identification /Authentication)
- สามารถใช้ในการเข้ารหัสลับ (Encryption) เพื่อรักษาความลับของข้อความในรูปข้อมูลอิเล็กทรอนิกส์

โดยพื้นฐานของเทคโนโลยี PKI ในการสร้างลายมือชื่ออิเล็กทรอนิกส์ จะทำการการสร้างกุญแจคู่ (key pair) อันประกอบด้วย กุญแจส่วนตัว (private key) และกุญแจสาธารณะ (public key) ซึ่งมีลักษณะเป็นอักษร อักขระ ตัวเลข หรือสัญลักษณ์ที่ไม่สามารถเข้าใจความหมายได้โดยกุญแจส่วนตัวของเจ้าของลายมือชื่อจะทำหน้าที่ เป็นข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์ (ลายมือชื่อดิจิทัล) ที่เจ้าของลายมือชื่อต้องเก็บรักษาไว้เป็นความลับ และกุญแจสาธารณะของเจ้าของลายมือชื่อจะทำหน้าที่ใช้ในการตรวจสอบลายมือชื่อดิจิทัล โดยในขั้นตอนการตรวจสอบลายมือชื่อดิจิทัล เทคโนโลยี PKI จะทำการตรวจสอบลายมือชื่อ และหากพบว่ามีการเปลี่ยนแปลงใดๆ เกิดขึ้นกับลายมือชื่อ และข้อความที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ เทคโนโลยี PKI ก็จะสามารถตรวจพบได้[18]

2. เทคโนโลยี Chip Card บนบัตรเครดิต หรือบัตร Smart Card เป็นเทคโนโลยีที่พัฒนาขึ้นจากระบบแถบแม่เหล็ก ซึ่งจะเป็นบัตรที่มี IC (Intregrated Circuit) เพื่อใช้ในการเก็บข้อมูลและประมวลผลข้อมูล และมีระดับความปลอดภัยสูงในการอ่าน เขียน อัพเดตข้อมูล โดย Chip นี้มีโครงสร้างและหลักการทำงานเหมือนคอมพิวเตอร์ขนาดเล็กที่ประกอบไปด้วย CPU ที่ทำหน้าที่ประมวลผล RAM ทำหน้าที่เก็บข้อมูลระหว่างการทำงาน ROM บรรจุระบบจัดการ (OS) และโปรแกรมพื้นฐาน EEPRAM ซึ่งทำหน้าที่บรรจุข้อมูลส่วนตัว และโปรแกรมต่างๆ ซึ่งสามารถเพิ่มฟังก์ชันการใช้งานได้ภายหลัง เทคโนโลยี Chip Card เป็นเทคโนโลยีที่พัฒนาขึ้นเพื่อใช้ป้องกันการทุจริต (fraud) บัตรเครดิตได้ ซึ่งมีความปลอดภัยสูง โดย Chip Card จะทำหน้าที่เป็นรหัสลับส่วนบุคคล ซึ่งมี หน่วยความจำบนบัตร ซึ่งสามารถนำไปใช้ในการพิสูจน์ยืนยันตัวบุคคล หรือประชาชนผู้ถือบัตรได้ จึงทำให้ผู้ใช้บัตรเครดิตเกิดความเชื่อมั่นในการใช้บัตรเครดิตเพิ่มมากขึ้น[19]

3. เทคโนโลยี Secure Socket Layer (SSL) เป็นเทคโนโลยีที่ใช้แปลงรหัสเมื่อมีการส่งข้อมูลผ่านเครือข่ายการสื่อสารและทำการเข้ารหัสเพื่อรักษาความปลอดภัย เมื่อ

---

[18] สุรางคณา วายุภาพ , สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ศูนย์เทคโนโลยีอิเล็กทรอนิกส์ และคอมพิวเตอร์แห่งชาติ , “สัมมนากฎหมายธุรกรรมทางอิเล็กทรอนิกส์ บริหารข้อมูลอย่างไร ให้ปลอดภัยและถูกกฎหมาย”

[19] บัตรประชน “สมาร์ทการ์ด” เปลี่ยนวิถีคนไทยสู่ไฮเทค <http://www.banprucity.go.th /smartcards/smartcard.html>

มีการใช้งานบนเว็บไซต์ โดย SSL จะทำการเข้าและแปลงรหัสข้อมูล คือ สลับที่ข้อมูลและแปลงเป็นรหัสตัวเลขทั้งหมด ซึ่งจะสามารถสร้างมั่นใจได้ว่าข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการจะส่งผ่านไปถึงผู้ประกอบก ารหรือผู้ให้บริการได้อย่างปลอดภัย โดยระบบ SSL จะทำการเข้ารหัสที่ระดับความละเอียด 128 บิท (128-bit encryption) ซึ่งเป็นระดับที่มีความละเอียดสูง เพราะหากระดับความละเอียดของการเข้ารหัสสูง ระดับความปลอดภัยก็จะสูงตาม[20]

4. เทคโนโลยี Firewall ซึ่งเป็นเทคโนโลยีที่ทำหน้าที่ ควบคุมดูแลการเข้าและการออกของข้อมูล โดยสามารถเปรียบได้กับทหารรักษาความปลอดภัยหน้าประตู ที่ไม่เปิดรับคนแปลกหน้า เข้า-ออกจากระบบ เพื่อป้องกันการถูกโจรกรรมข้อมูลจากผู้บุกรุก

5. โปรแกรมตรวจจับการบุกรุกและสิ่งผิดปกติ (Intrusion Detection Software) โดยโปรแกรมดังกล่าวจะทำหน้าที่ตรวจสอบและแจ้งข้อความเตือนทันทีที่มีความผิดปกติเกิดขึ้นในระบบ

6. โปรแกรม Automatic Sign off ซึ่งทำหน้าที่ ควบคุมระยะเวลาการเปิดหน้าจอคอมพิวเตอร์ โดยระบบจะทำการออกจากระบบทันที่ จากทำการ Sign off แทนลูกค้าหรือผู้บริการโดยอัตโนมัติ หากลูกค้าหรือผู้ใช้บริการเปิดหน้าจอทิ้งไว้ โดยไม่พิมพ์หรือทำรายการใดๆ บนหน้าจอ ฟังก์ชั่นพิเศษนี้มีไว้เพื่อป้องกันมิให้ผู้อื่นเข้ามาทำรายการในบัญชีของลูกค้าหรือผู้ใช้บริการโดยไม่ได้รับอนุญาต

---

[20] Bualuang i Banking มาตรฐานความปลอดภัยระดับสากล <http://www.bangkokbank.com/Online+Banking+Thai/For+Personal/iBanking/Security/Security+Features.htm>

บทที่ 3

แนวทางการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ในต่างประเทศ

3.1 แนวทางปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ขององค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา หรือ Organization for Economic Cooperation and Development (OECD)

OECD หรือ Organization for Economic Cooperation and Development หรือ องค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา เป็นองค์กรที่เกิดจากความร่วมมือระหว่างประเทศ ที่ให้ความสำคัญกับปัญหาการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ โดย OECD ได้กำหนดกฎเกณฑ์ขั้นพื้นฐาน (Guidelines) ในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้นานาประเทศได้มีแนวทางในการบัญญัติกฎหมายของตนเอง โดยที่ OECD ได้ออกกฎเกณฑ์เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่มีความสำคัญ คือ Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data ในปี 1980 ซึ่ง Guidelines ฉบับนี้ได้กลายเป็นที่ยอมรับกันโดยทั่วไปว่าเป็นหลักเกณฑ์พื้นฐานที่ประชาคมโลกต่างยอมรับ และบัญญัติเป็นกฎหมายภายในของตน และต่อมาในปี 1999 ก็ได้ออก Guidelines for Consumer Protection in the context of Electronic Commerce 1999 หรือ แนวทางปฏิบัติสำหรับการคุ้มครองผู้บริโภคบนพาณิชย์อิเล็กทรอนิกส์ เพื่อคุ้มครองผู้บริโภคในการทำธุรกรรมทางอิเล็กทรอนิกส์ และเป็นการสร้างกฎเกณฑ์ให้ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ต้องปฏิบัติตามมาตรฐานขั้นต่ำเกี่ยวกับกา รให้ความคุ้มครองผู้บริโภคตามที่กำหนดใน Guidelines ด้วย

3.1.1 OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data 1980

โดยหลักการคุ้มครองข้อมูลส่วนบุคคลจะมีหลักการซึ่งเป็นสาระสำคัญด้วยกันทั้งสิ้น 8 ประการด้วยกันดังต่อไปนี้[1]

---

[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่ อสาร ร่วมกับ สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ , การโอนข้อมูลส่วนบุคคลระหว่างประเทศ , (กรุงเทพมหานคร : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิ วเตอร์แห่งชาติ สำนักงาน

1. หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)

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

2. หลักคุณภาพของข้อมูล (Data Quality Principle)

ผู้ประกอบการจะต้องใช้ข้อมูลส่วนบุคคลภายในขอบวัตถุประสงค์ในการจัดเก็บหรืออาจใช้เพื่อวัตถุประสงค์อื่นได้ตามความจำเป็น โดยข้อมูลดังกล่าวจะต้องเป็นข้อมูลที่มีความถูกต้อง และเป็นปัจจุบัน (up-to-date)

3. หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)

ผู้ประกอบการจะต้องแจ้งวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลได้ทราบก่อนการรวบรวมข้อมูล อีกทั้งจะต้องใช้ข้อมูลส่ วนบุคคลภายในวัตถุประสงค์ดังกล่าวด้วย

4. หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)

ผู้ประกอบการจะต้องไม่เปิดเผย (disclose) ทำให้แพร่หลาย (made available) หรือใช้เพื่อวัตถุประสงค์อื่นใดนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบก่อนหน้านั้น เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลหรือมีกฎหมายบัญญัติเป็นอย่างอื่น

5. หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)

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

6. หลักการเปิดเผย (Openness Principle)

ผู้ประกอบการจะต้องประกาศนโยบายเกี่ยวกับการดำ เนินการใดๆ ต่อข้อมูลส่วนบุคคลให้ทราบโดยทั่วไป วัตถุประสงค์ในการใช้ข้อมูล รายละเอียดเกี่ยวกับผู้ควบคุมข้อมูล (controller) ถิ่นที่อยู่ผู้ควบคุมเป็นต้น

7. หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

ผู้ประกอบการจะต้องกำหนดให้เจ้ าของข้อมูลมีสิทธิในการได้รับการยืนยัน (confirmation) จากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูลมีข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลหรือไม่เพียงใด โดยจะต้องได้รับทราบผลการยืนยันภายในเวลาอันสมควร ทั้งนี้ อาจมีการคิดค่าใช้จ่ายในการดำเนินการได้ในอัตราที่เหมาะสม และในกรณีที่ไม่สามารถดำเนินการตามที่เจ้าของข้อมูลร้องขอข้างต้นก็จะต้องแสดงเหตุผลให้เจ้าของข้อมูลทราบ อีกทั้งบอกกล่าวให้เจ้าของข้อมูล

พัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี , 2548), หน้า 14-16.

ทราบถึงสิทธิในการโต้แย้งการไม่ปฏิบัติตามคำร้องขอดังกล่าว และหากต่อมาปรากฏว่าข้อโต้แย้งของเจ้าของข้อมูลสามารถรับฟังได้ เจ้าของข้ อมูลมีสิทธิที่จะขอให้มีการลบ แก้ไข ปรับปรุง หรือทำให้ข้อมูลมีความสมบูรณ์

8. หลักความรับผิดชอบ (Accountability Principle)

ผู้ประกอบการจะต้องมีหน้าที่ในการปฏิบัติการตามหลักการข้างต้นให้ครบถ้วนทุกประการ

3.1.2 OECD Guidelines for Consumer Protection in the context of Electronic Commerce 1999

OECD Guidelines for Consumer Protection in the context of Electronic Commerce 1999 หรือแนวทางปฏิบัติสำหรับการคุ้มครองผู้บริโภคบนพาณิชย์อิเล็กทรอนิกส์ มีสาระสำคัญที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กท รอนิกส์ ดังต่อไปนี้[2]

1) ขอบเขตการใช้บังคับ

แนวทางนี้ใช้กับพาณิชย์อิเล็กทรอนิกส์สำหรับผู้ประกอบธุรกิจกับผู้บริโภค (business-to-consumer electronic commerce) แต่ไม่รวมถึงพาณิชย์อิเล็กทรอนิกส์ระหว่างผู้ประกอบธุรกิจด้วยกัน (business-to-business electronic commerce)

2) หลักการทั่วไป

- หลักการคุ้มครองผู้บริโภคจะต้องมีความชัดเจนและมีประสิทธิภาพ (Transparent and effective protection) ผู้บริโภคที่เกี่ยวข้องกับพาณิชย์อิเล็กทรอนิกส์ควรได้รับการคุ้มครองที่ไม่น้อยไปกว่าการคุ้มครองผู้บริโภคในกรณีทั่วไป ตามหลักการคุ้มครอ ง ผู้บริโภคที่ชัดเจนและมีประสิทธิภาพ หน่วยงานภาครัฐ (governments) ผู้ประกอบธุรกิจ ผู้บริโภคและผู้เกี่ยวข้องควรประสานงานและร่วมมือกันในการบรรลุหลักการข้างต้น และพิจารณาปรับปรุงหลักการที่จำเป็นให้เหมาะสมสอดคล้องกับพาณิชย์อิเล็กทรอนิกส์

- แนวทางปฏิบัติว่าด้วย การดำเนินธุรกิจ การโฆษณา และวิธีการทางการตลาดที่เป็นธรรม (Fair business, advertising and marketing practices) ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ควรคำนึงถึงผลประโยชน์ของผู้บริโภค และควรปฏิบัติตามแนวทางปฏิบัติว่าด้วยการดำเนินธุรกิจ การโฆษณา และการตลาดที่เป็ นธรรม ผู้ประกอบธุรกิจไม่ควรโฆษณา หรืองดเว้นไม่โฆษณา หรือมีส่วนร่วมในการกระทำการใด ๆ ที่อาจก่อให้เกิดความเข้าใจผิด หรือเป็นการหลอกลวง หรือก่อให้เกิดความไม่เป็นธรรมแก่ผู้บริโภค ผู้ประกอบธุรกิจซึ่ง

---

[2] คำแปลของ OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)
<http://www.ecommerce.or.th/newsletter/sep01/index.html>

โฆษณา ทำกิจกรรมส่งเสริมการขาย หรือขายสินค้าหรือบริการแก่ผู้บริ โภค ควรงดเว้นการกระทำใดๆ ที่อาจเป็นเหตุให้เกิดอันตรายแก่ผู้บริโภค เมื่อมีการให้ข้อมูลเกี่ยวกับผู้ประกอบธุรกิจหรือข้อมูลสินค้าหรือบริการที่เผยแพร่แก่ผู้บริโภค ข้อมูลดังกล่าวต้องมีความถูกต้อง ชัดเจน สามารถเข้าใจได้ง่าย และมีวิธีการที่ผู้บริโภคสามารถตรวจดูข้อมูลได้โดยสะดวก ผู้ประกอบธุรกิจควรปฏิบัติตามนโยบายหรือแนวทางปฏิบัติเกี่ยวกับการดำเนินธุรกิจในเรื่องการทำนิติกรรมสัญญากับผู้บริโภค ผู้ประกอบธุรกิจควรคำนึงถึงลักษณะของพาณิชย์อิเล็กทรอนิกส์ในแต่ละประเทศ และพิจารณาถึงหลักเกณฑ์ทางกฎหมายที่แตกต่างกันของประเทศต่าง ๆ ผู้ประกอบธุรกิจควรหลีกเลี่ยงการใช้ลักษณะพิเศษบางประการของพาณิชย์อิเล็กทรอนิกส์ เพื่อปกปิดสถานประกอบการหรือลักษณะจำเพาะของผู้ประกอบธุรกิจ หรือเพื่อหลีกเลี่ยงการปฏิบัติตามมาตรฐานการคุ้มครองผู้บริโภค และหรือกลไกการคุ้มครอง ผู้บริโภคทั้งหลาย ผู้ประกอบธุรกิจไม่ควรใช้ข้อสัญญาที่ไม่เป็นธรรม (unfair contract terms) การโฆษณาและการตลาดที่สามารถระบุตัวผู้ที่เกี่ยวข้องได้ การโฆษณาและการตลาดควรระบุถึงผู้ประกอบธุรกิจที่เป็นผู้โฆษณาหรือผู้เกี่ยวข้องกับการตลาด ในกรณีที่ไม่สามารถระบุ ตัวบุคคลได้ อาจถือเป็นการหลอกลวง ผู้ประกอบธุรกิจควรสามารถตรวจสอบความถูกต้องของการโฆษณาโดยตรงหรือโดยอ้อม ตลอดเวลาที่มีการเผยแพร่และควรตรวจสอบตามกำหนดเวลาที่เหมาะสม ผู้ประกอบธุรกิจควรกำหนดวิธีการอย่างง่ายและใช้ได้ผล ซึ่งอนุญาตให้ผู้บริโภคสามารถเลือกว่า จะยินดีรับข้อความของไปรษณีย์อิเล็กทรอนิกส์ ที่มีวัตถุประสงค์เพื่อการค้า (unsolicited commercial e-mail) หรือไม่ ในกรณีที่เชื่อได้ว่าผู้บริโภคไม่ต้องการรับไปรษณีย์อิเล็กทรอนิกส์ (ผู้ประกอบธุรกิจ) ก็ควรปฏิบัติตามความประสงค์เช่นว่านั้น การส่งไปรษณีย์อิเล็กทรอนิกส์ถึงผู้บริโภค โดยที่ไม่ได้รับความยินยอม หรือเคยติดต่อกันมาก่อน ต้องปฏิบัติตามกฎหมายหรือแนวทางปฏิบัติของประเทศนั้นๆ ผู้ประกอบธุรกิจควรใช้ความระมัดระวังอย่างสูง ในกรณีที่เป็นการโฆษณาหรือการตลาดสำหรับเด็ก ผู้สูงอายุ หรือผู้ป่วยหนัก และบุคคลที่อาจไม่มีความสามารถเข้าใจข้อความนั้นได้อย่างถูกต้องสมบูรณ์

- การเปิดเผยข้อมูลผ่านระบบออนไลน์ (Online disclosures)

ก) ข้อมูลเกี่ยวกับการประกอบธุรกิจ ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์กับผู้บริโภค ควรจัดหาข้อมูลเกี่ยวกับการประกอบกิจการของตนที่มีความถูกต้อง ชัดเจน และมีวิธีการที่ผู้บริโภคสามารถตรวจดูข้อมูลได้ ข้ อมูลดังกล่าวได้แก่ ก-1) การระบุลักษณะจำเพาะของผู้ประกอบธุรกิจ ได้แก่ ชื่อของผู้ประกอบธุรกิจและชื่อทางการค้า ถิ่นอันเป็นที่ตั้งที่ทำการ ของผู้ประกอบกอบธุรกิจ (หรือภูมิลำเนาของนิติบุคคล) ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารทางอิเล็กทรอนิกส์อื่น หรื อเบอร์โทรศัพท์ และหากมีควรระบุถึงสถานที่ตั้งทางทะเบียนตามกฎหมาย ก-2) วิธีการติดต่อกับผู้ประกอบธุรกิจของผู้บริโภคที่สะดวก รวดเร็ว และมีประสิทธิภาพ ก-3) วิธีการระงับข้อพิพาทที่เหมาะสมและมีประสิทธิภาพ ก-4) บริการให้คำปรึกษาทางกฎหมาย และ ก-5) ถิ่นอันเป็นที่ตั้งที่ทำการ และถิ่นอันเป็นที่ตั้งของสำนักงานใหญ่ตามกฎหมาย

ในกรณีที่ผู้ประกอบธุรกิจประกาศแจ้งถึงสมาชิกภาพของตนที่เกี่ยวกับระเบียบขององค์กรที่เกี่ยวข้อง สมาคมของผู้ประกอบธุรกิจ องค์กรระงับข้อพิพาท หรือองค์กรออกใบรับรอง ผู้ประกอบธุรกิจควรแจ้งให้ผู้บริโภคทราบถึ งข้อมูลและวิธีการตรวจสอบยืนยันสมาชิกภาพนั้น ตลอดจนกฎเกณฑ์ แนวทางปฏิบัติขององค์กรที่ออกใบรับรอง

ข) ข้อมูลเกี่ยวกับสินค้าและบริการ ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์กับผู้บริโภค ควรจัดให้มีข้อมูลอธิบายเกี่ยวกับสินค้าหรือบริการของตนที่มีความถูกต้อง และผู้บริโภคจะสามารถตรวจดูข้อมูลเหล่านั้นได้โดยสะดวก เพื่อตัดสินใจว่าจะทำสัญญาหรือไม่ และจัดหาข้อมูลที่จำเป็นให้แก่ผู้บริโภค

ค) ข้อมูลเกี่ยวกับการทำสัญญา ผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์กับผู้บริโภค ควรจัดให้มีข้อมูลว่าด้วยข้อสัญญา เงื่อนไข และราคาสินค้าหรื อบริการตามสัญญาที่ครบถ้วนเพียงพอ เพื่อให้ผู้บริโภคสามารถตัดสินใจได้ว่าจะทำสัญญาหรือไม่ ข้อมูลข้างต้นนี้ควรมีความถูกต้อง ชัดเจน สามารถเข้าใจได้ง่าย และให้โอกาสผู้บริโภคในการพิจารณาสัญญาก่อนจะมีการตกลงทำสัญญา กรณีที่อนุญาตให้มีการจัดทำสัญญาได้มากกว่า 1 ภาษา ผู้ประกอบธุรกิจควรจัดทำข้อมูลที่เป็นภาษา ซึ่งผู้บริโภคสามารถเข้าใจได้ เพื่อให้ผู้บริโภคสามารถตัดสินใจตกลงทำสัญญา ผู้ประกอบธุรกิจควรจัดให้มีข้อมูลเกี่ยวกับสัญญาและเงื่อนไขที่เกี่ยวข้อง ที่มีเนื้อหาสมบูรณ์ ชัดเจนแก่ผู้บริโภค และผู้บริโภค สามารถตรวจดูข้อมูลนั้นได้ ในกรณีที่มีการทำสัญญา สัญญาควรมีข้อความดังต่อไปนี้ ค-1) รายชื่อรายการราคา (สินค้าหรือบริการ) ทั้งหมดที่ผู้ประกอบธุรกิจเรียกเก็บจากผู้บริโภค ค- 2) การแจ้งให้ผู้บริโภคทราบถึงเงินค่าใช้จ่ายซึ่งโดยปกติจะมีการเรียกเก็บ แต่ผู้ประกอบธุรกิจไม่ได้เรียกเก็บ ค-3) ข้อสัญญาเรื่องการจัดส่ง และการปฏิบัติตามสัญญา ค-4) ข้อสัญญา เงื่อนไข และวิธีการชำระเงิน ค-5) ข้อจำกัด หรือเงื่อนไขในการซื้อขาย เช่น ความยินยอมของผู้ปกครองหรือผู้พิทักษ์ ตลอดจนข้อจำกัดเรื่องเวลาและสถานที่ ค-6) ข้อแนะนำในการใช้ รวมทั้งคำเตือนเรื่องความปลอดภัยและสุขภาพ ค-7) ข้อมูลเกี่ยวกับบริการหลังการขาย ค-8) ข้อสัญญาและเงื่อนไขในการขอคืนเงิน การยกเลิกสัญญา การส่งของคืน การเปลี่ยนของ วิธีการยกเลิกและหรือนโยบายการส่งคืนของหรือเรียกคืนเงิน และ ค-9) ข้อสัญญาเรื่องการรับประกันคุณภาพ ข้อมูลทั้งหลายที่เกี่ยวกับราคาสินค้าหรือบริการควรระบุถึงอัตราแลกเปลี่ยนเงินตราต่างประเทศสกุลต่าง ๆ ไว้

- ขั้นตอนการยืนยัน (Confirmation process)

ผู้บริโภคสามารถกำหนดประเภทหรือชนิดของสินค้าหรือบริการที่ต้องการ สามารถแก้ไขปรับปรุงคำเสนอ (ซื้อหรือขอใช้บริการ) สามารถให้ความตกลงยินยอมเพื่อทำนิติกรรม สัญญา และได้รับข้อมูลเกี่ยวกับการตกลงทำสัญญาที่ถูกต้องสมบูรณ์ เพื่อหลีกเลี่ยงความสับสนที่อาจเกิดขึ้นของผู้บริโภค ผู้บริโภคสามารถยกเลิกการทำสัญญาก่อนตกลงทำสัญญาซื้อขาย (สินค้าหรือบริการ)

- การชำระเงิน (Payment)

การจัดให้มีวิธีการชำระเงินที่มี ความปลอดภัย และสามารถใช้ได้ง่าย รวมทั้งข้อมูลรายละเอียดเกี่ยวกับระดับความปลอดภัยของ วิธีการชำระเงินนั้นข้อจำกัดความรับผิดในกรณีมีการชำระเงินโดยไม่ได้รับอนุญาตหรือโดยมิชอบ และวิธีการเรียกคืนสินค้าหรือเงิน (chargeback) เป็นเครื่องมือที่มีประสิทธิภาพในการสร้ างความเชื่อมั่นแก่ผู้บริโภค จึงควรมีการนำวิธีการดังกล่าวมาใช้และ พัฒนาปรับปรุงให้เหมาะสมกับพาณิชย์อิเล็กทรอนิกส์

- การระงับข้อพิพาทและการเยียวยาความเสียหาย (Dispute resolution and redress)

ก) กฎหมายที่ใช้บังคับและเขตอำนาจศาล (APPLICABLE LAW AND JURISDICTION) การทำสัญญาระหว่างประเทศของผู้ประกอบธุรกิจและผู้บริโภค ไม่ว่าจะเกิดจากวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใดก็ตาม ต้องปฏิบัติตามกฎหมายที่ใช้บังคับได้และเขตอำนาจศาลในขณะนั้น ประเด็นที่น่าขบคิดคือ หลักกฎหมายที่ใช้ในปัจจุบันจะสามารถปรับใช้กับพาณิชย์อิเล็ กทรอนิกส์ได้หรือไม่ ต้องพิจารณาว่า หลักเกณฑ์ทางกฎหมายว่าด้วยกฎหมายที่จะใช้บังคับและเขตอำนาจศาลว่าควรมีการปรับปรุงแก้ไขหรือไม่ หรือควรมีหลักการเฉพาะในเรื่องนี้ เพื่อให้เกิดความเชื่อมั่นแก่ผู้บริโภค และส่งเสริมการพัฒนาพาณิชย์อิเล็กทรอนิกส์ การพิจารณาว่าควรมี ปรับปรุงกฎหมายที่ใช้บังคับอยู่หรือไม่ หน่วยงานภาครัฐต้องคำนึงถึงหลักการสำคัญเรื่อง การให้ความเป็นธรรมแก่ฝ่ายผู้บริโภคและผู้ประกอบธุรกิจและส่งเสริมพาณิชย์อิเล็กทรอนิกส์ นอกจากนี้ผู้บริโภคควรได้รับการคุ้มครองเช่นเดียวกับการคุ้มครองในธุรกิจอื่น อีกทั้งยังต้องจัดให้มีวิธีการระงับข้อพิพาทและการเยียวยาความเสียหายแก่ผู้บริโภคที่เป็นธรรมและทันการณ์ โดยไม่ก่อภาระอันเกินควรแก่ผู้บริโภค

ข) วิธีการระงับข้อพิพาทและการเยียวยาความเสียหายที่เหมาะสม (ALTERNATIVE DISPUTE RESOLUTION AND REDRES) ผู้บริโภคสามารถเข้าสู่กระบวนการระงับข้อพิพาทและการเยียวยาความเสียหายแก่ผู้บริโภคที่เป็นธรรมและทันการณ์ โดยไม่ก่อภาระอันเกินควรแก่ผู้บริโภค ผู้ประกอบธุรกิจ ตัวแทนของผู้บริโภค และหน่วยงานภาครัฐควรประสานงานและร่วมมือกันในการใช้และการพัฒนาแนวทางปฏิบัติระหว่างองค์กร รวมทั้งนโยบายและกระบวนก ารอื่นๆ ที่มีประสิทธิภาพและเป็นธรรม ซึ่งรวมถึงกลไกการระงับข้อพิพาทที่เหมาะสม เพื่อเสนอปัญหาของผู้บริโภคพร้อมกับแก้ไขข้อพิพาทที่เกิดจากพาณิชย์อิเล็กทรอนิกส์สำหรับผู้ประกอบธุรกิจกับผู้บริโภคโดยเฉพาะการทำนิติกรรม สัญญาระหว่างประเทศ ข-1) ผู้ประกอบธุรกิจและตัวแ ทนของผู้บริโภค ควรสร้างมาตรการการเรียกร้องสิทธิและการแก้ไขปัญหาตามข้อร้องเรียนของผู้บริโภคที่มีประสิทธิภาพ เป็นธรรม มีเวลาในการดำเนินการที่เหมาะสม ซึ่งผู้บริโภคไม่ต้องรับภาระค่าใช้จ่ายที่สูงเกินสมควร ผู้บริโภคควรจึงควรได้รับประโยชน์จากมาตรการดังกล่าว ข-2) ผู้ประกอบธุรกิจและตัวแทนของผู้บริโภค ควรจัดให้มีการศึกษาถึงการประสานงานระหว่างองค์กร (ของผู้ประกอบธุรกิจและผู้บริโภค)เพื่อเสนอข้อร้องเรียนของผู้บริโภคและให้ความช่วยเหลือในการระงับข้อพิพาทที่เกิดจากพาณิชย์

อิเล็กทรอนิกส์สำหรับผู้ประกอบธุรกิจกับผู้บริโภค ข-3) ผู้ประกอบธุรกิจ ตัวแทนของผู้บริโภค และหน่วยงานภาครัฐควรประสานงานให้มีการดำเนินการจัดให้มีวิธีการระงับข้อพิพาทที่เหมาะสมแก่ผู้บริโภค ซึ่งเป็นกระบวนการที่มีประสิทธิภาพและทันการณ์ ซึ่งผู้บริโภคไม่ต้องรับภาระค่าใช้จ่ายที่สูงเกินสมควร ข-4) เพื่อให้การปฏิบัติข้ างต้นบรรลุผล ผู้ประกอบธุรกิจ ตัวแทนของผู้บริโภค และหน่วยงานภารรัฐควรนำเทคโนโลยีสารสนเทศที่ทันสมัยมาใช้ในการสร้างความตื่นตัว และให้เสรีภาพในการเลือกผู้บริโภค ทั้งนี้ ควรมีการศึกษาวิจัยในเรื่องที่เกี่ยวข้องต่อไป เพื่อบรรลุวัตถุประสงค์ในระดับระหว่างประเทศ

- ความเป็นส่วนตัว (Privacy)

พาณิชย์อิเล็กทรอนิกส์สำหรับผู้ประกอบธุรกิจกับผู้บริโภค ควรสอดคล้องกับหลักการเรื่องความเป็นส่วนตัวที่กำหนดไว้ใน “แนวทางเรื่องการคุ้มครองความเป็นส่วนตัวและการโอนถ่ายข้อมูลส่วนบุคคล ”(ค.ศ. 1980)(OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980)) และควรพิจารณาถึง “ปฏิญญาว่าด้วย การคุ้มครองความเป็นส่วนตัวสำหรับเครือข่ายระหว่างประเทศ ”(ค.ศ.1998) เพื่อการกำหนดมาตรการเรื่องการคุ้มครองผู้บริโภคที่มีประสิทธิและเหมาะสม

- การเผยแพร่ความรู้ และการประ ชาสัมพันธ์ (Education and awareness) หน่วยงานภาครัฐ ผู้ประกอบธุรกิจ และตัวแทนของผู้บริโภคควรประสานงานและร่วมมือกันในการเผยแพร่ความรู้ ความเข้าใจเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์ เพื่อให้ผู้บริโภคสามารถตัดสินใจเรื่องการมีส่วนร่วมในพาณิชย์อิเล็กทรอนิกส์จากข้อมู ลที่ได้รับ และเพื่อให้ผู้ประกอบธุรกิจและผู้บริโภคตระหนักถึงความสำคัญของการคุ้มครองผู้บริโภค ที่เกี่ยวกับกิจกรรมพาณิชย์อิเล็กทรอนิกส์ระบบออนไลน์ (online activities) หน่วยงานภาครัฐ ผู้ประกอบธุรกิจ สื่อมวลชน สถาบันการศึกษา และตัวแทนของผู้บริโภค ควรใช้วิธีการติ ดต่อที่มีประสิทธิภาพ รวมทั้งเทคนิคที่ทันสมัย ซึ่งสามารถใช้ในการติดต่อสื่อสารทางเครือข่ายระหว่างประเทศ มาใช้เพื่อให้ความรู้แก่ผู้บริโภคและผู้ประกอบธุรกิจ หน่วยงานภาครัฐ ตัวแทนของผู้บริโภค และผู้ประกอบธุรกิจ ควรประสานงานในการเผยแพร่ข้อมูลแก่ ผู้บริโภคและผู้ ประกอบธุรกิจ เกี่ยวกับกฎหมายคุ้มครองผู้บริโภคและวิธีการเยียวยาความเสียหาย ซึ่งเป็นข้อมูลที่(ผู้บริโภค)สามารถตรวจดูและเข้าใจได้ง่าย

3) การบังคับใช้

เพื่อให้บรรลุวัตถุประสงค์ของแนวทางการคุ้มครองผู้บริโภคนี้ ประเทศสมาชิกควรประสานงานกับผู้ประกอบธุรกิจ ผู้บริ โภค และตัวแทนของผู้บริโภค ทั้งในระดับภายในประเทศและระหว่างประเทศ ควรดำเนินการดังต่อไปนี้

ก) หากมีความจำเป็น ควรพิจารณาและส่งเสริมให้มีการจัดทำแนวทางปฏิบัติ และหรือพิจารณาปรับปรุงกฎหมายและแนวทางปฏิบัติที่เกี่ยวข้องกับการคุ้มครองผู้บริโภค โดยให้มีความสอดคล้ องกับพาณิชย์อิเล็กทรอนิกส์ โดยคำนึงถึงหลักการเรื่องความ

เป็นกลางของเทคโนโลยีและสื่อที่ใช้ในการติดต่อสื่อสาร (คือไม่จำกัดเฉพาะเทคโนโลยีหรือสื่อประเภทหนึ่งประเภทใดเท่านั้น)

ข) สนับสนุนให้ภาคเอกชน (ผู้ประกอบธุรกิจ) มีบทบาทนำอย่างต่อเนื่อง ซึ่งรวมถึงการมีส่วนร่วมของตัวแทนผู้บริโภคในการพัฒนามาตรการในการคุ้มครองผู้บริโภคขององค์กรนั้นให้มีประสิทธิภาพ รวมถึงกฎเกณฑ์ วิธีการระงับข้อพิพาท และขั้นตอนการเรียกร้องสิทธิ

ค) สนับสนุนให้ภาคเอกชนมีบทบาทนำอย่างต่อเนื่องในการพัฒนาเทคโนโลยี เพื่อใช้เป็นเครื่องมือสำคัญในการคุ้มค รองผู้บริโภคและสร้างอำนาจต่อรองแก่ผู้บริโภค

ง) เผยแพร่ประชาสัมพันธ์เนื้อหา วัตถุประสงค์ของแนวทางการคุ้มครองผู้บริโภคให้แพร่หลาย และสนับสนุนให้มีการนำไปใช้ปฏิบัติและ

จ) อำนวยความสะดวกแก่ผู้บริโภคได้ตรวจดูข้อมูล ความรู้ คำปรึกษา และการให้คำแนะนำในการยื่นข้อร้องเรียนเกี่ยวกับพาณิชย์อิเล็กทรอนิกส์

4) ความร่วมมือระหว่างประเทศ

ประเทศสมาชิกควรดำเนินการเพื่อให้การคุ้มครองผู้บริโภคเป็นไปอย่างมีประสิทธิภาพ และเหมาะสมกับพาณิชย์อิเล็กทรอนิกส์ระหว่างประเทศ ในเรื่องการอำนวยความสะดวกในเรื่องการติดต่อสื่อสาร การประสานงาน รวมทั้งการพัฒนาและการสนับสนุนให้เกิดการริเริ่มร่วมกันของผู้ประกอบธุรกิจและตัวแทนของผู้บริโภค และหน่วยงานภาครัฐในระดับระหว่างประเทศ ป้องกันการกระทำที่มิชอบด้วยกฎหมายระหว่างประเทศ เช่น การหลอกลวง การก่อให้เกิดความเข้าใจผิด และการกระทำที่ไม่เป็นธรรมทางการค้า โดยความร่วมมือกันขององค์กรผู้มีอำนาจรับผิดชอบในการบังคับใช้กฎหมาย การออกระเบียบ กฎเกณฑ์ และการพิจารณาคดี ในการแลกเปลี่ยนข้อมูล การติดต่อประสานงานเรื่องต่างๆ ประสานงานกับเครือข่ายระหว่างประเทศต่างๆ ที่มีอยู่ และเข้าร่วมในการเจรจาเพื่อบรรลุข้อตกลงระหว่างเทศในระดับทวิภาคี และหรือระดับพหุภาคี และการดำเนินการอื่นตามที่มีความจำเป็นและตามความเหมาะสมเพื่อให้เกิดการร่วมมือกัน ก่อให้เกิดฉันทามติเรื่องการคุ้มครองผู้บริโภคทั้งในระดับประเทศและระดับระหว่างประเทศ เพื่อสร้างความมั่นใจแก่ผู้บริโภคในการคุ้มครองผู้บริโภค และผู้ประกอบธุรกิจในการดำเนินธุรกิจ ประสานงานและร่วมมือในการบรรลุข้อตกลงหรือการดำเนินการใดๆ เกี่ยวกับการบังคับคดีตามคำพิพากษาหรือคำสั่งศาล อันเนื่องมาจากคดีพิพาทระหว่างผู้บริโภคและผู้ประกอบธุรกิจ ซึ่งเป็นผลจากการบังคับใช้กฎหมายในกรณีการกระทำทุจริตการหลอกลวง หรือการกระทำที่ไม่เป็นธรรมทางการค้า

3.2 การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ตามที่ปรากฏในแนวทางในการประมวลแฟ้มข้อมูลส่วนบุคคลทางคอมพิวเตอร์ของสหประชาชาติ

แนวทางนี้ได้รับการจัดทำขึ้นเมื่อเมื่อวันที่ 14 ธันวาคม 1990 โดยสมัชชาใหญ่แห่งสหประชาชาติได้มีมติกำหนดแนวทางในการประมวลผลแฟ้มข้อมูลส่วนบุคคลทางคอมพิวเตอร์ขึ้น (Guidelines Concerning Computerized Personal Data Files) เพื่อให้ประเทศสมาชิกปฏิบัติตามหลักเกณฑ์ในการกำหนดมาตรฐานขั้นต่ำเกี่ยวกับการบัญญัติกฎหมายภายในของรัฐดังต่อไปนี้[3]

1) หลักเกี่ย วกับความชอบธรรมในการประมวลผลข้อมูล (Principle of Lawfulness and Fairness) ข้อมูลที่ได้รับการประมวลผลจะต้องได้มาโดยชอบธรรม และชอบด้วยกฎหมาย ทั้งนี้ โดยไม่ขัดหรือแย้งกับกฎบัตรสหประชาชาติ (Charter of the United Nations)

2) หลักความถูกต้อง (Principle of Accuracy) บุคคลมีหน้าที่รับผิดชอบในการเก็บรักษาข้อมูลจะต้องทำการตรวจสอบข้อมูลตลอดเวลาเพื่อให้แน่ใจว่าข้อมูลที่จัดเก็บนั้นถูกต้อง

3) หลักในการกำหนดวัตถุประสงค์พิเศษในการจัดเก็บข้อมูล (Principle of the Purpose-specification)

- ข้อมูลส่วนบุคคลจะต้องจัดเก็บและรวบรวมอย่างพอเพียง ตามวัตถุประสงค์ที่กำหนดไว้เป็นพิเศษ
- ห้ามมิให้มีการใช้ข้อมูลหรือเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง
- ระยะเวลาในการจัดเก็บจะต้องไม่เกินไปกว่าวัตถุประสงค์ที่กำหนดไว้เป็นพิเศษ

4) หลักในการเข้าถึงข้อมูลส่วนบุคคล (Principle of Interested-person Access) บุคคลมีสิทธิที่จะเข้าถึงข้อมูลของตนเองโดยการแสดงหลักฐานสำคัญเพื่อแสดงว่าตนเป็นใคร

5) หลักในการไม่เลือกปฏิบัติ (Principle of Non-discrimination) ในการจัดทำข้อยกเว้น จะต้องไม่มีการเลือกปฏิบัติไม่ว่าบุคคลนั้นจะมีสัญชาติ เชื้อชาติ ศาสนา เพศ ความเห็นทางการเมือง ความคิด ความเชื่อ หรือความเป็นสมาชิกภาพสถาบัน หรือสมาชิกภาพองค์กร แตกต่างกันก็ตาม

6) การกำหนดข้อยกเว้น (Power to make exceptions) ข้อห้ามในการเปิดเผยข้อมูลจะไม่นำไปบังคับใช้ หากกระทบต่อความมั่นคงของรัฐ ความสงบเรียบร้อยของประชาชน การสาธารณสุข หรือศีลธรรม รวมทั้งเสรีภาพของบุคคลอื่น

---

[3] นคร เสรีรักษ์, “การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย”, หน้า 100.

7) หลักความปลอดภัย (Principle of Security) จะต้องมีการนำมาตรการที่เหมาะสมมาใช้เพื่อป้องกันแฟ้มข้อมูลส่วนบุคคล ทั้งจากเหตุที่อาจเกิดขึ้นตามธรรมชาติ ความเสียหายอันเกิดจากการกระทำของมนุษย์ เช่น การเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต การนำข้อมูลไปใช้โดยไม่ชอบ หรือการใส่โปรแกรมไวรัสเข้าไปในระบบคอมพิวเตอร์เพื่อทำลายข้อมูล

8) หลักการตรวจสอบและบทลงโทษ (Supervision and Sanctions) กฎหมายภายในของประเทศสมาชิกจะต้องกำหนดให้มีระบบการตรวจสอบการปฏิบัติตามหลักเกณฑ์ข้างต้น และจะต้องกำหนดบทลงโทษทั้งทางอาญาและบทปรับในกรณีที่มีการล่วงละเมิดเกิดขึ้น

9) หลักการส่งข้อมูลไปต่างประเทศ (Tranborder Data Flows) ในการส่งข้อมูลไปยังต่างประเทศจะต้องทำได้โดยเสรี และมีหลักประกันความปลอดภัยในการส่งข้อมูลดังกล่าว

10) หลักการบังคับใช้ (Field of Application) หลักการข้างต้นใช้บังคับกับหน่วยงานภาครัฐและภาคเอกชน

3.3 การคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ของต่างประเทศอื่น ๆ

นอกจากองค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา หรือ Organization for Economic Cooperation and Development (OECD) ที่ให้ความสำคัญกับปัญหาการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์แล้ว องค์กรระหว่างประเทศ หรือประเทศอื่นๆ ต่างก็ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ด้วย เช่น สหประชาชาติ หรือ United Nation (UN) ได้กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขั้นต่ำไว้ใน Guidelines for the Regulation of Computerized Personal Data File ที่ออกเมื่อปี ค.ศ. 1990 และสหภาพยุโรป หรือ European Union (EU) ก็ได้ออกกฎเกณฑ์หลายฉบับที่มีสาระสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วย เช่น Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ซึ่งกฎเกณฑ์นี้มีวัตถุประสงค์ในการป้องกันความเป็นส่วนตัวของข้อมูลส่วนบุคคล และให้ความสำคัญกับการโอนถ่ายข้อมูลส่วนบุคคลด้วย ซึ่งข้อตกลงนี้จะมีการให้ความคุ้มครองข้อมูลที่อ่อนไหว หรือ Sensitive Data เป็นพิเศษด้วย ข้อตกลงอีกฉบับที่ EU กำหนดขึ้นก็คือ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ซึ่งกฎเกณฑ์นี้มีวัตถุประสงค์ในการ ป้องกันทุกกระบวนการที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และมีการคุ้มครองความเป็นส่วนตัวในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ด้วย นอกจากนี้ประเทศต่างๆ ทั้งโลก ก็ได้ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคลโดยการออกกฎหมายภายในประเทศของตนให้สอดคล้องกับหลักเกณฑ์ที่องค์การระหว่างประเทศได้

กำหนดขึ้นด้วย เช่น ประเทศอังกฤษ ได้ออก The Data Protection Act หรือ DPA ขึ้นในปี 1998, ประเทศสหรัฐอเมริกา ได้ออก Privacy Act ในปี 1974 และได้ออกกฎหมายพิเศษอื่นๆ เพื่อให้คุ้มครองข้อมูลส่วนบุคคลอื่นๆ อีก เช่น Fair Credit Reporting Act ในปี 1970, Health Insurance Portability and Accountability Act ในปี 1996, Financial Modernization Act ในปี 1999, Children's On line Privacy Protection Act ในปี 1998 เป็นต้น

สำหรับกรณีของประเทศสหรัฐอเมริกาแม้จะมีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอยู่หลายฉบับด้วยกัน อีกทั้งยังมีกลไกการกำกับดูแลตนเอง (self-regulation) ที่มีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) แต่เนื่องด้วยหลักเกณฑ์ทั่วไปในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ปรากฏในข้อกำหนด Directive 95/46/EC on the Protection of Individuals With regard to the Processing of Personal Data on the Free Movement of Such Data ซึ่งมีผลใช้บังคับเมื่อวันที่ 24 ตุลาคม 1995 นั้นได้มีเนื้อหาระบุ "ห้ามมิให้มีการโอนถ่ายข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศอื่นซึ่งมิได้เป็นสมาชิกสหภาพยุโรป หากประเทศดังกล่าว ไม่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ (adequate level of protection) เว้นแต่จะเป็นกรณีที่เข้าข้อยกเว้นเท่านั้น "[4] และเนื่องจากประเทศสหรัฐอเมริกาก็ไม่ได้มีองค์กรระดับประเทศด้านการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ จึงทำให้เกิดมุมมองจากสหภาพยุโรปว่า มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นยังไม่เพียงพอ ดังนั้น เพื่อเป็นการคุ้มครองข้อมูลส่วนบุคคลที่จะถูกถ่ายโอนจากผู้ประกอบการที่อยู่ในรัฐสมาชิกของสหภาพยุโรป ไปยังผู้ประกอบการในประเทศสหรัฐอเมริกา ให้มีมาตรฐานของการได้รับความคุ้มครองทัดเทียมกับมาตรฐานการถ่ายโอนข้อมูลส่วนบุคคลภายในรัฐสมาชิกสหภาพยุโรป ผู้แทนของสหภาพยุโรปและกระทรวงพาณิชย์ของประเทศสหรัฐอเมริกาจึงได้มีการทำความตกลงเบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (data protection) หรือที่เรียกว่า "Safe Harbor Principles" ขึ้น เมื่อวันที่ 26 กรกฎาคม 2000 ซึ่งสาระสำคัญของความตกลงดังกล่าว ก็คือ การอนุญาตให้การส่งข้อมูลจากรัฐสมาชิกของสหภาพยุโรปไปยังประเทศสหรัฐอเมริกาได้ ก็ต่อเมื่อผู้ประกอบการในประเทศสหรัฐอเมริกาได้เข้าร่วมในโครงการ Safe Harbor แล้ว โดยผู้ประกอบการจะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดใน Safe Harbor ทุกประการด้วย หรือในกรณีที่ผู้ประกอบการภายในประเทศสหรัฐอเมริกาสามารถแสดงให้เห็นได้ว่าตนเองมีการกำหนดมาตรการกำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพเพียงพอ โดยการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนเองให้สอดคล้องกับหลักเกณฑ์ของ Safe Harbor ดังนี้ หาก

---

[4] Article 25 Principles "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,"

ผู้ประกอบการในประเทศสหรัฐอเมริกาได้ปฏิบัติตามเงื่อนไขดังกล่าวแล้ว ก็จะสามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปได้อย่างปราศจากข้อจำกัดใดๆ ทำให้ผู้ประกอบการในสหรัฐอเมริกาสามารถติดต่อธุรกิจกับผู้ประกอบการของสหภาพยุโรปได้ภายใต้ความตกลงนี้

ดังนั้น จะเห็นได้ว่าสหภาพยุโรปก็เป็นอีกหนึ่งองค์กรระหว่างประเทศที่ให้ความสำคัญกับเรื่องการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ถือว่ามีมาตรฐานการให้ความคุ้มครองสูง ต่อไปจึงขอนำเสนอสาระสำคัญของกฎหมายที่เกี่ ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป ดังนี้

3.3.1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

ข้อตกลงนี้เป็นการให้ความคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคล รวมทั้งการโอนถ่ายข้อมูลส่วนบุคคล ข้อตกลงนี้ถูกจัดทำขึ้นเพื่อสร้างหลักประกันในเรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคลภายใต้วัตถุประสงค์เพื่อให้การถ่ายโอนข้อมูลส่วนบุคคลภายในรัฐสมาชิ กของสหภาพยุโรปสามารถทำได้โดยอิสระ และสร้างความเป็นมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของรัฐสมาชิกให้มีมาตรฐานเดียวกัน

โดยที่ขอบเขตของข้อตกลงนี้จะใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งการประมวลผลโดยอัตโนมัติและการประมวลผลโดยวิธีการ Manual สำหรับการประม วลผลโดยวิธีการ Manual นั้น ข้อมูลที่ถูกประมวลผลโดยวิธีนี้จะต้องเป็นส่วนหนึ่งหรือมีเจตนาที่จะให้เป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล (Filing System เช่น ระบบการจัดเก็บข้อมูลทางการเงินของธนาคาร เป็นต้น) อย่างไรก็ตาม กฎหมายไม่ได้บังคับกับการประมวลผลข้อมูลโดยบุ คคลธรรมดา ทั้งนี้ สาระสำคัญของข้อตกลงนี้มีดังต่อไปนี้[5]

1) ข้อมูลที่กฎหมายคุ้มครอง

ข้อมูลที่ได้รับความคุ้มครองตามข้อตกลงนี้ ก็คือ ข้อมูลส่วนบุคคล ซึ่งตามข้อตกลงนี้คำว่า “ข้อมูลส่วนบุคคล ” หรือ 'personal data' หมายถึง ข้อมูลข่าวสารใดๆ ที่สามารถระบุตัวหรืออาจระบุตัวบุคคลนั้นได้ ซึ่งบุคคลที่อาจระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมนี้ อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะตัวของบุคคล หรือจากปัจจัยอื่นๆ ที่มี

---

[5] โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. สาระสำคัญกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่างประเทศ. หน้า 1-5.

ลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรม และสภาพสังคมของบุคคลนั้น เป็นต้น[6]

2) กระบวนการหรือการดำเนินการที่กฎหมายควบคุม

กระบวนการหรือการดำเนินการที่กฎหมายควบคุมตามข้อตกลงนี้ คือ การประมวลผลข้อมูล (Processing) ซึ่งหมายความว่า การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีการอัตโนมัติ หรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึก การจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การส่งผ่าน การใช้ การเปิดเผย การเผยแพร่ หรือโดยวิธีการอื่นๆ ที่ทำให้เข้าถึงข้อมูลได้

3) บุคคลที่ถูกกฎหมายควบคุม

เมื่อพิจารณาจากบทนิยามของข้อตกลงดังกล่าวจะเห็นได้ว่า บุคคลที่ถูกควบคุม คือ ผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผลข้อมูล (Processor) โดยที่ผู้ควบคุมข้อมูล หมายความว่า บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือองค์กรอื่นใด ที่ทำหน้าที่ควบคุมข้อมูลส่วนบุคคลโดยลำพัง หรือร่วมกับผู้อื่นในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคค ลในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือข้อบังคับของรัฐสมาชิกหรือโดยสหภาพยุโรป ส่วนผู้ประมวลผลข้อมูล คือ บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่รัฐ หน่วยงานหรือองค์กรอื่นใดซึ่งประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล

4) หน้าที่ของบุคคลที่ถูกควบคุม

ข้อตกลงนี้กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่ต้องแจ้งก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติ โดยในการแจ้งนั้นต้องประกอบด้วยรายการข้อมูลดังนี้

1. ชื่อที่อยู่ของผู้ควบคุมข้อมูลและผู้แทน (ถ้ามี)
2. วัตถุประสงค์ของการประมวลผล
3. ประเภทของข้อมูลที่เก็บ
4. ผู้รับข้อมูล
5. วัตถุประสงค์ของการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

---

[6] 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

6. ข้อมูลเบื้องต้นเกี่ยวกับมาตรการที่ใช้เพื่อรักษาความปลอดภัยในการประมวลผลข้อมูล

ทั้งนี้ก่อนการประมวลผลข้อมูล ข้อตกลงนี้กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้ วยกฎหมาย ซึ่งการประมวลผลเช่นใดถึงจะเรียกว่าชอบด้วยกฎหมายนั้น ข้อตกลงนี้ได้กำหนดไว้ 7 กรณีดังนี้

1. ได้รับความยินยอมจากเจ้าของข้อมูล
2. เป็นกรณีจำเป็นเพื่อปฏิบัติตามสัญญาหรือเป็นการดำเนินการก่อนเข้าทำสัญญา
3. ตามที่กฎหมายกำหนด
4. เพื่อรักษาชีวิตของเจ้าของข้อมูล
5. เพื่อปฏิบัติภารกิจที่ผลประโยชน์ของสาธารณะ
6. เป็นการจำเป็นต่อการปฏิบัติหน้าที่ของของเจ้าพนักงาน
7. เพื่อประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลที่สาม และการประมวลผลดังกล่าวไม่เป็นการประทบกระเทือนต่อประโยชน์ของการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลโดยเฉพาะสิทธิในความเป็นส่วนตัว

5) หลักการทั่วไปเกี่ยวกับการประมวลผลข้อมูล

ข้อตกลงนี้กำหนดว่าประเทศสมาชิกต้องปฏิบัติการต่อไปนี้ในการดำเนินการต่อข้อมูลส่วนบุคคล อันได้แก่

1. ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย
2. ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (specified, explicit, and legitimate purpose) นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่การประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์
3. ข้อมูลส่ วนบุคคลต้องมีความเพียงพอ (adequate) ไม่มากเกินจำเป็น (not excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น
4. ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และกรณีจำเป็นต้องเป็นปัจจุบันด้วย
5. ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเ จ้าของข้อมูลไว้นานเกินไป อีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

นอกจากนี้ตามข้อตกลงได้กำหนดให้มีข้อมูลที่มีความอ่อนไหว (Sensitive Data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสมเพื่อคุ้มครองข้อครองข้อมูลส่วนบุคคลจาก

1. การทำลายข้อมูลโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย
2. การสูญเสียข้อมูลโดยอุบัติเหตุ
3. การแก้ไขเปลี่ยนแปลงโดยอุบัติเหตุ
4. การเปิดเผยหรือการเข้าถึงโดยปราศจากอำนาจ และ
5. ป้องกันการประมวลผลที่มิชอบด้วยกฎหมายทุกรูปแบบ

การพิจารณาถึงความเหมาะสมที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลนั้นต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นจากการประมวลผล และลักษณะของข้อมูลที่ทำการประมวลผล

โดยสรุปข้อกำหนดของ EU ได้กำหนดให้รัฐสมาชิกอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักทั่วไป ดังนี้[7]

1. ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล
2. การประมวลผลจะทำให้เท่าที่จำเป็นในการทำนิติกรรมสัญญาใด ๆ ของผู้เป็นเจ้าของข้อมูลเท่านั้น
3. การประมวลผลจะต้องอยู่ภายใต้กรอบของกฎหมาย
4. การประมวลผลจะต้องกระทำเพื่อปกป้องผลประโยชน์สำคัญของผู้เป็นเจ้าของข้อมูล
5. การประมวลผลจำเ ป็นที่จะต้องกระทำเพื่อผลประโยชน์ของสาธารณะ หรือในการดำเนินงานของหน่วยงานของรัฐที่ได้รับมอบหมายให้เป็นผู้ควบคุมข้อมูล หรือเปิดเผยข้อมูลต่อบุคคลที่สาม
6. การประมวลผลที่จำเป็นและอยู่ภายใต้กรอบของกฎหมายจะต้องไม่กระทบต่อผลประโยชน์ หรือสิทธิขั้นพื้นฐานของผู้เป็นเจ าของข้อมูล

นอกจากนี้ ข้อตกลงนี้ยังได้ให้ความสำคัญเกี่ยวกับความลับและความมั่นคง รวมถึงข้อยกเว้นในการเปิดเผยข้อมูลกรณีที่ไม่ได้นำข้อมูลไปใช้ประโยชน์สาธารณะ แต่นำไปใช้เพื่อประโยชน์ส่วนตัว และกำหนดเกี่ยวกับเรื่องความเสียหายที่เกิดขึ้นต่อข้อมูล เมื่อมีการประมวลผลโดยไม่ชอบด้วยกฎหมาย และการเปิดเผยข้อมูลจะต้องไม่ละเมิดต่อความมั่นคงของรัฐ

---

[7] สำนักเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ , โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ, (กรุงเทพมหานคร : เดือนตุลา, 2544.), หน้า 99-100.

6) การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

ข้อตกลงนี้ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลเพื่อประมวลผลหรือเจตนาที่จะประมวลผลไปยังต่างประเทศที่มิได้เป็นสมาชิกสหภาพยุโรป เว้นแ ต่ประเทศที่รับข้อมูลจะมีระดับการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ อย่างไรก็ตาม ข้อตกลงนี้ก็ได้กำหนดข้อยกเว้นไว้ เช่น ในกรณีที่ได้รับความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง หรือการส่งหรือโอนข้อมูลส่วนบุคคลจำเป็นเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลและผู้ควบคุมข้อมูลมีอยู่ระหว่างกัน หรือเพื่อปฏิบัติการให้เป็นไปตามข้อตกลงก่อนเข้าทำสัญญาตามคำร้องขอของเจ้าของข้อมูล

ในกรณีที่ผู้ประกอบการภายในสหภาพยุโรปต้องการโอนข้อมูลส่วนบุคคลที่ได้รับมาจากผู้บริโภคไปยังผู้ประกอบการ E-commerce ในประเทศสหรัฐอเมริกาได้นั้น การโอ น ถ่ายข้อมูลจะต้องอยู่ภายใต้ข้อตกลงที่เรียกว่า Safe Harbor ซึ่งเป็นการทำความตกลงระหว่างสหภาพยุโรปและประเทศสหรัฐอเมริกา ซึ่งผู้ประกอบการภายในประเทศสหรัฐอเมริกาที่จะได้รับอนุญาตให้สามารถรับโอนข้อมูลจากผู้ประกอบการภายในสหภาพยุโรปได้นั้น ผู้ประกอบการภายในประเทศ สหรัฐอเมริกาจะต้องปฏิบัติตามเงื่อนไขที่กำหนดตาม Safe Harbor Principles และมีรายชื่ออยู่ใน Safe Harbor List ที่จะปรากฏทางทะเบียนของกระทรวงพาณิชย์ของสหรัฐเมริการก่อน

7) สิทธิของเจ้าของข้อมูล

ข้อตกลงนี้ได้ให้สิทธิของเจ้าของข้อมูลดังนี้

1. สิทธิที่จะได้รับข้อมู ลตามที่กฎหมายกำหนดเมื่อถูกเก็บรวบรวมข้อมูล
2. สิทธิเข้าถึงข้อมูลส่วนบุคคลของตน
3. สิทธิที่จะแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้อง

8) องค์การที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย

ข้อตกลงนี้วางแนวทางให้ประเทศสมาชิกสหภาพยุโรป กำหนดให้มีองค์กรที่ทำหน้าที่ ควบคุมดูแลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความเป็นอิสระไว้ในกฎหมายคุ้มครองของแต่ละประเทศ ซึ่งประเทศสมาชิกส่วนใหญ่ก็จะกำหนดไว้ในรูปของ Commissioner ซึ่งตามข้อตกลงนี้กำหนดให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอย่างน้อยต้องกำหนดอำนาจหน้ าที่ดังต่อไปนี้ให้กับบุคคลหรือองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมาย คือ

1. อำนาจในการสืบสวน เช่น อำนาจในการเข้าถึงและเก็บรวบรวมข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ของผู้ควบคุมดูแล
2. อำนาจในการแทรกแซง เช่น อำนาจในการออกคำสั่งขัดขวาง ลบหรือทำลายข้อมูล หรือการห้ามการประมวลผลข้อมูลชั่วคราว

3. รับคำร้องทุกข์เกี่ยวกับการดำเนินการที่เป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลและวินิจฉัยคำร้องทุกข์ดังกล่าว
4. จัดทำรายงานการปฏิบัติงานและเผยแพร่รายงานดังกล่าวต่อสาธารณะ

โดยที่ข้อตกลงนี้ให้การคุ้มครองข้อมูลส่วนบุคคลโดยมีสาระสำคัญดังนี้

ข้อตกลงนี้ใช้กับกระบวนการทางอิเล็กทรอนิกส์ทุกขั้นตอนนับตั้งแต่ การเก็บรวบรวม การเก็บรักษา การเปิดเผยข้อมูลส่วนบุคคล โดยที่ข้อตกลงนี้ให้สิทธิแก่บุคคลเหนือข้อมูลส่วนบุคคลของตน และข้อตกลงนี้ได้กำหนดหน้าที่ให้ผู้ควบคุมดูแลข้อมูลมีหน้าที่ต้องรัก ษาข้อมูลส่วนบุคคลตามมาตรฐานที่กำหนดในข้อตกลงนี้ โดยรัฐสมาชิกของสหภาพยุโรป สามารถกำหนดได้ว่า ข้อมูลประเภทใดบ้างที่จะต้องดำเนินการภายใต้ตามข้อตกลงนี้ โดยผู้ควบคุมดูแลข้อมูลต้องดำเนินการดังต่อไปนี้

- ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องรวบรวมและจั ดเก็บข้อมูลส่วนบุคคลอย่างเป็นธรรมและถูกต้องตามกฎหมายเท่านั้น
- การเก็บรวบรวมและการดำเนินการจะต้องมีวัตถุประสงค์โดยเฉพาะเจาะจง ชัดแจ้ง และถูกต้องตามกฎหมาย มีความเหมาะสมและอยู่ภายใต้วัตถุประสงค์ที่เกี่ยวข้อง
- ข้อมูลส่วนบุคคลจะต้องมีความถูกต้องทันสมัย โดยต้องอนุ ญาตให้เจ้าของข้อมูลแก้ไขข้อมูลส่วนบุคคลของตนให้ถูกต้องได้
- ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลโดยจะนำข้อมูลส่วนบุคคลมาใช้ได้ต่อเมื่อได้รับความยินยอมอย่างชัดแจ้งจากผู้บริโภคสำหรับวัตถุประสงค์นั้นๆ แล้ว การนำข้อมูลมาใช้ต้องมีเอกสารให้ความยินยอมที่ชั ดแจ้ง เช่น ในสัญญา หรือในข้อตกลงต่างๆ
- ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องมีการบอกกล่าวว่าข้อมูลจะถูกเก็บรักษาและถูกนำไปใช้อย่างไร
- ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องอนุญาตให้ผู้เป็นเจ้าของข้อมูลส่วนบุคคลมีสิทธิที่จะดูข้อมูลและแก้ไขหากมีความผิดพลาดได้
- ก่อนที่ข้อมูลจะถูกให้แก่บุคคลที่สาม ผู้ประกอบการหรือผู้ควบคุมดูแลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลนั้น และเจ้าของข้อมูลมีสิทธิที่จะไม่ให้ข้อมูลส่วนบุคคลนั้นก็ได้
- ในกรณีที่ข้อมูลส่วนบุคคลดังกล่าวเป็นข้อมูลที่มี ความอ่อนไหว การเก็บรวบรวมข้อมูล จะต้องเกี่ยวข้องกับวัตถุประสงค์ที่ระบุ และจะต้องมีกฎระเบียบเป็นพิเศษสำหรับข้อมูลที่อ่อนไหว เช่น ข้อมูลทางการแพทย์ การเงิน ศาสนา การเมือง

3.3.2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[8]

ข้อตกลงเกี่ยวกับกระบวนการที่เกี่ยวข้องกับข้อมูลส่วนตัวและการป้องกันความเป็นส่วนตัวในก ารติดต่อสื่อสารทางอิเล็กทรอนิกส์ โดยที่ข้อตกลงนี้เป็นส่วนหนึ่งของ Telecom Package ซึ่งเป็นกฎระเบียบที่ใช้ควบคุมการติดต่อสื่อสารทางอิเล็กทรอนิกส์แทนระบบเดิมที่มีอยู่ ซึ่งใน Telecom Package ได้รวบรวมข้อตกลงต่าง ๆ โดยมีสาระสำคัญใน 4 เรื่องด้วยกัน คือ กรอบทั่วไป การเข้าถึงและการติดต่อสื่อสาร การอนุญาตและการให้บริการทั่วไป

ข้อตกลงนี้ได้เน้นถึงหลักการพื้นฐานที่ว่า รัฐสมาชิกต้องรับประกันการติดต่อสื่อสารที่กระทำผ่านเครือข่ายอิเล็กทรอนิกส์ ว่าเป็นการติดต่อสื่อสารที่เป็นการส่วนตัว การฟัง ดักฟัง และการเก็บบันทึกการติด ต่อสื่อสารของบุคคลอื่นโดยปราศจากความยินยอมจะกระทำไม่ได้ โดยที่การติดต่อสื่อสารจะต้องเป็นความลับ โดยมีข้อยกเว้นของการคุ้มครองข้อมูลส่วนบุคคล ก็คือ ข้อตกลงนี้ระบุว่ารัฐสมาชิกอาจจะยกเลิกการคุ้มครองข้อมูลได้ในกรณีที่เกี่ยวข้องกับความมั่นคงปลอดภัยของรัฐ การป้อง กันภัยสาธารณะ โดยการกระทำดังกล่าวสามารถทำได้เท่าที่จำเป็นและเหมาะสมเท่านั้น

ข้อตกลงนี้มีการนำระบบ Opt-in มาใช้ กล่าวคือ กำหนดให้ผู้ประกอบการจะต้องให้ผู้ใช้บริการสามารถเลือกว่า ในกรณีการเก็บรวบรวม การใช้ หรือการเปิดเผย ข้อมูลส่วนบุคคลของตนนั้น ผู้ใช้บริการจะอนุญาตให้ผู้ประกอบการ เก็บหรือไม่ให้เก็บ จะให้ใช้หรือไม่ให้ใช้ และจะให้เปิดเผยหรือไม่ให้เปิดเผย ข้อมูลส่วนบุคคลของตนนั้น และในการส่งข้อความหรือข่าวสารต่าง ๆ ไปยังผู้ใช้บริการตามข้อมูลส่วนบุคคลของผู้ใช้บริการ เช่น ที่อยู่ โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ ที่ ผู้ประกอบการได้รับมาอันเนื่องมาจาการประกอบธุรกิจ ผู้ใช้บริการจะต้องยินยอมก่อนที่จะมีการส่งข้อความ หรือข่าวสารต่าง ๆ ไปถึงผู้ใช้บริการ โดยการทำการตลาดต้องได้รับอนุญาตก่อนที่จะมีการส่งข้อความไปยังลูกค้า อันเป็นหลักตรงกันข้ามกับหลัก opt-out ซึ่งอนุญาตให้ส่งข้อ มูลได้จนกว่าจะมีคำสั่งให้หยุดส่ง หลัก opt-in เป็นระบบที่ป้องกัน E-mail ขยะ หรือข้อมูลต่าง ๆ ที่ลดความน่าเชื่อถือของระบบการติดต่อสื่อสารทางอิเล็กทรอนิกส์ อย่างไรก็ตาม หลัก opt-in ก็มีข้อยกเว้นคือ ในกรณีธุรกิจที่มีรายละเอียดข้อมูลของบุคคลอยู่แล้ว ภายใต้สัญญาซื้อขายหรือบริการ โดยผู้บริโภคต้องมีโอกาสในการปฏิเสธการให้ข้อมูลนั้นได้ด้วย

อย่างไรก็ตามหลัก opt-in นั้นรัฐสมาชิกมีการนำเอาหลักดังกล่าวไปใช้บังคับที่แตกต่างกันออกไป จึงทำให้มาตรฐานในการบังคับใช้ข้อตกลงมีความแตกต่างกัน ไม่มีเอกภาพ

---

[8] Official Journal of the European Communities, “Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002”
<europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>

ตามข้อตกลงนี้ อาจจัดทำระบบติ ดต่อสื่อสาร ซึ่งสามารถบันทึกข้อมูลการติดต่อสื่อสาร ซึ่งสามารถบันทึกข้อมูลการติดต่อสื่อสาร (โทรศัพท์ e-mail) เพื่อวัตถุประสงค์ในการเก็บเงิน ซึ่งหลังจากนั้นข้อมูลดังกล่าวอาจถูกนำไปใช้เพื่อวัตถุประสงค์อื่นๆ อย่างไรก็ตาม กฎหมายของรัฐนั้น อาจบังคับให้ผู้ดูแลระบ บต้องเก็บข้อมูลดังกล่าวเพื่อความจำเป็นในทางอาญาซึ่งเกี่ยวกับสิทธิความเป็นมนุษย์ ซึ่งสามารถเก็บข้อมูลนั้นไว้ได้ 24 เดือน ซึ่งอาจก่อให้เกิดภาระแก่ผู้ดูแลข้อมูลที่จะต้องเก็บข้อมูลไว้ก็ได้

นอกจากนี้ในข้อตกลงนี้ยังได้กล่าวถึงรูปแบบและวิธีการเก็บข้อมูลโดยอาศัยเ ทคโนโลยีอื่นๆ เช่น การทำ Spamming การใช้ Cookies และ Public directories เป็นต้น

1) สแปม Spamming

ข้อตกลงนี้ ใช้หลัก opt-in ซึ่งให้ความคุ้มครองในเรื่องการติดต่อการค้าทางอิเล็กทรอนิกส์ เช่น ผู้ใช้ต้องให้ความยินยอมก่อนที่ข้อความดังกล่าวจะเข้าถึงระบบของตน โดยให้ความคุ้มครองไปถึง SMS ข้อความทางอิเล็กทรอนิกส์อื่น ไม่ว่าจะผ่านทางเครื่องมือใดก็ตาม ซึ่งรวมไปถึงโทรศัพท์มือถือด้วย

2) คุกกี้ Cookies[9]

ข้อตกลงนี้ได้มีการกำหนดนิยาม Cookies ไว้ ว่าคือ ข้อมูลขนาดเล็กที่ถูกเก็บอยู่ในคอมพิวเตอร์ส่วนบุคคลเมื่อมีการใช้อินเทอร์ เน็ต ในทางกฎหมายมันถูกใช้เป็นตัวระบุสถานที่ที่ผู้ใช้เว็บไซต์นั้นใช้อยู่ ซึ่งสามารถช่วยผู้ดูแลเว็บไซต์ ในการตรวจสอบการเข้าใช้ย้อนหลังได้

Cookies ถือเป็นข้อมูลที่ซ่อนอยู่ที่เป็นการแลกเปลี่ยนระหว่างผู้ใช้อินเทอร์เน็ตกับผู้ให้บริการ ซึ่งจะบันทึกอยู่ในหน่วยความจำของผู้ใช้ ข้อตกลงนี้กำหนดว่าผู้ใช้ควรมีสิทธิที่จะปฏิเสธการมีคุกกี้ได้ และจะต้องได้รับการอธิบายอย่างชัดแจ้งเกี่ยวกับวัตถุประสงค์ของการใช้คุกกี้

3) Public directories

ข้อตกลงกำหนดว่า บุคคลจะต้องให้ความยินยอมให้ข้อมูลต่างๆ ก่อน แม้ว่าข้อมูลเหล่านั้นจะถูกระบุ ในรายการสาธารณะอยู่แล้วก็ตาม ตัวอย่างของข้อมูลในรายการสาธารณะ ก็เช่น เบอร์โทรศัพท์ ที่อยู่ทางอิเล็กทรอนิกส์ และที่อยู่ เป็นต้น

---

[9] คุกกี้ในที่นี้คือแฟ้มข้อมูลที่เว็บไซต์ส่งมาที่โปรแกรมค้นผ่าน (Browser) เมื่อผู้ใช้บริการเว็บไซต์เ ข้าเยี่ยมชมเว็บไซต์นั้นๆ โดยโปรแกรมค้นผ่านของผู้ใช้บริการจะเก็บคุกกี้ไว้ที่ Hard Drive และทุกครั้งที่ผู้ใช้บริการกลับเข้าไปเยี่ยมชมเว็บไซต์เดิมคุกกี้ของเว็บไซต์ดังกล่าวก็จะถูกส่งกลับไปยังเว็บไซต์นั้นโดยโปรแกรมค้นผ่านของผู้ใช้บริการเองโดยอัตโนมัติ การที่เว็ บไซต์ต่างๆ มีการติดตั้งคุกกี้ก็เนื่องจากคุกกี้ช่วยให้เว็บไซต์จดจำผู้ใช้บริการได้ว่าผู้ใช้บริการเคยเข้ามาเยี่ยมชมเว็บไซต์นี้หรือเปล่า นอกจากนี้คุกกี้ยังสามารถบันทึกข้อมูลเกี่ยวกับการเยี่ยมชมส่วนต่างๆ บนเว็บไซต์ของผู้ใช้บริการเอาไว้ด้วย

3.3.3 Safe Harbor Principle

สืบเนื่องมาจาก หลักเกณฑ์ทั่วไปในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรปที่ปรากฏในข้อกำหนด Directive 95/46/EC on the Protection of Individuals With regard to the Processing of Personal Data on the Free Movement of Such Data ซึ่งมีผลใช้บังคับเมื่อวันที่ 24 ตุลาคม 1995 ได้มีเนื้อหาระบุ “ห้ามมิให้มีการโอนถ่ายข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศอื่นซึ่งมิได้เป็นสมาชิกสหภาพยุโรป หากประเทศดังกล่าวไม่มีการคุ้มครองข้อมูลส่วนบุคคลในระดับที่เพียงพอ (adequate level of protection) เว้นแต่จะเป็นกรณีที่เข้าข้อยกเว้นเท่านั้น ”[10] โดยที่ข้อมูลส่วนบุคคล (personal data) นั้น ได้แก่ ข้อมูลที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคลธรรมดา (natural person) อาจเป็นข้อมูลที่เป็นรหัสประจำตัว หรือข้อมูลอื่นที่เกี่ยวข้องกับบุคคล ซึ่งอาจเป็นข้อมูลที่มีลักษณะทั่วไป หรือ ข้อมูลส่วนบุคคลชนิดพิเศษ (sensitive data)[11] นั้น โดยที่ข้อยกเว้นในบางกรณีที่ทำให้สามารถโอนถ่ายข้อมูลส่วนบุค คลจากประเทศสมาชิกสหภาพยุโรปไปยังประเทศอื่นซึ่งมิได้เป็นสมาชิกสหภาพยุโรปได้นั้น มีตัวอย่างเช่น ในกรณีที่เจ้าของข้อมูลได้ให้ความยินยอมให้มีการโอนข้อมูลได้อย่างชัดแจ้ง[12] การโอนข้อมูลส่วนบุคคลมีความจำเป็นเพื่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล หรือการดำเนินการใดๆ ก่อนการเข้าทำสัญญาตามที่เจ้าของข้อมูลร้องขอ กรณีที่มีความจำเป็นที่จะต้องโอนข้อมูลเพื่อหาข้อสรุปของสัญญาหรือปฏิบัติตามสัญญาซึ่งทำเพื่อประโยชน์ของเจ้าของข้อมูล และได้จัดทำขึ้นโดยผู้ควบคุมข้อมูลและบุคคลภายนอก[13] ในกรณีที่มีความจำเป็นที่ จะต้องทำการโอนข้อมูลเพื่อประโยชน์สาธารณะ หรือเพื่อการก่อตั้งสิทธิเรียกร้อง หรือการต่อสู้คดีตามกฎหมาย เพื่อคุ้มครองชีวิตของเจ้าของข้อมูล การโอนทางทะเบียนตามที่กฎหมายกำหนด การให้ข้อมูลข่าวสารแก่สาธารณะเพื่อเป็นข้อมูลประกอบการรับ

---

[10] *อ้างแล้ว*, *เชิงอรรถที่ 4*

[11] รายละเอียดโปรดดูบทที่ 2

[12] Article 26, 1. (a) By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer; or ...

[13] กระทรวงเทคโนโ ลยีสารสนเทศและการสื่อสาร ร่วมกับ สำนักงานเลขานุการคณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์, *อ้างแล้ว เชิงอรรถที่ 1*, หน้า19-20.

ฟังความคิดเห็นจากประชาชนหรือผู้ มีประโยชน์ได้เสียในข้อมูลส่วนบุคคลนั้น [14] รวมไปถึง ในกรณีที่มีการทำความตกลงระหว่างประเทศสมาชิกและประเทศอื่นๆ หรือออกกฎหมายที่ให้ความคุ้มครองข้อมูลส่วนบุคคลของประเทศผู้รับโอนข้อมูล และต้องมีการกำหนดเงื่อนไขในการคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมเพียงพอ [15] นอกจากนี้ข้อกำหนดดังกล่าวได้ให้อำนาจแก่คณะกรรมาธิการยุโรป (European Commission) ในการพิจารณาว่าประเทศนอกสหภาพยุโรปที่จะเป็นผู้รับข้อมูลส่วนบุคคลนั้นมีระดับการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอหรือไม่ ซึ่งผลของคำชี้ขาดจะมีผลให้ประเทศนั้นๆ รับโอนข้อมูลจากประเทศใน สหภาพยุโรปได้ ซึ่งจะมีสภาพบังคับให้ประเทศในสหภาพยุโรปต้องปฏิบัติให้สอดคล้องกับคำชี้ขาดด้วย

สำหรับประเทศสหรัฐอเมริกามีกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอยู่หลายฉบับด้วยกัน อาทิเช่น 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 รวมทั้งยังมีกลไกการกำกับดูแลตนเอง (self-regulation) ที่มีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ที่เกิดขึ้นโดยความร่วมมือขององค์กรต่างๆ ภายในประเทศด้วย อย่างไรก็ตาม แม้ว่าประเทศสหรัฐอเมริกาจะได้มีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลอยู่หลายมากมายหลายฉบับก็ตาม แต่เนื่องจากประเทศสหรัฐอเมริกาก็ไม่ได้มีองค์กรระดับประเทศด้านการคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะ จึงทำให้เกิดมุมมองจากสหภาพยุโรปว่า มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกานั้นยังไม่เพียงพอ นั่นเอง

ดังนั้น เพื่อเป็นการคุ้มครองข้อมูลส่วนบุคคลที่จะถูกถ่ายโอนจากผู้ประกอบการที่อยู่ในรัฐสมาชิกของสหภาพยุโรป ไปยังผู้ประกอบการในประเทศสหรัฐอเมริกา ให้มีมาตรฐานของการ

---

[14] Article 25, 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

[15] Article 25, 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

ได้รับความคุ้มครองทัดเทียมกับมาตรฐานการถ่ายโอนข้อมูลส่วนบุคคลภายในรัฐสมาชิกสหภาพยุโรป ผู้แทนของสหภาพยุโรปและกระทรวงพาณิชย์ของประเทศสหรัฐอเมริกาจึงได้มีการทำความตกลงเบื้องต้นเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (data protection) หรือที่เรียกว่า "Safe Harbor Principles" ขึ้น เมื่อวันที่ 26 กรกฎาคม 2000 ซึ่งสาระสำคัญของความตกลงดังกล่าว ก็คือ การอนุญาตให้การส่งข้อมูลจากรัฐสมาชิกของสหภาพยุโรปไปยังประเทศสหรัฐอเมริกาได้ ก็ต่อเมื่อผู้ประกอบการในประเทศสหรัฐอเมริกาได้เข้าร่วมในโครงการ Safe Harbor แล้ว โดยผู้ประกอบการจะต้องปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดใน Safe Harbor ทุกประการด้วย หรือในกรณีที่ผู้ประกอบการภายในประเทศสหรัฐอเมริกาสามารถแสดงให้เห็นได้ว่าตนเองมีการกำหนดมาตรการกำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่มีประสิทธิภาพเพี ยงพอ โดยการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนเองให้สอดคล้องกับหลักเกณฑ์ของ Safe Harbor ดังนี้ หากผู้ประกอบการในประเทศสหรัฐอเมริกาได้ปฏิบัติตามเงื่อนไขดังกล่าวแล้ว ก็จะสามารถรับโอนข้อมูลส่วนบุคคลจากประเทศสมาชิกสหภาพยุโรปได้ อย่างปราศจากข้อจำกัดใดๆ ทำ ให้ผู้ประกอบการในสหรัฐอเมริกาสามารถติดต่อธุรกิจกับผู้ประกอบการของสหภาพยุโรปได้ภายใต้ความตกลงนี้[16]

โดยหลักการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดใน Safe Harbor Principles มีอยู่ด้วยกัน 7 ประการ ดังต่อไปนี้[17]

1) Notice

การแจ้งให้ทราบเกี่ยวกับวัตถุประสงค์ของก ารจัดเก็บข้อมูลส่วนบุคคล การแจ้งให้ทราบเกี่ยวกับวิธีการติดต่อกับผู้ประกอบการ เพื่อติดต่อสอบถามหรือเพื่อการทำข้อร้องเรียน การแจ้งข้อมูลเกี่ยวกับประเภทของบุคคลที่สามที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคล รวมทั้งทางเลือกและวิธีการในการจำกัดการใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

2) Choice

ผู้ประกอบการจะต้องมีการเสนอทางเลือกให้บุคคลตัดสินใจว่าจะให้ข้อมูลส่วนบุคคลของตน ถูกเปิดเผยต่อบุคคลที่สาม หรือถูกนำไปใช้ภายใต้วัตถุประสงค์อื่นๆ และผู้ประกอบการจะต้องจัดเตรียมวิธีการ หรือกลไกที่ชัดเจนที่จะแสดงให้บุคคลสามารถใช้สิทธิ ในการเลือกให้ข้อมูลส่วนบุคคลได้ โดยเฉพาะในกรณีที่เป็นข้อมูลที่อ่อนไหว (Sensitive) บุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลต้องสามารถที่จะเลือกได้ว่าจะจะอนุญาตให้ผู้ประกอบการสามารถเปิดเผยต่อบุคคลที่สามได้หรือไม่ และเป็นไปเพื่อวัตถุประสงค์ใด

---

[16] Mike Markel, “Safe Harbor and Privacy Protection : A Looming Issue for IT Professional”, (Ieee Transaction on Professional Communication, Vol. 49, NO. 1, March 2006)

[17] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, *อ้างแล้ว เชิงอรรถที่ 1*, หน้า 32-34.

3) Onward Transfer

ในการโอนถ่ายข้อมูลส่วนบุคคลไปยังบุคคลที่สาม ผู้ประกอบการจะต้องปฏิบัติตามหลักการ Notice และ Choice อย่างเคร่งครัด การโอนถ่ายข้อมูลไปยังตัวแทนของผู้ประกอบการซึ่งเป็นผู้ถ่ายโอนข้อมูล อาจจะไม่ต้องปฏิบัติตามหลักการ Notice และ Choice ก็ได้ ถ้าหากตัวแทนของผู้ประก อบการนั้นๆ ได้ปฏิบัติตาม Safe Harbor Principles หรือได้ทำสัญญาเป็นลายลักษณ์อักษรในเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับผู้ประกอบการนั้นแล้ว

4) Security

ผู้ประกอบการที่สร้าง เก็บรักษา ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคล จะต้องมีระบบรักษาความปลอดภัยที่เหมาะสม เพื่ อการคุ้มครองข้อมูลส่วนบุคคล ไม่ให้สูญหาย ถูกนำไปใช้ผิดวัตถุประสงค์ หรือการเข้าถึง และการเปิดเผยข้อมูลโดยปราศจากอำนาจ รวมทั้งการเปลี่ยนแปลง แก้ไข และการทำลายข้อมูลส่วนบุคคลด้วย และผู้ประกอบการจะต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ

5) Data Integrity

การเก็บรักษา การใช้ หรือการเผยแพร่ข้อมูลส่วนบุคคลจะต้องเป็นไปเพื่อและสอดคล้องกับวัตถุประสงค์ที่ผู้ประกอบการได้แจ้งไว้เท่านั้น ผู้ประกอบการจะต้องไม่เก็บรักษา ใช้ หรือเผยแพร่ข้อมูลส่วนบุคคลในลักษณะที่ขัดต่อวัตถุประสงค์ในการจัดเก็บ หรือนอกเหนือไปจากที่เจ้าของข้อมูลได้ให้อนุญาตไว้

ในกรณีที่มีความจำเป็นจะต้องนำข้อมูลส่วนบุคคลไปใช้เพื่อวัตถุประสงค์ต่างๆ ผู้ประกอบการจะต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้แน่ใจว่าข้อมูลนั้น มีความสมบูรณ์ ถูกต้อง เชื่อถือได้ สำหรับการนำไปใช้เพื่อวัตถุประสงค์นั้นๆ

6) Access

ผู้ใช้บริการจะต้องมีวิธีการ และสามารถเข้าถึงข้อมูลส่วนบุคคลของตนได้ และสามารถแก้ไข เปลี่ยนแปลงข้อมูลให้ถูกต้องได้ ยกเว้นในกรณีที่ภาระความเสี่ยง หรือค่าใช้จ่ายที่เกิดขึ้นเนื่องจากการจัดการวิธีการเข้าถูกข้อมูลต่างๆ จะมีความเสี่ยง ที่จะละเมิดสิทธิของบุคคลอื่นมากว่า

7) Enforcement

ผู้ประกอบการจะต้องมีกลไกของการบังคับใช้ที่เหมาะสม จะต้องมีการติดตามถึงขั้นตอนการรับนโยบายและกลไกของ Safe Harbor ว่ามีความเหมาะสมและบรรลุผลตามวัตถุประสงค์ Safe Harbor รวมทั้ง จัดให้มีระบบการระงับข้อพิพาทที่เป็นอิสระ เพื่อแก้ไขปัญหาข้อร้องเรียนของผู้ใช้บริการ และมีการจัดการระบบการชดใช้ค่าเสียหาย โดยมีหน้าที่ในการเยียวยาปัญหาจากการที่ผู้ประกอบการเองไม่ได้ปฏิบัติตามหลักการ Safe Harbor ด้วย

3.3.4 <u>กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศญี่ปุ่น Act on Protection of Personal Information 2003</u>[18]

กฎหมายใหม่นี้มุ่งคุ้มครองข้อมูลส่วนบุคคลทั้งในความควบคุมดูแลของหน่วยงานของรัฐ หน่วยงานเอกชน และหน่วยงานอิสระของรัฐด้วย โดยมุ่งจะวางหลักกฎหมายทั่วไปในเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 1) ทั้งนี้โดยคำนึงถึงความจำเป็นใน การเอื้ออำนวยให้การประกอบการค้าและธุรกิจในยุคข้อมูลข่าวสารเป็นไปได้ รวมทั้งคำนึงถึงเสรีภาพในการแสดงความคิดเห็น และเสรีภาพอื่นๆ ตามรัฐธรรมนูญประกอบกันไป คำนิยามที่สำคัญในกฎหมายนี้มีอยู่หลายคำ อาทิเช่น

“ข้อมูลส่วนบุคคล” (Personal Information) ซึ่งหมายถึงบรรดาข้อมูลข่าวสารเกี่ยวกับบุคคลธรรมดาที่อาจใช้ในการระบุบ่งตัวบุคคลได้ เช่น ชื่อ วันเดือนปีเกิด หรือ ข้อมูลข่าวสารใดๆ ซึ่งอาจนำไปเปรียบเทียบประกอบกับข้อมูลข่าวสารอื่น เพื่อใช้ในการระบุบ่งตัวบุคคลได้ (มาตรา 2(1)) ข้อมูลของผู้ตาย และนิติบุคคลจึงไม่อยู่ในข่ายที่จะได้รับการคุ้มครองตามกฎหมายนี้

“ฐานข้อมูลส่วนบุคคล ” (Personal Information Database) หมายถึงระบบข้อมูลข่าวสารที่เก็บรวบรวมข้อมูลต่างๆ ซึ่งมีข้อมูลส่วนบุคคลรวมอยู่ด้วย ไม่ว่าจะเป็นระบบที่สามารถเรียกดูข้อมูลส่วนบุคคลที่เจาะจงได้โดยใช้เครื่องคอมพิวเตอร์ หรือเ ป็นระบบที่อาจตรวจดูข้อมูลส่วนบุคคลที่เจาะจงได้โดยง่ายโดยวิธีอื่นใด

“ข้อมูลบุคคล ” (Personal Data) ซึ่งหมายถึงข้อมูลบุคคลซึ่งได้รับการจัดระบบในลักษณะที่เป็นรากฐานข้อมูลส่วนบุคคล (มาตรา 2(4)) คือ อาจเรียกดูข้อมูลส่วนบุคคล โดยเจาะจงได้โดยวิธีอัตโนมัติ หรือวิธีอื่นใดตามที่กฎหมายลำดับรองกำหนด

“เจ้าของข้อมูล” หมายถึงบุคคลซึ่งอาจบ่งตัวได้โดยอาศัยข้อมูลส่วนบุคคลเป็นเครื่องสื่อ

กฎหมายกำหนดเป็นหลักเกณฑ์เบื้องต้นว่า ผู้ประกอบการเอกชนที่จัดระบบข้อมูลส่วนบุคคลจะต้องระบุวัตถุประสงค์ในการจัดระบบข้อมูลส่วนบุคคลในความควบคุมดู แลของตนให้ชัดเจน และจะต้องไม่นำข้อมูลส่วนบุคคลนั้นไปใช้นอกเหนือจากการใช้ตามปกติภายในขอบวัตถุประสงค์ที่ได้ระบุไว้ นอกจากนี้ ผู้ประกอบการต้องไม่จัดเก็บหรือรวบรวมข้อมูลส่วนบุคคลเกินกว่าที่จำเป็น ในการดำเนินการให้เป็นไปตามวัตถุประสงค์ของการจัดเก็บที่เจ้าของข้ อมูลได้ให้ความยินยอมไว้แล้วอีกด้วย ในกรณีที่ผู้ประกอบการเปลี่ยนวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคลเป็นอย่างอื่น ผู้ประกอบการนั้นจะต้องแจ้งให้เจ้าของข้อมูลทราบ หรือประกาศโฆษณาต่อสาธารณชน ลักษณะสำคัญของกฎหมายของญี่ปุ่นในเรื่องนี้คือ ไม่กำหนดให้ผู้ประกอบการต้ องขอความยินยอมจากเจ้าของเป็นรายบุคคล (Opt-in) อันเป็นหลักที่ใช้กันในกฎหมายของยุโรป แต่หันไปใช้หลักแจ้งให้เจ้าของข้อมูลทราบนับตั้งแต่เมื่อเริ่มจัดเก็บข้อมูลส่วนบุคคลทราบ หรือ

---

[18] กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข ”, (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ , 2549), หน้า 204-217.

โดยโฆษณาต่อสาธารณชน (มาตรา 18(1)) โดยต้องแจ้งวัตถุประสงค์ของการจัดเก็บ การใช้ข้อมูลร่วมกับบุคคลอื่น เพื่อให้เจ้าของข้อมูลมีโอกาสปฏิเสธหรือคัดค้านได้ (Opt-out) ทั้งนี้จะต้องแจ้งหรือกำหนดวิธีบอกกล่าวปฏิเสธหรือโต้แย้งมายังผู้ประกอบการให้เป็นโดยสะดวก (มาตรา 24)

ผู้ประกอบการยังมีหน้าที่ในการจัดให้มีระเบียบและหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและแจ้งให้เจ้าของข้อมูลหรือประกาศต่อสาธรณชน (มาตรา 43) ผู้ประกอบการมีหน้าที่ดูแลรักษาข้อมูลให้ถูกต้องและทันสมัยอยู่เสมอทั้งนี้ตามความจำเป็น เพื่อการบรรลุวัตถุประสงค์ในการจัดให้มีการใช้ประโยชน์ระบบข้อมูลนั้น (มาตรา 19) แต่ขณะเดียวกันเจ้าของข้อมูลก็มีสิทธิที่จะขอตรวจข้อมูลเกี่ยวกับตน และหากข้อมูลดังกล่าวไม่ถูกต้องเจ้าของข้อมูลเรียกให้ผู้ประกอบการแก้ไขข้อมูลเสียให้ถูกต้องได้ (มาตรา 25และ26) ทั้งนี้โดยผู้ประกอบการอาจวางระเบียบ หรือวิธีการในการขอตรวจดูข้อมูลส่วนบุคคลด้วยก็ได้ อย่างไรก็ดีหากแก้ไขข้อมูลตามคำขอของเจ้าของข้อมูลอาจเป็นเหตุให้ผู้ประกอบการต้องเสียค่าใช้จ่ายเกินสมควร ผู้ประกอบการมีสิทธิปฏิเสธไม่ดำเนินการแก้ไขได้ด้วย แต่ต้องดำเนินการอย่างใดอย่างหนึ่ง เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลตามสมควรเป็นการทดแทน (มาตรา26 ประกอบมาตรา34(1))

ผู้ประกอบการมีหน้าที่วางมาตรการต่างๆ เพื่อรักษาความปลอดภัยแก่ข้อมูลส่วนบุคคลและระบบฐานข้อมูลในความควบคุมดูแลของตนไม่ให้เกิดสูญหาย หรือมีผู้นำเอาไปเปิดเผยโดยมิชอบ (มาตรา 20) นอกจากนี้ยังต้องกำกับดูแลลูกจ้างของตน กฎหมายยังกำหนดให้ผู้ว่าจ้างต้องมีหน้าที่รับผิดชอบทำนอง เดียวกัน กฎหมายได้ขยายขอบเขตความรับผิดทางสัญญาและทางละเมิดของผู้ประกอบการให้กว้างขึ้นด้วย

หลักทั่วไปในกฎหมายคุ้มครองข้อมูลส่วนบุคคลคือ การคุ้มครองไม่ให้เปิดเผยหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลภายนอกโดยเจ้าของข้อมูลมิได้รับรู้ หรือยินยอมไว้ล่วงหน้าเว้นแต่จะเข้าข้อยกเว้นที่กฎหมายกำหนด (มาตรา23) ข้อยกเว้นดังกล่าวนี้มีหลายประการ เช่น มีเหตุจำเป็นเพื่อป้องกันภยันตราย หรือเป็นการเปิดเผยต่อเจ้าหน้าที่ผู้มีอำนาจโดยชอบ (มาตรา 23(1)) ที่สำคัญข้อยกเว้นดังกล่าวรวมถึง กรณีเปิดเผยแก่คู่สัญญา ผู้ได้รับมอบหมายให้เป็นผู้บริการเครือข่ายแก่ผู้ประกอบการอันซึ่งมีสิทธิใช้ข้อมูลส่วนบุคคลนั้น

กลไกคุ้มครองสำคัญในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายใหม่ของญี่ปุ่น ก็คือการส่งเสริมให้เอกชนพัฒนามาตรฐานการคุ้มครองขึ้นโดยความริเริ่มของตนเอง ซึ่งเป็นกลไกที่ญี่ปุ่นได้ส่งเสริมมานานแล้ว และได้พัฒนาขึ้นจนมีการออกเครื่องหมายรับรองมาตรฐาน หรือ Privacy mark ขึ้นเป็นมาตรฐานอุตสาหกรรมบริการอย่างหนึ่ง กำหมายญี่ปุ่นยังวางระบบจัดตั้งหน่วยงานเอกชนให้คำปรึกษาแนะนำ และระงับข้อพิพาท อนุญาตให้นิติบุคคลที่มีคุณสมบัติและความเชี่ยวชาญเพียงพอในการกำกับดูแลให้ผู้ ประกอบการดำเนินตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้อย่างถูกต้องเป็นองค์การคุ้มครองข้อมูลส่วนบุคคล

3.3.5 <u>กฎหมายธุรกิจสถาบันการเงินของประเทศสหรัฐอเมริกา (Gramm-Leach-Bliley Financial Modernization ACT 1999)</u>[19]

กฎหมายฉบับนี้มุ่งคุ้มครองความเป็นส่วนตัวของข้อ มูลส่วนบุคคล ในธุรกิจประเภทสถาบันการเงิน (financial institutions) โดยกฎหมายมีวัตถุประสงค์ต้องการให้ผู้ประกอบการประเภทสถาบันการเงินแจ้งนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่อธิบายให้ลูกค้าหรือผู้ใช้บริการทราบถึงวิธีการส่งหรือโอนข้อมูลส่วนบุคคลของผู้ประกอบการ แ ละเพื่อที่จะให้สิทธิแก่ลูกค้าหรือผู้ใช้บริการที่จะจำกัดการส่งหรือโอนข้อมูลส่วนบุคคลของตนได้

สถาบันการเงินตามความหมายของกฎหมายฉบับนี้หมายถึง ผู้ประกอบการที่เสนอผลิตภัณฑ์ทางการเงินในรูปแบบต่างๆ เช่น สินเชื่อ ที่ปรึกษาทางการเงินหรือการลงทุน ประกันภัย และผู้ที่ ได้รับความคุ้มครองตามกฎหมายฉบับนี้คือ ลูกค้าหรือผู้ใช้บริการที่เป็นผู้บริโภค

โดยที่กฎหมายฉบับนี้กำหนดว่า ผู้ประกอบการจะต้องแจ้งถึงสิทธิความเป็นส่วนตัวให้ชัดแจ้งในนโยบายของตน ซึ่งประกอบด้วย ข้อมูลส่วนบุคคลใดบ้างที่ผู้ประกอบการจะจัดเก็บและใครที่จะเกี่ยวข้องกับข้อมูลส่วนบุคคลของผู้บริโภคบ้าง และจะมีวิธีการในการป้องกันความปลอดภัยของข้อมูลอย่างไร โดยที่ข้อมูลที่ได้รับความคุ้มครองก็คือ ข้อมูลที่ไม่ใช่ข้อมูลสาธารณะ (nonpublic personal information) ซึ่งข้อมูลดังกล่าวผู้ประกอบการได้รับมาจากใบสมัครผลิตภัณฑ์ของตน หรือมาจากหน่วยงานหรือองค์กรที่เกี่ยวข้องเช่น บริษัทข้อมูลเครดิต (credit Bureau) หรือข้อมูลต่างๆ ที่ได้รับจากการประกอบกิจการเช่น ยอดเงินหรือวงเงินคงเหลือ (account balance) เป็นต้น แต่สำหรับข้อมูลประเภทที่เป็นข้อมูลสาธารณะจะไม่ได้รับความคุ้มครองเช่น ข้อมูลจดทะเบียนต่างๆ ข้อมูลหลักประกันซึ่งมีการจดทะเบียน เป็นต้น

โดยหลักสำคัญที่กำหนดในกฎหมายฉบับนี้ก็คือ สิทธิที่จะปฏิเสธไม่ให้โอนข้อมูลบางประเภทต่อบุคคลที่สาม (Opt-Out Right) โดยผู้ประกอบการจะต้องแจ้งสิทธิดังกล่าวให้แก่ลูกค้าหรือผู้ใช้บริการทราบด้วย ซึ่งข้อมูลส่วนบุคคลที่จะสามารถใช้สิทธินี้ได้ ก็เช่น ข้อมูลเครดิต ข้อมูลใบสมัคร เป็นต้น แต่สำหรับการส่งข้อมูลให้แก่บริษัทในเครือสามารถทำได้โดยที่ลูกค้าหรือผู้ใช้บริการไม่สามารถใช้สิทธิดังกล่าวได้ นอกจากนี้ยังมีข้อยกเว้นอื่นที่กำหนดให้ลูกค้าหรือผู้ใช้บริการไม่สามารถใช้ สิทธินี้ได้ เช่น การเปิดเผยข้อมูลตามกฎหมาย การเปิดเผยข้อมูลต่อบริษัทภายนอกที่ทำหน้าที่บริการจัดการธุรกิจทั่วไปให้แก่ผู้ประกอบการ และในกรณีที่ได้โอนข้อมูลส่วนบุคคลต่อบุคคลที่สามแล้ว บุคคลที่สามจะต้องใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์เท่าที่จำกัดเท่านั้น ไม่สามารถขายข้อมูลดังกล่าวให้แก่ผู้อื่นเพื่อวัตถุประสงค์ในการทำการตลาด

---

[19] In Brief : The Financial Privacy Requirements of the Gramm-Leach-Bliley Act <http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.pdf>

3.3.6 กฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศอื่น ๆ[20]

1) ประเทศอิตาลี

- ชื่อกฎหมาย Protection of individuals and other subjects with regard to the processing of personal data Act
- ขอบเขตการใช้บังคับ

ก) การประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการปกติ (manual) และวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติ (electronic or automatic)

ข) ใช้บังคับกับข้อมูลส่วนบุคคลของบุคคลธรรมดาและนิติบุคคล

- หลักการและสาระสำคัญของกฎหมาย

ก) กำหนดขอบเขตการประมวลผลข้อมูลในความหมายอย่างกว้าง

ข) กำหนดสิทธิของเจ้าของข้อมูลหน้าที่ของผู้ควบคุมข้อมูล

ค) ให้มีคณะกรรมการที่มีอำนาจหน้าที่กว้างขวางมาก ทั้งในด้านการส่งเสริม สนับสนุน คุ้มครอง ป้องกัน และมีคำสั่ง คำวินิจฉัยกรณีมีการทำผิดกฎหมายและกำหนดให้พนักงานเจ้าหน้าที่มีอำนาจเรียก สอบสวนบุคคล

2) ประเทศฮ่องกง

- ชื่อกฎหมาย Personal Data (Privacy) Ordiance
- ขอบเขตการใช้บังคับ

ก) การดำเนินการใด ๆ กับข้อมูลส่วนบุคคลด้วยวิธีการปกติ (manual) และวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติ (electronic or automatic)

ข) ใช้บังคับทั้งหน่วยงานภาครัฐและภาคเอกชน

- หลักการและสาระสำคัญของกฎหมาย

ก) วางมาตรการเพื่อควบคุมการกระทำเกี่ยวกับข้อมูลส่วนบุคคลที่ได้เก็บรวบรวม ครอบครอง ประมวลผล หรือใช้ประโยชน์

ข) กลไกควบคุมที่สำคัญคือ การจัดตั้งคณะกรรมการทำหน้าที่ตรวจสอบ ไต่สวน และลงโทษผู้ใช้ข้ อมูลส่วนบุคคลโดยมิชอบ และมีอำนาจออก Code of Practice

3) ประเทศนิวซีแลนด์

- ชื่อกฎหมาย The Privacy Act 1993

---

[20] ไพโรจน์ วายุภาพ, อนุกรรมการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยี, “สัมมนากฎหมายคุ้มครองข้อมูลส่วนบุคคล”

- ขอบเขตการใช้บังคับ

ก) การดำเนินการใดๆ กับข้อมูลส่วนบุคคลด้วยวิธีการปกติ (manual) และวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติ (electronic or automatic)

ข) ใช้บังคับกับหน่วยงานภาครัฐและภาคเอกชน

- หลักการและสาระสำคัญของกฎหมาย

ก) วางมาตรการเพื่อควบคุมการกระทำที่เกี่ยวกับข้อมูลส่วนบุคคลที่ได้มีการเก็บรวมรวม ครอบครอง ประมวลผล หรือใช้ประโยชน์

ข) กลไกควบคุมที่สำคัญคือ การจัดตั้งคณะกรรมการทำหน้าที่ตรวจสอบ ไต่สวน และลงโทษผู้ใช้ข้อมูลส่วนบุคคลโดยมิชอบ และมีอำนาจออก Code of Practice

3.4 ภาพรวมของกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

บทบัญญัติของต่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนของต่างประเทศที่ได้นำเสนอมาในบทนี้ หากพิจารณาถึงเนื้อหาสาระแล้วจะพบว่าแต่ละประเทศจะมีการบัญญัติเนื้อหาไว้อย่างละเอียดมาก ซึ่งโดยส่วนใหญ่นั้นได้ยึดหลักการตามที่ปรากฏอยู่ในกติการะหว่างประเทศที่ได้รับการยอมรับทั่วไป ความแตกต่างที่สำคัญระหว่างการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในภาครัฐ กับข้อมูลข่าวสารส่วนบุคคลในภาคเอกชน นั้นมีประเด็นอยู่ที่ในภาคเอกชน กฎหมายมักจะบัญญัติให้มีการควบคุมดูแลกันเองระหว่างเอกชนด้วยกัน ทั้งนี้ด้วยคำนึงถึงปัญหาการควบคุมจากภาครัฐอย่างเข้มงวดจะก่อให้เกิดปัญหากระทบต่อการดำเนินงานของภาคเอกชนที่ต้องการความรวดเร็วคล่องตัว ยืดหยุ่น ม ากกว่า และเนื่องจากโดยสภาพสังคมตะวันตกประชาชนมีความรู้สึกห่วงกันในสิทธิความเป็นส่วนตัวสูงมาก ซึ่งเป็นผลมาจากพื้นฐานในการพัฒนาทางประศาสตร์สังคม ที่ยึดมั่นในแนวคิดปัจเจกชนนิยม ฉะนั้นจึงมีความไว้วางใจในการควบคุมกันเอง และด้วยเหตุผลที่ภาคเอกชนเข้มแข็ง โดยไม่ต้ องการให้ภาครัฐเข้ามาแทรกแซงมากนัก รัฐจึงทำหน้าที่ในการกำกับดูแลเอกชนในการวางกรอบกติกาเพื่อให้ปฏิบัติตามกฎเกณฑ์ที่วางไว้ โดยที่ภาพรวมของบทบัญญัติกฎหมายทั้งหลายนี้ก็ตั้งอยู่บนพื้นฐานเดียวกันใน 6 ประการ ดังต่อไปนี้

1. ในการจัดเก็บข้อมูลข่าวสารต้องมีการบอกกล่าว หรือการแจ้ง ซึ่งในบางครั้งอาจหมายถึงการจดทะเบียน หรือการทำเอกสาร หรือการได้ใบอนุญาต ซึ่งหมายถึงการได้รับอำนาจในการดำเนินการจัดเก็บข้อมูลข่าวสาร ซึ่งผู้ดำเนินการ (Data controller) ต้องยื่นเอกสารต่อเจ้าพนักงานเกี่ยวกับการดำเนินการข้อมูลข่าวสารที่ถูกต้อง

2. การคุ้มครองข้อมูลข่าวสารที่เป็นความลับ หรือ Sensitive data เป็นประเด็นที่แต่ละประเทศต้องให้ความคุ้มครองอย่างเคร่งครัด แม้ว่าคำจำกัดความของ Sensitive data จะไม่สามารถกำหนดได้อย่างชัดเจนก็ตาม เช่นในเรื่องเกี่ยวกับการเมือง ลัทธิทางศาสนา แนวทาง

ในการดำเนินชีวิ ต ข้อมูลเกี่ยวกับสุขภาพ การเป็นสมาชิกสหภาพแรงงาน เป็นต้น ซึ่งการเก็บหรือ ประมวลผล อาจมีได้โดยการให้ความยินยอมของเจ้าของข้อมูลอย่างชัดเจน หรืออาจกำหนดว่าไม่สามารถที่จะส่งข้อมูลข่าวสารเหล่านี้ออกนอกประเทศได้ หรืออาจให้ความคุ้มครองที่มากกว่านี้ คือห้ามมิให้มี การดำเนินการใดๆ เกี่ยวกับข้อมูลข่าวสารเหล่านี้เลย เว้นแต่กฎหมายให้อำนาจ ซึ่งข้อมูลข่าวสารเหล่านี้ อาจไม่ได้อยู่ในความคุ้มครองของผู้ดำเนินการ แต่อาจอยู่ในความครอบครองของนายจ้าง ซึ่งได้เก็บข้อมูลข่าวสารของลูกจ้างไว้ เช่น ประวัติการรักษาสุขภาพ หรือข้อมูลข่าวสารที่เกี่ยวกับการทำสัญญา

3. การส่งข้อมูลข่าวสารระหว่างประเทศ (International data transfer or Tran border data flows) เป็นเรื่องที่นานาประเทศให้ความสำคัญและได้คุ้มครองการส่งข้อมูลข่าวสาร โดยส่วนมากจะไม่ยินยอมให้มีการเข้าถึงข้อมูลข่าวสารหรือส่งข้อมูลข่าวสารอ อกไปยังประเทศที่ไม่มีการคุ้มครองข้อมูลข่าวสารในระดับมาตรฐานที่น่าพอใจ เช่น ในกรณีอนุญาตให้มีเสรีในการส่งข้อมูลข่าวสารภายในประเทศสมาชิก EU ไปยังประเทศที่ไม่ได้เป็นสมาชิก และประเทศซึ่งไม่มีมาตรการที่เพียงพอในการคุ้มครองข้อมูลข่าวสาร

4. ส่วนมากของบทบัญญัติที่ คุ้มครองข้อมูลข่าวสารจะเริ่มต้นด้วย ขอบเขตในการคุ้มครอง เช่น การเก็บข้อมูลข่าวสาร ขอบเขตการประมวลผลข้อมูล ที่อาจมีได้ในระยะเวลาที่กำหนด ความชอบธรรม ซึ่งอยู่บนพื้นฐานของการให้ความยินยอม ในการเก็บ ประมวลผล และเปิดเผยข้อมูลข่าวสารของเจ้าของข้อมูล (Data subject) ภาระหน้าที่ในการให้การรับรองว่าข้อมูลข่าวสารดังกล่าวจะได้รับการแก้ไข ปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งต้องทำเพียงพอแก่การยอมรับโดยการกำหนดเป็นนโยบาย และกระบวนการที่เพียงพอ รวมทั้งการมีมาตรการรักษาความปลอดภัยอย่างเพียงพอ ที่จะป้องกันการเข้าถึงข้อมูลข่าวสา รโดยไม่ได้รับอนุญาต โดยเฉพาะอย่างยิ่งข้อมูลข่าวสารที่มีการส่งด้วยวิธีการทางอิเลคทรอนิกส์

5. สิทธิของเจ้าของข้อมูลข่าวสาร ซึ่งได้แก่ สิทธิในการอนุญาตให้ใช้ข้อมูล สิทธิในการเข้าถึงข้อมูลข่าวสารที่เกี่ยวกับตัวเขา สิทธิในการได้รับแจ้งการใช้ข้อมูลข่าวสาร สิทธิใ นการแก้ไขข้อมูลข่าวสารเมื่อพบว่าข้อมูลข่าวสารที่เกี่ยวกับตัวเขามีความผิดพลาด สิทธิในการได้รับการเยียวยาความเสียหาย เมื่อเขาได้รับความเสียหาย

6. การห้ามการกระทำบางอย่าง ในกิจกรรมบางประเภท เพื่อทำให้การคุ้มครองข้อมูลข่าวสารสำเร็จด้วยดี

เนื่องจากกฎเกณฑ์ระหว่ างประเทศที่ได้รับการยอมรับมากที่สุดซึ่งนานาประเทศต่างก็ได้รับเอาแนวทางไปปฏิบัติและบัญญัติเป็นกฎหมายของรัฐตน ก็คือกฎเกณฑ์ของ OECD หรือ Organization for Economic Cooperation and Development หรือองค์การเพื่อความร่วมมือทางด้านเศรษฐกิจและการพัฒนา เรื่อง Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data ซึ่งออกในปี 1980 แต่อย่างไรก็ตามเนื่องจากกฎเกณฑ์ดังกล่าวได้ประกาศใช้ตั้งแต่ปี 1980 จึงอาจไม่ทันสมัยเท่าที่ควร ดังนั้น เมื่อนำหลักเกณฑ์ที่สำคัญๆ ของ Guidelines on the Protection of Privacy and Transborder Data

Flows of Personal Data มาประกอบกับกฎหมายระหว่างประเทศและกฎหมายของประเทศต่างๆ แล้ว จะเห็นได้ว่า หลักเกณฑ์ที่ถือเป็นสาระสำคัญที่จะต้องให้ความสำคัญเพื่อใช้ประกอบในการจัดทำนโยบายส่วนบุคคลมีดังต่อไปนี้

1. หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)

ผู้ประกอบการจะต้องกำหนดหลักเกณฑ์เกี่ยวกับข้อจำกัดในการรวบรวมข้อมูลส่วนบุคคลว่าจะสามารถรวบรวมได้ต่อเมื่อได้ข้อมูลดังกล่าวมาโดยชอบด้วยกฎหมาย (lawful) วิธีการที่เป็นธรรม (fair means) และเหมาะสม (appropriate) ภายใต้การรับรู้หรือความยินยอมจากเจ้าของข้อมูลเท่านั้น ในกรณีที่ข้อมูลส่วนบุคคลดังกล่าวเป็นข้อมูลที่มีความอ่อนไหว การเก็บรวบรวมข้อมูล จะต้องเกี่ยวข้องกับวัตถุประสงค์ที่ระบุ และจะต้องมีกฎระเบียบเป็นพิเศษสำหรับข้อมูลที่อ่อนไหว เช่น ข้อมูลทางการแพทย์ การเงิน ศาสนา การเมือง

2. หลักคุณภาพของข้อมูล (Data Quality Principle)

ผู้ประกอบการจะต้องใช้ข้อมูลส่วนบุคคลภายในขอบวัตถุประสงค์ในการจัดเก็บหรืออาจใช้เพื่อวัตถุประสงค์อื่นได้ตามความจำเป็น โดยข้อมูลดังกล่าวจะต้องเป็นข้อมูลที่มีความถูกต้อง และเป็นปัจจุบัน (up-to-date)

3. หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)

ผู้ประกอบการจะต้องแจ้งวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลให้เจ้าของข้อมูลได้ทราบก่อนการรวบรวมข้อมูล อีกทั้งจะต้องใช้ข้อมูลส่วนบุคคลภายในวัตถุประสงค์ดังกล่าวด้วย ในกรณีที่มีการถ่ายโอนข้อมูลส่วนบุค คลไปยังบุคคลที่สาม ผู้ประกอบการจะต้องแจ้งให้เจ้าของข้อมูลทราบ และจะต้องให้สิทธิเจ้าของข้อมูลในการเลือกว่าจะให้ข้อมูลดังกล่าวหรือไม่

4. หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)

ผู้ประกอบการจะต้องไม่เปิดเผย (disclose) ทำให้แพร่หลาย (made available) หรือใช้เพื่อวัตถุประสงค์อื่นใดนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบก่อนหน้านั้น เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลหรือมีกฎหมายบัญญัติเป็นอย่างอื่น

5. หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)

ผู้ประกอบการจ ะต้องรักษาความปลอดภัยของข้อมูลโดยใช้มาตรการรักษาความปลอดภัยตามสมควร (reasonable security safeguards) เพื่อป้องกันการเข้าถึงข้อมูลโดยปราศจากอำนาจ (unauthorized access), การทำลาย (destruction), ใช้ (use), เปลี่ยนแปลง (modification), หรือการเปิดเผยข้อมูล (disclosure) และไม่ควรเก็บข้อมูลในรูปแบบที่สามารถระบุตัวจ้าของข้อมูลได้ อีกทั้งจะต้องไม่เก็บข้อมูลส่วนบุคคลไว้เป็นระยะเวลานานเกินไป

6. หลักการเปิดเผย (Openness Principle)

ผู้ประกอบการจะต้องประกาศนโยบายเกี่ยวกับการดำเนินการใดๆ ต่อข้อมูลส่วนบุคคลให้ทราบโดยทั่วไป วัตถุประสงค์ในการใช้ข้อมูล รายละเอียดเกี่ยวกับผู้ควบคุมข้อมูล (controller) ถิ่นที่อยู่ผู้ควบคุมเป็นต้น

7. หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

ผู้ประกอบการจะต้องกำหนดให้เจ้าของข้อมูลมีสิทธิในการได้รับการยืนยัน (confirmation) จากผู้ควบคุมข้อมูลว่าผู้ควบคุมข้อมูลมีข้อมูลที่เกี่ยวข้องกับเจ้าของข้อมูลหรือไม่เพียงใด โดยจะต้องได้รับทราบผลการยืนยันภายในเวลาอันสมควร ทั้งนี้ อาจมีการคิดค่าใช้จ่ายในการดำเนินการได้ในอัตราที่เหมาะสม และในกรณีที่ไม่สามารถดำเนินการตามที่เจ้าของข้ อมูลร้องขอข้างต้นก็จะต้องแสดงเหตุผลให้เจ้าของข้อมูลทราบ อีกทั้งบอกกล่าวให้เจ้าของข้อมูลทราบถึงสิทธิในการโต้แย้งการไม่ปฏิบัติตามคำร้องขอดังกล่าว และหากต่อมาปรากฏว่าข้อโต้แย้งของเจ้าของข้อมูลสามารถรับฟังได้ เจ้าของข้อมูลมีสิทธิที่จะขอให้มีการลบ แก้ไข ปรับปรุง หรือทำให้ข้อมูลมีความสมบูรณ์

8. หลักการให้สิทธิเลือกแก่เข้าของข้อมูล (Opt-in Right Principle)

ผู้ประกอบการจะต้องให้สิทธิแก่เจ้าของข้อมูลเลือกว่า ในกรณีการเก็บรวบรวม การใช้ หรือการเปิดเผย ข้อมูลส่วนบุคคลของตนนั้น ผู้ใช้บริการจะอนุญาตให้ผู้ประกอบการเก็บหรือไม่ให้เก็บ จะให้ใช้หรือไม่ให้ใช้ และจะให้เปิดเผยหรือไม่ให้เปิดเผย ข้อมูลส่วนบุคคลของตนนั้น

9. หลักความรับผิดชอบ (Accountability Principle)

ผู้ประกอบการจะต้องมีหน้าที่ในการปฏิบัติการตามหลักการข้างต้นให้ครบถ้วนทุกประการ

สำหรับการจัดทำนโยบายการคุ้มครองข้ อมูลส่วนบุคคลภายใต้ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ในหมวดที่ 2 ว่าด้วย จริยธรรมในการคุ้มครองข้อมูลส่วนบุคคล มาตรา 18 กำหนดว่า “...บุคคลหรือหน่วยงานอาจจัดทำประมวลจริยธรรมเพื่อกำหนดแนวทางในการคุ้มครองข้อมูลส่วนบุคคลก็ได้ ...” จากบ ทบัญญัติดังกล่าวจะเห็นได้ว่ากฎหมายไม่ได้บังคับให้ผู้ประกอบการต้องจัดทำประมวลจริยธรรม เพียงแต่ผู้ประกอบการจะจัดทำหรือไม่ขึ้นอยู่การให้ความสำคัญในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการของผู้ประกอบการเอง และขึ้นอยู่กับนโยบายในการบริหารกิจการของผู้ปร ะกอบการด้วย และร่างพระราชบัญญัติดังกล่าวก็ไม่ได้กำหนดว่าการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลจะต้องมีเนื้อหาสาระอย่างไรด้วย

จากแนวทางของกฎหมายระหว่างประเทศ และกฎหมายของต่างประเทศเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ได้นำเสนอข้างต้น จะเห็นได้ว่า มีหลักก ารสำคัญที่สอดคล้องกันหลายประการ ไม่ว่าจะเป็น หลักความยินยอมของเจ้าของข้อมูล หลักวัตถุประสงค์ในการจัดเก็บ หลักการคุ้มครองข้อมูลส่วนบุคคล หลักการรักษาความปลอดภัย เป็นต้น นอกจากนี้หลักการสำคัญอีกประการคือ หลักการห้ามโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยเฉพาะใ นประเทศที่ไม่ได้มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เท่าเทียม ซึ่งหลักการดังกล่าวส่งผลให้นานาประเทศจะต้องพัฒนาระดับการให้ความคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานทัดเทียมสากล

และหลักการดังกล่าวยังสามารถสร้างและรักษามาตรฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคลให้อยู่ในระดับเดียวกัน ซึ่งจะส่งผลดีความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ของผู้บริโภคทั่วโลกด้วย ทั้งนี้เนื่องจากธุรกรรมทางอิเล็กทรอนิกส์เป็นธุรกรรมมีความเกี่ยวข้องเกี่ยวโยงกันระหว่างประเทศด้วย นั่นเอง

บทที่ 4

กลไกการกำกับดูแลตนเอง (Self – regulation) โดยการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

4.1 ความจำเป็นและประโยชน์ของการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล

การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล ถือเป็นวิธีการหนึ่งของกลไกการกำ กับดูแลตนเอง หรือ Self – Regulation ซึ่งจัดเป็นวิธีการให้คุ้มครองข้อมูลส่วนบุคคลบนธุรกรรมทางอิเล็กทรอนิกส์ที่สามารถช่วยผ่อนคลายความเคร่งครัด หรือความเข้มงวดของกฎเกณฑ์หรือกฎหมายที่ออกโดยรัฐได้ เนื่องจากผู้ประกอบการสามารถที่จะวางหลักเกณฑ์ในทางปฏิบัติสอดคล้องกับการดำเนินงานภายในองค์กรของตนเองมากที่สุด และเป็นการประหยัดต้นทุนในการผลิตหรือการให้บริการที่เกิดขึ้นอันเนื่องมาจากการเปลี่ยนแปลงกฎเกณฑ์หรือกฎหมายที่ออกโดยรัฐได้ด้วย ทั้งนี้ เพื่อให้การประกอบธุรกิจของผู้ประกอบการเป็นไปอย่างราบรื่น และส่งผลกระทบในทางธุรกิ จกับผู้ประกอบการน้อยที่สุด โดยไม่ถือว่าปฏิบัติผิดกฎเกณฑ์หรือกฎหมายที่ออกโดยรัฐ

อย่างไรก็ตาม เนื่องจากการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการไม่ได้ถูกควบคุมโดยกฎหมายหรือองค์กรใด ๆ จึงอาจทำให้การกำหนดนโยบายของผู้ประกอบการต่าง ๆ ไม่ได้มาตรฐานแล ะไม่อาจคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริง ดังนั้น จึงมีความจำเป็นที่รัฐจะต้องมีการกำหนดมาตรการบังคับ (Enforcing) โดยการออกกฎหมายภายในเพื่อควบคุมการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้ประกอบการปฏิบัติตามนโยบายการคุ้มครองข้อ มูลส่วนบุคคลตามที่ตนได้ประกาศไว้ด้วย เพื่อให้นโยบายดังกล่าวสามารถบังคับใช้ได้จริงในทางปฏิบัติอย่างมีประสิทธิภาพ

สำหรับประเทศไทย แม้ว่าขณะนี้ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... จะยังอยู่ในระหว่างกระบวนการนิติบัญญัติ และยังไม่ได้มีผลบั งคับใช้ก็ตาม แต่ผู้ประกอบธุรกิจก็ควรตระหนักถึงการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยอาจจะกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนขึ้น ให้มีความสอดคล้องกับกฎหมายระหว่างประเทศ หรือกฎหมายของประเทศอื่นๆ ที่จัดได้ว่ามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สูง ทั้งนี้เพื่อเป็นการลดภาระของผู้ประกอบการเองในกรณีที่กฎหมายดังกล่าวจะมีผลใช้บังคับในอนาคต อีกทั้งยังเป็นการสร้างความน่าเชื่อถือให้แก่เว็บไซต์ของผู้ประกอบการอีกทางหนึ่งด้วย

สำหรับประโยชน์ที่ผู้ประกอบธุรกิจจะได้รับจากการจัดให้มีกลไกการกำกับดูแลตนเองโดยการจัดทำ นโยบายการคุ้มครองข้อมูลส่วนบุคคลนั้น เนื่องด้วย นโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ได้จัดทำขึ้นเอง โดยมีวัตถุประสงค์เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบถึงนโยบายหรือแนวทางในการบริหาร

จัดการข้อมูลส่วนบุคคล ของตน ดังนั้น การที่ผู้ประกอบธุรกิจจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลบนเว็บไซต์ของตนก็ย่อมแสดงให้เห็นว่า ผู้ประกอบธุรกิจให้ความสำคัญกับการให้ความคุ้มครองข้อมูลส่วนบุคคล อันเป็นการสร้างความเชื่อมั่นให้แก่ลูกค้าหรือผู้ใช้บริการที่เข้าไปใช้บริการในเว็บไซต์ของผู้ประกอบการนั้นเอง ดังนั้น หากผู้ประกอบการสามารถสร้างความเชื่อมั่นให้แก่ผู้บริโภคได้ ก็ย่อมส่งผลดีต่อการพาณิชย์อิเล็กทรอนิกส์โดยรวมได้ และทำให้การพาณิชย์อิเล็กทรอนิกส์มีอัตราการเติบโตตามที่ควรจะเป็นด้วย

4.2 การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กับเครื่องหมายรับรองความน่าเชื่อถือ

แม้ว่าผู้ประกอบการจะมีการจัดทำนโยบายคุ้มครองความเป็นส่วนตัวแล้ว แต่ลูกค้าหรือผู้ใช้บริการอาจยังไม่แน่ใจว่าเจ้าของเว็บไซต์จะปฏิบัติตามนโยบายที่ได้ประกาศไว้หรือไม่ ดังนั้น เพื่อสร้างความน่าเชื่อถือให้เกิดขึ้นกับลูกค้าหรือผู้ใช้บริการ ผู้ประกอบการจึงแสวงหาวิธีการที่จะทำให้ลูกค้าที่เข้ามาใช้บริการเห็นว่าตนจะปฏิบัติตามนโยบายที่ได้มีการประกาศไว้อย่างแน่นอน โดยที่วิธีการหนึ่งที่นิยมใช้กันอย่างมา กก็คือ การขอใช้เครื่องหมายรับรองความน่าเชื่อถือ (Trustmark) ของหน่วยงานหรือองค์กรที่ให้บริการเครื่องหมายดังกล่าว[1]

เครื่องหมายรับรองความน่าเชื่อถือ หมายถึง สัญลักษณ์ หรือเครื่องหมายที่แสดงไว้เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบว่าเว็บไซต์ของผู้ประกอบการนั้นได้ผ่านมาตรฐานการตรวจสอบคุณสมบัติหรือคุณลักษณะต่างๆ ตามมาตรฐานหรือตาม เกณฑ์ที่มีการกำหนดขึ้นโดยองค์กรนั้นๆ แล้ว โดยที่เครื่องหมายรับรองความน่าเชื่อถือ อาจแบ่งออกเป็นหลายประเภทขึ้นอยู่กับวัตถุประสงค์ของการใช้งาน เช่น Reliability Trustmark, Privacy Trustmark, Security Trustmark เป็นต้น โดยที่เครื่องหมายรับรองความน่าเชื่อถือที่รับรองความน่าเชื่อถือในเรื่องการคุ้มครองข้อมูลส่วนบุคคลก็คือ Privacy Trustmark นั้นเอง

ตัวอย่างของข้อกำหนดที่หน่วยงานให้บริการเครื่องหมายแสดงความน่าเชื่อถือกำหนดให้ผู้ประกอบการที่ขออนุญาตใช้เครื่องหมายรับรองความน่าเชื่อถือดังกล่าวทำ เช่น ผู้ประกอบการที่จะขอใช้เครื่องหมายจะต้องเปิดเผยข้อมูลรายการอย่างน้อย ดังนี้[2]

---

[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, Privacy Policy & Trustmark : กลไกการคุ้มครองข้อมูลส่วนบุคคลกับการสร้างความน่าเชื่อถือในการทำ e-Business, (กรุงเทพมหานคร : สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี, 2548), หน้า 13.

[2] *เพิ่งอ้าง*, หน้า 14-15.

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- ชื่อองค์กรหรือหน่วยงานที่เก็บรวบรวม
- ลักษณะการใช้ข้อมูลส่วนบุคคล
- บุคคลภายนอกที่เข้ามาใช้ข้อมูลร่วมด้วย
- ทางเลือกของลูกค้าที่เข้ามาใช้บริการเกี่ยวกับการเก็บรวบรวม กา รใช้หรือการเปิดเผลข้อมูลส่วนบุคคล
- วิธีการรักษาความปลอดภัยที่ใช้เพื่อป้องกับการสูญหาย การใช้ในทางที่ผิด หรือการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลโดยปราศจากอำนาจ
- วิธีการที่ผู้ใช้บริการจะเข้าถึง แก้ไข หรือปรับปรุงข้อมูลส่วนบุคคลของตน

โดยทั่วไปแล้วประโยชน์ของการใช้เครื่องหมายรับรองความน่าเชื่อถือมีดังนี้[3]

1. แสดงให้เห็นว่าเว็บไซต์ของท่าน มีความน่าเชื่อถือ มีแนวปฏิบัติในการดำเนินธุรกิจที่ดี ผ่านการรับรองจากกรมพัฒนาธุรกิจการค้าแล้ว
2. เว็บไซต์ของท่าน มีมาตรฐานเป็นที่ยอมรับในระดับสากล
3. สร้างความแตกต่างและสร้างศักยภาพในการแข่งขันให้กับเว็บไซต์ของท่าน
4. ขยายโอกาสในการสร้างตลาดใหม่ๆ ให้กับสินค้า/บริการของท่าน
5. เป็นการเพิ่มภาพลักษณ์ให้กับเว็บไซต์ของท่าน
6. เพิ่มช่องทางการประชาสัมพันธ์ให้กับเว็บไซต์ของท่าน โดยกรมฯจะประชาสัมพันธ์ผ่านสื่อต่างๆ เพื่อให้ผู้บริโภคตระหนักถึงความสำคัญข องเครื่องหมายรับรองฯ ตลอดจนมีการแสดงรายละเอียดเกี่ยวกับเว็บไซต์ที่ได้รับเครื่องหมายรับรองฯ โดยจัดแบ่งตามประเภทหมวดหมู่สินค้า/บริการ เพื่อให้ผู้บริโภคสามารถค้นหาผ่านเว็บไซต์กรมฯ ได้โดยสะดวก

สำหรับประเทศไทยนั้น เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ เป็นเครื่องหมายรับรองซึ่งออกโดยกรมพัฒนาธุรกิจการค้ากระทรวงพาณิชย์ โดยผู้บริโภคจะมั่นใจได้ว่า ซื้อสินค้า/บริการ จากเว็บไซต์ที่เชื่อถือได้ เว็บไซต์ที่ได้รับเครื่องหมายรับรองฯ จะต้องปฏิบัติหลักเกณฑ์ที่กรมฯ ระบุไว้ หากมีข้อพิพาท หรือประ สบปัญหา ท่านสามารถติดต่อหรือร้องเรียนมายังกรมพัฒนาธุรกิจการค้า เพื่อดำเนินการแก้ไขปัญหานั้นๆ ให้แก่ผู้ประกอบการและผู้บริโภค เครื่องหมายรับรองความน่าเชื่อถือในการประกอบพาณิชย์อิเล็กทรอนิกส์ หรือเรียกสั้นๆ ว่า Trustmark นั้น เกิดขึ้นจากปัญหาที่ว่า ทำอย่างไร จะให้ผู้บริโภคไทยและต่างประเทศหันมาซื้อสินค้า /บริการผ่านอินเทอร์เน็ตเพิ่มมากขึ้น และทำอย่างไรผู้ประกอบการไทย จะเป็นที่ยอมรับและมีความน่าเชื่อถือ กรมพัฒนาธุรกิจการค้ากระทรวงพาณิชย์ จึงได้จัดตั้ง "กองพาณิชย์อิเล็กทรอนิกส์ " ขึ้น เพื่อสนับสนุนให้เกิดการทำพาณิชย์อิเล็กทรอนิกส์และได้ริเริ่ม "โครงการเครื่องหมายรับรองความน่าเชื่อถือในการประกอบ

---

[3] เครื่องหมายรับรองความน่าเชื่อถือในการประกอบพาณิชย์อิเล็กทรอนิกส์ <http://www.trustmarkthai.com/>

ธุรกิจพาณิชย์อิเล็กทรอนิกส์" หรือ Trustmark โดยหลักเกณฑ์ของเครื่องหมาย Trustmark ได้ยึดแนวทางจากองค์กรเครื่องหมายรับรองในระดับสากล อาทิ Asia Trustmark โดย Trustmark เป็นเครื่องหมายรับรองซึ่งออกโดยกรมพัฒนาธุรกิจการค้ากระทรวงพาณิชย์ โดยมีวัตถุประสงค์เพื่อ สร้างความน่าเชื่อถือให้กับผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทยและเสริมสร้างความมั่นใจให้กับผู้บริโภคในการซื้อขายสินค้า /บริการผ่านทางอินเทอร์เน็ต ว่าเว็บไซต์นั้น ได้ผ่านหลักเกณฑ์ที่กรมฯ กำหนด และกรมฯ ให้การรับรองว่า เว็บไซต์นั้นเชื่อถือได้[4]

ตัวอย่างเครื่องหมายรับรองความน่าเชื่อถือที่ออกโดยกรมพัฒนาธุรกิจการค้า

โดยที่หลักเกณฑ์การขอเครื่องหมายรับรองความน่าเชื่อถือของประเทศไทยมีดังนี้

1) คุณสมบัติผู้ขอ Trustmark[5]

1. เป็นนิติบุคคล
2. จดทะเบียนพาณิชย์อิเล็กทรอนิกส์มาแล้ว ไม่น้อยกว่า 6 เดือน
3. เป็นเจ้าของชื่อโดเมนนั้น
4. มีคุณสมบัติตรงตามหลักเกณฑ์ข้อบังคับการขอใช้เครื่องหมายรับรองฯ

2) หลักเกณฑ์การพิจารณาให้เครื่องหมาย Trustmark แก่ผู้ประกอบธุรกิจประกอบด้วยหลักเกณฑ์ 8 ข้อ ได้แก่[6]

1. ความโปร่งใสของผู้ประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ (Operational Transparency) โดยเว็บไซต์ของท่านต้องมีข้อมู ลเบื้องต้นที่จำเป็น เช่น ที่อยู่ หมายเลขโทรศัพท์ วิธีการติดต่อ ฯลฯ เพื่อแสดงความมีตัวตนของท่านและเพื่อให้ผู้บริโภคสามารถติดต่อหรือสอบถามได้

2. การตลาดและประชาสัมพันธ์ (Advertising and Marketing Practices) การโฆษณา การเสนอซื้อหรือขายสินค้าหรือบริการ ในเว็บไซต์ต้องมีรูปแบบที่เหมาะสมไม่ขัดต่อบทบัญญัติแห่งกฎหมาย ความสงบเรียบร้อย หรือศีลธรรมอันดี จะต้องไม่กระทำการ

---

4 *เพิ่งอ้าง* <http://www.trustmarkthai.com/>

5 ข้อบังคับกรมพัฒนาธุรกิจการค้า ว่าด้วยการใช้เครื่องหมายรับรองความน่าเชื่อถือในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ พ.ศ. 2548 มาตรา 5

6 *เพิ่งอ้าง*

หลอกลวงหรือทำให้เกิดความเข้าใจผิดเกี่ยวกับสินค้า /บริการ รวมทั้งการใช้เทคโนโลยีอื่นใดที่ก่อให้เกิดความเข้าใจผิดในสาระสำคัญของสินค้า/บริการ

3. การให้ข้อ มูลของสินค้าและบริการที่ชัดเจนและเพียงพอ (Adequate and Timely Information About Offers) เว็บไซต์ของท่านจะต้องมีข้อมูลที่ชัดเจน เพื่อประกอบการตัดสินใจในเรื่องของข้อมูลของสินค้า / บริการ ราคาสินค้าหรือบริการ (หากมีค่าใช้จ่ายอื่นๆเพิ่มเติม เช่น ภาษี ,ค่าบริการจัดส่ง ฯลฯ ต้องระบุให้ชัดเจน) วิธีการและระยะเวลาในการชำระราคาค่าสินค้า /บริการ ข้อมูลอื่นๆ ที่จำเป็น เช่น เงื่อนไขการรับประกันสินค้า เงื่อนไขการคืนหรือเปลี่ยนสินค้า ฯลฯ

4. การยืนยันการสั่งซื้อและการจัดส่งสินค้าและบริการ (Acknowledgement of Order and Fulfillment) เว็บไซต์ของท่านจะต้องมีระบบทบทวนและยืนยันการสั่งซื้อ และมีทางเลือกในการยกเลิกหรือยืนยันการทำธุรกรรม เว็บไซต์ของท่านควรมีจัดเตรียมแบบฟอร์มการสั่งซื้อและวิธีการกรอกข้อมูลที่ชัดเจน และควรมีใบยืนยันการสั่งซื้อเพื่อให้บริโภคเข้าไปตรวจสอบหรือติดต่อได้ การจัดส่งสินค้า /บริการจะต้องระบุวิธีการและระยะเวลาที่ชัดเจน และดำเนินการจัดส่งภายในระยะเวลาที่กำหนด

5. ระบบความปลอดภัยในการทำธุรกรรม (Transactional Security) เว็บไซต์ของท่านต้องจัดให้มีมาตรการในการรักษาความปลอดภัยในการทำธุรกรรมของผู้ซื้อหรือผู้ขาย โดยมีการรักษาความปลอดภัยของข้อมูลที่มีมาตรฐานเป็นที่ยอมรับ เหมาะสมกับข้อมูลที่มีการจัดเก็บและส่งผ่าน

6. การคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค (Consumer Privacy) เว็บไซต์ของท่าน จะต้องแสดงนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy policy) ในที่ที่ผู้บริโภคสามารถค้นหาได้สะดวก

7. ช่องทางในการติดต่อสื่อสารและรับเรื่องร้องทุกข์ของผู้บริโภค (Consumer Inquiries and Complaints) เว็บไซต์ของท่าน ต้องจัดเตรียมช่องทางการติดต่อสื่อสารรวมถึงการตอบข้อสงสัยและมีกระบวนการในการจัดการข้อร้องเรียนที่เกิดขึ้น และจะต้องมีการตอบสนองข้อร้อง เรียนหรือข้อสอบถาม ภายใน 7 วัน นับแต่วันที่ได้รับข้อร้องเรียนหรือข้อสอบถาม

8. การคุ้มครองสิทธิเด็กและเยาวชน (Protection of Children) กรณีเว็บไซต์ของท่านมีสินค้าหรือบริการอาจมีผลกระทบต่อเด็กหรือเยาวชนจะต้องจัดให้มีข้อความเตือนบนเว็บไซต์ เพื่อให้ความคุ้มครอง สิทธิของเด็กและเยาวชนเช่น การห้ามจำหน่ายสุราและบุหรี่ ให้แก่เด็กอายุไม่เกิน ๑๘ ปี เด็กและเยาวชนที่ยังไม่บรรลุนิติภาวะที่จะซื้อสินค้าหรือบริการต้องได้รับความยินยอมจากผู้ปกครองก่อน ห้ามเด็กและเยาวชนออกไปพบกับคนแปลกหน้าตามลำพังโดยไม่มีผู้ปกครองไปด้วย เป็นต้น

และสำหรับตัวอย่าง ผู้ให้บริการเครื่องหมายรับรองความน่าเชื่อถือของต่างประเทศที่ได้นับความนิยม เช่น BBBOnline, TrustE, VeriSign, Netrust เป็นต้น

ตัวอย่าง เครื่องหมายรับรองความน่าเชื่อของผู้ให้บริการเครื่องหมายรับรองความน่าเชื่อถือรายอื่น ๆ

โดยจะขอยกตัวอย่าง หลักการ พิจารณาให้เครื่องหมาย Trustmark แก่ผู้ประกอบธุรกิจของ BBBOnline ซึ่งมีหลักเกณฑ์ 5 ข้อ ดังนี้[7]

1. หลักการแจ้งสิ่งที่ถูกต้องแท้จริง

ผู้ประกอบการจะต้องไม่จูงใจ หรือทำให้ผู้บริโภคหลงผิด โดยการทำโฆษณาหรือการทำการตลาด โดยอาศัยวิธีการพาณิชย์อิเล็กทรอนิกส์ หรืออาศัยเทคโนโลยีอื่น

2. หลักการเปิดเผยข้อมูล

ผู้ประกอบการต้องเปิดเผยรูปแบบธุรกิจ สินค้า และบริการ ให้แก่ลูกค้าทรับทราบ

3. หลักการรักษาความปลอดภัยของข้อมูล

ผู้ประกอบการจะต้องเก็บรักษาข้อมูลส่วนบุคคลด้วยความระมัด ระวัง ผู้ประกิบการจะต้องประการนโยบายการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสมและเป็นธรรม และผู้ประกอบการจะต้องจัดหามาตรการในการรักษาความปลอดภัยที่มีประสิทธิภาพด้วย

4. หลักการตอบสนองความพึงพอใจของผู้ใช้บริการ

ผู้ประกอบการจะต้องทำให้ลูกค้าหรือผู้ใช้บริการพึง พอใจโดยการรับผิดชอบตามสิ่งที่ตนเองได้ประกาศให้ลูกค้าทราบ ตอบคำถามหรือข้อสงสัยของลูกค้า และทำหน้าที่แก้ไขข้อร้องเรียม รวมทั้งจัดให้มีระบบการระงับข้อพิพาทที่ดี

5. หลักการคุ้มครองเด็กและเยาวชน

ผู้ประกอบการจะต้องให้ความสำคัญกับลูกค้าและผู้ใช้บริการที่เป็นเ ด็กอายุต่ำกว่า 13 โดยจะต้องให้ความดูแลเป็นพิเศษ โดยคำนึงถึงพัฒนาการ วิจารณญาณ และการรับรู้ของเด็กด้วย

อย่างไรก็ตาม เนื่องจากการสำรวจ พบว่าปัญหาในเรื่องมาตรฐานของการใช้ Trustmark ยังคงขาดความชัดเจน และขาดรูปแบบที่มีมาตรฐาน กล่าวคือ ผู้ที่มีหน้าที่ออก Trustmark มีอยู่หลายองค์กร และรูปแบบการให้เครื่องหมายก็มีรูปแบบและวิธีการต่างกัน จึงทำให้การใช้

---

[7] BBBOnline, “BBBOnline : Code of Online Business Practices”, p. 3.

Trustmark ขาดความน่าเชื่อถือ และไม่สามารถสร้างความเชื่อมั่นแก่ผู้บริโภคได้ [8] และในประการสำคัญเมื่อผู้ให้บริการ Trustmark ได้มีการให้ Trustmark แก่ผู้ประกอบการที่ได้ปฏิบัติตามข้อกำหนดและเงื่อนไขแล้ว แต่ผู้ให้บริการ Trustmark บางรายยังคงขาดระบบการจัดการสอดส่องดูแลภายหลังจากที่ได้มีการให้เครื่องหมายแก่ผู้ประกอบการแล้ว ซึ่งอาจก่อให้เกิดปัญหาในกรณีที่ขณะที่ขอรับเครื่องหมายผู้ประกอบการก็ยังคงรักษามาตรฐานการให้ความคุ้มครองความเป็นส่วนตัวได้ตามที่ผู้ให้บริการเครื่องหมายกำหนด แต่ภายหลังที่ผู้ประกอบการได้รับเครื่องหมายแล้ว ผู้ประกอบการอาจไม่ให้ความใส่ใจแก่การรักษามาตรฐานการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจทำให้ระดับความคุ้มครองลดต่ำลงหรือไม่เป็นไปตามมาตรฐานที่ผู้ให้บริการเครื่องหมายกำหนด อันส่งผลกระทบต่อความน่าเชื่อถือทั้งของตัวผู้ประกอบการเอง และของผู้ให้บริการ Trustmark ด้วย

4.3 สถานะทางกฎหมายของนโยบายการคุ้มครองข้อมูลส่วนบุคคลและผลของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล

เนื่องจากนโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้นก็คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ได้จัดทำขึ้นเอง โดยมีวัตถุประสงค์เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบถึงนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของตน การตีความว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลมีสถานะทางกฎหมายอย่างไรก็เป็นเรื่องสำคัญ เพราะในกรณีที่ผู้ประกอบการไม่สามารถคุ้มครองข้อมูลส่วนบุคคลได้ตามนโยบายที่ตนประกาศไว้นั้น ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้เสียหายจะสามารถฟ้องร้องหรือดำเนินการทางกฎหมายอย่างไรต่อผู้ประกอบการได้ และกฎหมายที่มีผลบังคับใช้อยู่จะเพียงพอหรือไม่ที่จะดำเนินการเอาผิดกับผู้ประกอบการนั้นๆ ดังนั้น จึงต้องมีการพิจารณาเสียก่อนว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลมีสถานะทางกฎหมายอย่างไร

เมื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้น คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ได้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อประกาศให้ลูกค้าหรือผู้ใช้บริการทราบถึงนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของตน จึงเปรียบเสมือนเป็นการแสดงเจตนาโดยฝ่ายเดียวของผู้ประกอบการที่จะยินยอมผูกพันตนที่จะปฏิบัติตามนโยบายการคุ้มครองส่วนบุคคลที่ตนกำหนดขึ้น เพื่อให้ลูกค้าหรือผู้ใช้บริการรับทราบถึงการกำหนดนโยบายดังกล่าว ซึ่งจะก่อให้เกิดหน้าที่แก่ผู้ประกอบการที่จะต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ตนได้กำหนดไว้ จากลักษณะทั่วไปของนโยบายการคุ้มครองข้อมูลส่วนบุคคลแสดงให้เห็นว่า มีลักษณะเป็นนิติกรรมฝ่ายเดียวอันเกิดจากการแสดงเจตนาของผู้ประกอบการที่จะ

---

[8] Elisabeth Wentworth, “Online Dispute Resolution : Global Issues and Australian Standards. Toward a global best practice model for B2C online dispute resolution”

ยอมผูกพันตนตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล อันอาจมีลักษณะเป็นได้ทั้ง “คำเสนอ” หรือมีลักษณะเป็นการให้ “คำมั่น” ต่อลูกค้าหรือผู้ใช้บริการของตน ซึ่งทั้ง “คำเสนอ” และ “คำมั่น” ต่างมีลักษณะเป็นการแสดงเจตนาฝ่ายเดียวเช่นกัน ดังนั้น จึงมีความจำ เป็นจะต้องตีความเพื่อให้เกิดความชัดเจนเนื่องจากลักษณะและผลทางกฎหมายของคำเสนอและคำมั่นนั้นมีความแตกต่างกัน

ตามประมวลกฎหมายแพ่งและพาณิชย์บรรพ 2 ว่าด้วยเรื่องสัญญา ไม่ได้บัญญัติ คำจำกัดความของคำว่า “คำเสนอ” เอาไว้ อย่างไรก็ตาม ตามพจนานุกรมศัพท์กฎหมายไทย ได้ให้คำนิยามว่า คำเสนอ หมายถึง การแสดงเจตนาว่าจะกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่งที่บุคคลฝ่ายหนึ่งแจ้งต่อบุคคลอีกฝ่ายหนึ่ง ซึ่งเมื่อได้รับคำสนองจากบุคคลฝ่ายนั้นแล้วก็เกิดมีความผูกพันเป็นสัญญาขึ้นตามกฎหมาย[9] และ

ตาม Black’s Law Dictionary ก็ได้ให้ความหมายของคำเสนอว่าหมายถึง ข้อเสนอที่จะกระทำการหรือชำระเงิน ซึ่งมักจะมีผลสมบูรณ์เมื่อมีการตอบสนอง หรือคำสนองที่กลายเป็นคำเสนอขึ้นใหม่ หรือมีการให้คำมั่นหรือการกระทำ[10]

ลักษณะทั่วไปของคำเสนอมีดังต่อไปนี้

1) เป็นนิติกรรมฝ่ายเดียวที่จะต้องมีผู้รับการแสดงเจตนา

2) เป็นการแสดงเจตนาโดยชัดแจ้งมีความชัดเจนและแน่นอน แต่วิธีการแสดงเจตนาทำคำเสนอนั้น สามารถทำเป็นลายลักษณ์อักษร หรืออยู่ในรูปข้อมูลอิเล็กทรอนิกส์ รวมทั้งอาจแสดงเจตนาโดยวาจาหรือกริยาท่าทางก็ได้

3) เป็นการแสดงเจตนาต่อบุคคลเฉพาะเจาะจงหรือต่อสาธารณชนทั่วไปก็ได้

4) ต้องไม่มีลักษณะเป็นการเลือกปฏิบัติหรือมีสิทธิปฏิเสธ ยกเว้นในกรณีคำเสนออันมีเงื่อนไข

และตามประมวลกฎหมายแพ่งและพาณิชย์ไม่ได้ให้นิยามความหมายของคำว่า “คำมั่น” เอาไว้โดยเฉพาะ แต่ตามพจนานุกรมฉบับราชบัณฑิตยสถาน ก็ได้ให้ความหมายว่าหมายถึง คำรับรองซึ่งบุคคลหนึ่งให้ไว้กับบุคคลอื่นว่าจะกระทำการอย่างใดอย่างหนึ่ง[11] และ

ตาม Black’s Law Dictionary ก็ได้ให้ความหมายของคำมั่นว่าหมายถึง การแสดงเจตนาซึ่งผูกมัดผู้ให้คำมั่นในการที่จะกระทำหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง โดยผู้รับคำมั่นนั้นมีสิทธิที่จะเรียกร้องให้ผู้ให้คำมั่นปฏิบัติการอย่างหนึ่งอย่างใดตามที่ให้คำมั่นได้[12]

---

[9] อรรยา สิงห์สงบ, กฎหมายว่าด้วยสัญญา, (กรุงเทพมหานคร : วิญญูชน), 2546, หน้า 19-22.

[10] A proposal to do a thing or pay amount, usually accompanied by an expected acceptance, counter-offer, return promise or act.

[11] อรรยา สิงห์สงบ, *อ้างแล้ว* เชิงอรรถที่ 9, หน้า 89-90.

และศาสตราจารย์ จิตติ ติงศภัทิย์ ได้ให้หมายเหตุท้ายคำพิพากษาฎีกาที่ 163/2518 ไว้ว่า คำมั่น คือ คำมั่น ไม่ใช่คำเสนอ หมายเหตุท้ายฎีกานี้ชี้ให้เห็นว่า คำมั่นและคำเสนอมีความแตกต่างกัน โดยที่ลักษณะทั่วไปของคำมั่นจะต้องมีลักษณะดังต่อไปนี้

1) เป็นนิติกรรมฝ่ายเดียวอันเกิดจากการแสดงเจตนาของบุคคลโดยฝ่ายเดียว โดยมุ่งผูกพันตนเองตามคำมั่นนั้น

2) ไม่มีกำหนดระยะเวลา ยกเว้น คำมั่นที่มีเงื่อนไขหรือเงื่อนเวลา

3) ก่อให้เกิดหนี้ผูกพันตามคำมั่น

จากความหมายและลักษณะของ “คำเสนอ” และ “คำมั่น” ดังกล่าวข้างต้น จะเห็นได้ว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลย่อมมีสถานะทางกฎหมายเป็น “คำมั่น” ดังนั้น ผลของการที่ผู้ประกอบการได้ประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็คือ ผู้ประกอบการต้องผูกพันตนที่จะต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วน บุคคลที่ตนได้ประกาศไว้นั่นเอง ดังนั้น ในกรณีที่ผู้ประกอบการไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลได้ตามนโยบายที่ตนประกาศไว้นั้น ผู้ประกอบการย่อมอยู่ในฐานะที่เป็นฝ่ายผิดคำมั่น ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้เสียหายจากการที่ข้อมูลส่วนบุคคลของตนถูกนำไปใช้ผิดวัตถุประสงค์ หรือถูกนำไปใช้โดยไม่มีอำนาจ ย่อมสามารถฟ้องร้องหรือดำเนินการทางกฎหมายต่อผู้ประกอบการได้ ในฐานะที่ผู้ประกอบการประพฤติปฏิบัติผิดคำมั่นที่ตนได้ให้ไว้ได้ ซึ่งบทบัญญัติแห่งกฎหมายในเรื่องการแสดงเจตนา ประกอบกับบทบัญญัติว่าด้วย เรื่องละเมิด [13] ที่มีผลบัง คับใช้อยู่นั้นก็สามารถนำมาใช้ดำเนินการเอาผิดกับผู้ประกอบการนั้นๆ ได้

ขอยกตัวอย่างข้อพิพาทที่เกิดขึ้นในต่างประเทศดังนี้[14]

1. Geocities Case[15]

โดยที่ Geocities เป็นเว็บไซต์ที่มีชื่อเสียงซึ่งปัจจุบันคือ Yahoo เนื่องจากในการสมัครใช้บริการเว็บไซต์ Geocities นั้น ลูกค้าหรือผู้ใช้บริการจะต้องกรอกข้อมูลส่วนบุคคลของตนลงในใบสมัคร โดยที่ Geocities เองก็ได้ประกาศว่าตนเองจะใช้ข้อมูลส่วนบุคคลที่ได้รับจากลูกค้าหรือผู้ใช้บริการอย่างจำกัด เพื่อวัตถุประสงค์ที่จำกัดเท่านั้น แต่ต่อมา Geocities ได้ทำการ

---

[12] Promise means a declaration which binds the person who make it, either in honor, conscience, or law, to do or forbear a certain specific act, and which gives to the person to whom made a right to expect or claim the performance of some particular thing.

[13] ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 บัญญัติว่า “ผู้ใดจงใจหรือประมาทเลินเล่อทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่า งใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น”

[14] J.T. Westermeier & Lee J. Plave, Piper Rudnick LLP, E- Business : The E-Business Legal Survival Kit, p. 57.

[15] Geocities, Inc., Docket No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999).

เปิดเผยข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการให้แก่ผู้ประกอบการค้าอื่น ซึ่งเป็นบุคคลที่สาม โดยผู้ประกอบการค้าดังกล่าวได้นำข้อมูลไปใช้เพื่อวัตถุประสงค์ทางการตลาด FTC จึงได้กล่าวหาว่าการกระทำดังกล่าวของ Geocities เป็นการทำผิดต่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ได้กำหนดไว้ และเป็นการละเมิดข้อมูลส่วนบุคคลของลูกค้าด้วย

2. Crowley v. CyberSource Corp.,[16]

โจทก์คือ Crowley จำเลยคือ CyberSource Corp. ซึ่งเป็นคู่สัญญากับ Amazon.com โดย CyberSource ทำหน้าที่ระบุตัวผู้ซื้อสินค้ากับ Amazon.com

โจทก์ฟ้อง Amazon.com ว่าละเมิดต่อนโยบายส่วนบุคคลของ Amazon.com ที่มีการเปิดเผยข้อมูลส่วนบุคคลของโจทก์ให้แก่ CyberSource เพื่อที่จะระบุตัวผู้ซื้อสินค้าทางเว็บไซต์ Amazon.com โดย Amazon.com อ้างว่า ตนเองมีสัญญา Participation Agreement ซึ่งมีข้อตกลงเรื่องการส่งข้อมูลอยู่กับ CyberSource ศาลเห็นว่า Amazon.com ไม่สามารถนำข้อตกลงตามสัญญาดังกล่าวที่ Amazon.com อ้างขึ้น มาใช้เป็นข้อต่อสู้ได้ นับตั้งแต่วันที่ Amazon.com ได้ประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคลแล้ว ซึ่ง Amazon.com ก็จะต้องปฏิบัติตามนโยบายส่วนบุคคลที่ตนประกาศไว้ด้วย

และสำหรับในประเด็นที่ว่า ในกรณีที่ผู้ประกอบการได้กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนไว้ แต่ได้มีการกำหนดข้อยกเว้นหรือข้อจำกัดความรับผิดของตนไว้ด้วยนั้น จะถือได้หรือไม่ว่าลูกค้าหรือผู้ใช้บริการได้ยอมรับด้วยกับข้อยกเว้นหรือข้อจำกัดความรับผิดนั้น และจะถือว่าเป็นธรรมต่อลูกค้าหรือผู้ประกอบการซึ่งเป็นผู้บริโภคหรือไม่ นั้น เห็นว่า เนื่องจากนโยบายการคุ้มครองข้อมูลส่วนบุคคลมีสถานะทางกฎหมายเป็น “คำมั่น” ดังนั้น ในกรณีที่ลูกค้าหรือผู้ใช้บริการเห็นว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการไม่เหมาะสม หรือไม่เป็นธรรม หรือเป็นการจำกัดความรับผิดของตนเองนั้น ทางเลือกของลูกค้าหรือผู้ใช้บริการก็คือการไม่เข้าไปซื้อสินค้า หรือเข้าไปใช้บริการของผู้ประกอบการรายนั้น ทั้งนี้ลูกค้าไม่มีสิทธิที่จะขอแก้ไขหรือไม่ยอมรับในข้อจำกัดความรับผิดของผู้ประกอบการตามที่กำหนดในนโยบายการคุ้มครองข้อมูลส่วนบุคคลได้ เนื่องจากนโยบายการคุ้มครองข้อมูลส่วนบุคคลไม่ได้มีลักษณะเป็นสัญญา เพราะเนื้อหาของนโยบายการคุ้มครองข้อมูลส่วนบุคคลไม่ได้มีการกำหนดหน้าที่ให้แก่ลูกค้าหรือผู้ใช้บริการที่จะต้องปฏิบัติตามกฎเกณฑ์ใดๆ ดังนั้น เนื้อหาของนโยบายการคุ้มครองข้อมูลส่วนบุคคลย่อมไม่อยู่ภายใต้การคุ้มครองของกฎหมายว่าด้วยข้อสัญญาไม่เป็นธรรม ซึ่งจะไม่เหมือนกับ ข้อตกลงและเงื่อนไข หรือ Term and Condition ที่ผู้ประกอบการได้กำหนดในเว็บไซต์ของตน เพราะข้อตกลงและเงื่อนไขจะมีการกำหนดหน้าที่และความรับผิดให้แก่ลูกค้าหรือผู้ใช้บริการด้วย ซึ่งข้อตกลงและ เงื่อนไขดังกล่าวย่อมอยู่ภายใต้การคุ้มครองของกฎหมายว่าด้วยข้อสัญญาไม่เป็นธรรม อย่างไรก็ตาม เนื่องจากลูกค้าหรือผู้ใช้บริการสามารถพิจารณาเนื้อหาที่กำหนดในนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการได้ก่อนที่จะตัดสินใจทำธุรกรรมร่วมกับผู้ประกอบอยู่แล้วนั่นเอง

---

[16] Crowley v. CyberSource Corp., 166 F. Supp.2d 1263 (N.D. Cal. 2001)

4.4 สรุปข้อสาระสำคัญที่ควรกำหนดไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาบทบัญญัติของกฎหมายในบทที่แล้ว และศึกษาคุณสมบัติและหลักเกณฑ์ที่ผู้ให้บริการเครื่องหมายรับรองความน่าเชื่อถือใช้พิจารณาเพื่ออนุญาตให้ผู้ประกอบการใช้เครื่องหมายรับรองความน่าเชื่อถือ จะเห็นได้ว่า สาระสำคัญที่ควรจะมีการกำหนดไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล ได้แก่ประเด็นดังต่อไปนี้[17]

1. ข้อมูลเบื้องต้น
   - ชื่อนโยบายการคุ้มครองความเป็นส่วนตัว
   - วันที่มีการปรับปรุงนโยบายการคุ้มครองความเป็นส่วนตัวล่าสุด
   - เครื่องหมายแสดงความน่าเชื่อถือเกี่ยวกับการคุ้มครองความเป็นส่วนตัว
   - ขอบเขตการใช้บังคับนโยบายคุ้มครองความเป็นส่วนตัว : บอกว่าข้อมูลใดบ้างที่จะตกอยู่ในบังคับของนโยบายการคุ้มครองความเป็นส่วนตัว
   - การแจ้งให้ทราบถึงการเปลี่ยนแปลงของนโยบายการคุ้มครองความเป็นส่วนตัว : หากจะมีการเปลี่ยนแปลงนโยบายก ารคุ้มครองความเป็นส่วนตัวแล้ว จะใช้วิธีการใดในการแจ้งให้ผู้ใช้บริการดังกล่าวทราบ
2. การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล ผู้ประกอบธุรกิจจะต้องให้รายละเอียดว่าตนเก็บข้อมูลอะไรบ้างผ่านทางเว็บไซต์ของตน และข้อมูลที่ถูกเก็บรวบรวมมานั้นจะถูกใช้ไปอย่างไร ทั้งนี้ ต้องระบุด้วยว่าส่วนใดของเว็บไซต์หรือว่าที่เว็บเพจไหนที่มีการเก็บรวบรวมข้อมูล
   - การติดต่อจากทางเว็บไซต์ : ถ้าหากว่าเจ้าของเว็บไซต์จะส่งการติดต่อใดๆ ไปยังผู้ใช้บริการ เจ้าของเว็บไซต์ควรจะบอกกล่าวผู้ใช้บริการได้รู้ตัวก่อทนล่วงหน้า โดยต้องบอกรายละเอียดผู้ใช้บริกา รได้ทราบว่ากรณีใดบ้างที่จะมีการติดต่อไป ไม่ว่าจะเป็นทางอีเมล์ โทรศัพท์ หรือว่าทางจดหมาย นอกจากนี้ หากเจ้าของเว็บไซต์ได้ใช้จอมูลร่วมกับบุคคลภายนอก และบุคคลภายนอกนั้นอาจติดต่อไปยังผู้ใช้บริการ ในกรณีอย่างนี้ก็ต้องระบุเอาไว้ด้วย
   - การใช้คุกกี้ (Cookies) : ถ้าหากเว็บไซต์มีการใช้คุกกี้ก็ต้องระบุเอาไว้ด้วย และต้องบอกด้วยว่าคุกกี้ดังกล่าวเชื่อมโยงกับข้อมูลที่ระบุตัวบุคคลได้หรือไม่ ต้องบอกด้วยว่าใช้เพื่อวัตถุประสงค์ใดและจะมีประโยชน์อย่างไรต่อตัวผู้ใช้บริการ ผู้เข่ามาใช้บริการเว็บไซต์นั้นมีสิทธิที่จะปฏิเสธไม่รับคุกกี้ หรือไม่ และหากไม่รับคุกกี้แล้วจะเกิดผลเช่นใด ในกรณีที่มีการโฆษณาผ่านทางเว็บไซต์ ต้องระบุด้วยว่าโฆษณาดังกล่าวมีคุกกี้หรือไม่ และหากมีคุกกี้แล้วคุกกี้ดังกล่าวมีการเก็บรวบรวมข้อมูลเกี่ยวกับผู้ใช้บริการหรือไม่

---

[17] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับ สำนักงานเลขานุการคณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์, *อ้างแล้ว เชิงอรรถที่ 1*, หน้า 25-40.

- การเก็บข้อมูลพื้นฐานบุคคล (Demographic Information) : ในกรณีที่เว็บไซต์มีการเก็บข้อมูลพื้นฐานบุคคล เช่น เพศ อายุ อาชีพ ระดับการศึกษาเป็นต้น เหล่านี้ก็ต้องระบุการเก็บรวบรวมข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองความเป็นส่วนตัวด้วยและต้องบอกไว้ด้วยว่าข้อมูลดังกล่าวจะถูกใช้ไปอย่างไร มีการให้บุคคลอื่นร่วมใช้ข้อ มูลดังกล่าด้วยหรือไม่

- บันทึกเข้าออก (Log Files) : ถ้าหากเจ้าของเว็บไซต์มีการเก็บบันทึกเข้าออกโดยอัตโนมัติ ตัวอย่างข้อมูลที่เก็บเช่น หมายเลขไอพี (IP Address) ผู้ให้บริการเชื่อมต่ออินเตอร์เน็ต (Internet Service Providers-ISPs) แบะประเภทของโปรแกรมค้นผ่าน (Browser) โดยได้มีการเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่สามารถระบุตัวบุคคลได้ เจ้าของเว็บไซต์ต้องระบุถึงการดำเนินการดังกล่าวเอาไว้ด้วย อีกทั้ง อธิบายให้ทราบด้วยว่าจะมีการใช้ข้อมูลดังกล่าวอย่างไร

- ข้อมูลที่เก็บเป็นข้อมูลที่ต้องให้ หรือเลือกได้ว่าจะให้หรือไม่ให้ก็ ได้ : ควรระบุไว้ด้วยว่าข้อมูลใดเป็นข้อมูลที่ต้องให้และข้อมูลใดเป็นข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้หรือไม่ให้ก็ได้ รวมถึงระบุผลของการให้หรือไม่ให้ข้อมูลดังกล่าวเอาไว้ด้วย

3. หน่วยงานหรือองค์กรที่เก็บข้อมูลผ่านทางเว็บไซต์ ในกรณีที่การดำเนินการของเว็บไซต์เกี่ยวข้องหรือมีความสัมพันธ์เป็นพิเศษกับหน่วยงานหรือองค์กรอื่นด้วย จะต้องมีระบุไว้ในนโยบายคุ้มครองความเป็นส่วนตัว จำเป็นจะต้องมีการกำหนดให้ชัดเจนโดยการระบุลงไปว่าใครคือผู้เก็บรวบรวมหรือผู้ที่รับเอาข้อมูลที่มีการเก็บรวบรวมผ่านทางเว็บไซต์ และใครบ้างเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวได้

4. การใช้ข้อมูลร่วมกับบุคคลอื่น ผู้ประกอบการจะต้องระบุไว้ในนโยบายการคุ้มครองความเป็นส่วนตัวด้วยว่าตนให้บุคคลอื่นๆใช้ข้อมูลที่ตนเก็บรวบรวมมาผ่านทางเว็บไซต์ร่วมด้วยหรือไม่ว่าจะเป็นการใช้ร่วมกันกับบริษัทในเครือ หรือว่ าบริษัทอื่นๆ นอกจากนี้ ในกรณีที่เจ้าของเว็บไซต์ให้บุคคลอื่นทำหน้าที่เป็นตัวกลางให้ เช่น บริษัทบัตรเครดิต เจ้าของเว็บไซต์จะต้องระบุถึงความสัมพันธ์ดังกล่าวไว้ในนโยบายการคุ้มครองความเป็นส่วนตัวด้วย

5. การใช้ข้อมูลร่วมกับผู้ที่ทำหน้าที่ตัวกลาง ในกรณีที่มีการใ ห้บุคคลทีทำหน้าที่เป็นตัวกลางใช้ข้อมูลร่วมด้วย เจ้าของเว็บไซต์จะต้องระบุเอาไว้ในนโยบายการคุ้มครองความเป็นส่วนตัวด้วยว่า ข้อมูลที่ให้บุคคลที่ทำหน้าที่ตัวกลางใช้ร่วมด้วยนั้นจะต้องเป็นไปเพื่อประโยชน์ในการกระจายสินค้าเท่านั้น และบุคคลที่ทำหน้าที่เป็นตัวกลางดัง กล่าวจะต้องไม่เก็บเอาไว้ หรือใช้ข้อมูลดังกล่าวเพื่อการอื่นอีก

6. การรวมข้อมูลที่ได้รับมาจากหลายๆ แหล่งเข้าด้วยกัน ถ้าเว็บไซต์นำข้อมูลที่ได้รับมาโดยตรงจากลูกค้าที่เข้ามาใช้บริการเว็บไซต์ไปรวมเข้ากับข้อมูลของลูกค้าที่ทางเว็บไซต์ได้รับมาจากบุคคลอื่น การที่เว็ บไซต์ทำเช่นนี้จะต้องระบุไว้ในนโยบายคุ้มครองความเป็นส่วนตัวด้วย

7. สิทธิในการเลือกที่จะเป็น Opt-Out หรือ Opt-In เจ้าของเว็บไซต์ต้องระบุไว้ในนโยบายการคุ้มครองความเป็นส่วนตัวด้วยว่าการเก็บรวบรวม การใช้ หรือการดปิดเผยข้อมูลส่วนบุคคลในกรณีใดบ้างที่ลูกค้ามีสิทธิ ที่เลือกว่าจะให้เก็บหรือไม่ให้เก็บ จะให้ใช้หรือไม่ให้ใช้ และจะให้เปิดเผยหรือไม่เปิดเผย ถ้าเป็นกรณีการใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่น หรือว่าเป็นกรณีการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลภายนอก ควรจะใช้วิธีการแบบ Opt-Out นั้น คือ ก่อนที่เว็บไซต์จะใช้ข้อมู ลในลักษณะดังกล่าวเว็บไซต์ได้ให้โอกาสคัดค้านแก่ลูกค้าเจ้าของงาข้อมูล ซึ่งถ้าเจ้าของข้อมูลไม่คัดค้านเว็บไซต์ก็สามารถที่จะใช้ข้อมูลดังกล่าวได้ Opt-In คือ รูปแบบที่ตั้งอยู่บนหลักการที่ว่าจะใช้ข้อมูลส่วนบุคคลได้ก็ต่อเมื่อได้รับความยินยอมโดยชัดแจ้งจาเจ้าของข้อมูลเสียก่อนในทุกครั้งที่ใช้ ซึ่งจะตรงกันข้ามกับ Opt-Out ซึ่งเป็นรูปแบบที่ตั้งอยู่บนหลักการที่ว่าข้อมูลส่วนบุคคลสามารถใช้ได้จนกว่าจะได้รับคำคัดค้านจากเจ้าของข้อมูล

8. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบันซึ่งข้อมูลส่วนบุคคล เจ้าของเว็บไซต์ ทั้งหลายจะต้องกำหนดให้มีวิธีการที่ลูกค้าผู้เข้ามาใช้บริการเว็บไซต์จะสามารถเข้าถึง แก้ไขให้ถูกต้อง หรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเอง

9. การรักษาความปลอดภัยของข้อมูล ผู้ประกอบการมีการตรวจสอบความปลอดภัยของเว็บไซต์ของตนหรือไม่ ถ้ามีบ่อยแค่ไหน และในกรณี ที่ข้อมูลส่วนบุคคลเป็นข้อมูลที่มีความสำคัญ เว็บไซต์ใช้วิธีการรักษาความปลอดภัยอันเป็นที่ยอมรับกันอยู่ทั่วไปในทางการค้า เช่น การเข้ารหัสลับ (Encryption) ในการให้ความคุ้ม ครองความปลอดภัยการส่งข้อมูลดังกล่าวผ่านทางอินเตอร์เน็ตหรือไม่

10. การติดต่อกับทางเว็บไซ ต์ เจ้าของเว็บไซต์จะต้องให้ข้อมูลลูกค้าผู้เข้ามาใช้บริการในการติดต่อกับทางเจ้าของเว็บไซต์ ข้อมูลที่เจ้าของเว็บไซต์ควรจะระบุไว้อย่างน้อยต้องประกอบไปด้วยข้อมูล เช่น ชื่อและที่อยู่, หมายเลขโทรศัพท์, หมายเลขโทรสาร, อีเมล์แอดเดรส

11. นโยบายเกี่ยวกับข้อมูลส่วนบุ คคลของเด็ก (ถ้ามี) ผู้ประกอบธุรกิจจะต้องกำหนดแนวปฏิบัติต่อข้อมูลส่วนบุคคลของเด็กไว้ในนโยบายการคุ้มครองความเป็นส่วนตัวของตนด้วย

ตารางแสดงสาระสำคัญที่ควรกำหนดไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล ซึ่งสอดคล้องตาม OECD Guidelines[18]

ข้อ	สิ่งที่ควรกำหนดไว้ใน นโยบายการคุ้มครองความเป็นส่วนตัว	หลักเกณฑ์ตาม OECD Guidelines
1	ข้อมูลเบื้องต้น - ชื่อนโยบายการคุ้มครองความเป็นส่วนตัว - วันที่มีการปรับปรุงนโยบายการคุ้มครองความเป็นส่วนตัวล่าสุด - กรณีได้รับเครื่องหมายแสดงความน่าเชื่อถือเกี่ยวกับการคุ้มครองความเป็นส่วนตัว - ขอบเขตการใช้บังคับนโยบายการคุ้มครองความเป็นส่วนตัว - การแจ้งให้ทราบถึงการเปลี่ยนแปลงของนโยบายการคุ้มครองความเป็นส่วนตัว	ในส่วนนี้กำหนดขึ้นเพื่อแจ้งให้ผู้ใช้บริการทราบถึงรายละเอียดเกี่ยวกับนโยบายการคุ้มครองความเป็นส่วนตัวเท่านั้นซึ่งสอดคล้องกับ OECD Guidelines ข้อ 6 หลักการเปิดเผย
2	การเก็บรวบรวมข้อมูลส่วนบุคคล - การติดต่อจากทางเว็บไซต์ - การใช้คุกกี้ (Cookies) - การเก็บข้อมูลพื้นฐานบุคคล - บันทึกเข้าออก - ข้อมูลที่เก็บเป็นข้อมูลที่ต้องให้หรือเลือกได้ว่าจะให้หรือไม่ให้ก็ได้	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการทราบว่าผู้ประกอบธุรกิจจะเก็บรวบรวมข้อมูลส่วนบุคคลอะไรด้วยวิธรการใด โดยผู้ใช้บริการสามารถเลือกหรือปฏิเสธรูปแบบการเก็บรวบรวมข้อมูลได้ในบางกรณี ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 1 หลักการรวบรวมข้อมูลอย่างจำกัด,ข้อ 1 หลักคุณภาพของข้อมูล และข้อ 7 หลักการมีส่วนร่วมของข้อมูล
3	หน่วยงานหรือองค์กรที่เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการทราบว่าการดำเนินการของเว็บไซต์นั้นมีส่วนเกี่ยวข้องสัมพันธ์กับองค์กรอื่นด้วย ซึ่งผู้ใช้บริการจะได้ทราบว่าองค์กรใดบ้างที่จะเข้ามามีส่วนร่วมในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลของตน ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 1 หลักการรวบรวมข้อมูลอย่างจำกัด และข้อ 2 หลักคุณภาพของข้อมูล

[18] *เพิ่งอ้าง*, หน้า 21-24.

4	การใช้ข้อมูลร่วมกับบุคคลอื่น	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการทราบว่าจะมีองค์กรใดบ้างที่สามารถเข้ามาใช้ข้อมูลส่วนบุคคลดังกล่าวได้ ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 3 หลักการระบุวัตถุประสงค์ และข้อ 4 หลักการใช้ข้อมูลอย่างจำกัด
5	การใช้ข้อมูลร่วมกับผู้ที่ทำหน้าที่เป็นตัวกลาง	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการทราบว่าผู้ที่ทำหน้าที่เป็นตัวกลางสามารถใช้ข้อมูลส่วนบุคคลดังกล่าวได้เพื่อประโยชน์ในการกระจายสินค้าเท่านั้น ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 4 หลักการใช้ข้อมูลอย่างจำกัด
6	การรวมข้อมูลที่ได้รับมาจากหลายๆแหล่งเข้าด้วยกัน	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการทราบว่าผู้ประกอบธุรกิจได้มีการนำข้อมูลส่วนบุคคลจากหลายแหล่งมารวมเข้าด้วยกันเพื่อประโยชน์ในการประกอบธุรกิจซึ่งสอดคล้องกับ OECD Guidelines ข้อ 7 หลักการมีส่วนร่วมของเจ้าของข้อมูล
7	สิทธิในการเลือกที่จะเป็น Opt-Out หรือ Opt-In	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการสามารถเลือกวิธีการเก็บรวบรวม หรือใช้ข้อมูลได้ ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 7 หลักการมีส่วนร่วมของเจ้าของข้อมูล
8	การเข้าถึง การแก้ไขให้ถูกต้องและการปรับปรุงข้อมูลส่วนบุคคลให้เป็นปัจจุบัน	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการมีส่วนร่วมในการแก้ไขปรับปรุงข้อมูลส่วนบุคคลของตนได้ ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 7 หลักการมีส่วนร่วมของเจ้าของข้อมูล
9	การรักษาความปลอดภัยของข้อมูล	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการทราบถึงแนวปฏิบัติเกี่ยวกับการรักษาความปลอดภัยของข้อมูลที่ผู้ประกอบธุรกิจจัดเตรียมไว้ ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 5 หลักการรักษาความปลอดภัยของข้อมูล
10	การติดต่อกับทางเว็บไซต์	ในส่วนนี้กำหนดขึ้นเพื่อให้ผู้ใช้บริการสามารถติดต่อกับทางเว็บไซต์ได้ในกรณีที่มีปัญหาเกิดขึ้น ซึ่งสอดคล้องกับ OECD Guidelines ข้อ 8 หลักความรับผิดชอบ

11	นโยบายเกี่ยวกับข้อมูลส่วนบุคคลของเด็ก(ถ้ามี)	ในส่วนนี้กำหนดขึ้นเพื่อคุ้มครองผู้ใช้บริการที่เป็นเด็ก ซึ่งอาจจะมีลักษณะเฉพาะในรายละเอียดที่อาจต่างไปจากการเขียนนโยบายการคุ้มครองความเป็นส่วนตัวข้อต่าง ๆข้างต้น

นอกจากนี้ การแสดงนโยบายส่วนบุคคลของผู้ประกอบการก็จะต้องแสดงไว้ในที่ที่ลูกค้าหรือผู้ใช้บริการสามารถเห็นไ ด้ชัดเจนด้วย เพื่อให้ลูกค้าหรือผู้ใช้บริการได้ทราบนโยบายในการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการก่อน ที่ตนเองจะได้เลือกว่าจะทำธุรกรรมร่วมกับผู้ประกอบการหรือไม่ด้วย

4.5 สภาพการณ์ปัจจุบันของการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ผู้ประกอบธุรกิจธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

จากการศึกษาสภาพการณ์ในปัจจุบันเกี่ยวกับแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต โดยการเข้าเยี่ยมชมเว็บไซต์ของธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต จะเห็นได้ว่า ผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตที่มีชื่อเสียงในประเทศไทย ส่วนใหญ่จะมีการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้โดยชัดแจ้ง ดังจะเห็นได้จากตารางแสดงการจัดทำนโยบายการ คุ้มครองข้อมูลส่วนบุคคล ตามที่ปรากฏข้างล่างนี้

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต

No	รายชื่อธนาคารพาณิชย์ สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิต	Website ของธนาคารพาณิชย์ สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิต	นโยบายคุ้มครองความเป็นส่วนตัว Privacy Policy	
			มี	ไม่มี
1	ธนาคารกรุงเทพ จำกัด (มหาชน) BANGKOK BANK PUBLIC COMPANY LTD.	www.bangkokbank.com	√	
2	ธนาคารกรุงไทย จำกัด (มหาชน) KRUNG THAI BANK PUBLIC COMPANY LTD.	www.ktb.co.th	√	
3	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) BANK OF AYUDHYA PUBLIC COMPANY LTD.	www.krungsri.com	√	

4	ธนาคารกสิกรไทย จำกัด (มหาชน) KASIKORNBANK PUBLIC COMPANY LTD.	www.kasikornbank.com	√	
5	ธนาคารทหารไทย จำกัด (มหาชน) TMB BANK PUBLIC COMPANY LTD.	www.tmbbank.com	√	
6	ธนาคารไทยธนาคาร จำกัด (มหาชน) BANKTHAI PUBLIC COMPANY LTD.	www.bankthai.co.th	√	
7	ธนาคารไทยพาณิชย์ จำกัด (มหาชน) THE SIAM COMMERCIAL BANK PUBLIC COMPANY LTD.	www.scb.co.th	√	
8	ธนาคารนครหลวงไทย จำกัด (มหาชน) SIAM CITY BANK PUBLIC COMPANY LTD.	www.scib.co.th	√	
9	บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด THE HONGKONG AND SHANGHAI BANKING CORP., LTD.	www.hsbc.co.th	√	
10	ธนาคารยูโอบี จำกัด (มหาชน) UNITED OVERSEAS BANK (THAI) PUBLIC COMPANY LTD.	www.uob.co.th	√	
11	ธนาคารธนชาต จำกัด (มหาชน) THANACHART BANK PUBLIC COMPANY LTD.	www.thanachartbank.co.th	√	
12	จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน) GE MONEY RETAIL BANK PUBLIC COMPANY LTD.	www.gemoneybank.co.th	√	
13	ซิตี้แบงก์ เอ็น.เอ. CITIBANK, N.A.	www.citibank.co.th	√	
14	บริษัท บัตรกรุงไทย จำกัด (มหาชน) KRUNGTHAI CARD PUBLIC COMPANY LTD.	www.ktc.co.th	√	

หมายเหตุ : สำรวจเมื่อวันที่ 2 มิถุนายน 2550

แต่อย่างไรก็ตาม แม้ว่าผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงินหรือผู้ประกอบธุรกิจบัตรเครดิต จะได้มีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้แล้ว แต่การจัดแสดงนโยบายการคุ้มครองข้อมูลส่วนบุคค ลของผู้ประกอบการบางแห่ง ก็ไม่ได้แสดงไว้ในจุดที่สามารถเห็นได้อย่างชัดเจน ซึ่งอาจจะทำให้ลูกค้าหรือผู้ใช้บริการไม่สามารถทราบได้ว่ามีผู้ประกอบการดังกล่าวมีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ ซึ่งจะได้จัดแสดงไว้ในตารางแสดงการจัดแสดงนโยบายการคุ้มครอง ข้อมูลส่วนบุคคลไว้ในหน้าเว็บเพจตามที่ได้แสดงไว้ในตารางตามที่ปรากฏข้างล่างนี้

ตารางแสดงการจัดแสดงนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ในหน้าเว็บเพจ

No	รายชื่อธนาคารพาณิชย์ สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิต	Website ของธนาคารพาณิชย์ สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิต	การแสดง Privacy Policy ไว้ในตำแหน่งที่เห็นได้ชัด	
			ใช่	ไม่ใช่
1	ธนาคารกรุงเทพ จำกัด (มหาชน) BANGKOK BANK PUBLIC COMPANY LTD.	www.bangkokbank.com	√	
2	ธนาคารกรุงไทย จำกัด (มหาชน) KRUNG THAI BANK PUBLIC COMPANY LTD.	www.ktb.co.th	√	
3	ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) BANK OF AYUDHYA PUBLIC COMPANY LTD.	www.krungsri.com	√	
4	ธนาคารกสิกรไทย จำกัด (มหาชน) KASIKORNBANK PUBLIC COMPANY LTD.	www.kasikornbank.com	√	
5	ธนาคารทหารไทย จำกัด (มหาชน) TMB BANK PUBLIC COMPANY LTD.	www.tmbbank.com	√	
6	ธนาคารไทยธนาคาร จำกัด (มหาชน) BANKTHAI PUBLIC COMPANY LTD.	www.bankthai.co.th	√	
7	ธนาคารไทยพาณิชย์ จำกัด (มหาชน) THE SIAM COMMERCIAL BANK PUBLIC COMPANY LTD.	www.scb.co.th	√	
8	ธนาคารนครหลวงไทย จำกัด (มหาชน) SIAM CITY BANK PUBLIC COMPANY LTD.	www.scib.co.th	√	
9	บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด THE HONGKONG AND SHANGHAI BANKING CORP., LTD.	www.hsbc.co.th	√	
10	ธนาคารยูโอบี จำกัด (มหาชน) UNITED OVERSEAS BANK (THAI) PUBLIC COMPANY LTD.	www.uob.co.th		√
11	ธนาคารธนชาต จำกัด (มหาชน) THANACHART BANK PUBLIC COMPANY LTD.	www.thanachartbank.co.th	√	
12	จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน) GE MONEY RETAIL BANK PUBLIC COMPANY LTD.	www.gemoneybank.co.th	√	
13	ซิตี้แบงก์ เอ็น.เอ. CITIBANK, N.A.	www.citibank.co.th	√	
14	บริษัท บัตรกรุงไทย จำกัด (มหาชน) KRUNGTHAI CARD PUBLIC COMPANY LTD.	www.ktc.co.th	√	

หมายเหตุ : สำรวจเมื่อวันที่ 2 มิถุนายน 2550

4.6 กรณีศึกษา : แนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบธุรกิจธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทย

สำหรับเนื้อหาโดยรวมของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตในประเทศไทยนั้น จากการพิจารณาจะเห็นได้ว่า ยังคงมีเนื้อหาไม่ครบถ้วนและยังไม่ สอดคล้องตามแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล กำหนดไว้ ซึ่งต่อไปจะได้ยกตัวอย่างโดยวิเคราะห์นโยบายคุ้มครองข้อมูลส่วนบุคคลของธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต ดังนี้

1. ธนาคารกรุงเทพ จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารกรุ งเทพ จำกัด (มหาชน)www.bangkokbank.com จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายการรักษาความปลอดภัย”
- มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน ซึ่งมีผลใช้บังคับ
- ไม่ได้กำหนดว่าข้อมูลส่วนบุคคลป ระเภทใดบ้างที่จะทำการจัดเก็บชัดเจน เพียงแต่กล่าวรวมๆ ว่า “ข้อมูลเกี่ยวกับท่าน”
- มีการกำหนดวัตถุประสงค์ในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บ มีการแจ้งอาจว่าจะใช้คุกกี้ แต่คุกกี้จะไม่ทำการเก็บข้อมูลของลูกค้าไว้
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ โดยมีการชี้แจงรายละเอียดถึงรูปแบบและความสามารถของเทคโนโลยีต่างๆ
- เปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกั บบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- กำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สามไว้
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงเทพ จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)	√		
6	หลักการเปิดเผย (Openness Principle)	√		
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)	√		
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

2. ธนาคารกรุงไทย จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารกรุงไทย จำกัด (มหาชน) www.ktb.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายการให้ความคุ้มครองความเป็นส่วนตัว”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน ซึ่งมีผลใช้บังคับ
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้อย่างชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บ และมีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยี
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่น หรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงไทย จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)	√		
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)	√		
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)	√		
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

3. ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) www.krungsri.com จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายการรักษาค วามปลอดภัย”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน
- ไม่ได้กำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้
- ไม่ได้ระบุวัตถุประสงค์ในการจัดเก็บ
- กำหนดเครื่องมือที่ใช้ในระบบแต่ไม่ได้กำหนดเครื่องมือใดบ้างที่เก็บข้อมูลส่วนบุคคล
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่าง ๆ โดยมีการชี้แจงรายละเอียดถึงรูปแบบและความสามารถของเทคโนโลยีต่าง ๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- ไม่ได้มีการแจ้งให้ทราบว่ ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- ไม่ได้กำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)			√
2	หลักคุณภาพของข้อมูล (Data Quality Principle)			√
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)			√
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)			√
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)	√		
6	หลักการเปิดเผย (Openness Principle)	√		
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)			√
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

4. ธนาคารกสิกรไทย จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารกสิกรไทย จำกัด (มหาชน) www.kasikornbank.com จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “Policy”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้อย่างชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บ และมีการระบุระยะเวลาในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บและมีการแจ้งว่าจะใช้คุก กี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- ไม่ได้กำหนดมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ ไว้อย่างชัดเจน
- มีข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารกสิกรไทย จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)	√		
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)	√		
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)	√		
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)			√
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

5. ธนาคารทหารไทย จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารทหารไทย จำกัด (มหาชน) www.tmbbank.com จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่ว นบุคคล ภายใต้ชื่อ “นโยบายของ ธนาคารทหารไทย จำกัด (มหาชน) ด้านการรักษาความลับของลูกค้า”
- มีการแจ้งว่านโยบายฉบับนี้ใช้บังคับตั้งแต่เมื่อใด
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้อย่างชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ใน การจัดเก็บและมีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่าง ๆ โดยคร่าว ๆ
- มีข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อ มูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่น หรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีการแจ้งกรณีที่มีการเปลี่ยนนโยบาย
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารทหารไทย จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)	√		
2	หลักคุณภาพของข้อมูล (Data Quality Principle)	√		
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)	√		
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)	√		
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)	√		
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

6. ธนาคารไทยธนาคาร จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารไทยธนาคาร จำกัด (มหาชน) www.bankthai.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายความเป็นส่วนตัว”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับล่าสุด
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้ไม่ชัดเจนโดยกำหนดว่าจะเก็บ “ข้อมูลเกี่ยวกับผู้ใช้ที่จำเป็น”
- มีการระบุวัตถุประสงค์ในการจัดเก็บ
- ไม่มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บและมีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่าง ๆ โดยคร่าว ๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- ไม่ได้แจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารไทยธนาคาร จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)			√
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

7. ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารไทยพาณิชย์ จำกัด (มหาชน) www.scb.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “มาตรการและวิธีการรักษาความปลอดภัยของข้อมูลผู้ใช้บริการ”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้ อย่างกว้างๆ โดยกำหนดว่า “ข้อมูลของท่าน”
- มีการระบุวัตถุประสงค์ในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บ และมีการแจ้งว่าจะหลีกเลี่ยงการใช้คุกกี้ในการเก็บข้อมูลของลูกค้า
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาควา มปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ โดยมีการชี้แจงรายละเอียดถึงรูปแบบและความสามารถของเทคโนโลยีต่างๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกั บหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารไทยพาณิชย์ จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)			√
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)			√
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

8. ธนาคารนครหลวงไทย จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารนครหลวงไทย จำกัด (มหาชน) www.scib.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายความปลอดภัยและความเป็นส่วนตัว”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน
- ไม่ได้กำหนดว่าข้อมูลประเภทใดบ้างที่จะทำการจัดเก็บไว้อย่างชัดเจน
- ไม่ได้ระบุวัตถุประสงค์ในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บและมีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่าง ๆ โดยมีการชี้แจงรายละเอียดถึงรูปแบบและความสามารถของเทคโนโลยีต่าง ๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- ไม่ได้มีกา รแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- ไม่ได้กำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารนครหลวงไทย จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)	√		
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)			√
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

9. บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด

จากการศึกษาเว็บไซต์ของ บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด www.hsbc.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายเกี่ยวกับสิทธิในความเป็นส่วนตัวของลูกค้าของเอชเอสบีซี”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับปัจจุบัน
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้ โดยระบุเหตุผลและวัตถุประสงค์ในการจัดเก็บ
- มีการกำหนดเครื่องมือที่ใช้ในการจัดเก็บและมีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ โดยมีการชี้แจงรายละเอียดถึงรูปแบบและความสามารถของเทคโนโลยีต่างๆ
- มีข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)	√		
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)	√		
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

10. ธนาคารยูโอบี จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารยูโอบี จำกัด (มหาชน) www.uob.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “ปลอดภัย”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับล่าสุด
- ไม่มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้
- ไม่ได้ระบุวัตถุประสงค์ในการจัดเก็บ
- ไม่ได้กำหนดเครื่องมือที่ใช้ในการจัดเก็บและไม่ได้มีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ โดยคร่าวๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- ไม่ได้มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- ไม่ได้กำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารยูโอบี จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)			√
2	หลักคุณภาพของข้อมูล (Data Quality Principle)			√
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)			√
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)			√
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)			√
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

11. ธนาคารธนชาต จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ ธนาคารธนชาต จำกัด (มหาชน) www.thanachartbank.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายความเป็นส่วนตัว”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับล่าสุด
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้อย่างชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บ
- ไม่ได้กำหนดเครื่องมือที่ใช้ในการจัดเก็บและไม่ได้มีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้า
- ไม่มีการให้สิทธิลูกค้าที่จะเลือกให้หรือไม่ให้ข้อมูลส่วนบุคคล
- ไม่ได้กำหนดมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ ไว้อย่างชัดเจน
- มีข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- ไม่ได้มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- ไม่ได้กำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ธนาคารธนชาต จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)			√
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)	√		
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

12. จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน) www.gemoneybank.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายรักษาความปลอดภัย”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับล่าสุด
- มีการกำหนดประเภทของข้อมูลที่จะทำการจัดเก็บแต่ไม่ชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บไว้คร่าวๆ
- ไม่ได้กำหนดเครื่องมือที่ใช้ในการจัดเก็บ แต่มีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่ได้กำหนดมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้ บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีการให้สิทธิแก่ลูกค้าที่จะเลือกว่าจะให้ข้อมูลขอ งตนหรือไม่ ในกรณีที่จะมีการเปิดเผยข้อมูลต่อบุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)			√
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

13. ซิตี้แบงก์ เอ็น.เอ.

จากการศึกษาเว็บไซต์ของ ซิตี้แบงก์ เอ็น.เอ. www.citibank.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “แนวทางการรักษาข้อมูลความเป็นส่วนตัวของลูกค้า”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับล่าสุด
- มีการกำหนดให้สิทธิแก่ลูกค้าว่าจะให้ข้อมูลส่วนบุคคลของตนหรือไม่ก็ได้
- ไม่ได้กำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้อย่างชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บไว้
- ไม่ได้กำหนดเครื่องมือที่ใช้ในการจัดเก็บและไม่ได้มีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- มีมาตรการรักษาความปลอดภัยของข้อมูลโดยใช้เทคโนโลยีต่างๆ โดยคร่าวๆ
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- ไม่ได้มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- ไม่ได้กำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
ซิตี้แบงก์ เอ็น.เอ. เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

14. บริษัท บัตรกรุงไทย จำกัด (มหาชน)

จากการศึกษาเว็บไซต์ของ บริษัท บัตรกรุงไทย จำกัด (มหาชน) www.ktc.co.th จะเห็นได้ว่า

- ให้ความคุ้มครองข้อมูลส่วนบุคคล ภายใต้ชื่อ “นโยบายการรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการ”
- ไม่มีการแจ้งว่านโยบายฉบับนี้เป็นฉบับล่าสุด
- ไม่ได้กำหนดประเภทของข้อมูลที่จะทำการจัดเก็บไว้อย่างชัดเจน
- มีการระบุวัตถุประสงค์ในการจัดเก็บ
- ไม่ได้กำหนดเครื่องมือที่ใช้ในการจัดเก็บและไม่ได้มีการแจ้งว่าจะใช้คุกกี้ในการเก็บข้อมูลของลูกค้าไว้ด้วย
- ไม่มีมาตรการรักษาความปลอดภัยของข้อมู ลโดยใช้เทคโนโลยีต่างๆ แต่แจ้งว่ามีการจัดทำระบบป้องกันความปลอดภัยของข้อมูล
- ไม่ได้วางข้อกำหนดเปิดโอกาสให้ลูกค้าหรือผู้ใช้บริการเข้าทำการแก้ไขข้อมูลส่วนบุคคลของตน
- มีการแจ้งให้ทราบว่ามีการใช้ข้อมูลร่วมกับบุคคลอื่นหรือใช้ข้อมูลร่วมกับหน่วยงานที่ทำหน้าที่เป็นตัวกลาง
- มีการกำหนดนโยบายสำหรับกรณีที่จะมีการเปิดเผยข้อมูลแก่บุคคลที่สาม
- ไม่มีการให้สิทธิแก่ลูกค้าที่จะเลือกว่าจะให้ข้อมูลของตนหรือไม่
- มีเครื่องหมายรับรองความน่าเชื่อถือ
- มีรายละเอียดเรื่องการติดต่อกับ Webmaster

ตารางแสดงการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
บริษัท บัตรกรุงไทย จำกัด (มหาชน) เปรียบเทียบกับ OECD Guidelines

No	แนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลที่ถือเป็นสาระสำคัญ	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines		
		สอดคล้องมาก	สอดคล้อง	ไม่สอดคล้อง
1	หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)		√	
2	หลักคุณภาพของข้อมูล (Data Quality Principle)		√	
3	หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)		√	
4	หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)		√	
5	หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguard Principle)		√	
6	หลักการเปิดเผย (Openness Principle)		√	
7	หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)		√	
8	หลักความรับผิดชอบ (Accountability Principle)		√	

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

ตารางเปรียบเทียบมาตรฐานการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines
ของผู้ประกอบการธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต

	การปฏิบัติตามแนวทางการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลตาม OECD Guidelines				
	หลัก คุณภาพ ของ ข้อมูล	หลักการระบุ วัตถุประสงค์	หลักการ ใช้ข้อมูล อย่าง จำกัด	หลักการ รักษา ความ ปลอดภัย ของ ข้อมูล	
	√	√	√	√ √	
	√	√ √	√ √	√	
	×	×	×	√ √	
	√	√ √	√ √	×	
	√ √	√ √	√ √	√	
	√	√	√	√	

	✓	✓	×	✓	
	✓	✓	✓	✓ ✓	
	✓	✓ ✓	✓	✓ ✓	
	×	×	×	✓	
	✓	✓	×	✓ ✓	
	✓	✓	✓	×	
	✓	✓	✓	✓	
	✓	✓	✓	✓	

✓ หมายถึง สอดคล้อง

✓ ✓ หมายถึง สอดคล้องมาก

× หมายถึง ไม่สอดคล้อง

หมายเหตุ : สำรวจเมื่อวันที่ 5 มิถุนายน 2550

จากการศึกษาเกี่ยวกับแนวทางการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต โดยการเข้าเยี่ยมชมเว็บไซต์ของธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต จะเห็นได้ว่าผู้ประกอบการทั้งหมดมีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนเองไว้ แต่การจัดแสดงนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการบางแห่ง ก็ไม่ได้แสดงไว้ในจุดที่สามารถเห็นได้อย่างชัดเจน ซึ่งอาจจะทำให้ลูกค้าหรือผู้ใช้บริการไม่สามารถทราบได้ว่ามีผู้ประกอบการดังกล่าวมีการจัดทำนโยบายการ คุ้มครองข้อมูลส่วนบุคคลหรือไม่ และจากการสำรวจเนื้อหาของนโยบายการคุ้มครองข้อมูลส่วนบุคคลพบว่า เนื้อหาของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการที่มีชื่อเสียงในประเทศไทย โดยส่วนมากจะยังคงไม่สอดคล้องกับ OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data 1980 ซึ่งเป็นแนวปฏิบัติที่มีความเป็นสากลและถือเป็นแนวทางที่ได้รับการยอมรับทั่วโลก และเนื่องจากความรู้ความเข้าใจของผู้จัดทำเว็บเพจที่ไม่ได้ทราบถึงเจตนารมณ์อันแท้จริงในการจัดทำนโยบายการคุ้มครองข้อมูลส่ วนบุคคล จึงทำให้การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลยังไม่เป็นไปในทิศทางเดียวกัน โดยสาเหตุประการหนึ่งก็คือ ประเทศไทยยังไม่มีกฎหมายเฉพาะในเรื่องการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลบนพาณิชย์อิเล็กทรอนิกส์อย่างชัดเจน และการขาดองค์กรกลางที่จะทำหน้าที่ค วบคุมดูแลการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล ดังนั้น เพื่อเป็นการแก้ไขปัญหาดังกล่าวจึงต้องมีการบัญญัติกฎหมายเพิ่มเติมให้มีความชัดเจนขึ้น ประกอบกับต้องแก้ไขกฎหมายเดิมที่ใช้ควบคุมธุรกิจประเภทต่างๆ ที่ใช้บังคับอยู่ให้มีความสอดคล้องกับกฎหมายใหม่ด้วย

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

โดยที่ปัญหาความเป็นส่วนตัว ถือเป็นปัญหาที่นานาประเทศต่างให้ความสำคัญ โดยเฉพาะปัญหาเกี่ยวกับการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคล ถือเป็นปัญหาสำคัญที่ผู้บริโภคให้ความสำคัญอย่างมาก เนื่องด้วยพัฒนาการทางเทคโนโลยีทำ ให้ผู้ประกอบการทั้งหลายสามารถเก็บรวบรวมข้อมูลส่วนบุคคล และสามารถเฝ้าติดตามพฤติกรรมในการใช้บริการเว็บไซต์ของลูกค้าได้ โดยลูกค้าหรือผู้ใช้บริการไม่ทราบและไม่ได้ให้ความยินยอมแก่การกระทำดังกล่าว หรือแม้จะมีการให้ความยินยอมแล้วก็อาจจะมีปัญหาการนำข้อมูลส่วนบุคค ลไปใช้เกินขอบเขตที่ได้ให้ความยินยอมไว้ได้ ทั้งนี้ เพื่อนำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในการทำการตลาดของผู้ประกอบการเอง หรือเพื่อประโยชน์ในทางธุรกิจอื่นๆ อันอาจส่งผลกระทบต่อความเป็นส่วนตัวของผู้บริโภค ทำให้ผู้บริโภคขาดความเชื่อถือในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นการทำลายความเชื่อมั่นต่อการพาณิชย์อิเล็กทรอนิกส์โดยรวม และส่งผลกระทบให้ธุรกิจ E-Commerce ไม่เติบโตเท่าที่ควร ดังนั้น เพื่อเป็นการสร้างความเชื่อมั่นให้แก่ผู้บริโภค สิ่งที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์จำเป็นต้อง สร้างขึ้นก็คือ การให้ความสำคัญกับเรื่องการให้ความคุ้มครองความเ ป็นส่วนตัวของข้อมูลส่วนบุคคล ซึ่ง วิธีการที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์สามารถดำเนินการหรือจัดทำได้เอง ก็คือ การสร้างกลไกการกำกับดูแลตนเอง (Self-Regulation) โดยการการจัดทำนโยบายความเป็นส่วนตัวหรือนโยบายการคุ้มครองข้อมูลส่ วนบุคคล หรือ Privacy Policy และการพัฒนาเทคโนโลยี หรือการนำเทคโนโลยีที่สามารถคุ้มครองความปลอดภัยในข้อมูลส่วนบุคคลของผู้บริโภค มาใช้ในการประกอบกิจการของตนนั่นเอง

การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล เป็นวิธีการที่ผู้ประกอบการสามารถ วางหลักเกณฑ์ในทางปฏิบัติ ให้สอดคล้องกับการดำเนินงานภายในองค์กรของตนเอง และเ ป็นเครื่องมืออย่างหนึ่งของผู้บริโภคที่จะใช้ประกอบการพิจารณาเพื่อขอรับบริการจากผู้ประกอบการ กล่าวคือ เมื่อลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้บริโภคได้ทราบถึงนโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการนั้น ๆ แล้ว ลูกค้าก็สามารถที่จะเลือกพิจารณาได้ว่าจะให้ข้อมูลส่วนบุคคลของตนแก่ผู้ประกอบการดังกล่าวหรือไม่ เพียงใด และเนื่องด้วยนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) คือ นโยบายที่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ประกาศให้แก่ลูกค้าหรือผู้ใช้บริการของตน ทราบว่า ผู้ประกอบการมีนโยบายหรือแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลอย่างไร เพื่อให้ลูกค้าหรือผู้ใช้บริการทราบและสามารถใช้พิจารณาตัดสินใจได้ว่าตนจะให้ข้อมูลส่วนบุคคลของตนหรือไม่ หากผู้ประกอบการ

กำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ไม่ได้มาตรฐานและไม่อา จคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริง ลูกค้าหรือผู้ใช้บริการก็มีสิทธิที่จะเลือกไม่ใช้บริการหรือทำธุรกรรมร่วมกับผู้ประกอบการดังกล่าวได้ และในกรณีที่ลูกค้าหรือผู้ใช้บริการประสงค์ที่จะเข้าใช้บริการของผู้ประกอบการ แล้ว ลูกค้าหรือผู้ใช้บริการก็ อาจเกิดข้อกังวลสงสัยว่าข้อมูลส่วนบุคคลของตนจะได้รับความคุ้มครองตามนโยบายที่ผู้ประกอบการกำหนดไว้หรือไม่ และหากไม่ได้รับการปฏิบัติดังเช่นที่ผู้ประกอบการได้ประกาศในนโยบายดังกล่าว ลูกค้าหรือผู้ใช้บริการจะได้รับการคุ้มครองหรือได้รับการเยียวยาอย่างไร ซึ่งข้อกังวลดังกล่าวย่อมได้รับการแก้ไขหากเราสามารถ ตีความ ได้ว่านโยบายการคุ้มครองข้อมูลส่วนบุคคล นั้น มีสถานะทางกฎหมายอย่างไร ซึ่งจากความหมายและลักษณะของ “คำเสนอ” และ “คำมั่น” ที่ได้นำเสนอในบทที่ 4 จะเห็นได้ว่านโยบายการคุ้มครองข้อมูลส่วนบุคคลย่อมมีสถานะทางกฎหมายเป็น “คำมั่น” ดังนั้น ผลของการที่ผู้ประกอบการได้ประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล ก็คือ ผู้ประกอบการต้องผูกพันตนที่จะต้องปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่ตนได้ประกาศไว้นั่นเอง ดังนั้น ในกรณีที่ผู้ประกอบการไม่สามารถให้การคุ้มครองข้อมูลส่วนบุคคลได้ตามนโยบายที่ตนประกาศไว้นั้น ผู้ประกอบการย่อมอยู่ในฐานะที่เป็นฝ่ายผิดคำมั่น ลูกค้าหรือผู้ใช้บริการซึ่งเป็นผู้เสียหายจากการที่ข้อมูลส่วนบุคคลของตนถูกนำไปใช้ผิดวัตถุประสงค์ หรือถูกนำไปใช้โดยไม่มีอำนาจ ย่อมสามารถฟ้องร้องหรือดำเนินการทางกฎหมายต่อผู้ประกอบการได้ ในฐานะที่ผู้ประกอบการประพฤติปฏิบัติผิดคำมั่นที่ตนได้ให้ไว้ได้ ซึ่งบทบัญญัติแห่งกฎหมายในเรื่องการแสดงเจตนา ประกอบกับบทบัญญัติว่าด้วย เรื่องละเมิด ที่มีผลบังคับใช้อยู่นั้นก็สามารถนำมาใช้ดำเนินการเอาผิดกับผู้ประกอบการนั้นๆ ได้

อย่างไรก็ตาม เนื่องจากการจัดทำนโ ยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการไม่ได้ถูกควบคุมโดยกฎหมายหรือองค์กรใดๆ จึงอาจทำให้การกำหนดนโยบายของผู้ประกอบการต่างๆ ไม่ได้มาตรฐานและไม่อาจคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการได้จริง ดังนั้น จึงมีความจำเป็นที่รัฐจะต้องมีการกำหนดมาตร การบังคับ (enforcing) โดยการออกกฎหมายภายในเพื่อควบคุมการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล โดยอาจมีการจัดตั้งองค์กรที่ทำหน้าที่กำกับดูแล (Regulatory) ซึ่งทำหน้าที่ เช่น ควบคุมทางทะเบียน ออกใบอนุญาต ประชาสัมพันธ์ ระงับข้อพิพาท รวมทั้งให้คำปรึกษาแก่ผู้ประ กอบการและผู้บริโภค เป็นต้น ทั้งนี้ เพื่อเป็นการควบคุมผู้ประกอบการให้ปฏิบัติตามนโยบายส่วนบุคคลที่ตนได้ประกาศไว้ อย่างไรก็ตาม ในการควบคุมดูแลการคุ้มครองข้อมูลส่วนบุคคล ของภาคเอกชน รัฐควรจะควบคุมดูแลกิจการเท่าที่จำเป็นเท่านั้น โดยรัฐควรอยู่ในฐานะให้การสนับสนุนแก่ภาคเอกชนให้มีบทบาทนำ เนื่องจากภาคเอกชนจะมีขีดความสามารถในการพัฒนาทางเทคโนโลยีสูงกว่าภาครัฐ ทั้งนี้ เพื่อให้เอกชนมีบทบาทในการพัฒนาด้านเทคโนโลยีอย่างต่อเนื่องโดยไม่ถูกจำกัดโดยกฎเกณฑ์ภาครัฐมากนักนั่นเอง

อนึ่ง สำหรับผู้ประกอบกิจการประเภท ธนาคาร ผู้ประกอบการ บัตรเครดิตและ /หรือสินเชื่อส่วนบุคคล ซึ่งมีการให้บริการทางการเงินในรูปแบบของพาณิชย์อิเล็กทรอนิกส์นั้น

เนื่องจากกิจการประเภทดังกล่าวเป็นกิจการที่กระทบต่อผู้บริโภคจำนวนมาก จะมีความเกี่ยวข้องโดยตรงกับข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ ไม่ว่าจะเป็นข้อมูลส่ วนบุคคลที่มีลักษณะทั่วไป และ /หรือข้อมูลส่วนบุคคลที่มีลักษณะอ่อนไหว เพราะการสมัครเข้ารับบริการหรือการทำธุรกรรมกับผู้ประกอบการรายนั้นๆ ลูกค้าหรือผู้ใช้บริการจะต้องให้ข้อมูลส่วนบุคคลของตนแก่ผู้ประกอบการนั้นๆ เพื่อใช้ประกอบในการสมัครเข้ารับบริการหรือทำธุรกรร มกับผู้ประกอบการรายนั้นๆ ดังนั้น ผู้ประกอบการก็ควรจะต้องมีการกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานในระดับสูง และเป็นมาตรฐานที่สอดคล้องกับแนวทางปฏิบัติที่มีความเป็นสากล เช่น แนวทางปฏิบัติของ OECD แนวทางปฏิบัติของสหประชาชาติ แนวทางปฏิบัติของสหภาพ ยุโรป หรือแนวทางปฏิบัติของประเทศที่มีมาตรฐานการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับสูง เช่น ประเทศสหรัฐอเมริกา หรือประเทศญี่ปุ่น เป็นต้น ดังนั้น เพื่อเป็นการแก้ไขปัญหาดังกล่าวจึงต้องมีการบัญญัติกฎหมายเพิ่มเติมให้มีความชัดเจนขึ้น ประกอบกับต้องแก้ไขกฎหมายเดิมที่ใช้ควบคุมธุรกิจประเภทต่างๆ ที่ใช้บังคับอยู่ให้มีความสอดคล้องกับกฎหมายใหม่ด้วย ทั้งนี้ เพื่อสร้างความน่าเชื่อถือให้เกิดขึ้นต่อผู้ใช้บริการ และสร้างภาพลักษณ์ที่ดีต่อภาพรวมของธุรกิจการเงินการธนาคารของประเทศไทย ซึ่งส่งผลดีต่อสภาพเศรษฐกิจของประเทศต่อไป

5.2 ข้อเสนอแนะทั่วไป

เพื่อเป็นการยกระดับมาตรฐานการการให้ความคุ้มครองข้อมูลส่วนบุคคลขึ้น ภาครัฐและภาคเอกชนควรมีส่วนร่วมในการพัฒนาควบคู่กันไปโดยให้ภาคเอกชนมีบาทบาทนำและภาครัฐมีบทบาทหน้าที่ในการให้การสนับสนุน

1. มาตรการของภาครัฐ

- บัญญัติกฎหมายว่าด้วยการคุ้มค รองข้อมูลส่วนบุคคล โดยกำหนดรูปแบบและสาระสำคัญที่จะต้องกำหนดในการจัดทำน โย บายส่วนบุคคล และเนื่องจาก ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ในหมวดที่ 2 ว่าด้วย จริยธรรมในการคุ้มครองข้อมูลส่วนบุคคล ไม่ได้บังคับ (Enforcing) ให้ผู้ประกอบการต้ องจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล ดังนั้น เพื่อเป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภค โดยรวมจึงควรกำหนดให้ธุรกิจบางประเภท เช่น ธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต จะต้องมีการจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วย ซึ่งรัฐจะต้องทำควบคู่ไปกับ การแก้ไขกฎหมายที่ใช้ควบคุมธุรกิจประเภทต่างๆ เฉพาะฉบับที่มีผลใช้บังคับอยู่ให้มีความสอดคล้องกับกฎหมายใหม่ด้วย

- การจัดตั้งองค์กรอิสระ หรือให้อำนาจแก่องค์กรที่ได้จัดตั้งแล้วเพิ่มเติม เพื่อให้ทำหน้าที่ควบคุมดูแลปัญหาการให้ความคุ้มครองข้อมูลส่วนบุ คคล สำหรับธุรกิจประเภท ธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิตโดยเฉพาะ
- สนับสนุนให้ภาคเอกชนมีบทบาทนำอย่างต่อเนื่องในการพัฒนาเทคโนโลยี เพื่อใช้เป็นเครื่องมือสำคัญในการคุ้มครองผู้บริโภคและสร้างอำนาจต่อรองแก่ผู้บริโภคซึ่งรวมถึง การมีส่วนร่วมของตัวแทนผู้บริโภคในการพัฒนามาตรการในการคุ้มครองข้อมูลส่วนบุคคลให้มี ประสิทธิภาพ รวมถึงกฎเกณฑ์ วิธีการระงับข้อพิพาท และขั้นตอนการเรียกร้องสิทธิของ ผู้บริโภคด้วย
- เผยแพร่ประชาสัมพันธ์เนื้อหา วัตถุประสงค์ของแนวทางการคุ้มครองข้อมูล ส่วนบุคคลให้แพร่หลาย และสนับสนุนให้มีการนำไปใช้ปฏิบัติ รวมทั้ง อำนวยความสะดวกแก่ ผู้บริโภคได้ตรวจดูข้อมูล ความรู้ คำปรึกษา และการให้คำแนะนำในการยื่นข้อร้องเรียนเกี่ยวกับ การคุ้มครองข้อมูลส่วนบุคคล
- สนับสนุนให้เกิดความร่วมมือระหว่างประเทศ โดยการประสานงานกับ เครือข่ายระหว่างประเทศต่างๆ ที่มีอยู่ และเข้าร่วมในการเจรจาเพื่อบรรลุข้อตกลงระหว่างเทศ ในระดับทวิภาคี และหรือระดับพหุภาคี และการดำเนินการอื่นตามที่มีความจำเป็นและตาม ความเหมาะสมเพื่อให้เกิด การร่วมมือกัน ในระดับระหว่างประเทศ เพื่อสร้างความมั่นใจแก่ ผู้บริโภคในการคุ้มครองผู้บริโภค และผู้ประกอบธุรกิจในการดำเนินธุรกิจ

2. มาตรการของภาคเอกชน

- ร่วมกันจัดตั้งองค์กรภาคเอกชนที่ทำหน้าที่รับรองคุณภาพของจัดทำกลไก การกำกับดูแลตนเอง รวมทั้ง ร่วมกันพัฒนาเทค โนโลยีเพื่อเพิ่มความปลอดภัยให้กับข้อมูลส่วน บุคคล รวมถึงการมีส่วนร่วมของตัวแทนของผู้ประกอบการ และตัวแทนของผู้บริโภคในการ พัฒนามาตรการในการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ รวมถึงกฎเกณฑ์ วิธีการ ระงับข้อพิพาท และขั้นตอนการเรียกร้องสิทธิของผู้บริโภคด้วย
- ร่วมกับภาครัฐ เผยแพร่ประชาสัมพันธ์เนื้อหา วัตถุประสงค์ของแนว ทางการคุ้มครองข้อมูลส่วนบุคคลให้แพร่หลาย รวมทั้ง อำนวยความสะดวกแก่ลูกค้าหรือผูใช้ บริการให้สามารถตรวจดูข้อมูล ความรู้ คำปรึกษา และการให้คำแนะนำในการยื่นข้อร้องเรียน เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- ปฏิบัติตามกฎเกณฑ์ที่ภาครัฐกำหนดขึ้น และร่วมมือกับภาครัฐในการ พัฒนากฎหมายให้มีความทันสมัย ให้มีสอดคล้องกับยุคสมัยเพื่อรองรับเทคโนโลยีที่ เจริญก้าวหน้าอย่างไม่หยุดยั้ง ร่วมทั้ง ให้ข้อมูล เบาะแส แก่ภาครัฐ เกี่ยวกับรูปแบบและวิธีการ ละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคล การทุจริตต่างๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลบน ธุรกรรมทางอิเล็กทรอนิกส์ด้วย

5.3 ข้อเสนอแนะสำหรับผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต

แม้ว่าขณะนี้ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ .ศ. ... จะยังอยู่ในระหว่างกระบวนการนิติบัญญัติ และยังไม่ได้มีผลบังคับใช้ก็ตาม แต่ผู้ประกอบธุรกิจ ประเภทธนาคาร สถาบันการเงินและผู้ประกอบธุรกิจบัตรเครดิต ก็ควรตระหนักถึงปัญหาการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยอาจจะกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคลของตนขึ้นให้มีความสอดคล้องกับกฎหมายระหว่างประเทศ หรือกฎหมายของประเทศอื่นๆ ที่จัดได้ว่ามีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สูง ทั้งนี้เพื่อเป็นการลดภาระของผู้ประกอบการเองในกรณีที่กฎหมายดังกล่าวจะมีผลใช้บังคับในอนาคต อีกทั้งยังเป็นการแสดงให้เห็นว่า ผู้ประกอบธุรกิจให้ความสำคัญกับการให้ความคุ้มครองข้อมูลส่วนบุคคล อันเป็นการสร้างความเชื่อมั่นให้แก่ลูกค้าหรือผู้ใช้บริการที่เข้าไปใช้บริการในเว็บไซต์ของผู้ประกอบการนั้นเอง

สำหรับขั้นตอนการจัดทำนโยบาย การคุ้มครองข้อมูลส่วนบุคคลให้มีมาตรฐานนั้น ผู้ประกอบธุรกิจ ประเภท ธนาคาร สถาบันการ เงินและผู้ประกอบธุรกิจบัตรเครดิตจะต้องดำเนินการจัดทำตามขั้นตอนดังต่อไปนี้[1]

1. การสำรวจแนวปฏิบัติต่อข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการที่เป็นอยู่ ซึ่งผู้ประกอบการจะต้องสำรวจรายละเอียดว่า เว็บไซต์ของตนมีการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ ข้อมูลส่วนบุคคล ประเภทใดบ้างที่มีการเก็บรวบรวม มีการเก็บรวบรวมข้อมูลอย่างไร (เก็บจากเจ้าของข้อมูลโดยตรงหรือเก็บจากบุคคลที่สาม ได้มีการเตือนให้เจ้าของข้อมูลทราบถึงการเก็บรวบรวมข้อมูลส่วนบุคคลนั้นหรือไม่ บุคคลใดเป็นผู้ตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้างและจะเก็บร วบรวมอย่างไร มีบุคคลอื่นนอกจากเจ้าของเว็บไซต์ที่เก็บรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์นี้หรือไม่ เพราะเหตุใดจึงต้องมีการเก็บรวบรวมข้อมูลส่วนบุคคล บุคคลใดเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมไป ข้อมูลที่ถูกเก็บรวบรวมไปมีการเปิดเผยต่อบุคคลที่สามหรื อไม่ และหากมีการเปิดเผยไปเพราะเหตุใด ข้อมูลส่วนบุคคลที่

---

[1] กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, Privacy Policy & Trustmark : กลไกการคุ้มครองข้อมูลส่วนบุคคลกับการสร้างความน่าเชื่อถือในการทำ e-Business, (กรุงเทพมหานคร : สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี, 2548), หน้า 16-44.

ถูกเก็บไปถูกเก็บรักษาไว้อย่างไร และเก็บรักษาอย่างไร มีการใช้มาตรฐานหรือแนวทางปฏิบัติที่หน่วยงานอื่นกำหนดในการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคลหรือไม่ เจ้าของข้อมูลมีทางเลือกอย่างไรบ้างเกี่ยวกับการเก็ บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อนุญาตให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตนหรือไม่ กรณีเจ้าของข้อมูลมีการร้องขอใดๆ เกี่ยวกับข้อมูลส่วนบุคคล (ขอให้แก้ไข หรือขอให้ลบทิ้ง) ต้องทำอย่างไร เป็นต้น

2. การสำรวจว่าแนวปฏิบัติต่อข้อมูลส่วนบุคคลเป็นธร รมและเหมาะสมต่อลูกค้าหรือผู้ใช้บริการหรือไม่หรือไม่อย่างไร โดยศึกษาจากแนวปฏิบัติต่อข้อมูลส่วนบุคคลที่เป็นธรรม ซึ่งเป็นที่ยอมรับกันโดยทั่วไปในกลุ่มประเทศสหภาพยุโรป ประเทศสหรัฐอเมริกา หรือประเทศญี่ปุ่น ก็คือ แนวปฏิบัติต่อข้อมูลส่วนบุคคลที่มีองค์ประกอบในเรื่อง การแจ้งให้ทราบ (Notice) ผู้ประกอบการจะต้องแจ้งให้ลูกค้าที่เข้ามาใช้บริการได้รู้ถึงแนวปฏิบัติต่อข้อมูลส่วนบุคคลก่อนที่จะเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้า , การให้ทางเลือก (Choice) ในกรณีที่ผู้ประกอบการจะใช้ข้อมูลเพื่อวัตถุประสงค์อย่างอื่นที่แตกต่างไปจากวัต ถุประสงค์ที่เก็บรวบรวมมา ผู้ประกอบการจะต้องให้ลูกค้ามีสิทธิเลือกว่าจะให้ใช้หรือไม่ให้ใช้ข้อมูลส่วนบุคคล และถ้าจะให้ใช้ข้อมูลได้จะให้ใช้อย่างไร ,การยอมให้เข้าถึง (Access) ผู้ประกอบการต้องยอมให้ลูกค้าตรวจดูและโต้แย้งเกี่ยวกับความถูกต้องสมบูรณ์ของข้อมูลส่วนบุคค ลเกี่ยวกับลูกค้า และการรักษาความปลอดภัย (Security) ผู้ประกอบการต้องใช้วิธีการที่เหมาะสมเพื่อให้ข้อมูลที่เก็บรวบรวมมาจากลูกค้ามีความครบถ้วนถูกต้องและไม่ถูกนำไปใช้โดยไม่ชอบ

3. เพื่อเป็นการสร้างความน่าเชื่อถือให้แก่ลูกค้าหรือผู้ใช้บริการอีกชั้นหนึ่ง ผู้ประกอบกา รควรจะขอรับเครื่องหมายรับรองความน่าเชื่อถือในการคุ้มครองข้อมูลส่วนบุคคล โดยผู้ประกอบการจะต้องสำรวจข้อกำหนดเกี่ยวกับการใช้เครื่องหมายแสดงความน่าเชื่อถือเกี่ยวกับการคุ้มครองความเป็นส่วนตัว โดยจะต้องสำรวจแนวปฏิบัติต่อข้อมูลส่วนบุคคลของตนให้ดีว่าสอดคล้องกับเงื่ อนไขหรือข้อกำหนดขององค์กรออกเครื่องหมายดังกล่าวหรือไม่ หากยังไม่สอดคล้องก็จำเป็นต้องปรับเปลี่ยนให้สอดคล้อง เพื่อให้ตนได้รับอนุญาตให้ใช้เครื่องหมายดังกล่าวด้วย

4. การกำหนดสาระสำคัญที่ควรต้องมีในนโยบายคุ้มครองข้อมูลส่วนบุคคล จะต้องกำหนดให้สอดคล้องกับ Guidelines Governing the Protection of Privacy and Tranborder Data Flows of Personal Data 1980 ตามรายละเอียดที่ได้อธิบายไว้ในบทที่ 4

5. ในการเผยแพร่นโยบายการคุ้มครองข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ ผู้ประกอบการจะต้อง จัดแสดงนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ที่หน้า โฮมเพจ ในตำแหน่งที่สังเกตเห็นได้ง่าย เพื่อที่ลูกค้าหรือผู้ใช้บริการจะได้รับรู้แนวปฏิบัติต่างๆ ก่อนที่จะเข้า

ไปใช้บริการในหน้าอื่นๆ ของเว็บไซต์ อย่างไรก็ตาม หากเจ้าของเว็บไซต์จะจัดทำเพียงให้มีจุดเชื่อมโยง (Link) ที่หน้าโฮมเพจและในทุกหน้าที่มีการเก็บรวบรวมข้อ มูลส่วนบุคคลก็ถือว่ามีความเหมาะสมแล้ว

จากข้อเสนอแนะที่ได้เสนอมาข้างต้น หากผู้ประกอบธุรกิจประเภทธนาคาร สถาบันการเงิน และผู้ประกอบธุรกิจบัตรเครดิตสามารถปฏิบัติได้แล้ว ย่อมทำให้นโยบายการคุ้มครองข้อมูลส่วนบุคคลของผู้ประกอบการที่มีมาตรฐานในระดับสูง และเป็นมาต รฐานที่สอดคล้องกับแนวทางปฏิบัติที่มีความเป็นสากล อันเป็นการสร้างความเชื่อมั่นให้แก่ลูกค้าหรือผู้ใช้บริการที่เข้าไปใช้บริการในเว็บไซต์ของผู้ประกอบการนั้นเอง และหากผู้ประกอบการสามารถสร้างความเชื่อมั่นให้แก่ผู้บริโภคได้ ก็ย่อมส่งผลดีต่อการพาณิชย์อิเล็กทรอนิกส์ โดยรวมของประเทศได้ และทำให้การพาณิชย์อิเล็กทรอนิกส์มีอัตราการเติบโตตามที่ควรจะเป็นด้วย

บรรณานุกรม

หนังสือและบทความในหนังสือ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, Privacy Policy & Trustmark : กลไกการคุ้มครองข้อมูลส่วนบุคคลกับการสร้างความน่าเชื่อถือในการทำ e-Business. พิมพ์ครั้งที่ 1. กรุงเทพมหานคร : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. 2548.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกับสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ , การโอนข้อมูลส่วนบุคคลระหว่างประเทศ . พิมพ์ครั้งที่ 1. กรุงเทพมหานคร : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. 2548.

ชวลิต อัตถศาสตร์ , ไพบูรณ์ อมรภิญโญเกียรติ , พัชรินทร์ ฉัตรวชิระกุล และอิทธินันท์ สุวรรณจูฑะ. กฎหมายไซเบอร์. กรุงเทพมหานคร: ซีเอ็ดยูเคชั่น, 2545.

ชัยวัฒน์ วงศ์วัฒนศานต์ , ทวีศักดิ์ กออนันตกูล และสุรางคณา แก้วจำนงค์ . คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544. กรุงเทพมหานคร: จิรรัชการพิมพ์, 2545.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ , แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล . พิมพ์ครั้งที่ 2. กรุงเทพมหานคร : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. 2546.

อรรยา สิงห์สงบ, กฎหมายว่าด้วยสัญญา. กรุงเทพมหานคร : วิญญูชน. 2546.

เอกสารอื่น ๆ

กิตติพงศ์ กมลธรรมวงศ์, “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข ”. วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ . 2549.

ศิริกุล ภู่พันธ์ , “ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล ”, วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์. 2548.

นคร เสรีรักษ์, “การคุ้มครองข้อมูลส่วนบุคคล : ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย ”. วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต สาขาสหวิทยาการ บัณฑิตวิทยาลัย มหาวิทยาลัยธรรมศาสตร์. 2548.

พินัย ณ นคร . “กฎหมายว่าด้วยพาณิชย์อิเล็กทรอนิกส์และลายมือชื่ออิเล็กทรอนิกส์ .” บทบัณฑิตย์ 56 ตอน 2 2543

_____. “สัญญาทางอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์.” พ.ศ. 2544.” รพี 46 (2546): 47-60

Books

Aunya Singsangob, “Consumer Online Privacy : Right of Individuals in the E-Business Environment”.

BBBOnline, “BBBOnline : Code of Online Business Practices”.

Budnitz, Mark E. Consumers Surfing for Sales in Cyberspace: What Constitutes Acceptance and What Legal Terms and Conditions Bind the Consumer?. 16 Georgia State University Law Review 741 (Summer 2000).

David Banisar, “Privacy and Human Rights : An International Survey of Ptivacy Laws and Developments”, EPIC, 2000.

Elisabeth Wentworth, “Online Dispute Resolution : Global Issues and Australian Standards. Toward a global best practice model for B2C online dispute resolution”

Ferrera, Gerald R., Lichtenstein, Stephen D., Reder, Margo E.K., August, Ray and Schiano, William T. Cyber Law: Text and Cases. Cincinnati, Ohio: West – Thomson Learning, 2001.

Ferguson, Gerald j. and Galvin, Manual Campos. Enforcing Electronic Contracts in the Americas. 15 – SPG International Law Practicum 42 (Spring 2002).

J.T. Westermeier & Lee J. Plave, Piper Rudnick LLP, E- Business : The E-Business Legal Survival Kit,

Malcom Crompton, “What is Privacy”, Privacy and Security in the Information Age Conference, Melbourne, 2001

Mike Markel, “Safe Harbor and Privacy Protection : A Looming Issue for IT Professional”, (Ieee Transaction on Professional Communication, Vol. 49, NO. 1, March 2006)

Official Journal of the European Communities, “Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002”

Reymond Wacks, Personal Information : Privacy and The Law. (London : Oxford, 1993.),

Samual Warren & Louis D. Brandeis, The Right to Privacy. (Harvard Law Review 193, 1980.)

ข้อมูลอิเล็กทรอนิกส์

www.ecommerce.or.th/newsletter/sep01/index.html
www.banprucity.go.th /smartcards/smartcard.html
www.trustmarkthai.com
www.oecd.org
www.consumerinternational.org
www.bbbonline.org
www.fedma.org
www.europa.eu.int
www.ftc.gov
www.privacyrights.org

www.bangkokbank.com

www.ktb.co.th

www.krungsri.com

www.kasikornbank.com

www.tmbbank.com

www.bankthai.co.th

www.scb.co.th

www.scib.co.th

www.hsbc.co.th

www.uob.co.th

www.thanachartbank.co.th

www.ktc.co.th

www.citibank.co.th

www.gemoneybank.co.th

http://coursewares.mju.ac.th/bt454/Chapter5/C1T5_01.htm

ภาคผนวก

ก. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงเทพ จำกัด (มหาชน)

ข. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงไทย จำกัด (มหาชน)

ค. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)

ง. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกสิกรไทย จำกัด (มหาชน)

จ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารทหารไทย จำกัด (มหาชน)

ฉ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารไทยธนาคาร จำกัด (มหาชน)

ช. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

ซ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารนครหลวงไทย จำกัด (มหาชน)

ฌ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด

ญ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารยูโอบี จำกัด (มหาชน)

ฎ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารธนชาต จำกัด (มหาชน)

ฏ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ บริษัท จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน)

ฐ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ซิตี้แบงก์ เอ็น.เอ.

ฑ. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ บริษัท บัตรกรุงไทย จำกัด (มหาชน)

ภาคผนวก ก.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงเทพ จำกัด (มหาชน)

ภาคผนวก ข.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงไทย จำกัด (มหาชน)

ภาคผนวก ค.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)

ภาคผนวก ง.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารกสิกรไทย จำกัด (มหาชน)

ภาคผนวก จ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารทหารไทย จำกัด (มหาชน)

ภาคผนวก ฉ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารไทยธนาคาร จำกัด (มหาชน)

ภาคผนวก ช.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

ภาคผนวก ซ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารนครหลวงไทย จำกัด (มหาชน)

ภาคผนวก ฌ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ
บริษัท ฮ่องกงและเซี่ยงไฮ้แบงกิ้งคอร์ปอเรชั่น จำกัด

ภาคผนวก ญ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ธนาคารยูโอบี จำกัด (มหาชน)

ภาคผนวก ฎ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ

ธนาคารธนชาต จำกัด (มหาชน)

ภาคผนวก ฏ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ บริษัท จีอี มันนี่ เพื่อรายย่อย จำกัด (มหาชน)

ภาคผนวก ฐ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ ซิตี้แบงก์ เอ็น.เอ.

ภาคผนวก ฑ.

นโยบายการคุ้มครองข้อมูลส่วนบุคคลของ บริษัท บัตรกรุงไทย จำกัด (มหาชน)

ประวัติผู้เขียน

ชื่อ – สกุล	**:**	นายธนัท สุวรรณปริญญา
วัน เดือน ปี	**:**	26 มิถุนายน 2524
วุฒิการศึกษา	**:**	ปี 2545 นิติศาสตร์บัณฑิต มหาวิทยาลัยธรรมศาสตร์
		ปี 2546 เนติบัณฑิตไทย
		ปี 2547 รัฐศาสตร์บัณฑิต มหาวิทยาลัยรามคำแหง
ประสบการณ์ทำงาน :		บริษัท กฎหมายกรุงไทย จำกัด
		บริษัท บัตรกรุงไทย จำกัด (มหาชน)