บทที่ 3

หลักการเกี่ยวกับการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูล

จากหลักการที่สำคัญของพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ที่ได้อธิบายถึงไปนั้น ในบทนี้จะทำการศึกษาเนื้อหาและรายละเอียดของหลักการให้ความยินยอมของเจ้าของข้อมูล เนื่องจากเป็นหลักการที่ส่งผลต่อการดำเนินการของธุรกิจข้อมูลเครดิต รวมไปถึงสมาชิก และเจ้าของข้อมูลเป็นอย่างมาก ซึ่งจากการศึกษาจะทำการวิเคราะห์ถึงหลักการของกฎหมาย และแนวทางปฏิบัติตามประกาศของคณะกรรมการคุ้มครองข้อมูลเครดิต เพื่อเป็นการแสดงให้เห็นถึงความเหมาะสมและประสิทธิภาพในทางปฏิบัติของหลักการดังกล่าว รวมไปถึงการศึกษาวิเคราะห์ในเรื่องหลักการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิต เพื่อตอบสนองวัตถุประสงค์ดังกล่าวด้วยเช่นเดียวกัน

1. หลักการและปัญหาเรื่องการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูล

การทำความเข้าใจในหลักการให้ความยินยอมนี้ จะเริ่มต้นจากพิจารณาถึงพัฒนาการและเหตุผลในการกำหนดหลักการดังกล่าวของพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต และการนำหลักการนี้ไปใช้ในทางปฏิบัติจริงโดยบริษัทข้อมูลเครดิต รวมไปถึงถึงการวิเคราะห์ประเด็นในเรื่องวิธีการให้ความยินยอม และระยะเวลาการมีผลบังคับของความยินยอมด้วย

1.1 เหตุผลของกฎหมายในเรื่องการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูล

หลักความยินยอมนั้น เป็นประเด็นที่มีการพิจารณาเปลี่ยนแปลงอยู่หลายครั้งในการพิจารณาร่างพระราชบัญญัติการ

ประกอบธุรกิจข้อมูลเครดิต การอธิบายในที่นี้จะทำ ตามลำ ดับช่วงเวลา ดังนี้

(1) หลักการให้ความยินยอมตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545

1. ในช่วงการยกร่างกฎหมายพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต โดยกระทรวงการคลังร่วมกับธนาคารแห่งประเทศไทย

กระทรวงการคลังได้ทำ การยกร่างพระราชบัญญัตินี้โดยการศึกษาค้นคว้าจากแบบอย่างของประเทศสหรัฐอเมริกา ตามกฎหมาย The Fair Credit Reporting Act จึงทำ ให้หลักการในเรื่องความยินยอมในชั้นนี้นั้น ได้มีการวางหลักไว้ว่า การจัดส่งและการเปิดเผยข้อมูลภายในขอบเขตของการประกอบธุรกิจข้อมูลเครดิตเป็นไปโดยอัตโนมัติ และไม่ต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล ซึ่งมาจากแนวคิดของการประกอบธุรกิจข้อมูลเครดิตในประเทศสหรัฐอเมริกาที่ถือว่า ความยินยอมนั้นได้เกิดขึ้นโดยปริยายเมื่อลูกค้าซึ่งเป็นเจ้าของข้อมูลได้แสดงความประสงค์ในการขอสินเชื่อ เท่ากับเป็นการอนุญาตให้ผู้ให้สินเชื่อตรวจสอบความน่าเชื่อถือของตนได้ โดยการตรวจสอบข้อมูลของลูกค้านั้นต้องเป็นไปภายใต้วัตถุประสงค์ซึ่งได้รับอนุญาตที่บัญญัติไว้ในกฎหมายเท่านั้น เพราะถือว่าวัตถุประสงค์ดังกล่าวเป็นวัตถุประสงค์ที่ลูกค้าได้อนุญาตแล้ว

จากเหตุผลข้างต้น ร่างพระราชบัญญัติจึงทำ หนดให้บริษัทข้อมูลเครดิตสามารถเปิดเผยหรือให้ข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการของตนได้ โดยมีหลักว่าไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล หากเป็นการนำ ไปใช้เพื่อประโยชน์สำ หรับการวิเคราะห์สินเชื่อ หรือเพื่อประโยชน์ในการประกอบธุรกิจตามที่กำหนดไว้ ยกเว้นการเปิดเผยข้อมูลเครดิตกรณีอื่นนอกจากที่กฎหมายกำ หนดไว้ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษร ซึ่งบทบัญญัตินี้ยังส่งผลให้การเปิดเผยข้อมูลที่เป็นไปตามขอบเขตที่กฎหมายกำ หนดนั้น ไม่ถือเป็นการละเมิดหรือไม่เป็นความผิดฐานเปิดเผยความลับ หรือฐานหมิ่นประมาท เนื่องจากเป็นสิ่งที่กระทำ ได้โดยกฎหมายให้อำ นาจไว้ จึงไม่ต้องระบุลงไปในกฎหมายอีก แต่อย่างไรก็ตาม การให้อำ นาจที่จะเปิด

เผยข้อมูลเครดิตทั้งสองกรณีข้างต้น เป็นการให้สิทธิเฉพาะเพื่อวัตถุประสงค์ตามพระราชบัญญัตินี้เท่านั้น มิได้มีผลเป็นการให้สิทธิที่จะเปิดเผยในกรณีอื่นได้ หรือแม้แต่การเปิดเผยโดยจงใจที่จะให้เกิดความเสียหายหรือเสื่อมเสียแก่เจ้าของข้อมูลก็จะไม่ได้รับความคุ้มครอง นอกจากนั้นร่างพระราชบัญญัติฉบับนี้ยังได้กำหนดให้สมาชิกและผู้ใช้บริการจะต้องนำข้อมูลเครดิตไปใช้เพื่อประโยชน์ในการวิเคราะห์สินเชื่อ หรือเพื่อประโยชน์ในการประกอบธุรกิจใดตามที่กำหนดไว้เท่านั้น และห้ามเปิดเผยข้อมูลให้แก่บุคคลอื่นต่อไปอีกด้วย

2. ในช่วงการพิจารณาร่างพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต โดยสภาผู้แทนราษฎร

คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตของสภาผู้แทนราษฎร ได้มีการเปลี่ยนแปลงหลักการในเรื่องความยินยอมนี้ โดยมีวัตถุประสงค์เพื่อให้พระราชบัญญัติดังกล่าวเป็นไปเพื่อการคุ้มครองข้อมูลส่วนบุคคลตามที่มีการศึกษาเปรียบเทียบจาก Data Protection Act 1998 ของประเทศอังกฤษ ซึ่งกำหนดให้การประมวลผลข้อมูลส่วนบุคคลซึ่งรวมไปถึงการเปิดเผยข้อมูลด้วยนั้นจะต้องเป็นไปโดยชอบด้วยกฎหมายและเป็นธรรม โดยหนึ่งในเงื่อนไขของความชอบด้วยกฎหมายในการประมวลผลดังกล่าว ก็คือการที่เจ้าของข้อมูลได้ให้ความยินยอม ตามที่มีการกำหนดไว้ใน Data Protection Principles ในหลักการข้อแรก และ Schedule 2 ของ Data Protection Act

คณะกรรมาธิการฯจึงแก้ไขร่างพระราชบัญญัติ โดยกำหนดให้ในกรณีที่บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการเพื่อวัตถุประสงค์ในการวิเคราะห์สินเชื่อ การรับประกันภัยหรือประกันชีวิต และการออกบัตรเครดิตนั้น โดยหลักแล้วจะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน ยกเว้นการเปิดเผยข้อมูลตามคำสั่งศาลหรือหมายศาล การเปิดเผยเพื่อประโยชน์ในการสอบสวน หรือกรณีอื่นๆ ที่กฎหมายกำหนด ไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูล ส่วนการเปิดเผยข้อมูลเครดิตเพื่อประโยชน์อย่างอื่นหรือเปิดเผยให้แก่

บุคคลอื่นนอกจากที่กฎหมายกำหนด จะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลเป็นการเฉพาะกรณีแต่ละครั้งไป

3. ในช่วงการพิจารณาร่างพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต โดยวุฒิสภา

คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตของวุฒิสภา ได้ทำการแก้ไขหลักในเรื่องความยินยอมของเจ้าของข้อมูลในการที่บริษัทข้อมูลเครดิตเปิดเผยข้อมูลให้แก่สมาชิกและผู้ใช้บริการ จากร่างพระราชบัญญัติฉบับที่สภาผู้แทนราษฎรกำหนดให้ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนนั้น เป็นให้บริษัทข้อมูลเครดิตเปิดเผยข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการได้โดยไม่ต้องได้รับความยินยอม หากเป็นการใช้ข้อมูลเครดิตเพื่อประโยชน์ในการให้สินเชื่อ หรือเป็นไปตามกรณีที่กฎหมายกำหนด ยกเว้นการเปิดเผยเพื่อประโยชน์อย่างอื่นหรือแก่บุคคลอื่นนอกจากที่กฎหมายกำหนดไว้ จะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน เป็นการเฉพาะกรณีเป็นครั้งๆ ไป

แต่เมื่อมีการนำเรื่องเข้าพิจารณาในวุฒิสภา ที่ประชุมวุฒิสภาเห็นว่าเป็นเรื่องที่ควรจะให้สิทธิเจ้าของข้อมูลในการให้ความยินยอมก่อน จึงได้แก้ไขประเด็นดังกล่าวโดยกำหนดหลักในการที่บริษัทข้อมูลเครดิตจะสามารถเปิดเผยข้อมูลเครดิตให้แก่สมาชิกและผู้ใช้บริการ จะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน ยกเว้นการเปิดเผยกรณีอื่นๆ ตามที่กฎหมายกำหนด เช่น การเปิดเผยตามคำสั่งศาลหรือหมายศาล การเปิดเผยเมื่อมีหนังสือจากพนักงานสอบสวน หรือเมื่อมีหนังสือจากหน่วยงานที่มีหน้าที่ในการกำกับดูแลหรือตรวจสอบสถาบันการเงิน เป็นต้นนั้นไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูล ส่วนกรณีที่บริษัทข้อมูลเครดิตประสงค์จะเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการเพื่อประโยชน์อย่างอื่นนอกจากที่กำหนดไว้ จะต้องได้รับความยินยอมจากเจ้าของข้อมูลเป็นการเฉพาะกรณีเป็นครั้งๆ ไป ซึ่งทำให้ร่างพระราชบัญญัติฉบับที่ผ่านสภาผู้แทนราษฎรและวุฒิสภาซึ่งมีการกำหนดให้ต้องมีความยินยอมจากเจ้าของข้อมูลก่อนนี้ เป็นประเด็นที่เปลี่ยนแปลงไปจากหลักการเดิมในการยกร่างพระราชบัญญัติอย่างเห็นได้ชัด

4. ในช่วงการพิจารณาร่างพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต โดยคณะกรรมาธิการร่วมกันของสภาผู้แทนราษฎรและวุฒิสภา

คณะกรรมาธิการร่วมฯ ไม่ได้มีการแก้ไขในประเด็นเรื่องความยินยอมจากร่างที่ผ่านการพิจารณาของวุฒิสภา เนื่องจากเป็นประเด็นที่วุฒิสภาไม่ได้แก้ไขหลักการของสภาผู้แทนราษฎร จึงส่งผลให้ในกรณีที่บริษัทข้อมูลเครดิตเปิดเผยข้อมูลเครดิตให้แก่สมาชิกและผู้ใช้บริการ จะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน สำหรับในส่วนของการเปิดเผยข้อมูลในกรณีอื่นๆ ตามที่กฎหมายกำหนด เช่น การเปิดเผยตามคำสั่งศาลหรือหมายศาล การเปิดเผยเมื่อมีหนังสือจากพนักงานสอบสวน หรือเมื่อมีหนังสือจากหน่วยงานที่มีหน้าที่ในการกำกับดูแลหรือตรวจสอบสถาบันการเงิน รวมไปถึงการเปิดเผยข้อมูลเกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณชนที่วุฒิสภาได้กำหนดเพิ่มเติมนั้น เป็นกรณียกเว้นซึ่งไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนแต่อย่างใด

นอกเหนือจากนั้น คณะกรรมาธิการร่วมฯ ยังได้พิจารณาในประเด็นของการเปิดเผยข้อมูลเครดิตในกรณีอื่นๆ ตามที่กฎหมายกำหนด กล่าวคือ ในกรณีที่เป็น การเปิดเผยข้อมูลหรือให้ข้อมูลเครดิตตามข้อยกเว้นที่กล่าวข้างต้น ซึ่งไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนนั้น ได้มีการบัญญัติเพิ่มเติมในส่วนที่ว่า ให้บริษัทข้อมูลเครดิตแจ้งเป็นหนังสือไปยังเจ้าของข้อมูลเพื่อให้ทราบถึงการเปิดเผยนั้นภายใน 30 วัน นับแต่วันที่เปิดเผยหรือให้ข้อมูลดังกล่าวด้วย หรือกรณีที่เป็นการให้ข้อมูลโดยรวมของสถาบันการเงิน ก็ให้แจ้งแก่สถาบันการเงินนั้นๆ ทราบ และคณะกรรมาธิการร่วมฯ ยังได้ตัดบทบัญญัติที่กำหนดให้บริษัทข้อมูลเครดิตสามารถเปิดเผยข้อมูลให้แก่สมาชิกหรือผู้ได้บริการเพื่อประโยชน์อย่างอื่นนอกจากการวิเคราะห์สินเชื่อตามปกติ โดยจะต้องได้รับความยินยอมจากเจ้าของข้อมูลเป็นการเฉพาะกรณีเป็นครั้งๆ ไป จึงส่งผลให้บริษัทข้อมูลเครดิตไม่สามารถเปิดเผยหรือให้ข้อมูลเครดิตเพื่อประโยชน์อย่างอื่นได้

จากพัฒนาการข้างต้นจึงจะเห็นได้ว่า หลักการในเรื่องความยินยอมนี้เป็นประเด็นที่มีการถกเถียงและแก้ไขตลอดช่วงการพิจารณาร่างพระราชบัญญัติ ในช่วงของการยกร่างกฎหมายได้มี

การกำหนดให้บริษัทข้อมูลเครดิตสามารถเปิดเผยข้อมูลเครดิตได้โดยไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน ซึ่งเป็นการนำหลักมาจากการศึกษาวิเคราะห์เปรียบเทียบกับ The Fair Credit Reporting Act ของประเทศสหรัฐอเมริกา เพื่อให้การดำเนินการต่างๆ ในการประกอบธุรกิจข้อมูลเครดิตเป็นไปได้อย่างสอดคล้องกับทางปฏิบัติตามความเป็นจริง แต่เมื่อมีการพิจารณาของสภาผู้แทนราษฎรที่ได้มีแนวคิดขยายขอบเขตของพระราชบัญญัติให้ไปถึงข้อมูลส่วนบุคคลประเภทอื่น และมีการศึกษาถึง Data Protection Act ของประเทศอังกฤษ จึงได้มีการแก้ไขร่างพระราชบัญญัติโดยนำหลักเรื่องความยินยอมของเจ้าของข้อมูลในการเปิดเผยข้อมูลเครดิตมาบังคับใช้ และถึงแม้คณะกรรมาธิการฯ ของวุฒิสภาจะได้ทำการแก้ไขร่างดังกล่าวเพื่อให้สามารถเปิดเผยข้อมูลเครดิตได้โดยไม่จำเป็นต้องได้รับความยินยอมก็ตาม แต่ที่ประชุมวุฒิสภาก็ยังคงยึดหลักการให้ความยินยอมของเจ้าของข้อมูลดังกล่าว และคณะกรรมาธิการร่วมฯ ก็ยังคงหลักนี้ไว้เช่นเดียวกัน

ดังนั้นในเรื่องหลักความยินยอมของเจ้าของข้อมูลตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 จึงมีการบัญญัติไว้ในมาตรา 20 ซึ่งได้กำหนดให้บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์การให้สินเชื่อ และการออกบัตรเครดิต ทั้งนี้ จะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลเพื่อให้เปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการนั้นก่อน แต่ต่อมาเมื่อได้มีการแก้ไขเพิ่มเติมพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต ครั้งที่ 2 ในพ.ศ.2549 ได้มีการแก้ไขมาตรา 20 จากเดิมเป็นให้บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูล เพื่อประโยชน์ในการวิเคราะห์สินเชื่อและการออกบัตรเครดิต โดยในการเปิดเผยหรือให้ข้อมูลดังกล่าวจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนทุกครั้ง เว้นแต่เจ้าของข้อมูลได้ให้ความยินยอมไว้เป็นอย่างอื่น ทั้งนี้ ตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการกำหนด

จากข้างต้นจึงสามารถสรุปได้ว่า การที่บริษัทข้อมูลเครดิตจะเปิดเผยหรือให้ข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการ จะต้องเป็นไปตามเงื่อนไข ดังนี้

(1) เงื่อนไขเรื่องความยินยอม กล่าวคือ

1) ต้องได้รับความยินยอมจากเจ้าของข้อมูล

2) ต้องได้รับความยินยอมก่อนที่จะทำ การเปิดเผย หรือให้ข้อมูลเครดิต

3) ความยินยอมนั้นต้องเป็นไปตามหลักเกณฑ์ วิธีการและเงื่อนไขที่คณะกรรมการประกาศกำ หนด และ

4) เป็นความยินยอมของเจ้าของข้อมูลที่ได้ให้ความยินยอมแก่บริษัทข้อมูลเครดิตในการเปิดเผยข้อมูลเครดิต

(2) เงื่อนไขเรื่องวัตถุประสงค์ของการใช้ข้อมูล กล่าวคือ

จะต้องเป็นการใช้เพื่อประโยชน์ในการพิจารณาสินเชื่อเท่านั้น

ในการที่พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตกำหนดให้การเปิดเผย หรือให้ข้อมูลเครดิตจะต้องได้รับคำ ยินยอมจากเจ้าของข้อมูลก่อนนั้น แม้ตามหลักการในการร่างกฎหมายนั้นจะต้องการให้ความคุ้มครองแก่เจ้าของข้อมูล เพื่อให้การเปิดเผยข้อมูลเครดิตนั้นจะสามารถกระทำ ได้ก็ต่อเมื่อมีการให้ความยินยอมเป็นหนังสือ ซึ่งเป็นการป้องกันการเปิดเผยข้อมูลโดยมิชอบ แต่ในความเป็นจริงนั้น ควรพิจารณาว่าเจ้าของข้อมูลมีสิทธิเลือกที่จะไม่ให้ความยินยอมได้หรือไม่ ดังตัวอย่างเช่น ในกรณีที่เจ้าของข้อมูลนั้นทำ การขอสินเชื่อจากสถาบันการเงินแห่งหนึ่ง ซึ่งสถาบันการเงินนั้นย่อมจะต้องมีการตรวจสอบข้อมูลเครดิตเพื่อเป็นส่วนหนึ่งของขั้นตอนการพิจารณาสินเชื่อนั้น หากเจ้าของข้อมูลไม่ให้ความยินยอมในการเปิดเผยข้อมูล การขอสินเชื่อก็ย่อมไม่สามารถกระทำ ได้ ดังนั้นจึงเหมือนเป็นการบังคับในทางอ้อมซึ่งเจ้าของข้อมูลนั้นไม่สามารถปฏิเสธการให้ความยินยอมในการเปิดเผยข้อมูลได้นั่นเอง

ในเบื้องต้น จึงควรทำ ความเข้าใจในเรื่องลักษณะของข้อมูลเครดิตเสียก่อน ซึ่งตามหลักการในเรื่องข้อมูลส่วนบุคคลแล้วนั้น สามารถแบ่งข้อมูลออกได้เป็นสองประเภท ได้แก่

1) ข้อมูลข่าวสารทั่วไป (non-sensitive data) เป็นข้อมูลข่าวสารใดๆ ที่เกี่ยวข้องกับบุคคลซึ่งสามารถบ่งชี้เฉพาะตัวบุคคล ได้แก่ ชื่อ นามสกุล ที่อยู่ หมายเลขโทรศัพท์ อายุ วุฒิการศึกษา ตำแหน่งหน้าที่การงาน สถานะ ลักษณะทางกายภาพของบุคคล ข้อมูลใดๆ ดังกล่าวข้างต้นสามารถนำ มาประมวลกันเป็นข้อเท็จจริงที่บ่งชี้ลักษณะเฉพาะตัวบุคคลได้ โดยสภาพของข้อมูลเหล่านี้เป็น

ข้อมูลข่าวสารที่สามารถเปิดเผยต่อสาธารณะได้เป็นเรื่องปกติธรรมดา

2) ข้อมูลข่าวสารประเภทที่มีความละเอียดอ่อน (sensitive data) ได้แก่ข้อมูลข่าวสารที่ถือว่าเป็นเรื่องเฉพาะตัว (intimate) ของบุคคลโดยเฉพาะ เป็นข้อมูลที่เป็นความลับหรือไม่ประสงค์จะให้มีการเปิดเผย ข้อมูลประเภทนี้ ได้แก่ เชื้อชาติ ความเชื่อทางศาสนา ความเชื่อทางการเมือง ข้อมูลเกี่ยวกับสุขภาพ ข้อมูลเกี่ยวกับเพศสัมพันธ์ ข้อมูลเกี่ยวกับการดำเนินคดีทางอาญา คำพิพากษาในคดีอาญา เป็นต้น ซึ่งข้อมูลประเภทนี้มีลักษณะพิเศษกว่าข้อมูลข่าวสารทั่วไป กล่าวคือ ถ้าหากมีการเปิดเผยจะกระทบต่อความรู้สึกของประชาชนทั่วไปในทางลบต่อชื่อเสียงเกียรติคุณหรืออาจก่อให้เกิดอันตรายต่อบุคคลได้[20]

จึงจะเห็นได้ว่า ข้อมูลเครดิตนั้นโดยลักษณะแล้วเป็นข้อมูลข่าวสารทั่วไป มิได้เป็นข้อมูลข่าวสารประเภทที่มีความละเอียดอ่อนแต่อย่างใด ซึ่งในการวิเคราะห์ถึงหลักเกณฑ์และเงื่อนไขในการเปิดเผยข้อมูลเครดิตนั้น จะต้องพิจารณาถึงในประเด็นนี้ควบคู่ไปด้วยเสมอ

อีกประเด็นหนึ่งที่มีความสำคัญต่อการวิเคราะห์ทำความเข้าใจ ก็คือ เรื่องความเป็นอยู่ส่วนตัว (privacy) ซึ่งในการพิจารณานั้นจะต้องแยกออกเป็น ความเป็นอยู่ส่วนตัวเป็นการทั่วไป (privacy in general) และความเป็นอยู่ส่วนตัวในข้อมูลข่าวสาร (information privacy หรือ data privacy) เนื่องจากความเป็นอยู่ส่วนตัวในข้อมูลข่าวสารเป็นเพียงส่วนหนึ่ง (subcategory) ของความเป็นอยู่ส่วนตัวเป็นการทั่วไปเท่านั้น โดยที่ความเป็นอยู่ส่วนตัวเป็นการทั่วไปจะตกอยู่ภายใต้ทฤษฎีเกี่ยวกับการรักษาความลับ (secrecy or confidentiality theory) และทฤษฎีจำกัดการเข้าถึง (restricted access theory) เป็นสำคัญ ในขณะที่ความเป็นอยู่ส่วนตัวในข้อมูลข่าวสารจะต้องอาศัยเกณฑ์ในการพิจารณาจากทฤษฎีการควบคุม (control theory) เพื่อให้สอดคล้องกับสภาพสังคมและเศรษฐกิจในปัจจุบันที่มีการใช้ประโยชน์จากข้อมูลต่างๆ ซึ่งรวม

---

[20] ศิริกุล ภู่พันธ์, "ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล" (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2548), น.83

ถึงข้อมูลส่วนบุคคลอย่างแพร่หลาย ส่งผลให้ไม่อาจเก็บรักษาข้อมูลส่วนบุคคลของตนไว้เป็นความลับอีกต่อไป เนื่องจากจำเป็นต้องยินยอมให้มีการรวบรวม เปิดเผย ประมวลผลข้อมูลดังกล่าวอยู่ตลอดเวลา จึงส่งผลให้การให้ความคุ้มครองในเรื่องความเป็นอยู่ส่วนตัวในปัจจุบันนี้ มีการเปลี่ยนแนวคิดไปจากเดิม กล่าวคือจากการเก็บรักษาข้อมูลไว้เป็นความลับ ไปเป็นความสามารถในการควบคุมการเปิดเผยและการใช้ข้อมูลที่เกี่ยวข้องกับชีวิตมนุษย์เป็นสำคัญ ซึ่งทฤษฎีการควบคุมนี้ มีหลักการสำคัญว่า "บุคคลจะมีความเป็นอยู่ส่วนตัวได้ต่อเมื่อสามารถควบคุมข้อมูลข่าวสารเกี่ยวกับตนเองได้ หรือการควบคุมการเผยแพร่และใช้ข้อมูลและใช้ข้อมูลที่เกี่ยวข้องกับชีวิตตนเองโดยบุคคลอื่น"[21]

ดังนั้น เมื่อทำการวิเคราะห์ถึงหลักการ (concept) ที่แท้จริงของการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูลในการดำเนินการของธุรกิจข้อมูลเครดิตแล้วนั้น จะเห็นได้ว่าข้อมูลเครดิตเป็นข้อมูลที่มีลักษณะเป็นข้อมูลข่าวสารทั่วไป ไม่ใช่ข้อมูลส่วนบุคคลที่มีลักษณะเป็น sensitive data โดยแท้ซึ่งมีลักษณะเป็น human dignity ที่จะต้องมีขอบเขตจำกัดการแทรกแซงของกฎหมาย ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูลในที่นี้เป็นเรื่องของ private autonomy ที่อาจออกกฎระเบียบ (public regulation) มาควบคุมในการให้ข้อมูลดังกล่าวได้ จึงอาจกล่าวได้ว่าการเปิดเผยข้อมูลเครดิต ไม่ใช่เป็นเรื่องของการเปิดเผยข้อมูลของความเป็นส่วนตัว แต่เป็นข้อมูลเกี่ยวกับการเป็นหนี้ของเจ้าของข้อมูลที่มีต่อสถาบันการเงิน ดังนั้น ลักษณะของการเปิดเผยข้อมูลเครดิตจึงอยู่บนพื้นฐานของหลักการ ดังนี้

1. ข้อมูลเครดิตเป็นข้อมูลของการเป็นหนี้ของบุคคลที่เป็นประโยชน์ต่อสาธารณะ (public interest) แก่สถาบันทางการเงิน กล่าวคือ เพื่อใช้ประโยชน์การอนุมัติสินเชื่อว่าบุคคลที่ขอสินเชื่อนั้นมีประวัติการชำระสินเชื่อเป็นอย่างไร และความสามารถในการชำระหนี้ได้หรือไม่

---

[21] ปฏิวัติ อุ่นเรือน, "ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ" (สารนิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2547), น.12-13

2. การเปิดเผยข้อมูลเครดิตตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตนี้ มีวัตถุประสงค์ที่ให้ประโยชน์แก่สถาบันการเงินต่างๆ ที่เป็นสมาชิก เพื่อการใช้ข้อมูลเครดิตของเจ้าของข้อมูลนั้นไปวิเคราะห์การให้สินเชื่อ ซึ่งเป็นไปตามวัตถุประสงค์ของกฎหมายที่ต้องการให้เกิดการใช้ข้อมูลเครดิตให้เป็นประโยชน์ในการวิเคราะห์สินเชื่อของสถาบันการเงินที่เป็นสมาชิก เพื่อให้เกิดการให้สินเชื่อที่มีเสถียรภาพ ซึ่งจะส่งผลดีต่อเศรษฐกิจโดยรวมของประเทศนั่นเอง

3. หลักการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูล จึงเป็นเพียงการเคารพสิทธิของเจ้าของข้อมูลในการที่เจ้าของข้อมูลจะได้รับรู้ (right to be informed) ว่าข้อมูลของตนนั้นจะถูกนำ ไปใช้เพื่อประโยชน์ในการวิเคราะห์สินเชื่ออย่างไร การให้ความยินยอมในลักษณะนี้จึงเป็นการที่เจ้าของข้อมูลได้รับข้อมูลอย่างเพียงพอแล้วว่า ข้อมูลของตนจะถูกใช้ในทางใดเพื่อวัตถุประสงค์ใด จึงแสดงเจตนายินยอมหรือยอมรับในทางข้อเท็จจริง หลักการในการที่จะต้องได้รับความยินยอมตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตจึงไม่ใช่เป็นหลักการในการคุ้มครองความเป็นอยู่ส่วนตัวเป็นการทั่วไปของบุคคล กล่าวคือมีลักษณะเป็นการคุ้มครองความเป็นอยู่ส่วนตัวในข้อมูลข่าวสาร ซึ่งอาศัยเกณฑ์ในการพิจารณาจากทฤษฎีการควบคุมนั่นเอง

4. หลักการของการเพิกถอนความยินยอม ซึ่งในพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตแม้จะไม่ได้มีการกำ หนดระยะเวลาความมีผลบังคับของความยินยอมไว้ เนื่องจากเมื่อเจ้าของข้อมูลได้ให้ความยินยอมในการเปิดเผยข้อมูลเครดิตที่จะนำ ไปใช้ตามกฎหมายแล้วเช่นนี้ ข้อมูลเครดิตของบุคคลดังกล่าว จะถูกนำ ไปใช้เพื่อการวิเคราะห์สินเชื่อของบุคคลนั้น ตลอดระยะเวลาของการมีหนี้อยู่ ดังนั้นกรณีการใช้สิทธิเพิกถอนความยินยอมที่ให้ไปแล้วนั้น โดยสภาพจึงไม่อาจเกิดขึ้นได้ตราบใดที่เจ้าของข้อมูลที่ให้ความยินยอมนั้นยังคงเป็นหนี้อยู่ แม้จะมีแนวคิดตามหลักการคุ้มครองข้อมูลส่วนบุคคลที่ว่า เจ้าของข้อมูลนั้นสามารถเพิกถอนความยินยอมได้ทุกเมื่อ เพื่อเป็นการให้คุ้มครองแก่เจ้าของข้อมูลก็ตาม แต่เมื่อพิจารณาถึงหลักการให้ความยินยอมของเจ้าของข้อมูลในการเปิดเผยข้อมูลเครดิตแล้ว จะเห็นได้ว่าในการปรับใช้นั้นไม่ได้มีลักษณะเป็นการให้สิทธิเลือกในการตัดสินใจแก่เจ้าของ

ข้อมูลที่จะเพิกถอนการให้ความยินยอมเมื่อใดก็ได้ เพราะการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตเป็นเงื่อนไขหรือองค์ประกอบสำคัญที่ว่าตราบใดที่เจ้าของข้อมูลยังมีความเป็นหนี้อยู่ตราบนั้นเจ้าของข้อมูลจะเพิกถอนการให้ความยินยอมไม่ได้ เพราะความยินยอมในการเปิดเผยข้อมูลเครดิตนั้นถือเป็นสาระสำคัญของการอนุมัติให้สินเชื่อนั่นเอง ซึ่งในประเด็นนี้จะมีการอธิบายโดยละเอียดต่อไปในหัวข้อระยะเวลาการมีผลบังคับของความยินยอมของเจ้าของข้อมูล

และเพื่อประโยชน์ในการศึกษาวิเคราะห์ ส่วนต่อไปจะเป็นการอธิบายถึงหลักความยินยอมในมุมมองของกฎหมายต่างประเทศ กล่าวคือ The Fair Credit Reporting Act (FCRA) ของประเทศสหรัฐอเมริกา และ Data Protection Act ของประเทศอังกฤษ ตามลำดับดังนี้

(2) หลักการให้ความยินยอมตาม The Fair Credit Reporting Act

FCRA ไม่ได้กำหนดให้การจัดส่งข้อมูลไปยังบริษัทข้อมูลเครดิต หรือ Credit Reporting Agency (CRA) และการใช้ข้อมูลรายงานลูกค้า (Consumer Report) จากบริษัทข้อมูลเครดิตจะต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลแต่อย่างใด เนื่องจากประเทศสหรัฐอเมริกาได้มีแนวคิดที่ว่าลูกค้าผู้เป็นเจ้าของข้อมูลได้ให้ความยินยอมโดยปริยายแล้ว จากการที่มาขอสินเชื่อจากสถาบันการเงินผู้ให้สินเชื่อ ซึ่งถือเป็นการอนุญาตให้สถาบันการเงินทำการตรวจสอบคุณสมบัติของตนเพื่อประกอบการพิจารณาสินเชื่อดังกล่าว โดยที่ FCRA ได้ใช้หลักการกำหนดในเรื่องวัตถุประสงค์ในการใช้ข้อมูลที่ได้รับอนุญาตแทน กล่าวคือ บริษัทข้อมูลเครดิตจะต้องใช้ข้อมูลลูกค้าภายในวัตถุประสงค์ที่ได้รับอนุญาตตามที่กำหนดไว้เท่านั้น ตามที่มีการบัญญัติไว้ใน Section 604 (a) ว่า บริษัทข้อมูลเครดิตสามารถเปิดเผยข้อมูลข่าวสารหรือสื่อข้อมูลอันมีลักษณะเป็นข้อมูลเกี่ยวกับบุคคลได้โดยจะต้องเป็นไปเพื่อวัตถุประสงค์ดังต่อไปนี้

1. เพื่อการปฏิบัติตามคำพิพากษาของศาล
2. เพื่อการปฏิบัติตามคำสั่งอันได้ทำขึ้นเป็นลายลักษณ์อักษรของบุคคลผู้เกี่ยวข้อง
3. เพื่อบุคคลที่มีเหตุผลที่น่าเชื่อถือได้ว่า

(1) มีเจตนาที่จะใช้ข้อมูลเพื่อกิจการด้านสินเชื่อให้แก่ผู้บริโภค

(2) มีเจตนาที่จะใช้ข้อมูลเพื่อวัตถุประสงค์ในการจ้างงาน

(3) มีเจตนาที่จะใช้ข้อมูลเพื่อการทำ สัญญาประกันให้กับผู้บริโภค

(4) มีเจตนาที่จะใช้ข้อมูลเพื่อการตรวจสอบถึงความเหมาะสมในการให้ใบอนุญาตหรือประโยชน์อื่นๆ จากฝ่ายบริหาร โดยเฉพาะ เมื่อกฎหมายในเรื่องดังกล่าวนั้นกำ หนดว่าต้องพิจารณาความรับผิดชอบทางการเงินหรือฐานะทางการเงินของผู้สมัคร

(5) มีเจตนาที่จะใช้ข้อมูลข้อมูลในฐานะของผู้ลงทุนที่มีประสิทธิภาพ หรือผู้ให้บริการ หรือผู้รับประกัน ในการตรวจสอบความเหมาะสม หรือการประเมินสินเชื่อ หรือความเสี่ยงในการจ่ายล่วงหน้าซึ่งเกี่ยวข้องกับภาระสินเชื่อที่คงอยู่

(6) ธุรกิจใดๆ ซึ่งต้องการข่าวสารนั้นๆ ในการติดต่อธุรกิจที่ลูกค้าเป็นผู้ริเริ่ม หรือในการทบทวนบัญชี เพื่อพิจารณาว่าลูกค้ายังคงมีคุณสมบัติต้องตาม เงื่อนไขในการใช้บัญชีนั้นอยู่หรือไม่

4.เปิดเผยให้กับหน่วยงานคุ้มครองเด็ก (หรือหน่วยงานของรัฐที่ได้รับอนุญาตจากหน่วยงานเช่นว่านั้น) โดยผู้ประสงค์จะใช้ข้อมูลได้แสดงต่อบริษัทข้อมูลเครดิตถึงเงื่อนไขตามที่กำ หนดไว้ใน Section 604 (a) (4)

5. เพื่อเปิดเผยแก่หน่วยงานทางปกครองของรัฐ ภายใต้ Section 454 ของ The Social Security Act เพื่อใช้กำ หนดหรือแก้ไขคำ ตัดสินเกี่ยวกับการคุ้มครองเด็ก

นอกจากนี้ยังได้กำ หนดข้อปฏิบัติในการเปิดเผยข้อมูลให้แก่หน่วยงาน FBI ของสหรัฐอเมริกาไว้เป็นการเฉพาะด้วยใน section 625

ในทางปฏิบัติ ถึงแม้ว่า FCRA จะไม่ได้กำ หนดให้ลูกค้าต้องให้ความยินยอม แต่โดยทั่วไปสถาบันการเงินผู้ให้สินเชื่อในประเทศสหรัฐอเมริกา จะมีข้อความขอความยินยอมจากลูกค้า เพื่อให้ลูกค้าลงนามให้ความยินยอมโดยแนบไปกับเอกสารใบคำ ขอสินเชื่อต่างๆ อยู่แล้วเสมือนเป็นธรรมเนียมในทางปฏิบัติ ส่วนการใช้ข้อมูลเพื่อวัตถุประสงค์อย่างอื่นนอกเหนือจากวัตถุประสงค์ที่ได้รับอนุญาตตามที่ FCRA กำหนดไว้ เช่น การใช้ข้อมูลเพื่อการจ้างงาน การใช้ข้อมูลเพื่อเสนอข้อเสนอใดๆ เกี่ยวกับธุรกรรมที่ลูกค้าไม่ได้

เป็นผู้ริเริ่มเอง การใช้ข้อมูลเกี่ยวกับการแพทย์ และการขอให้มีการจัดทำ และการใช้รายงานการสืบสวนลูกค้า (Investigative Consumer Report) นั้น กรณีเหล่านี้บริษัทข้อมูลเครดิตจะต้องปฏิบัติตามเงื่อนไขที่กฎหมายกำหนดไว้เป็นกรณีเฉพาะ

จะเห็นได้ว่าเนื่องมาจากลักษณะของการประกอบธุรกิจข้อมูลเครดิตในประเทศสหรัฐอเมริกาที่เริ่มต้นมาเป็นระยะเวลานาน และมีพัฒนาการของกฎหมายเพื่อควบคุมดูแลธุรกิจประเภทนี้เป็นประเทศแรก จึงมีการให้ความสำคัญในเรื่องของหลักการปฏิบัติตามความเป็นจริง เพื่อให้การดำเนินการของธุรกิจข้อมูลเครดิตนี้เป็นไปได้ตามวัตถุประสงค์ ส่งผลให้ FCRA มีการเน้นไปยังประเด็นในเรื่องของวัตถุประสงค์ในการใช้ข้อมูล มากไปกว่าในเรื่องของการให้ความยินยอมของเจ้าของข้อมูล อีกทั้งยังมีแนวคิดที่ว่าเจ้าของข้อมูลได้ให้ความยินยอมโดยปริยาย ด้วยการขอสินเชื่อจากสถาบันการเงินนั้นแล้ว จึงทำให้การเปิดเผยข้อมูลเครดิตโดยบริษัทข้อมูลเครดิตในประเทศสหรัฐอเมริกาโดยหลักนั้น ไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนแต่อย่างใด

(3) หลักการให้ความยินยอมตาม Data Protection Act 1998

ประเทศอังกฤษไม่มีกฎหมายเกี่ยวกับการประกอบธุรกิจข้อมูลเครดิตเป็นการเฉพาะ ดังนั้น การประกอบธุรกิจข้อมูลเครดิตจึงอยู่ภายใต้กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อเป็นการทำความเข้าใจถึงหลักการให้ความยินยอมแล้ว ในเบื้องต้นจะทำการอธิบายถึงประเด็นสำคัญที่เกี่ยวข้องจากหลักการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

ผู้ประกอบธุรกิจข้อมูลเครดิต หรือ Credit Reference Agency (CRA) มีฐานะเป็น "ผู้ควบคุมข้อมูล" (Data Controller) ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล กล่าวคือ เป็นบุคคลที่เป็นผู้รับผิดชอบในการตัดสินใจถึงวัตถุประสงค์ในการใช้และจัดเก็บข้อมูลว่าข้อมูลใดจะถูกนำมาประมวลผล ซึ่งถือเป็นประเด็นสำคัญที่จะต้องคำนึงถึงเนื่องจากใน Section 4 (4) กำหนดให้เป็นหน้าที่ของผู้ควบคุมข้อมูลที่จะต้องปฏิบัติตาม Data Protection Principles ในกรณีที่เกี่ยวข้องกับข้อมูลส่วนบุคคลซึ่งครอบครองอยู่

ส่วนการเปิดเผยข้อมูลเครดิตนั้น เข้าตามนิยามของคำว่า "การประมวลผลข้อมูล" (processing) ตาม section 1 ซึ่ง

หมายความถึง การได้มา, การบันทึก หรือการจัดเก็บข้อมูล หรือการดำเนินการใดๆ กับข้อมูล ซึ่งรวมไปถึง

(1) การจัดการ, การแก้ไข หรือการเปลี่ยนแปลงข้อมูล

(2) การเรียกใช้, การแลกเปลี่ยน หรือการใช้ข้อมูล

(3) การเปิดเผยข้อมูล โดยการจัดส่ง การเผยแพร่ หรือวิธีการอื่นใดเพื่อให้เข้าถึงข้อมูลได้

(4) การเรียบเรียง, การประกอบ, การกั้น, การลบ หรือการทำลายข้อมูล

ดังนั้นบริษัทข้อมูลเครดิตในประเทศอังกฤษจึงมีหน้าที่ตามกฎหมายที่จะต้องประมวลผลข้อมูลส่วนบุคคลให้เป็นไปตาม Data Protection Principles ด้วยนั่นเอง ซึ่งในหลักการข้อที่ 1 ได้แก่ "ข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผลโดยเป็นธรรมและชอบด้วยกฎหมาย" นั้นมีการกำหนดไว้ว่าข้อมูลส่วนบุคคลจะต้องได้รับการประมวลผลโดยเป็นธรรมและชอบด้วยกฎหมาย และจะต้องไม่มีการประมวลผลข้อมูลส่วนบุคคล ยกเว้นได้ดำเนินการดังต่อไปนี้ 1) อย่างน้อยจะต้องเป็นไปตามเงื่อนไขข้อใดข้อหนึ่งที่กำหนดไว้ใน Schedule 2

2) กรณีที่เป็น Sensitive Personal Data อย่างน้อยจะต้องเป็นไปตามเงื่อนไขข้อใดข้อหนึ่งที่กำหนดไว้ใน Schedule 3

จึงกล่าวได้ว่า การประมวลผลข้อมูลในการดำเนินธุรกิจข้อมูลเครดิต ซึ่งไม่เป็นการประมวลผล Sensitive Personal Data นั้น ผู้ควบคุมข้อมูลต้องดำเนินการตามเงื่อนไขที่กำหนดไว้ใน Schedule 2 ซึ่งอย่างน้อยจะต้องเป็นไปตามเงื่อนไขข้อใดข้อหนึ่งดังต่อไปนี้

1) เจ้าของข้อมูลได้ให้ความยินยอมในการประมวลผลข้อมูลนั้นแล้ว

2) จำเป็นต้องประมวลผลข้อมูล เพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลเป็นคู่สัญญาฝ่ายใดฝ่ายหนึ่ง หรือเพื่อการดำเนินการตามขั้นตอนซึ่งเจ้าของข้อมูลเป็นผู้กำหนดให้มุ่งหมายในการเข้าผูกพันตามสัญญา

3) ผู้ควบคุมข้อมูลมีหน้าที่ตามกฎหมายหรือหน้าที่ตามข้อกำหนดในสัญญาที่จะต้องประมวลผลข้อมูลนั้น

4) การประมวลผลนั้นจำเป็นเพื่อปกป้องผลประโยชน์เกี่ยวกับชีวิตของบุคคล

5) การประมวลผลข้อมูลนั้นจำเป็นสำหรับการบริหารความยุติธรรม หรือเพื่อดำเนินการตามหน้าที่ภายใต้พระบรมราชโองการ หรือเพื่อดำเนินการในฐานะของประมุขของประเทศ หรือส่วนราชการ หรือเพื่อดำเนินการตามหน้าที่อื่นๆ ซึ่งเป็นประโยชน์ต่อสาธารณะ

6) การประมวลผลจำเป็นเพื่อการปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูล หรือบุคคลที่สาม หรือบุคคลที่ข้อมูลถูกเปิดเผย ยกเว้นการประมวลผลโดยที่ไม่มีความมุ่งหมายในประการที่เกี่ยวข้องกับกรณี เพราะอาจก่อให้เกิดการละเมิดสิทธิและเสรีภาพหรือผลประโยชน์ตามกฎหมายของเจ้าของข้อมูล

เมื่อนำมาปรับใช้กับการประกอบธุรกิจข้อมูลเครดิต จะเห็นได้ว่าเพื่อให้การประมวลผลข้อมูลเป็นไปโดยชอบด้วยกฎหมายนั้น จะต้องอาศัยเงื่อนไขข้อที่ 1 คือจะต้องได้รับความยินยอมจากเจ้าของข้อมูลเท่านั้น

การให้ความยินยอม ไม่มีการกำหนดนิยามไว้ใน Data Protection Act 1998 แต่ตาม Directive 95/46/EC (on the protection of individuals with regard to the processing of personal data and the free movement of such data) ซึ่งเป็นต้นแบบในการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกสหภาพยุโรปนั้น ได้มีการให้นิยามคำว่า “การให้ความยินยอม” (consent) ไว้ว่ามีองค์ประกอบหลัก 3 ประการคือ

1) จะต้องมีความชัดเจน

2) จะต้องเป็นไปโดยสมัครใจ

3) จะต้องทราบถึงรายละเอียดโดยเฉพาะเจาะจง ถึงกิจกรรมในการประมวลผลทั้งหมดนั้น

จึงจะเห็นได้ว่าจากหลักการให้ความยินยอมตาม Directive 95/46/EC การให้ความยินยอมโดยปริยาย หรือโดยการสันนิษฐานนั้นย่อมไม่สามารถนำมาใช้ได้ เนื่องจากการแสดงออกถึงความยินยอมตาม Directive นี้จะต้องมีความชัดเจน กล่าวคือ จะต้องปราศจากความสงสัยว่าเจ้าของข้อมูลได้ให้ความยินยอมแล้ว

หรือไม่ โดยใช้ทั้งกับการแสดงออกทางวาจา และลายลักษณ์อักษร[22]

แต่เมื่อมีการนำมาบัญญัติเป็นกฎหมายภายในของประเทศอังกฤษ จากการหารือในรัฐสภา Lord Williams ได้แสดงความเห็นในการไม่กำหนดนิยามของการให้ความยินยอมไว้ว่า นิยามดังกล่าวนั้นเป็นสิ่งที่ไม่จำเป็น เนื่องจากมีวิธีการตีความตามกฎหมายอยู่แล้ว กล่าวคือ การให้ความยินยอมนั้นย่อมมีขอบเขต และเนื้อหาตามแนวคำพิพากษาของศาลในคดีก่อนๆ เป็นหลักอยู่แล้วนั่นเอง[23]

และเมื่อได้พิจารณาถึงการปรับใช้หลักในเรื่องความยินยอม ตาม Data Protection Act แล้วนั้น สามารถสรุปองค์ประกอบที่สำคัญได้ ดังนี้

1) การให้ความยินยอมจะต้องเป็นไปโดยสมัครใจ

โดยจะต้องมีการพิจารณาถึงระดับทางเลือกที่ปัจเจกบุคคลมี การปฏิบัติตามธรรมเนียมของธุรกิจในการใช้ข้อมูลซึ่งมีลักษณะเป็นการจำกัดทางเลือกของปัจเจกบุคคลอาจเป็นกรณีที่เกิดเป็นปัญหาได้ ถ้าหากการใช้ข้อมูลดังกล่าวนั้นไม่ใช่ส่วนสำคัญตามวัตถุประสงค์ของสัญญา

กรณีตัวอย่างที่สำคัญ ตามที่ the Article 29 Working Party ได้ให้ความเห็นไว้ คือการให้ความยินยอมในกรณีของการจ้างงาน กล่าวคือ การให้ความยินยอมในการใช้ข้อมูลส่วนบุคคลซึ่งเป็นส่วนหนึ่งของสัญญาจ้างแรงงานนั้น ไม่ถือว่าเป็นการให้ความยินยอมโดยสมัครใจ แต่ก็ได้มีการวิพากษ์วิจารณ์ตามมาอย่างมากมาย เนื่องจากความคิดที่ว่าพื้นฐานความสัมพันธ์ของคู่สัญญานั้น ก็คือการที่ฝ่ายหนึ่งยอมให้สิ่งใดสิ่งหนึ่งกับอีกฝ่าย เพื่อที่จะได้รับอย่างอื่นเป็นการตอบแทน ผู้ที่ยอมรับข้อตกลงในการใช้ข้อมูลส่วนบุคคลดังกล่าว เพื่อให้ตนมีรายได้จากการจ้างงาน จึงควรที่จะสามารถมีการให้ความยินยอมในลักษณะดังกล่าวได้ และจากตัวอย่างคำตัดสินของ European Court under the Human Rights

---

22 Federico Ferretti, The law and consumer credit information in the European Community, (NY : Routledge-Cavendish, 2008) p.162

23 Rosemary Jay, Data protection : law and practice, (London : Sweet & Maxwell, 2007) p.149

Convention ในคดี Stedman v. UK ที่ว่าปัจเจกบุคคลอาจเลือกที่จะให้ความยินยอมในการที่จะสละสิทธิของตนได้

2) การให้ความยินยอมจะต้องมีลักษณะเฉพาะเจาะจง

กล่าวคือ ควรเฉพาะเจาะจงถึงกระบวนการหรือวัตถุประสงค์ในการประมวลผลข้อมูล ถ้าหากข้อความของความยินยอมนั้นไม่ชัดเจน หรือมีลักษณะทั่วไป ก็ย่อมไม่สามารถนำ มาใช้ได้ แต่ถ้าข้อความของความยินยอมมีการกำ หนดไว้อย่างกว้างๆ จะสามารถใช้ได้ในกรณีที่ข้อความดังกล่าวมีความชัดเจนในประเด็นที่เกี่ยวข้องอย่างครบถ้วน

3) การให้ความยินยอมจะต้องเป็นไปโดยได้รับทราบข้อมูลแล้ว

เจ้าของข้อมูลไม่จำ เป็นจะต้องทราบถึงรายละเอียดทุกประการของการประมวลผลข้อมูล แต่จะต้องทราบถึงลักษณะพื้นฐานของการประมวลผล และประเด็นสำ คัญอื่นที่อาจส่งผลกระทบต่อตน

4) การให้ความยินยอมจะต้องมีการแสดงออกถึงการตกลง

การยอมรับโดยการนิ่งเฉยซึ่งไม่มีการแสดงออกถึงการตอบสนองนั้น ไม่เพียงพอที่จะถือว่าเป็นความยินยอม แต่จากเหตุผลข้างต้นก็ไม่เป็นการปิดทางเลือกที่จะใช้วิธีการให้ความยินยอมแบบ opt-out เพียงแต่จะเป็นการดีกว่าถ้าหากสามารถที่จะใช้วิธีการที่จะได้รับการตอบสนองถึงความยินยอมได้อย่างชัดเจน โดยที่ในการใช้วิธีการแบบ opt-out นั้น สามารถกระทำ ได้ถ้าหากมีการกระทำ ใดๆ ซึ่งเป็นการตอบสนองของเจ้าของข้อมูลที่จะถือได้ว่าเป็นการให้ความยินยอมแล้ว กล่าวคือ การให้ความยินยอมแบบ opt-out สามารถทำ ได้ในกรณีที่ผู้ควบคุมข้อมูลแจ้งไปยังเจ้าของข้อมูลถึงการใช้ข้อมูลส่วนบุคคลที่จะเกิดขึ้น ผ่านทางสื่อที่เหมาะสมซึ่งจะต้องส่งกลับไปยังผู้ควบคุมข้อมูล อาทิ คูปองตอบกลับ โดยมีการระบุว่าถ้าหากไม่มีการกระทำ ใดๆ ตามที่กำ หนด ซึ่งส่วนมากมักจะกำ หนดให้ทำ เครื่องหมายในช่องสี่เหลี่ยม เป็นต้น จะสันนิษฐานว่าเจ้าของข้อมูลได้มีการให้ความยินยอมแล้ว จากกรณีนี้จะถือว่าเจ้าของข้อมูลได้ให้ความยินยอมโดยปริยายด้วยการส่งสื่อดังกล่าวนั้นกลับไปโดยไม่มีการทำ เครื่องหมายในช่องสี่เหลี่ยม แต่อย่างไรก็ตาม เนื่องจากว่าเจ้าของข้อมูลอาจไม่สังเกตเห็นหรืออ่าน

เจอข้อความดังกล่าว จึงอาจมีข้อโต้แย้งได้ว่าไม่มีการแสดงออกอย่างชัดเจนถึงการตกลงโดยเจ้าของข้อมูล ซึ่งในประเด็นดังกล่าวนี้ยังไม่มีแนวคำพิพากษาของศาลในการวางหลักเกณฑ์ไว้แต่อย่างใด ในทางกลับกัน ในกรณีที่ผู้ควบคุมข้อมูลได้มีการประมวลผลข้อมูลไปแล้ว จึงค่อยให้ทางเลือกแก่เจ้าของข้อมูลในการ opt-out นั้น ไม่ถือว่าเป็นการให้ความยินยอมตามหลักการของกฎหมาย[24]

นอกจากนี้ แนวปฏิบัติในเรื่องการให้ความยินยอมตามการให้คำแนะนำ ของ The Information Commissioner นั้น จะเห็นได้ว่าการให้ความยินยอมนั้น เนื่องจากว่าไม่ได้มีการกำหนดไว้ใน Data Protection Act 1998 ดังนั้น ความคงอยู่หรือความมีผลของความยินยอมจึงจำเป็นที่จะต้องได้รับการประเมินจากข้อเท็จจริงเป็นกรณีๆ ไป และในกรณีที่เจ้าของข้อมูลไม่ได้แสดงความตกลงโดยชัดแจ้งในการอนุญาตให้มีการประมวลผลข้อมูลอันเกี่ยวกับตน แต่ถ้าเจ้าของข้อมูลได้รับการให้โอกาสในการคัดค้านการประมวลผลข้อมูลเช่นนั้นแล้ว แม้ว่ากรณีนี้จะไม่ได้เป็นการให้ความยินยอมโดยชัดแจ้ง แต่ก็อาจจัดว่าเป็นหลักการพื้นฐานสำหรับผู้ควบคุมข้อมูลในการปฏิบัติตามเงื่อนไขของ Schedule 2 ได้ ยกตัวอย่างเช่น การให้เจ้าของข้อมูลได้มีโอกาสที่จะโต้แย้งหรือมีสิทธิที่จะโต้แย้งก่อนที่ข้อมูลจะถูกประมวลผล ก็ถือว่าเป็นการปฏิบัติตามกฎหมายนี้แล้ว โดยที่เมื่อนำมาปรับใช้กับการประกอบธุรกิจข้อมูลเครดิตแล้วนั้น การบอกกล่าวเพื่อเป็นการให้สิทธิเจ้าของข้อมูลในการโต้แย้งหรือคัดค้านการประมวลผลข้อมูลของตน อาจทำได้โดยการบอกกล่าวว่าจะมีการตรวจสอบข้อมูลเครดิตของเจ้าของข้อมูล โดยการบอกกล่าวนั้นจะต้องแสดงอย่างชัดแจ้ง ซึ่งอาจระบุไว้ในเอกสารหลักฐานของการขาย โดยอาจระบุในส่วนของการแจ้งให้ทราบ หรือในข้อตกลงและเงื่อนไขของเอกสารการขายนั้น หรือระบุไว้ในใบคำขอสินเชื่อ หรือใบสมัครบัตรเครดิต เป็นต้น และเจ้าของข้อมูลจะต้องได้รับการแจ้งด้วยว่าบันทึกการใช้หรือการตรวจสอบข้อมูลของตนจะถูกเก็บรักษาไว้ และถ้าการติดต่อธุรกรรมนั้นกระทำโดยทางโทรศัพท์ เจ้าหน้าที่รับโทรศัพท์จะต้องบอกกล่าวโดยวาจาถึงการประมวลผลหรือการใช้ข้อมูล และยังต้องขอความยินยอมดังกล่าว

---

24 *Ibid*. pp.152-153

ด้วย ดังนั้น การประกอบธุรกิจข้อมูลเครดิต จึงได้รับการแนะนำ ให้มีการตรวจสอบเพื่อพิสูจน์ถึงการบอกกล่าวและความยินยอมนั้นด้วย[25]

ตามความเป็นจริงในการประกอบธุรกิจข้อมูลเครดิตในประเทศอังกฤษ ก็ได้มีการตั้งประเด็นในเรื่องการให้ความยินยอมเช่นเดียวกันโดยมีลักษณะคล้ายคลึงกับในประเทศไทยกล่าวคือ การให้ความยินยอมของเจ้าของข้อมูลในการเปิดเผยข้อมูลเครดิตนั้น เจ้าของข้อมูลไม่มีทางเลือกอย่างแท้จริง ถ้าหากจะเข้าสู่ขั้นตอนการพิจารณาการขอสินเชื่อ เจ้าของข้อมูลก็จำ ต้องให้ความยินยอมดังกล่าวโดยไม่มีทางเลือกนั่นเอง อีกทั้งลักษณะของอำนาจต่อรองระหว่างสถาบันการเงินกับเจ้าของข้อมูลซึ่งเป็นผู้บริโภคนั้น ย่อมมีความแตกต่างกันอย่างเห็นได้ชัด ซึ่งส่งผลกระทบโดยตรงต่อหลักการให้ความยินยอมที่จะต้องเป็นไปโดยสมัครใจ ซึ่งเหตุผลสำ คัญที่การเปิดเผยข้อมูลเครดิตในประเทศอังกฤษจะต้องมีการให้ความยินยอมของเจ้าของข้อมูลก่อนนั้น ก็เนื่องมาจากการที่ประเทศอังกฤษนั้นไม่มีกฎหมายที่ควบคุมดูแลการประกอบธุรกิจข้อมูลเครดิตโดยตรง ทำ ให้ต้องใช้หลักการของ Data Protection Act ในเรื่องการให้ความยินยอมมาใช้ เพื่อที่จะเป็นการให้ความคุ้มครองแก่เจ้าของข้อมูล จึงเกิดแนวคิดที่ว่า ถ้าหากมีกฎหมายเฉพาะเพื่อควบคุมดูแลกระบวนการต่างๆ ของธุรกิจข้อมูลเครดิตแล้ว หลักการให้ความยินยอมนี้ก็ย่อมไม่มีความจำ เป็นอีกต่อไป เนื่องจากบริษัทข้อมูลเครดิตนั้นย่อมอยู่ในกรอบของกฎหมายเฉพาะดังกล่าว ซึ่งจะส่งผลเป็นการให้ความคุ้มครองแก่เจ้าของข้อมูลในระดับที่เพียงพอแล้วว่าการประมวลผลนั้นจะเป็นไปโดยชอบด้วยกฎหมาย และไม่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูล[26]

ดังนั้น เมื่อวิเคราะห์จากหลักการของพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 และกฎหมายที่มีการบังคับใช้ในต่างประเทศ รวมไปถึงปัญหาในทางปฏิบัติที่เกิดขึ้น จะเห็นได้ว่าเรื่องการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูลนั้น มีส่วนสำ คัญและเป็นมาตรฐานสากลในการพิจารณาให้สินเชื่อของสถาบันการเงินต่างๆ และในเรื่องของหลักการให้ความยินยอมในการเปิดเผย

---

25 สุดธนา พันธุ์ธีรานุรักษ์, *อ้างแล้ว เชิงอรรถที่1,* ภาคผนวก ค

26 Federico Ferretti, *supra note22,* p.197

ข้อมูลเครดิตตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตนั้น มีลักษณะเป็นการคุ้มครองสิทธิที่จะได้รับข้อมูลของเจ้าของข้อมูล (right to be informed) มิได้มีลักษณะเป็นการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว (privacy right) แต่อย่างใด เนื่องจากข้อมูลเครดิตนั้นไม่ได้มีลักษณะเป็นข้อมูลที่มีประโยชน์เฉพาะต่อเจ้าของข้อมูลเท่านั้น แต่มีลักษณะเป็นข้อมูลที่เป็นประโยชน์ต่อสาธารณะ กล่าวคือเป็นข้อมูลทางการเงินที่จัดเก็บรวบรวมขึ้นเพื่อเป็นประโยชน์แก่สถาบันการเงินในการใช้ข้อมูลนั้นเพื่อวิเคราะห์การให้สินเชื่อ เพื่อให้เกิดการวิเคราะห์สินเชื่อได้อย่างมีประสิทธิภาพซึ่งจะส่งผลดีต่อเศรษฐกิจโดยรวมของประเทศในที่สุด ดังนั้นควรมีการปรับใช้ให้ถูกต้องกับหลักการของกฎหมายดังกล่าวด้วย

และการกำหนดให้บริษัทข้อมูลเครดิตต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนที่จะมีการเปิดเผยข้อมูลเครดิตนั้น เป็นข้อกำหนดที่อาจถือได้ว่าไม่มีความจำเป็น เนื่องจากตามความเป็นจริงแล้วนั้น การให้ความยินยอมดังกล่าวมีลักษณะเป็นการบังคับ ซึ่งเจ้าของข้อมูลนั้นไม่มีทางเลือกถ้าหากต้องการที่จะได้รับการพิจารณาสินเชื่อ ส่งผลให้วัตถุประสงค์ของกฎหมายที่ต้องการให้ความคุ้มครองแก่เจ้าของข้อมูลในการรับทราบ และมีสิทธิในการตัดสินใจในการเปิดเผยข้อมูลเครดิตของตนนั้นย่อมไม่สามารถเป็นไปได้ อีกทั้งยังเป็นการเพิ่มกระบวนการในการดำเนินธุรกิจข้อมูลเครดิต ซึ่งถ้าหากไม่มีบทบาทเป็นการให้ความคุ้มครองเจ้าของข้อมูลแล้วนั้น ย่อมถือได้ว่าเป็นภาระที่ไม่จำเป็นของบริษัทข้อมูลเครดิตอีกด้วย และเมื่อศึกษาวิเคราะห์กฎหมาย Data Protection Act 1998 ของประเทศอังกฤษ ซึ่งเป็นต้นแบบการศึกษาค้นคว้าในการพิจารณาร่างพระราชบัญญัติในชั้นการพิจารณาของรัฐสภา ที่ได้มีการกำหนดแก้ไขให้มีการกำหนดหลักในเรื่องความยินยอมไว้ในกฎหมายนี้ ก็จะเห็นได้ว่า ความจำเป็นในการใช้หลักการให้ความยินยอมของอังกฤษนั้น เกิดขึ้นจากการที่ธุรกิจข้อมูลเครดิตของประเทศนั้นไม่มีกฎหมายเฉพาะใดๆ เข้ามากำกับดูแล จึงทำให้เกิดความกังวลว่าการจัดเก็บและการเปิดเผยข้อมูลเครดิตซึ่งเป็นข้อมูลส่วนบุคคลที่มีความสำคัญนั้น อาจเกิดผลกระทบต่อเจ้าของข้อมูลได้ จึงต้องมีการใช้หลักการให้ความยินยอมนั่นเอง แต่ในกรณีของประเทศไทยนั้น ได้มีการประกาศใช้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 เป็นกฎหมายเฉพาะเพื่อกำกับดูแล

การประกอบธุรกิจข้อมูลเครดิต ซึ่งได้มีบทบัญญัติกำหนดในเรื่องวัตถุประสงค์ในการใช้ข้อมูลเครดิตไว้แล้ว จึงเป็นการสร้างเงื่อนไขที่ช่วยให้ความคุ้มครองแก่เจ้าของข้อมูลในการที่บริษัทข้อมูลเครดิตจะทำการเปิดเผยข้อมูลได้ เช่นเดียวกับ The Fair Credit Reporting Act ของประเทศสหรัฐอเมริกา อีกทั้งยังเป็นเครื่องยืนยันในการปฏิบัติตามกฎหมายของบริษัทข้อมูลเครดิตในทุกขั้นของการดำเนินการ และมีกลไกในการลงโทษในกรณีที่มีการฝ่าฝืนจากเหตุดังกล่าวข้างต้น จึงเห็นว่าการประกอบธุรกิจข้อมูลเครดิตในประเทศไทยนั้นไม่มีความจำเป็นที่จะต้องมีการให้ความยินยอมของเจ้าของข้อมูลในการเปิดเผยข้อมูลเครดิตอีก

1.2 วิธีการให้ความยินยอม และระยะเวลาการมีผลบังคับของความยินยอมของเจ้าของข้อมูล

ตามที่พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ในมาตรา 20 กำหนดให้บริษัทข้อมูลเครดิตต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนที่จะเปิดเผยข้อมูลให้แก่สมาชิกหรือผู้ใช้บริการดังที่อธิบายไว้ข้างต้นนั้น ทำให้เกิดประเด็นที่ควรจะพิจารณาต่อไป คือวิธีการให้ความยินยอม และระยะเวลาการมีผลบังคับของความยินยอม โดยสามารถอธิบายตามลำดับ ดังนี้

(1) วิธีการให้ความยินยอมในการเปิดเผยข้อมูลเครดิตของเจ้าของข้อมูล

ในทางปฏิบัติแล้วนั้น บริษัทข้อมูลเครดิตไม่ได้เป็นผู้มีนิติสัมพันธ์โดยตรงกับเจ้าของข้อมูลแต่อย่างใด การกำหนดให้บริษัทข้อมูลเครดิตเองเป็นผู้ขอความยินยอมจึงเป็นไปได้ไม่สะดวกนัก หน้าที่ดังกล่าวนี้จึงควรให้เป็นของสมาชิกซึ่งเป็นผู้มีนิติสัมพันธ์โดยตรงกับเจ้าของข้อมูล อีกทั้งในเบื้องต้นนั้นในพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 เองก็มิได้มีการกำหนดถึงวิธีการในการให้ความยินยอมดังกล่าวนี้ไว้ ซึ่งในประเด็นนี้มาตรา 20 ได้กำหนดให้เป็นหน้าที่ของคณะกรรมการคุ้มครองข้อมูลเครดิตที่จะกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขเพื่อบังคับให้เป็นไปตามกฎหมาย และต่อมาคณะกรรมการคุ้มครองข้อมูลเครดิตได้มีหนังสือเวียนที่ กคค.(ว) 2/2546 เรื่องซักซ้อมความเข้าใจแนวทาง

ปฏิบัติเกี่ยวกับการได้รับความยินยอมจากเจ้าของข้อมูลเพื่อการเปิดเผยข้อมูลเครดิต ลงวันที่ 19 มีนาคม พ.ศ.2546 โดยกำหนดให้สมาชิกหรือผู้ใช้บริการเป็นผู้ดำเนินการให้เจ้าของข้อมูลให้ความยินยอมแทนบริษัทข้อมูลเครดิต โดยมีรายละเอียด ดังนี้

1. บริษัทข้อมูลเครดิตอาจตกลงให้สมาชิกหรือผู้ใช้บริการเป็นผู้ดำเนินการให้เจ้าของข้อมูลทำหนังสือให้คำยินยอมแก่บริษัทข้อมูลเครดิต เพื่อบริษัทข้อมูลเครดิตสามารถเปิดเผยข้อมูลของเจ้าของข้อมูลนั้นแก่สมาชิกหรือผู้ใช้บริการ และอาจให้สมาชิกหรือผู้ใช้บริการเป็นผู้รับหนังสือให้คำยินยอมนั้นแทนบริษัทข้อมูลเครดิตเพื่อรวบรวมส่งให้บริษัทข้อมูลเครดิตในภายหลัง

2. เพื่อความสะดวก และความรวดเร็วในการอนุมัติสินเชื่อหรือเครดิต เมื่อเจ้าของข้อมูลทำหนังสือให้คำยินยอมตามข้อ 1.แล้ว บริษัทข้อมูลเครดิตอาจตกลงให้สมาชิกหรือผู้ใช้บริการแจ้งให้บริษัทข้อมูลเครดิตทราบการให้คำยินยอม ด้วยหนังสือ หรือสื่ออิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่ตกลงกันไว้ล่วงหน้า ก่อนส่งหนังสือให้คำยินยอมของเจ้าของข้อมูลให้บริษัทข้อมูลเครดิต

3. หนังสือให้คำยินยอมของเจ้าของข้อมูลต้องเป็นการยินยอมให้บริษัทข้อมูลเครดิตเปิดเผย หรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์การให้สินเชื่อ รวมทั้งการรับประกันภัย การรับประกันชีวิต และการออกบัตรเครดิตด้วย

4. หนังสือให้คำยินยอมจากเจ้าของข้อมูลที่มีอยู่แล้วก่อนวันที่ 14 มีนาคม พ.ศ.2546 และคำยินยอมดังกล่าวเป็นไปตามข้อ 3. โดยยังมีผลใช้บังคับอยู่ ก็สามารถใช้ต่อไปได้ ทั้งนี้บริษัทข้อมูลเครดิตจะต้องได้รับหนังสือดังกล่าวด้วย บริษัทข้อมูลเครดิตจึงควรดำเนินการให้สมาชิกหรือผู้ใช้บริการรวบรวมหนังสือให้คำยินยอมที่มีอยู่แล้ว ส่งให้บริษัทข้อมูลเครดิตโดยเร็ว

ปัญหาในเรื่องการขอความยินยอมจากเจ้าของข้อมูลโดยบริษัทข้อมูลเครดิตนั้น เมื่อคณะกรรมการคุ้มครองข้อมูลเครดิตได้มีหนังสือเวียนเพื่อซักซ้อมความเข้าใจในเรื่องดังกล่าว โดยกำหนดให้สมาชิกหรือผู้ใช้บริการเป็นผู้ดำเนินการให้เจ้าของข้อมูลทำหนังสือให้ความยินยอมแทนบริษัทข้อมูลเครดิต เนื่องจากบริษัทข้อมูลเครดิตนั้นไม่ได้เป็นผู้มีนิติสัมพันธ์ หรือทำการติดต่อกับ

เจ้าของข้อมูลที่เป็นลูกค้านั้นโดยตรง การให้สมาชิกเป็นผู้มีหน้าที่ดำเนินการในเรื่องการขอความยินยอมนี้จึงเป็นไปเพื่อให้สอดคล้องกับการปฏิบัติงานตามสถานการณ์จริง อีกทั้งยังรองรับการสื่อสารทางอิเล็กทรอนิกส์อื่นๆ เพื่อความรวดเร็วในการดำ เนินการก่อนส่งหนังสือยินยอมฉบับจริง

และภายหลังจากนั้นได้มีประกาศคณะกรรมการคุ้มครองข้อมูลเครดิตเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการได้รับความยินยอมจากเจ้าของข้อมูลเพื่อการเปิดเผยข้อมูล ลงวันที่ 14 กันยายน พ.ศ.2550 โดยอาศัยอำ นาจตามความในมาตรา 20 แห่งพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการได้รับความยินยอมจากเจ้าของข้อมูล เพื่อการเปิดเผยข้อมูล ดังนี้

1. ในการที่บริษัทข้อมูลเครดิตจะเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการที่ประสงค์จะใช้ข้อมูลเพื่อประโยชน์ในการวิเคราะห์สินเชื่อ หรือการออกบัตรเครดิต จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน โดยถือปฏิบัติ ดังนี้

(1) การได้รับความยินยอมอาจเป็นหนังสือ หรือวิธีการอื่นอันได้แก่ ผ่านทาง website โทรสาร เครื่องเบิกถอนเงินอัตโนมัติ (ATM) หรือผ่านทางระบบตอบรับอัตโนมัติทางโทรศัพท์ (interactive voice response : IVR)

ทั้งนี้ วิธีการให้ความยินยอมดังกล่าวจะต้องเป็นไปตามความสมัครใจของเจ้าของข้อมูลเท่านั้น และบริษัทข้อมูลเครดิตต้องแจ้งให้ลูกค้าทราบถึงวิธีการและเงื่อนไขของวิธีการให้ความยินยอมแต่ละวิธีที่ลูกค้าเลือกใช้อย่างชัดเจน

(2) ในการได้รับความยินยอมจากเจ้าของข้อมูล บริษัทข้อมูลเครดิตต้องจัดให้มีกระบวนการตรวจสอบตัวตนของเจ้าของข้อมูล เพื่อป้องกันการให้ความยินยอมโดยบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูลและสามารถใช้เป็นหลักฐานเพื่อพิสูจน์ข้อเท็จจริงกับเจ้าของข้อมูลได้

2. เปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการตามนัยมาตรา 20 วรรคหนึ่ง ซึ่งบริษัทข้อมูลเครดิตจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนทุกครั้ง เว้นแต่เจ้าของข้อมูลได้ให้ความยินยอมไว้เป็นอย่างอื่น บริษัทข้อมูลเครดิตอาจขอให้เจ้าของ

ข้อมูลไม่ต้องให้ความยินยอมใหม่ทุกครั้งในกรณีที่สมาชิกหรือผู้ใช้บริการรายนั้นประสงค์จะใช้ข้อมูลเพื่อประโยชน์ ดังต่อไปนี้

(1) การทบทวนสินเชื่อ

(2) การต่ออายุสัญญาสินเชื่อและสัญญาบัตรเครดิต

(3) การบริหารและป้องกันความเสี่ยงตามคำ สั่งของธนาคารแห่งประเทศไทย

ทั้งนี้ ให้บริษัทข้อมูลเครดิตระบุการให้ความยินยอมในการเปิดเผยข้อมูลเพื่อประโยชน์ดังกล่าวไว้ เพื่อให้เจ้าของข้อมูลทราบก่อนให้ความยินยอม

สำหรับความยินยอมที่เจ้าของข้อมูลได้ให้แก่บริษัทข้อมูลเครดิตไว้เดิมก่อนวันที่ประกาศฉบับนี้จะมีผลบังคับใช้ หากความยินยอมดังกล่าวระบุไว้ว่า การเปิดเผยข้อมูลเป็นไปตามกฎหมายว่าด้วยการประกอบธุกิจข้อมูลเครดิต ให้บริษัทข้อมูลเครดิตเปิดเผยข้อมูลเพื่อประโยชน์ตามข้อ (1) ถึง (3) ดังกล่าวได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลอีก แต่ให้บริษัทข้อมูลเครดิตแจ้งวัตถุประสงค์ในการใช้ข้อมูลตามข้อ (1) ถึง (3) ให้เจ้าของข้อมูลทราบด้วย

3. บริษัทข้อมูลเครดิตอาจตกลงให้สมาชิกหรือผู้ใช้บริการเป็นผู้ดำ เนินการแจ้งวัตถุประสงค์ในการใช้ข้อมูลตามข้อ (1) ถึง (3) ไปยังเจ้าของข้อมูล หรือให้เจ้าของข้อมูลให้ความยินยอมแก่บริษัทข้อมูลเครดิต แล้วแต่กรณี เพื่อบริษัทข้อมูลเครดิตสามารถเปิดเผยข้อมูลของเจ้าของข้อมูลนั้น แก่สมาชิกหรือผู้ใช้บริการ และอาจให้สมาชิกหรือผู้ใช้บริการเป็นผู้รับความยินยอมนั้นแทนบริษัทข้อมูลเครดิต เพื่อรวบรวมส่งให้บริษัทข้อมูลเครดิตในภายหลัง

4. เพื่อความสะดวกและรวดเร็วในการพิ จารณาอนุมัติสินเชื่อหรือเครดิต เมื่อเจ้าของข้อมูลให้ความยินยอมแก่บริษัทข้อมูลเครดิตแล้ว บริษัทข้อมูลเครดิตอาจตกลงให้สมาชิกหรือผู้ใช้บริการแจ้งให้บริษัทข้อมูลเครดิตทราบการให้ความยินยอมด้วยหนังสือ หรือสื่ออิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่ตกลงกันไว้ล่วงหน้า ก่อนส่งหลักฐานการให้ความยินยอมของเจ้าของข้อมูลให้บริษัทข้อมูลเครดิต

จากประกาศฉบับนี้จะเห็นได้ว่า คณะกรรมการคุ้มครองข้อมูลเครดิต โดยอาศัยอำ นาจตามพระราชบัญญัติคุ้มครองข้อมูลเครดิต มาตรา 20 ได้มีการกำ หนดแนวทางปฏิบัติในเรื่องการให้ความยินยอมของเจ้าของข้อมูลไว้ โดยมีสาระสำ คัญสรุปได้ ดังนี้

1.วิธีการให้ความยินยอม

ตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 นั้นกำ หนดไว้แต่เพียงว่าต้องมีการให้กำ ยินยอมโดยเจ้าของข้อมูล โดยไม่ได้ระบุวิธีการไว้โดยเฉพาะ และกำ หนดให้เป็นหน้าที่ของคณะกรรมการในการออกประกาศต่อไป ซึ่งในปัจจุบันนี้การติดต่อสื่อสารกันนั้นสามารถทำ ได้หลายทาง มีเทคโนโลยีในการสื่อสารมากยิ่งขึ้น เพื่อให้การให้ความยินยอมนั้นเป็นไปโดยสะดวกและรวดเร็วทั้งในด้านของเจ้าของข้อมูลและในด้านสมาชิกเอง จึงมีการกำ หนดวิธีการในการให้ความยินยอมไว้ในประกาศฉบับนี้ กล่าวคือ การได้รับความยินยอมอาจเป็นหนังสือ หรือวิธีการทางเทคโนโลยีอื่นๆ อันได้แก่ ผ่านทางเว็บไซต์ โทรสาร เครื่องเบิกถอนเงินอัตโนมัติ (ATM) หรือผ่านทางระบบตอบรับอัตโนมัติทางโทรศัพท์ (interactive voice response : IVR) แต่อย่างไรก็ตามยังคงให้ความคุ้มครองแก่เจ้าของข้อมูลอยู่ โดยกำ หนดไว้ให้วิธีการให้ความยินยอมดังกล่าวจะต้องเป็นไปตามความสมัครใจของเจ้าของข้อมูลเท่านั้น และบริษัทข้อมูลเครดิตต้องแจ้งให้ลูกค้าทราบถึงวิธีการและเงื่อนไขของวิธีการให้ความยินยอมแต่ละวิธีที่ลูกค้าเลือกใช้อย่างชัดเจน จึงเป็นหน้าที่อย่างหนึ่งของบริษัทข้อมูลเครดิต หรือสมาชิกผู้ขอความยินยอมจากเจ้าของข้อมูลที่จะต้องระบุไว้ถึงวิธีการ และเงื่อนไขต่างๆ ในการให้ความยินยอมนั้นให้เจ้าของข้อมูลเข้าใจได้อย่างชัดเจนด้วย

อีกทั้งยังได้กำ หนดให้บริษัทข้อมูลเครดิตจัดให้มีกระบวนการตรวจสอบตัวตนของเจ้าของข้อมูลผู้ที่ให้ความยินยอมนั้นว่าเป็นเจ้าของข้อมูลที่แท้จริง ซึ่งถือเป็นมาตรการที่สำ คัญยิ่งในการคุ้มครองเจ้าของข้อมูลอีกชั้นหนึ่ง เพื่อป้องกันการให้ความยินยอมโดยบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูล อีกทั้งยังช่วยให้มีหลักฐานเพื่อพิสูจน์ข้อเท็จจริงกับเจ้าของข้อมูลได้ในกรณีที่มีการโต้แย้งความถูกต้องของการให้ความยินยอมในภายหลัง

2.กรณีที่กำ หนดให้ไม่จำ เป็นต้องมีการให้ความยินยอมใหม่

โดยหลักแล้วนั้นการให้ความยินยอมของเจ้าของข้อมูลในการเปิดเผย หรือให้ข้อมูลแก่สมาชิก หรือผู้ใช้บริการในครั้งใด ก็จะมีผลเป็นการให้ความยินยอมในครั้งนั้นโดยเฉพาะ ถ้าหากจะมีการเปิดเผยข้อมูลของเจ้าของข้อมูลนั้นในครั้งต่อไป ก็จะต้องมีการให้

ความยินยอมกันใหม่ แต่ถ้าหากเป็นกรณีที่เป็นไปตามในประกาศฉบับนี้ บริษัทข้อมูลเครดิตอาจขอให้เจ้าของข้อมูลไม่ต้องให้ความยินยอมใหม่ทุกครั้ง ซึ่งได้แก่กรณีที่สมาชิกหรือผู้ใช้บริการรายนั้นประสงค์จะใช้ข้อมูลเพื่อประโยชน์ ดังต่อไปนี้

(1) การทบทวนสินเชื่อ

(2) การต่ออายุสัญญาสินเชื่อและสัญญาบัตรเครดิต

(3) การบริหารและป้องกันความเสี่ยงตามคำ สั่งของธนาคารแห่งประเทศไทย

ซึ่งถึงแม้จะไม่ต้องมีการขอความยินยอมใหม่ แต่ก็เป็นหน้าที่ของบริษัทข้อมูลเครดิตที่จะต้องระบุการให้ความยินยอมในการเปิดเผยข้อมูลเพื่อประโยชน์ดังกล่าวไว้ เพื่อให้เจ้าของข้อมูลทราบก่อนให้ความยินยอมด้วย

สำหรับความยินยอมที่เจ้าของข้อมูลได้ให้แก่บริษัทข้อมูลเครดิตไว้เดิมก่อนวันที่ประกาศฉบับนี้จะมีผลบังคับใช้ หากความยินยอมดังกล่าวระบุไว้ว่า การเปิดเผยข้อมูลเป็นไปตามกฎหมายว่าด้วยการประกอบธุกิจข้อมูลเครดิต ให้บริษัทข้อมูลเครดิตเปิดเผยข้อมูลเพื่อประโยชน์ตามข้อ (1) ถึง (3) ดังกล่าวได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลอีก แต่ให้บริษัทข้อมูลเครดิตแจ้งวัตถุประสงค์ในการใช้ข้อมูลตามข้อ (1) ถึง (3) ให้เจ้าของข้อมูลทราบด้วย

จะเห็นได้ว่ากรณีที่กำ หนดให้ไม่ต้องมีการขอความยินยอมจากเจ้าของข้อมูลใหม่นั้น ล้วนเป็นการที่ใช้ข้อมูลเพื่อประโยชน์ในกรณีที่เกี่ยวข้องกับผู้ที่ลูกหนี้มีนิติสัมพันธ์ด้วยอยู่แล้ว กล่าวคือเป็นสมาชิกหรือผู้ใช้บริการที่ลูกหนี้ได้เคยให้ความยินยอมในการเปิดเผยข้อมูลไว้แล้วนั่นเอง จึงไม่เป็นการล่วงล้ำ สิทธิของเจ้าของข้อมูลนั้นมากจนเกินสมควร อีกทั้งก็ได้กำ หนดให้บริษัทข้อมูลเครดิตต้องแจ้งให้เจ้าของข้อมูลทราบโดยชัดแจ้งถึงวิธีการ และเงื่อนไขในการให้ความยินยอมของตนก่อนที่จะทำ การให้ความยินยอมอยู่แล้ว จึงเป็นมาตรการที่เหมาะสม และเป็นไปเพื่อความสะดวกของทุกฝ่าย

3. การแจ้งความยินยอมนั้นไปยังบริษัทข้อมูลเครดิต

ดังที่ได้กล่าวไปแล้วข้างต้นว่าบริษัทข้อมูลเครดิตอาจให้สมาชิกหรือผู้ใช้บริการเป็นผู้รับความยินยอมจากเจ้าของข้อมูลได้แทนได้ แล้วรวบรวมส่งให้บริษัทข้อมูลเครดิตในภายหลัง ในกรณี

การแจ้งวัตถุประสงค์ในการใช้ข้อมูลตามข้อ (1) ถึง (3) ไปยังเจ้าของข้อมูลก็ถูกกำหนดไว้ในแนวเดียวกัน คือบริษัทข้อมูลเครดิตอาจตกลงให้สมาชิกหรือผู้ใช้บริการเป็นผู้ดำเนินการแทนได้ ซึ่งจะทำให้สอดคล้องกับข้อเท็จจริงในทางปฏิบัตินั่นเอง

อีกทั้งการรวบรวมหลักฐานการให้ความยินยอมของเจ้าของข้อมูลส่งให้บริษัทข้อมูลเครดิตนั้นอาจต้องใช้ระยะเวลา ซึ่งอาจไม่ทันกับสถานการณ์เร่งด่วนของการประกอบธุรกิจในปัจจุบัน ประกาศนี้จึงกำหนดให้บริษัทข้อมูลเครดิตอาจตกลงให้สมาชิกหรือผู้ใช้บริการแจ้งให้บริษัทข้อมูลเครดิตทราบการให้ความยินยอมด้วยหนังสือ หรือสื่ออิเล็กทรอนิกส์ หรือวิธีการอื่นใดก่อนที่จะส่งหลักฐานดังกล่าวนั้นให้บริษัทข้อมูลเครดิตก็ได้

นอกจากนี้ยังมีประเด็นในเรื่องการใช้หนังสือให้ความยินยอมฉบับเดียว ในการพิจารณาสินเชื่อที่ประกอบไปด้วยสินเชื่อหลายประเภทในคราวเดียวกัน หรือพิจารณาสินเชื่อที่เป็น package เช่น บัตรเครดิต และสินเชื่อส่วนบุคคล หรือ O/D ,P/N และ Loan ซึ่งแต่ละวงเงินต้องลงนามในสัญญาต่างฉบับกัน แต่มีการพิจารณาในครั้งเดียวกัน ซึ่งในเรื่องนี้ ถ้าหากพิจารณาถึงวัตถุประสงค์ของพระราชบัญญัติฉบับนี้ก็เห็นได้ว่าเป็นไปเพื่อต้องการให้มีข้อมูลเกี่ยวกับการใช้สินเชื่อของลูกค้าครบทุกประเภท ดังนั้นจึงควรมีการกำหนดให้หนังสือให้ความยินยอมฉบับเดียวนั้นมีผลสำหรับสินเชื่อทุกประเภทที่พิจารณาในคราวเดียวกันนั้นได้ ซึ่งกรณีที่ลูกค้ามาขอสินเชื่อหลายประเภทในคราวเดียวกันนี้ ควรจะให้ลูกค้าทำหนังสือให้ความยินยอมฉบับเดียวทั้ง package ได้ แต่อย่างไรก็ดีหากลูกค้ารายเดิมมาขอสินเชื่อเพิ่มเติมภายหลัง ก็จะต้องให้ความยินยอมใหม่อีกครั้ง ซึ่งเป็นไปตามหลักของการให้ความยินยอมนั่นเอง

และคณะกรรมการคุ้มครองข้อมูลเครดิตได้มีหนังสือตอบข้อหารือที่กคค. 40/2550 เรื่องการหารือเกี่ยวกับแนวทางปฏิบัติในการประกอบธุรกิจข้อมูลเครดิต โดยระบุว่ากรณีที่มีการพิจารณาสินเชื่อที่ประกอบไปด้วยสินเชื่อหลายประเภทในคราวเดียวกัน หรือพิจารณาสินเชื่อที่เป็น package เช่น บัตรเครดิต และสินเชื่อส่วนบุคคล หรือ O/D, P/N และ Loan โดยมีสัญญาต่างฉบับกันสามารถ

ใช้หนังสือให้ความยินยอมฉบับเดียวกันได้ หากลูกค้าทราบว่าเป็นการให้ความยินยอมทุกประเภทสินเชื่อ[27]

เมื่อพิจารณาถึงการออกประกาศของคณะกรรมการคุ้มครองข้อมูลเครดิตในลักษณะดังกล่าวข้างต้นแล้ว จะเห็นได้ว่าแม้จะเป็นการอำนวยความสะดวกในการขอความยินยอมจากเจ้าของข้อมูล แต่ในขณะเดียวกันก็ส่งผลเป็นการลดความเคร่งครัดของหลักการให้ความยินยอมลง จากที่เดิมเมื่อมีการประกาศใช้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ได้มีการกำหนดไว้ว่า ความยินยอมนี้จะต้องเป็นหนังสือ แต่ต่อมาเมื่อมีการแก้ไขเพิ่มเติมพระราชบัญญัติในพ.ศ.2549 นั้นก็ได้กำหนดให้ความยินยอมต้องเป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะกรรมการประกาศกำหนด และภายหลังก็มีการออกประกาศต่างๆ ในเรื่องหลักเกณฑ์ วิธีการ และเงื่อนไขเกี่ยวกับการได้รับความยินยอมจากเจ้าของข้อมูลเพื่อการเปิดเผยข้อมูลของคณะกรรมการคุ้มครองข้อมูลเครดิต โดยกำหนดวิธีการให้ความยินยอมหลายรูปแบบที่สามารถกระทำได้โดยง่าย ซึ่งในมุมมองหนึ่งอาจเป็นการให้ความสะดวกในการดำเนินธุรกิจข้อมูลเครดิตให้สามารถเป็นไปได้อย่างรวดเร็ว แต่ในอีกมุมหนึ่งนั้นก็ยิ่งเป็นการเน้นถึงประเด็นในเรื่องความจำเป็นของการให้ความยินยอมดังกล่าว ที่ได้มีการอธิบายไว้ข้างต้นนั่นเอง ส่งผลให้หลักการให้ความยินยอมนั้นหมดความสำคัญลง ซึ่งในประเด็นดังกล่าวนี้มีความเห็นว่า แทนที่จะมีการออกประกาศซึ่งมีลักษณะหละหลวม และลดความเคร่งครัดของหลักการของกฎหมายในเรื่องการให้ความยินยอมลงนั้น ควรที่จะมีการพิจารณาถึงความสำคัญ ความจำเป็น และประสิทธิภาพในทางปฏิบัติของการให้ความยินยอมของเจ้าของข้อมูลแทน เพื่อให้เกิดเป็นการแก้ปัญหาได้อย่างตรงตามสาเหตุที่แท้จริง และจะส่งผลดีต่อระบบการประกอบธุรกิจข้อมูลเครดิตได้มากกว่าอีกด้วย

(2) ระยะเวลาการมีผลบังคับของความยินยอมของเจ้าของข้อมูล

---

[27] รายงานการประชุมคณะกรรมการคุ้มครองข้อมูลเครดิต ครั้งที่2/2550 วันที่ 25 กรกฎาคม พ.ศ.2550

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ไม่ได้กำหนดในเรื่องระยะเวลาของความยินยอมที่ได้ให้ไว้แล้วว่าจะมีผลใช้ได้เพียงใด และเมื่อพิจารณาถึงกฎหมาย Data Protection Act 1998 ของประเทศอังกฤษก็ไม่ได้กำหนดในเรื่องดังกล่าวนี้ด้วยเช่นกัน แต่หากพิจารณาจากแนวทางของประเทศอังกฤษซึ่ง The Information Commissioner ได้ให้คำแนะนำเพื่อวางแนวทางในเรื่องความยินยอมนี้ โดยระบุว่า แม้จะมีการให้ความยินยอมไว้แล้ว ก็ไม่จำเป็นที่ความยินยอมนั้นจะต้องคงอยู่ตลอดไป ในกรณีส่วนใหญ่ความยินยอมจะยังคงอยู่ตราบเท่าที่การประมวลผลที่เกี่ยวข้องนั้นยังคงดำเนินต่อไป ผู้ควบคุมข้อมูลจะต้องคำนึงว่าเจ้าของข้อมูลสามารถเพิกถอนความยินยอมนั้นได้ โดยขึ้นอยู่กับลักษณะของความยินยอม และข้อเท็จจริงของการประมวลผลข้อมูล อีกทั้งความยินยอมนั้นจะต้องมีความเหมาะสมตามแต่ละสถานการณ์ด้วย อาทิ ถ้าหากการประมวลผลข้อมูลซึ่งเกี่ยวข้องนั้นจะดำเนินต่อไปโดยไม่มีกำหนด หรือจะดำเนินต่อไปภายหลังจากที่ความสัมพันธ์ทางการค้าได้สิ้นสุดลง ในกรณีเช่นนั้น ความยินยอมก็ควรจะครอบคลุมถึงสถานการณ์เหล่านั้นด้วย[28]

แต่ถ้าหากมีการปรับใช้หลักการดังกล่าวกับการประกอบธุรกิจข้อมูลเครดิต ก็อาจเกิดเป็นปัญหาในทางปฏิบัติขึ้นได้ กล่าวคือหากเจ้าของข้อมูลมีสิทธิเพิกถอนความยินยอมเมื่อใดก็ได้แล้ว ก็ย่อมเกิดอุปสรรคในการดำเนินธุรกิจข้อมูลเครดิตขึ้น ยกตัวอย่างจากกรณีที่เจ้าของข้อมูลได้ให้ความยินยอม และสามารถดำเนินกระบวนการต่อไปจนได้รับสินเชื่อแล้ว จึงทำการเพิกถอนความยินยอมดังกล่าว ปัญหาจะเกิดจากการที่สมาชิกซึ่งเป็นผู้ให้สินเชื่ออาจจะไม่ได้รับข้อมูลที่ครบถ้วนต่อไปในการพิจารณาสินเชื่อได้

การพิจารณาในประเด็นนี้ จึงต้องคำนึงถึงลักษณะของความยินยอม ข้อเท็จจริงของการประมวลผลข้อมูล และวัตถุประสงค์ในเรื่องดังกล่าวประกอบด้วย เมื่อเป็นการให้ความยินยอมเพื่อให้สมาชิกสามารถใช้ข้อมูลเครดิตของเจ้าของข้อมูลในการพิจารณาสินเชื่อแล้วนั้น ความยินยอมดังกล่าวจึงจะต้องยังคงมีผลอยู่ตลอดเพื่อการใช้ข้อมูลให้เป็นไปตามวัตถุประสงค์นั้น ดังนั้นความยินยอมของเจ้าของข้อมูลจึงจะต้องมีผลภายในระยะเวลา

---

28 Rosemary Jay, *supra note23,* p.154

ตราบเท่าที่ความเป็นหนี้ของเจ้าของข้อมูลนั้นยังมีอยู่ ไม่สามารถนำหลักการที่อนุญาตให้สิทธิในการเพิกถอนความยินยอมมาปรับใช้กับธุรกิจข้อมูลเครดิตได้ เนื่องจากตามหลักการในเรื่องให้ความยินยอมนั้น ความยินยอมในการเปิดเผยข้อมูลเครดิตถือเป็นสาระสำคัญของการอนุมัติให้สินเชื่อ ส่งผลให้เป็นเงื่อนไขหรือองค์ประกอบสำคัญที่ว่าในระยะเวลาที่เจ้าของข้อมูลยังมีความเป็นหนี้อยู่ เจ้าของข้อมูลจะเพิกถอนการให้ความยินยอมไม่ได้ กล่าวคือตราบใดที่มีหนี้ระหว่างสมาชิกผู้ใช้ข้อมูลกับเจ้าของข้อมูล ความยินยอมนั้นก็จะต้องยังคงมีผลอยู่ เจ้าของข้อมูลไม่มีสิทธิในการที่จะเพิกถอนความยินยอมได้ทุกเมื่อ แต่ควรกำหนดให้เพิกถอนได้เฉพาะในบางกรณี อาทิ เมื่อมีการใช้ข้อมูลโดยไม่ถูกต้องหรือไม่ชอบด้วยกฎหมาย หรือเมื่อมีการเปิดเผยข้อมูลอื่นๆ นอกเหนือไปจากข้อมูลที่เกี่ยวข้องกับความสามารถในการชำระสินเชื่อ เป็นต้น

2. หลักการและปัญหากรณีการเปิดเผยข้อมูลเครดิตโดยไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 20 วรรคสอง

หลักการให้ความยินยอมของเจ้าของข้อมูลในการเปิดเผยข้อมูลเครดิตนั้น ได้มีกรณีที่เป็นข้อยกเว้นไว้ตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 มาตรา 20 วรรคสอง ซึ่งในหัวข้อนี้จะมีการอธิบายถึงกรณียกเว้นเหล่านี้ รวมไปทั้งประเด็นปัญหาที่อาจเกิดขึ้น

2.1 เหตุผลของกฎหมายในกรณีการเปิดเผยข้อมูลเครดิตโดยไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลตามมาตรา 20 วรรคสอง

การกำหนดกรณียกเว้นที่ทำให้บริษัทข้อมูลเครดิตทำการเปิดเผยข้อมูลเครดิตได้โดยไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนนั้น ถ้าหากศึกษาดูจากขั้นตอนการพิจารณาร่างพระราชบัญญัติ ก็จะเห็นได้ว่าในเบื้องแรกเลยนั้น การเปิดเผยข้อมูลเครดิตไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูล แต่พอได้มีการพิจารณาร่างพระราชบัญญัตินี้ในรัฐสภา ก็ได้มีการนำ

หลักเรื่องความยินยอมนี้มาใช้ โดยกำ หนดข้อยกเว้นไว้ในกรณีหลักๆ คือการเปิดเผยข้อมูลตามคำ สั่งศาลหรือหมายศาล การเปิดเผยเพื่อประโยชน์ในการสอบสวน หรือกรณีอื่นๆ ที่กฎหมายกำ หนด และเมื่อมีการพิจารณาในวุฒิสภา หลักการให้ความยินยอมนี้ก็ยังคงอยู่ โดยในเรื่องของข้อยกเว้นได้มีการกำ หนดเพิ่มเติมกล่าวคือ การเปิดเผยตามคำ สั่งศาลหรือหมายศาล การเปิดเผยเมื่อมีหนังสือจากพนักงานสอบสวน การเปิดเผยเมื่อมีหนังสือจากหน่วยงานที่มีหน้าที่ในการกำ กับดูแล หรือตรวจสอบสถาบันการเงิน ส่วนในการพิจารณาร่วมกันของกรรมาธิการของทั้งสองสภานั้น ได้มีการกำหนดเพิ่มเติมอีกกรณีหนึ่ง คือ การเปิดเผยข้อมูลเกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณชน ให้สามารถทำ ได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูลเช่นเดียวกัน นอกจากนั้นยังมีการกำ หนดหน้าที่ของบริษัทข้อมูลเครดิตเพิ่มเติมในกรณีที่มีการเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลก่อนตาม กรณีที่เป็นข้อยกเว้นเหล่านี้ คือต้องแจ้งเป็นหนังสือไปยังเจ้าของข้อมูลเพื่อให้ทราบถึงการเปิดเผยนั้นภายใน 30 วัน นับแต่วันที่เปิดเผยหรือให้ข้อมูลดังกล่าวด้วย หรือกรณีที่เป็นการให้ข้อมูลโดยรวมของสถาบันการเงิน ก็ให้แจ้งแก่สถาบันการเงินนั้นๆ ทราบ

เมื่อวิเคราะห์ถึงการพิจารณาร่างพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต ข้างต้นจึงจะเห็นได้ว่าการกำ หนดข้อยกเว้นของหลักการให้ความยินยอมดังกล่าวนั้น ก็ให้เป็นไปเพื่อให้สามารถมีการใช้ข้อมูลเครดิตเป็นพยานหลักฐานในการพิจารณาคดี การสืบสวนสอบสวนของเจ้าหน้าที่ และเพื่อประโยชน์ในการตรวจสอบกำ กับดูแลของเจ้าหน้าที่ เป็นต้น และได้มีการกำ หนดให้มีการแจ้งการเปิดเผยข้อมูลดังกล่าวนั้นไปยังเจ้าของข้อมูลด้วย ซึ่งในประเด็นดังกล่าวนี้ อาจเป็นประเด็นที่จะต้องมีการวิเคราะห์ถึงความจำเป็น และความเหมาะสม ซึ่งจะกล่าวถึงต่อไปภายในหัวข้อนี้

ดังนั้น เมื่อมีการประกาศใช้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ในมาตรา 20 วรรคสอง จึงมีการบัญญัติไว้ว่า

นอกจากการเปิดเผยหรือให้ข้อมูลแก่สมาชิกหรือผู้ใช้บริการตามวรรคหนึ่ง ให้บริษัทข้อมูลเครดิตเปิดเผยหรือให้ข้อมูลได้ในกรณีดังต่อไปนี้โดยไม่ต้องได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลก่อน

(1) เมื่อมีคำสั่งศาลหรือตามหมายศาลหรือเป็นข้อมูลเกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ

(2) เมื่อมีหนังสือจากพนักงานสอบสวนเพื่อประโยชน์ในการสอบสวนความผิดอาญาเกี่ยวกับธุรกิจการเงินซึ่งตนเป็นผู้รับผิดชอบการสอบสวนคดีดังกล่าว

(3) เมื่อมีหนังสือจากกระทรวงการคลัง ธนาคารแห่งประเทศไทย คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เพื่อประโยชน์ในการปฏิบัติการกำกับดูแล หรือตรวจสอบสถาบันการเงินตามกฎหมายว่าด้วยการนั้น

(4) เมื่อมีหนังสือจากบรรษัทตลาดรองสินเชื่อเพื่อที่อยู่อาศัยตามกฎหมายว่าด้วยบรรษัทตลาดรองสินเชื่อเพื่อที่อยู่อาศัยหรือนิติบุคคลเฉพาะกิจเพื่อการแปลงสินทรัพย์เป็นหลักทรัพย์ตามกฎหมายว่าด้วยนิติบุคคลเฉพาะกิจเพื่อการแปลงสินทรัพย์เป็นหลักทรัพย์ เพื่อใช้ประโยชน์ในการประเมินฐานะสินทรัพย์ที่นำมาแปลงเป็นหลักทรัพย์ตามกฎหมายว่าด้วยการนั้น ตามความจำเป็นแห่งกรณี

(5) เมื่อมีหนังสือจากบรรษัทบริหารสินทรัพย์ไทย ตามกฎหมายว่าด้วยบรรษัทบริหารสินทรัพย์ไทย บรรษัทบริหารสินทรัพย์สถาบันการเงิน ตามกฎหมายว่าด้วยบรรษัทบริหารสินทรัพย์สถาบันการเงิน หรือบริษัทบริหารสินทรัพย์ตามกฎหมายว่าด้วยบริษัทบริหารสินทรัพย์ เพื่อใช้ประโยชน์ในการประเมินราคาสินทรัพย์ที่รับซื้อหรือรับโอนตามกฎหมายว่าด้วยการนั้น ตามความจำเป็นแห่งกรณี

ทั้งนี้ การเปิดเผยข้อมูลตาม (4) หรือ (5) ต้องได้รับความเห็นชอบจากคณะกรรมการคุ้มครองข้อมูลเครดิต

และเมื่อมีการเปิดเผยหรือให้ข้อมูลตามวรรคสองแล้ว ให้บริษัทข้อมูลเครดิตแจ้งเป็นหนังสือแก่เจ้าของข้อมูลทราบภายใน 30 วันนับแต่วันเปิดเผยหรือให้ข้อมูล ในกรณีที่เป็นข้อมูลโดยรวมของสถาบันการเงินแห่งหนึ่งแห่งใดให้แจ้งแก่สถาบันการเงินนั้นทราบ

2.2 ปัญหาการเปิดเผยข้อมูลเครดิตกรณีที่มีคำสั่งศาลหรือตามหมายศาล

ดังที่มีการกล่าวข้างต้น ข้อยกเว้นหลักความยินยอมของเจ้าของข้อมูลนั้นมีการกำหนดไว้ 5 กรณีด้วยกัน โดยที่ส่วนใหญ่แล้วกรณีข้อยกเว้นเหล่านั้นจะมีการกำหนดวัตถุประสงค์ในการใช้ข้อมูลไว้ด้วย กล่าวคือ เพื่อประโยชน์ในการสอบสวนความผิดอาญา เกี่ยวกับธุรกิจการเงิน, เพื่อประโยชน์ในการปฏิบัติการกำกับดูแล หรือตรวจสอบสถาบันการเงิน, เพื่อประโยชน์ในการประเมินฐานะสินทรัพย์ที่นำมาแปลงเป็นหลักทรัพย์ หรือเพื่อประโยชน์ในการประเมินราคาสินทรัพย์ที่รับซื้อหรือรับโอน แต่มีเพียงกรณีตามข้อ (1) การเปิดเผยข้อมูลเครดิตกรณีที่มีคำสั่งศาลหรือตามหมายศาล เท่านั้นที่มีลักษณะเป็นการกำหนดไว้อย่างกว้างๆ โดยไม่มีการกำหนดวัตถุประสงค์ในการเปิดเผยและใช้ข้อมูลเครดิต

การกำหนดกรณียกเว้นของหลักความยินยอมในลักษณะดังกล่าว เมื่อพิจารณาแล้วอาจจะเห็นได้ว่าสามารถเกิดเป็นประเด็นปัญหา และส่งผลกระทบต่อเจ้าของข้อมูลได้ โดยที่การเปิดเผยข้อมูลตามคำสั่งศาลหรือตามหมายศาลนั้น อาจเกิดขึ้นได้ในกรณีข้อเท็จจริงที่ว่าคู่ความในคดีฝ่ายหนึ่งต้องการที่จะใช้รายงานข้อมูลเครดิตของอีกฝ่ายเพื่อจะกล่าวอ้างประเด็นในเรื่องสถานะทางการเงิน หรือความน่าเชื่อถือทางสินเชื่อของอีกฝ่ายนั้น หรือเพื่อหักล้างประเด็นดังกล่าวของอีกฝ่าย รวมถึงการเป็นพยานหลักฐานในการบังคับคดี เป็นต้น ถ้าหากมีการกำหนดข้อยกเว้นไว้อย่างกว้างตามกฎหมายเช่นนี้ จำเป็นหรือไม่ที่ศาลจะต้องอนุญาตให้มีการเปิดเผยข้อมูลดังกล่าวในทุกกรณี และควรจะมีหลักเกณฑ์หรือเงื่อนไขในการออกหมายหรือคำสั่งเพื่อเปิดเผยข้อมูลในลักษณะดังกล่าวนี้หรือไม่ อย่างไร ซึ่งสิ่งที่ควรพิจารณาก็คือ ความเกี่ยวข้องและความจำเป็นในการใช้ข้อมูลเครดิตในการพิจารณาตัดสินคดีดังกล่าว รวมไปถึงเงื่อนไขในการใช้ข้อมูลเครดิตด้วย

โดยลักษณะแล้วนั้น ข้อมูลเครดิตเป็นข้อมูลทางการเงินของบุคคลประเภทหนึ่งที่มีความสำคัญเป็นอย่างมาก การใช้ การจัดเก็บ หรือการเปิดเผยก็ควรจะเป็นไปเพื่อวัตถุประสงค์โดยเฉพาะเจาะจงที่มีความเกี่ยวข้องเท่านั้น ถ้าหากมีกฎหมายฉบับอื่นให้อำนาจองค์กรบังคับการตามกฎหมาย ในการใช้ข้อมูลเครดิตเพื่อให้มีการดำเนินการให้เป็นไปตามกฎหมายนั้นๆ ดังเช่นกรณีข้อยกเว้นตาม (2) ถึง (5) ก็ถือได้ว่ามีเหตุที่เพียงพอในการที่บริษัทข้อมูลเครดิตจะเปิดเผยข้อมูลเครดิตได้โดยไม่จำเป็นต้องได้รับความ

ยินยอมจากเจ้าของข้อมูล แต่ข้อยกเว้นในกรณีการเปิดเผยข้อมูลตามคำสั่งหรือหมายศาลนั้น แม้จะเป็นการออกหมายหรือคำสั่งโดยศาลก็ตาม แต่เมื่อพิจารณาแล้วเห็นว่าควรมีการกำหนดขอบเขตของข้อยกเว้นดังกล่าว เพื่อให้การใช้ข้อมูลเครดิตนั้นเป็นไปตามหลักการของกฎหมายด้วยนั่นเอง

และเมื่อศึกษาถึง Data Protection Act 1998 ของประเทศอังกฤษ ก็เห็นได้ว่ามีการกำหนดข้อยกเว้นกรณีที่การประมวลผลข้อมูลนั้นมิจำเป็นจะต้องกระทำตาม Data Protection Principles ไว้หลายกรณีด้วยกัน ซึ่งรวมไปถึง

(1) เพื่อความมั่นคงของประเทศ ตาม section 28

(2) เพื่อป้องกัน หรือตรวจพบการกระทำความผิดทางอาญา หรือเพื่อจับหรือดำเนินคดีกับผู้กระทำความผิด ตาม section 29 ซึ่งในข้อยกเว้นดังกล่าวนี้จะไม่รวมไปถึงการดำเนินคดีทางแพ่ง

(3) กรณีการเปิดเผยตามข้อกำหนดของกฎหมาย, หลักกฎหมาย, หรือคำสั่งของศาล ตาม section 35 (1) โดยข้อกำหนดของกฎหมายนั้น ได้แก่กฎหมายที่ออกโดยรัฐสภา และกฎหมายลำดับรองของกฎหมายดังกล่าว ส่วนหลักกฎหมายนั้นมักจะเป็นหลักตามกฎหมาย common law และคำสั่งศาลนั้น คือคำสั่งของศาล หรือ tribunal ที่มีสถานะของศาล โดยในกรณีที่มีการเปิดเผยข้อมูลเพื่อใช้ในการพิจารณาคดีในศาลแล้วนั้น หากคู่ความไม่ต้องการที่จะให้ข้อมูลของตนถูกเปิดเผยในเอกสารรายงานการพิจารณาคดี ซึ่งเป็นเอกสารที่สาธารณะชนสามารถขอตรวจสอบได้นั้น คู่ความดังกล่าวจะต้องทำการยื่นคำร้องขอต่อศาล เนื่องจากหลักการคุ้มครองความลับของข้อมูลส่วนบุคคลจะไม่นำมาปรับใช้อีกต่อไป

(4) กรณีที่การเปิดเผยนั้นจำเป็นเพื่อวัตถุประสงค์หรือเกี่ยวเนื่องกับการดำเนินคดีตามกฎหมาย (รวมไปถึงการดำเนินคดีที่คาดว่าจะเกิดขึ้นด้วย) ตาม section 35 (2) โดยที่มีเงื่อนไขที่ว่าจะต้องเป็นการเปิดเผยซึ่งผู้ที่เกี่ยวข้องนั้นเป็นคู่ความหรือเป็นพยานในการดำเนินคดีทางกฎหมาย หรือคาดว่าจะมีการดำเนินคดีทางกฎหมาย ซึ่งการคาดดังกล่าวนั้นอาจจะเป็นในลักษณะใดก็ได้

เนื่องจากไม่มีการกำหนดไว้ จึงเกิดความไม่ชัดเจนว่าจะต้องมีองค์ประกอบ หรือมีเจตนาเพียงใดในการที่จะดำเนินคดีทางกฎหมาย[29]

กรณีที่เกิดเป็นประเด็นในเรื่องข้อยกเว้นในการเปิดเผยข้อมูลส่วนบุคคลในประเทศอังกฤษนี้มักจะเป็นการเปิดเผยข้อมูลตามคำร้องขอของหน่วยงานทางกฎหมาย กล่าวคือ ผู้ควบคุมข้อมูลซึ่งได้รับคำร้องขอจากเจ้าหน้าที่ตำรวจ หรือหน่วยงานทางกฎหมายอื่นๆ ให้ทำการเปิดเผยข้อมูลส่วนบุคคลนั้น อาจพบว่าตนเองอยู่ในฐานะที่ลำบากเนื่องจากต้องชั่งน้ำหนักระหว่างการกระทำตามคำร้องขอดังกล่าว และการคุ้มครองผลประโยชน์ของลูกค้าของตน ในแง่หนึ่งผู้ควบคุมข้อมูลต้องคำนึงถึงสิทธิของเจ้าของข้อมูลตาม Data Protection Act 1998 และข้อยกเว้นตาม section 29 รวมไปถึงสิทธิตาม the Human Rights Act 1998 แต่อีกแง่หนึ่งเป็นปัญหาในเรื่องหน้าที่ในการให้ข้อมูลแก่เจ้าหน้าที่ โดยที่ section 29 นั้นไม่ได้กำหนดหน้าที่ใดๆ ในการเปิดเผยข้อมูล ดังนั้น หน้าที่ดังกล่าว ถ้าหากมีอยู่นั้น จึงจะต้องมีฐานมาจากกฎหมายฉบับอื่น

ใน Part 3 ของ Anti-Terrorism Crime and Security Act 2001 (ATCSA) ได้ขยายเหตุในการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลให้แก่หน่วยงานทางกฎหมาย ซึ่งโดยหลักแล้ว จะต้องมีจุดประสงค์เพื่อการสอบสวน หรือการดำเนินคดีทางอาญา และกฎหมายนี้ยังได้ยกเลิกข้อจำกัดในการเปิดเผยข้อมูลซึ่งรวมไปถึงข้อมูลส่วนบุคคลที่ได้กำหนดไว้ในกฎหมายกว่า 66 ฉบับ รวมไปถึง Data Protection Act ด้วย แต่อย่างไรก็ตาม ATCSA ไม่ได้มีลักษณะเป็นการบังคับแก่ผู้ควบคุมข้อมูลให้เปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานทางกฎหมาย

ตัวอย่างกรณีที่เกิดขึ้นในประเด็นเรื่องการเปิดเผยข้อมูลนี้อาทิ คดี R (on the application of NTL Group Ltd.) v. Crown Court at Ipswich ซึ่งได้มีการให้ความชัดเจนแก่ผู้ควบคุมข้อมูลในเรื่องนี้ไว้ กล่าวคือ NTL ผู้ร้องซึ่งเป็นบริษัทที่ให้บริการด้าน telecommunications ได้รับหมายจากเจ้าหน้าที่สืบสวนในการส่งมอบหลักฐานพิเศษ ตาม section 9 (Schedule 1) ของ the Police and Criminal Evidence Act 1984 (PACE) โดยตามกฎหมายแล้วนั้น ผู้ที่ได้รับหมายดังกล่าวจะต้องไม่ปกปิด, ทำลาย,

---

29 *Ibid*. p. 490, 565 and 567

แก้ไข หรือทำ จัดหลักฐานที่เกี่ยวข้อง เว้นแต่จะมีการทำ หนดยกเว้นหน้าที่ดังกล่าวโดยศาล หรือมีคำ อนุญาตเป็นหนังสือจากเจ้าหน้าที่สืบสวน ส่งผลให้ผู้ร้องมีความกังวลว่าการกระทำ ตามหมายของเจ้าหน้าที่ ซึ่งก็คือการย้ายการจัดเก็บจดหมายอิเล็กทรอนิกส์ของลูกค้าไปยังระบบอื่นนอกเหนือจากที่ผู้ส่งมีเจตนานั้น จะเป็นการละเมิด Regulation of Investigatory Powers Act 2000 (RIPA) ใน section 1 คือการดักจับข้อมูลการสื่อสารในระหว่างการส่งข้อมูล จึงนำ เรื่องขึ้นสู่ศาล

โดยศาลได้ตัดสินว่า ผู้ร้องไม่ได้มีการกระทำ ความผิดอาญาเมื่อได้รับหมายจากเจ้าหน้าที่ดังกล่าว โดยอาศัยเหตุผลที่ว่าตามเงื่อนไขของ Schedule 11 paragraph 11 ของ PACE นั้นผู้ที่ได้รับหมายดังกล่าวมีอำ นาจที่จะกระทำ การใดๆ เพื่อรักษาการสื่อสารทางอิเล็กทรอนิกส์ให้คงอยู่ในระบบจนกระทั่งถึงเวลาที่ศาลตัดสินว่าจะมีการออกคำ สั่งหรือไม่ ดังนั้น ระหว่างที่ยังไม่มีการออกคำสั่งของศาล เจ้าหน้าที่สืบสวนก็ไม่มีสิทธิในการเข้าถึงข้อมูลที่ผู้ร้องจัดเก็บไว้ จึงไม่เกิดการกระทบต่อสิทธิของบุคคลที่สามแต่อย่างใด

และในอีกคดีหนึ่ง คือคดี Totalise Plc v. Motley Fool Ltd. ซึ่งมีข้อเท็จจริงว่า Motley Fool จำเลยเป็นบริษัทให้บริการบริหารและจัดการเว็บไซต์ ซึ่งมีหน้าเว็บไซต์ที่มีพื้นที่ให้แสดงความคิดเห็น (discussion forum) แก่บริษัทต่างๆ รวมไปถึงบริษัทโจทก์ Totalise ด้วย และได้มีผู้ไม่ออกนาม ซึ่งใช้ชื่อว่า Z เข้าไปแสดงความคิดเห็นในหลายเว็บไซต์ของจำ เลยในลักษณะที่เป็นการกล่าวอ้างให้ร้าย ทำให้เสื่อมเสียชื่อเสียงแก่บริษัทโจทก์ ซึ่งหลังจากที่โจทก์ได้ร้องเรียนไปยังจำ เลยถึงเรื่องดังกล่าว จำเลยได้ทำ การลบข้อความเช่นว่านั้น และห้าม Z เข้าสู่ระบบ แต่อย่างไรก็ตาม จำเลยปฏิเสธที่จะเปิดเผยข้อมูลรายละเอียดของ Z ให้แก่โจทก์ทราบ โจทก์จึงนำ คดีขึ้นสู่ศาลร้องขอให้จำ เลยเปิดเผยตัวตนของ Z จำเลยนั้นได้กล่าวอ้างถึงนโยบายภายในของตนในการรักษาความลับและไม่เปิดเผยตัวตนของผู้ใช้ โดยอาศัยหลักตาม section 35 ของ Data Protection Act ซึ่งทำ หนดว่า ข้อมูลส่วนบุคคลที่จะได้รับการยกเว้นจากข้อทำ หนดในการห้ามเปิดเผย ในกรณีที่การเปิดเผยดังกล่าวนั้นมีความจำ เป็นตามกฎหมายเกี่ยวข้องกับการดำ เนินคดีนั้น จะต้องได้รับการตีความอย่างเคร่งครัด เพื่อให้ข้อมูลของ Z

นั้นได้รับความคุ้มครองตาม Data Protection Principles ซึ่งป้องกันการการเปิดเผยข้อมูลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ส่วนฝ่ายโจทก์ได้อ้างว่าไม่มีเหตุผลในการจำกัดการตีความตาม section 35 อีกทั้งอ้างถึงหลักอำนาจของศาลในการที่จะมีคำสั่งต่อบุคคลที่มีความเกี่ยวข้องกับการกระทำที่เป็นการละเมิดของผู้อื่นว่าสามารถนำมาใช้ได้และไม่ถูกจำกัดโดย Data Protection Act

ศาลได้มีคำตัดสินว่า ไม่มีเหตุในการจำกัดการตีความของ section 35 โดยที่ section นี้ไม่การจำกัดสิทธิของโจทก์ในการที่จะได้รับการเปิดเผยข้อมูลของผู้กระทำการละเมิด จากกรณีนี้เห็นได้ชัดว่า Z ได้ทำให้โจทก์เสื่อมเสียชื่อเสียงอย่างร้ายแรงโดยกระทำให้ลักษณะที่ไม่ออกนาม และโจทก์ก็ไม่มีวิธีอื่นที่จะทราบถึงตัวตนของ Z ได้ เมื่อชั่งน้ำหนักแล้วจึงเห็นว่าควรมีคำสั่งเพื่อเป็นประโยชน์แก่โจทก์ตามคำฟ้อง เพราะหากมิเป็นเช่นนี้ อาจเกิดการทำให้ผู้อื่นเสื่อมเสียชื่อเสียงโดยอาศัยวิธีการทางเว็บไซต์เช่นเดียวกับกรณีนี้ได้อีก

ดังนั้นจะเห็นได้ว่าในประเทศอังกฤษ หากมีกรณีตามข้อยกเว้นในการเปิดเผยข้อมูลเมื่อมีคำสั่งของเจ้าหน้าที่เช่นนี้ ถ้าหากผู้ควบคุมข้อมูลมีข้อสงสัยหรือเกิดความไม่แน่ใจในความชอบด้วยกฎหมายของการเปิดเผยข้อมูลส่วนบุคคลดังกล่าว ก็สามารถที่จะร้องขอให้เจ้าหน้าที่ออกหมายหรือมีคำสั่งเป็นลายลักษณ์อักษรหรืออย่างน้อยที่สุดก็ให้มีคำยืนยันเป็นลายลักษณ์อักษรจากเจ้าหน้าที่ว่าข้อมูลส่วนบุคคลนั้นจำเป็นต่อการสืบสวนความผิดทางอาญา และการขอความยินยอมจากเจ้าของข้อมูลนั้นจะเป็นการขัดขวางต่อการสืบสวน และถ้าหากเป็นไปได้ควรมีการกำหนดไว้ในข้อสัญญาเบื้องต้นกับเจ้าของข้อมูลว่า ผู้ควบคุมข้อมูลสามารถทำการเปิดเผยข้อมูลส่วนบุคคลแก่เจ้าหน้าที่ได้ ในกรณีที่มีเหตุสมควรที่จะเชื่อได้ว่ามีการกระทำการที่ไม่ชอบด้วยกฎหมาย[30]

เมื่อวิเคราะห์ใช้ในเรื่องการประกอบธุรกิจข้อมูลเครดิตแล้วนั้น การที่บริษัทข้อมูลเครดิตจะทำการเปิดเผยข้อมูลโดยไม่จำเป็นต้องมีความยินยอมจากเจ้าของข้อมูลนั้นก็ย่อมจะต้องเข้าข้อยกเว้นตาม Data Protection Act หรือตามกฎหมายฉบับอื่นที่ให้อำนาจด้วยเช่นเดียวกัน แต่จะเห็นได้ว่ากรณีที่มีความแตกต่างจากการปรับ

---

30 *Ibid*. pp. 493-496

ใช้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 อย่างเห็นได้ชัดก็คือการจำกัดขอบเขตการเปิดเผยข้อมูลไว้เฉพาะกรณีการสืบสวน หรือดำเนินคดีอาญาเท่านั้น ตามหลักการชั่งน้ำหนักระหว่างประโยชน์ของสาธารณะในการดำเนินคดีต่อผู้กระทำความผิดทางอาญา กับสิทธิในข้อมูลส่วนบุคคลของปัจเจกบุคคล ซึ่งต่างจากข้อยกเว้นกรณีการเปิดเผยข้อมูลเครดิตตามคำสั่งศาลหรือตามหมายศาล ตามมาตรา 20 วรรคสอง (1) ที่ไม่มีการกำหนดเงื่อนไขใดๆ ประกอบไว้ด้วยเลย ซึ่งอาจส่งผลกระทบต่อสิทธิของเจ้าของข้อมูลได้

ดังนั้นจากการพิจารณาข้างต้น จึงเห็นได้ว่าในการใช้กฎหมายนั้น ข้อยกเว้นควรจะมีการตีความอย่างเคร่งครัด การกำหนดข้อยกเว้นในลักษณะที่กว้างดังเช่นกรณีตามมาตรา 20 วรรคสอง (1) ดังกล่าวนี้ อาจเกิดปัญหาในการตีความและปรับใช้กฎหมายได้ ดังนั้นเพื่อให้การปรับใช้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิตเป็นไปได้อย่างมีประสิทธิภาพตรงตามวัตถุประสงค์ จึงเห็นว่าควรมีการกำหนดขอบเขต หรือเงื่อนไขในการเปิดเผยข้อมูลเครดิตโดยไม่จำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลในกรณีของการเปิดเผยตามคำสั่งศาลหรือหมายศาล โดยอาจกำหนดในลักษณะที่ว่า จะต้องเป็นการเปิดเผยตามคำสั่งศาลหรือหมายศาล เพื่อประโยชน์ในการเป็นพยานหลักฐานในประเด็นแห่งคดีในการพิจารณาคดีอาญา และการใช้ข้อมูลดังกล่าวนั้นควรจะมีการจำกัดในเรื่องการเปิดเผยข้อมูลต่อไปด้วย กล่าวคือเมื่อมีการใช้เป็นพยานหลักฐานในการพิจารณาคดีในศาลแล้วนั้น ข้อมูลเครดิตดังกล่าวก็ไม่ควรจะถูกเปิดเผยไปยังบุคคลที่สามต่อไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลด้วยนั่นเอง

3. หลักการและปัญหาในเรื่องการรักษาความปลอดภัยและการคุ้มครองความลับของข้อมูลเครดิต

หลักการที่มีความสำคัญอีกเรื่องหนึ่งของพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ก็คือเรื่องการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิต ซึ่งมีวัตถุประสงค์ในการที่จะคุ้มครองข้อมูลเครดิตของเจ้าของข้อมูลที่มีการจัดเก็บไว้โดยบริษัทข้อมูลเครดิต รวมไปถึงขั้นตอนในการ

ดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูลดังกล่าวด้วย โดยในหัวข้อนี้จะทำการอธิบายถึงหลักการของกฎหมาย วิธีการ และมาตรฐานในการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิต รวมไปถึงวิเคราะห์ปัญหาความรับผิดที่อาจเกิดขึ้นจากกรณีการฝ่าฝืนหน้าที่ในด้านการรักษาความปลอดภัยของข้อมูลดังกล่าวนี้ด้วย

3.1 หลักการของกฎหมายในเรื่องการรักษาความปลอดภัยและการคุ้มครองความลับของข้อมูลเครดิต

ข้อมูลเครดิตนั้น ถือเป็นข้อมูลที่มีความละเอียดอ่อน และอาจส่งผลกระทบต่อเจ้าของข้อมูลได้เป็นอย่างมากถ้าหากมีการเปิดเผย หรือนำไปใช้โดยมิชอบด้วยกฎหมาย ซึ่งในเรื่องนี้พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 มาตรา 17 (3) ได้กำหนดให้บริษัทข้อมูลเครดิตหรือผู้ที่ได้รับมอบหมายให้เป็นผู้ประมวลผลข้อมูลแทนจะต้องมีการจัดระบบและข้อกำหนดในเรื่องระบบรักษาความลับและความปลอดภัยของข้อมูลเพื่อป้องกันมิให้มีการนำข้อมูลไปใช้ผิดวัตถุประสงค์และมิให้ผู้ไม่มีสิทธิได้รับรู้ข้อมูล รวมทั้งระบบป้องกันมิให้ข้อมูลถูกแก้ไข ทำให้เสียหาย หรือถูกทำลายโดยไม่ชอบหรือโดยไม่ได้รับอนุญาต ทั้งนี้การจัดระบบหรือข้อกำหนดดังกล่าว ให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการประกาศกำหนด จึงจะเห็นได้ว่าการศึกษาวิเคราะห์ถึงการกำหนดมาตรฐานขั้นต่ำ ในทางปฏิบัติเพื่อเป็นการรักษาความปลอดภัยนั้นมีความสำคัญเป็นอย่างยิ่งในการแสดงให้เห็นถึงเป็นประสิทธิภาพด้านการรักษาความปลอดภัยของข้อมูลของบริษัทข้อมูลเครดิต อีกทั้งยังช่วยแสดงให้เห็นว่าบทบัญญัติของกฎหมายนี้ในทางปฏิบัติแล้วนั้นจะสามารถป้องกันการละเมิดสิทธิของบุคคลผู้เป็นเจ้าของข้อมูลได้อย่างแท้จริงหรือไม่ด้วยนั่นเอง

หน้าที่ของบริษัทข้อมูลเครดิตในการรักษาความปลอดภัยและคุ้มครองความลับของข้อมูลตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต อาจสรุปได้ ดังนี้

(1) จะต้องมีการจัดระบบและข้อกำหนดในเรื่องระบบรักษาความปลอดภัย และคุ้มครองความลับของข้อมูลเพื่อป้องกันมิให้มีการนำข้อมูลไปใช้ผิดวัตถุประสงค์

(2) จะต้องมีการจัดระบบและข้อกำหนดในเรื่องระบบรักษาความปลอดภัย และคุ้มครองความลับของข้อมูลเพื่อป้องกันมิให้ผู้ไม่มีสิทธิได้รับรู้ข้อมูล

(3) จะต้องมีการจัดระบบป้องกันมิให้ข้อมูลถูกแก้ไขทำให้เสียหาย หรือถูกทำลายโดยไม่ชอบหรือโดยไม่ได้รับอนุญาต

นอกเหนือจากนั้น การจัดระบบหรือข้อกำหนดดังกล่าวยังจะต้องเป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลเครดิตได้มีการออกประกาศกำหนดอีกด้วย

3.2 วิธีการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิต

การกำหนดหลักการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิตตามพระราชบัญญัติที่อธิบายข้างต้นนั้น เป็นการกำหนดไว้เพียงแต่หลักการอย่างกว้าง โดยจะต้องอาศัยประกาศคณะกรรมการคุ้มครองข้อมูลเครดิตเป็นเครื่องมือในการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในทางปฏิบัติต่อไป อีกทั้งในปัจจุบันนี้ กระบวนการรับส่ง ประมวลผล หรือจัดเก็บข้อมูลของบริษัทข้อมูลเครดิตล้วนกระทำโดยคอมพิวเตอร์ซึ่งมีการเชื่อมโยงเป็นเครือข่าย ที่แม้จะช่วยให้การดำเนินงานต่างๆ เป็นไปได้อย่างสะดวกรวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น แต่ก็มีความเสี่ยงสูงที่อาจเกิดการละเมิดด้านความปลอดภัยได้ การรักษาความปลอดภัยของระบบการทำงานของบริษัทข้อมูลเครดิต รวมไปถึงสมาชิกและผู้ใช้บริการจึงมีความสำคัญเป็นอย่างยิ่ง การกำหนดมาตรฐานขั้นต่ำในการรักษาความปลอดภัยดังกล่าวนั้นจึงเป็นสิ่งที่จำเป็น และควรได้รับความสนใจเพื่อพัฒนาให้เจ้าของข้อมูลได้รับความคุ้มครองอย่างเพียงพอ และเพื่อเป็นการกำหนดมาตรฐานการดำเนินงานดังกล่าวนั้น ได้มีการกำหนดหลักปฏิบัติของบริษัทข้อมูลเครดิตไว้โดยสามารถอธิบายได้ ดังนี้

(1) แนวปฏิบัติในเรื่องการรักษาความปลอดภัยของข้อมูลเครดิต ตามประกาศคณะกรรมการคุ้มครองข้อมูลเครดิตเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการจัดระบบและข้อกำหนดเพื่อประมวลผลข้อมูล

คณะกรรมการคุ้มครองข้อมูลเครดิตได้มีการออกประกาศเรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการจัดระบบและข้อกำหนดเพื่อประมวลผลข้อมูล โดยอาศัยอำนาจตามความในมาตรา 17 ลงวันที่ 26 ธันวาคม พ.ศ. 2546 โดยมีสาระสำคัญในประเด็นที่เกี่ยวข้อง สรุปได้ดังนี้

1. บริษัทข้อมูลเครดิตต้องมีระบบรักษาความลับและความปลอดภัยของข้อมูลเพื่อป้องกันไม่ให้มีการนำข้อมูลไปใช้ผิดวัตถุประสงค์ของการประกอบธุรกิจข้อมูลเครดิต และไม่ให้ผู้ไม่มีสิทธิได้รับรู้ข้อมูลได้ล่วงรู้ข้อมูลดังกล่าว รวมทั้งระบบป้องกันไม่ให้ข้อมูลถูกแก้ไข ทำให้เสียหาย หรือถูกทำลายโดยไม่ชอบหรือโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(1) กำหนดให้สมาชิกหรือผู้ใช้บริการต้องมีระบบยืนยันผู้ใช้ โดยอย่างน้อยต้องกำหนดให้มี “รหัสผู้ใช้งาน” (User ID) และ “รหัสผ่านเพื่อการใช้งาน” (password) เพื่อป้องกันการเรียกดูข้อมูลโดยไม่ได้รับอนุญาต หรือโดยบุคคลที่ไม่เกี่ยวข้อง

(2) การเข้าถึง และ/หรือ แก้ไขข้อมูลของสมาชิกหรือผู้ใช้บริการทุกครั้ง ต้องมีระบบบันทึกและยืนยันไว้เพื่อเป็นหลักฐานที่อ้างอิงได้

(3) คอมพิวเตอร์ หรืออุปกรณ์ หรือเครื่องมือใดๆ ทุกชนิดที่เชื่อมต่อกับฐานข้อมูลของบริษัทข้อมูลเครดิตไม่ว่าจะใช้สายหรือไร้สาย จะต้องได้รับการออกแบบติดตั้งระบบรักษาความปลอดภัยและมีระบบเตือนภัย (Alert report) เพื่อป้องกันการดักหรือลักลอบหรือโจรกรรมข้อมูล หรือก่อความเสียหายที่อาจจะเกิดขึ้นหรือเกิดแก่ข้อมูล และ/หรือฐานข้อมูลของบริษัทข้อมูลเครดิต นอกจากนี้ต้องมีระเบียบปฏิบัติให้ผู้ที่เกี่ยวข้องมีการทดสอบ หรือใช้ระบบรักษาความปลอดภัยดังกล่าวตามกำหนดเวลาที่ชัดเจนและเคร่งครัด

2. บริษัทข้อมูลเครดิตต้องมีระบบบันทึกการขอใช้ข้อมูลและการรายงานผลทุกครั้งเมื่อมีผู้เข้าถึงข้อมูล โดยระบบและการรายงานต้องสามารถระบุรหัสผู้ใช้งาน พร้อมทั้งวันที่เข้าถึงข้อมูลซึ่งสามารถตรวจสอบได้เมื่อมีปัญหาและข้อโต้แย้ง ทั้งนี้ ให้เก็บข้อมูลดังกล่าวมีกำหนดระยะเวลาไม่น้อยกว่าสองปีนับแต่วันที่มีการบันทึกของการเข้าถึงและออกจากข้อมูลเพื่อให้เจ้าของข้อมูลตรวจสอบได้

3. บริษัทข้อมูลเครดิตต้องจัดให้มีระบบสำรองข้อมูลและระบบประมวลผลสำรองเตรียมพร้อมอยู่เสมอ หากเกิดปัญหาขึ้นกับระบบข้อมูลหลัก

4. บริษัทข้อมูลเครดิตต้องจัดให้มีผู้เชี่ยวชาญภายนอกซึ่งธนาคารแห่งประเทศไทยได้ให้ความเห็นชอบ ทำการตรวจสอบระบบที่เกี่ยวข้องกับการประมวลผลข้อมูลทุกระบบ (System Audit) และออกรายงานยืนยันความถูกต้องครบถ้วนของทุกระบบอย่างน้อยปีละหนึ่งครั้ง

จะเห็นได้ว่าตามประกาศคณะกรรมการคุ้มครองข้อมูลเครดิตฉบับนี้ ได้มีการวางมาตรฐานขั้นต่ำ ในการปฏิบัติตามกฎหมายในเรื่องการรักษาความปลอดภัย และคุ้มครองความลับของข้อมูลเครดิต ที่บัญญัติไว้ในมาตรา 17 โดยกำหนดหน้าที่แก่บริษัทข้อมูลเครดิตไว้ในประเด็นหลักๆ กล่าวคือ การใช้มาตรการรหัสผู้ใช้งานและรหัสผ่าน, การใช้ระบบบันทึกการเข้าถึงและแก้ไขข้อมูล, การติดตั้งระบบรักษาความปลอดภัยและระบบเตือนภัย รวมไปถึงการจัดให้มีระบบสำรองข้อมูลและระบบประมวลผลสำรอง อีกทั้งต้องทำ การตรวจสอบระบบโดยผู้เชี่ยวชาญจากภายนอก ซึ่งธนาคารแห่งประเทศไทยได้ให้ความเห็นชอบ อย่างน้อยปีละหนึ่งครั้งด้วย

(2) แนวปฏิบัติตามหนังสือเวียนของคณะกรรมการคุ้มครองข้อมูลเครดิต เรื่องแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิต

เนื่องจากปัจจุบันการประกอบธุรกิจของบริษัทข้อมูลเครดิตเกี่ยวข้องกับการให้บริการผ่านเครือข่ายสาธารณะ เช่น เครือข่ายอินเตอร์เน็ต ซึ่งต้องมีการเชื่อมต่อกับเครือข่ายภายในของบริษัทข้อมูลเครดิต สมาชิก และผู้ใช้บริการ จึงมีความเสี่ยงสูงที่จะเกิดภัยคุกคามในรูปแบบต่างๆ โดยเฉพาะจากผู้บุกรุก (Hacker) ซึ่งสามารถสร้างความเสียหายต่อเจ้าของข้อมูล สมาชิก หรือผู้ใช้บริการได้ ซึ่งความเสี่ยงต่อความเสียหายดังกล่าวนี้เป็นความเสี่ยงในรูปแบบเดียวกันที่อาจเกิดต่อการประกอบธุรกิจผ่านเครือข่ายสาธารณะของสถาบันการเงินเช่นเดียวกัน โดยที่ในเรื่องดังกล่าวนี้ธนาคารแห่งประเทศไทยได้ตระหนักถึง และออกหนังสือเวียนที่ ธปท.สนส.(11) ว.2484/2546 ลงวันที่ 19 พฤศจิกายน พ.ศ.2546 เรื่องแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงิน

ทางอิเล็กทรอนิกส์ กำหนดแนวปฏิบัติในการรักษาความปลอดภัยการให้บริการการเงินทางอิเล็กทรอนิกส์ให้สถาบันการเงินถือปฏิบัติ และคณะกรรมการคุ้มครองข้อมูลเครดิตก็ได้มีมติเห็นชอบ อนุมัติให้มีการนำ แนวปฏิบัติของธนาคารแห่งประเทศไทยในเรื่องดังกล่าวมาปรับใช้กับการประกอบธุรกิจข้อมูลเครดิตด้วย ดังนั้น จึงได้มีการกำหนดแนวปฏิบัติเกี่ยวกับแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตและแนวทางการให้คำ แนะนำ แก่สมาชิกหรือผู้ใช้บริการ ให้บริษัทข้อมูลเครดิตถือปฏิบัติเพิ่มเติมจากประกาศคณะกรรมการคุ้มครองข้อมูลเครดิต เพื่อให้บริษัทข้อมูลเครดิตมีการรักษาความปลอดภัยในการให้บริการข้อมูลเครดิตเป็นแนวทางเดียวกันกับแนวปฏิบัติของสถาบันการเงินต่างๆ และส่งผลเป็นการคุ้มครองสิทธิของเจ้าของข้อมูลซึ่งจะเกิดประโยชน์ต่อผู้บริโภคโดยตรง[31]

เพื่อเป็นการกำ หนดแนวปฏิบัติเพิ่มเติมดังกล่าว จึงได้มีการออกหนังสือเวียนที่ กคค.(ว) 6/2546 เรื่องแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิต ลงวันที่ 29 ธันวาคม พ.ศ. 2546 และแนวทางการให้คำ แนะนำ แก่สมาชิกและผู้ใช้บริการ เพื่อให้บริษัทข้อมูลเครดิตใช้เป็นแนวทางในการกำ หนดกรอบการรักษาความปลอดภัยสำ หรับการให้บริการข้อมูลเครดิต และเป็นการรักษาผลประโยชน์ของเจ้าของข้อมูล และสมาชิก โดยเนื้อหาของแนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตตามหนังสือเวียนนี้ สามารถแบ่งเป็น 3 ส่วน คือ

1. นโยบายการรักษาความปลอดภัย
2. กระบวนการหลักในการรักษาความปลอดภัย ได้แก่
   2.1 การควบคุมการเข้าถึงระบบให้บริการ และฐานข้อมูล
   2.2 การตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ
   2.3 การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล
   2.4 การรักษาความลับของข้อมูล

---

[31] รายงานการประชุมคณะกรรมการคุ้มครองข้อมูลเครดิต ครั้งที่3/2546 วันที่ 24 ธันวาคม พ.ศ.2546

2.5 การรักษาความพร้อมใช้ของระบบให้บริการ

2.6 การติดตามตรวจสอบความผิดปกติและจุดอ่อนของระบบให้บริการ

2.7 การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้อง หรือได้รับความเสียหายจากภัยคุกคาม

3. กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ ได้แก่

3.1 การฝึกอบรมและให้ความรู้แก่พนักงานของบริษัทข้อมูลเครดิต

3.2 การให้ข้อมูลและคำแนะนำแก่สมาชิกหรือผู้ใช้บริการ

3.3 การควบคุมภายใน

ซึ่งในที่นี้จะขอทำการอธิบายถึงประเด็นสำคัญที่มีความเกี่ยวข้องพอสังเขป ดังนี้

1. นโยบายการรักษาความปลอดภัย

1.1 บริษัทข้อมูลเครดิตต้องกำหนดนโยบายและกระบวนการศึกษาความปลอดภัยของการให้บริการข้อมูลเครดิตที่ชัดเจน โดยต้องพิจารณาถึงความเสียหายที่อาจเกิดขึ้นต่อระบบให้บริการ เจ้าของข้อมูล สมาชิก และผู้ใช้บริการ อันเนื่องมาจากพฤติกรรมที่ไม่พึงประสงค์ รวมทั้งต้องคำนึงถึงการเปลี่ยนแปลงทางเทคโนโลยีที่รวดเร็วด้วย

1.2 บริษัทข้อมูลเครดิตต้องกำหนดให้มีผู้บริหารและพนักงานที่รับผิดชอบในการดำเนินการ มีการสื่อสารให้พนักงานได้รับทราบอย่างทั่วถึง มีการติดตามดูแลให้พนักงานและผู้ที่เกี่ยวข้องกับระบบให้บริการปฏิบัติตามนโยบายและกระบวนการรักษาความปลอดภัยอย่างเคร่งครัด รวมทั้งมีการตรวจสอบการปฏิบัติตามอย่างเหมาะสม

1.3 บริษัทข้อมูลเครดิตต้องจัดให้มีการประเมินประสิทธิภาพของกระบวนการรักษาความปลอดภัยอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบต่อการรักษาความปลอดภัย เช่น การเปลี่ยนแปลงเทคโนโลยีที่ใช้ หรือการลักลอบเข้าถึงระบบให้บริการ (Hacking Incidents) ทั้งนี้ การประเมินควรกระทำโดยผู้เชี่ยวชาญจากภายนอกที่ไม่เป็นผู้พัฒนาหรือปฏิบัติการระบบ นอกจากนั้น บริษัทข้อมูลเครดิตควรมีการ

ติดตามความก้าวหน้าทางเทคโนโลยีอย่างใกล้ชิดเพื่อนำ มาพัฒนานโยบายและกระบวนการศึกษาความปลอดภัยให้มีประสิทธิภาพมากขึ้น

2. กระบวนการหลักในการรักษาความปลอดภัย

การให้บริการข้อมูลเครดิตแก่สมาชิกหรือผู้ใช้บริการจะต้องมีระบบป้องกันภัยคุกคามจากผู้บุกรุกในรูปแบบต่างๆ ที่สามารถสร้างความเสียหายต่อระบบให้บริการ เจ้าของข้อมูล สมาชิก และผู้ใช้บริการได้ เช่น การลักลอบเข้าถึงเครือข่ายภายใน การโจมตีระบบให้บริการ โดยมีเป้าหมายเพื่อให้ระบบทำ งานไม่ได้หรือให้เปิดเผยข้อมูลที่สำ คัญ การปลอมแปลงข้อมูล หรือการโจมตีระบบให้บริการโดยไวรัสคอมพิวเตอร์ เป็นต้น

บริษัทข้อมูลเครดิตต้องมีกระบวนการศึกษาความปลอดภัยที่ดีและเลือกใช้เทคโนโลยีสำ หรับการรักษาความปลอดภัยที่มีประสิทธิภาพและเป็นที่ยอมรับตามมาตรฐานที่เกี่ยวข้อง เพื่อป้องกันภัยคุกคามต่างๆ และเมื่อเกิดภัยคุกคามก็สามารถควบคุมความเสียหาย และแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว ทั้งนี้ กระบวนการหลักในการรักษาความปลอดภัยดังกล่าวควรประกอบด้วย

2.1 การควบคุมการเข้าถึงระบบให้บริการ และฐานข้อมูล

กระบวนการและเทคโนโลยีที่ใช้ควบคุมการเข้าถึงระบบให้บริการและฐานข้อมูลต้องสามารถป้องกันการลักลอบเข้าถึงโดยผู้ที่ไม่มีสิทธิทั้งจากภายในและภายนอกองค์กร โดยมีการควบคุมการเข้าถึงสถานที่ตั้งของระบบให้บริการและอุปกรณ์สำ คัญ และมีการควบคุมการเข้าถึงระบบให้บริการและข้อมูลด้วยวิธีการทางคอมพิวเตอร์ ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

1) การกำ หนดสิทธิการเข้าถึงระบบให้บริการให้เหมาะสมกับการเข้าใช้บริการของสมาชิกหรือผู้ใช้บริการ และสิทธิหน้าที่ของพนักงานในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำ เสมอ

2) การกำ หนดให้ผู้มีอำ นาจเท่านั้นที่สามารถเข้าแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงต่างๆ ได้

3) การบันทึกรายละเอียดการเข้าถึงระบบให้บริการและฐานข้อมูล การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออก

สถานที่ตั้งของระบบให้บริการไว้เพื่อเป็นหลักฐานการตรวจสอบในกรณีเกิดปัญหา

2.2 การตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ

บริษัทข้อมูลเครดิตต้องจัดให้มีระบบการตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ เพื่อป้องกันการเข้าถึงระบบให้บริการและฐานข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ กระบวนการดังกล่าวควรครอบคลุมถึง

1) วิธีการตรวจสอบตัวตนและสิทธิในการใช้บริการของสมาชิกหรือผู้ใช้บริการก่อนเข้าถึงระบบให้บริการหรือฐานข้อมูล

2) การควบคุมการเข้าถึงและการแก้ไขเปลี่ยนแปลงข้อมูลในฐานข้อมูลที่ใช้ในการตรวจสอบตัวตน

3) การตรวจสอบตัวตนสมาชิกหรือผู้ใช้บริการต้องกระทำอย่างต่อเนื่อง หากมีการหยุดชะงักควรเริ่มตรวจสอบตัวตนสมาชิกหรือผู้ใช้บริการใหม่

4) การบันทึกรายละเอียดการเข้าถึงข้อมูลสมาชิกหรือผู้ใช้บริการ เพื่อใช้เป็นหลักฐานการตรวจสอบ รวมทั้งมีการจัดเก็บบันทึกดังกล่าวอย่างปลอดภัย

5) การจัดให้มีการทบทวนวิธีการตรวจสอบตัวตนอย่างสม่ำเสมอ โดยคำนึงถึงพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป

ตัวอย่างเทคโนโลยีที่ใช้ในการตรวจสอบตัวตน อาทิ รหัสผู้ใช้งาน (User ID) รหัสผ่านเพื่อการใช้งาน (password) เทคโนโลยีการเข้ารหัสลับ (Encryption Technology) ข้อมูลที่ใช้ตรวจสอบตัวตนสมาชิกหรือผู้ใช้บริการ และการใช้ช่องทางที่มีความปลอดภัยสูงในการรับส่งข้อมูลการตรวจสอบตัวตน เช่น Secure Sockets Layer (SSL) เป็นต้น

2.3 การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล

กระบวนการที่ใช้ในการรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล ควรครอบคลุมถึง

1) การออกแบบระบบให้บริการและการเลือกใช้เทคโนโลยีที่มีประสิทธิภาพ

2) การทดสอบระบบให้บริการให้ทำงานได้อย่างถูกต้องก่อนเริ่มใช้งานหรือทุกครั้งที่มีการเปลี่ยนแปลง

3) การควบคุมการทำงานของระบบให้บริการในขั้นตอนที่สำคัญ เช่น ขั้นตอนการประมวลผล การรับส่ง และการจัดเก็บข้อมูล เพื่อให้สามารถป้องกันและตรวจสอบการลักลอบเข้าถึงระบบให้บริการได้

4) การควบคุมการแก้ไขเปลี่ยนแปลงระบบให้บริการและข้อมูลอย่างรัดกุม

2.4 การรักษาความลับของข้อมูลเครดิต

กระบวนการและเทคโนโลยีที่ใช้ในการรักษาความลับของข้อมูลเครดิต โดยเฉพาะข้อมูลเครดิตที่อยู่ระหว่างการรับส่ง การประมวลผล และการจัดเก็บ ควรครอบคลุมถึง

1) วิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลในลักษณะที่ปลอดภัยตามระดับความสำคัญของข้อมูล เพื่อป้องกันการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

2) การควบคุมเพื่อให้ผู้ที่มีสิทธิและได้รับการตรวจสอบตัวตนแล้วเท่านั้นที่จะเข้าถึงหรือเปลี่ยนแปลงข้อมูลได้

2.5 การรักษาความพร้อมใช้ของระบบให้บริการ

กระบวนการที่ใช้รักษาความพร้อมใช้ของระบบให้บริการควรครอบคลุมถึงการดำเนินการให้ระบบให้บริการมีประสิทธิภาพและมีความพร้อมในการให้บริการตามช่วงเวลาที่ได้ตกลงไว้กับสมาชิกหรือผู้ใช้บริการ สามารถรองรับการใช้บริการได้อย่างพอเพียง ทั้งในช่วงเวลาปกติและช่วงเวลาที่มีการใช้บริการอย่างหนาแน่น รวมทั้งมีระบบสำรองข้อมูลและระบบการเรียกคืนข้อมูลอย่างทันท่วงทีในกรณีที่เกิดความเสียหายหรือขัดข้อง

ในการเตรียมการรองรับเหตุการณ์ความเสียหายที่อาจเกิดขึ้นโดยไม่ได้คาดหมาย บริษัทข้อมูลเครดิตควรจัดให้มีแผนฉุกเฉินในการรักษาความพร้อมใช้ของการให้บริการโดยให้คำนึงถึงปัญหาขัดข้องที่เกิดจากระบบขององค์กรภายนอกที่บริษัทข้อมูลเครดิตพึ่งพาหรือเชื่อมต่อด้วย

2.6 การติดตามตรวจสอบความผิดปกติ และจุดอ่อนของระบบให้บริการ

กระบวนการและเทคโนโลยีที่ใช้ในการติดตามตรวจสอบความผิดปกติและจุดอ่อนของระบบให้บริการควรครอบคลุมถึง

1) การตรวจสอบความผิดปกติของระบบให้บริการอย่างสม่ำเสมอ โดยอาจตรวจสอบจากหลักฐานที่บันทึกไว้ เช่น การเข้า

ถึงระบบให้บริการของสมาชิกหรือผู้ใช้บริการ การเข้าถึงฐานข้อมูล การตรวจสอบตัวตน และการปฏิบัติงานของพนักงาน เป็นต้น

2) การตรวจสอบจุดอ่อนของระบบให้บริการอย่างต่อเนื่อง โดยเฉพาะในส่วนของระบบเครือข่าย โปรแกรมระบบงาน และฐานข้อมูล เนื่องจากผู้บุกรุกสามารถใช้ข้อบกพร่องดังกล่าวเป็นช่องทางในการโจมตี หรือลักลอบเข้าถึง

3) การทดสอบเจาะระบบ (Penetration Test) เพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความปลอดภัย

ตัวอย่างเทคโนโลยีที่เกี่ยวข้องกับการตรวจสอบความผิดปกติและความเปราะบาง อาทิ ระบบตรวจจับการบุกรุก (Intrusion Detection System - IDS) เทคโนโลยีที่ใช้ในการตรวจสอบโปรแกรมหรือข้อมูลที่แปลกปลอมเข้ามาในระบบให้บริการ เช่น Network scanner, Network Analyzer, Security Alert ต่างๆ และโปรแกรมตรวจสอบและป้องกันไวรัสคอมพิวเตอร์ (Anti-virus Software) เป็นต้น

2.7 การแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้องหรือได้รับความเสียหายจากภัยคุกคาม

กระบวนการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้องหรือได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง ควรครอบคลุมถึง

1) การวิเคราะห์วิธีการคุกคามและลักลอบเข้าถึงข้อมูลที่อาจเกิดขึ้น รวมทั้งประเมินความเสียหายและผลกระทบจากเหตุการณ์ดังกล่าว

2) เมื่อตรวจพบปัญหาหรือความผิดปกติ ต้องรายงานผู้บริหารหรือผู้รับผิดชอบทันที

3) กำหนดทีมผู้รับผิดชอบในการแก้ไขปัญหาหรือความผิดปกติ ซึ่งควรได้รับการฝึกฝนทั้งในด้านทักษะและความสามารถในการจัดการปัญหาต่างๆ ที่เกิดขึ้น

4) การจัดเตรียมข้อมูล และขั้นตอนการขอความช่วยเหลือในกรณีฉุกเฉินจากผู้เชี่ยวชาญทั้งจากภายในและภายนอกองค์กร โดยเฉพาะความช่วยเหลือทางเทคนิค

5) การสื่อสาร ชี้แจง และทำ ความเข้าใจกับพนักงาน สื่อมวลชน สมาชิก และผู้ใช้บริการอย่างรวดเร็ว เกี่ยวกับปัญหาที่เกิดขึ้นและการแก้ไข เพื่อรักษาภาพพจน์และชื่อเสียงของบริษัท

ข้อมูลเครดิต รวมทั้งสร้างความเชื่อมั่นแก่เจ้าของข้อมูล สมาชิก และผู้ใช้บริการ

6) การรวบรวมหลักฐานต่างๆ ที่เป็นประโยชน์ในการดำเนินคดีกับผู้บุกรุก เช่น หลักฐานที่บันทึกการเข้าถึงข้อมูลและส่วนต่างๆ ของระบบให้บริการ เครื่องคอมพิวเตอร์ที่ผู้บุกรุกใช้เป็นเครื่องมือติดต่อสื่อสาร ข้อมูลที่แสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง วัน เวลา และอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสาร เป็นต้น

7) การจัดทำรายงานที่เป็นลายลักษณ์อักษร เพื่อเสนอต่อคณะกรรมการบริษัทข้อมูลเครดิต ทั้งนี้ คณะกรรมการบริษัทข้อมูลเครดิตอาจมอบหมายให้ผู้บริหารหรือทีมที่รับผิดชอบพิจารณารายงานดังกล่าวและดำเนินการต่อไป

รายงานที่จัดทำเป็นลายลักษณ์อักษรควรมีสาระสำคัญดังนี้

(1) วัน เวลา และสถานที่ที่ระบบให้บริการได้รับความเสียหายจากภัยคุกคามหรือการลักลอบเข้าถึง

(2) ลักษณะ วิธีการที่ใช้ในการลักลอบเข้าถึง และผู้บุกรุก (กรณีทราบ)

(3) สาเหตุและลักษณะความเสียหายที่เกิดขึ้น โดยระบุถึงข้อมูลหรือระบบการให้บริการที่ได้รับความเสียหาย

(4) การประเมินความเสียหายที่เกิดขึ้น

(5) การแก้ไขปัญหาที่ได้ดำเนินการแล้ว และแนวทางที่จะดำเนินการต่อไป

3. กระบวนการเสริมการรักษาความปลอดภัยให้มีประสิทธิภาพ

3.1 การฝึกอบรมและให้ความรู้แก่พนักงาน

บริษัทข้อมูลเครดิตควรจัดให้มีการพัฒนาฝึกอบรมและให้ความรู้แก่ผู้บริหาร และพนักงานทุกระดับที่เกี่ยวข้องกับการให้บริการอย่างต่อเนื่อง เพื่อให้ตระหนักถึงความปลอดภัยในการให้บริการและสามารถปฏิบัติตามนโยบายและกระบวนการศึกษาความปลอดภัยได้อย่างมีประสิทธิภาพ นอกจากนี้ ผู้บริหารและพนักงานที่เกี่ยวข้องควรมีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นอย่างใกล้ชิด รวมทั้งเผยแพร่ข้อมูลที่เป็นประโยชน์แก่พนักงานอื่นในองค์กรด้วย

3.2 การให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ

บริษัทข้อมูลเครดิตควรให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่สมาชิกหรือผู้ใช้บริการ เช่น วิธีการใช้บริการอย่างปลอดภัย ข้อมูลทางเทคนิคหรือวิธีการรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ที่สมาชิกหรือผู้ใช้บริการใช้ในการเข้าถึงข้อมูล คำแนะนำควรรวมถึงการให้สมาชิกหรือผู้ใช้บริการระมัดระวังการใช้หรือดาวน์โหลดซอฟท์แวร์จากแหล่งที่ไม่เป็นที่รู้จักหรือน่าสงสัย เนื่องจากอาจมีโปรแกรมของผู้บุกรุกแฝงมาด้วย

การให้ข้อมูลและคำแนะนำ ดังกล่าวควรใช้ภาษาที่เข้าใจง่ายและเปิดเผยไว้บนเว็บไซต์ของบริษัทข้อมูลเครดิตโดยให้สมาชิกหรือผู้ใช้บริการสามารถเรียกดูได้โดยสะดวก และเพื่ออำนวยความสะดวกให้แก่สมาชิกหรือผู้ใช้บริการ บริษัทข้อมูลเครดิตอาจจัดให้มี Help Desk เพื่อทำหน้าที่ตอบปัญหาและให้คำแนะนำ ต่างๆ แก่สมาชิกหรือผู้ใช้บริการในการใช้บริการข้อมูลเครดิตด้วย นอกจากนี้ บริษัทข้อมูลเครดิตอาจจัดให้มีการฝึกอบรมสมาชิกหรือผู้ใช้บริการเพื่อสร้างความรู้ความเข้าใจเกี่ยวกับวิธีการรักษาความปลอดภัยในส่วนที่เกี่ยวข้องกับสมาชิกหรือผู้ใช้บริการ รวมทั้งระบบการรักษาความปลอดภัยของบริษัทข้อมูลเครดิตที่สมาชิกหรือผู้ใช้บริการควรทราบ ซึ่งเป็นการให้ความรู้และความมั่นใจในการใช้บริการข้อมูลเครดิตได้อีกทางหนึ่ง

3.3 การควบคุมภายใน

บริษัทข้อมูลเครดิตควรจัดให้มีกระบวนการควบคุมภายในที่เหมาะสมกับการให้บริการข้อมูลเครดิต อาทิ ระมัดระวังไม่ให้การให้บริการข้อมูลเครดิตขัดต่อกฎหมาย ทั้งในเรื่องของวิธีการดำเนินงานและเทคโนโลยีที่ใช้ กำหนดขั้นตอน วิธีการปฏิบัติงาน การแบ่งแยกหน้าที่ และการควบคุมการปฏิบัติงานของพนักงานที่ชัดเจนและเหมาะสม รวมทั้งมีการบันทึกหลักฐานการปฏิบัติงานของพนักงาน และเก็บรักษาหลักฐานและเอกสารสำคัญเกี่ยวกับการให้บริการไว้อย่างปลอดภัย

นอกจากนั้น ในหนังสือเวียนที่ กคค.(ว) 6/2546 เรื่อง แนวทางการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตดังกล่าวยังได้กำหนดแนวทางในการที่บริษัทข้อมูลเครดิตควรจะให้คำแนะนำ แก่สมาชิกและผู้ใช้บริการ เพื่อให้การดำเนินการที่มีลักษณะ

เครือข่ายนั้นมีความปลอดภัยมากยิ่งขึ้น โดยแนวทางดังกล่าวนั้น มีสาระสำคัญสรุปได้ ดังนี้

<u>แนวทางการให้คำแนะนำแก่สมาชิกหรือผู้ใช้บริการ</u>

บริษัทข้อมูลเครดิตควรให้คำแนะนำที่เป็นประโยชน์แก่สมาชิกหรือผู้ใช้บริการเพื่อให้เข้าใจและตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้บริการ โดยควรรวมถึงคำแนะนำดังต่อไปนี้

1) แนะนำ สมาชิกหรือผู้ใช้บริการไม่ให้เปิดเผยข้อมูลรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งานให้บุคคลอื่นทราบ ไม่เขียนหรือจดรหัสไว้ในที่ที่เห็นได้ง่าย ทำลายเอกสารที่ใช้แจ้งรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งาน รวมทั้งแนะนำ สมาชิกหรือผู้ใช้บริการให้ระมัดระวังการถูกแอบอ้างหรือหลอกลวงให้เปิดเผยข้อมูลรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งาน

2) แนะนำ สมาชิกหรือผู้ใช้บริการเกี่ยวกับวิธีการกำหนดรหัสอย่างปลอดภัย มีการเปลี่ยนรหัสผ่านเพื่อการใช้งานเป็นประจำ และแนะนำ ให้สมาชิกหรือผู้ใช้บริการทราบถึงช่องทางในการแจ้งให้บริษัทข้อมูลเครดิตทราบทันทีที่พบว่าข้อมูลรหัสผู้ใช้งานและรหัสผ่านเพื่อการใช้งานเกิดปัญหา

3) แนะนำ สมาชิกหรือผู้ใช้บริการให้รู้จักการรักษาความปลอดภัยเครื่องคอมพิวเตอร์ของตนเอง เช่น จัดตั้งและใช้งานโปรแกรมป้องกันไวรัสที่มีการปรับปรุงฐานข้อมูลไวรัสให้ทันสมัย และใช้บริการกรองไวรัสทางอินเตอร์เน็ตที่เชื่อถือได้, มีการควบคุมการเข้าถึงข้อมูลส่วนตัว, มีการเข้าและออกจากระบบให้บริการอย่างถูกต้อง, ไม่ละทิ้งเครื่องคอมพิวเตอร์หรืออุปกรณ์ในระหว่างการเข้าถึงฐานข้อมูล และออกจากระบบให้บริการอย่างถูกต้องเมื่อเสร็จสิ้นการใช้บริการ, ใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่เหมาะสมกับระบบการรักษาความปลอดภัยของบริษัทข้อมูลเครดิต, หลีกเลี่ยงการใช้เครื่องคอมพิวเตอร์และอุปกรณ์ที่ไม่ได้มาตรฐานหรือมาจากแหล่งที่เชื่อถือไม่ได้ และหลีกเลี่ยงการติดตั้ง ดาวน์โหลด หรือใช้ซอฟท์แวร์จากแหล่งที่ไม่รู้จัก หรือไม่สามารถตรวจสอบแหล่งที่มาได้ เนื่องจากระบบของสมาชิกหรือผู้ใช้บริการอาจได้รับโปรแกรมไวรัสหรือโปรแกรมอื่นๆ ที่ผู้บุกรุกสามารถใช้ในการลักลอบเข้าถึงติดมาด้วย

4) ชี้แจงให้สมาชิกหรือผู้ใช้บริการทราบถึงขอบเขตความรับผิดชอบทั้งในส่วนของบริษัทข้อมูลเครดิต และในส่วนของสมาชิกหรือผู้ใช้บริการ

จากแนวปฏิบัติข้างต้นจะเห็นได้ว่า มีการกำหนดแนวทางในการกำหนดกรอบการรักษาความปลอดภัยสำหรับการให้บริการข้อมูลเครดิตในรายละเอียด เพื่อให้บริษัทข้อมูลเครดิตสามารถนำไปใช้ในการกำหนดมาตรการในการรักษาความปลอดภัย และคุ้มครองความลับของข้อมูลในทุกขั้นตอนของการดำเนินการ ตั้งแต่ในเรื่องของการกำหนดนโยบายการรักษาความปลอดภัย, กระบวนการหลักในการรักษาความปลอดภัย ซึ่งได้แก่ การควบคุมการเข้าถึงระบบให้บริการและฐานข้อมูล, การตรวจสอบตัวตนของสมาชิกหรือผู้ใช้บริการ, การรักษาความถูกต้องเชื่อถือได้ของระบบให้บริการและข้อมูล, การรักษาความลับของข้อมูล, การรักษาความพร้อมใช้ของระบบให้บริการ, การติดตามตรวจสอบความผิดปกติและจุดอ่อนของระบบให้บริการ และการแก้ไขปัญหาและการรายงานในกรณีระบบให้บริการขัดข้อง หรือได้รับความเสียหายจากภัยคุกคาม รวมไปถึงมาตรการเสริมในเรื่องดังกล่าว ซึ่งได้แก่ การฝึกอบรมและให้ความรู้แก่พนักงานของบริษัทข้อมูลเครดิต, การให้ข้อมูลและคำแนะนำ แก่สมาชิกหรือผู้ใช้บริการ และการควบคุมภายใน อีกทั้งยังมีการกำหนดแนวทางการให้คำแนะนำ แก่สมาชิกและผู้ใช้บริการอีกด้วย

และเพื่อเป็นประโยชน์ในการศึกษาวิเคราะห์มากยิ่งขึ้น ในประเด็นต่อไปจะทำการอธิบายถึงหลักการรักษาความปลอดภัยของข้อมูลตามกฎหมายของต่างประเทศ กล่าวคือ ประเทศสหรัฐอเมริกา และประเทศอังกฤษตามลำดับ

(3) วิธีการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิตตามกฎหมายของต่างประเทศ

1. ประเทศสหรัฐอเมริกา

การกำกับดูแลองค์กร, ความเป็นส่วนตัวของปัจเจกบุคคล, ความน่าเชื่อถือของข้อมูลทางการเงิน, ความถูกต้องแท้จริงของข้อมูล และความปลอดภัยของข้อมูลล้วนเป็นสิ่งที่ผลักดันให้เกิดการออกกฎหมายและระเบียบเพื่อก่อให้เกิดการรักษาความ

ปลอดภัยที่เหมาะสมสำ หรับข้อมูลของแต่ละองค์กร การริเริ่มกฎหมายและระเบียบเหล่านี้สร้างหน้าที่ให้แก่ธุรกิจที่จะต้องใช้มาตรการรักษาความปลอดภัยของข้อมูล เพื่อปกป้องข้อมูลของตนและทำ การเปิดเผยการละเมิดด้านความปลอดภัยที่เกิดขึ้น โดยในประเทศสหรัฐอเมริกา แนวทางของกฎหมายที่เกิดขึ้นในเรื่องการรักษาความปลอดภัยของข้อมูลนั้น สามารถแบ่งได้เป็น 4 แนวทาง ซึ่งล้วนแต่ส่งผลกระทบถึงการพัฒนาของกฎหมายระหว่างประเทศด้วยเช่นกัน ซึ่งแนวทางเหล่านั้น ได้แก่

1. การขยายหน้าที่ในการรักษาความปลอดภัยอย่างต่อเนื่อง
2. การเกิดขึ้นของมาตรฐานทางกฎหมายในการรักษาความปลอดภัย
3. การมุ่งประเด็นไปยังหน้าที่ในการรักษาความปลอดภัยบางประการ
4. การสร้างหน้าที่ในการเตือน

ถึงแม้กฎหมายจะอยู่ในระหว่างการพัฒนา และอาจมีการบังคับใช้กับธุรกิจบางประเภทเท่านั้น แต่แนวทางดังกล่าวได้สร้างหน้าที่ใหม่ให้กับธุรกิจส่วนใหญ่ โดยสามารถอธิบายได้ ดังนี้

<u>การขยายหน้าที่ในการรักษาความปลอดภัย</u>

ในโลกของการสื่อสาร การดำ เนินธุรกิจ และการจัดเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ ผู้ที่มีความเกี่ยวข้องในกระบวนการเหล่านี้ล้วนแต่ต้องมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลและกระบวนการทางอิเล็กทรอนิกส์นั้น และผู้ที่ได้รับผลกระทบจากกระบวนการเหล่านั้น อาทิ ปัจเจกบุคคลที่ข้อมูลส่วนบุคคลของตนได้ถูกจัดเก็บก็ถือเป็นผู้ที่ได้รับประโยชน์จากหน้าที่ในการรักษาความปลอดภัยนี้ ซึ่งแนวทางในด้านกฎหมายในเรื่องนี้ได้มีการพัฒนาอย่างรวดเร็วทั้งในประเทศสหรัฐอเมริกา และในกฎหมายระหว่างประเทศ จนถึงจุดที่ธุรกิจส่วนใหญ่มีหน้าที่ในการจัดการรักษาความปลอดภัยที่เหมาะสมสำ หรับข้อมูลเกือบทั้งหมดของตน รวมไปถึงข้อมูลที่เกี่ยวข้องกับการดำ เนินการทางอิเล็กทรอนิกส์ของตนด้วย

เบื้องต้น หน้าที่ในการรักษาความปลอดภัยนี้จะใช้กับภาคธุรกิจบางประเภทเท่านั้น อาทิ ภาคสาธารณสุข ดังที่ปรากฏใน The Health Insurance Portability and Accountability Act 1996

(HIPAA) และภาคการเงิน ดังที่ปรากฏใน The Gramm-Leach-Bliley Act 1999 (GLBA) แต่ภายหลังจากนั้นก็ได้มีการเปลี่ยนแปลงไป โดยในปัจจุบันกฎหมายของประเทศสหรัฐอเมริกาได้ขยายการบังคับใช้หน้าที่ในการรักษาความปลอดภัยไปยังทุกธุรกิจโดยไม่คำนึงถึงประเภทของกิจการ ซึ่งเป็นไปในแนวทางเดียวกับสหภาพยุโรปในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยสามารถอธิบายการเกิดขึ้นได้เป็น 3 ประการ คือ

ประการแรก ผ่านทางการบังคับใช้กฎหมายและการออกคำสั่ง (consent decrees) ที่เริ่มขึ้นในค.ศ.2002 ซึ่งทั้ง The Federal Trade Commission (FTC) และอัยการของหลายรัฐได้ขยายหน้าที่ในการรักษาความปลอดภัยในข้อมูลส่วนบุคคลไปยังภาคธุรกิจที่ไม่มีกฎหมายเฉพาะกำกับดูแล โดยอาศัย section 5 ของ The Federal Trade Commission Act และกฎหมายของรัฐที่คล้ายคลึงกัน โดยในตอนต้นการดำเนินคดีนั้นมีฐานจากการที่บริษัทไม่สามารถจัดการรักษาความปลอดภัยของข้อมูลที่เพียงพอตามที่ได้มีการแสดงตนไว้ต่อลูกค้า กล่าวคือเป็นการกล่าวอ้างถึงการปฏิบัติทางการค้าที่มีลักษณะเป็นการหลองลวง (deceptive trade practice) แต่ต่อมาโดยเริ่มต้นในเดือนมิถุนายน ค.ศ.2005 FTC ได้ขยายขอบเขตการบังคับใช้กฎหมายเป็นอย่างมาก โดยการอ้างหลักการที่ว่า การไม่จัดหาการรักษาความปลอดภัยที่เหมาะสมสำหรับข้อมูลส่วนบุคคลของลูกค้านั้นถือว่าเป็นการปฏิบัติทางการค้าที่มีลักษณะไม่เป็นธรรม (unfair trade practice) ในการกระทำนั้นเอง แม้ในกรณีที่ไม่มีการกล่าวอ้างแสดงตนไว้ของจำเลยในเรื่องระดับความปลอดภัยก็ตาม

ประการที่สอง หลายรัฐได้มีการออกกฎหมายกำหนดหน้าที่ทั่วไปของบริษัทในการรักษาความปลอดภัยข้อมูลส่วนบุคคล โดยรัฐแรกคือ California ซึ่งได้ออกกฎหมายในค.ศ.2004 กำหนดให้ธุรกิจทั้งหมด “ใช้และดูแลกระบวนการและการปฏิบัติในด้านการรักษาความปลอดภัยที่เหมาะสม” เพื่อป้องกันข้อมูลส่วนบุคคลของผู้ที่อาศัยอยู่ใน California จากการเข้าถึง, ทำลาย, ใช้ เปลี่ยนแปลงแก้ไข หรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รัฐอื่นก็ได้มีการดำเนินการในลักษณะเดียวกัน อาทิ Arkansas, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas และ Utah

ประการสุดท้าย แนวคำพิพากษาของศาลในระยะหลังก็ได้มีการยอมรับว่าอาจจะมีหน้าที่ตาม common law ในการจัดการด้านการรักษาความปลอดภัยของข้อมูลส่วนบุคคล และการฝ่าฝืนหน้าที่ดังกล่าวถือเป็นการละเมิด ในคดี Bell v. Michigan Council ศาลได้ตัดสินว่าจำเลยมีหน้าที่ต่อโจทก์ในการป้องกันการเกิด identity theft โดยการจัดหามาตรการเพื่อรักษาความปลอดภัยของข้อมูลซึ่งเป็นความลับ ในคดี Guin v. Brazos Education ศาลได้รับว่าในคดีประมาทเลินเล่อบางกรณีนั้น หน้าที่ในการป้องกันอาจเกิดจากตัวบทของกฎหมาย (ซึ่งในคดีนั้นได้แก่ GLBA) และในคดี Wolfe v. MBNA America Bank ศาลได้ตัดสินว่าในกรณีที่ความเสียหายสามารถคาดเห็นได้ล่วงหน้า และสามารถป้องกันได้ จำเลยมีหน้าที่ในการตรวจสอบถึงความแท้จริงและความถูกต้องของคำขอเปิดบัญชีสินเชื่อ ล่าสุดในคดี In Re TJX Companies Retail Security Breach Litigation ศาลได้อนุญาตให้โจทก์ดำเนินคดีตามหลักการกล่าวอ้างที่ไม่เป็นจริงโดยประมาทเลินเล่อ (negligent misrepresentation) โดยมีฐานจากทฤษฎีที่ TJX และ requiring bank ได้แสดงตนโดยนัยต่อ issuing bank ว่าได้มีการใช้มาตรการรักษาความปลอดภัยตามที่ได้กำหนดไว้ในแนวทางการปฏิบัติของภาคธุรกิจเพื่อรักษาความปลอดภัยของข้อมูลทางการเงินและข้อมูลส่วนบุคคล โดยศาลได้วางหลักว่า TJX ได้รู้ว่า issuing bank เป็นส่วนหนึ่งของเครือข่ายทางการเงินซึ่งเชื่อว่าสมาชิกจะมีการใช้มาตรการรักษาความปลอดภัยที่เหมาะสม

<u>การเกิดขึ้นของมาตรฐานทางกฎหมายในการรักษาความปลอดภัย</u>

หน้าที่โดยทั่วไปในการจัดให้มีการรักษาความปลอดภัยของข้อมูลมักจะมีการระบุไว้ในกฎหมายแต่เพียงว่า หน้าที่ในการจัดให้มีการรักษาความปลอดภัย “ที่เหมาะสม” หรือ ”ตามสมควร” เพื่อให้บรรลุวัตถุประสงค์บางประการ ในบางกรณีกฎหมายและระเบียบได้นิยามวัตถุประสงค์เหล่านั้นในแง่ผลลัพธ์ด้านบวกที่จะได้รับ อาทิ ก่อให้เกิดประสิทธิภาพของระบบและข้อมูล, ควบคุมการเข้าถึงระบบและข้อมูล และก่อให้เกิดการรักษาความลับ, ความถูกต้องแท้จริง และความน่าเชื่อถือของข้อมูล ในกรณีอื่นอาจมีการนิยามวัตถุประสงค์เหล่านั้นในแง่ของอันตรายที่ควรหลีกเลี่ยง อาทิ

ป้องกันระบบและข้อมูลจากการเข้าถึง, ใช้, เปิดเผยหรือโอน, แก้ไขหรือเปลี่ยนแปลง และการประมวลผลโดยไม่ได้รับอนุญาต

การบรรลุวัตถุประสงค์เหล่านี้ จะต้องมีการใช้มาตรการรักษาความปลอดภัยที่ออกแบบเพื่อป้องกันระบบและข้อมูลจากการคุกคามต่างๆ ซึ่งอาจมีความแตกต่างกันไปตามแต่กรณี และการตอบสนองต่อการคุกคามเหล่านั้นด้วยมาตรการด้านความปลอดภัยที่เหมาะสมทั้งทางกายภาพ, ทางเทคนิค และทางองค์กรนั้นก็ถือเป็นประเด็นสำคัญของหน้าที่ในการจัดการรักษาความปลอดภัย

ปัญหาสำคัญที่เกิดขึ้นก็คือการระบุถึงขอบเขตของหน้าที่ในการรักษาความปลอดภัย ซึ่งกฎหมายและระเบียบต่างๆ มักจะไม่กำหนดเฉพาะเจาะจงถึงมาตรการรักษาความปลอดภัยที่ธุรกิจควรจะใช้เพื่อเป็นการปฏิบัติตามหน้าที่ซึ่งกฎหมายกำหนด กฎหมายส่วนใหญ่กำหนดหน้าที่ในการก่อตั้งและดูแล "กระบวนการ", "การควบคุม" หรือ "มาตรการรักษาความปลอดภัย" เพื่อบรรลุวัตถุประสงค์ที่ได้กล่าวข้างต้น แต่มักจะไม่มีการกำหนดถึงวิธีการหรือแนวปฏิบัติ

การนิยามถึงขอบเขตของหน้าที่ด้านความปลอดภัยเริ่มจากการทำความเข้าใจว่ากฎหมายมองการรักษาความปลอดภัยเป็นแนวคิดแบบสัมพัทธ์[32] ดังนั้นมาตฐานในการปฏิบัติจึงกำหนดไว้แต่เพียงแค่ว่าการรักษาความปลอดภัยจะต้อง "เหมาะสม" หรือ"ตามสมควร" คำอื่นๆ ที่ใช้กำหนดมาตรฐานที่ปรากฏในกฎหมายต่างๆ อาทิ "ตามความจำเป็น" หรือ"เพียงพอ" เป็นต้น แต่จะไม่มีแนวปฏิบัติในเรื่องของประเภทของมาตรการรักษาความปลอดภัยที่จะต้องนำไปใช้ หรือในเรื่องการรักษาความปลอดภัยเพียงใดที่จะถือว่าเพียงพอ

<u>นิยามตามกฎหมายของการรักษาความปลอดภัยที่เหมาะสม</u>

พัฒนาการของกฎหมายในช่วงสองสามปีที่ผ่านมาได้แสดงให้เห็นว่ามาตรฐานทางกฎหมายของการรักษาความปลอดภัย "ที่เหมาะสม" ได้เริ่มมีความชัดเจนมากขึ้น โดยที่มาตรฐานนั้นไปปฏิเสธการบังคับใช้มาตรการรักษาความปลอดภัยที่เจาะจงถึงรูป

---

32 แนวคิดที่ว่ามูลฐานต่างๆ ของการวิเคราะห์นั้นมีความสัมพันธ์และเปลี่ยนแปลงไปตามบุคคลและสภาพแวดล้อม

แบบ อาทิ firewalls, PKI หรือรหัสผ่าน แต่กลับใช้แนวทางตามข้อเท็จจริงในแต่กรณี ซึ่งกำหนดถึง "กระบวนการ" ที่ควรนำมาใช้เมื่อเกิดข้อเท็จจริงที่แตกต่างกันในแต่ละสถานการณ์ ดังนั้น แทนที่จะใช้วิธีการระบุถึงมาตรการเฉพาะที่บริษัทต้องนำมาใช้ แนวทางของกฎหมายกลับใช้วิธีการกำหนดให้บริษัทใช้กระบวนการที่ต่อเนื่องและซ้ำเดิมที่ได้ออกแบบเพื่อประเมินความเสี่ยง, ระบุและใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อตอบสนองความเสี่ยงเหล่านั้น, ตรวจสอบถึงประสิทธิภาพของมาตรการดังกล่าว และอัพเดทอย่างต่อเนื่องถึงพัฒนาการใหม่ๆ โดยการตัดสินใจใช้มาตรการรักษาความปลอดภัยใดโดยเฉพาะเจาะจงนั้นจะขึ้นอยู่กับแต่ละบริษัท กฎหมายนั้นมุ่งเน้นไปที่การใช้มาตรการรักษาความปลอดภัยที่สนองต่อการคุกคามที่บริษัทต้องเผชิญ โดยยอมรับว่ามีมาตรการรักษาความปลอดภัยหลากหลายรูปแบบที่สามารถสนองต่อการคุกคามแต่ละประเภทได้ และการคุกคาม รวมไปถึงมาตรการตอบสนองที่เหมาะสมนั้นก็ได้มีการเปลี่ยนแปลงอยู่ตลอดเวลา

หลักสำคัญของการปฏิบัติตามกฎหมายในเรื่องการรักษาความปลอดภัย โดยพิจารณาจากด้านของกระบวนการนั้น ได้แก่การใช้โปรแกรมที่ทำให้บริษัท

1) ระบุถึงข้อมูลที่ตนครอบครอง

2) ประเมินความเสี่ยงเป็นระยะเพื่อระบุถึงการคุกคาม และจุดอ่อน

3) พัฒนา และใช้โปรแกรมรักษาความปลอดภัย เพื่อจัดการ และควบคุมความเสี่ยงที่พบ

4) ตรวจตราและทดสอบโปรแกรมเพื่อให้แน่ใจถึงประสิทธิภาพ

5) ตรวจสอบและปรับปรุงโปรแกรมอย่างต่อเนื่องตามการเปลี่ยนแปลงที่เกิดขึ้นอยู่เสมอ รวมถึงมีการตรวจสอบจากบุคคลที่เป็นอิสระตามความเหมาะสม

6) ดูแลและควบคุมการจัดการของบุคคลที่สามที่มีความเกี่ยวข้อง

โดยแง่มุมสำคัญของกระบวนการนี้ก็คือการยอมรับว่ากระบวนการนี้ไม่มีทางเสร็จสมบูรณ์ และมีลักษณะต่อเนื่องซึ่งจะต้องมีการตรวจสอบ ปรับปรุง และอัพเดทอยู่เสมอ

มาตรฐานทางกฎหมายที่อิงกระบวนการสำหรับการรักษาความปลอดภัยของข้อมูลนี้ได้ถูกกำหนดขึ้นครั้งแรกในระเบียบการรักษาความปลอดภัยของธุรกิจภาคการเงินตาม GLBA ที่เรียกว่า Guidelines Establishing Standard for Safeguarding Consumer Protection ในปีค.ศ.2001 และต่อมา FTC ได้นำไปใช้ใน GLBA Safeguards Rule ในปีค.ศ.2002 ภายหลัง FTC ได้ยอมรับแนวคิดที่ว่าการรักษาความปลอดภัยของข้อมูลที่อิงกระบวนการซึ่งกำหนดไว้ในกฎระเบียบเหล่านี้ เป็นการกำหนด "แนวปฏิบัติที่ดีที่สุด" (best practice) เพื่อการดำเนินการให้เป็นไปตามกฎหมาย ซึ่งควรนำไปใช้กับธุรกิจทุกประเภท รวมไปถึงการประกอบธุรกิจข้อมูลเครดิตด้วยนั่นเอง FTC จึงได้ใช้แนวคิดแบบอิงกระบวนการนี้ในการตัดสินและออกคำสั่งที่เกี่ยวข้องกับกรณีการไม่สามารถจัดให้มีการรักษาความปลอดภัยที่เหมาะสม

ดังตัวอย่างในคดี Guin v. Brazos Education ศาลได้ปฏิเสธแนวคิดที่ว่ากฎหมายได้กำหนดให้มีการใช้มาตรการใดโดยเฉพาะเจาะจง (ซึ่งในคดี คือการเข้ารหัส) แต่กลับเน้นไปยังข้อเท็จจริงที่ว่าจำเลยได้กระทำตาม "กระบวนการ" ที่เหมาะสม อาทิ ได้ใช้นโยบายด้านการรักษาความปลอดภัยที่กำหนดไว้เป็นลายลักษณ์อักษร, ได้ทำการประเมินความเสี่ยง และได้ใช้มาตรการที่เหมาะสมตามที่ GLBA กำหนดไว้ เนื่องจากจำเลยได้ดำเนินการตามกระบวนการดังกล่าวนั้นแล้ว ศาลจึงตัดสินว่าไม่มีความรับผิดในการละเมิดที่เกิดขึ้น ในทางกลับกัน คดี Bell v. Michigan Council ศาลตัดสินว่ามีความรับผิดเมื่อจำเลยได้ทราบถึงความเสี่ยงด้านความปลอดภัยแล้ว แต่กลับไม่กระทำการใดๆ เพื่อป้องกัน

ดังนั้น จะเห็นได้ว่าการรักษาความปลอดภัยนั้นมีลักษณะเป็นกระบวนการ มิใช่ผลิตภัณฑ์สำเร็จรูป การดำเนินการเพื่อให้เป็นไปตามกฎหมายในเรื่องของหน้าที่ในการรักษาความปลอดภัยจึงเกี่ยวข้องกับ "กระบวนการ" ที่นำมาใช้กับข้อเท็จจริงที่เกิดขึ้นในแต่ละกรณีเพื่อบรรลุวัตถุประสงค์ ซึ่งได้แก่การกำหนดและใช้มาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับสถานการณ์นั้นๆ มิใช่การกำหนดมาตรการโดยเฉพาะเพื่อเป็นมาตรฐานในทุกกรณีไป หน้าที่ตามกฎหมายในเรื่องความปลอดภัยจึงเน้นไปยังสิ่งที่เหมาะสมในสถานการณ์นั้นๆ เพื่อให้บรรลุวัตถุประสงค์ด้านความปลอดภัย ดังนั้นแนวทางของกฎหมายจึงมุ่งเน้นที่จะกำหนดให้ธุรกิจต่างๆ

พัฒนาโปรแกรมรักษาความปลอดภัยที่มีประสิทธิภาพ แต่มิได้กำหนดในรายละเอียด โดยให้ขึ้นอยู่กับข้อเท็จจริงและสถานการณ์แต่ละกรณี

โดยที่กระบวนการซึ่งกฎหมายกำหนดสำหรับการรักษาความปลอดภัยที่เหมาะสม สามารถสรุปได้ ดังนี้

1. การประเมินข้อมูลที่ครอบครอง

ก้าวแรกของการรักษาความปลอดภัยของข้อมูลคือการระบุถึงขอบเขต กล่าวคือ ข้อมูล การสื่อสาร และกระบวนการใดบ้างที่จะต้องได้รับความคุ้มครอง ระบบข้อมูลใดบ้างที่เกี่ยวข้อง และมีกฎหมายฉบับใดที่สามารถนำมาบังคับใช้

2. การประเมินความเสี่ยงเป็นระยะ

การใช้โปรแกรมรักษาความปลอดภัยที่มีประสิทธิภาพเพื่อคุ้มครองข้อมูลนั้น จำเป็นต้องมีการประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบและข้อมูลขององค์กร ซึ่งเกี่ยวข้องกับการระบุถึงการคุกคามทั้งภายในและภายนอกที่สามารถคาดเห็นได้ของข้อมูลที่ได้รับความคุ้มครอง การคุกคามเหล่านี้ควรจะพิจารณาในทุกส่วนของการปฏิบัติการที่เกี่ยวข้อง รวมถึงระบบข้อมูล, รูปแบบเครือข่ายและซอฟท์แวร์, ระบบประมวลผล, ระบบจัดเก็บและทำลายข้อมูล, ระบบป้องกัน ตรวจหา และตอบสนองการโจมตี, การบุกรุก หรือความล้มเหลวของระบบอื่นๆ และการอบรม บริหารจัดการพนักงาน

และเมื่อระบุได้ถึงการคุกคามที่อาจเกิดขึ้น องค์กรควรที่จะทำการประเมินความเสี่ยงที่เกิดจากการคุกคามนั้น โดย

1) ประเมินความเป็นไปได้ที่การคุกคามนั้นจะเกิดขึ้นจริง

2) ประเมินความเสียหายที่น่าจะเกิดขึ้น

3) ประเมินประสิทธิภาพของนโยบาย, กระบวนการ และมาตรการรักษาความปลอดภัยที่มีเพื่อป้องกันการคุกคามนั้น

การประเมินความเสี่ยงควรพิจารณาถึงสภาพขององค์กร, ความสามารถในการดำเนินการคุณค่าและความสำคัญของข้อมูลที่จัดเก็บ ซึ่งกระบวนการดังกล่าวนี้จะเป็นฐานในการตัดสินใจเลือกมาตรการด้านความปลอดภัยที่จะนำมาใช้ โดยมีจุดมุ่งหมายเพื่อทำความเข้าใจถึงความเสี่ยงที่ธุรกิจจะต้องเผชิญ และตัดสินว่าระดับความเสี่ยงใดซึ่งสามารถยอมรับได้ เพื่อที่จะระบุถึงมาตรการที่เหมาะสมและมีประสิทธิภาพในการจัดการความเสี่ยงนั้น

3. พัฒนาโปรแกรมรักษาความปลอดภัยเพื่อจัดการและควบคุมความเสี่ยง

จากผลลัพธ์ที่ได้จากการประเมินความเสี่ยง องค์กรควรจะออกแบบและใช้โปรแกรมรักษาความปลอดภัยที่ประกอบไปด้วยมาตรการรักษาความปลอดภัยที่เหมาะสมด้านกายภาพ, เทคนิค และการบริหาร เพื่อจัดการและควบคุมความเสี่ยงที่ระบุได้จากการประเมิน โปรแกรมรักษาความปลอดภัยควรมีการกำหนดเป็นลายลักษณ์อักษรและดำเนินการประสานกันในทุกส่วนขององค์กร โดยมีเป้าหมายเพื่อลดความเสี่ยงและความอ่อนแอของระบบให้อยู่ในระดับที่ยอมรับได้ อาจกล่าวได้ว่าไม่เพียงแต่จะต้องมีการใช้มาตรการรักษาความปลอดภัยที่เชื่อถือได้เท่านั้น แต่มาตรการดังกล่าวต้องสอดคล้องกับการคุกคามที่ธุรกิจต้องเผชิญด้วย อาทิ การใช้ซอฟท์แวร์ตรวจหาการคุกคามและ Firewalls นั้นมีประสิทธิภาพในการหยุดผู้บุกรุก (Hacker) และป้องกันฐานข้อมูล แต่หากบริษัทนั้นมีความเสี่ยงในด้านพนักงานที่จงใจหรือประมาทเลินเล่อเปิดเผยรหัสผ่านหรือข้อมูลขององค์กร ดังนั้นแม้มาตรการรักษาความปลอดภัยทางเทคนิคที่ทันสมัยจะมีความสำคัญ แต่ก็ไม่เพียงพอที่จะแก้ไขปัญหาได้

1) ปัจจัยเกี่ยวข้องที่ควรพิจารณา

ในการกำหนดว่ามาตรการรักษาความปลอดภัยใดที่ควรนำมาใช้กับองค์กรจะต้องพิจารณาถึงหลายปัจจัยที่เกี่ยวข้อง กฎหมายเรื่องประมาทเลินเล่อวางหลักไว้ว่าปัจจัยที่เกี่ยวข้องนั้น ได้แก่ (1) ความเป็นไปได้ที่อันตรายจะเกิดขึ้น กล่าวคือ ความน่าจะเป็นซึ่งการคุกคามที่คาดเห็นล่วงหน้านั้นจะเกิดขึ้นจริง (2) ความรุนแรงของความเสียหายที่จะเกิดถ้าหากการคุกคามนั้นเกิดขึ้นจริง (3) ลักษณะและขอบเขตของธุรกิจ (4) ลักษณะและความสำคัญของข้อมูลที่ได้รับความคุ้มครอง (5) โครงสร้างทางเทคนิค และความสามารถของฮาร์ดแวร์และซอฟท์แวร์รักษาความปลอดภัยขององค์กร (6) ประสิทธิภาพของเทคโนโลยีและการรักษาความปลอดภัย (7) ค่าใช้จ่ายในด้านมาตรการรักษาความปลอดภัย

2) หมวดของมาตรการรักษาความปลอดภัย

โดยทั่วไปแล้ว กฎหมายที่กำลังพัฒนาในประเทศสหรัฐอเมริกานั้นจะไม่มีการกล่าวถึงมาตรการหรือเทคโนโลยีเฉพาะเจาะจงที่บริษัทจะต้องใช้ อาทิ ดังที่ระบุไว้ในกฎระเบียบเรื่องการ

รักษาความปลอดภัยของ HIPAA ซึ่งกำหนดว่าบริษัท "อาจใช้มาตรการรักษาความปลอดภัยใดๆ" ที่ได้ออกแบบอย่างเหมาะสมเพื่อบรรลุวัตถุประสงค์ที่ได้ระบุไว้ การให้ความสำคัญกับความยืดหยุ่นนี้ มีลักษณะเช่นเดียวกับหน้าที่ในการใช้ "ความระมัดระวังตามสมควร" ในกฎหมายละเมิด ซึ่งทำให้การพิจารณาถึงการปฏิบัติตามกฎหมายนั้นอาจทำได้ยากยิ่งขึ้น แต่อย่างไรก็ตาม กฎหมายในระยะหลังมักจะกำหนดให้บริษัทพิจารณาถึงหมวดของการรักษาความปลอดภัยบางประการ แม้จะไม่มีการระบุถึงรายละเอียดโดยเฉพาะเจาะจงก็ตาม

หมวดของมาตรการรักษาความปลอดภัยที่กฎระเบียบต่างๆ มักจะกำหนดให้บริษัทต้องพิจารณานั้นมีหลายประการ ซึ่งได้แก่

(1) การควบคุมด้านความปลอดภัยของเครื่องมือและอุปกรณ์ทางกายภาพ มีขั้นตอนเพื่อคุ้มครองเครื่องมือ มีมาตรการเพื่อป้องกันการทำลาย, เสียหาย หรือสูญหายของข้อมูลเนื่องจากอันตรายทางสภาพแวดล้อมที่อาจเกิดขึ้น อาทิ ไฟไหม้ น้ำท่วม หรือความล้มเหลวทางเทคนิค และขั้นตอนที่ควบคุมการใช้และการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(2) การควบคุมการเข้าถึงทางกายภาพ มีข้อจำกัดการเข้าถึงอาคาร, อุปกรณ์คอมพิวเตอร์ และอุปกรณ์จัดเก็บข้อมูลเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(3) การควบคุมการเข้าถึงทางเทคนิค มีนโยบายและขั้นตอนที่ทำให้ผู้ที่ได้รับอนุญาตเข้าสู่ระบบได้อย่างเหมาะสม และป้องกันบุคคลอื่นเข้าสู่ระบบ รวมไปถึงมีขั้นตอนในการอนุญาตและควบคุมการเข้าสู่ระบบ ขั้นตอนการตรวจสอบความแท้จริงของผู้ที่จะเข้าสู่ระบบ

(4) ขั้นตอนการตรวจหาการบุกรุก ขั้นตอนการตรวจตราความพยายามเข้าสู่ระบบ และรายงานความไม่สอดคล้อง กล่าวคือ ตรวจตราระบบ มีระบบและขั้นตอนในการตรวจหาการบุกรุกเพื่อค้นหาการโจมตี หรือการพยายามโจมตี หรือการบุกรุกระบบข้อมูลของบริษัท และขั้นตอนในการป้องกัน, ตรวจหา และรายงานซอฟท์แวร์ที่สร้างความเสียหาย อาทิ ไวรัส หรือ Trojan horses

(5) ขั้นตอนด้านพนักงาน ขั้นตอนการควบคุมการทำงาน, การแบ่งแยกหน้าที่ และการตรวจสอบประวัติของพนักงานที่รับผิด

ชอบหรือสามารถเข้าถึงข้อมูลที่ได้รับความคุ้มครอง และมีการควบคุมเพื่อป้องกันมิให้พนักงานให้ข้อมูลแก่บุคคลที่ไม่ได้รับอนุญาต

(6) ขั้นตอนการปรับปรุงระบบ มีขั้นตอนที่ออกแบบเพื่อให้การปรับปรุงระบบสอดคล้องกับโปรแกรมรักษาความปลอดภัยของบริษัท

(7) ความน่าเชื่อถือของข้อมูล การรักษาความลับ และการจัดเก็บ มีขั้นตอนในการป้องกันการเข้าถึง, แก้ไข, เปิดเผย หรือทำลายข้อมูลโดยไม่ได้รับอนุญาตระหว่างการจัดเก็บหรือการโอน รวมไปถึงการจัดเก็บข้อมูลในรูปแบบที่ไม่สามารถตีความหมายได้ ถ้าหากเปิดในลักษณะ plain-text file หรือเปิดในส่วนที่สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และ/หรือมีการป้องกันโดยใช้ firewalls

(8) การทำลายข้อมูล และการกำจัดสื่อและฮาร์ดแวร์ ขั้นตอนในการกำจัดขั้นสุดท้ายของข้อมูล และ/หรือฮาร์ดแวร์ที่ข้อมูลบรรจุอยู่ และขั้นตอนการลบข้อมูลจากสื่อก่อนที่จะนำไปใช้ซ้ำ

(9) การควบคุมด้านการตรวจสอบ จัดทำประวัติเพื่อบันทึกถึงการซ่อมแซม และปรับปรุงอุปกรณ์ทางกายภาพที่เกี่ยวข้องกับการรักษาความปลอดภัย อาทิ ประตู กำแพง กุญแจ รวมไปถึงฮาร์ดแวร์ ซอฟท์แวร์ และ/หรือกลไกควบคุมด้านการตรวจสอบซึ่งบันทึกและทดสอบการทำงานของระบบ

(10) แผนการณ์สำหรับเหตุการณ์ในอนาคต ขั้นตอนที่ออกแบบเพื่อให้มีการดำเนินการได้อย่างต่อเนื่องในกรณีที่มีเหตุฉุกเฉิน อาทิ แผนการสำรองข้อมูล, แผนการณ์ในกรณีเกิดภัยพิบัติ และแผนการณ์ดำเนินการในกรณีฉุกเฉิน

(11) แผนการณ์ตอบสนอง แผนการณ์ในการดำเนินการตอบสนองในกรณีที่บริษัทสงสัยหรือตรวจพบว่าเกิดการละเมิดด้านความปลอดภัย รวมถึงการเลือกบุคคลที่เหมาะสมภายในองค์กรเป็นผู้รับแจ้งในทันทีที่เกิดการละเมิดด้านความปลอดภัยขึ้น และการดำเนินการดังกล่าวควรจะเกิดขึ้นในทันทีเพื่อตอบสนองต่อการละเมิดนั้น อาทิ เพื่อหยุดการรั่วไหลของข้อมูล และรายงานไปยังเจ้าหน้าที่ตำรวจ รวมไปถึงการแจ้งไปยังบุคคลที่อาจได้รับความเสียหายจากการนั้น

4. การฝึกอบรมและการให้ความรู้

การฝึกอบรมและให้ความรู้แก่พนักงานถือเป็นองค์ประกอบหลักของโปรแกรมรักษาความปลอดภัย กฎหมาย ระเบียบและคำสั่งในระยะหลังของประเทศสหรัฐอเมริกาได้ยอมรับว่า แม้จะมีมาตรการทางกายภาพ, เทคนิค และการจัดการที่ดีเยี่ยม แต่ถ้าพนักงานไม่เข้าใจถึงบทบาทและหน้าที่ของตนในด้านการรักษาความปลอดภัยแล้วนั้น ก็ย่อมไม่อาจประสบความสำเร็จได้ การให้ความรู้ด้านความปลอดภัยเริ่มจากการสื่อสารกับพนักงานถึงนโยบาย, ขั้นตอน, มาตรฐาน และแนวปฏิบัติด้านการรักษาความปลอดภัยที่ใช้ รวมไปถึงการจัดโปรแกรมให้ความรู้ด้านความปลอดภัย การเตือนความจำเรื่องความปลอดภัยเป็นระยะ และพัฒนาอุปกรณ์การฝึกอบรมพนักงานอย่างต่อเนื่อง อีกทั้งควรมีการกำหนดโทษสำหรับพนักงานที่ไม่ปฏิบัติตามนโยบายและขั้นตอนด้านความปลอดภัยด้วย

5. การตรวจตราและการทดสอบ

เพียงแค่การใช้มาตรการรักษาความปลอดภัยนั้นยังไม่เพียงพอ บริษัทจะต้องแน่ใจได้ว่ามีการใช้มาตรการดังกล่าวอย่างเหมาะสมและมีประสิทธิภาพ จึงควรทำการประเมินความเพียงพอของมาตรการรักษาความปลอดภัยที่ใช้เพื่อควบคุมความเสี่ยงที่พบและทำการทดสอบและตรวจตราประสิทธิภาพของมาตรการเหล่านั้นอย่างสม่ำเสมอ บรรทัดฐานในปัจจุบันยังได้วางหลักไว้ว่าบริษัทต้องมีการตรวจตราการปฏิบัติตามโปรแกรมด้านการรักษาความปลอดภัยของตน โดยการตรวจสอบบันทึกการทำงานของระบบอยู่เสมอ

6. การตรวจสอบและการปรับปรุง

ดังที่กล่าวข้างต้นว่า การรักษาความปลอดภัยของข้อมูลนั้นมีการเปลี่ยนแปลงเคลื่อนไหวอยู่ตลอดเวลา ธุรกิจจึงต้องพยายามติดตามความเสี่ยง, การคุกคาม และมาตรการรักษาความปลอดภัยเพื่อการตอบสนองสิ่งดังกล่าว โดยเป็นกระบวนการที่ไม่มีที่สิ้นสุด ดังนั้นธุรกิจจึงต้องมีการตรวจสอบภายในเป็นระยะเพื่อประเมินและปรับปรุงโปรแกรมรักษาความปลอดภัย โดยอาศัย (1) ผลลัพธ์จากการทดสอบและตรวจตรา (2) การเปลี่ยนแปลงของธุรกิจหรือการบริหารจัดการ (3) การเปลี่ยนแปลงทางเทคโนโลยี (4) การเปลี่ยนแปลงของการคุกคามภายใน หรือภายนอก (5) การ

เปลี่ยนแปลงทางสภาพแวดล้อม หรือการดำเนินการ (6) สถานการณ์อื่นๆ ที่อาจส่งผลกระทบ

นอกเหนือจากการตรวจสอบภายในเป็นระยะแล้วนั้น ตามหลักการปฏิบัติที่ดีที่สุด (best practice) และมาตรฐานทางกฎหมายอาจกำหนดให้ธุรกิจต้องมีการตรวจสอบและประเมินโดยผู้ประกอบอาชีพจากภายนอกที่มีคุณสมบัติและเป็นอิสระ ซึ่งใช้ขั้นตอนและมาตรฐานที่ได้รับการยอมรับโดยทั่วไป เพื่อรับรองว่าโปรแกรมรักษาความปลอดภัยเป็นไปตามข้อกำหนด และดำเนินการอย่างมีประสิทธิภาพเพียงพอที่จะรับรองความปลอดภัย ความลับ และความน่าเชื่อถือของข้อมูลที่ได้รับความคุ้มครอง จากนั้นควรมีการปรับปรุงโปรแกรมให้เป็นไปตามผลและคำแนะนำจากการตรวจสอบนั้น

อย่างไรก็ตาม ประเด็นสำคัญของมาตรฐานตามกฎหมายในเรื่องการรักษาความปลอดภัยนั้น ก็คือการประเมินความเสี่ยง ดังที่กล่าวแล้วว่าเพียงแต่การใช้มาตรการรักษาความปลอดภัยที่เข้มแข็งนั้น ยังไม่เพียงพอที่จะถือได้ว่าเป็นการปฏิบัติตามกฎหมาย แต่จะต้องใช้มาตรการที่ตอบสนองต่อความเสี่ยงเฉพาะที่ธุรกิจต้องเผชิญด้วย การประเมินความเสี่ยงเน้นไปที่การระบุถึงการคุกคามต่อระบบและข้อมูลของบริษัทที่สามารถคาดเห็นได้ และมีบทบาทสำคัญในการตัดสินว่าเกิดหน้าที่หรือความรับผิดหรือไม่ ในคดี Wolfe v. MBNA America Bank ศาลได้ตัดสินว่าความเสียหายเป็นผลมาจากการออกบัตรเครดิตอย่างประมาทเลินเล่อ (ให้แก่บุคคลอื่นที่อ้างว่าเป็นโจทก์) ถือว่าเป็นสิ่งที่สามารถคาดเห็นได้ล่วงหน้าและสามารถป้องกันได้ โดยที่จำเลยมีหน้าที่ในการพิสูจน์ความถูกต้องแท้จริงของใบสมัครขอเปิดบัญชี ในคดี Bell v. Michigan Council ศาลได้ตัดสินว่าในกรณีที่อันตรายนั้นสามารถคาดเห็นได้และความรุนแรงที่อาจเกิดขึ้นจากความเสี่ยงนั้นมีสูง จำเลยมีความผิดในการที่ไม่จัดให้มีการรักษาความปลอดภัยที่เหมาะสมสำหรับอันตรายที่อาจเกิดขึ้น ในทางกลับกันในคดี Guin v. Brazos Education ศาลได้ตัดสินว่าในกรณีที่ได้ทำการประเมินความเสี่ยงอย่างเหมาะสมแล้ว แต่อันตรายที่เกิดขึ้นนั้นไม่สามารถคาดเห็นได้ล่วงหน้า จำเลยจึงไม่มีความรับผิดจากการที่ไม่สามารถดำเนินการเพื่อป้องกันดังกล่าวได้

โดยทั่วไปแล้วกฎหมายจะไม่ระบุอย่างเจาะจงว่าจะต้องมีการดำเนินการใดบ้างเพื่อประเมินความเสี่ยง แต่ Federal Financial Institutions Examinations Counsel (FFIEC) ได้ให้คำแนะนำแก่สถาบันการเงินใน the Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards[33] และ the FFIEC IT Examination Handbook, Information Security booklet[34] อีกทั้งยังมีการกำหนดแนวปฏิบัติในการกระทำการประเมินความเสี่ยงโดย the National Institute of Standards and Technology (NIST) อีกด้วย

และในปัจจุบันได้มีการสร้างมาตรฐานด้านการรักษาความปลอดภัยของข้อมูลในระดับสากลที่มีชื่อว่า ISO/IEC 27001 โดยเป็นมาตรฐานระดับสากลที่สามารถตรวจสอบได้ซึ่งระบุข้อกำหนดต่างๆ สำหรับระบบการจัดการด้านความปลอดภัยของข้อมูล (Information Security Management System หรือ ISMS) และมีรูปแบบตัวอย่างในการจัดตั้ง, ใช้งาน, ดำเนินการ, ตรวจตรา, ตรวจสอบ, ดูแลและปรับปรุงระบบข้อมูลบริหารรวม (Integrated Management Information System หรือ IMIS) มาตรฐาน ISO/IEC 27001 นี้เกิดขึ้นจากการพัฒนาร่วมกันของ the International Organization for Standardization (ISO) และ the International Electro technical Commission (IEC) โดยเริ่มใช้อย่างเป็นทางการเมื่อเดือนตุลาคม ค.ศ.2005 และถือได้ว่าเป็นทางปฏิบัติที่ดีที่สุดในระดับสากล

แม้ว่า ISO/IEC 27001 จะมีลักษณะเป็นมาตรฐานทางเทคนิค แต่ก็มีฐานมาจากประเด็นที่สำคัญเช่นเดียวกับมาตรฐานทางกฎหมายที่ได้อธิบายข้างต้น โดยที่มีการใช้แนวทางที่อิงกระบวนการในการจัดตั้ง, ใช้งาน, ดำเนินการ, ตรวจตรา, ตรวจสอบ, ดูแลและปรับปรุง IMIS ขององค์กร และมีข้อกำหนดทั้งหมด

---

33 www.federalreserve.gov/boarddocs/press/bcreg/2005/20051214/default.htm. (Feb 9, 2009)

34 www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf. (Feb 9, 2009)

ตามที่มาตรฐานทางกฎหมายได้ระบุไว้ กล่าวคือ เพื่อการปฏิบัติให้เป็นไปตามมาตรฐาน ISO/IEC 27001 บริษัทจะต้องทำ การระบุถึงข้อมูลที่ตนมี, ทำการประเมินความเสี่ยง, เลือกการควบคุมด้านความปลอดภัยเพื่อตอบสนองความเสี่ยงนั้น, ใช้และจัดการ ISMS, ตรวจตราและตรวจสอบ ISMS, ดูแลและปรับปรุง ISMS และจัดการด้านความปลอดภัยของบุคคลที่สาม ดังนั้นจะเห็นได้ว่าการนำ ISO/IEC 27001 มาใช้โดยกลุ่มกำ หนดมาตรฐานสากลสองกลุ่มที่ประกอบไปด้วยตัวแทนจากหลายประเทศนั้น ถือเป็นกลยุทธอย่างหนึ่งในการปฏิบัติตามมาตรฐานทางกฎหมายเรื่องความปลอดภัยในระดับสากล ยิ่งไปกว่านั้น แม้การปฏิบัติตามมาตรฐาน ISO/IEC 27001 จะไม่เป็นการรับรองการปฏิบัติตามกฎหมาย แต่ก็ถือเป็นการให้จุดเริ่มต้นที่ดีแก่บริษัทในการกระทำ ตามข้อกำ หนดทางกฎหมายระหว่างประเทศในเรื่องความปลอดภัย[35]

<u>การมุ่งประเด็นไปยังหน้าที่ตามกฎหมายบางประการมากยิ่งขึ้น</u>

1. การทำ ลายข้อมูล

แนวทางใหม่ของกฎหมายที่เพิ่งปรากฏในช่วงสองสามปีที่ผ่านมานี้ คือข้อกำ หนดในเรื่องความปลอดภัยที่เกี่ยวข้องกับวิธีการทำลายข้อมูล กฎหมายเหล่านี้มักจะไม่กำ หนดให้ต้องมีการทำ ลายข้อมูล แต่จะควบคุมวิธีการในการกระทำ ดังกล่าวหากบริษัทตัดสินใจที่จะทำ ลายข้อมูล โดยกฎหมายนี้มักจะนำ ไปใช้กับการทำ ลายข้อมูลส่วนบุคคลด้วย โดยในระดับมลรัฐ ทั้งองค์กรที่มีหน้าที่กำ กับดูแลธนาคาร และ Securities and Exchange Commission (SEC) ได้มีการใช้ระเบียบข้อกำ หนดด้านความปลอดภัยในการทำ ลายข้อมูลส่วนบุคคล ส่วนในระดับรัฐ อย่างน้อย 19 รัฐได้มีการออกข้อกำหนดที่คล้ายคลึงกันนี้ กฎหมายและระเบียบเหล่านี้โดยทั่วไปมักจะกำ หนดให้บริษัทกำ จัดข้อมูลส่วนบุคคลโดยใช้มาตรการที่เหมาะสมเพื่อป้องกันการเข้าถึงหรือการใช้ข้อมูลที่เกี่ยวข้องกับการ

---

[35] Thomas J. Smedinghoff, Wildman Harrold. "THE EMERGING LAW OF DATA SECURITY: A FOCUS ON THE KEY LEGAL TRENDS" <u>Practising Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series</u> (June-July, 2008).

ทำลายโดยไม่ได้รับอนุญาต กรณีข้อมูลในรูปแบบกระดาษ มักจะมีการกำหนดให้มีการใช้และตรวจตราการปฏิบัติตามนโยบายและขั้นตอนที่จะต้องมีการเผา, บด หรือฉีกเอกสารที่มีข้อมูลส่วนบุคคลเพื่อให้ไม่สามารถอ่านหรือนำกลับไปใช้ได้อีก และในกรณีข้อมูลอิเล็กทรอนิกส์ มักจะมีการกำหนดให้มีการทำลายหรือลบสื่ออิเล็กทรอนิกส์ที่บรรจุข้อมูลส่วนบุคคล เพื่อให้ไม่สามารถอ่านหรือนำกลับมาใช้ได้อีก[36]

2. การพิสูจน์ตัวตนออนไลน์

การปฏิบัติหน้าที่ตามกฎหมายในการจัดให้มีการรักษาความปลอดภัยของข้อมูลจะต้องรวมไปถึงหน้าที่ในการพิสูจน์ความแท้จริงของตัวตนบุคคลที่ต้องการจะเข้าสู่ระบบคอมพิวเตอร์หรือระบบข้อมูลของบริษัท โดยประเด็นไม่ได้อยู่ที่ว่ามีการกำหนดให้ต้องใช้การพิสูจน์ความแท้จริงหรือไม่ แต่เป็นการพิจารณาว่าการพิสูจน์ความแท้จริงรูปแบบใดที่เหมาะสมตามกฎหมาย ซึ่งในอดีตนั้นมักจะใช้รหัสผู้ใช้ (user ID) และรหัสผ่าน (password) แต่เมื่อมีพัฒนาการต่างๆ มากขึ้นระเบียบในภาคการเงินจึงเริ่มที่จะมีการกำหนดอย่างเป็นทางการว่าการใช้รหัสผู้ใช้ (user ID) และรหัสผ่าน (password) แต่เพียงอย่างเดียวนั้นถือว่าไม่เพียงพอ โดยที่มุมมองในเรื่องการพิสูจน์ความแท้จริงออนไลน์นี้ได้มีการระบุไว้ในเอกสารแนวปฏิบัติที่ออกโดย FFIEC ในปีค.ศ.2005 ที่เรียกว่า Authentication in an Internet Banking Environment[37] และถึงแม้ว่าแนวปฏิบัติดังกล่าวจะใช้กับภาคธุรกิจการเงินเท่านั้น แต่ก็เป็นไปในทิศทางเดียวกับกฎหมายด้านความปลอดภัยที่กำลังมีการพัฒนา และอาจเป็นทางปฏิบัติที่ดีที่สุดตามกฎหมายสำหรับทุกธุรกิจ และเช่นเดียวกับเรื่องอื่นของการรักษาความปลอดภัย กฎหมายของประเทศสหรัฐอเมริกาในปัจจุบันไม่มีการระบุประเภทหรือชนิดของวิธีการหรือเทคโนโลยีในการพิสูจน์ความแท้จริงที่จะต้องนำไปใช้ แต่กลับกำหนดให้บริษัททำการประเมินความเสี่ยง

---

[36] Benjamin J. Keele. "PRIVACY BY DELETION: THE NEED FOR A GLOBAL DATA DELETION PRINCIPLE" Indiana Journal of Global Legal Studies. (Winter, 2009).

[37] http://www.ffiec.gov/pdf/authentication_guidance.pdf (Feb 9, 2009)

และใช้ผลลัพธ์จากกระบวนกการนั้นในการระบุวิธีการในการพิสูจน์ความแท้จริงที่เหมาะสม ซึ่งตามแนวปฏิบัติของ FFIEC ได้สรุปข้อกำหนดเหล่านี้ โดยเน้นไปยังประเด็นสำคัญ 4 ประการ คือ

1) เมื่อมีการเสนอสินค้าหรือบริการแก่ลูกค้าทางอินเตอร์เน็ต บริษัทควรจะใช้วิธีการที่มีประสิทธิภาพเพื่อพิสูจน์ความแท้จริงของตัวตนลูกค้าที่ใช้สินค้าหรือบริการเหล่านั้น

2) เทคนิคในการพิสูจน์ความแท้จริงที่นำ มาใช้ควรจะเหมาะสมกับความเสี่ยงที่เกี่ยวข้องกับสินค้า และบริการ

3) บริษัทควรจะทำ การประเมินความเสี่ยง เพื่อระบุถึงประเภทและระดับความเสี่ยงที่เกี่ยวข้องกับการใช้อินเตอร์เน็ตของตน

4) ในกรณีที่การประเมินความเสี่ยงระบุว่าการใช้มาตรการพิสูจน์ตัวตนที่ใช้ปัจจัยเดียวนั้นไม่เพียงพอ บริษัทควรใช้การพิสูจน์ตัวตนโดยอาศัยหลายปัจจัย, มีการรักษาความปลอดภัยเป็นระดับชั้น หรือการควบคุมอื่นๆ ที่เหมาะสมเพื่อลดความเสี่ยงเหล่านั้น

<u>การบังคับใช้หน้าที่ในการแจ้งเตือนถึงการละเมิดด้านความปลอดภัย</u>

นอกเหนือจากแนวทางของกฎหมายที่กำ หนดหน้าที่ในการจัดให้มีมาตรการรักษาความปลอดภัยเพื่อป้องกันข้อมูลแล้ว อีกแนวทางหนึ่งที่เกิดขึ้นในระดับสากลคือ การออกกฎหมายและระเบียบกำ หนดหน้าที่ในการเปิดเผยการละเมิดด้านความปลอดภัยแก่บุคคลที่ได้รับผลกระทบ ซึ่งกฎหมายนี้ได้ออกแบบเพื่อช่วยให้ความคุ้มครองบุคคลซึ่งอาจได้รับผลกระทบในทางลบจากการละเมิดด้านความปลอดภัยของข้อมูลส่วนบุคคลของตน โดยกฎหมายได้สร้างหน้าที่ให้แก่บริษัทซึ่งคล้ายคลึงกับหน้าที่ในการเตือน (duty to warn) ตามกฎหมาย common law โดยมีฐานจากความคิดที่ว่าฝ่ายที่มีความรู้มากกว่าถึงอันตรายที่อาจก่อให้เกิดความเสียหายต่ออีกฝ่าย จะต้องแจ้งเตือนไปยังอีกฝ่ายที่ไม่ทราบถึงการณ์นั้น โดยกำ หนดให้มีการแจ้งไปยังบุคคลซึ่งอาจได้รับผลกระทบในทางลบจากการละเมิดด้านความปลอดภัยนั้น กฎหมายเหล่านี้ต้องการให้บุคคลได้รับการแจ้งเตือนว่าข้อมูลส่วนบุคคลของตนได้ถูกเปิดเผย และมีโอกาสที่จะดำ เนินการเพื่อป้องกันตนจากการเกิด identity Theft

ในด้านของข้อมูลส่วนบุคคล 42 รัฐในประเทศสหรัฐอเมริกา และ District of Columbia, Puerto Rico และ the Virgin Islands ได้ออกกฎหมายการแจ้งเตือนการละเมิดด้านความปลอดภัย โดยมีฐานมาจากกฎหมายของ California ในปีค.ศ.2003 นอกเหนือจากนั้น องค์กรกำกับดูแลการธนาคารระดับมลรัฐก็ได้ออกแนวปฏิบัติสำหรับสถาบันการเงินในเรื่องหน้าที่ในการเปิดเผยการละเมิดด้านความปลอดภัย โดยทั่วไปกฎหมายเหล่านี้กำหนดให้ธุรกิจที่ครอบครองข้อมูลส่วนบุคคลในรูปของข้อมูลคอมพิวเตอร์จะต้องเปิดเผยการละเมิดด้านความปลอดภัยของข้อมูลแก่ผู้ที่ได้รับผลกระทบ ซึ่งข้อมูลส่วนบุคคลนั้นมักจะมีการให้คำนิยามไว้ว่า คือ ข้อมูลที่ประกอบไปด้วย (1) ชื่อต้นหรือชื่อย่อ และนามสกุล และ (2) ข้อใดข้อหนึ่งต่อไปนี้ หมายเลขประกันสังคม, หมายเลขใบขับขี่ หรือบัตรประชาชน, หมายเลขบัญชี หรือหมายเลขบัตรเครดิตหรือเดบิต (พร้อมกับ PIN หรือรหัสผ่านในกรณีที่จำเป็นต้องใช้เพื่อเข้าถึงบัญชีนั้น), ในบางรัฐอาจมีการกำหนดที่กว้างออกไป โดยอาจรวมไปถึงข้อมูลทางการแพทย์, รหัสผ่าน, ข้อมูลทางชีวภาพ, ใบอนุญาตประกอบอาชีพ หรือลายเซ็นอิเล็กทรอนิกส์ เป็นต้น และยังมีการกำหนดหน้าที่ในการแจ้งเตือนแตกต่างกันไปในแต่ละรัฐ โดยข้อกำหนดพื้นฐานนั้นอาจสรุปได้ ดังนี้

1) ประเภทของข้อมูล กฎหมายส่วนมากมักจะบังคับใช้กับข้อมูลส่วนบุคคลที่ไม่ถูกเข้ารหัส

2) นิยามของคำว่า “การละเมิดด้านความปลอดภัย” กฎหมายส่วนมากกำหนดให้มีการแจ้งเตือนภายหลังจากที่มีการเรียกดูข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต ทำให้เกิดความเสี่ยงต่อระบบการรักษาความปลอดภัย การรักษาความลับ หรือความน่าเชื่อถือของข้อมูล อย่างไรก็ตาม ในบางรัฐนั้นหน้าที่ในการแจ้งเตือนจะยังไม่เกิดขึ้น เว้นแต่จะมีเหตุตามสมควรให้เชื่อได้ว่าการละเมิดด้านความปลอดภัยนั้นจะส่งผลเสียอย่างร้ายแรงแก่ลูกค้า

3) บุคคลที่จะได้รับการแจ้งเตือน จะต้องมีการแจ้งเตือนไปยังผู้ที่อาศัยในรัฐนั้นที่ข้อมูลส่วนบุคคลซึ่งไม่ถูกเข้ารหัสของตนได้ถูกละเมิดด้านความปลอดภัย

4) เวลาที่จะต้องแจ้งเตือน บุคคลจะต้องได้รับแจ้งภายในระยะเวลาที่เร็วที่สุดเท่าที่จะเป็นไปได้โดยไม่มีการล่าช้าโดยไม่มีเหตุสมควร อย่างไรก็ตาม รัฐส่วนใหญ่จะขยายระยะเวลาในการแจ้ง

เตือนในกรณีที่เป็นความจำเป็นที่มีเหตุสมควรของเจ้าหน้าที่ตำรวจ ถ้าหากการแจ้งเตือนจะขัดขวางการสืบสวนทางอาญา หรือในกรณีที่มีการใช้มาตรการที่จำเป็นในการระบุถึงขอบเขตของการละเมิดด้านความปลอดภัย และการกู้ระบบ

5) รูปแบบของการแจ้งเตือน การแจ้งเตือนอาจทำเป็นลายลักษณ์อักษร อาทิ ในรูปของจดหมาย หรือรูปแบบอิเล็กทรอนิกส์ อาทิ จดหมายอิเล็กทรอนิกส์ หรือโดยวิธีการสำรอง

6) ทางเลือกสำรองในการแจ้งเตือน ถ้าหากค่าใช้จ่ายในการแจ้งเตือนรายบุคคลนั้นมากกว่าจำนวนที่กำหนด หรือมีจำนวนบุคคลมากกว่าจำนวนที่กำหนด อาจใช้วิธีการแจ้งเตือนสำรองได้ ซึ่งประกอบไปด้วยการใช้จดหมายอิเล็กทรอนิกส์ ในกรณีที่มีที่อยู่, การแจ้งอย่างเด่นชัดในเว็บไซท์ของบริษัท และการประกาศแจ้งเตือนในสื่อระดับรัฐ[38]

จึงจะเห็นได้ว่าธุรกิจข้อมูลเครดิตในประเทศสหรัฐอเมริกา ซึ่งอยู่ในความดูแลของ The Federal Trade Commission (FTC) นั้น แม้จะไม่มีกฎหมายเฉพาะกำหนดมาตรฐานในเรื่องการรักษาความปลอดภัยของข้อมูลไว้ แต่ก็จะต้องจัดให้มีการรักษาความปลอดภัยของข้อมูลตามหน้าที่ซึ่งได้มีการขยายให้ครอบคลุมถึงภาคธุรกิจทุกประเภทดังที่ได้อธิบายข้างต้นด้วยนั่นเอง อีกทั้งการปรับใช้ section 5 ของ Federal Trade Commission Act ซึ่งถือว่าการที่บริษัทข้อมูลเครดิตไม่จัดให้มีการรักษาความปลอดภัยของข้อมูลที่เหมาะสมนั้น นับว่าเป็นการปฏิบัติทางการค้าที่มีลักษณะไม่เป็นธรรม (unfair trade practice) ซึ่งเป็นความผิดตามกฎหมายด้วย

โดยที่ในเรื่องการรักษาความปลอดภัยของข้อมูลนี้ ประเทศสหรัฐอเมริกาได้มีแนวทางในการปรับใช้ที่อาศัย

---

[38] Donald A. Cohn, Jonathan P. Armstrong, Bruce J. Heiman. "WHAT WENT WRONG? WHAT WENT RIGHT? CASE STUDIES IN CORPORATE RESPONSES TO PRIVACY AND SECURITY BREACHES" Practising Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series (June-July, 2007).

กระบวนการ มากกว่าที่จะเน้นไปยังการกำหนดมาตรการเฉพาะเจาะจงที่องค์กรจะต้องนำไปใช้ มีการให้ความสำคัญกับการประเมินความเสี่ยง เพื่อกำหนดถึงมาตรการรักษาความปลอดภัยที่เหมาะสม และการใช้มาตรการดังกล่าวเพื่อตอบสนองความเสี่ยงเหล่านั้น รวมไปถึงการตรวจสอบประสิทธิภาพของมาตรการรักษาความปลอดภัย และติดตามพัฒนาการของเทคโนโลยี และความเสี่ยงต่างๆ อย่างต่อเนื่อง นอกเหนือจากนั้น ยังมีการเน้นในประเด็นเรื่องการทำลายข้อมูล, การพิสูจน์ตัวตน และหน้าที่ในการแจ้งเตือนไปยังผู้ที่อาจได้รับผลกระทบ ในกรณีที่มีการละเมิดด้านความปลอดภัยของข้อมูลเกิดขึ้นอีกด้วย

2. ประเทศอังกฤษ

ในเรื่องการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลนี้ ตาม Data Protection Act 1998 ได้มีการกำหนดไว้ใน Data Protection Principles ของ Schedule 1 เป็นหลักการข้อที่ 7 ซึ่งกำหนดไว้ว่าจะต้องมีการใช้มาตรการทางเทคนิคและทางองค์กรที่เหมาะสม เพื่อป้องกันการประมวลผลข้อมูลโดยไม่ได้รับอนุญาตหรือมิชอบด้วยกฎหมาย และเพื่อป้องกันการสูญหาย หรือการทำลาย หรือความเสียหายต่อข้อมูลส่วนบุคคล ดังนั้นจะเห็นได้ว่า ข้อกำหนดพื้นฐานที่ผู้ควบคุมข้อมูลจะต้องปฏิบัติตามนั้น ก็คือจะต้องมีการรักษาความปลอดภัยที่เหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลจากการสูญหาย เสียหาย หรือการเปิดเผยอันเนื่องมาจากการกระทำที่ไม่ชอบด้วยกฎหมาย และยังมีการกำหนดข้อกำหนดเพิ่มเติมอีก 2 ประการ คือ ข้อกำหนดในเรื่องพนักงานที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล โดยนายจ้างมีหน้าที่ตามกฎหมายในการสร้างความแน่ใจว่าพนักงานเหล่านั้นมีความรับผิดชอบไว้ใจได้ และข้อกำหนดในเรื่องการเอาท์ซอร์ส

ข้อกำหนดพื้นฐานในเรื่องการรักษาความปลอดภัยของข้อมูล

ตาม Data Protection Act ได้กำหนดให้มีการรักษาความปลอดภัยของข้อมูลที่เหมาะสม คำแนะนำในการตัดสินว่าการรักษาความปลอดภัยนั้นมีความเหมาะสมเพียงพอหรือไม่นั้นได้มีการระบุไว้ในบทบัญญัติการตีความตาม Data Protection Act 1998, Schedule 1, part 2, paragraph 9 กล่าวคือ มาตรการรักษาความ

ปลอดภัยนั้นเมื่อพิจารณาถึงระดับความก้าวหน้าทางเทคโนโลยีและค่าใช้จ่ายในการใช้มาตรการนั้น ควรจะมีความเหมาะสมกับ

(1) อันตรายที่อาจเกิดขึ้นจากการประมวลผลข้อมูลโดยไม่ได้รับอนุญาตหรือมิชอบด้วยกฎหมาย หรือการสูญหาย หรือการทำลาย หรือความเสียหายตามที่ระบุไว้ในหลักการข้อที่ 7

(2) ลักษณะของข้อมูลที่ได้รับการคุ้มครอง

โดยบทบัญญัติในการตีความดังกล่าวได้ให้คำ อธิบายว่าหน้าที่ในการรักษาความปลอดภัยนี้ไม่ได้มีลักษณะเฉพาะเจาะจง และยังได้ระบุถึงปัจจัยที่ควรพิจารณาเมื่อทำ การประเมินถึงความเหมาะสมของมาตรการรักษาความปลอดภัย กล่าวคือ ปัจจัยแรกคือการคำ นึงถึงระดับของเทคโนโลยีที่มีการพัฒนาอย่างสูงสุดในช่วงระยะเวลานั้น องค์กรควรจะติดตามพัฒนาการของเทคโนโลยีระบบการรักษาความปลอดภัย โดยมีระบบการรักษาความปลอดภัยตามมาตรฐานของประเภทธุรกิจนั้นเป็นเกณฑ์ขั้นต่ำ ในการพิจารณาสำหรับธุรกิจประเภทเดียวกัน ปัจจัยที่สอง คือค่าใช้จ่ายในการใช้มาตรการรักษาความปลอดภัย ซึ่งความเหมาะสมในแง่ของเรื่องค่าใช้จ่ายนั้น จะต้องทำ การพิจารณาถึงสถานะทางการเงินของผู้ควบคุมข้อมูลประกอบด้วย และปัจจัยสุดท้าย ก็คือลักษณะของข้อมูล ซึ่งอาจชี้ให้เห็นถึงอันตรายที่อาจเกิดขึ้นที่เป็นผลจากการเข้าถึง หรือประมวลผลข้อมูลโดยไม่ได้รับอนุญาต

ตามมุมมองของ The Information Commissioner แล้วนั้น ไม่สามารถที่จะมีการทำ หนดมาตรฐานด้านรักษาความปลอดภัยเพื่อให้เป็นไปตาม Data Protection Principles ในหลักการข้อที่ 7 ได้ เนื่องจากมาตรการรักษาความปลอดภัยที่ควรจะมีการนำ ไปใช้นั้นย่อมแตกต่างกันไปในแต่ละสถานการณ์ อีกทั้งการประเมินความเหมาะสมของมาตรการรักษาความปลอดภัยนั้นยังขึ้นอยู่กับการคาดการณ์ถึงอันตรายที่อาจเกิดขึ้นจากการเข้าถึง, ประมวลผล หรือทำ ลายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต ดังนั้น The Information Commissioner จึงสนับสนุนให้ผู้ควบคุมข้อมูลใช้วิธีการรักษาความปลอดภัยที่เหมาะสมโดยอิงตามความเสี่ยงที่อาจเกิดขึ้น

การปฏิบัติเพื่อให้เป็นไปตามหลักการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ตามหลักการข้อที่ 7 ซึ่งได้ทำ หนดให้มีการใช้มาตรการรักษาความปลอดภัยด้านเทคนิค และด้านองค์กรเพื่อ

คุ้มครองข้อมูลส่วนบุคคลนั้น ถึงแม้ว่าจะมีการสนับสนุนให้ใช้มาตรการรักษาความปลอดภัยที่อิงกับความเสี่ยงของแต่ละองค์กรก็ตาม แต่ The Information Commissioner ก็ยังได้มีการวางหลักมาตรการรักษาความปลอดภัยพื้นฐานสำหรับธุรกิจซึ่งทุกองค์กรควรจะต้องปฏิบัติตาม สำหรับการประมวลผลข้อมูลโดยคอมพิวเตอร์แล้วนั้น หลักดังกล่าว รวมไปถึง

1. มาตรการทางเทคนิค

(1) มีการคุ้มครองโดย firewalls สำหรับการเชื่อมต่ออินเตอร์เน็ต เพื่อจำกัดการบุกรุกและป้องกันการติดไวรัส

(2) ใช้ซอฟท์แวร์ระบุและป้องกันไวรัส เพื่อทำจัดหรืออย่างน้อยเพื่อลดความเสี่ยงของการติดไวรัส

(3) จำกัดการเข้าสู่ฐานข้อมูลเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น เพื่อป้องกันการเข้าถึงหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

(4) ใช้มาตรการป้องกันแบบรหัสผ่านสำหรับระบบคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงหรือการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

(5) มีอุปกรณ์สำรองข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลไม่ได้ในกรณีที่เกิดปัญหา หรือเกิดความเสียหายที่ไม่อาจกู้คืนได้กับระบบข้อมูล

2. มาตรการทางกายภาพ

(1) มีระบบกล้องวงจรปิด เพื่อปกป้องบริเวณที่มีความสำคัญ และเป็นการป้องกันพนักงานหรือบุคคลภายนอกในการกระทำใดๆ ที่ไม่เหมาะสม

(2) ติดตั้งสัญญาณกันขโมย เพื่อปกป้องพื้นที่ และป้องกันบุคคลภายนอกพยายามเข้าสู่สำนักงานนอกเวลาทำการ

(3) มีนโยบายการลงชื่อผู้เข้าติดต่อ เพื่อควบคุมบริเวณที่มีการจัดเก็บ และประมวลผลข้อมูล

(4) ใช้ระบบล็อคประตูภายนอก เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลในช่วงนอกเวลาทำการ

นอกเหนือจากมาตรการรักษาความปลอดภัยที่กล่าวข้างต้นแล้ว องค์กรควรทำการตรวจสอบระบบปฏิบัติการประมวลผลข้อมูลส่วนบุคคล เพื่อระบุถึงความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนบุคคล ซึ่งเป็นไปตามหลักการอิงความเสี่ยงตามที่ the

Information Commissioner แนะนำ นั่นเอง ซึ่งในการกำ หนดถึงระดับความเสี่ยงนั้น ต้องคำ นึงถึงปัจจัยหลายประการ กล่าวคือผลกระทบจากการละเมิดด้านความปลอดภัย, ความเป็นไปได้ที่จะเกิดเหตุการณ์ดังกล่าว, จำนวนบุคคลที่อาจได้รับผลกระทบ และค่าใช้จ่ายในการใช้มาตรการป้องกัน และมาตรการเหล่านี้จะไม่สามารถเกิดผลได้ ถ้าหากไม่มีการสื่อสารกับพนักงานที่เพียงพอ เพื่อให้เกิดประสิทธิภาพในการรักษาความปลอดภัยอย่างแท้จริง จึงควรที่จะมีการฝึกอบรมพนักงาน โดยแต่ละองค์กรควรมีการใช้ขั้นตอนที่เหมาะสม และติดตามผลโดยให้พนักงานรู้ตัวว่ากำ ลังถูกสังเกตการณ์อยู่ อีกทั้งให้ความรู้ถึงโทษทางอาญาตาม Data Protection Act, section 55 ในกรณีที่พนักงานเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตด้วย

<u>พนักงานกับการรักษาความปลอดภัยของข้อมูลส่วนบุคคล</u>

ตามหลักการของ Data Protection Principles ใน Schedule 1, part 2, para.11 ที่ได้มีการให้คำ อธิบายการตีความหลักการข้อที่ 7 ไว้ว่า ผู้ควบคุมข้อมูลจะต้องใช้มาตรการที่เหมาะสมเพื่อให้แน่ใจได้ถึงความรับผิดชอบเชื่อถือได้ของพนักงานที่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ กล่าวคือนายจ้างมีหน้าที่ตามกฎหมายในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่ตนเป็นผู้ควบคุมข้อมูล โดยการควบคุมการกระทำ ต่างๆ ของลูกจ้าง เพื่อเป็นการปฏิบัติตามข้อกำ หนดดังกล่าวนี้ซึ่งไม่ได้มีการกำ หนดหน้าที่ไว้อย่างเฉพาะเจาะจง นายจ้างจึงเพียงแค่ใช้มาตรการที่เหมาะสมก็ถือว่าเพียงพอแล้ว โดยหน้าที่ดังกล่าวนี้มีลักษณะต่อเนื่อง กล่าวคือต้องมีการปฏิบัติทั้งก่อนที่พนักงานจะสามารถเข้าถึงข้อมูลได้ และต้องปฏิบัติต่อไปภายหลังจากนั้นอีกด้วย

ความเหมาะสมของมาตรการนั้นย่อมขึ้นอยู่กับแต่ละสถานการณ์ โดยมี the Employment Practices Data Protection Code (the Employment Code) ซึ่งจัดทำ โดย the Information Commissioner เป็นเครื่องช่วยในการกำ หนดแนวทางในการดำ เนินการที่นายจ้างควรจะต้องปฏิบัติ โดยในเบื้องต้นนั้น นายจ้างควรจะทำให้แน่ใจได้ว่าพนักงานทราบถึงขอบเขตความรับผิดทางอาญาที่ตนอาจได้รับในกรณีที่มีการจงใจหรือประมาทเลินเล่อเปิดเผย

ข้อมูลส่วนบุคคลนอกเหนือไปจากตามนโยบายและขั้นตอนของนายจ้าง อีกทั้งนายจ้างจะต้องใช้ขั้นตอนเพื่อให้แน่ใจได้ถึงความรับผิดชอบน่าเชื่อถือของพนักงานที่สามารถเข้าถึงข้อมูล โดยไม่จำกัดเพียงเฉพาะการตรวจสอบประวัติพนักงานเท่านั้น แต่รวมไปถึงการฝึกอบรม และการทำความเข้าใจในเรื่องหน้าที่ในการรักษาความลับของข้อมูล และการระบุข้อสัญญาเรื่องการรักษาความลับไว้ในสัญญาจ้างแรงงานด้วย นอกจากนี้ the Employment Code ยังได้แนะนำให้มีการกำหนดโทษทางวินัยกรณีที่มีการละเมิดด้านความปลอดภัยอย่างรุนแรงไว้ด้วย

<u>มาตรการในการจัดการความเสี่ยง</u>

ผลกระทบสำคัญจากการปรับใช้หลักการข้อที่ 7 ในเรื่องการรักษาความปลอดภัยของข้อมูลนี้ก็คือ การเกิดความจำเป็นที่จะต้องมีการกระทำการประเมินความเสี่ยงที่อาจเกิดขึ้นกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลทั้งหมด โดยเมื่อมีการระบุถึงความเสี่ยงได้แล้ว ก็ควรที่จะต้องมีการใช้มาตรการที่เหมาะสม ซึ่งพิจารณาจากระดับของความเสี่ยง, พัฒนาการของเทคโนโลยี และค่าใช้จ่ายในการใช้มาตรการนั้น มาตรการรักษาความปลอดภัยของแต่ละองค์กรบางส่วนนั้นย่อมขึ้นอยู่กับนโยบายและขั้นตอนด้านเอกสาร อาทิ clean desk policy กล่าวคือนโยบายที่กำหนดห้ามการวางเอกสารที่มีข้อมูลส่วนบุคคลทิ้งไว้บนโต๊ะในสำนักงาน การใช้เครื่องทำลายเอกสาร เป็นต้น การฝึกอบรมพนักงาน นโยบายและขั้นตอนการประสานงานก็เป็นสิ่งที่มีความจำเป็นและควรมีลักษณะต่อเนื่อง นอกจากนี้ the Information Commissioner ยังได้มีการกำหนดให้ผู้ควบคุมข้อมูลทำการตรวจสอบอย่างเป็นประจำเพื่อให้แน่ใจได้ว่านโยบายและขั้นตอนต่างๆ นั้นเพียงพอ, ใช้ได้จริงและมีการนำไปใช้ในทางปฏิบัติ[39]

ในเรื่องของการรักษาความปลอดภัยของข้อมูลในประเทศอังกฤษนั้นอาจสรุปได้ว่า ตาม Data Protection Principles ในหลักการข้อที่ 7 นั้นมีองค์ประกอบหลักสามประการ ประการแรก คือการกำหนดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับข้อมูลส่วนบุคคลที่มีการประมวลผลขององค์กร ประการที่สอง คือการทำให้แน่ใจถึงความรับผิดชอบน่าเชื่อถือของพนักงานที่มีหน้าที่

---

[39] Mandy Webster, *supra note18,* pp.83-85, 95

เกี่ยวข้องกับข้อมูลส่วนบุคคล และประการสุดท้าย คือการตรวจตราการปฏิบัติตามกฎหมายของผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งจะเห็นได้ว่าการคงไว้ซึ่งระดับการรักษาความปลอดภัยที่เหมาะสมขององค์กรนั้นจะต้องอาศัยนโยบายและขั้นตอนการปฏิบัติงานที่มีประสิทธิภาพ ซึ่งจะเกิดขึ้นได้ต่อเมื่อมาตรการรักษาความปลอดภัยนั้นเหมาะสมในทางปฏิบัติและไม่เกินความเป็นจริง รวมไปถึงมีการสื่อสารที่ดีกับพนักงาน และการตรวจสอบก็เป็นอีกเรื่องหนึ่งที่มีความสำคัญซึ่งจะช่วยแสดงให้เห็นถึงขั้นตอนที่ไม่เหมาะสมหรือไม่สามารถปฏิบัติได้ในสถานการณ์จริง อีกทั้งการจัดทำ the Employment Code ซึ่งช่วยในการกำหนดแนวทางและให้คำแนะนำ ในการฝึกอบรมและให้ความรู้แก่พนักงานในเรื่องการคุ้มครองข้อมูลส่วนบุคคลอีกด้วย

จากข้างต้น ก็จะเห็นได้ว่าข้อกำหนดตามกฎหมายในเรื่องการรักษาความปลอดภัย และคุ้มครองความลับของข้อมูลตามกฎหมายต่างประเทศนั้น จะไม่เป็นการกำหนดเจาะจงเพื่อใช้กับการประกอบธุรกิจข้อมูลเครดิตเท่านั้น แต่จะเป็นการกำหนดเพื่อให้สามารถนำไปปรับใช้ได้กับข้อมูลส่วนบุคคลทุกประเภทของแต่ละองค์กร ข้อกำหนดต่างๆ จึงมีลักษณะเป็นการวางหลักการ ซึ่งไม่ระบุถึงมาตรการที่จะต้องนำไปใช้โดยเฉพาะเจาะจง ประเทศสหรัฐอเมริกานั้น ให้ความสำคัญกับการประเมินความเสี่ยง และใช้มาตรการรักษาความปลอดภัยที่อิงกระบวนการ กล่าวคือจะต้องเป็นการปรับใช้ แก้ไข พัฒนาอย่างต่อเนื่องไม่มีที่สิ้นสุด ส่วนในประเทศอังกฤษก็มีลักษณะคล้ายกัน โดยเน้นไปที่การประเมินความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลของแต่ละองค์กร อีกทั้งยังให้ความสำคัญในเรื่องของพนักงานที่สามารถเข้าถึงข้อมูลได้ และเมื่อพิจารณาเปรียบเทียบกับแนวปฏิบัติที่มีการบังคับใช้กับบริษัทข้อมูลเครดิตของประเทศไทยในปัจจุบันแล้วนั้น จะเห็นได้ว่ามีหลักการพื้นฐานในลักษณะเดียวกันในเรื่องการรักษาความปลอดภัยของข้อมูล โดยอาจมีแนวทางการกำหนดหน้าที่ที่แตกต่างกันออกไปบ้าง อีกทั้งในเรื่องหน้าที่บางประการตามกฎหมายของไทย ซึ่งตามกฎหมายแล้วนั้นยังไม่มีการกำหนดไว้อย่างชัดเจนเช่นดังต่างประเทศ อาทิ หน้าที่ในการแจ้งเตือนไปยังผู้ที่ได้รับผลกระทบจากการละเมิดด้านความปลอดภัย ตามกฎหมายของประเทศสหรัฐอเมริกา หรือหน้าที่ของนายจ้างในการทำให้เกิดความแน่ใจ

ในความรับผิดชอบเชื่อถือได้ของลูกจ้าง ตาม Data Protection Act ของประเทศอังกฤษ เป็นต้น

และเมื่อพิจารณาจากแนวโน้มในเรื่องการรักษาความปลอดภัยของข้อมูลในประเทศไทยแล้วนั้น ประเด็นที่มีความเสี่ยงที่อาจเกิดการละเมิดด้านความปลอดภัยได้มากที่สุด ก็คือเรื่องของภัยคุกคามภายในองค์กร กล่าวคือการโจมตีระบบข้อมูลเทคโนโลยีสารสนเทศขององค์กรนั้น มีสาเหตุมาจากภัยคุกคามภายในองค์กรเพิ่มมากยิ่งขึ้น โดยมีลักษณะเป็นการเกิดจากบัญชีผู้ใช้ที่ถูกเปิดเผยข้อมูล หรือจากบุคคลภายในองค์กรที่มีเจตนาไม่ชอบด้วยกฎหมาย ทั้งนี้ บัญชีผู้ใช้ภายในองค์กรมักมีสิทธิในระดับสูงสุดสำหรับการเข้าถึงระบบและข้อมูลสำคัญ Aligning Data Protection Priorities with Risks ในเดือนเมษายน 2006 ของ Farrester Research ระบุว่ารูปแบบการโจมตีที่พบเห็นได้มากที่สุด โดยคิดเป็นร้อยละ 39 ของการโจรกรรมข้อมูลมีสาเหตุมาจากผู้ใช้ที่ใช้สิทธิของตนในทางที่ผิด ดังนั้น เพื่อเป็นการป้องกันเหตุการณ์ดังกล่าว จึงเห็นว่าบริษัทข้อมูลเครดิตควรมีการให้ความสำคัญในประเด็นของระบบการรักษาความปลอดภัยในเรื่องการเข้าถึงระบบข้อมูล ซึ่งนอกจากจะต้องเป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลเครดิต และแนวปฏิบัติในเรื่องการรักษาความปลอดภัยการให้บริการข้อมูลเครดิตแล้วนั้น ยังจะต้องเป็นไปตามพัฒนาการของเทคโนโลยีที่เป็นที่ยอมรับกันโดยทั่วไปในปัจจุบันด้วย รวมไปถึงมาตรการด้านพนักงาน ที่จะต้องมีการฝึกอบรมให้ความรู้ในเรื่องการรักษาความปลอดภัยและความลับของข้อมูล รวมไปถึงการแจ้งให้พนักงานทราบถึงโทษตามกฎหมายในกรณีที่มีการฝ่าฝืน กล่าวคือ ตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ในมาตรา 53 ซึ่งบัญญัติว่า บุคคลใดซึ่งรับรู้ข้อมูลของบุคคลจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ถ้าผู้นั้นนำข้อมูลดังกล่าวไปเปิดเผยแก่บุคคลอื่น ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงสิบปี หรือปรับไม่เกินห้าแสนบาท หรือทั้งจำทั้งปรับด้วย

ยิ่งไปกว่านั้น เพื่อเป็นการพัฒนาระบบการรักษาความปลอดภัย และคุ้มครองความลับของข้อมูลเครดิตให้ดียิ่งขึ้นนั้น การให้ความสำคัญกับการประเมินความเสี่ยง และการติดตามความก้าวหน้าของเทคโนโลยี และอันตรายการคุกคามในรูปแบบต่างๆ

เป็นปัจจัยสำคัญที่ไม่ควรมีการมองข้าม รวมไปถึงการพัฒนาระบบให้เป็นไปตามมาตรฐานสากล เพื่อรับรองความปลอดภัยของข้อมูลให้เป็นไปตามมาตรฐานที่มีการยอมรับอย่างกว้างขวาง อาทิ มาตรฐาน ISO/IEC 27001 อีกทั้งการตรวจสอบระบบอย่างเป็นประจำ ก็เป็นอีกแนวทางหนึ่งที่จะทำให้เกิดความมั่นใจได้ว่ามีการปฏิบัติถูกต้องเป็นไปตามหน้าที่ซึ่งกฎหมายได้กำหนดไว้ ซึ่งตามประกาศของคณะกรรมการข้อมูลเครดิตในเรื่องการรักษาความปลอดภัยของข้อมูลนี้ ก็ได้กำหนดให้บริษัทข้อมูลเครดิตต้องจัดให้มีผู้เชี่ยวชาญภายนอก ซึ่งธนาคารแห่งประเทศไทยได้ให้ความเห็นชอบ ทำการตรวจสอบระบบที่เกี่ยวข้องกับการประมวลผลข้อมูลทุกระบบ (System Audit) และออกรายงานยืนยันความถูกต้องครบถ้วนของทุกระบบอย่างน้อยปีละหนึ่งครั้ง โดยรายงานดังกล่าวนั้นจะต้องส่งไปยังคณะกรรมการคุ้มครองข้อมูลเครดิตด้วย จึงเป็นการกำกับดูแลด้านความปลอดภัยของข้อมูลเครดิตที่มีความเหมาะสมและส่งผลเป็นการให้ความคุ้มครองแก่เจ้าของข้อมูลด้วยในที่สุดนั่นเอง

3.3 ปัญหาความรับผิดในกรณีที่เกิดการฝ่าฝืนการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิต

ข้อมูลเครดิตที่มีการจัดเก็บ ใช้ และเปิดเผยโดยระบบคอมพิวเตอร์ที่มีลักษณะเป็นเครือข่ายนี้ ย่อมมีความเสี่ยงที่จะเกิดภัยคุกคามต่างๆ ต่อข้อมูลได้ ถ้าหากกรณีการฝ่าฝืนการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิตได้เกิดขึ้น ผู้ที่จะได้รับผลกระทบอย่างหลีกเลี่ยงไม่ได้ก็คือเจ้าของข้อมูล ซึ่งเมื่อเกิดการละเมิดด้านความปลอดภัยขึ้นแล้วนั้น ข้อมูลเครดิตซึ่งเป็นข้อมูลด้านการเงินที่มีความสำคัญของเจ้าของข้อมูลนั้นอาจนำถูกนำไปใช้ในทางที่มิชอบด้วยกฎหมาย ซึ่งอาจก่อให้เกิดความเสียหายเป็นอย่างมากแก่เจ้าของข้อมูลได้ จึงมีความจำเป็นที่จะต้องพิจารณาถึงความรับผิดของบริษัทข้อมูลเครดิตซึ่งมีหน้าที่ตามกฎหมายในการรักษาความปลอดภัยของข้อมูลหากเกิดเหตุการณ์ในลักษณะดังกล่าวนี้

ในปัจจุบัน การดำเนินคดีกับบริษัทข้อมูลเครดิตในเรื่องการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลใน

ประเทศไทยนั้นยังไม่เกิดขึ้น เพื่อประโยชน์ในการศึกษาวิเคราะห์เทียบเคียง ในเบื้องต้นนี้จึงจะทำการอธิบายถึงลักษณะของความรับผิด และดำเนินคดีที่เกิดขึ้นในต่างประเทศ กล่าวคือ

<u>การดำเนินคดีในกรณีเกิดการละเมิดด้านความปลอดภัยของข้อมูล</u>

ประเทศสหรัฐอเมริกานั้น กรณีที่ได้รับความเสียหายทางการเงินจากการละเมิดด้านความปลอดภัย เนื่องจากบริษัทมีการใช้มาตรการรักษาความปลอดภัยที่ล้าสมัยซึ่งไม่มีประสิทธิภาพเพียงพอ โจทก์อาจอาศัยฐานในการดำเนินคดีที่ว่า บริษัทมีความประมาทเลินเล่อที่ไม่ใช้มาตรการรักษาความปลอดภัยที่ทันสมัยกว่านั้น แล้วโจกท์ควรจะอ้างด้วยว่าแม้บริษัทจะปฏิบัติตามแนวทางปฏิบัติของภาคอุตสาหกรรมแล้วก็ตาม แนวทางปฏิบัตินั้นกลับส่งผลให้เกิดความล้มเหลวซ้ำอีก และยังมีทางเลือกอื่นที่สามารถนำมาใช้ได้ เพื่อที่โจทก์จะสามารถเรียกค่าเสียหายจากการประมาทเลินเล่อดังกล่าว แต่อย่างไรก็ตาม การกล่าวอ้างเช่นนั้นก็อาจเกิดอุปสรรคในการต่อสู้คดีได้หลายประการ ในเบื้องต้น จำเลยอาจอ้างว่าโจทก์ไม่สามารถอ้างหลักประมาทเลินเล่อได้ เนื่องจากความเสียหายของโจทก์มีลักษณะเป็นทางการเงินเท่านั้น หลักเดิมในการอ้างการประมาทเลินเล่อ ศาลจะอนุญาตให้มีการจ่ายค่าชดเชยความเสียหายทางการเงิน เฉพาะกรณีที่ความเสียหายนั้นมีความสัมพันธ์กับความเสียหายทางร่างกายหรือทรัพย์สิน แต่ก็มีความคิดที่ว่ามุมมองแบบเดิมนั้นเริ่มจะอ่อนผลลง โดยที่ศาลได้หันมาใช้แนวคิดเรื่องการฉ้อโกงและหลอกลวง การกล่าวอ้างที่ไม่เป็นจริงโดยประมาทเลินเล่อ และการใช้ความลับทางการค้าในทางที่มิชอบ ศาลบางแห่งได้ลดการตีความอย่างเคร่งครัด ในกรณีที่ความเสียหายทางเศรษฐกิจนั้นสามารถคาดเห็นได้อย่างแน่ชัด

ยิ่งไปกว่านั้น ถึงแม้ว่าจะยังคงมีการใช้หลักเดิมอยู่ โจทก์ซึ่งได้รับความเสียหายจากการสูญเสียข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินของตนก็สามารถอ้างได้ว่าเป็นสถานการณ์ที่เป็นข้อยกเว้น การที่ศาลได้จำกัดการเรียกค่าชดเชยทางการเงินในคดีประมาทเลินเล่อนั้นก็เนื่องมาจากเชื่อว่าโจทก์สามารถอ้างกฎเรื่องละเมิดอื่นๆ เพื่อเรียกร้องค่าเสียหายอย่างอื่นที่ไม่ใช่ตัวเงิน อาทิ ค่าเสียหายทางจิตใจ หรือค่าเสียหายด้านการเงิน ซึ่งกฎอื่นนั้นรวมไปถึง dignitary interests ซึ่งรวมถึงสิทธิในความเป็นอยู่ส่วนตัวด้วย

นั่นเอง ซึ่งจากข้อเท็จจริงในกรณีลักษณะนี้ หนึ่งในสาเหตุสำคัญที่ทำให้โจทก์เกิดความเสียหายทางการเงินก็คือการละเมิดสิทธิในความเป็นอยู่ส่วนตัวของโจทก์ ประชาชนได้วางใจให้ข้อมูลของตนแก่องค์กร โดยมีความคาดหวังว่าองค์กรนั้นจะใช้ขั้นตอนที่เหมาะสมในการรักษาความปลอดภัยข้อมูลของตนจากบุคคลที่สาม ถ้าการปฏิบัติด้านความปลอดภัยของโจทก์หละหลวมจนทำให้ผู้บุกรุก (Hacker) สามารถได้ข้อมูลของโจทก์ไป ความประมาทเลินเล่อขององค์กรนั้นได้ส่งผลให้ Hacker สามารถจงใจละเมิดสิทธิในความเป็นอยู่ส่วนตัวของโจทก์ได้ หรืออาจกล่าวได้ว่าความประมาทเลินเล่อขององค์กรเป็นการอนุญาตให้ Hacker สามารถใช้วิธีการที่ไม่ชอบด้วยกฎหมายทำการละเมิดต่อโจทก์โดยการลักข้อมูลส่วนบุคคล และใช้ข้อมูลนั้นสร้างความเสียหายทางการเงินแก่โจทก์ เนื่องจากการละเมิดสิทธิความเป็นอยู่ส่วนตัวของโจทก์เป็นส่วนที่เป็นสาระสำคัญของการกระทำความผิดนั่นเอง ซึ่งทำให้เกิดความเห็นของศาลที่จะยกเว้นการเรียกค่าเสียหายจากการประมาทเลินเล่อ ซึ่งเป็นค่าเสียหายทางการเงินเท่านั้น

ในคดี Jones v. Commerce Bancorp, Inc ในปี ค.ศ. 2006 โจทก์ได้ยื่นฟ้องธนาคารหลังจากพบว่าเงินหายไปจากในบัญชี เนื่องจากอาชญากรได้ขโมยข้อมูลส่วนบุคคลของโจทก์จากธนาคาร และใช้ข้อมูลนั้นเพื่อถอนเงินไป โดยโจทก์อ้างว่าเนื่องจากบัญชีของตนมีเงินไม่เพียงพอ ทำให้โจทก์ได้รับความเสียหายทางการเงินหลายประการ รวมไปถึงการยกเลิกกรมธรรม์ประกันภัยของโจทก์ เนื่องจากขาดส่งเบี้ยประกัน โดยประเด็นในคำฟ้องได้รวมไปถึงการประมาทเลินเล่อ และจงใจทำให้เกิดความเครียดทางจิตใจ ท้ายที่สุดศาลได้ตัดสินยกฟ้องในประเด็นจงใจทำให้เกิดความเครียดทางจิตใจ แต่ไม่ยกฟ้องในประเด็นประมาทเลินเล่อ ซึ่งมีการเรียกร้องค่าเสียหายทางเศรษฐกิจเท่านั้น

ในหลายคดีที่เกี่ยวข้องกับการละเมิดด้านความปลอดภัยจำเลยพ้นจากความรับผิดเนื่องจากทฤษฎีที่ว่าค่าเสียหายของโจทก์เป็นเพียงการคาดการณ์ซึ่งไม่สามารถกำหนดได้จนกว่า Hacker จะใช้ข้อมูลที่ขโมยมานั้นก่อให้เกิดความเสียหายแก่โจทก์ บางศาลได้ให้ความเห็นว่าความเสียหายของโจทก์จากการขโมยข้อมูลส่วนบุคคลนั้นยังห่างไกลเกินไปจนกว่าจะเกิดความเสียหายทางการเงินอย่างแท้จริง และยังยกเว้นค่าเสียหายแม้โจทก์ได้อ้างว่าได้เสียค่า

ใช้จ่ายในการ credit monitoring เนื่องมาจากการละเมิดด้านความปลอดภัยดังกล่าว โดยศาลหนึ่งได้ระบุว่าค่าใช้จ่ายเหล่านี้ไม่ได้เป็นผลจากความเสียหายในปัจจุบัน แต่เป็นการคาดการณ์ถึงความเสียหายในอนาคตที่ยังไม่เกิดขึ้น แม้แนวทางนี้จะเป็นความเห็นส่วนใหญ่ แต่ก็มีการโต้แย้งที่มีเหตุผลและมีบางแนวคำพิพากษาที่เป็นประโยชน์ต่อโจทก์ โดยอาศัยการเทียบเคียงกับคดีละเมิดที่โจทก์ได้สัมผัสกับสารพิษแต่ยังไม่แสดงอาการเจ็บป่วย ซึ่งศาลได้อนุญาตให้โจทก์ในกรณี toxic-tort นี้ได้รับค่าชดเชยค่าใช้จ่ายในการตรวจตราทางการแพทย์ หากว่าการสัมผัสสารพิษนั้นเป็นการเพิ่มความเสี่ยงเป็นอย่างมากที่จะเกิดการเจ็บป่วย

ในคดีการละเมิดด้านความปลอดภัยของข้อมูล ได้มีการเพิ่มความเสี่ยงที่จะเกิดความเสียหายทางการเงินในอนาคตเป็นอย่างมาก กล่าวคือในกรณีที่ข้อมูลที่ถูกขโมยไปนั้นเป็นข้อมูลทางการเงิน จึงเป็นไปได้อย่างสูงว่าท้ายที่สุดอาชญากรจะใช้ข้อมูลนั้นเพื่อผลประโยชน์ของตน และสร้างความเสียหายให้แก่โจทก์ ดังนั้น credit monitoring จึงไม่เป็นเพียงการใช้ความรอบคอบเท่านั้น แต่เป็นสิ่งที่จำเป็นอีกด้วย

ในคดี Lockwood v. Certegy Check Services, Inc ได้เริ่มมีการใช้มุมมองที่ตรงกับสถานการณ์จริงที่โจทก์ต้องประสบในกรณีของการละเมิดด้านความปลอดภัยมากยิ่งขึ้น โดยศาลได้กล่าวว่า แม้บางศาลจะตัดสินว่าเนื่องจากการที่โจทก์ซึ่งได้ถูกขโมยข้อมูลไปแต่ยังไม่มีการใช้ข้อมูลดังกล่าวโดยมิชอบนั้น ยังไม่ถือว่าได้รับความเสียหายตามความเป็นจริง แต่การพิสูจน์ถึงความเสียหายตามความเป็นจริงนั้นสามารถทำได้ โดยการแสดงถึงความเสี่ยงที่จะเกิดอันตรายในอนาคต หรือการกระทำที่สร้างความเสียหายให้แก่โจทก์ เพียงแต่เพิ่มความเสี่ยงที่จะเกิดอันตรายในอนาคตซึ่งโจทก์ต้องได้รับเนื่องจากการกระทำของจำเลย

ในคดี Ruiz v. Gap,Inc ศาลได้มีคำสรุปคล้ายคลึงกัน โดยยอมรับหลักดังกล่าวว่าความเสี่ยงที่จะเกิดความเสียหายในอนาคตจะต้องเชื่อถือได้ มิใช่เป็นเพียงการคาดการณ์หรือเหตุสมมติ และศาลได้ตัดสินว่าข้อกล่าวอ้างของโจทก์ในเรื่องการเพิ่มความเสี่ยงที่จะเกิด identity theft นั้นเพียงพอที่จะผ่านเกณฑ์ได้

อีกกรณีหนึ่งคือการที่จำเลยอาจต่อสู้ว่าไม่เป็นการประมาทเลินเล่อ เนื่องจากมาตรการรักษาความปลอดภัยของตนนั้นเป็นไป

ตามมาตรฐานของอุตสาหกรรมแล้ว และยิ่งไปกว่านั้น ถ้าหากเป็นกรณีที่มีธรรมเนียมทางการค้าที่เป็นเอกภาพในเรื่องการรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ศาลได้มองว่าการปฏิบัติตามธรรมเนียมนั้นไม่ถือเป็นการหักล้างประเด็นในเรื่องประมาทเลินเล่อ ถึงแม้จะเคยมีแนวคำพิพากษาในคดีละเมิดว่า การที่จำเลยปฏิบัติตามธรรมเนียมด้านการรักษาความปลอดภัยแล้วนั้นถือเป็นการปฏิบัติอย่างเหมาะสมแล้วก็ตาม แต่แนวคำพิพากษานั้นก็ได้ถูกวิพากษ์วิจารณ์อย่างกว้างขวาง ในปัจจุบัน แนวคิดที่ได้รับการยอมรับอย่างทั่วไปก็คือ แม้ว่าหลักฐานแห่งการปฏิบัติตามธรรมเนียมนั้นมีความเกี่ยวข้องและรับฟังได้ก็ตาม แต่ก็ไม่ใช่ข้อตัดสินในเรื่องประมาทเลินเล่อ อุตสาหกรรมไม่สามารถได้รับอนุญาตให้กำหนดมาตรฐานความระมัดระวังของตนเพื่อจุดประสงค์ทางกฎหมายละเมิด ดังนั้น บริษัทจึงไม่หลุดพ้นจากความรับผิดเรื่องการประมาทเลินเล่อเพียงเพราะการปฏิบัติด้านการรักษาความปลอดภัยของตนนั้นเป็นไปตามมาตรฐานของอุตสาหกรรม ท้ายที่สุดก็เป็นหน้าที่ของศาลในการตัดสินว่าธรรมเนียมปฏิบัตินั้นถือเป็นการกระทำที่เหมาะสมแล้วหรือไม่ เพื่อทำการตัดสินดังกล่าว ศาลจะต้องทำการวิเคราะห์ถึงผลดีและผลเสียอย่างระมัดระวัง

จำเลยอาจต่อสู้ว่าการวิเคราะห์ผลดีและผลเสียนั้นไม่เป็นการให้เหตุผลในการสร้างหน้าที่แก่องค์กรซึ่งครอบครองข้อมูลส่วนบุคคลในรูปของข้อมูลคอมพิวเตอร์ ในการเพิ่มกระบวนการรักษาความปลอดภัยให้รวมไปถึงการเข้ารหัส และการพิสูจน์ความแท้จริงของตัวตน และไม่สามารถพิสูจน์ได้ว่าการปฏิบัติด้านการรักษาความปลอดภัยของธุรกิจในปัจจุบันมีลักษณะไม่เหมาะสมหรือเป็นการประมาทเลินเล่อ จำเลยอ้างว่าการกระทำใดๆ ของมนุษย์ล้วนก่อให้เกิดอันตรายได้ และไม่อาจคาดหวังให้บุคคลหรือนิติบุคคลใดทำการป้องกันความเสี่ยงได้ทั้งหมด ซึ่งในการตัดสินว่าเมื่อใดที่กฎหมายละเมิดกำหนดให้จำเลยป้องกันความเสี่ยงนั้น กฎหมายใช้วิธีการการวิเคราะห์ถึงผลดีและผลเสีย ศาลหลายแห่งได้ใช้วิธีการดั้งเดิมในการตัดสินใจ โดยพิจารณาความเป็นไปได้ที่การกระทำของจำเลยจะส่งผลให้เกิดความเสียหาย, ความรุนแรงของความเสียหายที่คาดเห็น และค่าใช้จ่ายในการหลีกเลี่ยงความเสียหายนั้น โดยที่ปัจจัยเหล่านี้จะช่วยในการวิเคราะห์ของศาลว่ากฎหมายละเมิดควรจะกำหนดเรียกร้องให้ธุรกิจใช้มาตรการรักษา

ความปลอดภัยที่ใหม่และเข้มแข็งมากยิ่งขึ้นหรือไม่ ซึ่งข้อดีจากการสร้างหน้าที่นี้สามารถเห็นได้อย่างชัดเจน แต่ก็จำเป็นที่จะต้องพิสูจน์ให้ศาลเห็นด้วยว่ามีมาตรการรักษาความปลอดภัยอื่นที่สามารถนำมาใช้ได้จริงทั้งในทางเทคนิคและทางปฏิบัติ ซึ่งการใช้มาตรการรักษาความปลอดภัยแบบใหม่ย่อมก่อให้เกิดค่าใช้จ่ายรวมไปถึงการฝึกอบรมพนักงาน แต่ถ้าหากชั่งน้ำหนักแล้วจะพบว่าผลดีจากการกำหนดหน้าที่ในการรักษาความปลอดภัยนี้มีมากกว่าผลเสีย แม้จะต้องใช้เงินจำนวนมากในการเริ่มมาตรการรักษาความปลอดภัยใหม่ แต่การหยุดความเสียหายทางการเงินที่เกิดขึ้นจากการเจาะเข้าสู้ระบบ และการรักษาความลับของข้อมูลส่วนบุคคลในฐานข้อมูลนั้น ก็ส่งผลดีมากกว่าอย่างชัดเจน

จึงจะเห็นได้ว่า แม้จะมีอุปสรรคที่โจทก์อาจต้องพบ แต่การใช้ทฤษฎีใหม่ในเรื่องการประมาทเลินเล่อนี้ โจทก์ทั้งที่เป็นปัจเจกบุคคล และกรณี class action จะได้รับการบรรเทาความเสียหาย และที่สำคัญไปกว่านั้นยังอาจเป็นการสร้างแรงจูงใจในทางปฏิบัติให้แก่องค์กรเอกชนในการใช้มาตรการรักษาความปลอดภัยที่ทันสมัยเพื่อคุ้มครองข้อมูลส่วนบุคคลอีกด้วย[40]

อีกประเด็นหนึ่งที่เกิดขึ้นในประเทศสหรัฐอเมริกาในกรณีเช่นนี้ คือความยากในการที่จะแสดงให้เห็นถึงความสัมพันธ์ของการกระทำและผลระหว่างการกระทำของจำเลยและความเสียหายที่โจทก์นั้นได้รับ ซึ่งนับเป็นอุปสรรคอีกอย่างหนึ่งในการดำเนินคดีและพิสูจน์ให้เห็นถึงค่าเสียหาย ในคดีการละเมิดด้านความปลอดภัยของข้อมูล ถึงแม้โจทก์จะสามารถแสดงได้ว่าตนตกเป็นเหยื่ออาชญากรรม identity theft ก็เป็นการยากที่จะแสดงให้เห็นว่าความเสียหายนี้มีเหตุสมควรที่จะเชื่อได้ว่าน่าจะเกิดขึ้นเนื่องจากการละเมิดด้านความปลอดภัยของจำเลย ในคดี Stollenwerk v. Tri-West Healthcare Alliance ศาลได้ตัดสินว่าข้อเท็จจริงที่ว่าข้อมูลของโจทก์ถูกใช้ในการเปิดบัญชีที่เป็นการฉ้อโกง ไม่เป็นการแสดงให้เห็นถึงความเกี่ยวเนื่องระหว่างการกระทำและผล เนื่องจากโจทก์ได้มีการเปิดเผยข้อมูลเดียวกันนั้นให้แก่บุคคลอื่นด้วย แต่อย่างไรก็ตาม ในการอุทธรณ์ศาลได้กลับคำ

---

[40] Edward J. Imwinkelried, Michael Cherry . "REDRESS FOR LOSS OF PRIVATE E-DATA" Trial (February, 2009).

พิพากษา โดยถือว่าการแสดงให้เห็นถึงการเกิด identity theft ถึงหกเหตุการณ์แยกกันภายหลังจากการลักข้อมูลนั้น เพียงพอที่จะชี้ให้เห็นว่ามีความสัมพันธ์ระหว่างการกระทำ และผลของการลักข้อมูลนั้น ซึ่งจากคดีนี้ทำ ให้ต้องมีการติดตามต่อไปว่าจะส่งผลเป็นการลดมาตรฐานในการแสดงให้เห็นถึงความสัมพันธ์ระหว่างการกระทำ และผลของโจทก์หรือไม่

การดำ เนินคดีตามกฎหมายระดับรัฐอาจจะมีแนวโน้มที่ดีกว่าสำ หรับโจทก์ในคดีการละเมิดด้านความปลอดภัย โดยเฉพาะในกรณีที่ฝ่ายจำ เลยมี Fiduciary duty หรือความสัมพันธ์ลักษณะพิเศษต่อโจทก์ซึ่งก่อให้เกิดหน้าที่ในการคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลของโจทก์ ตัวอย่างคดีที่มีการวิพากษ์วิจารณ์คือคดี ChoicePoint, Inc ซึ่ง ChoicePoint มีหน้าที่ต้องแจ้งเตือนเป็นลายลักษณ์อักษรตาม California's Breach Notification Statute, S.B.1386 และได้เกิดการฟ้องร้องแบบ class action เพื่อเรียกร้องค่าเสียหายโดยผู้ที่ข้อมูลส่วนบุคคลของตนถูกเปิดเผยไปยังผู้ก่ออาชญากรรม identity theft แต่ในเดือนตุลาคม ค.ศ.2006 คดี class action ของ Harrington v. ChoicePoint, Inc ดังกล่าวนี้ได้ถูกศาลยกฟ้อง เนื่องจากการที่คำ ฟ้องของโจทก์ไม่ได้มีการระบุอ้างถึงความผิดตาม FCRA จึงเป็นตัวอย่างหนึ่งที่แสดงให้เห็นถึงความพยายามที่ไม่เป็นผลของโจทก์ในการกล่าวอ้างความเสียหายต่อบริษัทที่มีการละเมิดด้านความปลอดภัยของข้อมูล

คดีที่น่าสนใจอีกคดีหนึ่งคือ คดี class action ฟ้องร้อง TJX Companies โดยกล่าวหาว่าบริษัทประมาทเลินเล่อไม่ดูแลให้มีการรักษาความปลอดภัยที่เพียงพอของข้อมูลบัตรเครดิตและบัตรเดบิตของลูกค้า และไม่เปิดเผยการละเมิดด้านความปลอดภัยเป็นระยะเวลาถึงหนึ่งเดือนหลังจากเกิดเหตุ ในเดือนกันยายน ค.ศ. 2007 TJX ได้ประกาศข้อตกลงในการยอมความสำ หรับลูกค้าที่ได้รับผลกระทบการเหตุการณ์ดังกล่าว โดยที่ TJX เสนอบริการ credit monitoring ให้แก่ลูกค้า 500,000 คนจากจำ นวนลูกค้า 46 ล้านคนที่ได้รับผลกระทบ และจะชดใช้ค่าเสียหายในการที่ลูกค้าต้องทำการเปลี่ยนใบขับขี่เนื่องจากการการละเมิดด้านความปลอดภัยของข้อมูล นอกจากคดี class action ของผู้บริโภคแล้ว Banking Association หลายรัฐก็ได้ทำ การยื่นฟ้องแบบ class action ต่อ TJX ในเดือนเมษายน ค.ศ.2007 เพื่อเรียกร้องค่าชดเชยความเสีย

หายที่เกิดจากการออกบัตรเครดิตและบัตรเดบิตใหม่ทดแทนให้แก่ลูกค้า และการจ่ายเงินที่เกิดจากการใช้บัตรเครดิตและบัตรเดบิตของลูกค้าอย่างไม่ชอบด้วยกฎหมายซึ่งเกี่ยวเนื่องกับการละเมิดด้านความปลอดภัย โดยมีการตกลงยอมความกันได้เป็นจำนวนเงิน 40.9 ล้านเรียญสหรัฐในเดือนธันวาคม ค.ศ.2007

คดี Walter v. DHL Exp. ศาลยกฟ้องคดีของโจทก์ในการเรียกร้องค่าเสียหายจากการเพิ่มขึ้นของความเสี่ยงที่จะเกิด identity theft ในอนาคต แต่มีการหมายเหตุไว้ว่า โจทก์สามารถกล่าวอ้างโดยอาศัยกฎหมายละเมิดได้

คดี Kahle v. Litton Loan Servicing LP ซึ่งมีข้อเท็จจริงว่าเกิดการขโมยฮาร์ดไดรฟ์ที่มีการใช้รหัสผ่านป้องกันซึ่งบรรจุข้อมูลส่วนบุคคลของผู้บริโภค หลังจากเกิดเหตุจำเลยได้มีหนังสือแจ้งเตือนเป็นลายลักษณ์อักษรไปยังแต่ละบุคคลที่มีข้อมูลอยู่ในฮาร์ดไดรฟ์ และแนะนำให้บุคคลเหล่านั้นดำเนินขั้นตอน fraud alert ในบัญชีของตน ความเสียหายที่โจทก์ได้รับนั้นจึงมีเพียงค่าใช้จ่ายที่เกิดขึ้นจากการซื้อบริการ credit monitoring ซึ่งเป็นผลมาจากการขโมยฮาร์ดไดรฟ์ ศาลได้ตัดสินยกฟ้องคดีของโจทก์ทั้งหมด เนื่องจากความเสียหายที่โจทก์อ้างว่าได้รับนั้นเป็นเพียงความกลัวว่าจะมีการเกิด identity theft ในอนาคต ซึ่งคดีนี้ได้ส่งผลเป็นการเน้นให้เห็นถึงเส้นแบ่งของศาลระหว่าง identity theft กับ ID exposure โดยถือหลักที่ว่า การเพิ่มขึ้นของความเสี่ยงที่จะเกิดความเสียหายในอนาคตจากการที่ข้อมูลด้านตัวตนของตนได้ถูกเปิดเผยนั้น ไม่เพียงพอที่จะสนับสนุนคำฟ้องว่าเกิดความเสียหายหรือแสดงให้เห็นถึงค่าเสียหาย

นอกเหนือจากการดำเนินคดีตามหลักกฎหมายที่ได้อธิบายข้างต้นนั้น ในประเทศสหรัฐอเมริกาซึ่งมีกฎหมายที่เกี่ยวข้องในเรื่องเรื่องการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลหลายฉบับด้วยกัน ส่งผลให้เกิดความรับผิดตามกฎหมายฉบับอื่นได้อีก เพื่อให้เกิดความชัดเจนมากยิ่งขึ้น ในประเด็นดังกล่าวสามารถอธิบายได้ดังนี้

<u>การบังคับใช้กฎหมายโดย FTC ในกรณีของการรักษาความปลอดภัยของข้อมูล</u>

ตั้งแต่ปี ค.ศ.1999 the Federal Trade Commission (FTC) ได้มีการดำเนินคดีอย่างน้อย 12 คดีในเรื่องของการปฏิบัติ

ด้านการรักษาความปลอดภัยของข้อมูลของบริษัท ในบางคดี FTC ได้ใช้หลักว่าบริษัทนั้นได้กล่าวอ้างอย่างไม่เป็นจริงต่อลูกค้าของตนในเรื่องขอบเขตของมาตรการรักษาความปลอดภัย ซึ่งเป็นการกระทำ ที่ FTC ถือว่าเป็นการปฏิบัติที่หลอกลวง (deceptive practice) ในกรณีอื่นๆ FTC ใช้หลักที่ว่ามาตรการรักษาความปลอดภัยที่ไม่เพียงพอซึ่งทำ ให้เกิดการละเมิดด้านความปลอดภัยและก่อให้เกิดความเสียหายแก่ลูกค้า ส่งผลให้เป็นการปฏิบัติที่ไม่เป็นธรรม (unfair practice)

คดีของ FTC ในเรื่องการรักษาความปลอดภัยของข้อมูลที่เป็นที่รู้จักก็คือคดีของ ChoicePoint, Inc ซึ่งดำ เนินการเป็น data broker ที่ได้มีการขายข้อมูลส่วนบุคคลของลูกค้าจำ นวน 160,000 คนของตนให้กับเครือข่ายอาชญากร identity theft อย่างไม่จงใจ และต่อมาข้อมูลบางส่วนนั้นได้ถูกใช้ในการกระทำ identity theft นอกจากนั้น ChoicePoint ยังถูกกล่าวหาว่าได้ใช้มาตรการที่หละหลวมในการตรวจสอบผู้ซื้อข้อมูลส่วนบุคคลของลูกค้าของตน โดยท้ายที่สุด ChoicePoint ได้ตกลงยอมความโดยจ่ายเงินจำ นวน 15 ล้านเหรียญสหรัฐ และตกลงที่จะจัดตั้งมาตรการรักษาความปลอดภัยใหม่ คดีของ FTC ในลักษณะเช่นนี้เป็นการสร้างความชัดเจนว่าบริษัทจำ เป็นที่จะต้องใช้มาตรการที่เหมาะสมและสมควรในการรักษาความปลอดภัยของข้อมูล นอกจากนั้นยังมีตัวอย่างคดีในระยะหลังของ FTC ในเรื่องการปฏิบัติด้านการรักษาความปลอดภัยของข้อมูล อาทิ คดี Goal Financial[41] ซึ่ง Goal Financial ได้ตกลงยอมความกับ FTC ซึ่งได้กล่าวหาว่า Goal Financial ได้ละเมิด Safe Guards Rule, The Privacy Rule และ FTCA จากการที่ไม่สามารถจัดให้มีการรักษาความปลอดภัยของข้อมูลที่เหมาะสมและสมควรสำ หรับข้อมูลส่วนบุคคลของลูกค้า ซึ่ง FTC ถือว่าการกระทำ ของบริษัทดังกล่าวอาจถือได้ว่าเป็นการปฏิบัติที่ไม่เป็นธรรมหรือหลอกลวง ความล้มเหลวด้านการรักษาความปลอดภัยของข้อมูลของบริษัทส่งผลให้พนักงานกระทำ การโอนไฟล์จำ นวนกว่า 7,000 ไฟล์ซึ่งมีข้อมูลของลูกค้าไปยังบุคคลที่สามโดยไม่ได้รับอนุญาต และพนักงานอีกคนหนึ่งได้ทำ การขายฮาร์ดไดรฟ์ซึ่งบรรจุข้อมูลที่ไม่ได้เข้ารหัสของลูกค้ากว่า 34,000 คน ซึ่งเป็นการละเมิด

---

41 Press Release, FTC (March 4, 2008).

Disposal Rule ทำให้ FTC ฟ้องร้อง Goal Financial ในประเด็นที่ว่า กระทำการหลอกลวงลูกค้าในเรื่องขอบเขตของการรักษาความปลอดภัยของข้อมูลของตน และไม่กระทำการดังต่อไปนี้ (1) ประเมินความเสี่ยงที่มีของข้อมูลของลูกค้าได้อย่างเหมาะสม (2) จำกัดการเข้าถึงข้อมูลเฉพาะพนักงานที่ได้รับอนุญาตเท่านั้น (3) ใช้โปรแกรมการรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพและเหมาะสม (4) จัดให้มีการฝึกอบรมพนักงานที่เหมาะสม (5) มีข้อกำหนดด้านสัญญากับผู้ให้บริการซึ่งเป็นบุคคลที่สามในการคุ้มครองข้อมูล โดยที่ในส่วนหนึ่งของข้อตกลงยอมความนั้น บริษัทได้ถูกกำหนดให้ต้องใช้มาตรการรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพ และมีการตรวจสอบโดยบุคคลภายนอกทุกๆ 2 ปี เป็นระยะเวลา 10 ปี

การปฏิบัติด้านข้อมูลที่อาจถือว่าเป็นการปฏิบัติที่ไม่เป็นธรรมหรือหลอกลวงโดย FTC นั้น รวมไปถึง

(1) ให้คำรับรองที่อาจทำให้เข้าใจผิด หรือเป็นเท็จในเรื่องนโยบายการรักษาความปลอดภัยหรือการรักษาความลับของบริษัท

(2) สร้างความเสี่ยงที่ไม่จำเป็นแก่ sensitive information โดยการจัดเก็บข้อมูลดังกล่าวนั้นนานเกินกว่าความจำเป็นของธุรกิจ

(3) ไม่ใช้นโยบายรหัสผ่านอย่างเหมาะสม หรือไม่ทำการประเมินความเสี่ยงที่มีต่อข้อมูลของลูกค้า

(4) ไม่ใช้มาตรการรักษาความปลอดภัยที่มีอยู่ เพื่อจำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ผ่านทาง wireless access point

(5) ไม่เข้ารหัสข้อมูลของลูกค้าเมื่อมีการจัดเก็บข้อมูลในคอมพิวเตอร์

(6) ไม่ใช้มาตรการที่เพียงพอในการตรวจหาการเข้าถึงโดยไม่ได้รับอนุญาต

โดยมาตรการทางกฎหมายของ FTC คือการออกคำสั่ง (consent orders) ซึ่งโดยส่วนมากจะไม่ส่งผลเป็นการลงโทษปรับโดยตรงต่อบริษัท แต่เป็นการตกลงยอมความระหว่างบริษัทกับ FTC โดยเป็นการสร้างภาระครั้งเดียวหรือต่อเนื่องแก่บริษัท โดยข้อกำหนดที่มักพบในคำสั่งของ FTC นั้นได้แก่ (1) ข้อตกลงที่จะเลิกหรือระงับการกระทำที่เป็นการละเมิดต่อกฎหมาย (2) ข้อตกลงที่จะ

ใช้มาตรการรักษาความปลอดภัยที่ดีขึ้นหรือใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลที่สูงยิ่งขึ้น เพื่อที่จะไม่เกิดการกระทำซ้ำอีก (3) คำรับรองของบริษัทที่จะใช้ผู้ตรวจสอบซึ่งเป็นบุคคลที่สามและมีความอิสระทำ การตรวจสอบระบบการรักษาความปลอดภัยของข้อมูล (ซึ่งโดยทั่วไปจะกำ หนดให้ต้องทำ การตรวจสอบทุกๆ 2 ปีเป็นระยะเวลา 10 หรือ 20 ปี)

<u>การดำ เนินคดีตาม The Federal Trade Commission's Disposal Rule</u>

FTC ประกาศใช้ระเบียบนี้มีผลบังคับใช้ในวันที่ 1 มิถุนายน ค.ศ.2005 โดยมีวัตถุประสงค์เพื่อลดความเสี่ยงในการฉ้อโกงผู้บริโภค และ identity theft ซึ่งเกิดจากการทำ จัดข้อมูลของผู้บริโภคอย่างไม่เหมาะสม โดยระเบียบนี้บังคับใช้กับบุคคลใดๆ ที่ FTC มีเขตอำ นาจ และมีวัตถุประสงค์ของธุรกิจในการครอบครองข้อมูลของผู้บริโภค จึงจะเห็นได้ว่ารวมไปถึง Consumer Reporting Agencies (CRA) ด้วยนั่นเอง โดยมีการกำ หนดมาตรฐานไว้ว่า ผู้ใดที่ครอบครองข้อมูลของผู้บริโภคจะต้องทำ การกำจัดข้อมูลโดยใช้มาตรการที่เหมาะสม เพื่อป้องกันการเข้าถึงหรือการใช้ข้อมูลนั้นโดยไม่ได้รับอนุญาต โดยที่มาตรการที่เหมาะสมนั้นรวมถึงตัวอย่าง ดังต่อไปนี้

(1) เผา บด หรือฉีกเอกสารที่มีข้อมูลของผู้บริโภค

(2) ทำลาย หรือลบสื่ออิเล็กทรอนิกส์ที่บรรจุข้อมูลของผู้บริโภค

(3) ทำสัญญากับบุคคลที่สามที่ประกอบธุรกิจทำ ลายบันทึกข้อมูล เพื่อทำ จัดข้อมูลของผู้บริโภค หลังจากที่ได้มีการตรวจสอบอย่างเพียงพอถึงการดำ เนินการและการปฏิบัติให้เป็นไปตามกฎหมายของบริษัทนั้น

โดยที่ระเบียบนี้จะไม่ส่งผลกระทบหรือเป็นการแก้ไขข้อกำหนดในเรื่องการทำ จัดข้อมูลของผู้บริโภคในกฎหมายระดับรัฐหรือมลรัฐอื่นๆ

โดยคดีตัวอย่างในกรณี FTC Disposal Rule นั้น ได้แก่คดี American United Mortgage Company[42] โดยที่ American United Mortgage Company ซึ่งถูกกล่าวหาว่าทิ้งเอกสารการกู้ซึ่ง

---

42 Press Release, FTC (December 18, 2007).

มีข้อมูลส่วนบุคคลของลูกค้าในที่ทิ้งขยะที่ไม่ปลอดภัย ได้ตกลงที่จะจ่ายค่าปรับ 50,000 เหรียญสหรัฐ โดยที่ FTC ได้ตั้งข้อหาแก่บริษัทว่า (1) ฝ่าฝืน FTC Disposal Rule ซึ่งกำหนดให้บริษัทต้องกำจัดข้อมูลจากรายงานข้อมูลเครดิตโดยวิธีการที่ปลอดภัย (2) ฝ่าฝืน FTC Safeguard Rule ซึ่งกำหนดให้สถาบันการเงินต้องใช้มาตรการในการรักษาความปลอดภัยข้อมูลของลูกค้า (3) ฝ่าฝืน FTC Privacy Rule โดยการไม่แจ้งเตือนด้านการรักษาความลับไปยังลูกค้า ซึ่งระบุถึงการที่บริษัทใช้ข้อมูลส่วนบุคคล โดยที่นอกเหนือจากค่าปรับแล้วนั้น บริษัทยังถูกกำหนดให้ต้องเปลี่ยนแปลงนโยบายของตนให้เป็นไปตามระเบียบทั้งสาม และทำการตรวจสอบระบบการรักษาความปลอดภัยโดยบุคคลที่สาม ทุกๆ 2 ปี เป็นระยะเวลา 10 ปี

<u>การดำเนินคดีตามกฎหมายการแจ้งเตือนถึงการละเมิดด้านความปลอดภัย</u>

ตัวอย่างการดำเนินคดีโดยอัยการในแต่ละรัฐตามกฎหมายการแจ้งเตือนถึงการละเมิดด้านความปลอดภัย ในสหรัฐอเมริกานั้น อาทิ คดี CS STARS LLC ในปีค.ศ.2007 ซึ่งอัยการแห่งรัฐ New York สามารถดำเนินคดีจนมีการยอมความเป็นครั้งแรกของรัฐ โดยมีข้อเท็จจริงในคดีว่า CS STARS ได้ทำการล่าช้าเกินสมควร จากการรอเป็นระยะเวลา 7 สัปดาห์ จึงจะทำการแจ้งเตือนว่าเครื่องคอมพิวเตอร์ที่มีข้อมูลส่วนบุคคลได้ถูกขโมยไป ซึ่งเป็นการให้เวลาแก่ผู้ที่กระทำความผิดในการที่จะใช้ข้อมูลอย่างไม่ชอบด้วยกฎหมาย โดยส่วนหนึ่งของการตกลงยอมความ CS STARS ได้ตกลงที่จะพัฒนาโปรแกรมการรักษาความปลอดภัยของตน และจะมีการตอบสนองที่ดียิ่งขึ้นถ้าหากเกิดกรณีการละเมิดด้านความปลอดภัยอีกในอนาคต อีกทั้งยังจ่ายค่าชดเชยค่าใช้จ่ายในการสอบสวนให้แก่รัฐเป็นจำนวน 60,000 เหรียญสหรัฐ

<u>การดำเนินคดีตามกฎหมาย The Fair Credit Reporting Act</u>

The Fair Credit Reporting Act (FCRA) ได้อนุญาตให้เอกชนสามารถดำเนินคดีในกรณีที่มีการฝ่าฝืนกฎหมายโดยจงใจหรือประมาทเลินเล่อตาม section 616 และ 617 ตามลำดับ กล่าวคือ ในกรณีการฝ่าฝืนกฎหมายโดยจงใจนั้น section 616 ได้กำหนดไว้ว่า ผู้ใดที่จงใจไม่ปฏิบัติตามข้อกำหนดตามกฎหมายใน

ส่วนที่เกี่ยวข้องกับผู้บริโภคนั้น มีความรับผิดต่อผู้บริโภค เป็นจำนวนเท่ากับ

(1) ค่าเสียหายที่เกิดขึ้นจริงที่ผู้บริโภคได้รับ ซึ่งเป็นผลมาจากการไม่ปฏิบัติตามกฎหมายดังกล่าว หรือค่าเสียหายเป็นจำนวนไม่น้อยกว่า 100 เหรียญสหรัฐ และไม่เกินกว่า 1,000 เหรียญสหรัฐ

(2) ค่าเสียหายเชิงลงโทษ (punitive damages) ตามที่ศาลเห็นสมควร

(3) ค่าใช้จ่ายในการฟ้องร้องคดี และค่าทนายความตามสมควรที่ศาลเป็นผู้กำหนด ในกรณีที่ชนะคดีและสามารถบังคับใช้กฎหมายเพื่อลงโทษผู้ฝ่าฝืนได้เป็นผลสำเร็จ

และในกรณีการฝ่าฝืนกฎหมายโดยประมาทเลินเล่อ ตาม section 617 ได้กำหนดไว้ว่า ผู้ใดที่ประมาทเลินเล่อไม่ปฏิบัติตามข้อกำหนดตามกฎหมายในส่วนที่เกี่ยวข้องกับผู้บริโภคนั้น มีความรับผิดต่อผู้บริโภค เป็นจำนวนเท่ากับ

(1) ค่าเสียหายที่เกิดขึ้นจริงที่ผู้บริโภคได้รับ ซึ่งเป็นผลมาจากการไม่ปฏิบัติตามกฎหมายดังกล่าว

(2) ค่าใช้จ่ายในการฟ้องร้องคดี และค่าทนายความตามสมควรที่ศาลเป็นผู้กำหนด ในกรณีที่ชนะคดีและสามารถบังคับใช้กฎหมายเพื่อลงโทษผู้ฝ่าฝืนได้เป็นผลสำเร็จ

จึงจะเห็นได้ว่านอกจาก FCRA จะมีบทบัญญัติให้เจ้าของข้อมูลสามารถฟ้องร้องคดีความรับผิดตาม FCRA ได้เองแล้วนั้น ในกรณีฝ่าฝืนบทบัญญัติของกฎหมายโดยจงใจนั้น ผู้เสียหายยังมีสิทธิได้รับค่าเสียหายเชิงลงโทษ (punitive damages) อีกด้วย และนอกจากนั้น FTC ยังมีอำนาจในการดำเนินคดีตาม FCRA และผู้ฝ่าฝืนยังอาจได้รับโทษตาม Federal Trade Commission Act (FTCA) อีกประการหนึ่ง โดยที่ FTC นั้นมีอำนาจในการดำเนินคดีทางแพ่งในศาลระดับมลรัฐ[43]

เมื่อวิเคราะห์ตามหลักกฎหมายของประเทศไทยแล้วนั้น

หากเกิดกรณีที่บริษัทข้อมูลเครดิตไม่กระทำการตามข้อ

---

[43] John B. Kennedy. "A PRIMER ON KEY INFORMATION SECURITY LAWS IN THE UNITED STATES" Practising Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series (June-July, 2008).

กำหนดของกฎหมายในเรื่องการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิตทั้งตามที่บัญญัติไว้ในพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต และประกาศคณะกรรมการคุ้มครองข้อมูลเครดิต รวมไปถึงแนวปฏิบัติที่ออกโดยคณะกรรมการนั้น บริษัทข้อมูลเครดิตจะเกิดความรับผิด คือ

1. ความรับผิดตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 ในมาตรา 47 กล่าวคือ ในกรณีที่บริษัทข้อมูลเครดิตไม่ปฏิบัติตามมาตรา 17 วรรคหนึ่ง หรือไม่ปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการกำหนดตามมาตรา 17 วรรคสอง ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทตลอดเวลาที่ยังมีการฝ่าฝืนอยู่หรือจนกว่าจะได้ปฏิบัติให้ถูกต้อง

อีกทั้งในมาตรา 62 ยังได้กำหนดไว้ว่าในกรณีที่ปรากฏว่ามีการกระทำความผิดอย่างใดอย่างหนึ่งตามพระราชบัญญัตินี้ ให้ถือว่าธนาคารแห่งประเทศไทยเป็นผู้เสียหายตามประมวลกฎหมายวิธีพิจารณาความอาญา และในคดีอาญานั้น ให้พนักงานอัยการมีอำนาจเรียกทรัพย์สิน หรือราคาหรือค่าสินไหมทดแทน เพื่อความเสียหายแทนเจ้าของข้อมูลหรือผู้เสียหายที่แท้จริงได้ ในการนี้ให้นำบทบัญญัติว่าด้วยการฟ้องคดีแพ่งที่เกี่ยวเนื่องกับคดีอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับโดยอนุโลม โดยที่บทบัญญัติตามมาตรา 62 นี้ไม่เป็นการตัดสิทธิเจ้าของข้อมูลหรือผู้เสียหายที่แท้จริงในการใช้สิทธิฟ้องร้องหรือดำเนินการใดๆ ตามกฎหมายต่อผู้กระทำความผิดนั้น

2. ในกรณีที่การกระทำดังกล่าวของบริษัทข้อมูลเครดิตส่งผลให้เกิดความเสียหายแก่เจ้าของข้อมูล บริษัทข้อมูลเครดิตนั้นจะเกิดความรับผิดตามประมวลกฎหมายแพ่งและพาณิชย์ ในเรื่องละเมิด ตามมาตรา 420 และมาตรา 422 อีกด้วย กล่าวคือเป็นการจงใจหรือประมาทเลินเล่อทำให้ผู้อื่นได้รับความเสียหาย และความเสียหายนี้เกิดจากการละเมิดกฎหมายที่มีวัตถุประสงค์เพื่อป้องกันสิทธิของบุคคลอื่น

จากข้างต้นจึงจะเห็นได้ว่า หากมีการฝ่าฝืนการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิต บริษัทข้อมูลเครดิตนั้นนอกจากจะมีความรับผิดตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต ซึ่งกำหนดโทษปรับไว้ตามมาตรา 47 โดยมี

ธนาคารแห่งประเทศไทยเป็นผู้เสียหายแล้วนั้น เจ้าของข้อมูลผู้ที่ได้รับความเสียหายจากเหตุดังกล่าวก็มีสิทธิที่จะฟ้องร้องคดีทางแพ่งกับบริษัทข้อมูลเครดิตในเรื่องละเมิดได้อีกด้วย ถึงแม้ว่าในคดีอาญาพนักงานอัยการจะมีอำ นาจเรียกทรัพย์สินหรือราคาหรือค่าสินไหมทดแทน เพื่อความเสียหายแทนเจ้าของข้อมูลหรือผู้เสียหายที่แท้จริงได้ก็ตาม แต่เนื่องจากพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต มาตรา 62 ได้บัญญัติไว้ว่าไม่เป็นการตัดสิทธิในการฟ้องร้องคดีของเจ้าของข้อมูล ดังนั้นในการดำ เนินการฟ้องร้องคดีทางแพ่งกับบริษัทข้อมูลเครดิตของเจ้าของข้อมูลนั้น การอ้างถึงการกระทำ ละเมิดโดยจงใจหรือประมาทเลินเล่อของบริษัทข้อมูลเครดิตซึ่งมีหน้าที่ตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต ในการที่จะต้องรักษาความลับและความปลอดภัยของข้อมูลนั้นย่อมสามารถเป็นเหตุในการฟ้องร้องคดีได้ โดยความเสียหายที่เจ้าของข้อมูลได้รับนั้นย่อมขึ้นอยู่กับข้อเท็จจริงตามสถานการณ์ที่เกิดขึ้นนั่นเอง

ในส่วนของการมาตรการตามกฎหมายในการเยียวยาความเสียหายที่เกิดขึ้นกับเจ้าของข้อมูลในกรณีของการฝ่าฝืนการรักษาความปลอดภัย และการคุ้มครองความลับของข้อมูลเครดิตนั้น ในพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ.2545 เองนั้นไม่ได้มีการกำ หนดไว้ เพียงแต่ให้สิทธิเจ้าของข้อมูลที่ฟ้องร้องคดีต่อบริษัทข้อมูลเครดิตตามประมวลกฎหมายแพ่งและพาณิชย์ต่อไป จึงเป็นความแตกต่างที่เห็นได้ชัดจาก The Fair Credit Reporting Act (FCRA) ของประเทศสหรัฐอเมริกา ซึ่งเป็นกฎหมายเฉพาะที่ใช้กับการประกอบธุรกิจข้อมูลเครดิตเช่นเดียวกับกฎหมายของไทย แต่ได้มีการบัญญัติอนุญาตให้เอกชนสามารถดำ เนินคดีในกรณีที่มีการฝ่าฝืนกฎหมายโดยจงใจหรือประมาทเลินเล่อได้ตาม section 616 และ 617 และยังมีการกำ หนดค่าเสียหายเชิงลงโทษ และค่าใช้จ่ายในการฟ้องร้องคดีและค่าทนายความไว้อีกด้วย และอีกประเด็นหนึ่งที่อาจเกิดเป็นปัญหาขึ้นได้ก็คือ มาตรการในทางปฏิบัติถ้าหากเกิดการละเมิดด้านความปลอดภัยของข้อมูลเครดิตเกิดขึ้นกล่าวคือถ้าหากเกิดเหตุการณ์ดังกล่าวบริษัทข้อมูลเครดิตจะเกิดหน้าที่ใดบ้าง และเจ้าของข้อมูลนั้นต้องดำ เนินการอย่างไรบ้างเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับตนได้ อาทิ การกำ หนดหน้าที่ในการแจ้งเตือนไปยังเจ้าของข้อมูลตามกฎหมายของประเทศ

สหรัฐอเมริกา เพื่อให้เจ้าของข้อมูลทราบถึงการละเมิดด้านความปลอดภัย รวมไปถึงให้คำแนะนำในการป้องกันความเสียหายที่อาจเกิดขึ้นได้จากการใช้ข้อมูลในลักษณะดังกล่าว เป็นต้น แม้ว่าเหตุการณ์ในลักษณะดังกล่าวนี้จะยังไม่เคยเกิดขึ้นในประเทศไทยก็ตาม แต่การศึกษาถึงแนวปฏิบัติในกรณีดังกล่าวของกฎหมายต่างประเทศย่อมมีประโยชน์ในการช่วยคุ้มครองเจ้าของข้อมูลเครดิตต่อไปได้ในอนาคต