รายงานฉบับสมบูรณ์ (Final Report)

โครงการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคล ภายใต้ประชาคมอาเซียน



เสนอต่อ

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

โดย

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

กันยายน ๒๕๕๘



รายนามคณะผู้ศึกษา

อาจารย์กิตติพงศ์ กมลธรรมวงศ์ หัวหน้าคณะผู้ศึกษา

อ.ดร.นคร เสรีรักษ์ ผู้ศึกษา

คุณยุคลธร เตชะวนากร ผู้ศึกษา

สารบัญ

หน้า

บทคัดย่อ

บทที่ 1 บทนำ **1**

1.1 ความเป็นมาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์โครงการ 2
1.3 เป้าหมายและขอบเขตของโครงการ 2
1.4 วิธีดำเนินการศึกษา 4
1.5 แผนการดำเนินการศึกษา 5
1.6 ประโยชน์ที่คาดว่าจะได้รับ 7

บทที่ 2 หลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและกรอบข้อตกลงระหว่างประเทศ **8**

2.1 หลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคล 10
2.2 การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) 14
2.3 การคุ้มครองข้อมูลส่วนบุคคลตามข้อบังคับสหภาพยุโรป (European Union Directive 95/46/EC) และข้อตกลงรัฐสภายุโรป 16
2.4 กรอบการคุ้มครองข้อมูลส่วนบุคคลตามของสหประชาชาติ (United Nations) 22
2.5 กรอบการคุ้มครองข้อมูลส่วนบุคคลของ APEC 24
2.6 รูปแบบการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ 29

บทที่ 3 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประชาคมอาเซียน **34**

3.1 ภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประชาคมอาเซียน 34
3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศอินโดนีเซีย 43
3.3 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศมาเลเซีย 46
3.4 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศฟิลิปปินส์ 51
3.5 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสิงคโปร์ 55

สารบัญ

หน้า

3.6 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย 59

3.6.1 พัฒนาการการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย 61

3.6.2 การคุ้มครองข้อมูลส่วนบุคคลใน พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. 2540 90

3.6.3 การคุ้มครองข้อมูลส่วนบุคคลในร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ..... ที่เสนอโดย สขร. 93

3.6.4 การคุ้มครองข้อมูลส่วนบุคคลในร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ..... ที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร 100

บทที่ 4 กรณีศึกษาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสิงคโปร์กับการนำมาปรับใช้ในประเทศไทย 112

4.1 ข้อมูลพื้นฐานเกี่ยวกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ 113

4.2 การเตรียมความพร้อมก่อนการบังคับใช้กฎหมายของสิงคโปร์ 115

4.3 การสร้างเครือข่ายความร่วมมือกับกลุ่มองค์กรทางการค้าและอุตสาหกรรม 117

4.4 การเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายไปยังประชาชนและองค์กรเอกชน 118

บทที่ 5 ข้อเสนอแนะในการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยและการเตรียมความพร้อมของ สขร. 121

5.1 ข้อเสนอแนะการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย 121

5.2 การเตรียมความพร้อมของ สขร. ในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล 126

บรรณานุกรม 132

ภาคผนวก

ก. ฐานข้อมูลกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มอาเซียนเพื่อใช้ในการเผยแพร่ของ สขร. 139

ข. กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนที่เป็นกรณีศึกษา 149

1. Law of The Republic of Indonesia Number 11 of 2008 Electronic Information and Transactions (Indonesia)
2. Personal Data Protection Act 2010 (Malaysia)
3. Data Privacy Act of 2012 (Philippines)
4. Personal Data Protection Act 2012 (Singapore)

บทคัดย่อ (Abstract)

ปัจจุบันในภูมิภาคอาเซียนประเทศที่ได้มีการตรากฎหมายที่ใช้คุ้มครองข้อมูลส่วนบุคคลแล้วมี 4 ประเทศ ซึ่งเป็นกรณีศึกษาในรายงานฉบับนี้ ได้แก่ อินโดนีเซีย มี Law No.11 of 2008 (EIT Law) กฎหมายว่าด้วยธุรกรรมและข้อมูลอิเล็กทรอนิกส์ ซึ่งไม่ใช่กฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลทุกประเภท แต่นอกจากกฎหมายฉบับนี้ก็ยังมีการคุ้มครองตามกฎหมายเฉพาะเรื่อง ได้แก่ Banking Law No.7 of 1992 และ The Capital Market Law No. 8 of 1995

มาเลเซีย เป็นประเทศแรกในอาเซียนที่ได้ประกาศใช้กฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลPersonal Data Protection Act 2010 (PDPA) ฟิลิปปินส์ คือ Data Privacy Act of 2012 (REPUBLIC ACT NO. 10173) มีความมุ่งหมายในการคุ้มครองข้อมูลส่วนบุคคลและการติดต่อสื่อสารในภาครัฐและภาคเอกชน ประเทศสุดท้ายคือสิงคโปร์มี Personal Data Protection Act 2012 (No. 26 of 2012) เพิ่งมีผลบังคับใช้อย่างสมบูรณ์เมื่อวันที่ 2 กรกฎาคม 2014

ประเทศอื่นๆแม้ยังไม่มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะแต่ก็มีกฎหมายที่มีบทบัญญัติคุ้มครองในบางเรื่อง ได้แก่ ประเทศไทยมีพ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่คุ้มครองข้อมูลส่วนบุคคลในภาครัฐ ประเทศเวียดนามในปีค.ศ.2010 ได้มีการประกาศใช้ Law 59 ที่ถือว่าเป็นการคุ้มครองข้อมูลของผู้บริโภค Consumer Rights Protection Law ซึ่งมีผลวันที่ 1 กรกฎาคม 2011 ในประเทศบรูไนมีการคุ้มครองในส่วนกฎหมายทรัพย์สินทางปัญญา เครื่องหมายการค้า กฎหมายลิขสิทธิ์ ในส่วนที่เป็นข้อมูลความลับทั่วไปก็ได้รับการคุ้มครองตามหลักกฎหมายCommon Law และหลัก Equity ขณะที่ประเทศในกลุ่มอาเซียนที่ยังไม่มีความคืบหน้าในการเตรียมการออกกฎหมาย คือ เมียร์มาร์ ลาว และกัมพูชา

สำหรับประเทศที่มีกฎหมายประกาศใช้แล้วได้กำหนดมาตรการที่สอดคล้องกับหลักการสากล เช่น หลักความยินยอม หลักการแจ้งวัตถุประสงค์ หลักความปลอดภัย โดยเฉพาะมาตรการเกี่ยวกับการส่งข้อมูลไปต่างประเทศ (transfer of data) ต่างมีการจำกัดประเภทของข้อมูลที่สามารถส่งต่อไปต่างประเทศ และกำหนดเงื่อนไขให้ต้องได้รับความยินยอมหรือให้มีหลักประกันว่าประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลไม่ด้อยไปกว่าประเทศตน

เมื่อศึกษาวิเคราะห์ถึงประสบการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน 4 ประเทศ เราอาจสรุปถึงมีลักษณะสำคัญที่ค้นพบ คือ1.การปฏิบัติตามมาตรฐานสากล (standardization)2.การคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาทางเศรษฐกิจ3.การยอมรับมาตรฐานสากล และกรอบความร่วมมือระหว่างประเทศ

คณะผู้ศึกษาเห็นว่าประเทศที่สามารถถือว่าเป็นตัวอย่างกรณีศึกษาที่ดีในการนำประสบการณ์มาเป็นบทเรียนในการเตรียมความพร้อมสำหรับการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในอนาคต คือ ประเทศสิงคโปร์ ด้วยเหตุที่มีการวางระบบกลไกการบังคับใช้กฎหมาย การเตรียมความพร้อมให้กับหน่วยงานเอกชนที่ต้องปฏิบัติตามกฎหมาย การให้ความรู้แก่ประชาชนเกี่ยวกับสิทธิที่ได้รับการคุ้มครองตามกฎหมายเป็นอย่างดี และการสร้างเครือข่ายร่วมมือกับกลุ่มองค์กรทางการค้าและอุตสาหกรรม โดยสำนักงาน PDPC

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550 ได้บัญญัติถึงสิทธิขั้นพื้นฐานประการหนึ่งของบุคคลเกี่ยวกับสิทธิในความเป็นส่วนตัวหรือสิทธิส่วนบุคคล (Privacy Right) ไว้ในมาตรา 35 ว่า “สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัวย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูล ส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ”

ฉะนั้นการคุ้มครองสิทธิพื้นฐานการดำเนินการเกี่ยวกับการคุ้มครองสิทธิความเป็นส่วนตัวในประเทศไทยจึงมีความจำเป็นต้องมีการตราพระราชบัญญัติออกมารองรับอีกชั้นหนึ่ง ซึ่งที่ผ่านมาคณะรัฐมนตรีมีมติเห็นชอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่คณะกรรมการกฤษฎีกาได้ตรวจพิจารณาแล้วตามที่สำนักงานปลัดสำนักนายกรัฐมนตรีเสนอ โดยอยู่ระหว่างการพิจารณาของสภาผู้แทนราษฎร และมีการแต่งตั้งคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แต่เนื่องจากได้มีการประกาศพระราชกฤษฎีกายุบสภาผู้แทนราษฎรเมื่อวันที่ 9 ธันวาคม 2556 ทำให้การพิจารณาร่างกฎหมายดังกล่าวต้องหยุดชะงักลง ส่งผลให้ขณะนี้ยังไม่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลใช้บังคับเป็นการทั่วไปทั้งๆที่เป็นกฎหมายสำคัญและเวลาก็ได้ล่วงเลยมาหลายปีแล้ว คงมีแต่การคุ้มครองข้อมูลส่วนบุคคลเฉพาะที่อยู่ในภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

นอกจากนี้หากพิจารณาบริบทในความสัมพันธ์ระหว่างประเทศ ประเทศไทยซึ่งเป็นสมาชิกอาเซียน ก็มีพันธกรณีในการสร้างประชาคมเศรษฐกิจอาเซียน (AEC) ตั้งแต่ปี พ.ศ. 2518 ให้มีความเชื่อมโยงกันระหว่างประเทศสมาชิกอาเซียนไม่ว่าจะเป็นด้านเทคโนโลยีสารสนเทศการเปิดเสรีและอำนวยความสะดวกทางการค้า การบริการ และการลงทุน พิธีการในการข้ามพรมแดน เป็นรากฐานที่เอื้อต่อกันในด้านเศรษฐกิจ การเมืองและความมั่นคง สังคมวัฒนธรรม

สำหรับประเทศสมาชิกอาเซียนที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว มีอยู่หลายประเทศเช่น มาเลเซีย (พ.ศ. 2533) ฟิลิปปินส์ (พ.ศ. 2554) สิงคโปร์ (พ.ศ. 2555) และอินโดนีเซีย (พ.ศ. 2555) ส่วนเวียดนามนั้นแม้ไม่มีกฎหมายนี้โดยตรง แต่ก็มีกฎหมายพาณิชย์อิเล็กทรอนิกส์ที่มีบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลอยู่

ดังนั้น เพื่อเป็นการเตรียมความพร้อมของประเทศไทยในการเข้าสู่ประชาคมเศรษฐกิจอาเซียน และเมื่อคำนึงถึงบทบาทภารกิจของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ (สขร.) ซึ่งเป็นหน่วยงานหลักในการดำเนินการเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นที่ควรต้องมีการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนต่างๆ ตลอดจนจะได้มีการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนเพื่อให้ประชาชนสามารถเข้าใจและปฏิบัติตามข้อปฏิบัติทางกฎหมายอย่างถูกต้อง อันจะเป็นเงื่อนไขสำคัญทางการค้าระหว่างประเทศเมื่อเข้าสู่การเป็นประชาคมเศรษฐกิจอาเซียนโดยสมบูรณ์ จึงเป็นที่มาของโครงการศึกษานี้

1.2 วัตถุประสงค์โครงการ

1) เพื่อศึกษาวิเคราะห์การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายของประเทศสมาชิกอาเซียน บางประเทศ เช่น มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์

2) เพื่อศึกษาจัดทำข้อเสนอเพื่อใช้เป็นแนวทางในการพัฒนากฎหมายข้อมูลส่วนบุคคลของประเทศไทย

3) เพื่อศึกษาการบังคับใช้กฎหมายข้อมูลส่วนบุคคลตามกฎหมายของประเทศสมาชิกอาเซียนบางประเทศ เช่น มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์

4) เพื่อศึกษาวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนบางประเทศ ได้แก่ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์ และเปรียบเทียบกับร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่หน่วยราชการไทยและคณะบุคคลต่างๆเคยเสนอให้พิจารณา รวมกับทั้งที่มีระบุไว้ใน พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540 เพื่อใช้เป็นแนวทางในการปรับใช้กับประเทศไทย และใช้เป็นข้อมูลสำหรับหน่วยงานที่จะได้รับมอบหมายให้รับผิดชอบงานคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายต่อไป

5) เพื่อจัดทำฐานข้อมูลเพื่อบันทึกรายละเอียดกฎหมายข้อมูลส่วนบุคคลและวิธีการบังคับใช้กฎหมายข้อมูลส่วนบุคคลของประเทศสมาชิกที่กล่าวถึงในข้อ3) ไว้ในฐานข้อมูลของ สขร. เพื่อให้ประชาชนคนไทยผู้สนใจเข้ามาศึกษาและนำไปใช้งานได้

1.3 เป้าหมายและขอบเขตของโครงการ

การศึกษาตามโครงการนี้มีเป้าหมายสำคัญในการวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนบางประเทศ ได้แก่ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์ เพื่อใช้เป็นแนวทางในการปรับใช้กับประเทศไทย และใช้เป็นข้อมูลสำหรับหน่วยงานที่จะได้รับ

มอบหมายให้รับผิดชอบงานคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายต่อไป ซึ่งมีขอบเขตการดำเนินงานแบ่งเป็นสองส่วน คือ

1.3.1 ขอบเขตด้านเนื้อหา

การวิเคราะห์ข้อมูลด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนที่มีการประกาศใช้ ได้แก่ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์ โดยมีประเด็นการศึกษาในด้านต่างๆ ดังนี้

1) การศึกษาถึงรูปแบบของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ในแต่ละประเทศ

2) การวิเคราะห์กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อนำจุดเด่นมาเป็นแนวทางในการนำมาปรับใช้กับประเทศไทย

3) การศึกษาจัดทำแนวทางการเผยแพร่กฎหมาย/หลักการคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนให้ประชาชนไทยเพื่อเตรียมพร้อมการเข้าสู่ประชาคมอาเซียน

4) การศึกษาเปรียบเทียบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนและร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยที่มีทั้งหมด ที่หน่วยราชการไทยและคณะบุคคลต่างๆเคยเสนอให้ทางการพิจารณา รวมทั้งกับที่มีระบุใน พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และกฎหมายอื่นๆที่เกี่ยวข้อง เพื่อให้ทราบถึงพัฒนาการของการจัดทำร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5) การจัดทำฐานข้อมูลกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิกอาเซียน ไว้ในระบบคอมพิวเตอร์ของ สขร. เพื่อเป็นฐานข้อมูลให้ นิสิต นักศึกษา ประชาชนเข้าสืบค้น

6) ทำการวิเคราะห์ผลข้อมูล เปรียบเทียบข้อดีข้อเสีย การบังคับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนที่ทำการศึกษา อันได้แก่ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์

7) นำเสนอข้อเสนอแนะมาตรการและแนวทางปฏิบัติให้แก่ สขร. ในการผลักดันการพัฒนากฎหมายและข้อเสนอแนะในการบังคับใช้กฎหมายที่เหมาะสมสำหรับประเทศไทย เพื่อนำเสนอ กขร. ในการกำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

1.3.2 ขอบเขตด้านพื้นที่

1) ศึกษาแนวคิด วิธีการปฏิบัติ รวมถึงปัญหาอุปสรรค เพื่อการเปรียบเทียบ จากหน่วยงาน/องค์กรในประเทศสมาชิกอาเซียนจำนวน 4 ประเทศ อันได้แก่ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์

2) การจัดสัมมนาเพื่อรับฟังข้อเสนอแนะข้อคิดเห็นจากองค์กรธุรกิจ เอกชน หน่วยงานที่เกี่ยวข้อง เพื่อนำข้อเสนอแนะที่ได้รับจากการสัมมนา พร้อมข้อสังเกต ที่มีต่อร่างรายงานการศึกษาฉบับสมบูรณ์มาปรับปรุงเป็นรายงานการศึกษาฉบับสมบูรณ์

1.4 วิธีดำเนินการศึกษา

ในการศึกษาวิจัยตามโครงการ ทางคณะผู้ศึกษาได้ออกแบบวิธีการศึกษาโดยอาศัยเครื่องมือทางวิจัยที่มีการผสมผสาน ดังต่อไปนี้

1) การศึกษาข้อมูลด้านเอกสาร

ในที่นี้จะได้ทำการศึกษาเอกสารทางวิชาการต่างๆ ได้แก่ กฎหมายข้อมูลข่าวสารของราชการในกลุ่มประเทศสมาชิกอาเซียนจำนวน 4 ประเทศที่เป็นกลุ่มตัวอย่าง ได้แก่ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์ โดยครอบคลุมมาตรการทางกฎหมาย มาตรการทางบริหารและการกำหนดนโยบาย เอกสารราชการ และเอกสารในการปฏิบัติงานของหน่วยงานและองค์กรต่างๆ ที่รับผิดชอบการดำเนินงานในประเทศนั้นๆ ทำการสำรวจสถานะปัจจุบันของการคุ้มครองข้อมูลส่วนบุคคลของประเทศอาเซียนเปรียบเทียบกับประเทศไทย ศึกษาสภาพข้อเท็จจริงในการออกกฎหมาย การบังคับใช้กฎหมาย และผลดีผลเสียของการดำเนินการตามกฎหมาย

2) การศึกษาข้อมูลจากภาคสนาม

ในที่นี้จะได้ทำศึกษาการปฏิบัติและประสบการณ์จากหน่วยงานและองค์กรทั้งภายในและต่างประเทศ ที่เป็นกลุ่มตัวอย่างในการศึกษาโดยการจัดประชุมกลุ่มย่อย และการสัมภาษณ์ผู้ที่เกี่ยวข้อง เพื่อเก็บรวบรวมข้อมูลประกอบการศึกษา และเพื่อระดมความคิดเห็นและรับทราบปัญหา ตลอดจนข้อคิดเห็นและข้อแนะนำต่างๆ จาก ผู้บริหารภาครัฐ เอกชน นักวิชาการ นักธุรกิจ องค์กรพัฒนาภาคเอกชน ฯลฯ

ทั้งนี้ทางคณะผู้วิจัยได้เดินทางพร้อมคณะเจ้าหน้าที่ของ สขร. ไปศึกษาดูงานการคุ้มครองข้อมูลส่วนบุคคล ณ ประเทศสิงคโปร์ ระหว่างวันที่ 25-27 กันยายน 2557 โดยได้เข้าพบปะแลกเปลี่ยนความคิดเห็นในการบังคับใช้กฎหมายข้อมูลส่วนบุคคลกับภาคธุรกิจที่เป็นบริษัทต่างชาติที่มีสำนักงานตั้งอยู่ที่สิงคโปร์ได้แก่ Google และMicrosoft ตลอดจนได้ศึกษาดูงานยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission)พร้อมรับฟังบรรยายสรุปกฎหมายข้อมูลส่วนบุคคลของสิงคโปร์และผลการบังคับใช้ที่ผ่านมา

3) การประชุมรับฟังความคิดเห็นต่อผลการศึกษา

ภายหลังจากการศึกษาเสร็จสิ้นและจัดทำเป็นร่างรายงานผลการศึกษาแล้ว จะได้จัดให้มีการประชุมรับฟังความคิดเห็นระหว่างบุคคลที่เกี่ยวข้องฝ่ายต่างๆ ต่อผลการศึกษา เพื่อนำข้อเสนอแนะต่างๆ มาใช้ในการปรับปรุงแก้ไข และจัดทำรายงานผลการศึกษาฉบับสมบูรณ์ โดยมีกลุ่มเป้าหมายในการเข้าร่วมสัมมนาได้แก่ ตัวแทนหน่วยราชการที่เกี่ยวข้อง กรรมการข้อมูลข่าวสาร

ของราชการ กรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารของราชการ ตัวแทนหน่วยงานองค์กรภาคเอกชน นักวิชาการภายนอก และประชาชนทั่วไปผู้สนใจ

ทั้งนี้ในการศึกษาตามโครงการเพื่อให้เกิดประโยชน์สูงสุดแก่สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ คณะผู้ศึกษาจะได้ปฏิบัติงานร่วมกันระหว่างที่ปรึกษา โดยมีเจ้าหน้าที่ของ สขร. เป็นผู้ปฏิบัติงานสนับสนุน (Counterpart) เพื่อการแลกเปลี่ยนเรียนรู้และเป็นการเรียนรู้ระหว่างการปฏิบัติ (On the job training) เป็นการพัฒนาขีดความสามารถในการปฏิบัติงาน (Capacity building) ในประสบการณ์การวิจัย

ในส่วนการศึกษาจะเน้นการวิเคราะห์ข้อมูลเชิงเปรียบเทียบ และจัดทำข้อเสนอมาตรการและแนวทางให้แก่ สขร. ในการผลักดันการพัฒนากฎหมายและข้อเสนอแนะในการบังคับใช้กฎหมายที่เหมาะสมสำหรับประเทศไทย เพื่อนำเสนอ กขร. ในการกำหนดนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล

1.5 แผนการดำเนินการศึกษา

ในการดำเนินงานศึกษาตามโครงการมีแผนการดำเนินงานที่กำหนดไว้ตามตาราง ดังนี้

การดำเนินงาน / ระยะเวลา (เดือนที่)	1	2	3	4	5	6
1. การรวบรวมข้อมูลเอกสารต่าง ๆที่เกี่ยวข้องกับการศึกษาวิจัย	━	━	━	━	━	
2. การศึกษาเรียบเรียงเพื่อจัดทำรายงานความก้าวหน้า/วิธีการเก็บข้อมูล/ แนวทางการทำงาน (Inception Report)	▬					
3. จัดประชุมกลุ่มย่อย(การประชุม/เจรจา/กรอบความร่วมมือเวที ASEAN)		▬				
4. การศึกษาวิเคราะห์ข้อมูลและจัดทำร่างรายงานผลการดำเนินการ		▬				
5. การจัดเก็บข้อมูลภาคสนาม การสัมภาษณ์ และจัดประชุมกลุ่มย่อย		━	━	━	━	
5.1 การจัดเก็บข้อมูลที่อินโดนีเซีย และ/หรือสิงคโปร์		▬				
5.2 การศึกษาวิเคราะห์ข้อมูลและจัดทำร่างรายงานผลการดำเนินการ			▬			
6. จัดประชุมกลุ่มย่อย/เสวนา/ระดมความเห็น(ความเหมาะสมภาพรวม)			▬			
7. การศึกษาวิเคราะห์ข้อมูลและจัดทำร่างรายงานผลการดำเนินการ				▬		
8. การเก็บ/ศึกษา/วิเคราะห์ข้อมูล/ปรับปรุง-ส่งร่างรายงาน Draft Report				▬	▬	
9. การประชุมรับฟังความคิดเห็นร่างรายงานผลการศึกษา					▬	
10. นำข้อเสนอจากการสัมมนารับฟังความคิดเห็นมาปรับปรุงไขร่างรายงาน						▬
11. ส่งรายงานฉบับสมบูรณ์-Final Report						▬

การดำเนินงานศึกษาตามโครงการนี้ ในแต่ละขั้นตอนคณะผู้ศึกษาได้ให้ความสำคัญของการดำเนินงานร่วมกันระหว่างที่ปรึกษาและเจ้าหน้าที่สนับสนุน (Counterpart) เนื่องจากพิจารณาเห็นว่า การเตรียมความพร้อมของประเทศไทยในการเข้าสู่ประชาคมเศรษฐกิจอาเซียน สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ (สขร.) นับเป็นหน่วยงานหลักในการดำเนินการเกี่ยวกับ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงมีความจำเป็นที่ควรต้องมีการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนต่างๆ ตลอดจนจะได้มีการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียนเพื่อให้ประชาชนสามารถเข้าใจและปฏิบัติตามข้อปฏิบัติทางกฎหมายอย่างถูกต้อง อันจะเป็นเงื่อนไขสำคัญทางด้านความสัมพันธ์ระหว่างประเทศเมื่อเข้าสู่การเป็นประชาคมเศรษฐกิจอาเซียนโดยสมบูรณ์

ดังนั้นการพัฒนาขีดความสามารถบุคลากรของ สขร. ทั้งในด้านความรู้และทักษะการวิเคราะห์เพื่อจัดทำข้อเสนอเชิงนโยบาย จึงเป็นเรื่องจำเป็น เพราะจะเป็นเครื่องมือสำคัญที่จะนำไปสู่การกำหนดนโยบายและมาตรการในการขับเคลื่อนภารกิจของ กขร. และ สขร. ให้บรรลุวัตถุประสงค์อย่างมีประสิทธิภาพ

การบรรลุวัตถุประสงค์ดังกล่าวคณะผู้ศึกษาจึงได้วางแนวทางการดำเนินงานตามโครงการโดยเป็นการปฏิบัติงานร่วมกันระหว่างที่ปรึกษา โดยมีเจ้าหน้าที่ของ สขร. เป็นผู้ปฏิบัติงานสนับสนุน (Counterpart) เพื่อการแลกเปลี่ยนเรียนรู้และเป็นการเรียนรู้ระหว่างการปฏิบัติ (On the job training) เป็นการพัฒนาขีดความสามารถในการปฏิบัติงาน (Capacity building) ด้านวิชาการและการค้นคว้าวิจัย โดยเฉพาะการพัฒนาความสามารถในการปฏิบัติงานที่เกี่ยวข้องกับการประชุมนานาชาติ โดยเจ้าหน้าที่ผู้ปฏิบัติงานสนับสนุน (Counterpart) จะมีบทบาทและหน้าที่ในการดำเนินงานตามโครงการดังนี้

1. ร่วมประชุมหารือกับที่ปรึกษาโครงการ และนักวิจัยในโครงการ ในการกำหนดกรอบวิธีการทำงานตามโครงการ

2. ร่วมการประชุมสัมมนาที่จะเกิดขึ้นตามโครงการ ได้แก่ การจัดสัมมนาให้ความรู้โดยวิทยากรผู้เชี่ยวชาญจากหน่วยงาน/องค์กรทั้งภายในและต่างประเทศที่ดำเนินงานด้านคุ้มครองข้อมูลส่วนบุคคล ประเทศสมาชิกASEAN และการสัมมนาเพื่อรับฟังความคิดเห็น/ข้อเสนอแนะจากหน่วยงานที่เกี่ยวข้อง

3. ร่วมกับที่ปรึกษาและนักวิจัย ในการเก็บรวบรวมข้อมูล และการติดต่อสัมภาษณ์แหล่งข้อมูลต่างๆ ทั้งข้อมูลเอกสารทางวิชาการ กฎหมาย มาตรการทางกฎหมาย มาตรการทางบริหารและการกำหนดนโยบาย เอกสารราชการ และเอกสารในการปฏิบัติงานของหน่วยงานและองค์กรต่างๆทั้งภายในและต่างประเทศ และสนับสนุนการประสานงานกับหน่วยงานต่างๆ เพื่อขอเอกสารมาใช้ในการศึกษา การพัฒนาฐานข้อมูลเพื่อการเรียนรู้ และการสนับสนุนการติดต่อประสานงานกับหน่วยงานทั้งภาครัฐและเอกชน ทั้งในและต่างประเทศ

4. ร่วมปรึกษาหารือกับที่ปรึกษาในการวิเคราะห์ โดยเฉพาะการเน้นการจัดทำข้อเสนอมาตรการและแนวทางให้แก่ สขร. ในการพิจารณาการเข้าร่วมหรือทำความตกลงตามกรอบความตกลงใน ASEAN หรือข้อตกลงอื่นๆในระดับสากลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนทิศทางการพัฒนา สขร. ในอนาคต

1.7 ประโยชน์ที่คาดว่าจะได้รับ

การศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียนในโครงการศึกษาวิจัยนี้ จะได้มาซึ่งผลการศึกษาวิเคราะห์และข้อมูลอื่นๆที่เป็นประโยชน์ ใช้ในการเผยแพร่แก่ประชาชนทั่วไปและใช้เป็นข้อมูลสนับสนุนเพื่อให้คณะกรรมการข้อมูลข่าวสารของราชการสามารถนำไปใช้ในการตัดสินใจกำหนดนโยบายการคุ้มครองข้อมูลส่วนบุคคล และการจัดทำแผนพัฒนาการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในอนาคตที่มีความเหมาะสม สอดคล้องกับหลักการสากลและมีประสิทธิภาพ

บทที่ 2
หลักการพื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและกรอบข้อตกลงระหว่างประเทศ

การคุ้มครองข้อมูลข่าวสารส่วนบุคคลนั้น หากพิจารณาถึงพัฒนาการทางความคิด ก็จะพบว่าได้เติบโตและก้าวหน้า จนได้รับการยอมรับและกลายเป็นหลักกฎหมายสากลซึ่งใช้บังคับกันในระหว่างประเทศ มานานแล้ว บทบัญญัติในกฎหมายระหว่างประเทศที่กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลที่เป็นแม่บทหลักในทางระหว่างประเทศปัจจุบัน นั้นอาจกล่าวได้ว่ามีที่มาสำคัญจาก **ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนของสหประชาชาติ** ที่ได้ประกาศเมื่อวันที่ 10 ธันวาคม ค.ศ.1948 ซึ่งได้กล่าวรับรองไว้ในมาตรา 12 ว่า “บุคคลใดๆจะถูกสอดแทรกโดยพลการในชีวิตส่วนบุคคลในครอบครัว ในเคหสถานหรือในการสื่อสาร หรือจะถูกลบลู่ในเกียรติยศและชื่อเสียงมิได้ ทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายต่อการแทรกสอดหรือการลบหลู่ดังกล่าวนั้น”[1]

สิทธิมนุษยชนขั้นพื้นฐานในปฏิญาณสากลฉบับนี้มีความหมายกว้างขวางครอบคลุมถึงสิทธิอื่นๆ ไม่ว่าจะเป็น ความเป็นส่วนตัวในข้อมูลข่าวสารส่วนบุคคล (Information Privacy) ความเป็นส่วนตัวในอาณาเขตหรือสถานที่ของตนเอง (Territorial Privacy) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)[2] ซึ่งความเป็นส่วนตัวเหล่านี้ได้กลายเป็นหลักการพื้นฐานที่ได้รับการยอมรับกันทั่วไป ทั้งนี้จะขอหยิบยกเนื้อหาของความเป็นส่วนตัวดังกล่าวมาอธิบายดังนี้

(1) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)

เป็นการให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้ ทั้งนี้บทบัญญัติที่สะท้อนการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารในกฎหมายไทยปรากฏเห็นได้ในกฎหมายหลายฉบับ

(2) ความเป็นส่วนตัวในดินแดนหรืออาณาเขต (Territorial Privacy)

เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้ ทั้งนี้ รวมทั้งการติดกล้องวีดิโอ และการตรวจสอบรหัสประจำตัวบุคคล (ID Checks)

---

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

[2] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, **โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ,** พิมพ์ครั้งที่ 3, (กรุงเทพมหานคร: เดือนตุลา, 2544), หน้า 88.

(3) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy)

เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม หรือการทดลองยา

(4) ความเป็นส่วนตัวเกี่ยวกับข้อมูลข่าวสาร (Information Privacy)

เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล หรือเป็นที่รู้จักกันภายใต้คำว่า “Data Protection”

จากแนวทางของปฏิญญาสากลว่าด้วยสิทธิมนุษยชนของสหประชาชาตินี้ ก็กลายเป็นแนวคิดที่ได้รับการนำไปบัญญัติในลักษณะทำนองเดียวกันในทางกฎหมายระหว่างประเทศต่อๆ มา ได้แก่

กติการะหว่างประเทศว่าด้วยสิทธิพลเมือง ข้อ 17 ซึ่งกำหนดว่า “บุคคลจะถูกแทรกแซงความเป็นส่วนตัว ครอบครัว เคหสถาน หรือการติดต่อสื่อสารโดยพลการ หรือโดยมิชอบด้วยกฎหมายมิได้ และจะถูกลบหลู่เกียรติและชื่อเสียงโดยมิชอบด้วยกฎหมายมิได้

บุคคลทุกคนมีสิทธิที่จะได้รับความคุ้มครองตามกฎหมายมิให้ถูกแทรกแซง หรือลบหลู่เช่นว่านั้น”[3]

อนุสัญญาว่าด้วยสิทธิเด็กของสหประชาชาติ ข้อ 16 กำหนดว่า “เด็กจะไม่ถูกแทรกแซงโดยพลการหรือโดยไม่ชอบด้วยกฎหมายในความเป็นส่วนตัว ครอบครัว บ้าน หรือหนังสือโต้ตอบ รวมทั้งจะไม่ถูกกระทำการโดยไม่ชอบด้วยกฎหมายต่อเกียรติและชื่อเสียง

เด็กมีสิทธิได้รับความคุ้มครองจากการแทรกแซงหรือการกระทำดังกล่าว”[4]

อนุสัญญาแห่งชาติยุโรป ว่าด้วยสิทธิมนุษยชน ข้อ 8 กำหนดว่า “บุคคลทุกคนมีสิทธิที่จะได้รับความเคารพในชีวิตความเป็นส่วนตัว และชีวิตครอบครัว บ้าน และการติดต่อสื่อสาร”

ทั้งนี้คณะกรรมการสิทธิมนุษยชนแห่งยุโรป ได้ให้ความหมาย ของชีวิตความเป็นส่วนตัว ว่ามีลักษณะเช่นเดียวกับมาตรา 2 (1) ของรัฐธรรมนูญเยอรมัน คือการกำหนดบุคลิกภาพของตนเองโดยอิสระ (Free determination of personality)

จากปฏิญญาสากลว่าด้วยสิทธิมนุษยชนของสหประชาชาตินี้ก็ ได้นำไปสู่การวางแนวทางข้อตกลงระหว่างประเทศที่สำคัญอื่นๆเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลเพิ่มเติม ที่ได้ยอมรับกันเป็นมาตรฐานสากล ฉะนั้นในเบื้องต้นจึงมีความจำเป็นที่ต้องศึกษาถึงหลักเกณฑ์ดังกล่าวเพื่อนำมาประกอบการศึกษาวิเคราะห์และตรวจสอบถึงบทบัญญัติของกฎหมายไทยว่าได้มีวางมาตรฐานไว้เพียงพอหรือไม่ ในฐานะที่ประเทศไทยเป็นส่วนหนึ่งของประชาคมโลกจึงจำเป็นต้องเคารพหลักเกณฑ์ดังกล่าวและนำมาใช้ปฏิบัติภายในประเทศเพื่อให้เกิดการยอมรับในนานาอารยะประเทศ และสร้างมาตรฐานที่จะเป็นหลักประกันในการคุ้มครองสิทธิเสรีภาพของบุคคลที่ครบถ้วน

---

[3] กุลพล พลวัน, **พัฒนาการแห่งสิทธิมนุษยชน,** พิมพ์ครั้งที่ 3, (กรุงเทพมหานคร: วิญญูชน, 2538), น. 210.

[4] **เรื่องเดียวกัน**, น. 241.

สมบูรณ์ ทั้งนี้หลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคลและข้อตกลงระหว่างประเทศที่สำคัญ มีดังต่อไปนี้

2.1 หลักการพื้นฐานในการคุ้มครองข้อมูลส่วนบุคคล

"ข้อมูลข่าวสารส่วนบุคคล" (Personal Information) นับว่าเป็นคำที่มีความหมายกว้าง และยังมีความเห็นที่หลากหลายที่โต้แย้งกันอยู่ว่าอะไรบ้างคือข้อมูลข่าวสารส่วนบุคคล ซึ่งกฎหมายของแต่ละประเทศก็ได้มีการบัญญัติให้คำนิยามที่แตกต่างกันไป ซึ่งจะขอยกตัวอย่างนิยามของข้อมูลข่าวสารส่วนบุคคลที่ปรากฏในกฎหมายบางประเทศที่น่าสนใจ ดังนี้

1. ความหมายตาม EU Directive "ข้อมูลส่วนบุคคล (Personal Information)" หมายถึง "ข้อความ (Information) ใดๆ ที่เกี่ยวกับบุคคลธรรมดา (Natural Person) อันระบุตัว (Identified) หรืออาจระบุตัว (Identifiable) บุคคลนั้นได้ ซึ่งบุคคลที่อาจถูกระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อมนี้อาจทำได้โดยการอ้างอิงจากหมายเลขเฉพาะของบุคคล (Identification Number) หรือจากปัจจัยอื่น ๆ ที่มีลักษณะเฉพาะในทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสังคมของบุคคลนั้นเป็นต้น" [5]

2. ความหมายตามแนวทางของ OECD "ข้อมูลส่วนบุคคล" หมายความว่า "ข้อความ (Information) ใด ๆ อันระบุตัว (Identified) หรืออาจระบุตัว (Identifiable) บุคคล (Individual) ได้"[6]

3. ความหมายในสหราชอาณาจักร ตามพระราชบัญญัติคุ้มครองข้อมูลข่าวสาร 1998 (Data Protection Act) ได้ให้ความหมายของข้อมูลส่วนบุคคล (Personal Data) หมายความว่า ข้อมูลเกี่ยวกับความเป็นอยู่ของบุคคลซึ่งสามารถระบุตัวบุคคลได้จากข้อมูลนั้นเอง หรือจากข้อมูลหรือจากข่าวสารจากการควบคุมของผู้ควบคุมข้อมูล (data controller) และรวมถึงการแสดงความคิดเห็นคำบอกเล่าใดๆที่เกี่ยวกับบุคคลที่บุคคลอื่นหรือบุคคลที่ 3ได้กล่าวถึงเจ้าของข้อมูล[7]

---

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

[6]Personal Data means any information relating to an identified or identifiable individual (data subject)

[7]Personal data means data which relate to a living individual who can be identified

(a) from those data or

(b) from those data and other information which is in the possession of , the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

4. ความหมายในฝรั่งเศส “ข้อมูลที่ระบุชื่อ” หมายถึง ข้อมูลต่างๆซึ่งแสดงถึงลักษณะประจำตัวของบุคคลธรรมดาที่เกี่ยวข้องกับข้อมูลนั้นๆ ไม่ว่าโดยทางตรงหรือทางอ้อม ไม่ว่าจะได้กระทำในรูปแบบใด และไม่ว่าระบบข้อมูลจะได้จัดทำขึ้นโดยบุคคลธรรมดาหรือนิติบุคคล

5. ความหมายในแคนาดา “ข้อมูลข่าวสารส่วนบุคคล” หมายถึง ข้อมูลข่าวสาร หรือความคิดเห็น (รวมถึงข้อมูลข่าวสารหรือความคิดเห็นที่อยู่ในรูปแบบของฐานข้อมูล) ไม่ว่าจะเป็นจริงหรือเท็จ และไม่ว่าจะถูกบันทึกไว้หรือไม่

6. ความหมายในสหพันธรัฐเยอรมัน **“**ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลข่าวสารใดๆ เกี่ยวกับบุคคลหรือข้อความแวดล้อมใดๆที่บ่งชี้หรือสามารถชี้เฉพาะถึงตัวบุคคล (บุคคลผู้เป็นเจ้าของข้อมูลข่าวสาร)ได้

7. ความหมายในสหรัฐอเมริกา ใน Privacy Act 1974 ได้ให้ความหมายของบันทึกข้อมูลส่วนบุคคล ว่าหมายถึง การบันทึกใดๆ การจัดเก็บรวบรวม หรือการจัดกลุ่มข้อมูลเกี่ยวกับบุคคล ซึ่งเก็บรักษาไว้โดยหน่วยงานรัฐบาลกลาง โดยรวมถึง ข้อมูลเกี่ยวกับการศึกษา ข้อมูลเกี่ยวกับธุรกรรมทางการเงิน ประวัติการแพทย์ และประวัติอาชญากรรม หรือประวัติการทำงาน และข้อมูลนั้นได้ระบุชื่อหรือหมายเลขประจำตัว สัญลักษณ์ หรือรหัสบ่งชี้อื่นๆซึ่งสามารถแสดงได้ว่าหมายถึงบุคคลใด เช่น ลายนิ้วมือ หรือแผ่นบันทึกเสียง หรือภาพถ่าย

8. ความหมายในญี่ปุ่น ในกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคล (Act on The Protection of Personal Information 2003) “ข้อมูลส่วนบุคคล” (Personal Information - Kojin Joho) หมายถึงบรรดาข้อมูลข่าวสารเกี่ยวกับบุคคลธรรมดาที่อาจใช้ในการระบุบ่งตัวบุคคลได้ เช่น ชื่อ วันเดือนปีเกิดหรือข้อมูลข่าวสารใดๆ ซึ่งอาจนำไปเปรียบเทียบหรือประกอบกับข้อมูลข่าวสารอื่นเพื่อใช้ในการระบุตัวบุคคลได้ ทั้งนี้ในกฎหมายฉบับเดียวกันได้ให้ความหมายของข้อมูลบุคคล (Personal Data) หมายถึง ข้อมูลส่วนบุคคลซึ่งได้รับการจัดระบบในลักษณะที่เป็นฐานข้อมูลส่วนบุคคล คืออาจเรียกดูข้อมูลส่วนบุคคลโดยเจาะจงได้โดยวิธีอัตโนมัติหรือวิธีอื่นใดตามที่กฎหมายลำดับรองกำหนด

จากความหมายของข้อมูลข่าวสารส่วนบุคคล ที่ได้นำเสนอข้างต้น เราอาจสรุปถึงการแบ่งการให้ความหมายของข้อมูลข่าวสารส่วนบุคคลได้ออกเป็น สองประเภทใหญ่ ได้แก่

1) <u>การให้ความหมายข้อมูลข่าวสารส่วนบุคคลในความหมายกว้าง</u> ในกรณีเป็นการบัญญัติตามแนวทางของ EU Directive 95/46/EC ซึ่งได้แก่ประเทศสมาชิก EU และประเทศที่ไม่ได้เป็นสมาชิกแต่ต้องการมีกฎหมายที่ได้มาตรฐานทัดเทียมกันในระดับสากล เช่น อังกฤษ ฝรั่งเศส ออสเตรเลีย เป็นต้น

2) <u>การให้ความหมายข้อมูลข่าวสารส่วนบุคคลในความหมายแคบ</u> ในกรณีนี้มักจะพบในประเทศที่ไม่ได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลไว้ในลักษณะที่เป็นกฎหมายกลาง แต่จะมีการตราบทบัญญัติเฉพาะขึ้นเป็นเรื่องๆ ซึ่งได้แก่ประเทศสหรัฐอเมริกา

ข้อมูลข่าวสารส่วนบุคคลโดยทั่วไปสามารถแบ่งได้ เป็น 2 ลักษณะ คือ ข้อมูลข่าวสารทั่วไป (Non- Sensitive data) และข้อมูลข่าวสารประเภทที่มีความละเอียดอ่อน (Sensitive Information) ซึ่งลักษณะของข้อมูลทั้งสองประเภทมีความแตกต่างกันดังนี้ [8]

1. ข้อมูลข่าวสารทั่วไป (Non- Sensitive data) เป็นข้อมูลข่าวสารใดๆที่เกี่ยวข้องกับบุคคล ซึ่งสามารถบ่งชี้เฉพาะตัวบุคคล ได้แก่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อายุ วุฒิการศึกษา ตำแหน่งหน้าที่การงาน สถานะและลักษณะทางกายภาพของบุคคล ข้อมูลใดๆดังกล่าวสามารถนำมาประมวลกันเป็นข้อเท็จจริงที่บ่งชี้ลักษณะเฉพาะตัวบุคคลได้ โดยสภาพของข้อมูลเหล่านี้เป็นข้อมูลข่าวสารที่สามารถเปิดเผยต่อสาธารณะได้เป็นเรื่องปรกติธรรมดา

2. ข้อมูลข่าวสารประเภทที่มีความละเอียดอ่อน (Sensitive Information) ได้แก่ข้อมูลข่าวสารที่ถือว่าเป็นเรื่องเฉพาะตัว (Intimate) ของบุคคลโดยเฉพาะ เป็นข้อมูลที่เป็นความลับหรือไม่พึงประสงค์ที่จะให้มีการเปิดเผย ข้อมูลประเภทนี้ได้แก่ การนับถือลัทธิความเชื่อทางศาสนา ปรัชญาชีวิต การดำเนินชีวิตส่วนตัว ลัทธิทางการเมือง เพศสัมพันธ์ ข้อมูลสุขภาพ ข้อมูลที่เกี่ยวกับการดำเนินคดีทางอาญา เช่น คำพิพากษาในคดีอาญา มาตรการในการดำเนินการทางอาญา หรือการกระทำของฝ่ายปกครองที่เป็นการจำกัดเสรีภาพ เป็นต้น

โดยการให้นิยามถึงความหมายของข้อมูลข่าวสารส่วนบุคคลในทางอย่างกว้างนั้นจะครอบคลุมข้อมูลทั้งสองลักษณะข้างต้น ขณะที่การให้ความหมายอย่างแคบจะจำกัดเฉพาะข้อมูลประการหลังเท่านั้น ซึ่งส่วนใหญ่การให้ความคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่ได้รับการยอมรับกันทั่วไปนั้นหลายประเทศจะยึดถือการให้ความหมายอย่างกว้างที่จะช่วยในการคุ้มครองสิทธิเสรีภาพและข้อมูลข่าวสารส่วนบุคคลได้อย่างกว้างขวางและครบถ้วนมากกว่า

อนึ่งก็มีข้อสังเกตที่น่าตั้งคำถามว่า “การเปิดเผยโดยปรกติของข้อมูลส่วนบุคคลที่เป็นข้อมูลทั่วไปต่อสาธารณะนั้นสามารถทำได้ทุกกรณีหรือไม่ ? “ในความเห็นของผู้ศึกษามีทัศนะว่าการเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่ถือว่าเป็นข้อมูลข่าวสารทั่วไป ซึ่งตามหลักการแล้วสามารถเปิดเผยต่อสาธารณะได้นั้น ก็มีข้อพิจารณาประการสำคัญ หากการเปิดเผยออกไปจะกระทบกระเทือนต่อชีวิตความเป็นอยู่ส่วนตัวของเจ้าของข้อมูล หรือกระทบกระเทือนต่อสิทธิเสรีภาพอื่นๆจนเกินสมควร หรือการเปิดเผยนั้นก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลด้วยแล้ว ก็พึงที่จะงดเว้นเสีย แต่หากมีการเปิดเผยไปจนเกิดความเสียหายขึ้น เจ้าของข้อมูลก็ย่อมมีสิทธิเรียกร้องค่าสินไหมทดแทนเพื่อการทำละเมิดนั้นตามกฎหมายแพ่ง กฎหมายอาญา เว้นแต่การเปิดเผยข้อมูลข่าวสารส่วนบุคคลนั้นจะมีกฎหมายให้อำนาจไว้อย่างชัดเจน หรือเป็นไปเพื่อคุ้มครองประโยชน์สาธารณะอย่างแท้จริงก็ย่อมสามารถทำได้ โดยในกรณีนี้จำเป็นต้องอาศัยหลักความได้สัดส่วนมาใช้ประกอบการพิจารณาตัดสินใจในการเปิดเผยข้อมูล

[8] ศิริกุล ภู่พันธ์, **“ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล,”** (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2548), น. 83.

การที่จะถือว่าข้อมูลข่าวสารใดเป็นข้อมูลข่าวสารส่วนบุคคลนั้นตามการให้ความหมายของข้อมูลข่าวสารส่วนบุคคลอย่างกว้างซึ่งเป็นหลักกฎหมายที่ได้รับการยอมรับในนานาประเทศว่าจะสามารถคุ้มครองสิทธิส่วนบุคคลได้มากกว่านั้น จะต้องประกอบด้วยองค์ประกอบ 2 ประการ สำคัญกล่าวคือ[9]

1) ข้อมูลนั้นจะต้องเป็นข้อมูลข่าวสารที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล คือ ข้อมูลข่าวสารที่เป็นเรื่องเฉพาะตัวของบุคคลและมีผลเฉพาะตัวไม่เกี่ยวข้องกับบุคคลภายนอก ได้แก่

1.1 คุณสมบัติติดตัวของบุคคล ซึ่งอาจเป็นคุณสมบัติที่ติดตัวบุคคลไปตลอดชีวิตหรือลักษณะทางพันธุกรรมของบุคคล เช่นเชื่อชาติ กลุ่มเลือด สีผิว สีตา ลายพิมพ์นิ้วมือ ความพิการของร่างกายที่มีมาแต่กำเนิดอันมีลักษณะติดตัวของบุคคลไปจนตาย หรือเป็นสิ่งเฉพาะตัวของบุคคลที่เป็นคุณสมบัติที่สามารถเปลี่ยนแปลงได้ตามกาลเวลา เช่นน้ำหนัก อายุ ส่วนสูง วุฒิการศึกษา ความสามารถ ตำแหน่งหน้าที่การงาน ประวัติการทำงาน ประวัติสุขภาพ ประวัติอาชญากรรม ฯลฯ บรรดาที่มีชื่อของผู้นั้น

1.2 การประเมินคุณค่าในตัวบุคคล เช่นทัศนะคติ การประเมินความประพฤติ และความเห็นเกี่ยวกับการกระทำต่างๆของบุคคล เนื่องจากข้อมูลข่าวสารเหล่านี้เป็นสิ่งที่สื่อให้เห็นถึงความคิด ความสามารถ และการแสดงออกถึงความมีตัวตนของบุคคลได้

1.3 แนวความคิด ความเชื่อ พฤติกรรมซึ่งอาจเปลี่ยนแปลงไปตามวัยและวันเวลา เช่น ความสนใจทางการเมือง ความสนใจทางเพศ ความรักหรือความชอบ ความสามารถ

2) ข้อมูลนั้นจะต้องเป็นข้อมูลข่าวสารที่สามารถพิสูจน์ตัวบุคคลได้ กล่าวคือ สิ่งที่บอกลักษณะที่ทำให้รู้จักบุคคลจากข้อมูลข่าวสารนั้นได้ หรือเรียกได้ว่าเป็นข้อมูลที่บอกถึงความเป็นตัวตนของบุคคล หรือเป็นข้อมูลที่แสดงถึงลักษณะเฉพาะตัวที่แตกต่างไปจากบุคคลอื่น ได้แก่

2.1 เครื่องหมายบ่งชี้ตัวบุคคล เช่น ชื่อ นามสกุล ฉายาหรือนามแฝง หรือเลขรหัส กล่าวคือ หมายเลขประจำตัวประชาชน หมายเลขในใบอนุญาตขับขี่ หมายเลขประกันสังคม หมายเลขบัญชีสมุดฝากธนาคาร หมายเลขบัตรเครดิต หมายเลขโทรศัพท์

2.2 ลักษณะทางกายภาพของบุคคลภายนอก เช่นความสูงต่ำ ดำขาว ความสมบูรณ์หรือความพิการของบุคคลในทางกายภาพ

2.3 ข้อเท็จจริงต่างๆที่สามารถแสดงได้ว่าเป็นบุคคลหรือข้อเท็จจริงที่เกี่ยวข้องกับบุคคล เช่น ยศ ตำแหน่ง หน้าที่การงานซึ่งเป็นสถานะที่สามารถแสดงออกได้ชัดว่าหมายถึงผู้ที่ดำรงตำแหน่งดังกล่าวในขณะนั้น เช่นตำแหน่งนายกรัฐมนตรี ประธานสภาผู้แทนราษฎร เป็นต้น

2.4 ข้อมูลที่มีลักษณะเป็นการประเมินคุณค่าของบุคคล ทัศนคติต่อบุคคล การประพฤติปฏิบัติและการกระทำต่างๆของบุคคล ซึ่งข้อมูลข่าวสารเหล่านี้เป็นสิ่งที่สื่อให้เห็นถึงความคิดของบุคคลสามารถแสดงออกถึงความมีตัวตนของบุคคลได้ทั้งสิ้นเช่น ผลการสอบ การประเมินผลงาน หรือการให้

[9] **เรื่องเดียวกัน,** น. 84-85.

ความเห็นเกี่ยวกับความประพฤติและการกระทำของบุคคลเป็นการแสดงให้เห็นถึงคุณค่า คุณสมบัติที่จะแสดงถึงความเป็นตัวตนของบุคคลได้

จากองค์ประกอบของข้อมูลข่าวสารส่วนบุคคลดังกล่าว เมื่อพิจารณาต่อมาถึงการแบ่งประเภทของข้อมูลส่วนบุคคลที่มีอยู่หลายรูปแบบ และหลายลักษณะนั้นก็มีความพยายามในการจัดแบ่งประเภทของข้อมูลให้ชัดเจนมากยิ่งขึ้น ซึ่งกล่าวโดยกว้าง ๆ ได้ว่าการแบ่งประเภทของข้อมูลข่าวสารส่วนบุคคลนั้นหลักการทั่วไปที่ได้รับการยอมรับจะขึ้นอยู่กับการประเมินประเภทของข้อมูลในประเด็นความอ่อนไหว ที่จะส่งผลกระทบต่อเจ้าของข้อมูลหากมีการเปิดเผยหรือล่วงรู้ข้อมูลนั้น โดยสามารถแบ่งได้ออกเป็น 3 ระดับ[10] ดังนี้

1. ข้อมูลที่มีความอ่อนไหวระดับสูง (High sensitivity- HS) ข้อมูลประเภทนี้ ได้แก่ ข้อมูลรายละเอียดส่วนตัวของบุคคลในส่วนที่เกี่ยวข้องกับประวัติทางการแพทย์ พฤติกรรมทางเพศ หรือข้อเท็จจริงด้านอื่น ๆ ในชีวิตของบุคคลซึ่งสามารถกล่าวได้ว่าเป็นเรื่อง “ส่วนตัว” หรือ “ลับเฉพาะ” สำหรับข้อมูลประเภทความอ่อนไหวระดับสูงนี้ เหตุผลความจำเป็นที่จะต้องปกปิดข้อมูลก็มีความเหมาะสมมากที่สุด และเป็นข้อมูลที่ไม่ควรมีการเก็บโดยสิ้นเชิง

2. ข้อมูลที่มีความอ่อนไหวระดับปานกลาง (Moderate sensitivity-MS) นี่เป็นข้อมูลที่มีความอ่อนไหวมากในแง่ที่ว่าโอกาสที่จะก่อให้เกิดความเสียหายเมื่อข้อมูลถูกนำเอาไปใช้ในทางที่ผิดอยู่ในระดับสูง ข้อมูลประเภทนี้ครอบคลุมข้อมูลประเภทที่เกี่ยวกับความคิดเห็นของบุคคล (Judgmental data) ซึ่งมีความครอบคลุมทุกเรื่องของชีวิต ข้อมูลที่มีความอ่อนไหวระดับปานกลางนี้ ก็เช่นเดียวกับข้อมูลที่มีความอ่อนไหวระดับสูง คือไม่ควรถูกเก็บรวบรวมโดยสิ้นเชิง

3. ข้อมูลที่มีความอ่อนไหวระดับต่ำ (Low sensitivity- LS) ข้อมูลประเภทนี้เป็นข้อมูลที่เกี่ยวข้องกับบุคคล เป็นข้อมูลที่มีความอ่อนไหวเนื่องด้วยข้อมูลเหล่านี้อาจช่วยทำให้ได้มาซึ่งข้อมูลที่มีระดับความอ่อนไหวสูงขึ้น ดังนั้นข้อมูลเกี่ยวกับนายจ้างคนเก่าช่วยปูทางให้เข้าถึงข้อมูลที่มีความอ่อนไหวระดับสูงยิ่งขึ้นไป

2.2 การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

แนวทางดังกล่าวได้เกิดขึ้นในปี ค.ศ.1980 (พ.ศ. 2523) ซึ่งมีการวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขึ้นอย่างเป็นรูปธรรมและเป็นหลักเกณฑ์ที่ประเทศส่วนใหญ่ให้การยอมรับ คือ Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder flows of Personal Data โดย OECD (Organization for Economic Cooperation and Development) ภายใต้ Guidelines ฉบับนี้ได้กลายเป็นที่ยอมรับกันโดยทั่วไปว่าเป็นหลักเกณฑ์

[10] Raymond Wacks, **Personal Information : Privacy and the Law**, (London: Oxford, 1993), pp. 29-230.

พื้นฐานเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่สำคัญ ซึ่งประเทศส่วนใหญ่ในโลกต่างรับและนำไปบัญญัติเป็นกฎหมายภายในของตน

องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) ได้ออกแนวทางปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อการดูแลการส่งผ่านข้อมูลระหว่างประเทศ (Transborder flow) การคุ้มครองข้อมูลส่วนบุคคล (personal data) และการคุ้มครองสิทธิความเป็นส่วนตัว (privacy) ซึ่งเริ่มต้นมาจากปัญหาความไม่เท่าเทียมกันในบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลในแต่ละประเทศ ซึ่งอาจเป็นการขัดขวางการไหลเวียนของข้อมูลข่าวสารระหว่างประเทศ วัตถุประสงค์หลักของแนวทางนี้ก็เพื่อเป็นเครื่องมือในการสร้างความเป็นอันหนึ่งอันเดียวกันของประเทศสมาชิก OECD ทั้งนี้เพื่อก่อให้เกิดความเชื่อมั่นแก่ภาคเอกชนและผู้ประกอบธุรกิจทั้งหลายในการติดต่อสัมพันธ์ทางการค้า

กฎเกณฑ์ของแนวทางฉบับนี้ เป็นแนวปฏิบัติขั้นต่ำของหลักการเพื่อให้ประเทศสมาชิกได้นำไปปฏิบัติภายในแต่ละประเทศ แนวปฏิบัติฉบับนี้ไม่ได้แยกระหว่างหน่วยงานของรัฐและหน่วยงานเอกชน และไม่ได้แยกว่าเป็นการประมวลผลข้อมูลเกี่ยวกับบุคคลโดยวิธีการอัตโนมัติหรือโดยวิธีการประมวลผลด้วยมือ

ขอบเขตความหมายของข้อมูลส่วนบุคคล (Personal data) หมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องเฉพาะตัวบุคคล หรือสามารถชี้ให้เห็นลักษณะเฉพาะตัวบุคคลเจ้าของข้อมูลได้ ซึ่งโดยภาพรวมของการคุ้มครองข้อมูลส่วนบุคคลมีหลักการดังนี้

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล ข้อมูลส่วนบุคคลที่จัดเก็บจะต้องได้มาโดยวิธีการที่ถูกต้องและชอบด้วยกฎหมาย โดยต้องให้บุคคลผู้เป็นเจ้าของข้อมูลรับทราบและยินยอมในการจัดเก็บข้อมูล

2. หลักคุณภาพของข้อมูล ข้อมูลส่วนบุคคลที่จัดเก็บต้องเป็นข้อมูลที่มีความเกี่ยวข้องกับวัตถุประสงค์ในการใช้ และต้องเป็นข้อมูลที่ถูกต้อง สมบูรณ์และถูกต้องตรงตามความเป็นจริงอยู่เสมอ

3. หลักการกำหนดวัตถุประสงค์ ต้องมีการกำหนดวัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคลก่อนที่จะมีการจัดเก็บข้อมูลส่วนบุคคลนั้น

4. หลักการจำกัดการใช้ข้อมูล การใช้ข้อมูลจะกระทำได้โดยขัดต่อวัตถุประสงค์ในการจัดเก็บมิได้เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูล หรือได้รับอนุญาตตามเงื่อนไขที่กฎหมายกำหนด

5. หลักการรักษาความปลอดภัย ต้องจัดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลเพื่อป้องกันความเสื่อมเสีย การเข้าถึง การทำลาย การใช้ การเปลี่ยนแปลงแก้ไข หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6. หลักการเปิดเผยข้อมูล ต้องกำหนดวิธีการทั่วไปในการเปิดเผยข้อมูล รูปแบบของการเปิดเผย หลักเกณฑ์ในการขอให้มีการเปิดเผยข้อมูล ซึ่งต้องไม่เป็นการกระทบต่อความเป็นอยู่ส่วนตัวของเจ้าของข้อมูล

7. หลักการมีส่วนร่วมของปัจเจกบุคคล กำหนดให้ปัจเจกชนมีสิทธิต่างๆ ดังต่อไปนี้

- มีสิทธิได้รับการแจ้งว่ามีข้อมูลของตนจัดเก็บอยู่
- มีสิทธิตรวจสอบข้อมูลของตนที่มีผู้จัดเก็บ
- มีสิทธิขอให้แก้ไขข้อมูลที่ไม่ถูกต้อง
- มีสิทธิปฏิเสธไม่ให้มีการจัดเก็บข้อมูลของตน

8. หลักความรับผิดชอบ กำหนดความรับผิดในกรณีมีการละเมิดข้อมูลส่วนบุคคลของตน

ในส่วนของการไหลเวียนของข้อมูลระหว่างประเทศ ได้กำหนดหลักการให้ประเทศสมาชิกรับรองการไหลเวียนข้อมูลส่วนบุคคล ซึ่งรวมถึงการส่งข้อมูลทั้งหมดในประเทศสมาชิกอย่างต่อเนื่องและปลอดภัย และให้ประเทศสมาชิกงดเว้นจากการจำกัดการไหลเวียนของข้อมูลระหว่างประเทศ เว้นแต่ประเทศที่มีวัตถุประสงค์ที่จะไม่ปฏิบัติตามแนวทาง หรือเมื่อมีการส่งออกไปใหม่ของข้อมูลที่อาจถูกจำกัดโดยกฎหมายคุ้มครองข้อมูล หรือในกรณีข้อมูลส่วนบุคคลบางชนิด หรือในกรณีประเทศอื่นที่มีบทบัญญัติในการคุ้มครองข้อมูลที่ไม่เท่าเทียมกันหรือไม่เป็นไปตามมาตรฐานที่ยอมรับได้

2.3 การคุ้มครองข้อมูลส่วนบุคคลตามข้อบังคับสหภาพยุโรป (European Union Directive 95/46/EC) และข้อตกลงรัฐสภายุโรป

แนวทางการคุ้มครองตาม(The EU Directive 95/46/EC) เกิดขึ้นโดยคณะกรรมาธิการ (European Commission) แห่งประชาคมเศรษฐกิจยุโรป (European Economic Community) ที่ได้มีข้อเสนอแนะ (Recommendation) เกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับอนุสัญญาของคณะมนตรีแห่งยุโรป (Commission Recommendation : Relating to the Council of Europe Convention for the Protection of individuals with regard to Automatic Processing of Personal Data) เพื่อประกันสิทธิขั้นพื้นฐานของประชาชน ดังนั้นสหภาพยุโรป จึงได้กำหนดให้ประเทศสมาชิกให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เทียบเท่ากันในยุโรป โดยใช้อนุสัญญาของคณะมนตรีแห่งยุโรปเป็นแนวทางในการยกร่างกฎหมาย ทั้งนี้ เพื่อให้กฎหมายอยู่ในลักษณะเป็นเอกภาพทั่วทั้งยุโรป (for the purpose of creation a uniform level of data protection in Europe)

การคุ้มครองข้อมูลส่วนบุคคลภายใต้ข้อบังคับสหภาพยุโรป 95/46 เริ่มต้นขึ้นในปี 1995 นับเป็นบทบัญญัติที่มีผลบังคับระหว่างประเทศฉบับแรกที่ให้ความคุ้มครองข้อมูลส่วนบุคคล ที่ถูกสร้างขึ้นโดยประเทศสมาชิกสหภาพยุโรป ข้อบังคับฉบับนี้ให้การคุ้มครองข้อมูลส่วนบุคคล และเสรีภาพในการเคลื่อนไหวของข้อมูล ทั้งยังให้การรับรองว่าข้อมูลจะได้รับการคุ้มครองอย่างเท่าเทียมกันตลอดทั้งตลาดร่วมยุโรป โดยมีขอบเขตการบังคับใช้ คือ ในมาตรา 2 ได้ให้คำจำกัดความของข้อมูลส่วนบุคคล (personal data) ว่าหมายถึงข้อมูลข่าวสาร (information) ใดๆ ที่ชี้เฉพาะตัวบุคคล หรือสามารถบ่งชี้ลักษณะเฉพาะที่เกี่ยวข้องกับตัวบุคคล ซึ่งหมายถึงบุคคลธรรมดา (natural person) ที่เป็นเจ้าของข้อมูล (data subject) การชี้เฉพาะตัวบุคคลอาจเป็นไปโดยตรงหรือโดยอ้อม การอ้างอิงถึงข้อมูลส่วนบุคคล เช่น หมายเลขประจำตัว ลักษณะสำคัญทางกาย สรีระ จิตใจ สถานะทางการเงิน สังคม วัฒนธรรม ซึ่งเป็นข้อมูลที่สามารถชี้เฉพาะตัวบุคคลได้ และในขอบเขตของการบังคับใช้ทั้งในการ

ประมวลข้อมูลโดยวิธีการปกติ (manual) และการประมวลผลข้อมูลโดยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอัตโนมัติ (electronic or automatic)

ดังนั้น ประชาชนทุกคนในสหภาพยุโรป ทุกหน่วยงานราชการ และในทุกบริษัทห้างร้านและองค์กรธุรกิจเอกชนทุกแห่งต้องสามารถให้ความมั่นใจได้ว่าได้มีการนำกฎเกณฑ์การคุ้มครองไปปฏิบัติจริงในมาตรฐานเดียวกันทั่วทั้งสหภาพยุโรป โดยมีวัตถุประสงค์หลัก 2 ประการ คือ เพื่อให้ประเทศสมาชิกของสหภาพยุโรป มีแนวทางการบัญญัติกฎหมายคุ้มครองข้อมูลที่สอดคล้องกัน และเพื่อให้มีมาตรฐานในการปฏิบัติในการส่งข้อมูลส่วนบุคคลภายในประเทศสมาชิก

ข้อบังคับฉบับนี้ได้เรียกร้องให้มีการบัญญัติกฎหมายคุ้มครองข้อมูลในแต่ละประเทศ เพื่อให้การคุ้มครองประชาชนมากขึ้น สำหรับการคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวกับภาคเอกชน โดยเฉพาะในบริษัทเอกชนที่ประกอบธุรกิจการค้า ต้องยึดหลักการที่เป็นสาระสำคัญดังนี้

1. การรักษาคุณภาพของข้อมูล
2. มาตรการของการประมวลผลข้อมูลที่ชอบด้วยกฎหมาย
3. ข้อกำหนดในการประมวลผลข้อมูลชนิดพิเศษ เช่น ข้อมูลส่วนตัวโดยเฉพาะ (sensitive data)
4. สิทธิในการได้รับแจ้งการเก็บข้อมูลต่างๆ ของเจ้าของข้อมูล
5. สิทธิในการเข้าถึงข้อมูลของเจ้าของข้อมูล
6. สิทธิในการคัดค้านการประมวลผลของเจ้าของข้อมูล
7. การรักษาความปลอดภัยในการประมวลผลข้อมูล
8. การส่งผ่านข้อมูลส่วนบุคคลไปยังประเทศที่สาม

นอกจากการควบคุมการส่งข้อมูลภายในประเทศสมาชิกแล้ว สำหรับประเทศที่ไม่ได้เป็นสมาชิกสหภาพยุโรป หากจะทำการติดต่อรับ-ส่งข้อมูลกับประเทศสมาชิกสหภาพยุโรป ก็ต้องมีมาตรการการคุ้มครองข้อมูลข่าวสารที่เหมาะสมเป็นที่พอใจแก่สหภาพยุโรปด้วยเช่นกัน ซึ่งมาตรการที่เหมาะสมที่สหภาพยุโรปได้ตั้งไว้ แม้กระทั่งประเทศสหรัฐอเมริกา ที่มีการค้าและการลงทุนกับประเทศสมาชิกสหภาพยุโรปมากที่สุด และมีการเคลื่อนไหวของข้อมูลข่าวสารมากที่สุด ก็ยังมีรูปแบบการคุ้มครองไม่เหมือนกับสหภาพยุโรป ทั้งนี้สหรัฐอเมริกาใช้ระบบควบคุมตนเอง(self-regulation) โดยภาคเอกชนกำหนดการควบคุมข้อมูลขึ้นมาด้วยตนเอง ซึ่งทั้งสองฝ่ายมีการพยายามหาวิธีการที่ประนีประนอมเพื่อเป็นทางออกและแก้ไขปัญหาความขัดแย้งของทั้งสองฝ่ายนี้

ขอบเขตของ Directive ใช้บังคับกับการประมวลผลข้อมูลส่วนบุคคลทั้งการประมวลผลโดยอัตโนมัติและการประมวลผลด้วยวิธีการ Manual สำหรับการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการ Manual นั้น ข้อมูลส่วนบุคคลที่ถูกประมวลผลด้วยวิธีนี้ต้องเป็นส่วนหนึ่งหรือมีเจตนาที่จะให้เป็นส่วนหนึ่งของระบบการจัดเก็บข้อมูล (Filling System) เช่น ระบบการจัดเก็บข้อมูลประวัติคนไข้ของ

โรงพยาบาลต่าง ๆ) อย่างไรก็ตาม กฎหมายไม่ใช้บังคับกับการประมวลผลข้อมูลโดยบุคคลธรรมดาในกรณีของ A purely personal or household activity ทั้งนี้สาระสำคัญของสหภาพยุโรปนี้มีดังต่อไปนี้ [11]

ก. ข้อมูลที่กฎหมายคุ้มครอง

คือ ข้อมูลส่วนบุคคล (Personal Data) ซึ่งหมายความว่า ข้อเท็จจริงหรือรายละเอียดใด ๆ ที่เกี่ยวกับบุคคลธรรมดา (Natural Person) ที่ถูกระบุตัวหรือสามารถถูกระบุตัวได้ไม่ว่าโดยตรงหรือโดยอ้อม

บุคคลที่ถูกระบุตัวหรือสามารถถูกระบุตัวจากข้อมูลดังกล่าว ตามกฎหมายนี้เรียก Data Subject กรณีของบุคคลที่ถูกระบุตัว (Identified person) จะเป็นกรณีที่ระบุตัวบุคคลดังกล่าวได้จากชื่อของบุคคลนั้น ส่วนกรณีของบุคคลที่สามารถถูกระบุตัว (Identifiable person) เป็นกรณีที่สามารถระบุตัวบุคคลดังกล่าวได้จากข้อมูลใดโดยใช้วิธีการที่สมเหตุสมผล (Reasonable) โดยเฉพาะจากข้อมูลดังต่อไปนี้ เลขบัตรประจำตัวประชาชนซึ่งถือเป็นกรณีระบุโดยตรง ส่วนการระบุโดยอ้อมก็เช่นการระบุตัวบุคคลโดยอาศัยข้อมูลเกี่ยวกับลักษณะเฉพาะทางร่างกาย จิตใจ ฐานะทางเศรษฐกิจ เอกลักษณ์ทางวัฒนธรรมและสังคม เป็นต้น

ข. การดำเนินการที่กฎหมายควบคุม

คือ การประมวลผลข้อมูล (Processing) ซึ่งหมายความว่า การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีการอัตโนมัติหรือวิธีการอื่นใด เช่น การเก็บรวบรวม การบันทึก การจัดเรียบเรียง การเก็บรักษา การแก้ไขเปลี่ยนแปลง การค้นคืน consultation การใช้ การเปิดเผยโดยการส่งผ่าน การเผยแพร่ (dissemination) หรือโดยวิธีการอื่น ๆ ที่ทำให้เข้าถึงข้อมูลได้ การจัดกลุ่มหรือการรวมข้อมูล การขัดขวาง การลบ หรือการทำลายข้อมูล

เมื่อพิจารณาจากคำนิยามคำว่า “ข้อมูลส่วนบุคคล” ซึ่งเป็นสิ่งที่กฎหมายประสงค์จะคุ้มครอง จะเห็นว่ากฎหมายมุ่งประสงค์จะคุ้มครองเฉพาะข้อมูลส่วนบุคคลของบุคคลธรรมดาเท่านั้น ดังนั้น นิติบุคคลจึงมิได้รับความคุ้มครองตามกฎหมายนี้ บุคคลที่ถูกควบคุมคือ ผู้ควบคุมข้อมูล (Controller) และผู้ประมวลผลข้อมูล (Processor) ซึ่งผู้ควบคุมข้อมูลหมายความว่า บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่ของรัฐ หน่วยงานหรือองค์กรอื่นใด โดย โดยลำพังหรือร่วมกับผู้อื่นกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคลในกรณีที่วัตถุประสงค์และวิธีการของการประมวลผลถูกกำหนดโดยกฎหมายหรือกฎเกณฑ์ของรัฐสมาชิกหรือของสหภาพยุโรป ผู้ควบคุมข้อมูลหรือวิธีการแต่งตั้งหรือเลือกตั้งเป็นผู้ควบคุมข้อมูลอาจถูกกำหนดโดยกฎหมายภายในของรัฐสมาชิกหรือกฎหมายของสหภาพยุโรป

[11]โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, **สาระสำคัญกฎหมายคุ้มครองข้อมูลส่วนบุคคลต่างประเทศ,** (อัดสำเนา), น. 1-5.

ส่วนผู้ประมวลผลข้อมูล หมายความว่า บุคคลธรรมดาหรือนิติบุคคล เจ้าหน้าที่ของรัฐ หน่วยงานหรือองค์กรอื่นใดซึ่งประมวลผลข้อมูลส่วนบุคคลแทนผู้ควบคุมข้อมูล แต่ทั้งนี้ก็มีข้อยกเว้นทั่วไปในการควบคุม 2 กรณี คือ

(1) การประมวลผลในกิจกรรมที่อยู่นอกขอบเขตของ Community Law เช่น กิจกรรมเกี่ยวกับนโยบายต่างประเทศและความมั่นคง หรือการประมวลผลในกิจกรรมของรัฐที่เกี่ยวกับกฎหมายอาญา เป็นต้น

(2) การประมวลผลโดยบุคคลธรรมดาเพื่อกิจกรรมส่วนตัว (Purely Personal and Household Activity)

ค. หน้าที่ของบุคคลที่ถูกควบคุม

Directive กำหนดให้ผู้ควบคุมข้อมูลมีหน้าที่แจ้งแก่ Supervisory Authority ก่อนที่จะทำการประมวลผลข้อมูลส่วนบุคคลด้วยวิธีการอัตโนมัติ โดยในการแจ้งนั้นต้องประกอบด้วยรายการข้อมูลดังนี้

(1) ชื่อที่อยู่ของผู้ควบคุมข้อมูลและผู้แทน (ถ้ามี)

(2) วัตถุประสงค์ของการประมวลผล

(3) ประเภทของข้อมูลที่เก็บ

(4) ผู้รับข้อมูล

(5) วัตถุประสงค์ของการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

(6) ข้อมูลเบื้องต้นเกี่ยวกับมาตรการที่ใช้เพื่อรักษาความปลอดภัยในการประมวลผลข้อมูล

ทั้งนี้ก่อนการประมวลผลข้อมูลDirective กำหนดว่าการประมวลผลข้อมูลส่วนบุคคลต้องกระทำโดยชอบด้วยกฎหมาย ซึ่งการประมวลผลเช่นใดถึงจะเรียกว่าชอบด้วยกฎหมายนั้น Directive ได้กำหนดไว้ 7 กรณีดังนี้

(1) ได้รับความยินยอมจากเจ้าของข้อมูล (Unambiguous Consent of Data Subject)

(2) เป็นกรณีจำเป็นเพื่อปฏิบัติตามสัญญาหรือเป็นการดำเนินการก่อนเข้าทำสัญญา

(3) ตามที่กฎหมายกำหนด

(4) เพื่อรักษาชีวิตของเจ้าของข้อมูล (Vital Interest)

(5) เพื่อปฏิบัติภารกิจที่ผลประโยชน์ของสาธารณะหรือจำเป็นต่อการปฏิบัติหน้าที่ของเจ้าพนักงาน

(6) เพื่อประโยชน์ที่ชอบด้วยกฎหมายของผู้ควบคุมข้อมูลหรือบุคคลที่สาม และการประมวลผลดังกล่าวไม่เป็นการกระทบกระเทือนต่อประโยชน์ของการคุ้มครองสิทธิขั้นพื้นฐานของเจ้าของข้อมูลโดยเฉพาะสิทธิในความเป็นส่วนตัว

ง. หลักการทั่วไปเกี่ยวกับการประมวลผลข้อมูล

Directive กำหนดว่าประเทศสมาชิกต้องปฏิบัติต่อไปนี้ในการดำเนินการต่อข้อมูลส่วนบุคคล อันได้แก่

(1) ข้อมูลส่วนบุคคลต้องถูกประมวลผลอย่างเป็นธรรมและชอบด้วยกฎหมาย

(2) ข้อมูลส่วนบุคคลต้องถูกจัดเก็บโดยมีวัตถุประสงค์ที่ชัดเจน แน่นอน และชอบด้วยกฎหมาย (specified, explicit and legitimate purposes) นอกจากนี้จะต้องไม่มีการประมวลผลข้อมูลที่ขัดแย้งกับวัตถุประสงค์นั้น เว้นแต่การประมวลผลข้อมูลที่มีวัตถุประสงค์ทางด้านประวัติศาสตร์ สถิติ หรือวิทยาศาสตร์

(3) ข้อมูลส่วนบุคคลต้องมีความเพียงพอ (adequate) ไม่มากเกินจำเป็น (not excessive) และสอดคล้องกับวัตถุประสงค์ในการจัดเก็บ หรือประมวลผลข้อมูลนั้น

(4) ข้อมูลส่วนบุคคลต้องมีความถูกต้องครบถ้วน และกรณีจำเป็นต้องเป็นปัจจุบันด้วย

(5) ไม่ควรเก็บไว้ในรูปแบบที่สามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลไว้นานเกินไป อีกทั้งต้องใช้มาตรการที่เหมาะสมในการรักษาความปลอดภัยของข้อมูล

นอกจากนี้ตามข้อตกลงได้กำหนดให้มีข้อมูลชนิดพิเศษ (Sensitive Data) ซึ่งกฎหมายกำหนดให้เป็นหน้าที่ของผู้ควบคุมการประมวลผลข้อมูลส่วนบุคคลที่ต้องใช้มาตรการทางเทคนิคและการจัดการที่เหมาะสมเพื่อคุ้มครองข้อมูลส่วนบุคคลจาก

(1) การทำลายข้อมูลโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย

(2) การสูญเสียข้อมูลโดยอุบัติเหตุ

(3) การแก้ไขเปลี่ยนแปลงโดยอุบัติเหตุ

(4) การเปิดเผยหรือการเข้าถึงโดยปราศจากอำนาจ และ

(5) ป้องกันการประมวลผลที่มิชอบด้วยกฎหมายทุกรูปแบบ

การพิจารณาถึงความเหมาะสมที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลนั้นต้องพิจารณาถึงความเสี่ยงที่เกิดขึ้นจากการประมวลผล และลักษณะของข้อมูลที่ทำการประมวลผล

โดยสรุปข้อกำหนดของ EU ได้กำหนดให้รัฐสมาชิกอนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักทั่วไป ดังนี้[12]

(1) ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

(2) การประมวลผลจะทำได้เท่าที่จำเป็นในการทำนิติกรรมสัญญาใด ๆ ของผู้เป็นเจ้าของข้อมูลเท่านั้น

(3) การประมวลผลจะต้องอยู่ภายใต้กรอบของกฎหมาย

(4) การประมวลผลจะต้องกระทำเพื่อปกป้องผลประโยชน์สำคัญของผู้เป็นเจ้าของข้อมูล

---

[12] สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, **โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ,** พิมพ์ครั้งที่ 3, (กรุงเทพมหานคร: เดือนตุลา, 2544), น. 99-100.

(5) การประมวลผลจำเป็นที่จะต้องกระทำเพื่อผลประโยชน์ของสาธารณะ หรือในการดำเนินงานของหน่วยงานของรัฐที่ได้รับมอบหมายให้เป็นผู้ควบคุมข้อมูล หรือเปิดเผยข้อมูลต่อบุคคลที่สาม

(6) การประมวลผลที่จำเป็นและอยู่ภายใต้กรอบของกฎหมายจะต้องไม่กระทบต่อผลประโยชน์ หรือสิทธิขั้นพื้นฐานของผู้เป็นเจ้าของข้อมูล

ทั้งนี้ตามข้อกำหนดของสหภาพยุโรปยังได้ให้ความสำคัญเกี่ยวกับความลับและความมั่นคง รวมถึงข้อยกเว้นในการเปิดเผยข้อมูลกรณีที่มิได้นำข้อมูลไปใช้ประโยชน์สาธารณะ แต่นำไปใช้เพื่อประโยชน์ส่วนตัว และกำหนดเกี่ยวกับเรื่องความเสียหายที่เกิดขึ้นต่อ ผู้เป็นเจ้าของข้อมูล เมื่อมีการประมวลผลโดยไม่ชอบด้วยกฎหมาย และการเปิดเผยข้อมูลจะต้องไม่ละเมิดต่อความมั่นคงของรัฐ

จ. การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ

Directive ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลเพื่อประมวลผลหรือเจตนาที่จะประมวลผลไปยังประเทศที่มิได้เป็นสมาชิกสหภาพยุโรป เว้นแต่ ประเทศที่รับข้อมูลจะได้ให้ความคุ้มครองข้อมูลส่วนบุคคลใน “ระดับที่เพียงพอ (Adequate Level)” อย่างไรก็ตาม Directive ก็กำหนดข้อยกเว้นไว้ เช่น ได้รับความยินยอมอย่างชัดแจ้งจากเจ้าของข้อมูล หรือการส่งหรือโอนข้อมูลส่วนบุคคลจำเป็นเพื่อปฏิบัติตามสัญญาที่เจ้าของข้อมูลและผู้ควบคุมข้อมูลเป็นคู่กรณีต่อกัน หรือเพื่อปฏิบัติการให้เป็นไปตามข้อตกลงก่อนเข้าทำสัญญาตามคำร้องขอของเจ้าของข้อมูล

ฉ. สิทธิของเจ้าของข้อมูล

Directive ได้กำหนดสิทธิของเจ้าของข้อมูลที่สำคัญ ๆ ไว้ดังนี้

(1) สิทธิได้รับแจ้งข้อมูลตามที่กฎหมายกำหนดเมื่อถูกเก็บรวบรวมข้อมูล

(2) สิทธิเข้าถึงข้อมูลส่วนบุคคลเกี่ยวกับตน

(3) สิทธิแก้ไขข้อมูลส่วนบุคคลที่เกี่ยวกับตนให้ถูกต้อง

ช. องค์กรที่ทำหน้าที่ควบคุมและบังคับการให้เป็นไปตามกฎหมาย

Directive วางแนวทางให้ประเทศสมาชิกสหภาพยุโรป (European Union) กำหนดให้มีองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความเป็นอิสระไว้ในกฎหมายคุ้มครองของแต่ละประเทศ ซึ่งประเทศสมาชิกส่วนใหญ่ก็จะกำหนดไว้ในรูปของ Commissioner ซึ่ง Directive กำหนดให้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอย่างน้อยต้องกำหนดอำนาจหน้าที่ดังต่อไปนี้ให้กับบุคคลหรือองค์กรที่ทำหน้าที่ควบคุมดูแลให้เป็นไปตามกฎหมาย คือ

(1) อำนาจในการสืบสวน เช่น อำนาจในการเข้าถึงและเก็บรวบรวมข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ของผู้ควบคุมดูแล

(2) อำนาจในการแทรกแซง เช่น อำนาจในการออกคำสั่งขัดขวาง ลบ หรือทำลายข้อมูล หรือ การห้ามการประมวลผลข้อมูลชั่วคราว

(3) รับคำร้องทุกข์เกี่ยวกับการดำเนินการที่เป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลและวินิจฉัยคำร้องทุกข์ดังกล่าว

(4) จัดทำรายงานการปฏิบัติงานและเผยแพร่รายงานดังกล่าวต่อสาธารณะ

(5) ผู้ควบคุมดูแลและเจ้าหน้าที่ของผู้ควบคุมดูแลต้องรักษาความลับของข้อมูลที่มี Confidential ซึ่งตนได้เข้าถึงเนื่องจากการปฏิบัติหน้าที่

นอกจากข้อตกลงของสหภาพยุโรปแล้ว กลุ่มประเทศทวีปยุโรปได้มีแนวทางอีกข้อหนึ่งของการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามข้อตกลงของรัฐสภายุโรป ซึ่ง ข้อตกลงดังกล่าว(Convention of Council of Europe) ได้ประกาศใช้เมื่อปี ค.ศ. 1984 มีบทบัญญัติถึงการคุ้มครองสิทธิความเป็นส่วนตัว และการคุ้มครองข้อมูลข่าวสารส่วนบุคคล การประมวลผลโดยวิธีอัตโนมัติ และการเปิดเสรีของการไหลเวียนข้อมูลระหว่างประเทศ โดยมีหลักการสำคัญๆ ได้แก่[13]

1) หลักการเก็บรวบรวมข้อมูล การประมวลผลข้อมูลต้องดำเนินการโดยถูกต้อง และการเปิดเผยต้องทำด้วยเจตนาที่สุจริต

2) หลักการกำหนดระยะเวลาในการใช้ข้อมูล เมื่อสิ้นสุดความจำเป็นในการใช้ข้อมูลต้องยกเลิกการจัดเก็บทันที

3) หลักการจัดเก็บและการประมวลผลต้องทำภายใต้วัตถุประสงค์ และเพียงเท่าที่จำเป็น

4) หลักความถูกต้องของข้อมูลข่าวสาร ต้องมีคุณภาพ และมีการปรับปรุงให้ทันสมัยอยู่เสมอ

5) หลักการรักษาความปลอดภัยของข้อมูลข่าวสาร มาตรการการคุ้มครองข้อมูลข่าวสารตามกฎหมายและให้ความคุ้มครองในทางเทคนิค

ภายใต้ข้อตกลงของรัฐสภายุโรปนี้ เพื่อควบคุมการคุ้มครองให้เป็นไปตามกฎหมาย จึงได้มีการกำหนดให้มีองค์กรที่ชื่อ The Council of European's Committee ทำหน้าที่คอยดูแลการละเมิดสิทธิส่วนบุคคลอันเกิดจากการละเมิดข้อมูลข่าวสารส่วนบุคคลด้วย

2.4 กรอบการคุ้มครองข้อมูลส่วนบุคคลตามของสหประชาชาติ (United Nations)

แนวทางนี้ได้รับการจัดทำขึ้นเมื่อวันที่ 14 ธันวาคม 1990 โดยสมัชชาใหญ่แห่งสหประชาชาติได้มีมติกำหนดแนวทางในการประมวลผลแฟ้มข้อมูลส่วนบุคคลทางคอมพิวเตอร์ (Guidelines Concerning Computerized Personal Data Files)ขึ้น เพื่อให้ประเทศสมาชิกปฏิบัติตามหลักเกณฑ์ในการกำหนดมาตรฐานขั้นต่ำเกี่ยวกับการบัญญัติกฎหมายภายในของรัฐ

[13]นคร เสรีรักษ์, **การคุ้มครองข้อมูลส่วนบุคคล: ข้อเสนอเพื่อการพัฒนาสิทธิรับรู้ข้อมูลข่าวสารในกระบวนการธรรมรัฐไทย**, (กรุงเทพมหานคร: ม.ป.ท., ม.ป.ป.), น. 102.

สหประชาชาติก็ได้กำหนดหลักเกณฑ์เกี่ยวกับข้อมูลส่วนบุคคลไว้ใน “แนวทางการควบ คุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์” (Guidelines for the Regulation of Computerized Personal Data Files) ซึ่งมีสาระสำคัญดังนี้

1. หลักความชอบด้วยกฎหมายและความเป็นธรรม (Principle of lawfulness and fairness)

ข้อมูลส่วนบุคคลจะต้องไม่ถูกเก็บรวบรวมหรือประมวลผลด้วยวิธีการที่ไม่เป็นธรรมหรือไม่ชอบด้วยกฎหมายและการใช้ข้อมูลส่วนบุคคลจะต้องไม่ขัดกับวัตถุประสงค์และหลักการของกฎบัตรสหประชาชาติ

2. หลักความถูกต้อง (Principle of accuracy)

ในการเก็บรวบรวมข้อมูลส่วนบุคคลจะต้องมีการตรวจสอบอย่างสม่ำเสมอว่ากระทำด้วยความถูกต้อง ข้อมูลมีความสมบูรณ์ ทันสมัยอยู่เสมอ และเก็บได้ภายในระยะเวลาเท่าที่จะมีการประมวลผลหรือใช้ข้อมูลเหล่านั้น

3. หลักการระบุวัตถุประสงค์โดยเฉพาะเจาะจง (Principle of the purpose-specification)

จะต้องมีการระบุวัตถุประสงค์ในการจัดเก็บและเงื่อนไขของการใช้ประโยชน์ข้อมูลที่เก็บตามวัตถุประสงค์ซึ่งชอบด้วยกฎหมายโดย

(1) เก็บรวบรวมเพียงเท่าที่เกี่ยวข้อง และเหมาะสมกับวัตถุประสงค์ที่ระบุไว้

(2) ข้อมูลส่วนบุคคลจะต้องไม่ถูกใช้หรือเปิดเผย เว้นแต่ได้รับความยินยอมจากบุคคลที่เกี่ยวข้อง

(3) ระยะเวลาที่จัดเก็บข้อมูลส่วนบุคคลจะต้องไม่เกินกว่าระยะเวลาที่การดำเนินการตามวัตถุประสงค์ที่ระบุไว้ได้สำเร็จลง

4. หลักการเข้าถึงข้อมูล (Principle of interested-person access)

เจ้าของข้อมูลมีสิทธิที่จะได้รู้ว่ามีการประมวลผลข้อมูลข่าวสารที่เกี่ยวกับตน โดยได้รับข้อมูลในรูปแบบที่เข้าใจได้ในเวลาอันสมควรและปราศจากค่าใช้จ่าย และสามารถขอให้แก้ไขหรือลบในกรณีมีการเก็บข้อมูลโดยไม่ชอบด้วยกฎหมาย ไม่จำเป็น หรือมีการเก็บข้อมูลโดยไม่ถูกต้อง ข้อกำหนดแห่งหลักการนี้ให้บังคับใช้กับบุคคลทุกคนโดยไม่คำนึงถึงสัญชาติหรือ ถิ่นที่อยู่

5. หลักการไม่เลือกปฏิบัติ (Principle of non-discrimination)

ห้ามเก็บรวบรวมข้อมูลซึ่งอาจทำให้เกิดการเลือกปฏิบัติที่ขัดต่อกฎหมาย เช่น ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ สีผิว พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง การนับถือศาสนา ความเชื่อทางปรัชญาหรือความเชื่ออื่นๆ รวมทั้งข้อมูลการเป็นสมาชิกสหภาพ หรือสมาคมทางการค้า

6. การกำหนดข้อยกเว้น (Power to make exceptions)

ข้อยกเว้นจากหลักการข้อที่ 1-4 อาจกำหนดได้ในกรณีจำเป็นเพื่อรักษาความมั่นคงของชาติ ระเบียบสังคม สาธารณสุข หลักคุณธรรม และสิทธิและเสรีภาพของบุคคลอื่น

ข้อยกเว้นจากหลักการข้อที่ 5 อาจเป็นกรณีเพื่อการป้องกันการเลือกปฏิบัติ ภายใต้ข้อบัญญัติของปฏิญญาสากลว่าด้วยสิทธิมนุษยชนหรือกลไกของกฎหมายอื่นๆ ที่เกี่ยวกับการคุ้มครองสิทธิมนุษยชนและการป้องกันการเลือกปฏิบัติ

7. **หลักการรักษาความปลอดภัย** (Principle of security)

จะต้องมีการรักษาความปลอดภัยข้อมูลที่จัดเก็บ เพื่อป้องกันอันตรายทั้งจากภัยธรรมชาติ การสูญหายหรือเสียหาย การทำลายโดยบุคคล การเข้าถึงโดยปราศจากอำนาจ การใช้ในทางที่ผิด หรือการทำลายโดยไวรัสคอมพิวเตอร์

8. **หลักการกำกับดูแล** (Supervision and sanctions)

กฎหมายของประเทศต่างๆ จะต้องระบุหน่วยงานที่รับผิดชอบในการ ควบคุมดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติตามหลักการนี้

9. **หลักการส่งข้อมูลข้ามพรมแดน** (Transborder data flows)

การส่งข้อมูลระหว่างประเทศจะสามารถกระทำได้ในกรณีที่ประเทศสองประเทศหรือมากกว่าสองประเทศ มีกลไกในการคุ้มครองสิทธิความเป็นส่วนตัวในระดับเดียวกัน

10. **หลักขอบเขตการใช้ข้อปฏิบัติ** (Field of application)

หลักปฏิบัติดังกล่าวควรได้มีการปฏิบัติใช้สำหรับข้อมูลในภาครัฐและเอกชนที่จัด เก็บด้วยคอมพิวเตอร์ (Computerized Files) เช่นเดียวกับการจัดเก็บด้วยวิธีการอื่นๆ ที่มีการปรับปรุงให้เหมาะสมกับเอกสารที่จัดเก็บด้วยมือ (Manual Files)

2.5 กรอบการคุ้มครองข้อมูลส่วนบุคคลของ APEC

กลุ่มความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก หรือ เอเปค (APEC) ก่อตั้งขึ้นเมื่อปี ค.ศ. 1989 (พ.ศ. 2532) มีวัตถุประสงค์เพื่อมุ่งเน้นการพัฒนาที่ยั่งยืนทางเศรษฐกิจในภูมิภาค และผลักดันให้การเจรจาการค้าเสรีหลายฝ่ายประสบผลสำเร็จ เอเปคมีสมาชิกรวมทั้งสิ้น 21 เขตเศรษฐกิจ (19 ประเทศ และ 2 เขตเศรษฐกิจ) อาทิ สหรัฐอเมริกา แคนาดา เม็กซิโก ออสเตรเลีย นิวซีแลนด์ สาธารณรัฐประชาชนจีน จีนฮ่องกง จีนไทเป ญี่ปุ่น สาธารณรัฐเกาหลี สิงคโปร์ และประเทศไทย ฯลฯ โดยได้จัดตั้งมีสำนักงานเลขาธิการเอเปค (APEC Secretariat) ขึ้นเมื่อปี ค.ศ. 1992 (พ.ศ. 2535) ซึ่งตั้งอยู่ ณ ประเทศสิงคโปร์[14] เอเปคมีการดำเนินการในรูปกลุ่มความร่วมมือ โดยไม่จัดตั้งเป็นรูปแบบองค์กรถาวรเหมือนกลุ่มประเทศอาเซียน (ASEAN) หรือสหภาพยุโรป (European Union) ดังนั้นการดำเนินงานต่างๆ จะเป็นในรูปของมติที่เป็นเอกฉันท์ (Consensus) และความร่วมมือ (Cooperation)

การกำหนดกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปค (APEC Privacy Framework) มีเพื่อส่งเสริมเศรษฐกิจการค้าเสรีระหว่างสมาชิก โดยให้สมาชิกซึ่งมีกฎหมายและวิธีการดำเนินงานใน

[14]ข้อมูลจากสำนักงานนโยบายและแผนพลังงาน กระทรวงพลังงาน, http://www.eppo.go.th/inter/apec/int-APEC-summary-T.html, เมื่อวันที่ 25 สิงหาคม 2557.

การคุ้มครองข้อมูลส่วนบุคคลที่มีความแตกต่างกันสามารถนำไปปรับใช้ให้เหมาะสม วัตถุประสงค์ของกรอบการคุ้มครองฯ กำหนดมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคล (Minimum privacy standard) เพื่อสนับสนุนการส่งผ่านข้อมูลภายในเขตเศรษฐกิจสมาชิก (free flow of personal data)

ในช่วงก่อนปี ค.ศ. 2003 (พ.ศ. 2546) การพัฒนากฎหมายและระเบียบเกี่ยวกับข้อมูลส่วนบุคคลของเอเปคยังอยู่ในวงจำกัดจนกระทั่งในปี ค.ศ. 2003 รัฐบาลออสเตรเลียได้เสนอแก่ที่ประชุมให้เอเปคนำแนวทางการคุ้มครองข้อมูลส่วนบุคคลขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD guidelines of 1981) มาเป็นแนวทางในการกำหนดกรอบการคุ้มครองฯ ของเอเปค หลังจากที่ผ่านการพิจารณาและแก้ไขร่าง การประชุมระดับรัฐมนตรี (APEC Ministerial Meeting) ที่ประเทศชิลี ได้ประกาศกรอบการคุ้มครองข้อมูลส่วนบุคคลในเดือนพฤศจิกายน ค.ศ. 2004 (พ.ศ. 2547) วัตถุประสงค์หลักของกรอบการคุ้มครองฯ คือรักษาความปลอดภัยและความต่อเนื่องของข้อมูลที่ส่งผ่านธุรกรรมอิเล็กทรอนิกส์ทั้งในภาคธุรกิจ ผู้บริโภค และรัฐบาล และเพิ่มประสิทธิภาพและลดค่าใช้จ่ายในการส่งผ่านข้อมูล ในขณะเดียวกัน ก็ช่วยลดข้อจำกัดในการไหลเวียนของข้อมูลส่วนบุคคลระหว่างประเทศในเขตเศรษฐกิจของสมาชิก กรอบการคุ้มครองฯ กำหนดหลักการที่สำคัญ จำนวน 9 ข้อ ดังนี้

1. Preventing harm: เพื่อเป็นการรักษาผลประโยชน์ของบุคคลในเรื่องสิทธิความเป็นส่วนตัว จึงต้องมีการกำหนดมาตรการการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันการใช้ข้อมูลโดยมิชอบ

2. Notice: ต้องแจ้งเจ้าของข้อมูลอย่างชัดเจน ว่าจะมีการเก็บข้อมูลส่วนบุคคล วัตถุประสงค์ของการจัดเก็บ ประเภทบุคคลหรือองค์กรที่ข้อมูลดังกล่าวอาจจะได้รับการเปิดเผย การเข้าถึง และการแก้ไข

3. Collection limitation: ต้องมีการจัดเก็บอย่างจำกัดเท่าที่เป็นไปตามวัตถุประสงค์ของการเก็บเท่านั้น การจัดเก็บต้องทำโดยวิธีที่ถูกต้องตามกฎหมายกำหนด ด้วยวิธีการที่เป็นธรรมและเหมาะสม โดยได้แจ้งและได้รับความยินยอมจากเจ้าของข้อมูลแล้ว

4. Use: ข้อมูลที่เก็บไว้จะเอาไปใช้ได้เฉพาะตามวัตถุประสงค์ของการจัดเก็บเท่านั้น เว้นแต่ได้รับคำยินยอมจากเจ้าของข้อมูลหรือเป็นไปตามข้อยกเว้นตามที่กฎหมายกำหนด

5. Choice: เจ้าของข้อมูลมีสิทธิเลือกว่าจะยินยอมให้มีการจัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลของตน

6. Security safeguards: ข้อมูลที่จัดเก็บต้องมีความถูกต้อง สมบูรณ์ เป็นปัจจุบันตามความจำเป็นและตามวัตถุประสงค์ของการจัดเก็บ

7. Integrity: ต้องมีมาตรการคุ้มครองข้อมูลอย่างเหมาะสมเพื่อป้องกันอันตรายและความเสียหายที่อาจเกิดขึ้น เช่น การสูญหาย เสียหาย และการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การทำลายโดยไม่ได้รับอนุญาต การใช้ ปรับเปลี่ยน แก้ไข หรือการเปิดเผยข้อมูลโดยมิชอบ

8. Access and correction: เจ้าของข้อมูลมีสิทธิรับรู้ว่ามีการเก็บข้อมูลส่วนบุคคลของตน มีสิทธิเข้าถึงข้อมูลของตนเอง และมีสิทธิขอให้ตรวจสอบความถูกต้อง และขอให้ปรับปรุง แก้ไข เพิ่มเติม หรือทำลายข้อมูลของตน

9. Accountability (Including due diligence in transfers): ผู้เก็บข้อมูลจะต้องรับผิดชอบการจัดมาตรการต่างๆ ให้เป็นไปตามหลักเกณฑ์หรือกรอบการคุ้มครองดังกล่าว การส่งข้อมูลส่วนบุคคลไปยังบุคคลหรือองค์การอื่นๆ ทั้งภายในประเทศหรือระหว่างประเทศจะต้องได้รับคำยินยอมจากเจ้าของข้อมูล และจะต้องมีมาตรการที่เหมาะสมที่ประกันได้ว่าบุคคลหรือองค์กรที่ได้รับข้อมูลไปแล้วจะเก็บรักษาข้อมูลให้เป็นไปตามหลักเกณฑ์นี้

อย่างไรก็ตาม กรอบการคุ้มครองฯ ของเอเปคถูกนำไปเปรียบเทียบกับการคุ้มครองข้อมูลส่วนบุคคลภายใต้ข้อบังคับของสหภาพยุโรป (EU Directive) และการคุ้มครองข้อมูลส่วนบุคคลตามข้อตกลง (Convention) ของรัฐสภาแห่งยุโรป (Council of Europe) ซึ่งกรอบการคุ้มครองฯ มีความแตกต่างที่ชัดเจนกับแนวปฏิบัติของยุโรปในหลักการข้อที่ 1 และ 9[15] กล่าวคือ กรอบการคุ้มครองฯ ไม่ครอบคลุมประเด็นสำคัญ อาทิ การประมวลผลโดยวิธีอัตโนมัติ (Automated processing) ซึ่งถือเป็นประเด็นสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป และรัฐสภาแห่งยุโรป นอกจากนั้น นักวิชาการและนักกฎหมายได้วิจารณ์เกี่ยวกับจุดบกพร่องในการคุ้มครองการจัดเก็บและใช้ข้อมูลส่วนบุคคลที่กำหนดในกรอบการคุ้มครองฯ (Greenleaf, 2006) กล่าวคือ กรอบการคุ้มครองฯ ไม่ได้แก้ไขจุดอ่อนที่มีในแนวปฏิบัติเกี่ยวกับข้อมูลส่วนบุคคลขององค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD) อาทิ กรอบการคุ้มครองฯ อนุญาตให้มีการใช้ข้อมูลระดับทุติยภูมิสำหรับการใช้ข้อมูลที่มีวัตถุประสงค์ในการใช้งานที่สอดคล้องหรือเกี่ยวข้องกัน หลักการจำกัดการจัดเก็บข้อมูลก็ไม่ได้แก้ไขช่องว่างที่ปรากฏในแนวปฏิบัติขององค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD)

แม้ว่ากรอบการคุ้มครองฯ ได้ปรับปรุงแนวปฏิบัติของ OECD โดยการเพิ่มเติมในส่วนของการแจ้งเจ้าของข้อมูลในการจัดเก็บ เปิดเผย เข้าถึงและแก้ไข (Notice) แต่ในส่วนของการกำหนดข้อยกเว้นในการอนุญาตให้จัดเก็บและใช้ข้อมูล กรอบการคุ้มครองฯ กลับกำหนดมาตรฐานที่ต่ำกว่า

[15] **Implementing the APEC Privacy Framework: A New Approach,** https://privacyassociation.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/ ข้อมูลเมื่อวันที่ 25 สิงหาคม 2557.

แนวปฏิบัติของ OECD และไม่ได้ระบุหลักการกำหนดวัตถุประสงค์ (Purpose specification) และหลักการเปิดเผยข้อมูล (Openness principle) ที่ถือเป็นหลักการสำคัญในแนวปฏิบัติของ OECD

นอกจากนี้ นักวิชาการยังได้วิจารณ์ว่ากรอบการคุ้มครองฯ ไม่ได้พิจารณานำเอากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิก หรือเขตเศรษฐกิจที่กฎหมายดังกล่าวมีความชัดเจนและเข้มแข็งและเหมาะสมที่จะนำมาปรับใช้ เช่น กฎหมายของสาธารณรัฐเกาหลี จีนฮ่องกง ออสเตรเลีย นิวซีแลนด์ และแคนาดา ซึ่งประเทศเหล่านี้มีการใช้กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลมานานกว่า 17 ปี ซึ่งเอเปคสามารถนำมาอ้างอิงและใช้เป็นมาตรฐานได้

ในการนำหลักการทั้ง 9 ประการที่บัญญัติไว้ในกรอบการคุ้มครองฯ ของเอเปคดังกล่าวมาปฏิบัติ กรอบของเอเปคไม่ได้มีการกำหนดรูปแบบหรือมาตรฐานในการนำไปใช้งาน และไม่ได้กำหนดให้สมาชิกต้องตรากฎหมายเฉพาะแต่ประการใด อนึ่ง กรอบการคุ้มครองฯ ได้กำหนดแนวทางในการนำกรอบการคุ้มครองฯ ไปใช้งานในลักษณะข้อแนะนำที่สมาชิกสามารถนำไปปรับใช้ให้เหมาะสม โดยแบ่งออกเป็นการใช้งานภายในเขตเศรษฐกิจ และการใช้งานระหว่างประเทศ สำหรับการนำกรอบการคุ้มครองฯ ไปปฏิบัติ**ภายในเขตเศรษฐกิจของสมาชิก** สมาชิกสามารถเลือกใช้รูปแบบและวิธีการที่เห็นว่าเหมาะสมกับการดำเนินงานภาย ซึ่งสามารถกระทำผ่านการออกเป็นกฎหมาย การดำเนินงานของหน่วยงานภาครัฐ หรือการที่เอกชนและภาคธุรกิจกำหนดกฎเกณฑ์ขึ้นใช้เอง หรือเป็นการผสมผสานรูปแบบและวิธีการที่กล่าวมาทั้งหมด ทั้งนี้ ควรมีหน่วยงานหรือองค์กรที่เป็นผู้รักษาการตามกรอบการคุ้มครองฯ และเป็นศูนย์รวมของการดำเนินการและประสานงานภายในเขตเศรษฐกิจ โดยการคุ้มครองความเป็นส่วนตัวผ่านการใช้งานกรอบการคุ้มครองฯ จะต้องไม่ขัดขวางการรักษาความมั่นคงความปลอดภัยของสาธารณะและพันธกิจของนโยบายสาธารณะของสมาชิก

ในส่วนของ**การแลกเปลี่ยนข้อมูลระหว่างสมาชิก** แต่สมาชิกเขตเศรษฐกิจมีรูปแบบในการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน กล่าวคือ บางเขตเศรษฐกิจอาจกำหนดเป็นนโยบายและกฎหมายเฉพาะ ในขณะที่บางเขตเศรษฐกิจอาจใช้วิธีให้ภาคธุรกิจออกนโยบายความเป็นส่วนบุคคลเพื่อกำกับการปฏิบัติกับข้อมูลส่วนบุคคลในหน่วยของตนเอง (Self-regulation) กรอบการคุ้มครองฯ จึงได้กำหนดแนวทางการสร้างความร่วมมือระหว่างสมาชิกในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลข้ามพรมแดน (Cross-border cooperation) โดยอาจจะอยู่ในลักษณะทวิภาคี หรือพหุภาคี ทั้งนี้ประเด็นที่สำคัญของกรอบเอเปคคือการพัฒนาแนวทางในการคุ้มครองข้อมูลส่วนบุคคลข้ามพรมแดน (Cross-border Privacy Rules (CBPR)) ที่เป็นที่ยอมรับร่วมกันระหว่างสมาชิก (Mutual acceptance, voluntary system)

อนึ่ง เมื่อเปรียบเทียบกับการคุ้มครองข้อมูลส่วนบุคคลภายใต้ข้อบังคับของสหภาพยุโรป (EU Directive) กรอบการคุ้มครองฯ ของเอเปคมีความแตกต่างในส่วนที่เกี่ยวกับการส่งผ่านข้อมูลส่วนบุคคลไปนอกเขตเศรษฐกิจสมาชิก (Data exports) กล่าวคือกรอบของเอเปคมิได้ห้ามสมาชิกส่ง

ข้อมูลไปยังประเทศที่ไม่ปฏิบัติตามแนวทางหรือไม่มีมาตรฐานการคุ้มครองที่ใกล้เคียงกับกรอบของเอเปค ซึ่งเป็นข้อแตกต่างที่สำคัญระหว่างกรอบการคุ้มครองฯ ของเอเปคกับแนวปฏิบัติของ OECD และ EU Directive นักวิชาการจึงมองว่าการบังคับใช้กรอบการคุ้มครองฯ ของเอเปคจะผลกระทบโดยตรงเพียงเล็กน้อยกับการส่งผ่านข้อมูลส่วนบุคคลระหว่างเอเชีย-แปซิฟิกและสหภาพยุโรป (Greenleaf, 2006, 2009) ทั้งนี้เป็นเพราะกรอบของเอเปคพยายามส่งเสริมการไหลเวียนของข้อมูลส่วนบุคคลระหว่างประเทศเพื่อการค้าเสรี ในขณะที่ปรัชญาของข้อบังคับของสหภาพยุโรปมุ่งเน้นการคุ้มครองความเป็นส่วนบุคคลของปัจเจกชนเป็นสำคัญตามหลักสิทธิมนุษยชน

กล่าวโดยสรุป การคุ้มครองข้อมูลส่วนบุคคลในข้อตกลงระหว่างประเทศ ไม่ว่าจะเป็นแนวทางของ OECD ข้อบังคับสหภาพยุโรป 95/46 หรือข้อตกลงของรัฐสภาแห่งยุโรป ล้วนเป็นกรอบที่ใช้บังคับเกี่ยวกับการส่งและรับข้อมูลข่าวสารระหว่างประเทศ หลักสำคัญประการหนึ่งที่ปรากฏอยู่ในกฎหมายนี้ คือบทบัญญัติว่าด้วยเรื่องการส่งข้อมูลส่วนบุคคลระหว่างประเทศ (International data transfers or Trans-border data flows) ซึ่งกำหนดว่าการแลกเปลี่ยนข้อมูลจะดำเนินการได้เฉพาะระหว่างประเทศที่มีกฎหมายหรือมีมาตรการในการให้ความคุ้มครองข้อมูลส่วนบุคคลที่มีมาตรฐานเพียงพอ กฎเกณฑ์ดังกล่าวเป็นผลมาจากการส่งข้อมูลในบางกรณีที่ต้องอยู่ภายใต้บทบัญญัติระหว่างประเทศ เช่น การส่งข้อมูลไปยังประเทศสมาชิกสหภาพยุโรป ซึ่งต้องปฏิบัติตามข้อบังคับสหภาพยุโรปที่กำหนดมาตรการเพื่อการคุ้มครองข้อมูล โดยได้กำหนดห้ามส่งและรับข้อมูลข่าวสารกับประเทศที่ไม่มีมาตรการที่มีมาตรฐานในการคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคลและมาตรการรักษาความปลอดภัยของข้อมูลข่าวสารอย่างเพียงพอ

เมื่อเปรียบเทียบ APEC Privacy Framework กับกรอบระหว่างประเทศอื่นจะพบว่าเป็นมาตรฐานที่เกิดขึ้นหลังจากมาตรฐานสากลอื่นๆ ของ UN, OECD และ EU ไม่ได้มีลักษณะผูกพันตามกฎหมายในฐานะสนธิสัญญาระหว่างประเทศ ไม่ได้สร้างเงื่อนไขด้านเวลา และไม่ได้สร้างระบบการลงโทษ หรือหน่วยงานตรวจสอบ การยอมรับและปฏิบัติตามมาตรฐานนี้ตั้งอยู่บนหลักของความสมัครใจ หลักเกณฑ์ต่างๆ ของ APEC นั้นเน้นไปที่การคุ้มครองข้อมูลส่วนบุคคลและความเป็นส่วนตัวในบริบทของการค้าระหว่างประเทศ ในลักษณะที่สามารถเกิดขึ้นได้จริงในภูมิภาค มากกว่าจะเน้นย้ำความสำคัญในฐานะสิทธิมนุษยชนตามแบบ UN หรือเน้นไปที่ศักดิ์ศรีความเป็นมนุษย์ตามแบบของ EU

ในแง่ของเนื้อหานั้น APEC Privacy Framework ต้องการจะสร้าง minimum standards ซึ่งอาจจะไปเสริมเนื้อหาของมาตรฐานสากลอื่นๆ และมาตรฐานของกฎหมายภายในที่ดำเนินตามหลักมาตรฐานสากลนั้นๆ ในกรอบของ APEC ได้เพิ่มหลักการสำคัญสองประการ ในสิ่งที่ OECD guidelines และ EU directive นั้นไม่ได้เน้นย้ำมากนัก นั่นก็คือหลักการป้องกันอันตรายและหลักการมีทางเลือก

โดยเฉพาะหลักการมีทางเลือก (Choice) นั้น หากนำไปปฏิบัติอย่างเคร่งครัดน่าจะช่วยนำไปสู่การคุ้มครองอย่างแท้จริงได้ เพราะในสภาพความเป็นจริงแล้ว แม้จะใช้หลักความยินยอมหรือหลักการแจ้งวัตถุประสงค์เป็นมาตรฐาน แต่ภาคธุรกิจก็มักจะใช้การเก็บข้อมูลส่วนบุคคลเป็นเงื่อนไขใน

การให้บริการต่างๆ หรือใช้การแจ้งวัตถุประสงค์กว้างๆ ทั้งที่ไม่จำเป็นเสมอไป ถ้าหากผู้บริโภคต้องการจะใช้บริการก็จำเป็นจะต้องให้ข้อมูลส่วนบุคคลแกผู้ประกอบการไป โดยทางเลือกของผู้บริโภคมีจำกัดเพียงแค่จะให้หรือไม่ให้เท่านั้น ทั้งที่ในความเป็นจริงสามารถสร้างตัวเลือกให้ผู้บริโภคเลือกเองได้ว่าต้องการจะให้ข้อมูลในระดับใด ซึ่งก็จะช่วยป้องกันการนำข้อมูลไปใช้โดยไม่จำเป็น หรือเกินวัตถุประสงค์

นอกจากนี้การสร้างทางเลือกตามความต้องการของผู้บริโภค (customization) ยังเป็นการเพิ่มประสิทธิภาพในการใช้ข้อมูลที่ได้มาให้เกิดประโยชน์สูงสุดสำหรับตัวผู้ประกอบการเองด้วย กล่าวคือ ผู้ประกอบการจะสามารถทราบได้ว่าผู้บริโภครายใดต้องการและเต็มใจรับบริการแบบใดบ้าง ทำให้ลดต้นทุนในการทำการตลาดแบบหว่านแห ลดต้นทุนการเก็บรักษาข้อมูลที่ไม่จำเป็น และไม่สร้างความรำคาญใจให้กับผู้บริโภคโดยใช่เหตุ อันจะทำให้เกิดความไว้วางใจและความสัมพันธ์อันดีระหว่างผู้ประกอบการและผู้บริโภคในระยะยาว ลักษณะเด่นอีกอย่างของ APEC Privacy Framework คือถูกออกแบบมาให้ใช้ได้ทั้งภาครัฐและเอกชน หลักการทั้ง 9 ประการสามารถนำไปใช้เป็นต้นแบบในการออกกฎหมายกำกับการดูแลหน่วยงานภาครัฐ หรือนำไปเป็นหลักการการควบคุมตนเองของภาคเอกชนได้ด้วย

2.6 รูปแบบการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศ

ในปัจจุบันจากการสำรวจบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศต่างๆ ในโลกจะพบว่ามีแนวทางการตรากฎหมายในเรื่องนี้แยกเป็นสองแนวทางที่สำคัญได้แก่

1. การตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะกฎหมายกลาง (Comprehensive law)

แนวทางนี้เป็นการออกกฎหมายหลักเพียงฉบับเดียวที่ครอบคลุมกรณีการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในลักษณะต่างๆ ซึ่งแนวทางการตรากฎหมายเช่นนี้ส่วนใหญ่จะปรากฏอยู่ในประเทศภาคพื้นยุโรป สหราชอาณาจักร และประเทศที่ใช้ระบบประมวลกฎหมาย (Civil Law) ได้แก่ สวีเดน เยอรมัน ฝรั่งเศส เป็นต้น

สำหรับการตรากฎหมายคุ้มครองคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่เป็นการทั่วไปนั้นได้เกิดขึ้นเป็นครั้งแรกในลักษณะที่เป็นกฎหมายระดับมลรัฐ Hessen ซึ่งเป็นรัฐหนึ่งของประเทศเยอรมัน เมื่อปี ค.ศ. 1970 ซึ่งถือว่าเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกในโลก หลังจากนั้นจึงได้มีการตรากฎหมายระดับประเทศของเยอรมันขึ้น ในปี ค.ศ.1977 ซึ่งจากแนวคิดของการออกกฎหมายกลางมาเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคลนี้ ก็ได้เป็นต้นแบบให้ประเทศอีกหลายประทศออกกฎหมายในลักษณะเดียวกันนี้มา เช่น ประเทศสวีเดนในปี ค.ศ.1973 สหรัฐอเมริกาในปี ค.ศ. 1974 และประเทศฝรั่งเศสในปี ค.ศ.1978 เป็นต้น

การตรากฎหมายในลักษณะกลางนี้มักจะมีการจัดตั้งองค์กรกลางที่ทำหน้าที่ดูแลวินิจฉัยกรณีปัญหาการละเมิดข้อมูลข่าวสารส่วนบุคคลที่เกิดขึ้นโดยเฉพาะขึ้นในลักษณะของคณะกรรมการ

(Commissioner) ทั้งนี้องค์กรที่ทำหน้าที่คุ้มครองข้อมูลข่าวสารส่วนบุคคลจะมีการดำเนินงานในสองลักษณะ กล่าวคือ[16]

1) องค์กรที่ทำหน้าที่กำกับดูแล (Regulatory)

ประเทศที่ได้จัดตั้งองค์กรในลักษณะเช่นนี้ได้แก่ ประเทศสวีเดน และประเทศฝรั่งเศส โดยในกรณีประเทศสวีเดนนั้นก็ได้จัดตั้ง Data Inspection Board and National Commission on Informatics and Liberties ซึ่งมีบทบาทหน้าที่ค่อนข้างกว้างขวางในการกำกับดูแลการประมวลข้อมูลในประเทศ อาทิ อำนาจในการอนุญาตหรือไม่อนุญาตให้มีการประมวลผลข้อมูลทั้งโดยหน่วยงานของรัฐและหน่วยงานภาคเอกชน ส่วนในประเทศฝรั่งเศสก็ได้มีการจัดตั้ง Commission Nationale Informatique Liberte's (CNIL) ซึ่งมีบทบาทหน้าที่ในทำนองเดียวกับประเทศสวีเดน แต่จะแตกต่างกันตรงที่มีการจัดตั้งคณะอนุกรรมการ (submissions) ขึ้นเพื่อทำหน้าที่ศึกษาวิจัยเกี่ยวกับข้อมูลทางสถิติ (statistics) การประมวลผลโดยหน่วยงานของรัฐส่วนท้องถิ่น (local government)ด้านเทคโนโลยีและการรักษาความปลอดภัย (technology and security) ขึ้นเป็นการเฉพาะด้วย

อย่างไรก็ตาม การจัดให้องค์กรซึ่งมีโครงสร้างการทำงานที่เป็นอิสระและมีอำนาจหน้าที่กว้างขวางของประเทศสวีเดน และฝรั่งเศสข้างต้น ก็หามีผลให้สามารถคุ้มครองสิทธิความเป็นอยู่ส่วนตัวในข้อมูลส่วนบุคคลของประชาชนได้อย่างมีประสิทธิภาพแต่อย่างใด เนื่องจากมีงบประมาณอย่างจำกัด ในขณะที่มีภาระหน้าที่ซึ่งจะต้องปฏิบัติอยู่เป็นจำนวนมาก ไม่ว่าจะเป็นการรับจดทะเบียนหน่วยงานที่ทำการประมวลผลข้อมูล การไต่สวนข้อร้องเรียน การประชาสัมพันธ์ให้ประชาชนเข้าใจเกี่ยวกับหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล เป็นต้น

2) องค์กรที่ทำหน้าที่ให้คำปรึกษา (Advisory)

ประเทศที่ได้จัดตั้งองค์กรในลักษณะเช่นนี้ได้แก่ ประเทศเยอรมัน ซึ่งได้มีการจัดตั้งกรรมการคุ้มครองข้อมูลส่วนบุคคล (Federal Data Protection Commissioner) ขึ้นเป็นองค์กรหนึ่งในกระทรวงมหาดไทย (Ministry of the Interior) และอยู่ภายใต้การกำกับดูแลของรัฐมนตรีว่าการกระทรวงมหาดไทย

กรรมการคุ้มครองข้อมูลส่วนบุคคลมีบทบาทหน้าที่หลักในการให้คำปรึกษา (advise) ให้ความช่วยเหลือ (assist) และว่ากล่าวตักเตือน (admonish) หน่วยงานต่าง ๆ ในกิจกรรมที่เกี่ยวข้องกับการประมวลผลข้อมูล นอกจากนี้ กรรมการดังกล่าวสามารถยื่นคำร้องเรียนอย่างเป็นทางการ (formal complaints) เกี่ยวกับการประมวลผลข้อมูลที่เห็นว่าไม่ถูกต้องไปยังกระทรวงซึ่งมีหน้าที่รับผิดชอบ แต่ไม่มีอำนาจในการออกคำสั่งหรือให้ดำเนินการอย่างหนึ่งอย่างใดโดยอาศัยอำนาจของกรรมการเอง

ต่อมาประเทศอื่น ๆ ที่บัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นมาภายหลังก็ได้พัฒนารูปแบบขององค์กรหรือหน่วยงานด้านการคุ้มครองข้อมูลส่วนบุคคลในลักษณะที่ผสมผสานกัน

---

[16]ปฏิวัติ อุ่นเรือน, **"ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ",** (สารนิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2547), น. 16-17.

ระหว่างหลักการกำกับดูแลซึ่งใช้อยู่ในประเทศสวีเดนและฝรั่งเศส และหลักการให้คำปรึกษาที่ใช้อยู่ในประเทศเยอรมัน ด้วยเหตุนี้เองจึงทำให้ระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลในภาคพื้นยุโรปในช่วงต้นมีความแตกต่างกันค่อนข้างมาก

อย่างไรก็ตาม ต่อมาภายหลังประเทศต่าง ๆ ในภาคพื้นยุโรปก็ได้มีการบัญญัติกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความสอดคล้องและเป็นไปในทิศทางเดียวกันมากขึ้น เนื่องจากได้มีการพัฒนากรอบนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลในระดับสากลโดยองค์การระหว่างประเทศต่าง ๆ อาทิ การออกแนวปฏิบัติด้านการคุ้มครองความเป็นอยู่ส่วนตัวและการโอนข้อมูลส่วนบุคคลระหว่างประเทศ (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data) โดยองค์การเพื่อเศรษฐกิจและการพัฒนา (OECD) ในปี ค.ศ.1980 ซึ่งมีวัตถุประสงค์เพื่อให้ข้อเสนอแนะแก่ประเทศสมาชิกในการนำเอาหลักการคุ้มครองข้อมูลส่วนบุคคลขั้นพื้นฐาน (basic principles) ไปใช้บังคับในประเทศสมาชิก ซึ่งอาจอยู่ในรูปของการบัญญัติกฎหมายหรือมาตรการอื่นใดที่มีสภาพบังคับได้ โดยหลักการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวมีทั้งสิ้น 8 ประการ ซึ่งได้กลายเป็นมาตรฐานให้นานาประเทศยึดเป็นหลักเพื่อใช้ในการตรากฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลขึ้นสำหรับประเทศตน

2. การตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะของกฎหมายเฉพาะ แยกเป็นเรื่อง ๆ (Sectoral law & self-regulations)

แนวทางนี้จะพบได้ในประเทศสหรัฐอเมริกา ที่แม้จะมีการบังคับใช้กฎหมายคุ้มครองสิทธิส่วนบุคคล (Privacy Act 1974) ซึ่งเป็นกฎหมายหลักคุ้มครองอยู่แล้วก็ตาม แต่รัฐสภาจะตรากฎหมายเฉพาะออกมาเมื่อ ถึงคราวเกิดปัญหาการป้องกันความลับหรือความเป็นอยู่ส่วนตัวของประชาชนถูกละเมิดขึ้นที่มีลักษณะพิเศษ ก็จะออกกฎหมายเรื่องนั้นๆมาแก้ปัญหา อาทิเช่น [17]

กรณีการตรากฎหมาย The Driver Privacy Protection Act เนื่องจากว่านักแสดงหญิงชื่อว่า Rebecca Shaeffer ได้ถูกฆาตกรรมที่บ้านของเธอเองเมื่อปี 1988 คนซึ่งคนร้ายสามารถสืบหาที่อยู่ของเธอได้โดยการหาข้อมูลจากใบขับขี่ของเธอจาก California Department of Motor Vehicles

กรณีการตรากฎหมาย The Video Privacy Protection Act เนื่องจากผู้พิพากษา Robert Bork ได้เสนอชื่อให้เป็นที่ผู้ชิงตำแหน่งผู้พิพากษาศาลสูงของสหรัฐอเมริกา และปรากฏว่ามีผู้สื่อข่าวขอและเผยแพร่ข้อมูลการเช่าวิดีโอเทป ของผู้พิพากษาท่านนี้ ปรากฏว่ามีรายการวิดีโอเทปเกี่ยวกับหนังโป๊หรือภาพลามกอนาจาร (pornography) อยู่ด้วย ทำให้มีการวิพากษ์วิจารณ์ถึงความประพฤติของผู้พิพากษาท่านนี้ เป็นเหตุให้ท่านไม่ได้รับการคัดเลือกเป็นผู้พิพากษาศาลสูง

[17]ประสิทธิ์ ปิวาวัฒนาพานิช, "กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสหรัฐอเมริกาและประเทศออสเตรเลีย", **วารสารนิติศาสตร์** (ปีที่ 34 ธันวาคม 2547), น. 537-538.

กรณีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวกับข้อมูลทางการเงิน เรียกว่า Gramm-Leach-Bliley Financial Modernization Act 1999 เนื่องจากมีบริษัทเอกชนชื่อว่า U.S. Bankcorp ได้เปิดเผยเลขบัญชีของลูกค้าแก่บุคคลภายนอกซึ่งเป็นบุคคลที่สามโดยปราศจากความยินยอมของลูกค้า

นอกเหนือจากกฎหมายสามฉบับที่ยกมาข้างต้น แล้วก็ยังมีกฎหมายเฉพาะอื่นๆที่ได้รับการตราขึ้นในสหรัฐอเมริกา เช่น Fair Credit Reporting Act 1970 ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์เพื่อควบคุมการใช้ข้อมูลเครดิตของภาคธุรกิจ โดยการกำหนดหลักเกณฑ์ที่สำคัญ อาทิ ผู้มีสิทธิใช้ข้อมูลเครดิต การจำกัดการเปิดเผยข้อมูลเครดิต ตลอดจนการให้สิทธิแก่ผู้บริโภคในการเข้าถึง หรือแก้ไขข้อมูลเครดิตของตนให้ถูกต้อง กฎหมาย Health Insurance Portability and Accountability Act 1996 ซึ่งตราขึ้นเพื่อคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวข้องกับการรักษาพยาบาล Children 's On line Privacy Protection Act 1998 ซึ่งเป็นกฎหมายที่มีวัตถุประสงค์ห้ามไม่ให้ผู้ประกอบกิจการพาณิชย์อิเล็กทรอนิกส์ และบริการแบบออนไลน์ต่างๆ ทำการเก็บรวบรวมข้อมูลจากผู้เยี่ยมชมเว็บไซต์หรือผู้ใช้บริการที่เป็นเด็กอายุต่ำกว่า 13 ปี เว้นแต่ผู้ประกอบการที่ได้ใช้กลไกการกำกับดูแลตนเอง ซึ่งได้ผ่านความเห็นชอบจากคณะกรรมาธิการการค้า (FTC)

กฎหมาย Financial Modernization Act 1999 ซึ่งได้ตราขึ้นเพื่อให้สถาบันการเงินต่างๆ เพิ่มระดับการคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคในกิจกรรมที่เกี่ยวข้องทางการเงินเพิ่มมากขึ้น อาทิ การประกาศนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคลให้ลูกค้าทราบ และหน้าที่ในการปฏิบัติตามข้อเรียกร้องของผู้บริโภคที่เกี่ยวกับข้อมูลส่วนบุคคล เป็นต้น

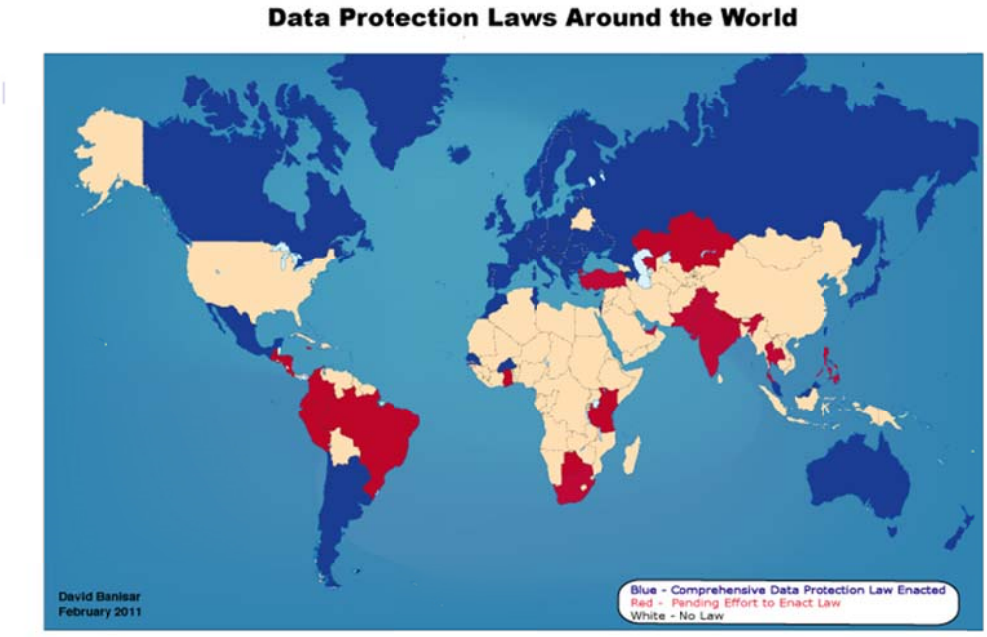
ทั้งนี้แนวคิดของประเทศสหรัฐอเมริกาที่เลือกจะตรากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลเป็นเรื่องๆนั้น มีข้อวิเคราะห์ที่น่าสนใจซึ่งศึกษาไว้โดยประสิทธิ์ ปิวาวัฒนาพานิช วิเคราะห์ว่าอาจมีเหตุผลจาก ปรัชญาหรือที่มาทางประวัติศาสตร์สร้างชาติของประเทศสหรัฐอเมริกาที่พยายามจะมิให้เจ้าหน้าที่ของรัฐลิดรอนสิทธิเสรีภาพของประชาชน ในขณะเดียวกัน ประชาชนก็มีสิทธิเสรีภาพที่จะดำเนินธุรกิจแบบทุนนิยมหรือ Free enterprise อันเป็นปรัชญาที่ชาวอเมริกันยึดถือมาเป็นเวลานาน ซึ่งโดยทั่วไปแล้วในประเทศสหรัฐอเมริกาไม่มีกฎหมายให้ประชาชนต้องให้ความยินยอมในเรื่องประมวลผลข้อมูล การจัดทำการตลาดและการขายข้อมูลส่วนบุคคลให้กับบุคคลที่สาม ดังนั้น อเมริกาจึงมีบริษัทขนาดใหญ่หลายแห่งที่ทำธุรกิจเกี่ยวกับการจัดเก็บและขายข้อมูลส่วนบุคคลของคนอเมริกัน เช่น บริษัทCatalina Marketing Corporation บริษัท Aristotle Industries บริษัท Winland Services เป็นต้น

นอกจากนั้น ประเทศสหรัฐอเมริกา ยังได้ให้ความสำคัญเกี่ยวกับ Freedom access มากกว่า Privacy ซึ่งเห็นได้จากบทบัญญัติของกฎหมายหลายฉบับที่รัฐบาลกลางปล่อยให้เอกชนดูแลควบคุมกันเอง ด้วยการให้เอกชนออก Self- regulations แล้วเจ้าหน้าที่ของรัฐจะควบคุมอีกที่หนึ่ง เช่น Federal Trade Commission (FTC) ซึ่งการควบคุมกันเองนี้มีข้อดีในเรื่องของความยืดหยุ่นในการสามารถแก้ไขปัญหาได้ทันท่วงทีสอดคล้องกับความเปลี่ยนแปลงด้านเทคโนโลยีที่รวดเร็ว ทั้งนี้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหรัฐอเมริกาหลายฉบับ ยังมีลักษณะพิเศษที่ให้สิทธิเจ้าของ

ข้อมูลที่ถูกละเมิดสามารถดำเนินคดีทางศาลได้อย่างเต็มที่โดยที่ศาลสามารถกำหนดค่าเสียหายในเชิงลงโทษแก่ผู้กระทำละเมิดได้ด้วยซึ่งเรียกว่า punitive damages

อย่างไรก็ตาม เมื่อศึกษาวิเคราะห์ลงไปในเนื้อหาของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ประเทศต่างในโลกได้ประกาศใช้ก็จะพบว่ามีกรอบมาตรฐานในทางระหว่างประเทศที่สำคัญ คือ มาตรฐานของสหภาพยุโรปตาม ข้อบังคับสหภาพยุโรป 95/46 และมาตรฐานของสหรัฐอเมริกาตามกรอบของ APEC Privacy Framework ซึ่งในทางวิชาการต่างก็เห็นว่ามาตรฐานของสหภาพยุโรปค่อนข้างจะมีหลักเกณฑ์ที่เข้มงวดในการคุ้มครองข้อมูลส่วนบุคคลมากกว่ากรอบของเอเปคที่มีความยืดหยุ่นมากกว่า

ดังนั้น เมื่อประเทศใดต้องการตรากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลขึ้นบังคับใช้ในประเทศก็จำเป็นต้องพิจารณาว่าจะเลือกใช้มาตรฐานของกลุ่มประเทศใดเป็นแนวทางในการตรากฎหมายขึ้น ทั้งนี้ปัจจุบัน(พ.ศ. 2557) ได้มีประเทศต่าง ๆในโลกมากกว่า 100 ประเทศที่มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้แล้วโดยสามารถพิจารณาได้จากภาพแผนที่ซึ่งจัดทำโดย David Banlsar ที่เผยแพร่ในเว็บไซต์ www.privacyinternational.org ดังนี้



บทที่ 3
กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประชาคมอาเซียน

3.1 ภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประชาคมอาเซียน

ประชาคมอาเซียน มีจุดเริ่มจากการถือกำเนิดสมาคมอาเซียน (ASEAN : Association of South East Asian Nations) ที่ก่อตั้งมาตั้งแต่ปี ค.ศ.1967 (พ.ศ. 2510) ปัจจุบันมีประเทศสมาชิกอยู่รวมกัน 10 ประเทศ ได้แก่ บรูไนดารุสซาลาม ราชอาณาจักรกัมพูชา สาธารณรัฐอินโดนีเซีย สาธารณรัฐประชาธิปไตยประชาชนลาว สหพันธรัฐมาเลเซีย สหภาพเมียร์มาร์ สาธารณรัฐฟิลิปปินส์ สาธารณรัฐสิงคโปร์ สาธารณรัฐสังคมนิยมเวียดนาม และราชอาณาจักรไทย

เมื่อพิจารณาถึงสถานภาพปัจจุบันในปีพ.ศ. 2557 (คศ.2014) ประเทศที่ได้มีการตรากฎหมายที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลแล้ว ได้แก่ อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ สิงคโปร์[18] ขณะที่ ค.ศ.2000 ยังไม่มีประเทศใดในอาเซียนที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่หากมาถึงในช่วงปีค.ศ. 2010 เป็นต้นมา 4 ประเทศในภูมิภาคนี้คือ อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์ ได้ผ่านกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความทันสมัย สอดคล้องกับมาตรฐานสากลต่างๆ และประกอบด้วยรายละเอียดชัดเจน โดยเริ่มมีผลบังคับใช้จริงในระยะใกล้เคียงกันคือช่วงปี ค.ศ.2012-2013 ซึ่งต่างก็มุ่งคุ้มครอบข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ใช้ และเผยแพร่โดยภาคเอกชน โดยกำหนดมาตรการที่สอดคล้องกับหลักสากล เช่น หลักความยินยอม หลักการแจ้งวัตถุประสงค์ หลักความปลอดภัย โดยเฉพาะมาตรการเกี่ยวกับการส่งข้อมูลไปต่างประเทศ (transfer of data) ต่างมีการจำกัดประเภทของข้อมูลที่สามารถส่งต่อไปต่างประเทศ และกำหนดเงื่อนไขให้ต้องได้รับความยินยอมหรือให้มีหลักประกันว่าประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลไม่ด้อยไปกว่าประเทศตน

ประเทศเพื่อนบ้านเหล่านี้ นอกจะมีความสัมพันธ์กับไทยในแง่ของการค้าอย่างมากแล้ว ยังต่างเป็นผู้เล่นที่สำคัญในการพัฒนาระบบเศรษฐกิจและสังคมของภูมิภาคอาเซียนอีกด้วย ประเทศมาเลเซียเป็นกรณีศึกษาที่น่าสนใจ เนื่องจากการผลักดันกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีความเชื่อมโยงอย่างชัดเจนกับแผนเศรษฐกิจของประเทศที่ต้องการให้มาเลเซียเป็นศูนย์กลางการบริการด้าน

[18]สำหรับประเทศอื่นๆในภูมิภาคอาเซียนมีข้อพิจารณาที่น่าสนใจว่าบางประเทศแม้ยังไม่มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะแต่ก็มีกฎหมายที่มีบทบัญญัติคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง ได้แก่ ประเทศไทยมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่บัญญัติการคุ้มครองข้อมูลส่วนบุคคลในภาครัฐ ประเทศเวียดนามในปีค.ศ.2010 ได้มีการประกาศใช้ Law 59 ที่ถือว่าเป็นการคุ้มครองข้อมูลของผู้บริโภค Consumer Rights Protection Law ซึ่งมีผลวันที่ 1 กรกฎาคม 2011 ในประเทศบรูไนมีการคุ้มครองในส่วนกฎหมายทรัพย์สินทางปัญญา เครื่องหมายการค้า กฎหมายลิขสิทธ์ ในส่วนที่เป็นข้อมูลความลับทั่วไปก็ได้รับการคุ้มครองตามหลักกฎหมายCommon Law และหลัก Equity ขณะที่ประเทศในกลุ่มอาเซียนที่ยังไม่มีความคืบหน้าในการเตรียมการออกกฎหมายคือ เมียร์มาร์ ลาวและกัมพูชา.

เทคโนโลยีโทรคมนาคม (IT Hub) เห็นได้จากการจัดตั้งองค์กร The Multimedia Development Corporation (MDC) เพื่อสนับสนุนการพัฒนาของอุตสาหกรรม ICT ตั้งแต่ขนาดกลางและขนาดเล็ก (SMEs) ให้สามารถเติบโตเป็นธุรกิจระดับโลกได้และมีเป้าหมายการแข่งขันกับประเทศในภูมิภาคเช่น สิงคโปร์อย่างชัดเจน นอกจากนี้ยังได้กำหนดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) เป็นองค์กรอิสระที่กำกับดูแลการบังคับใช้กฎหมายและออกแนวปฏิบัติ (guidelines) ต่างๆ ด้วย แสดงให้เห็นว่ามีความพยายามของภาครัฐที่จะทำให้กฎและข้อบังคับต่างๆ สามารถบังคับใช้ได้จริง และเป็นไปในทางที่ไม่เป็นอุปสรรคกีดขวางการเจริญเติบโตทางเศรษฐกิจ

ปัจจุบัน ประเทศมาเลเซียอยู่ในระยะเริ่มต้นบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล หน่วยงานต่างๆ โดยเฉพาะภาคเอกชนมีความตื่นตัวในการแลกเปลี่ยนข้อมูลเพื่อหาแนวทางปฏิบัติตามกฎหมายกันอย่างมาก องค์กรในภาคการเงินที่มีมาตรฐานการคุ้มครองข้อมูลค่อนข้างสูงอยู่แล้วเป็นแนวหน้าในการปฏิบัติตามกฎหมายและแบ่งปันแนวปฏิบัติให้ภาคธุรกิจส่วนอื่นๆ ด้วย อนึ่ง แต่เดิมองค์กรที่มีความเชื่อมโยงกับบริษัทในต่างประเทศโดยเฉพาะประเทศใน EU ต่างก็มีแนวปฏิบัติที่เป็นมาตรฐานสากลซึ่งสูงกว่ามาตรฐานใหม่ตามกฎหมายของมาเลเซียอยู่แล้ว เนื่องจากบริษัทเหล่านี้มักจะต้องเพิ่มเติม Standard Contractual Clauses หรือ Binding Corporate Rules เพื่อให้ปฏิบัติตามมาตรฐานของประเทศต้นทางข้อมูลอยู่แล้ว จึงไม่ค่อยมีปัญหาในการปฏิบัติตามกฎหมายใหม่ ข้อสำคัญคือการแบ่งปันความรู้และประสบการณ์ไปสู่ผู้ประกอบการขนาดกลางและขนาดเล็กอื่นๆ ที่เริ่มต้องเกี่ยวข้องกับการรับส่งข้อมูลไปต่างประเทศ

เมื่อศึกษาวิเคราะห์ถึงประสบการณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน 4 ประเทศ เราอาจสรุปถึงมีลักษณะสำคัญที่ค้นพบ ดังต่อไปนี้

1. การปฏิบัติตามมาตรฐานสากล (standardization)

เราสามารถสรุปท่าทีของประเทศต่างๆ ในภูมิภาคเอเชียแปซิฟิคต่อการคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นไปในทิศทางเดียวกัน คือจำเป็นต้องมีการยกระดับมาตรฐานการคุ้มครองให้มากขึ้น มิใช่เพื่อรักษาสิทธิของบุคคลเพียงอย่างเดียว แต่การมีมาตรฐานที่ชัดเจนนั้นเป็นการเพิ่มพูนโอกาสทางเศรษฐกิจให้กับเอกชนของประเทศตนด้วย กล่าวคือ ทั้งภาครัฐและเอกชนต่างตระหนักถึงความจำเป็นในการสร้างสมดุล (balance) ระหว่าง “การคุ้มครองความเป็นส่วนตัว (privacy protection)” กับ “การส่งเสริมการเคลื่อนไหวเสรีของข้อมูล (free flow of information)” ซึ่งนำไปสู่ในการการสร้างโอกาสทางการแข่งขันเชิงเศรษฐกิจ เนื่องจากการเพิ่มความไว้วางใจของผู้บริโภคทั้งในประเทศตนเองและในต่างประเทศเป็นกุญแจสำคัญในการเพิ่มขีดความสามารถในการแข่งขันสำหรับธุรกิจที่ต้องจัดการกับข้อมูลส่วนบุคคลจำนวนมาก ไม่ว่าจะเป็นธุรกิจเชิงไอทีที่มีจุดขายอยู่ที่การเคลื่อนย้ายข้อมูลอย่างยืดหยุ่นและเสรี หรือธุรกิจบริการที่เกี่ยวข้องกับการตอบสนองความต้องการของลูกค้ารายคนที่จำเป็นจะต้องล่วงรู้และรักษาข้อมูลที่อาจจะเกี่ยวข้องกับข้อมูลที่เป็นข้อมูลส่วนตัวโดยเฉพาะ (sensitive data) ของลูกค้าด้วย

แม้ว่าแต่ละประเทศต่างมีความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคลต่างๆ กันไปตามสภาพเศรษฐกิจและสังคม ประชากรในแต่ละประเทศก็อาจมีทัศนคติและความไว้วางใจในการเปิดเผย

ข้อมูลแตกต่างกัน หากแต่ทุกประเทศก็คำนึงถึงความสอดคล้องระหว่างมาตรการภายในประเทศกับมาตรฐานสากล พยายามปรับปรุงให้ระบบการคุ้มครองนั้นมีความทันสมัยอยู่เสมอทั้งในเชิงของกฎหมาย และในเชิงของเทคโนโลยี

2. การคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาทางเศรษฐกิจ

การพัฒนาทางเศรษฐกิจอย่างยั่งยืนจำเป็นจะต้องดำเนินไปโดยคำนึงถึงผลกระทบในด้านอื่นๆ เช่นเดียวกับการลงทุนในภาคอุตสาหกรรมที่ไม่ควรจะต้องแลกมาด้วยการทำลายสภาพแวดล้อม การลงทุนในภาคการบริการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเพื่อสร้างคุณภาพชีวิตที่ดีขึ้นก็ไม่ควรจะต้องสละแลกกับความเป็นส่วนตัว จนนำมาซึ่งความหวาดระแวงเทคโนโลยีอันไม่จำเป็นและอาจจะกลายเป็นอุปสรรคต่อการพัฒนานวัตกรรมใหม่ๆ ได้

การสร้างมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่ด้อยไปกว่าประเทศอื่นๆ และสอดคล้องกับมาตรฐานสากลจึงเป็นพื้นฐานที่จำเป็นต่อการพัฒนาธุรกิจบริการในอนาคตให้มีความสามารถแข่งขันกับนานาชาติ นอกจากนี้ยังช่วยสร้างวัฒนธรรมการเคารพสิทธิส่วนบุคคลให้เกิดขึ้นในสังคม รวมทั้งจะช่วยสร้างความตระหนักรู้ในสิทธิที่จะเข้าถึง ปกป้อง และควบคุมข้อมูลส่วนบุคคลของเอกชนให้เกิดขึ้น ทำให้เกิดความเข้าใจระหว่างผู้ประกอบการและผู้บริโภค ลดต้นทุนของผู้ประกอบการในการสร้างภาพเพื่อเรียกความน่าเชื่อถือ และมีความคล่องตัวในการใช้ข้อมูลที่เก็บมาให้เป็นประโยชน์อย่างแท้จริง

3. การยอมรับมาตรฐานสากล และกรอบความร่วมมือระหว่างประเทศ

ปัจจุบัน มีมาตรฐานสากลหลากหลายที่กำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ทั้ง OECD Guidelines ที่ไม่มีผลผูกพันทางกฎหมายแต่มีอิทธิพลต่อการร่างกฎหมายของหลายประเภท และ EU Directive ที่สร้างมาตรฐานอันเคร่งครัดของยุโรปซึ่งส่งผลกระทบให้คู่ค้าของยุโรปต้องเร่งจัดทำกฎเกณฑ์ภายในของตนให้มีมาตรฐานไม่ต่ำกว่าของยุโรปด้วย

นอกจากการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะเพื่อให้เกิดการบังคับใช้จริง และเพื่อให้มีหน่วยงานกำกับดูแลแล้ว สำหรับประเทศไทยควรจะยอมรับมาตรฐานสากลในกรอบความร่วมมือระหว่างประเทศด้วย เพื่อแสดงจุดยืนว่าการบังคับใช้กฎหมายภายในของไทยเป็นไปตามมาตรฐานสากล และเปิดโอกาสในการเรียนรู้แบ่งปันพัฒนาการด้านกฎหมายต่างๆ ของประเทศในกรอบความร่วมมือ (best practice sharing) เพื่อปรับปรุงระบบภายในให้ทันยุคทันสมัยอีกด้วย ซึ่งภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของอินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์สามารถสรุปได้ ดังนี้

ตารางสรุปข้อมูลเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มอาเซียนที่เป็นกรณีศึกษา

ประเด็น/ประเทศ	Indonesia	Malaysia	Philippines	Singapore
ข้อมูลทั่วไป	กฎหมายที่เกี่ยวข้องกับ data privacy protection ของประเทศอินโดนีเซีย คือ Provision of Electronic System and Transaction ซึ่งมีผลใช้บังคับเมื่อวันที่ 15 ตุลาคม 2555 ซึ่งนอกจากกฎหมายฉบับนี้ดังกล่าวแล้วยังมี กฎหมายอื่น ที่เกี่ยวข้อง เช่น ● Telecommunications Sector ● Public Information Sector ● Banking and Capital Market Sector	Personal Data Protection Act 2013 (PDPA) ได้มีการประกาศลงในราชกิจจานุเบกษาและมีผลใช้บังคับแล้ว เมื่อวันที่ 15 พฤศจิกายน 2556 กฎหมายฉบับนี้ใช้บังคับกับหน่วยงานของรัฐบาล	Data Privacy Act of 2012 มีผลใช้บังคับเมื่อวันที่ 8 กันยายน 2555	สิงคโปร์มี Personal Data Protection Act 2012 (No 26 0f 2012) เรียกโดยย่อว่า PDPA เป็นกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ในภาคเอกชนซึ่งประกาศใช้เมื่อเดือนธันวาคม 2012 และมีผลบังคับใช้กฎหมายทั้งฉบับเมื่อ 2 กรกฎาคม 2557
คำจำกัดความของข้อมูลส่วนบุคคล (Definition of personal data)	ข้อมูลส่วนบุคคล ซึ่งถูกเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ ถูกต้องตรงตามความจริงเสมอ	-ได้มีการให้คำจำกัดความข้อมูลส่วนบุคคลไว้โดยเน้นในเรื่องของการส่งข้อมูลทางธุรกิจ -มีการกำหนดเรื่องการให้ความยินยอมของเจ้าข้อมูลไว้ว่า ในกรณีที่เจ้าของข้อมูลมีอายุต่ำกว่า 18 ปี ผู้ให้ความยินยอมได้ต้องเป็นผู้ปกครองหรือผู้ดูแลเจ้าของข้อมูลนั้น	ได้มีการกำหนดคำจำกัดความของข้อมูลส่วนบุคคลไว้โดยละเอียด	ข้อมูลส่วนบุคคลตามกฎหมายของประเทศสิงคโปร์นั้นได้มีการให้คำนิยามไว้อย่างกว้างๆว่าคือข้อมูลส่วนบุคคลซึ่งไม่ว่าจริงหรือไม่ โดยสามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าจะจากข้อมูลๆ เอง หรือจากข้อมูลอื่นๆ ที่นำมาประกอบกัน

ประเด็น/ประเทศ	Indonesia	Malaysia	Philippines	Singapore
คำจำกัดความของข้อมูลส่วนตัวโดยเฉพาะ (Definition of sensitive data)	ยังมิได้มีการให้คำจำกัดความไว้ในกฎหมายฉบับนี้	มีการให้คำนิยามของข้อมูลส่วนบุคคลโดยเฉพาะ (sensitive data) หมายถึง ข้อมูลส่วนบุคคลซึ่งประกอบไปด้วยข้อมูลที่เกี่ยวข้องกับสุขภาพ (ร่างกาย,จิตใจ) ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือความเชื่ออื่นๆ	มีการให้คำจำกัดความของข้อมูลส่วนตัวโดยเฉพาะไว้ ว่าเป็นข้อมูลส่วนบุคคลซึ่งเกี่ยวกับเชื้อชาติ สถานะ อายุ ศาสนา ความคิดเห็นทางการเมือง ประวัติสุขภาพ หรือพฤติกรรมทางเพศ หรือข้อมูลอื่นๆที่หน่วยงานชองรัฐเป็นผู้กำหนดเพิ่มเติม	ไม่ได้มีให้คำนิยามของข้อมูลส่วนตัวโดยเฉพาะไว้ในกฎหมายฉบับนี้
หน่วยงานที่รับผิดชอบในการปฏิบัติตามหลักกฎหมายนี้	มิได้มีการกำหนดหน่วยงานที่รับผิดชอบ	ปัจจุบันมี Abu Hassan bin Ismail เป็น Personal Data Protection Commissioner	ตามกฎหมายฉบับนี้ได้มีการกำหนดให้มีการจัดตั้งคณะกรรมการดูแลข้อมูลส่วนบุคคลแห่งชาติ แต่ปัจจุบันยังมิได้มีการจัดตั้งขึ้น	กฎหมายของสิงคโปร์กำหนดให้แต่ละองค์กรมีผู้ดูแล/ควบคุมข้อมูลส่วนบุคคล โดยมีหน้าที่ดูแลรับผิดชอบการดำเนินการต่างๆที่เกี่ยวข้องกับข้อมูลส่วนบุคคลขององค์กรนั้นๆ ว่าเป็นไปตามที่กฎหมายกำหนดหรือไม่

ประเด็น/ประเทศ	Indonesia	Malaysia	Philippines	Singapore
การเก็บและการใช้ข้อมูลส่วนบุคคลตามกฎหมาย	ผู้ดำเนินการ(data controller) สามารถเก็บและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลได้ ภายใต้เงื่อนไขดังต่อไปนี้ เช่น ●เจ้าของข้อมูลให้ความยินยอม ●ผู้ดำเนินการจัดเก็บข้อมูลตามหลักเกณฑ์ที่กฎหมายกำหนด ●เป็นการจัดเก็บข้อมูลตามที่กฎหมายหรือรัฐบาลของประเทศอินโดนีเซียกำหนด และ/หรือเพื่อประโยชน์สาธารณะ	ผู้ดำเนินการ (data controller) มีหน้าที่ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยในการจัดเก็บข้อมูล	การเก็บและใช้ข้อมูลต้องเป็นไปตามหลักการทั่วไปของข้อมูลส่วนบุคคล a ต้องมีการแจ้งถึงวัตถุประสงค์ของการจัดเก็บข้อมูลก่อนหรือเร็วที่สุดเท่าที่จะทำได้แก่เจ้าของของข้อมูล b การดำเนินการต่างๆ ต้องเป็นไปด้วยชอบด้วยกฎหมาย c ….. นอกจากนี้แล้ว การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต้องเป็นไปตามเงื่อนไขที่กำหนด มิเช่นนั้น ก็จะต้องห้ามมิให้มีการดำเนินการดังกล่าว a ต้องได้รับความยินยอมจากเจ้าของข้อมูล ….. d การจัดเก็บข้อมูลมีความจำเป็นเพื่อปกป้องชีวิต หรือสุขภาพของเจ้าของข้อมูล ตามกฎหมายของประเทศฟิลิปฟินส์ ห้ามมิให้มีการจัดเก็บข้อมูลส่วนตัวโดยเฉพาะ (sensitive data) เว้นแต่กรณีดังต่อไปนี้	กำหนดให้แต่ละองค์กรเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลได้ในกรณีที่ -มีการให้ความยินยอมโดยเจ้าของข้อมูลก่อนดำเนินการใดๆ -เจ้าของข้อมูลสามารถปฏิเสธหรือยกเลิกความยินยอมได้หากมีเหตุผลจำเป็น

ประเด็น/ประเทศ	Indonesia	Malaysia	Philippines	Singapore
			a เจ้าของข้อมูลได้ให้ความยินยอมก่อนการจัดเก็บข้อมูลและมีการแจ้งถึงวัตถุประสงค์ในการจัดเก็บข้อมูลอย่างชัดเจน .... c ในกรณีที่เจ้าของข้อมูลไม่มีสิทธิหรือไม่สามารถแสดงออกซึ่งความยินยอมได้ แต่จำเป็นต้องดำเนินการกับข้อมูลเพื่อปกป้องชีวิต สุขภาพของเจ้าของข้อมูล หรือบุคคลอื่น	
การส่งข้อมูล (Transfer)	ในกรณีที่มีการส่งข้อมูลทางอิเล็กทรอนิกส์ที่หรือเอกสารอิเล็กทรอนิกส์ ผู้ให้บริการ (provider) ต้องอธิบายให้ผู้ดำเนินการ(data controller) และผู้ครอบครองข้อมูลทราบว่ามีการส่งข้อมูล		การส่งข้อมูลส่วนบุคคลนั้นสามารถกระทำได้ตามกฎหมายของประเทศฟิลิปฟินส์ แต่ผู้ดำเนินการ (data controller) ยังคงมีหน้าที่รับผิดชอบข้อมูลซึ่งอยู่ในความดูแลของตนในกรณีที่มีการส่งข้อมูลไปยังหน่วยงานอื่น อย่างไรก็ดี ข้อมูลส่วนตัวโดยเฉพาะนั้นกฎหมายห้ามมิให้มีการส่งต่อข้อมูลในส่วนนี้ไม่ว่ากรณีใดๆ	การส่งข้อมูลออกไปยังประเทศอื่นนั้นสามารถกระทำได้หากองค์กร (ผู้ดูแลข้อมูล) สามารถพิสูจน์ได้ว่าประเทศอื่นที่มีการส่งออกข้อมูลนั้นมีมาตรฐานด้านความปลอดภัยเทียบเท่าหรือสูงกว่าสิงคโปร์

ประเด็น/ประเทศ	Indonesia	Malaysia	Philippines	Singapore
การบังคับใช้ (Enforcement)	บทลงโทษกรณีที่มีการไม่ปฏิบัติตามกฎหมาย คือ มีการกำหนดโทษปรับ และหากมีการพิสูจน์ได้ว่าการฝ่าฝืนกฎหมายนั้นมีขึ้นด้วยความตั้งใจ ผู้กระทำผิดอาจได้รับโทษถึงจำคุก	ตามกฎหมายฉบับนี้อนุญาตให้เจ้าของข้อมูลยกเลิกความยินยอมให้การจัดเก็บข้อมูลได้ซึ่งหากผู้ดำเนินการฝ่าฝืนอาจได้รับโทษปรับเป็นเงินถึง RM 100,000 หรือต้องโทษจำคุกเป็นไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ตรวจสอบว่าผู้ควบคุมดำเนินการตามกฎหมายหรือไม่ อย่างไรก็ดีคณะกรรมการฯ ไม่สามารถฟ้องร้อง หรือดำเนินคดีกับผู้ควบคุมข้อมูลได้เอง ในกรณีนี้เป็นหน้าที่ของกระทรวงยุติธรรมในการดำเนินการ	การบังคับใช้กฎหมายนั้น เป็นหน้าที่ของคณะกรรมการโดยที่คณะกรรมการมีอำนาจดังต่อไปนี้ - สั่งให้หยุดการเก็บ การใช้ การเปิดเผยข้อมูล ส่วนบุคคลหากพบการกระทำที่ฝ่าฝืนต่อบทบัญญัติของกฎหมาย - ทำลายข้อมูลส่วนบุคคลที่มีการเก็บไว้โดยฝ่าฝืนต่อกฎหมาย
การรักษาความปลอดภัยของข้อมูล (Security)			ผู้ดำเนินการต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลทั้งทางด้านกายภาพและด้านเทคนิค รวมทั้งต้องมีมาตรการรักษาความปลอดภัยจากอุบัติภัยและการเข้าใช้ข้อมูลโดยผิดกฎหมาย และที่สำคัญคือต้องมีมาตรการรักษาความปลอดภัยตามที่คณะกรรมการกำหนด	องค์กรมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่อยู่ในความครอบครอง ทั้งนี้ตามกฎหมายของสิงคโปร์ไม่ได้มีการกำหนดมาตรการด้านความปลอดภัยไว้เป็นพิเศษ จึงเป็นหน้าที่ขององค์กรที่ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยที่เหมาะสม
การแจ้งว่ามีการกระทำผิด (Breach of notification)			ผู้ควบคุมต้องแจ้งให้คณะกรรมการข้อมูลส่วนบุคคลทราบทันที เมื่อพบว่ามีการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคล หรือมีเหตุอันควรเชื่อได้มีการกระทำผิดดังกล่าว	

ประเด็น/ประเทศ	Indonesia	Malaysia	Philippines	Singapore
อื่นๆ		ตามกฎหมายฉบับนี้กำหนดให้ผู้ครอบครองข้อมูลต่างๆ ต่อไปนี้จดทะเบียน(มีใบอนุญาตในการดำเนินการ) เช่น -องค์กรที่เกี่ยวข้องกับการสื่อสาร -ธนาคารและสถาบันทางการเงิน -ธุรกิจประกันภัย -ธุรกิจที่เกี่ยวข้องกับสุขภาพ -การศึกษา -การขายตรง		

สำหรับรายละเอียดของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศ คณะผู้ศึกษาจะได้นำเสนอเป็นลำดับเรียงตามช่วงเวลาที่มีการประกาศใช้กฎหมายแต่ละประเทศไปโดยเริ่มจากอินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์ สำหรับบทบัญญัติของกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นต้นฉบับภาษาอังกฤษ ได้แนบไว้ในภาคผนวกท้ายรายงานกรศึกษานี้ด้วยแล้ว อย่างไรก็ตามในการศึกษาและพัฒนาแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายใต้ประชาคมอาเซียนนี้ คณะผู้ศึกษาไม่ได้นำเสนอในลักษณะการแปลตัวบทบัญญัติจากภาษาอังกฤษมาเป็นภาษาไทยทั้งหมดซึ่งจะกลายเป็นโครงการแปลตัวบทกฎหมายที่ไม่ใช่วัตถุประสงค์ของการศึกษาตามโครงการนี้ แต่จะนำเสนอในเชิงการวิเคราะห์เจตนารมณ์และชี้ให้เห็นประเด็นที่เป็นหลักการเหตุผลในการตรากฎหมาย โครงสร้างกฎหมายตลอดจนเนื้อหาที่เป็นสาระสำคัญในแต่ละส่วน และจะได้ทำการศึกษาวิเคราะห์เปรียบเทียบมาตรฐานกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่อยู่ในวาระการพิจารณาของสภานิติบัญญัติแห่งชาติในปัจจุบัน ทั้งนี้สาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศที่เป็นกรณีศึกษามีรายละเอียดดังต่อไปนี้

3.2 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศอินโดนีเซีย

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของอินโดนีเซียที่ใช้บังคับในปัจจุบัน คือ Law No.11 of 2008 ซึ่งรู้จักในชื่อย่อว่า EIT Law กฎหมายว่าด้วยธุรกรรมและข้อมูลอิเล็กทรอนิกส์ (Electronic Information and Transactions Law) ซึ่งไม่ใช่กฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลทุกประเภท แต่นอกจากกฎหมายฉบับนี้ที่ถือเป็นกฎหมายหลักฉบับสำคัญแล้ว ก็ยังมีการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายเฉพาะเรื่องได้แก่ Banking Law No.7 of 1992 และ The Capital Market Law No. 8 of 1995

สำหรับหน่วยงานที่รับผิดชอบดูแลกฎหมายฉบับนี้คือ กระทรวงการสื่อสารและข้อมูลข่าวสาร (Ministry of Communication and Information) ในส่วนข้อมูลส่วนบุคคลที่เกี่ยวกับธนาคารและตลาดทุนจะมีผู้ที่ดูแลแยกไปคนละหน่วยงาน คือ The Financial Services Authority

เนื้อหาสาระของEIT Law ที่ได้รับการบัญญัติไว้มีจำนวนทั้งสิ้น 54 มาตรา แบ่งออกเป็น13 หมวด ได้แก่

Chap. I: General Provisions
หมวด 1 บททั่วไป (มาตรา 1-2)

Chap. II: Principles and Objectives
หมวด 2 หลักการและวัตถุประสงค์(มาตรา 3-4)

Chap. III: Electronic Information, Records, and Signatures
หมวด 3 ข้อมูลอิเล็กทรอนิกส์ การจัดเก็บ และการลงลายมือชื่อ (มาตรา 5-12)

Chap. IV: Provision of Electronic Certification and Electronic Systems
หมวด 4 บทบัญญัติว่าด้วยการรับรองทางอิเล็กทรอนิกส์ และระบบอิเล็กทรอนิกส์ (มาตรา 13-16)

Chap. V: Electronic Transactions
หมวด 5 การทำธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 17-22)

Chap. VI: Domain Names, Intellectual Property Rights and Protection of Privacy Rights
หมวด 6 ชื่อโดเมน สิทธิในทรัพย์สินทางปัญญา และการคุ้มครองสิทธิส่วนบุคคล (มาตรา 23-26)

Chap. VII: Prohibited Acts
หมวด 7 การกระทำที่เป็นข้อห้าม(มาตรา 27-37)

Chap. VIII: Dispute Resolution
หมวด 8 การแก้ไขข้อพิพาท (มาตรา 38-39)

Chap. IX: Role of the Government and Role of the Public
หมวด 9 การปฏิบัติของหน่วยงานรัฐและสาธารณะ(มาตรา 40-41)

Chap. X: Investigation
หมวด 10 การสอบสวน (มาตรา 42-44)
Chap. XI: Penal Provisions
หมวด 11 บทลงโทษ (มาตรา 45-52)
Chap. XII: Transitional Provisions
หมวด 12 บทบัญญัติการส่งผ่าน (มาตรา 53)
Chap. XIII: Concluding Provisions
หมวด 13 บทบัญญัติสุดท้าย (มาตรา 54)

ทั้งนี้การคุ้มครองข้อมูลส่วนบุคคลได้รับการพิจารณาว่าสิทธิความเป็นส่วนตัวของอินโดนีเซียถูกมองว่าเป็นหนึ่งในสิทธิพลเมืองตามกฎหมายรัฐธรรมนูญปีค.ศ. 1945 ภายใต้การตีความมาตรา 28 G (1) ที่รับรองสิทธิของบุคคลที่จะปกป้องตนเอง ครอบครัว ศักดิ์ศรีความเป็นมนุษย์ และทรัพย์สิน ว่าหมายเรารวมถึงสิทธิในการปกป้องข้อมูลส่วนบุคคลด้วย นอกจากนี้สิทธิในการที่จะไม่ถูกแทรกแซงเสรีภาพและความลับในการสื่อสารผ่านเครื่องมืออิเล็คทรอนิคส์ก็ยังถูกรับรองภายได้มาตรา 32 ของ กฎหมายสิทธิมนุษยชน Act. No. 39/1999 อีกด้วย[19]

ด้วยความตื่นตัวในด้านของสิทธิมนุษยชน และกรณีการละเมิดความเป็นส่วนตัวหรือการรั่วไหลของข้อมูลที่เกิดขึ้นอยู่บ่อยครั้งจึงทำให้เกิดความตื่นตัวในการผลักดันกฎหมายเฉพาะที่คุ้มครองข้อมูลส่วนบุคคลโดยตรง หากแต่ปัจจุบันประเทศอินโดนีเซียยังไม่มีกฎหมายฉบับที่คุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ หากแต่การใช้ข้อมูลอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลถูกกำกับภายใต้แนวคิดเรื่องสิทธิความเป็นส่วนตัว ซึ่งถูกกำหนดหลักการไว้อย่างกว้างของมาตรา 26 ของ Law on Electronic Information and Transaction (Act No. 11, 2008) และได้รับการขยายความเพิ่มเติมในบางประเด็นภายใต้ Regulation on the Electronic System and Transaction (No.82 of 2012) ซึ่งเป็นกฎหมายลูกของ 2008 Law มีผลใช้บังคับเมื่อ 15 ต.ค. 2012 มีมาตรา 15 เป็นกฎเกณฑ์สำคัญที่กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลโดยตรง

3.2.1 ขอบเขตของกฎหมาย

กฎหมายฉบับนี้บังคับใช้กับผู้ดำเนินการระบบอิเล็กทรอนิกส์ (Electronic system operator) ใดๆ ที่ดำเนินธุรกรรมอิเล็กทรอนิกส์ที่มีผลกระทบทางกฎหมาย หรือมีอิทธิพลยิ่งยวดต่อผลประโยชน์ของอินโดนีเซีย อาจเป็นภาครัฐหรือภาคเอกชนก็ได้ ซึ่งการตีความมีโอกาสขยายขอบเขตการบังคับใช้ออกไปนอกอาณาเขต (extraterritorial jurisdiction) ได้ด้วย

[19]Wahyudi Djafar, **Control Policy versus Internet Freedom: Brief introduction of the development and dynamics of regulation related to internet and human rights in Indonesia, Malaysia and Philippines,** Institute for Policy Research and Advocacy (ELSAM) (2013), p. 31.

3.2.2 คำจำกัดความของข้อมูลส่วนบุคคล

มาตรา 1 (27) ของ 2012 Regulation ให้นิยามข้อมูลส่วนบุคคลว่า เป็นข้อมูลซึ่งถูกเก็บ ถูกปฏิบัติ และถูกรักษาไว้อย่างปลอดภัยเพื่อคุ้มครองข้อเท็จจริง และความลับของข้อมูลนั้นๆ

อนึ่ง กฎหมายของอินโดนีเซียไม่มีการให้คำจำกัดความของข้อมูลส่วนบุคคลโดยเฉพาะ (Sensitive Personal Data) ดังนั้นระดับการคุ้มครองจึงเป็นมาตรฐานเดียวกับข้อมูลส่วนบุคคลโดยทั่วไป

3.2.3 หน่วยงานที่รับผิดชอบตามกฎหมาย

กระทรวงการสื่อสารและข้อมูลข่าวสาร (Ministry of Communication and Information) โดยความสนับสนุนของสภาผู้แทนราษฎรและประธานาธิบดี นอกจากนี้ หน่วยงานอื่นๆ ที่มีความรับผิดชอบเฉพาะทางก็มีส่วนในการควบคุมให้เกิดการปฏิบัติตามกฎหมายนี้ด้วย เช่น หน่วยงานที่มีอำนาจควบคุมการให้บริการการเงิน

3.2.4 หลักการสำคัญของกฎหมาย

1. <u>การเก็บ การใช้ และการเปิดเผยข้อมูล (collection, use and discloser)</u>

ผู้ดำเนินการ (data controller) สามารถเก็บและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลได้ภายใต้เงื่อนไขเจ้าของข้อมูลให้ความยินยอม จัดเก็บข้อมูลตามหลักเกณฑ์ที่กฎหมายกำหนด หรือเป็นการจัดเก็บข้อมูลตามที่ กฎหมายหรือรัฐบาลของประเทศ อินโดนีเซียกำหนดและ/หรือเพื่อประโยชน์สาธารณะ

2. <u>การรักษาความปลอดภัยของข้อมูล (security)</u>

มาตรา 18-29 ของ 2012 Regulation กำหนดอย่างละเอียดถึง มาตรการรักษาความปลอดภัยของข้อมูลโดยมีหน่วยงานรัฐกำกับดูแล

3. <u>การส่งข้อมูลไปต่างประเทศ (Transfer)</u>

กำหนดให้การส่งข้อมูลไปต่างประเทศต้องได้รับความยินยอมจากเจ้าของข้อมูล และในกรณีที่มีการส่งข้อมูลทางอิเล็กทรอนิกส์หรือเอกสารอิเล็กทรอนิกส์ ผู้ให้บริการ (provider) ต้องอธิบายให้ผู้ควบคุมข้อมูลและเจ้าของข้อมูลทราบว่ามีการส่งข้อมูล

4. <u>การแจ้งว่ามีการกระทำผิด (breach notification)</u>

มาตรา 15 ของ 2012 Regulation กำหนดให้ผู้ดำเนินการระบบข้อมูลอิเล็กทรอนิกส์ (electronic system operator) จะต้องแจ้งให้บุคคลเจ้าของข้อมูลทราบเมื่อเกิดความล้มเหลวในการปกป้องความลับของข้อมูลที่อยู่ในความรับผิดชอบ

3.2.5 การบังคับใช้และบทลงโทษ

2012 Regulation, Art. 84 ได้ กำหนดบทลงโทษทางปกครอง สำหรับผู้ไม่ปฏิบัติตามหน้าที่ที่กฎหมายกำหนด ซึ่งอาจเป็นคำเตือนเป็นลายลักษณ์อักษร ค่าปรับทางปกครอง คำสั่งหยุดกิจการชั่วคราว หรือการตัดชื่อออกจากรายชื่อที่ลงทะเบียนไว้กับหน่วยงานรัฐ อันจะส่งผลให้ไม่สามารถดำเนินกิจการเกี่ยวกับข้อมูลส่วนบุคคลได้อีก และบทลงโทษทางปกครองไม่ทำให้ความรับผิด

ทางแพ่งและอาญาหมดไป แม้ 2008 Law จะไม่ได้กำหนดบทลงโทษเกี่ยวกับการคุ้มครองข้อมูลส่วนตัวโดยตรง หากแต่ได้กำหนดบทลงโทษทางอาญาในกรณีของอาชญากรรมคอมพิวเตอร์

3.2.6 ท่าทีต่อการเข้าร่วมในกรอบความร่วมมือระหว่างประเทศ

รัฐบาลอินโดนีเซียได้รับแรงกดดันโดยเฉพาะจากภาคธุรกิจให้ผลักดันกฎหมายคุ้มครองข้อมูลส่วนบุคคล และยกระดับมาตรฐานการคุ้มครองให้เท่ากับมาตรฐานสากล เพราะมิเช่นนั้น มาตรฐานสากลจะกลายเป็นเครื่องกีดขวางที่ทำให้ภาคธุรกิจของอินโดนีเซียไม่สามารถแข่งขันในตลาดโลกได้[20] ถ้าอินโดนีเซียจะเข้าร่วมระบบ APEC Cross-Border Privacy Rules (CBPRs) Chapter VII ของ 2012 Regulation ที่ว่าด้วย Reliability Certification Agencies อาจเป็นหน่วยงานที่มีความสำคัญในการดำเนินงาน[21]

3.3 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศมาเลเซีย

ในบรรดาการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในประชาคมอาเซียน มาเลเซียถือเป็นประเทศแรกที่ได้ประกาศใช้กฎหมายลักษณะนี้ที่ชื่อ Personal Data Protection Act 2010 (PDPA) เมื่อวันที่ 10 มิถุนายน คศ.2010โดยมีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ดูแล (The Malaysain Personal Data Protection Commissioner) ซึ่งเพิ่งมีผลบังคับใช้อย่างสมบูรณ์ในวันที่ 15 พฤศจิกายน 2013 (พ.ศ. 2556)ที่ผ่านมา โดยมีวัตถุประสงค์สำคัญในการคุ้มครองส่วนบุคคลของประชาชน การจัดเก็บ การประมวลผลข้อมูลส่วนบุคคลที่ใช้ในธุรกรรมทางการค้า

พระราชบัญญัติฉบับนี้มี146 มาตราซึ่งถือว่าเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลในอาเซียนที่มีจำนวนมาตรามากกว่ากฎหมายของประเทศอื่นในภูมิภาคเดียวกัน เนื้อหาของกฎหมายฉบับนี้แบ่งจำนวนส่วนออกเป็น 11 ภาค ดังต่อไปนี้

PART I – PRELIMINARY

ภาค 1 ความเบื้องต้น (มาตรา 1 – 4)

PART II - PERSONAL DATA PROTECTION

ภาค 2 การคุ้มครองข้อมูลส่วนบุคคล (มาตรา 5-44)

Division 1 - Personal Data Protection Principles

แผนก 1 หลักการคุ้มครองข้อมูลส่วนบุคคล

Division 2 – Registration

---

[20]Heppy Endah Palupy, **Privacy and Data Protection: Indonesia Legal Framework**, Thesis of Master Program in Law and Technology University of Tilberg (2011), pp. 52-54.

[21]Graham Greenleaf & Sinta Dewi Rosadi, “Indonesia’s data protection Regulation 2012: A brief code with data breach notification”, *Privacy Laws & Business International Report,* Issue 122 (2013), p. 5.

แผนก 2 การลงทะเบียน

Division 3 - Data user forum and code of practice

แผนก 3 สภาผู้ใช้ข้อมูลและประมวลการปฏิบัติ

Division 4 - Rights of data subject

แผนก 4 สิทธิของเจ้าของข้อมูล

PART III – EXEMPTION

ภาค 3 ข้อยกเว้น (มาตรา 45-46)

PART IV - APPOINTMENT, FUNCTIONS AND POWERS OF COMMISSIONER

ภาค 4 การแต่งตั้ง หน้าที่และอำนาจของคณะกรรมการ (มาตรา 47-60)

PART V - PERSONAL DATA PROTECTION FUND

ภาค 5 กองทุนคุ้มครองข้อมูลส่วนบุคคล (มาตรา 61-69)

PART VI - PERSONAL DATA PROTECTION ADVISORY COMMITTEE

ภาค 6 คณะกรรมการที่ปรึกษาการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 70-82)

PART VII - APPEAL TRIBUNAL

ภาค 7 คณะกรรมการอุทธรณ์ (มาตรา 83-100)

PART VIII - INSPECTION, COMPLAINT AND INVESTIGATION

ภาค 8 การตราจสอบ การร้องเรียน และ การสอบสวน (มาตรา101-109)

PART IX – ENFORCEMENT

ภาค 9 การบังคับใช้ (มาตรา 110-127)

PART X – MISCELLANEOUS

ภาค 10 บทเบ็ดเตล็ด (มาตรา 128-144)

PART XI - SAVINGS AND TRANSITIONAL PROVISIONS

ภาค 11 บทเฉพาะกาล (มาตรา 145-146)

หลักการสำคัญของการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในกฎหมายของมาเลเซียมีทั้งหมด 7 ประการ ได้แก่

- General หลักทั่วไป
- Notice and Choice หลักการแจ้งให้ทราบและทางเลือก
- Disclosure หลักการเปิดเผย
- Retention หลักการเก็บรักษา
- Security หลักคุ้มครองความปลอดภัย
- Access หลักการเข้าถึง
- Data integrity principle หลักความถูกต้องของข้อมูล

3.3.1 ขอบเขตของกฎหมาย

กฎหมายนี้บังคับใช้กับบุคคลในมาเลเซีย และบุคคลที่ใช้เครื่องมือในมาเลเซียเพื่อจัดการข้อมูล หรือเพื่อส่งข้อมูลผ่านมาเลเซียในบริบทของการทำธุรกรรมทางการค้า ไม่บังคับใช้กับข้อมูลส่วนบุคคลที่ถูกประมวลผลภายนอกประเทศมาเลเซียถ้าหากข้อมูลนั้นมิได้มีวัตถุประสงค์จะนำมาใช้ในประเทศมาเลเซีย

3.3.2 คำจำกัดความของข้อมูลส่วนบุคคล

มาตรา 4 ให้คำจำกัดความข้อมูลส่วนบุคคลว่าหมายถึงข้อมูลในบริบทธุรกรรมทางการค้าที่ถูกประมวลผลหรือจัดเก็บไว้เพื่อการประมวลผล (process) ซึ่งสามารถระบุตัวบุคคล หรือข้อมูลที่เมื่อนำไปประกอบกับข้อมูลอื่นๆ ที่มีแล้วสามารถระบุตัวบุคคลได้ โดยไม่รวมถึงข้อมูลที่ถูกประมวลผลเพื่อรายงานตามกฎหมาย Credit Reporting Agencies Act 2010

ทั้งยังให้คำนิยามข้อมูลส่วนบุคคลโดยเฉพาะ (sensitive data) ไว้ว่าเป็นข้อมูลส่วนบุคคลซึ่งประกอบไปด้วย ข้อมูลที่เกี่ยวข้องกับสุขภาพทั้งร่างกาย จิตใจ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือ ความเชื่ออื่นๆ ที่มีลักษณะคล้ายคลึงกัน หรือข้อมูลอื่นๆ ที่ คณะกรรมการข้อมูลส่วนบุคคล (Personal Data Commissioner) หรือรัฐมนตรีจะประกาศให้เป็นข้อมูลส่วนบุคคลโดยเฉพาะ ข้อมูลประเภทนี้ได้รับการคุ้มครองมากกว่าข้อมูลส่วนบุคคลทั่วไป คือบุคคลไม่สามารถประมวลผลข้อมูลได้ หากไม่ได้รับความยินยอมอย่างชัดแจ้ง หรือมีความจำเป็นตามที่กำหนดไว้ในมาตรา 40 (b) เช่น ความจำเป็นทางการแพทย์และเพื่อการดำเนินงานกระบวนการยุติธรรม ซึ่งเป็นข้อยกเว้นด้านความจำเป็นที่แคบกว่ากรณีข้อมูลส่วนบุคคลทั่วไป หรือข้อมูลนั้นถูกทำให้เป็นสาธารณะโดยเจตนาของเจ้าของข้อมูลเอง ผู้กระทำผิดจะต้องโทษปรับไม่เกิน 200,000 ริงกิต หรือโทษจำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ

3.3.3 หน่วยงานที่รับผิดชอบตามกฎหมาย

Part IV (มาตรา 47-60) ของกฎหมายฉบับนี้กำหนดให้รัฐมนตรีแต่งตั้ง Personal Data Protection Commissioner เป็นผู้บังคับใช้กฎหมายนี้กับภาคเอกชน ให้คำปรึกษารัฐบาลในประเด็นนโยบายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล รับการร้องเรียนจากประชาชนผู้ถูกละเมิดเกี่ยวกับข้อมูลส่วนบุคคล สืบสวนข้อเท็จจริง และเป็นผู้แทนรัฐบาลมาเลเซียในความร่วมมือเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในระดับระหว่างประเทศด้วย โดยมี Personal Data Protection Advisory Committee (Part VI) ให้คำปรึกษาแต่คำปรึกษานั้นไม่ผูกพัน Commissioner และหากบุคคลได้รับความเดือดร้อนจากการตัดสินใจของ Commissioner เช่น การออกใบรับรองหน่วยงานผู้ใช้ข้อมูล หรือการปฏิเสธข้อร้องเรียนของเจ้าของข้อมูล บุคคลสามารถฟ้องต่อ Appeal Tribunal ได้

ปัจจุบัน Commissioner คนแรกของประเทศมาเลเซียดำรงตำแหน่งโดย Abu Hassan bin Ismail มีนโยบายสำคัญที่ต้องการจะช่วยเหลือให้ภาคธุรกิจของมาเลเซียมีความคล่องตัวในการส่งรับข้อมูลกับต่างประเทศให้ได้มากที่สุด และมองว่ากฎหมายคุ้มครองข้อมูลส่วนบุคคลของมาเลเซียนั้นแม้จะมีลักษณะเป็นข้อบังคับเพิ่มเติมที่ภาคธุรกิจต้องปฏิบัติ หาก

มิได้อุปสรรคต่อการขยายตัวของภาคธุรกิจ แต่เป็นเครื่องมือในการยกระดับมาตรฐานด้านข้อมูลให้สามรถแข่งขันในระดับสากลได้[22]

หน้าที่สำคัญอีกประการของ Commissioner คือการจัดให้มีการขึ้นทะเบียนผู้ใช้ข้อมูลบางประเภท และออกใบรับรอง (Certificate of registration) ตามข้อบังคับในมาตรา 13-20 โดยเฉพาะองค์กรที่เกี่ยวข้องกับการ สื่อสาร ธนาคารและสถาบันทางการเงิน ธุรกิจประกันภัย ธุรกิจที่เกี่ยวข้องกับสุขภาพ การศึกษาการขายตรง Commissioner อาจปฏิเสธคำร้องขอขึ้นทะเบียน เพิกถอนใบรับรอง หรือไม่ต่อใบรับรอง ในกรณีที่เอกสารไม่ครบหรือผู้ใช้ข้อมูล (data user) ไม่ปฏิบัติตามกฎหมายฉบับนี้ **ซึ่งในทางปฏิบัติแล้ว แทบทุกบริษัทที่มีการเก็บข้อมูลส่วนบุคคลไปใช้เพื่อการทำธุรกรรมทางการค้าจำเป็นต้องขึ้นทะเบียน หน่วยงานด้านการเงิน เช่น บริษัท Maybank เป็นหน่วยงานแรก ๆ ที่ยื่นเอกสารคำร้องขอขึ้นทะเบียน**

นอกจากนี้ยังอาจมีการขึ้นทะเบียน Data user forum ซึ่งเป็นการรวมกลุ่มระหว่างผู้ใช้ข้อมูลประเภทเดียวกันเพื่อจัดทำ code of practice ตามลักษณะการใช้งานข้อมูลของแต่ละหน่วยงานและเสนอให้ Commissioner รับรอง ซึ่งวิธีการนี้จะทำให้เกิดการนำหลักการที่ระบุไว้ในกฎหมายฉบับนี้ไปใช้ในทางปฏิบัติอย่างเป็นรูปธรรมและสอดคล้องกับลักษณะของข้อมูลและธรรมชาติของธุรกิจนั้นๆ

3.3.4 หลักการสำคัญของกฎหมาย

1. <u>การเก็บ การใช้ และการเปิดเผยข้อมูล (collection, use and discloser)</u>

มาตรา 6 กำหนดหลักการความยินยอมของเจ้าของข้อมูลส่วนบุคคลในการประมวลผลข้อมูล และกำหนดข้อยกเว้นในบางกรณี เช่น การประมวลผลข้อมูลเพื่อปฏิบัติตามสัญญาที่ให้ไว้กับเจ้าของข้อมูลนั้นเอง

มาตรา 7 กำหนดให้ผู้ใช้ข้อมูล (data user) ต้องแจ้งเป็นลายลักษณ์อักษรถึงเจ้าของข้อมูลเมื่อมีการประมวลผลข้อมูล โดยระบุรายละเอียดเกี่ยวกับวัตถุประสงค์ แหล่งที่มาของข้อมูล สิทธิของเจ้าของข้อมูล ลักษณะของบุคคลอื่นที่อาจมีการเปิดเผยข้อมูล และทางเลือกที่เจ้าของข้อมูลสามารถจำกัดการประมวลข้อมูลได้ ซึ่งจะต้องแจ้งอย่างเร็วที่สุดเท่าที่สามารถทำได้ (as soon as practicable) เมื่อมีการเก็บข้อมูลเป็นครั้งแรก หรือเมื่อจะใช้ข้อมูลเพื่อวัตถุประสงค์อื่นๆ ที่ไม่ได้แจ้งไว้ในครั้งแรก หรือเมื่อจะเปิดเผยข้อมูลไปยังบุคคลอื่น ซึ่งการแจ้งนี้จะต้องเป็นไปอย่างชัดเจนและเข้าถึงได้ง่ายด้วย

2. <u>การส่งข้อมูลไปต่างประเทศ (transfer)</u>

มาตรา 129 ห้ามการส่งข้อมูลส่วนบุคคลไปต่างประเทศ ยกเว้นประเทศที่รัฐมนตรีประกาศตามคำแนะนำของ Commissioner ว่ามีระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเช่นเดียวกับกฎหมายฉบับนี้ ยกเว้นจะได้รับความยินยอมจากเจ้าของข้อมูล หรือมีความจำเป็นต้อง

[22] อ้างอิงจากคำกล่าวของ Commissioner ในงานประชุม ALB Data Protection Conference ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย วันที่17 มิถุนายม 2557.

กระทำเพื่อผลประโยชน์ของเจ้าของข้อมูล หรือได้ดำเนินมาตรการเพื่อรับรองว่าข้อมูลนั้นจะไม่ถูกประมวลผลในลักษณะที่ผิดกฎหมายฉบับนี้

ปัจจุบัน รัฐบาลมาเลเซียยังไม่ได้ออกรายชื่อของประเทศที่สามารถส่งข้อมูลไปได้ ภาคธุรกิจจึงใช้หลักความยินยอมหรือดำเนินมาตรการอื่น ๆ เป็นการเฉพาะเรื่องเพื่อรับประกันความปลอดภัยและความเป็นส่วนตัวของข้อมูลส่วนบุคคล มีเสียงสะท้อนจากภาคธุรกิจหลายส่วนว่าควรจะมีการออกรายชื่อให้เร็วที่สุดเพื่อความคล่องตัวในการประกอบกิจกรรมธุรกิจข้ามพรมแดนที่เกี่ยวข้องกับการรับส่งข้อมูลส่วนบุคคล หาก Commissioner คนปัจจุบันเห็นว่าถึงแม้จะไม่มีรายชื่อที่ชัดเจน แต่ภาคธุรกิจก็สามารถดำเนินการส่งข้อมูลไปต่างประเทศได้โดยทำตามเงื่อนไขของมาตรา 129[23]

3. <u>การรักษาความปลอดภัยของข้อมูล (security)</u>

มาตรา 9 กำหนดให้ผู้ใช้ข้อมูล (data user) ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยของข้อมูลส่วนบุคคลจากความเสียหาย การใช้ผิดวัตถุประสงค์ การปรับแต่ง การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือจากการทำลายข้อมูล ในกรณีที่ให้บุคคลอื่นประมวลผลข้อมูลให้จะต้องมีมาตรการประกันความปลอดภัยของข้อมูลนั้นอย่างเพียงพอ

4. <u>การเก็บรักษาข้อมูล (retention)</u>

มาตรา 10 กำหนดให้เก็บรักษาข้อมูลไว้เท่าที่จำเป็นตามวัตถุประสงค์เท่านั้น และจะต้องทำลายข้อมูลเมื่อหมดความจำเป็นแล้ว ทั้งมาตรา 11 กำหนดให้ต้องดูแลและปรับปรุงข้อมูลให้ถูกต้องอยู่เสมอ

5. <u>การเข้าถึงข้อมูล (access)</u>

มาตรา 12 กำหนดให้ต้องเปิดช่องทางให้เจ้าของข้อมูลเข้าถึง และแก้ไขข้อมูลให้ถูกต้องได้ หากได้รับการปฏิเสธอย่างไม่เป็นธรรมจากผู้ใช้ข้อมูล เจ้าของข้อมูลสามารถร้องเรียนหรือขอให้มีการตรวจสอบโดย Advisory Committee ได้

3.3.5 ข้อยกเว้นของกฎหมาย

Part III (มาตรา 45-46) กำหนดลักษณะการใช้งานข้อมูลที่ได้รับการยกเว้นไม่ต้องปฏิบัติตามหลักการบางประการของกฎหมายฉบับนี้ คือกรณีที่เป็นไปเพื่อการป้องกันอาชญากรรม การคำนวณภาษี เพื่อดำเนินงานในกระบวนการยุติธรรม การป้องกันอันตรายที่อาจเกิดขึ้นกับสุขภาพของผู้ป่วย การเก็บข้อมูลสถิติเพื่อการวิจัยในลักษณะที่ผลการวิจัยจะไม่ถูกเปิดเผยข้อมูลที่ระบุตัวตนได้ และการประมวลผลข้อมูลไปเพื่อวัตถุประสงค์เชิงการสื่อสารมวลชน วรรณกรรม และศิลปะ ทั้งนี้เป็นการยกเว้นเฉพาะเมื่อหากการกิจกรรมต่าง ๆ ที่กล่าวมาไม่สามารถกระทำโดยสอดคล้องกับหลักการต่าง ๆ ของกฎหมายนี้ได้เท่านั้น

[23] อ้างอิงจากการชี้แจ้งตอบคำถามระหว่างภาคธุรกิจของมาเลเซียและ Commissioner ในงานประชุม ALB Data Protection Conference ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย วันที่17 มิถุนายม 2557

3.3.6 การบังคับใช้และบทลงโทษ

ผู้ดำเนินการฝ่าฝืนกฎหมายอาจได้รับ โทษปรับสูงถึง 500,000 ริงกิตหรือ ต้องโทษจำคุกเป็นไม่เกิน 3 ปี หรือ ทั้งจำทั้งปรับ ผู้อำนวยการและเจ้าหน้าที่ของ หน่วยงานสามารถถูกฟ้องร้องความ รับผิดชอบร่วมหรือแยกจากหน่วย งานนั้นๆ ได้

3.3.7 ท่าทีต่อการเข้าร่วมในกรอบความร่วมมือระหว่างประเทศ

ประเทศมาเลเซียให้ความสนใจการยกระดับมาตรฐานให้เท่าเทียมกับมาตรฐานระหว่างประเทศเป็นอย่างมาก โดยเฉพาะมาตรฐานของประเทศในกลุ่ม EU

3.4 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศฟิลิปปินส์

กฎหมายของประเทศฟิลิปปินส์ คือ Data Privacy Act of 2012 (REPUBLIC ACT NO. 10173) กฎหมายนี้ได้ประกาศใช้เมื่อวันที่ 15 สิงหาคม พ.ศ. 2556 มีผลบังคับใช้เมื่อ 8 กันยายน 2012 โดยพระราชบัญญัติฉบับนี้มีความมุ่งหมายในการคุ้มครองข้อมูลส่วนบุคคลของบุคคล และการติดต่อสื่อสารในภาครัฐและภาคเอกชน ตลอดจนการจัดตั้งคณะกรรมการว่าด้วยความเป็นส่วนตัวแห่งชาติขึ้น (NATIONAL PRIVACY COMMISSION) ซึ่งกฎหมายฉบับนี้มีเพียง 45 มาตรา น้อยกว่าของอินโดนีเซีย แบ่งออกเป็นหมวดต่างๆ 9 หมวด ดังนี้

CHAPTER I GENERAL PROVISIONS

หมวด 1 บททั่วไป (มาตรา 1-6)

CHAPTER II THE NATIONAL PRIVACY COMMISSION

หมวด 2 คณะกรรมการว่าด้วยความเป็นส่วนตัวแห่งชาติ (มาตรา 7-10)

CHAPTER III PROCESSING OF PERSONAL INFORMATION

หมวด 3 การประมวลผลข้อมูลข่าวสารส่วนบุคคล (มาตรา 11-15)

CHAPTER IV RIGHTS OF THE DATA SUBJECT

หมวด 4 สิทธิในข้อมูลของบุคคล (มาตรา 16-19)

CHAPTER V SECURITY OF PERSONAL INFORMATION

หมวด 5 การดูแลความปลอดภัยของข่าวสารส่วนบุคคล (มาตรา 20)

CHAPTER VI ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

หมวด 6 ความรับผิดสำหรับในการส่งต่อข้อมูลส่วนบุคคล (มาตรา 21)

CHAPTER VII SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

หมวด 7 การรักษาความปลอดภัยของข้อมูลข่าวสารส่วนบุคคลที่อ่อนไหวในภาครัฐ (มาตรา 22-24)

CHAPTER VIII PENALTIES

หมวด 8 บทลงโทษ (มาตรา 25-37)

CHAPTER IX MISCELLANEOUS PROVISIONS

หมวด 9 บทเบ็ดเตล็ด (มาตรา 38-45)

กฎหมายที่มีวัตถุประสงค์เพื่อตอบสนองนโยบายแห่งชาติฟิลิปปินส์ที่มุ่งปกป้องสิทธิมนุษยชนขั้นพื้นฐานเกี่ยวกับความเป็นส่วนตัวและการสื่อสาร พร้อมกับรับรองการไหลเวียนอย่างเสรีของข้อมูลข่าวสารเพื่อสนับสนุนนวัตกรรมและการพัฒนา ซึ่งรัฐฟิลิปปินส์มีหน้าที่ต้องปกป้องข้อมูลส่วนบุคคลในระบบการติดต่อสื่อสารข้อมูลทั้งส่วนภาครัฐและภาคเอกชน (มาตรา 2)

ลักษณะเด่นของกฎหมายฟิลิปปินส์ฉบับนี้คือใช้หลักการเดียวกันทั้งภาครัฐและภาคเอกชน ทั้งในธุรกรรมที่เกี่ยวข้องและไม่เกี่ยวข้องกับการค้า ทั้งยังมีระดับความคุ้มครองที่สอดคล้องกับมาตรฐานของ EU Parliament และ APEC Privacy Framework ซึ่งได้รับการตอบรับอย่างดีจากภาคธุรกิจในฟิลิปปินส์ที่มีความจำเป็นต้องติดต่อแลกเปลี่ยนข้อมูลกับกลุ่มประเทศทั้งยุโรปและเอเชีย[24]

3.4.1 ขอบเขตของกฎหมาย

มาตรา 4 กำหนดให้กฎหมายนี้บังคับใช้กับบุคคลในฟิลิปปินส์ที่ประมวลผลข้อมูลส่วนบุคคลทุกประเภทรวมถึงบุคคลผู้ไม่อยู่ในประเทศฟิลิปปินส์แต่ใช้เครื่องมืออยู่ในประเทศ หรือมีสาขา สำนักงาน ตัวแทนอยู่ในประเทศฟิลิปปินส์ หากแต่กำหนดประเภทของข้อมูลที่พ้นขอบเขตการบังคับใช้ไว้ดังนี้ ข้อมูลของบุคคลที่เป็นหรือเคยเป็นพนักงานหรือลูกจ้างขององค์กรรัฐในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ของบุคคลนั้น ข้อมูลเกี่ยวกับสัญญาบริการที่บุคคลทำกับรัฐ ข้อมูลเกี่ยวกับผลประโยชน์เชิงตัวเงิน สัมปทาน หรือใบอนุญาตที่บุคคลได้รับจากรัฐ ข้อมูลเพื่อการสื่อสารมวลชน เพื่อศิลปะ วรรณกรรม หรือเพื่อการศึกษาวิจัย ข้อมูลที่จำเป็นต่อการดำเนินงานของภาครัฐ รวมถึงหน่วยงานการเงินกลางและผู้บังคับใช้กฎหมายที่เกี่ยวข้อง

กฎหมายฉบับนี้จะไม่ทำให้เกิดการเปลี่ยนแปลงต่อกฎหมายที่เกี่ยวกับความลับของเงินฝากธนาคาร หรือระบบข้อมูลเครดิต ข้อมูลที่จำเป็นต่อการปฏิบัติตามกฎหมายต่อต้านการฟอกเงิน ข้อมูลที่ถูกเก็บจากต่างประเทศอย่างถูกกฎหมายของประเทศนั้นๆ

ซึ่งจะเห็นได้ว่ากฎหมายฉบับนี้พยายามจะปกป้องข้อมูลส่วนบุคคลโดยไม่ให้ไปกระทบระบบการทำงานต่าง ๆ ที่จำเป็นต้องกระทำเป็นความลับ และพยายามไม่ให้การคุ้มครองสิทธิความเป็นส่วนตัวนั้นไปกระทบเสรีภาพในการแสดงออกต่าง ๆ ทั้งมาตรา 5 ยังกำหนดไว้ว่ากฎหมายนี้จะไม่เปลี่ยนแปลงหลักการการปกป้องความลับของแหล่งข่าวที่ได้รับการคุ้มครองตามกฎหมายเกี่ยวกับข้อมูลข่าวสาร

[24]"BPAP applauds signing of Data Privacy Act into Law", 27 August 2012, available at http://www.teamasia.com/newsroom/read-client-news.aspx?id=341:bpap-applauds-signing-of-data-privacy-act-into-law.

มาตรา 6 ยังกำหนดกรณีที่กฎหมายฉบับนี้อาจใช้บังคับกับกิจกรรมที่เกิดขึ้นนอกประเทศฟิลิปปินส์ (Extraterritoria application) เช่น กิจกรรมนั้นๆ มีจุดเกาะเกี่ยวกับบุคคลสัญชาติฟิลิปปินส์ หรือสัญญาที่ทำขึ้นในประเทศหรือหน่วยงานสาขาในประเทศสามารถเข้าถึงข้อมูลส่วนบุคคลในกิจกรรมนั้นๆ ได้ หรือองค์กรที่ใช้ข้อมูลส่วนบุคคลนั้นทำธุรกิจในประเทศฟิลิปปินส์

3.4.2 คำจำกัดความของข้อมูลส่วนบุคคล

มาตรา 3 ให้คำจำกัดความข้อมูลส่วนบุคคล (personal information) หมายถึงข้อมูลใดๆ ไม่ว่าจะถูกบันทึกในรูปแบบใดที่สามารถระบุตัวตนของเจ้าของข้อมูลได้อย่างชัดเจน หรือระบุได้โดยอ้อมเมื่อนำไปประกอบกับข้อมูลอื่น

ทั้งยังมีคำนิยามข้อมูลส่วนบุคคลเฉพาะ (sensitive personal information) หมายถึงข้อมูลเกี่ยวกับเชื้อชาติ ถิ่นกำเนิด สถานะการแต่งงาน อายุ สีผิว ศาสนาและความเชื่อทางปรัชญาหรือทางการเมือง ข้อมูลเกี่ยวกับสุขภาพ การศึกษา รสนิยมทางเพศ ประวัติอาชญากรรมหรือประวัติการถูกกล่าวหา ข้อมูลเกี่ยวกับหมายเลขประจำตัวที่ออกให้โดยรัฐ เช่น เลขประจำตัวผู้เสียภาษี เลขประจำตัวผู้รับสวัสดิการสังคม หรือข้อมูลอื่นๆ ที่กฎหมายกำหนดให้เก็บเป็นความลับ ซึ่งข้อมูลส่วนบุคคลประเภทนี้จะได้รับการคุ้มครองมากกว่าข้อมูลส่วนบุคคลทั่วไป และมีบทลงโทษในกรณีที่มีการละเมิดหนักกว่าด้วย

3.4.3 หน่วยงานที่รับผิดชอบตามกฎหมาย

Chapter II (มาตรา 7-10) กำหนดเกี่ยวกับ National Privacy Commission ซึ่งมีหน้าที่บังคับใช้กฎหมายนี้ และกำกับดูแลให้รัฐปฏิบัติตามมาตรฐานสากลว่าด้วยการคุ้มครองข้อมูล **ซึ่งหน่วยงานนี้มีพันธกรณีค่อนข้างกว้าง** สามารถรับคำร้องเรียนจากบุคคล มีอำนาจออกคำสั่งให้หยุดหรือระงับการประมวลผลข้อมูลที่อาจเป็นภัยต่อความมั่นคงของชาติหรือประโยชน์สาธารณะได้ ทั้งยังมีหน้าที่ร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนในการออกแผนปฏิบัติงานและนโยบายเพื่อเพิ่มความเข้มแข็งในการคุ้มครองข้อมูลส่วนบุคคล ทั้งมีหน้าที่ตรวจสอบแนวปฏิบัติเกี่ยวกับความเป็นส่วนตัว (privacy codes) ของหน่วยงานต่างๆ ให้คำแนะนำเกี่ยวกับประเด็นความเป็นส่วนตัว และเป็นตัวแทนรัฐบาลในการติดต่อร่วมมือกับประเทศต่างๆรวมถึงการอำนวยความสะดวกให้กับการคุ้มครองความเป็นส่วนตัวข้ามพรมแดนด้วย

แต่ปัจจุบันหน่วยงานนี้ยังไม่ได้รับการแต่งตั้ง ทำให้ยังไม่ได้ออก Implementing Rules and Regulations (IRR) ตามมาตรา 39 ซึ่งจะทำให้การปฏิบัติตามกฎหมายนี้เกิดขึ้นได้อย่างเป็นรูปธรรม ขณะนี้ภาคประชาสังคมของฟิลิปปินส์กำลังผลักดันให้มีร่าง Implementing Rules and Regulations (IRR) ที่มีรายละเอียดของมาตรฐานการปฏิบัติตามกฎหมายฉบับนี้เพื่อให้ออกมามีผลบังคับใช้หากมีการแต่งตั้ง National Privacy Commission ขึ้นในเร็ววัน[25]

[25]ข้อมูลจากการสัมภาษณ์ Alan Alegre ผู้เชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของฟิลิปปินส์ ปัจจุบันเป็น Executive Director ของ The Foundation of Media Alternatives (FMA) องค์กรไม่แสวงหากำไรที่รณรงค์ด้านสิทธิในการเข้าถึงข้อมูลและสิทธิความเป็นส่วนตัวของฟิลิปปินส์.

3.4.4 หลักการสำคัญของกฎหมาย

1. <u>การเก็บ การใช้ และการเปิดเผยข้อมูล (collection, use and discloser)</u>

มาตรา 11 วางหลักการทั่วไป คือการประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับความยินยอม ต้องแจ้งวัตถุประสงค์ก่อนหรือเร็วที่สุดเท่าที่จะทำได้ เนื้อหาของข้อมูลมีความถูกต้อง จัดเก็บไว้นานเท่าที่จำเป็นเท่านั้น ยกเวลาเป็นข้อมูลที่ต้องใช้เพื่อเก็บสถิติทางประวัติศาสตร์หรือวัตถุประสงค์ทางวิทยาศาสตร์อาจเป็นข้อยกเว้น การใช้และเผยแพร่ต้องชอบด้วยกฎหมายและเป็นไปตามหลักเกณฑ์ในมาตรา 12

มาตรา 13 ห้ามการจัดเก็บข้อมูลส่วนตัวโดยเฉพาะ (sensitive data) เว้นแต่มีความยินยอมก่อนการจัดเก็บ ข้อมูลและแจ้งวัตถุประสงค์ชัดเจน ในกรณีที่ไม่มีสิทธิหรือไม่สามารถแสดงออกซึ่งความยินยอมได้ ต้องมีความจำเป็นอย่างยิ่ง เช่น ในการประมวลผลข้อมูลเพื่อปกป้องชีวิต สุขภาพ ของเจ้าของข้อมูล หรือบุคคลอื่น

2. <u>การรักษาความปลอดภัยของข้อมูล (security)</u>

มาตรา 20 กำหนดให้มีมาตรการรักษาความปลอดภัยของข้อมูลทั้งทางด้านกายภาพและด้านเทคนิค รวมทั้งรักษาความปลอดภัยจากอุบัติภัยและการเข้าใช้ข้อมูลโดยผิดกฎหมาย และต้องมีมาตรการรักษาความปลอดภัยตามที่ National Privacy Commission กำหนด ทั้งยังกำหนดให้ต้องแจ้งให้ National Privacy Commission ทราบทันที เมื่อพบว่ามีการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคล หรือมีเหตุอันควรเชื่อได้มีการกระทำผิดดังกล่าว (breach notification)

3. <u>การส่งข้อมูลไปต่างประเทศ (Transfer)</u>

การส่งข้อมูลส่วนบุคคลนั้นสามารถกระทำได้ตามกฎหมายของประเทศฟิลิปปินส์ แต่ผู้ประมวลผลข้อมูลยังคงมีหน้าที่รับผิดชอบข้อมูลซึ่งอยู่ ในความดูแลของตนในกรณีที่มีการ ส่งข้อมูลไปยังหน่วยงานอื่น อย่างไรก็ดี ข้อมูลส่วนตัวโดยเฉพาะ (sensitive personal information) นั้น กฎหมายห้ามมิให้มีการส่งต่อข้อมูลในส่วนนี้ไม่ว่ากรณีใดๆ

4. <u>การบังคับใช้และบทลงโทษ</u>

ผู้ทำผิดกฎหมายนี้อาจต้องโทษปรับสูงสุด 2,000,000 เปโซ หรือโทษจำคุกสูงสุด 7 ปี National Privacy Commission มีหน้าที่ตรวจสอบว่าผู้ควบคุมดำเนินการตามกฎหมาย แต่คณะกรรมการฯ ไม่สามารถฟ้องร้องหรือดำเนินคดีกับผู้ควบคุมข้อมูลได้เอง ในกรณีนี้เป็นหน้าที่ของกระทรวงยุติธรรม

3.4.5 ท่าทีต่อการเข้าร่วมในกรอบความร่วมมือระหว่างประเทศ

ระบบการคุ้มครองข้อมูลส่วนบุคคลของประเทศฟิลิปปินส์นับได้ว่าให้ความคุ้มครองกว้างขวางและครอบคลุมมากที่สุดเมื่อเปรียบเทียบกับกฎหมายของประเทศอื่นในภูมิภาค นอกจากนี้ประเทศฟิลิปปินส์ยังมีท่าทีในทิศทางบวกต่อการเข้าร่วมในกรอบความร่วมมือระหว่างประเทศ เห็นได้จากการอ้างอิงหลักการของ APEC Privacy Framework ในการร่างกฎหมาย และซึ่งภายใต้ระบบกฎหมายคุ้มครองข้อมูลส่วนบุคคลของฟิลิปปินส์ในปัจจุบัน ถ้าหากสามารถบังคับใช้ได้อย่างมี

ประสิทธิภาพก็จะทำให้ฟิลิปปินส์มีความพร้อมอย่างมากที่จะเข้าร่วมในระบบ APEC Cross-Border Privacy Rules (CBPRs)[26]

3.5 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสิงคโปร์

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ เพิ่งมีผลบังคับใช้ทุกบทบัญญัติอย่างสมบูรณ์ เมื่อวันที่ 2 กรกฎาคม พ.ศ. 2557 ที่ผ่านมา อันที่จริงกฎหมายนี้ได้ผ่านการพิจารณาจากรัฐสภาสิงคโปร์ตั้งแต่เมื่อวันที่ 15 ตุลาคม 2555 (ค.ศ.2012) และประธานาธิบดีได้ลงนามเมื่อวันที่ 20 พฤศจิกายน ค.ศ.2012 โดยได้มีการตีพิมพ์ประกาศทั่วไปเมื่อวันที่ 7 ธันวาคม 2012 ซึ่งกฎหมายนี้ชื่อ Personal Data Protection Act 2012 (No. 26 of 2012) มีทั้งหมด 68 มาตรา และมีรายการท้ายกฎหมายอีก 9 เรื่องซึ่งกำหนดรายละเอียดเพิ่มเติมของเนื้อหาที่เกี่ยวข้องกับบางมาตราในกฎหมาย โดยกฎหมายฉบับนี้แบ่งเนื้อหาออกเป็น 10 ส่วน ได้แก่

PART I PRELIMINARY

ภาค 1 ความเบื้องต้น (มาตรา 1-4)

PART II PERSONAL DATA PROTECTION COMMISSION AND ADMINISTRATION

ภาค 2 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและการจัดองค์กร (มาตรา 5-10)

PART III GENERAL RULES WITH RESPECT TO PROTECTION OF PERSONAL DATA

ภาค 3 กฎเกณฑ์ทั่วไปในการเคารพคุ้มครองข้อมูลส่วนบุคคล (มาตรา 11-12)

PART IV COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

ภาค 4 การจัดเก็บ การใช้ และการเปิดเผยข้อมูลส่วนบุคคล (มาตรา 13-17)

Division 1 –Consent

แผนก 1 การได้รับความยินยอม

Division 2 –Purpose

แผนก 2 วัตถุประสงค์

PART V ACCESS TO AND CORRECTION OF PERSONAL DATA

ภาค 5 การเข้าถึงและแก้ไขข้อมูลส่วนบุคคล (มาตรา 21-22)

PART VI CARE OF PERSONAL DATA

ภาค 6 การดูแลข้อมูลส่วนบุคคล (มาตรา 23-26)

PART VII ENFORCEMENT OF PARTS III TO VI

ภาค 7 การบังคับใช้บทบัญญัติในภาค 3 ถึง 6 (มาตรา 27-32)

---

[26]Philippines: New privacy law enables APEC CBPR implementation, 30 August 2012, Data Guidance, available at http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=1856.

PART VIII APPEALS TO DATA PROTECTION APPEAL COMMITTEE, HIGH COURT AND COURT OF APPEAL

ภาค 8 การร้องเรียนถึงคณะกรรมการพิจารณาร้องเรียนข้อมูลส่วนบุคคล ศาลสูง และศาลอุทธรณ์ (มาตรา 33-35)

PART IX DO NOT CALL REGISTRY

ภาค 9 การลงทะเบียนห้ามการติดต่อ (มาตรา 36-48)

Division 1 — Preliminary

แผนก 1 ความเบื้องต้น

Division 2 — Administration

แผนก 2 การบริหารงาน

Division 3 — Specified message to Singapore telephone number

แผนก 3 ข้อความเฉพาะเจาะจงไปยังหมายเลขโทรศัพท์สิงคโปร์

Part X GENERAL

ภาค 10 บททั่วไป (มาตรา 49-68)

วัตถุประสงค์ของการตรากฎหมายฉบับนี้ปรากฏตามมาตรา 3 เพื่อกำกับดูแลการจัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลโดยองค์กรต่างๆ โดยคำนึงทั้งสิทธิของบุคคลในการปกป้องข้อมูลของตน และความจำเป็นในการจัดเก็บ ใช้ และเปิดเผยข้อมูลตามวัตถุประสงค์ที่วิญญูชน (reasonable persons) พึงพิจารณาว่าเหมาะสม

3.5.1 ขอบเขตของกฎหมาย

มาตรา 4 กำหนดให้ Part III และ IV ของกฎหมายนี้ซึ่งกล่าวถึงกฎเกณฑ์ทั่วไปเกี่ยวกับการคุ้มครอง การจัดเก็บ ใช้ และการเปิดเผยข้อมูลส่วนบุคคลจะไม่บังคับใช้กับบุคคลทั่วไปที่กระทำการไปตามความสามารถเฉพาะบุคคลนั้น ไม่ได้เป็นไปในนามขององค์กร รวมถึงลูกจ้างขององค์กร ตัวแทนขององค์กร และไม่บังคับใช้กับองค์กรที่ตั้งขึ้นมาเพื่อวัตถุประสงค์ชองการใช้กฎหมายนี้

กฎหมายฉบับนี้ไม่บังคับใช้กับข้อมูลส่วนบุคคลที่ถูกเก็บไว้อย่างน้อย 100 ปี หรือกับผู้ที่เสียชีวิตแล้ว ยกเว้นหลักการเกี่ยวกับการเปิดเผยข้อมูลจะบังคับใช้กับผู้ที่เสียชีวิตแล้ว 10 ปี หรือต่ำกว่านั้น ทั้งยังไม่บังคับใช้กับข้อมูลติดต่อเชิงธุรกิจเว้นแต่จะมีการระบุไว้อย่างชัดแจ้ง

กฎหมายฉบับนี้จะไม่ส่งผลกระทบต่อสิทธิพิเศษใดๆที่บุคคลเคยได้รับอยู่แล้วรวมถึงกฎหมายอื่นๆ หากขัดกับหลักการของกฎหมายนี้ กฎหมายนั้นถือว่ามีผลบังคับเหนือกว่ากฎหมายฉบับนี้

3.5.2 คำจำกัดความของข้อมูลส่วนบุคคล

มาตรา 2 ให้คำนิยามข้อมูลส่วนบุคคล (personal data) ไว้อย่างกว้างๆว่า คือ ข้อมูลส่วนบุคคลซึ่งอาจเป็นข้อมูลจริงหรือไม่จริงก็ได้ที่สามารถระบุตัวตนของบุคคลได้โดยตัวข้อมูลนั้นเอง หรือสามารถระบุตัวได้จากข้อมูลอื่นๆ ที่นำมาประกอบกัน

อนึ่งกฎหมายของสิงคโปร์ไม่มีการให้คำจำกัดความของข้อมูลส่วนบุคคลโดยเฉพาะ (Sensitive Personal Data) ดังนั้นระดับการคุ้มครองจึงเป็นมาตรฐานเดียวกับข้อมูลส่วนบุคคลโดยทั่วไป

3.5.3 หน่วยงานที่รับผิดชอบตามกฎหมาย

มาตรา 5 กำหนดให้รัฐมนตรีแต่งตั้ง Personal Data Protection Commission ซึ่งมีหน้าที่ตามมาตรา 6 คือสนับสนุนความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลในสิงคโปร์ ให้คำปรึกษากับหน่วยงานต่างๆและรัฐบาลเป็นตัวแทนรัฐบาลในเวทีระหว่างประเทศที่เกี่ยวข้องกับประเด็นนี้ ศึกษาวิจัย สร้างความร่วมมือกับต่างประเทศ และที่สำคัญที่สุดเป็นผู้บังคับใช้กฎหมายฉบับนี้ โดยอาจแต่ต่าง Advisory Committees เป็นที่ปรึกษาอีกทีหนึ่ง

3.5.4 หลักการสำคัญของกฎหมาย

เพื่อให้การปฏิบัติตามกฎหมายฉบับนี้เกิดขึ้นได้อย่างเป็นรูปธรรม มาตรา 11 กำหนดให้แต่ละองค์กรจะต้องแต่งตั้งบุคคลขึ้นรับผิดชอบการปฏิบัติตามกฎหมายฉบับนี้ และเปิดเผยข้อมูลติดต่อทางธุรกิจของบุคคลนั้นๆ ให้สาธารณชนรับทราบ มาตรา 12 กำหนดให้แต่ละองค์กรกำหนดนโยบายและแนวปฏิบัติที่จำเป็นสำหรับการปฏิบัติตามกฎหมายฉบับนี้ สร้างช่องทางในการร้องเรียนที่เกี่ยวข้อง รวมถึงประกาศให้สาธารณชนรับทราบทั้งนโยบายและช่องทางร้องเรียน และซักซ้อมความเข้าใจกับบุคลากรภายในองค์กร

กฎหมายฉบับนี้ยังกำหนดหลักการอื่นๆ ที่องค์กรจะต้องปฏิบัติตาม **เมื่อพิจารณารายละเอียดของข้อกฎหมายแล้วพบว่าค่อนข้างกำหนดหน้าที่ของมีความชัดเจน และประนีประนอมต่อความจำเป็นในการใช้ข้อมูลโดยเฉพาะในเชิงธุรกิจค่อนข้างมาก ดังจะพบได้ว่ามีข้อยกเว้นของกฎต่างๆ อยู่หลากหลาย ซึ่งสร้างภาระให้กับองค์กรในการคุ้มครองข้อมูลส่วนบุคคลเฉพาะในส่วนที่จะส่งผลกระทบโดยตรงต่อเจ้าของข้อมูลหรือสิทธิของผู้ที่เกี่ยวข้องเท่านั้น**

1. <u>หลักความยินยอม (consent)</u>

มาตรา 13 และ 14 กำหนดให้แต่ละองค์กรเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลได้ใน กรณีที่มีการให้ความยินยอมโดยเจ้าของข้อมูลก่อนดำเนินการใดๆ และเจ้าของข้อมูลสามารถปฏิเสธ หรือยกเลิกความยินยอมได้ ซึ่งองค์กรไม่อาจกำหนดให้การให้ความยินยอมเป็นเงื่อนไขในการขายสินค้าและบริการในระดับที่เกินกว่าความสมเหตุสมผลต่อการให้บริการนั้น (beyond what is reasonable) องค์กรไม่สามารถขอความยินยอมโดยปลอมแปลงข้อเท็จจริง ความยินยอมที่ได้มาด้วยวิธีการข้างต้นนั้นไม่ถือเป็นความยินยอมที่มีผลใช้ได้ตามกฎหมายฉบับนี้ ความยินยอมนั้นอาจเป็นความยินยอมแบบโดยปริยายได้แต่ต้องอยู่ในขอบเขตของมาตรา 15

2. <u>หลักวัตถุประสงค์ (purpose)</u>

มาตรา 18 กำหนดให้เก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลได้ต่อเมื่อวัตถุประสงค์นั้นเหมาะสมกับสถานการณ์และเจ้าของข้อมูลได้รับแจ้งถึงวัตถุประสงค์ ตามมาตรา 20

3. การเข้าถึงและแก้ไขข้อมูล (access and correction)

มาตรา 21 กำหนดสิทธิของบุคคลในการเข้าถึงข้อมูลและวิธีการที่ข้อมูลถูกใช้และเปิดเผยออกไปภายในหนึ่งปีตั้งแต่ถูกร้องขอ เว้นแต่การเข้าถึงนั้นจะเป็นอันตรายต่อตัวเจ้าของข้อมูลเองหรือกระทบสิทธิของผู้อื่น และมาตรา 22 กำหนดสิทธิของบุคคลในการร้องขอให้องค์กรแก้ไขข้อมูลของตนเองได้ เว้นแต่จะมีเหตุผลอันสมควร

4. ความถูกต้องของข้อมูล (accuracy)

มาตรา 23 กำหนดให้องค์กรมีหน้าที่จัดการให้ข้อมูลส่วนบุคคลที่เก็บรักษาไว้มีความถูกต้องครบถ้วนถ้าหากข้อมูลนั้นอาจถูกใช้โดยหน่วยงานที่จะตัดสินใจในประเด็นที่ส่งผลกระทบต่อตัวเจ้าของข้อมูลหรือผู้เกี่ยวข้อง หรือในกรณีที่อาจต้องเปิดเผยข้อมูลของบุคคลนั้นให้องค์กรอื่น

5. การรักษาความปลอดภัยของข้อมูล (security)

มาตรา 24 กำหนดให้องค์กรมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่อยู่ในความครอบครอง **แต่ไม่ได้มีการกำหนดมาตรการด้านความปลอดภัยไว้เป็นพิเศษ จึงเป็นหน้าที่ขององค์กรเองที่ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยที่เหมาะสมกับลักษณะและการใช้ข้อมูลนั้น ๆ**

มาตรา 25 กำหนดให้ทำลายข้อมูลเมื่อหมดความจำเป็นตามวัตถุประสงค์แล้ว และการเก็บข้อมูล (retention) นั้นไม่จำเป็นต่อวัตถุประสงค์เชิงกฎหมายหรือธุรกิจอื่นๆ อีก

6. การส่งข้อมูลไปต่างประเทศ (Transfer)

มาตรา 26 ห้ามการส่งข้อมูลออกไปยังประเทศอื่นยกเว้นกรณีที่องค์กรผู้ดูแลข้อมูลสามารถพิสูจน์ได้ว่า ประเทศอื่นที่มีการส่งออกข้อมูล นั้นมีมาตรฐานด้านความปลอดภัยเทียบเท่าหรือสูงกว่ากฎหมายของสิงคโปร์ Commissioner อาจออกข้อยกเว้นให้กับบางองค์กรที่เห็นว่าเหมาะสมได้

7. การแจ้งว่ามีการกระทำผิด (breach notification)

ไม่มีการกำหนดไว้ หากแต่หน่วยงานย่อยของรัฐ อาจจะสามารถออกข้อบังคับเป็นพิเศษเกี่ยวกับหน้าที่นี้ได้

3.5.5 การบังคับใช้และบทลงโทษ

การบังคับใช้กฎหมายเป็นหน้าที่ ของคณะกรรมการโดยที่คณะกรรมการมีอำนาจดังต่อไปนี้สั่งให้หยุดการเก็บ การใช้ การ เปิดเผยข้อมูล ส่วนบุคคลหากพบ การกระทำที่ฝ่าฝืนต่อบทบัญญัติ ของกฎหมายทำลายข้อมูลส่วนบุคคลที่มีการ เก็บไว้โดยฝ่าฝืนต่อกฎหมาย การฝ่าฝืนกฎหมายอาจมีโทษถึง 100,000 SGD หรือต้องโทษจำคุก ไม่เกิน 12 เดือน หรือทั้งจำทั้ง ปรับ

ทั้งนี้ ผู้อำนวยการและเจ้าหน้าที่ของหน่วยงานสามารถถูกฟ้องร้อง ความรับผิดชอบจากความผิดที่ หน่วยงานเป็นผู้กระทำได้ด้วย

3.5.6 ท่าทีต่อการเข้าร่วมในกรอบความร่วมมือระหว่างประเทศ

สิงคโปร์เป็นหนึ่งใน 8 ประเทศสมาชิก APEC ที่มีหน่วยงานรัฐเข้าร่วมเป็นสมาชิก APEC Cross-Border Privacy Enforcement Arrangement (CPEA) ซึ่งเป็นองค์กรด้านความร่วมมือระหว่างรัฐเพื่อสร้างเครือข่ายรองรับ ระบบ APEC Cross-Border Privacy Rules (CBPRs) และความร่วมมือเกี่ยวกับการคุ้มครองความเป็นส่วนตัวทั่วๆ ไปในภูมิภาคด้วย ประเทศอื่นๆ ที่มีหน่วยงานรัฐเป็นสมาชิกอยู่แล้วคือสหรัฐอเมริกา แคนาดา เม็กซิโก นิวซีแลนด์ ออสเตรเลีย ญี่ปุ่น และเกาหลีใต้[27]

3.6 กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

ปัจจุบัน (พ.ศ. 2557) ประเทศไทยยังไม่มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในรูปแบบเช่นเดียวกับประเทศในประชาคมอาเซียนที่ได้นำเสนอมาก่อนหน้านี้ แต่อย่างไรก็ตามรัฐธรรมนูญแห่งราชอาณาจักรไทยที่ผ่านมาในอดีต ก็มีการรับรองไว้เป็นสิทธิพื้นฐานของประชาชนประการหนึ่ง ดังจะเห็นได้จากรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ที่ได้รับรองไว้ในมาตรา 35 ว่า

*"**มาตรา 35** สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง*

การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว จะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ ตามที่กฎหมายบัญญัติ"

แม้รัฐธรรมนูญแห่งราชอาณาจักรไทยข้างต้นได้สิ้นสุดลงเพราะการทำรัฐประหารโดย คณะรักษาความสงบแห่งชาติ เมื่อวันที่ 22 พฤษภาคม 2557 แต่รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2557 ก็ได้มีการรับรองในเรื่องสิทธิเสรีภาพของประชาชนไว้ปรากฏตามมาตรา 4 ของรัฐธรรมนูญซึ่งสามารถตีความได้ว่า "สิทธิความเป็นส่วนตัว" ยังได้รับการคุ้มครองไว้เช่นเดิมดังนี้

มาตรา 4 ภายใต้บังคับบทบัญญัติแห่งรัฐธรรมนูญนี้ ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพและความเสมอภาค บรรดาที่ชนชาวไทยเคยได้รับการคุ้มครองตามประเพณีการปกครองประเทศไทยในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขและตามพันธกรณีระหว่างประเทศที่ประเทศไทยมีอยู่แล้ว ย่อมได้รับการคุ้มครองตามรัฐธรรมนูญนี้

นอกเหนือจากการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการคุ้มครองเป็นสิทธิพื้นฐานตามรัฐธรรมนูญแห่งราชอาณาจักรไทยนั้น เมื่อทำการสำรวจบรรดาบทกฎหมายที่ใช้บังคับในประเทศไทยยังคงมีกฎหมายระดับพระราชบัญญัติที่คุ้มครองสิทธิในข้อมูลส่วนบุคคลไว้ด้วยเพียงแต่การคุ้มครอง

[27] **APEC Privacy Update- Beijing Meetings**, 13 August 2014, Hunton and William LPP, available at https://www.huntonprivacyblog.com/2014/08/articles/apec-privacy-update-beijing-meetings/.

ดังกล่าวยังไม่ครอบคลุมข้อมูลส่วนบุคคลทุกประเภทในลักษณะของกฎหมายกลาง โดยเราอาจแบ่งแยกกฎหมายระดับพระราชบัญญัติที่คุ้มครองไว้เป็นสองกลุ่ม ได้แก่

1. การคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

2. การคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติเฉพาะเรื่องต่างๆ ได้แก่

2.1 การคุ้มครองโดยกฎหมายประกอบรัฐธรรมนูญ และกฎหมายสำคัญที่ออกตามความในรัฐธรรมนูญ

2.2 การคุ้มครองตามประมวลกฎหมายแพ่งและประมวลกฎหมายอาญา และกฎหมายที่เกี่ยวข้องกับคดีอาญา

2.3 การคุ้มครองตามกฎหมายปกครอง และที่เกี่ยวข้องกับบุคคล

2.4 การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการติดต่อสื่อสาร สื่อมวลชนและ สถิติ

2.5 การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการขออนุมัติ อนุญาต การประกอบธุรกิจและกิจการที่เกี่ยวข้องกับการเงินการธนาคาร และธุรกรรมทางอิเล็กทรอนิกส์

2.6 การคุ้มครองตามกฎหมายที่เกี่ยวข้องกับการควบคุมการประกอบวิชาชีพต่างๆ

หากวิเคราะห์ถึงการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามที่ปรากฏในกฎหมายฉบับต่างๆ ในประเทศไทย ที่ได้นำเสนอข้างต้น มีข้อสังเกตที่สำคัญคือการคุ้มครองตามพระราชบัญญัติ ข้อมูลข่าวสารของราชการ พ.ศ. 2540 มีลักษณะที่เป็นกฎหมายกลางที่พยายามวางหลักเกณฑ์ทั่วไปในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐขึ้นมา แตกต่างจากกฎหมายเฉพาะอื่นที่มีมาตรการการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามแต่ลักษณะของกฎหมายนั้นๆ และเป็นบทบัญญัติที่กำหนดถึงกระบวนการเข้าถึงข้อมูลข่าวสารของราชการโดยประชาชนเกี่ยวกับการเปิดเผยข้อมูลข่าวสาร แต่ไม่ได้บัญญัติถึงมาตรฐานขั้นตอนในการจัดเก็บข้อมูลข่าวสารส่วนบุคคลในภาครัฐไว้โดยละเอียด ซึ่งขอบเขตในการบังคับใช้กฎหมายก็จะจำกัดเฉพาะข้อมูลข่าวสารส่วนบุคคลที่เป็นข้อมูลข่าวสารของราชการซึ่งอยู่ในการครอบครองของหน่วยงานรัฐ ไม่รวมถึงข้อมูลข่าวสารที่อยู่ในความครอบครองของภาคเอกชน ทั้งนี้ตามมาตรา 4 โดยความหมายของหน่วยงานของรัฐ” ก็หมายความถึง ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ ส่วนราชการสังกัดรัฐสภา ศาลเฉพาะในส่วนที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี องค์กรควบคุมการประกอบวิชาชีพ หน่วยงานอิสระของรัฐและหน่วยงานอื่นตามที่กำหนดในกฎกระทรวง

สำหรับบทบัญญัติในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติเฉพาะต่างๆ ที่มีอยู่หลายกลุ่มกฎหมายนั้น การคุ้มครองส่วนใหญ่จะได้รับการบัญญัติในสองลักษณะ คือ

1) การบัญญัติข้อห้ามมิให้มีการเปิดเผยข้อมูลส่วนบุคคลที่ได้รับรู้มาในการดำเนินการตามกฎหมาย แก่บุคคลอื่น รวมถึงมีบทกำหนดโทษสำหรับผู้ฝ่าฝืน ยกตัวอย่างเช่น พระราชบัญญัติฟื้นฟูสมรรถภาพผู้ติดยาเสพติด พ.ศ. 2545 พระราชบัญญัติคุ้มครองเด็ก พ.ศ. 2546 เป็นต้น

2) การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องตามความเป็นจริง เช่น พระราชบัญญัติการทะเบียนราษฎร พ.ศ. 2534 พระราชบัญญัติประกอบรัฐธรรมนูญว่าด้วยการเลือกตั้งสมาชิกสภาผู้แทนราษฎรและสมาชิกวุฒิสภา พ.ศ. 2541 เป็นต้น

ทั้งนี้มีบทบัญญัติในกลุ่มกฎหมายที่มีลักษณะพิเศษ ที่ให้อำนาจรัฐ เข้าไปแทรกแซงสิทธิส่วนบุคคลในเรื่องข้อมูลข่าวสารส่วนบุคคล ซึ่งเป็นข้อจำกัดในหลักความยินยอมของเจ้าของข้อมูล โดยต้องมีเหตุที่กฎหมายยกเว้นไว้ เช่น สถานการณ์ฉุกเฉิน การสืบสวนสอบสวนคดียาเสพติด คดีพิเศษ การป้องกันการปราบปรามการฟอกเงิน เป็นต้น

เมื่อพิจารณาจากบรรดากฎหมายที่มีอยู่ในประเทศไทยขณะนี้ก็จะเห็นได้ว่า บทบัญญัติข้อห้ามในการจัดเก็บข้อมูลส่วนบุคคลบางประเภทแทบไม่มีการรับรองไว้ เท่าที่ปรากฏอยู่ในปัจจุบันคงมีแต่พระราชบัญญัติประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 ฉะนั้นฝ่ายปกครองจึงมีอำนาจอย่างกว้างในการจัดเก็บข้อมูลส่วนบุคคลจากประชาชน และส่วนมากยังมีเป็นอำนาจออกกฎเกณฑ์ระเบียบกำหนดหน้าที่ให้ภาคเอกชน ต้องจัดเก็บข้อมูลเพื่อให้หน่วยงานรัฐตรวจสอบอย่างสม่ำเสมอ เช่น พระราชบัญญัติโรงแรม พ.ศ. 2547 พระราชบัญญัติโรงรับจำนำ พ.ศ. 2505 พระราชบัญญัติหอพัก พ.ศ. 2507 เป็นต้น ซึ่งอำนาจที่กว้างกว้างเช่นนี้จึงย่อมส่งผลกระทบต่อการคุ้มครองสิทธิส่วนบุคคลอย่างหลีกเลี่ยงไม่ได้ ดังนั้นการพิจารณาวิเคราะห์ถึงปัญหาอุปสรรคในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย จึงมีความจำเป็นต้องเริ่มพิจารณาจากเนื้อหาสาระที่ได้กำหนดไว้ในพระราชบัญญัติข้อมูลข่าวสารของราชการพ.ศ. 2540 เป็นสำคัญในฐานะที่เป็นกฎหมายกลางที่กำหนดวางหลักเกณฑ์ทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของภาครัฐไว้

3.6.1 พัฒนาการการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย

แนวคิดของความจำเป็นที่ต้องมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยได้เริ่มปรากฏให้เห็นจากมติคณะรัฐมนตรีเมื่อวันที่ 28 กุมภาพันธ์ พ.ศ. 2539 ที่ได้เห็นชอบต่อนโยบายเทคโนโลยีสารสนเทศ (ไอที 2000) ที่เสนอโดยกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม ซึ่งมีจุดมุ่งหมายสำคัญเพื่อพัฒนาสังคมและ เสริมสร้างความแข็งแกร่งทางธุรกิจ อุตสาหกรรม และการค้าระหว่างประเทศ ในการก้าวเข้าสู่สังคมสารสนเทศซึ่งเป็นยุคเศรษฐกิจใหม่แห่งศตวรรษที่ 21 โดยหนึ่งในมาตรการที่สำคัญ คือ *การปฏิรูปกฎหมายเทคโนโลยีสารสนเทศ* (Information Technology Law) ซึ่งประกอบด้วยกฎหมาย 6 ฉบับ ได้แก่

1. กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์
2. กฎหมายเกี่ยวกับลายมือชื่อทางอิเล็กทรอนิกส์
3. กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์
4. กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์
5. กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
6. กฎหมายที่ออกเพื่อรองรับรัฐธรรมนูญมาตรา 78 ว่าด้วยการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน

เมื่อวันที่ 15 ธันวาคม พ.ศ. 2541 คณะรัฐมนตรีก็ได้เห็นชอบต่อการจัดทำโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศที่เสนอโดยกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม และเห็นชอบให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee) หรือเรียกย่อว่า "คณะกรรมการไอทีแห่งชาติ หรือ กทสช. (NITC)[28]" ทำหน้าที่เป็นศูนย์กลางและประสานงานระหว่างหน่วยงานต่าง ๆที่กำลังดำเนินการจัดทำกฎหมายเทคโนโลยีสารสนเทศและกฎหมายอื่น ๆที่เกี่ยวข้อง ทั้งนี้ คณะกรรมการดังกล่าวได้แต่งตั้งคณะอนุกรรมการเฉพาะกิจเพื่อยกร่างกฎหมายไอทีทั้ง 6 ฉบับ แยกตามกฎหมายขึ้นมา 6 คณะ โดยมอบหมายให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center , NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมในฐานะสำนักงานเลขานุการคณะกรรมการไอทีแห่งชาติ เป็นเลขานุการในการยกร่างกฎหมาย [29] ซึ่งได้มีการแต่งตั้งคณะอนุกรรมการเฉพาะกิจยกร่างกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้นตามคำสั่งคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ที่ 13/2542 ประกอบด้วยกรรมการทั้งสิ้น 20 ท่าน[30]

ในการศึกษาและจัดทำร่างพระราชบัญญัติคุ้มครองข้อมูลข่าวสารส่วนบุคคล พ.ศ. ... โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center: NECTEC) ซึ่งจะเป็นกฎหมายฉบับแรกที่ให้ความคุ้มครองความเป็นส่วนตัวในข้อมูลส่วนบุคคลโดยเฉพาะ ได้ให้เหตุผลและความจำเป็นในการยกร่างกฎหมายคุ้มครองข้อมูลข่าวสารเกี่ยวกับบุคคลไว้ดังนี้

---

[28]คณะกรรมการชุดนี้จัดตั้งขึ้นตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศ พ.ศ. 2535 โดยมีอำนาจหน้าที่หลักในการเสนอแนะแผนการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติต่อคณะรัฐมนตรีเพื่อพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศ สร้างบรรยากาศให้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงานต่าง ๆ พัฒนาโครงสร้างพื้นฐานด้านโทรคมนาคม ปรับปรุงกฎหมายระเบียบข้อบังคับให้สอดคล้องกับการดำเนินธุรกิจสมัยใหม่โดยสื่ออิเล็กทรอนิกส์ ส่งเสริมการผลิต การบริการ การวิจัยและพัฒนาให้มีเทคโนโลยีด้านสารสนเทศขึ้นในประเทศไทยและส่งเสริมผู้ประกอบการขนาดกลางและขนาดเล็ก.

[29]สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, **โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ**, พิมพ์ครั้งที่ 3, (กรุงเทพมหานคร: เดือนตุลา, 2544), น. 16-17.

[30]อนุกรรมการตามคำสั่งคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ที่ 13/2542 มี ศาสตราจารย์เศรษฐพร คูศรีพิทักษ์ เป็นประธานอนุกรรมการ อนุกรรมการประกอบด้วย อธิบดีผู้พิพากษาศาลแพ่ง อธิบดีผู้พิพากษาศาล อธิบดีผู้พิพากษาศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง ศาสตราจารย์วิฑิต มันตาภรณ์ รองศาสตราจารย์ วรพจน์ วิศรุตพิชญ์ รองศาสตราจารย์ กมลชัย รัตนสกาววงศ์ รองศาสตราจารย์ วิษณุ วรัญญู นายเธียรชัย ณ นคร ผู้แทนสำนักงานคณะกรรมการกฤษฎีกา ผู้แทนกระทรวงมหาดไทย ผู้แทนสำนักงานอัยการสูงสุด ผู้แทนสำนักงานคณะกรรมการกำกับหลักทรัพย์ฯ ผู้แทนกระทรวงการต่างประเทศ ผู้แทนกระทรวงการคลัง ผู้แทนกระทรวงพาณิชย์ ผู้แทนตลาดหลักทรัพย์แห่งประเทศไทย ผู้แทนสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ผู้แทนสมาคมธุรกิจคอมพิวเตอร์ไทย และผู้แทนศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

1. เนื่องจากประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลข่าวสารเกี่ยวกับบุคคลเป็นการเฉพาะ

2. เพื่อพัฒนากฎหมายคุ้มครองข้อมูลข่าวสารเกี่ยวกับบุคคลให้เป็นระบบและสอดคล้องกับกฎหมายที่มีอยู่

3. เพื่อรักษาดุลยภาพระหว่างเสรีภาพในการติดต่อสื่อสาร สิทธิในความเป็นส่วนตัว และความมั่นคงแห่งรัฐ

4. เพื่อพัฒนากฎเกณฑ์ในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลให้สอดคล้องกับที่นานาอารยะประเทศยอมรับ

หลักการและเหตุผลของร่างพระราชบัญญัติฉบับนี้ มีเจตนารมณ์เพื่อคุ้มครองสิทธิความเป็นส่วนตัวในข้อมูลข่าวสารของบุคคล กล่าวคือให้การคุ้มครองสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นส่วนตัว การไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชน อันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคล หรือความเป็นส่วนตัวของบุคคลจะกระทำมิได้ บุคคลมีสิทธิในความเป็นเจ้าของข้อมูลข่าวสารของตน ห้ามผู้ใดนำไปประมวล หรือหากนำไปประมวลผลต้องได้รับความยินยอม และต้องดำเนินการภายในวัตถุประสงค์ของการประมวลผลนั้น ซึ่งการประมวลผลสามารถทำได้ทั้งแบบทั่วไปปกติโดยบุคคล(Manual) และโดยระบบอิเล็กทรอนิกส์ ที่ทำให้สามารถประมวลผลและเผยแพร่ถึงบุคคลจำนวนมากได้โดยง่าย รวดเร็ว และสะดวก โดยอาศัยเทคโนโลยีที่ทันสมัย ดังนั้นการละเมิดสิทธิดังกล่าวจึงทำได้โดยง่ายและเกิดขึ้นโดยเจ้าของไม่รู้ตัว ดังนั้นจึงจำเป็นต้องกำหนดหลักเกณฑ์ที่แน่นอนในการประมวลผลข้อมูลข่าวสารส่วนบุคคล รวมทั้งจำเป็นต้องมีคณะกรรมการเพื่อวางนโยบาย และกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลข่าวสารเกี่ยวกับบุคคล

การศึกษาเพื่อยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของคณะอนุกรรมการเฉพาะกิจนี้ก่อนที่ร่างพระราชบัญญัติฯ จะได้ผ่านความเห็นชอบจากคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ได้มีการปรับเปลี่ยนแนวทางของการยกร่างสองครั้ง ได้แก่ [31]

<u>การยกร่างครั้งแรก</u> ได้ยกร่างขึ้นตามแนวทาง Directive 95/46/EC ของสหภาพยุโรป[32] โดยเน้นที่ประเทศอิตาลีเป็นหลัก รวมทั้งของประเทศอื่นๆในภาคพื้นยุโรปด้วย เนื่องจากประเทศอิตาลีเป็นประเทศที่มีระบบประมวลกฎหมายเช่นเดียวกับประเทศไทย ประกอบกับประเทศในภาคพื้นยุโรปมีพัฒนาการเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลแล้วในระดับหนึ่ง

---

[31]สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, **แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล**, พิมพ์ครั้งที่ 2, (กรุงเทพมหานคร: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547),น. 12-13.

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

อย่างไรก็ตาม ในการประชุมพิจารณาร่างกฎหมายตามแนวทางดังกล่าวพบว่ากลไกหรือหลักการของกฎหมายบางประการจำเป็นต้องพิจารณาอย่างรอบคอบ เนื่องจากการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ได้รับผลกระทบจากพัฒนาการทางเทคโนโลยีค่อนข้างเป็นเรื่องใหม่ ดังนั้น การนำกลไกที่ค่อนข้างเข้มงวดมาบัญญัติเป็นกฎหมายอาจก่อให้เกิดปัญหาทางปฏิบัติในการบังคับใช้กฎหมายได้ ด้วยเหตุนี้จึงได้มีการปรับเปลี่ยนแนวทางของการยกร่างกฎหมายเสียใหม่

<u>การยกร่างครั้งที่สอง</u> เป็นการศึกษากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประเทศอื่นๆเพิ่มเติมนอกเหนือจากสหภาพยุโรปและประเทศภาคพื้นยุโรป ได้แก่ กฎหมายของออสเตรเลีย ฮ่องกงและนิวซีแลนด์ ที่แม้จะมีการกำหนดหลักการใกล้เคียงกับกฎหมายของสหภาพยุโรปก็ตาม แต่ก็มีหลักการและกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลในอีกรูปแบบหนึ่งที่น่าสนใจในลักษณะที่ว่าประเทศดังกล่าวเป็นประเทศที่เพิ่งเริ่มมีพัฒนาการเกี่ยวกับแนวคิดดังกล่าวได้ไม่นาน และมีกลไกการใช้บังคับที่ไม่เข้มงวดมากจนเกินไป นอกจากนี้กฎหมายดังกล่าวยังได้กำหนดกลไกในการกำกับดูแลตนเอง (Self Regulation) โดยให้ผู้ซึ่งเก็บหรือรวบรวมข้อมูล สามารถที่จะกำหนด หรือวางหลักเกณฑ์ในทางปฏิบัติที่สอดคล้องกับการดำเนินงานของตนเองได้ ซึ่งการบัญญัติกฎหมายในแนวทางนี้ค่อนข้างมีความยืดหยุ่น และน่าจะเหมาะสมกับประเทศไทยซึ่งยังอยู่ในช่วงเริ่มต้นของการพัฒนาการให้ความคุ้มครองข้อมูลส่วนบุคคล

ด้วยเหตุดังกล่าว คณะอนุกรรมการฯ และคณะทำงานจึงได้พิจารณาปรับแก้ร่างพระราชบัญญัติฯ ให้เป็นไปในทิศทางเดียวกันกับแนวกฎหมายของออสเตรเลีย ฮ่องกงและนิวซีแลนด์ แทนการจัดทำร่างพระราชบัญญัติฯในรูปแบบเดิมที่มีความเข้มงวดมากกว่า

ขอบเขตของการคุ้มครองตามร่างพระราชบัญญัติฉบับนี้ จากผลการประชุมคณะอนุกรรมการร่างพระราชบัญญัติข้อมูลส่วนบุคคล พ.ศ.... เมื่อวันที่ 24-26 สิงหาคม พ.ศ. 2544 ได้ข้อสรุปดังนี้

1. ขอบเขตการคุ้มครองตามร่างพระราชบัญญัตินี้ ใช้บังคับกับองค์กรเอกชนหรือหน่วยงานอื่นๆที่ไม่ได้เป็นหน่วยงานราชการที่อยู่ภายใต้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 การเขียนข่าวของสื่อสารมวลชน การดำเนินการของนายจ้างอันเกี่ยวข้องกับข้อมูลของลูกจ้าง และการกระทำของบุคคลที่มีวัตถุประสงค์เพื่อประโยชน์ส่วนตัว โดยที่ไม่กระทบต่อประโยชน์ได้เสียของเจ้าของข้อมูล

นิยามของ"ข้อมูลข่าวสารส่วนบุคคล" หมายถึง ข้อเท็จจริงเกี่ยวกับบุคคลใดบุคคลหนึ่งหรือเชื่อได้ว่าเกี่ยวกับบุคคลนั้น ไม่ว่าข้อมูลหรือความเห็นนั้นจะจริงหรือไม่ และไม่ว่าจะมีการบันทึกข้อมูลหรือความเห็นนั้นในสื่อรูปแบบใดก็ตาม

2. การให้ความคุ้มครองข้อมูลส่วนบุคคล โดยการเก็บรวบรวม การใช้ การเปิดเผย แก้ไขหรือเปลี่ยนแปลง ลบ หรือกระทำการใดๆเกี่ยวกับข้อมูลส่วนบุคคล ต้องทำตามวัตถุประสงค์ที่ชอบด้วยกฎหมาย และต้องทำเพียงเท่าที่จำเป็น หรือเกี่ยวข้องโดยตรงกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูลข่าวสารนั้น และต้องแจ้งแก่บุคคลที่เกี่ยวข้องทราบก่อนหรือในทันทีที่มีการเก็บรวบรวมข้อมูลส่วน

บุคคลนั้น และการเปิดเผยต้องได้รับความยินยอมจากเจ้าของข้อมูลนั้นก่อน หรือในขณะที่มีการเปิดเผย

ทั้งนี้ การประมวลผลข้อมูล (Processing) หมายถึง การดำเนินการใดๆอันเกี่ยวกับ การรวบรวม การบันทึก การจัดเก็บ การเปลี่ยนแปลงแก้ไข การใช้ประโยชน์ การเปิดเผย การลบ การทำลาย ฯลฯ

3. การรักษาความปลอดภัยของข้อมูลส่วนบุคคล ผู้เก็บบันทึกหรือครอบครองข้อมูลส่วนบุคคล ต้องมีมาตรการในการรักษาความปลอดภัยข้อมูลข่าวสารไม่ให้สูญหาย มาตรการในการใช้ การเข้าถึง การเปลี่ยนแปลงแก้ไข การเปิดเผยโดยปราศจากอำนาจ หรือการนำไปใช้โดยมิชอบ และระมัดระวังในการเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลอื่นทราบ การกำหนดการเข้าถึงข้อมูล การแก้ไขเปลี่ยนแปลง หลักการใช้ การเปิดเผย

4. ห้ามมิให้เก็บข้อมูลข่าวสารที่มีลักษณะเป็น Sensitive data ได้แก่ ข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ทัศนะทางการเมือง ลัทธิทางศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ หรือข้อมูลอื่นๆที่กระทบความรู้สึกของประชาชน เว้นแต่กฎหมายให้อำนาจ

5. ห้ามมิให้มีการส่งข้อมูลส่วนบุคคลออกนอกราชอาณาจักร ในกรณีที่ประเทศนั้นไม่ได้ให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกัน

6. สิทธิของเจ้าของข้อมูลในการขอให้ ลบ ระงับการใช้ชั่วคราว หรือเปลี่ยนแปลงข้อมูลให้อยู่ในรูปแบบข้อมูลที่ไม่ระบุชื่อ ในกรณีที่มีการดำเนินการโดยมิชอบ หรือมีการเก็บข้อมูลไว้เกินกว่าที่จำเป็น

7. จัดให้มีคณะกรรมการเรียกว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” โดยมีหน้าที่หลักดังต่อไปนี้

(1) กำหนดนโยบาย และตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามพระราชบัญญัติฉบับนี้

(2) ให้คำแนะนำต่อคณะรัฐมนตรีในการตราพระราชกฤษฎีกา ปรับปรุงแก้ไขกฎหมายหรือกฎข้อบังคับ

(3) ให้คำแนะนำ ปรึกษาเกี่ยวกับการดำเนินการเพื่อการคุ้มครองข้อมูลส่วนบุคคล

(4) ส่งเสริมและประชาสัมพันธ์ ให้ความรู้แก่ประชาชนเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล และพิจารณาคำร้องทุกข์ในกรณีการละเมิดข้อมูลข่าวสารส่วนบุคคล

(5) จัดทำรายงานเกี่ยวกับการปฏิบัติการตามพระราชบัญญัติฉบับนี้เสนอต่อคณะรัฐมนตรี

(6) พิจารณาการร้องเรียนและการอุทธรณ์ เมื่อมีการร้องเรียนต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เมื่อมีเหตุอันควรสงสัยว่าจะมีการดำเนินการใดๆเกี่ยวกับข้อมูลส่วนบุคคลที่ทำให้เกิดความเสียหายแก่บุคคลที่เกี่ยวข้อง

(7) กำหนดความรับผิดในทางแพ่ง ในกรณีมีการกำหนดให้มีการรับผิดชดใช้ค่าสินไหมทดแทนเพื่อการดำเนินการใดๆที่เกี่ยวกับข้อมูลข่าวสารส่วนบุคคลที่ก่อให้เกิดความเสียหายต่อบุคคลที่เกี่ยวข้องไม่ว่าจะจงใจหรือประมาทเลินเล่อ

ร่างพระราชบัญญัติฉบับนี้ ถูกนำเสนอเข้าสู่การพิจารณาของคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ โดยได้ผ่านความเห็นชอบในหลักการเมื่อวันที่ 3 ตุลาคม พ.ศ. 2544 ซึ่งต่อมากระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อมได้ส่งเรื่องไปยังสำนักเลขาธิการคณะรัฐมนตรี เมื่อวันที่ 28 ธันวาคม พ.ศ. 2544 เพื่อนำสู่การพิจารณาของคณะรัฐมนตรีต่อไป อย่างก็ตาม ทางสำนักเลขาธิการคณะรัฐมนตรีได้มีการแจ้งขอความเห็นจากหน่วยงานที่เกี่ยวข้องในเรื่องนี้ ซึ่งส่วนใหญ่หน่วยงานต่างๆก็เห็นชอบในหลักการของความจำเป็นที่ต้องมีกฎหมายฉบับนี้ แต่ก็มีการเสนอความเห็นที่เป็นข้อสังเกตถึงอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นใหม่ โดยหน่วยงานที่ไม่เห็นด้วยคือ กระทรวงมหาดไทย สำนักงบประมาณ สำนักงานคณะกรรมการปฏิรูประบบราชการ และสำนักงานปลัดสำนักนายกรัฐมนตรีซึ่งเป็นหน่วยงานที่กำกับดูแลสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

ผลจากความเห็นที่ขัดแย้งดังกล่าว สำนักเลขาธิการคณะรัฐมนตรีจึงยังไม่บรรจุเรื่องเข้าสู่การพิจารณาของคณะรัฐมนตรี โดยส่งเรื่องคืนมาเมื่อวันที่ 20 มีนาคม พ.ศ. 2545 ขอให้กระทรวงวิทยาศาสตร์ฯ โดยเนคเทคในฐานะผู้รับผิดชอบจัดประชุมและหารือกับส่วนราชการที่เสนอความเห็นให้ได้ข้อยุติเสียก่อน ซึ่งก็ยังไม่สามารถหาข้อยุติได้ ดังนั้นกระทรวงวิทยาศาสตร์ฯ จึงได้เสนอร่างกฎหมายฉบับเดิมกลับไปยังสำนักเลขาธิการคณะรัฐมนตรีโดยไม่มีการแก้ไข แต่ได้แนบความเห็นของหน่วยงานไปเพื่อประกอบการพิจารณาของคณะรัฐมนตรีด้วย ซึ่งก็ยังไม่ได้รับการบรรจุเข้าสู่การพิจารณา

เมื่อถึงเดือนตุลาคม พ.ศ. 2545 ซึ่งได้มีการประกาศใช้พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. 2545 โดยมีการจัดตั้งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารขึ้น ตามมาตรา 24 ของพระราชบัญญัติ ซึ่งกำหนดให้มีอำนาจหน้าที่เกี่ยวกับการวางแผน ส่งเสริม พัฒนา และดำเนินกิจการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสาร การอุตุนิยมวิทยา และการสถิติ และราชการอื่นตามที่มีกฎหมายกำหนด ให้เป็นอำนาจหน้าที่ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือส่วนราชการที่สังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ก็มีผลทำให้กระทรวงวิทยาศาสตร์และเทคโนโลยี ได้โอนเรื่องการจัดทำร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ไปให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบตามอำนาจหน้าที่ซึ่งเกี่ยวข้อง ในฐานะที่กฎหมายฉบับนี้เกี่ยวข้องกับภารกิจของกระทรวงโดยตรง

ภายหลังจากที่กระทรวงวิทยาศาสตร์และเทคโนโลยีได้นำส่งร่างพระราชบัญญัติไปยังกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแล้ว เนคเทคได้มีการจัดตั้งคณะทำงานเพื่อศึกษาประเด็นปัญหากฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขึ้นเมื่อวันที่ 27 มีนาคม 2546 ดำเนินการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศเพิ่มเติม และปรับร่างพระราชบัญญัติใน

นัยสำคัญบางประเด็นให้มีความชัดเจนมากขึ้น โดยมีศาสตราจารย์ ดร. ประสิทธิ์ เอกบุตร เป็นประธาน คณะทำงานฯได้เข้าพบรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อวันที่ 7 กรกฎาคม 2546 เพื่อรายงานสถานภาพการพัฒนากฎหมายและรับทราบนโยบายในการปรับร่างพระราชบัญญัติในบางประการก่อนที่จะได้มีการนำเสนอร่างพระราชบัญญัติที่มีการปรับแก้มายังกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ก่อนนำเสนอเข้าสู่กระบวนการนิติบัญญัติตามลำดับต่อไป โดยผลจากการเข้าพบและการศึกษากฎหมายต่างประเทศเพิ่มเติม ทำให้มีการพิจารณาทบทวนหลักการตามร่างพระราชบัญญัติฯ เพื่อให้มีความชัดเจนสอดคล้องกับแนวทางระหว่างประเทศ และแนวปฏิบัติของภาคเอกชนมากขึ้น โดยเฉพาะอย่างยิ่งการพิจารณาประเด็นขอบเขตของกฎหมาย หลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และบทกำหนดโทษ เป็นต้น[33]

ในส่วนการดำเนินการของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการนั้น อยู่บนพื้นฐานความคิดที่ว่าการคุ้มครองข้อมูลส่วนบุคคลส่วนหนึ่ง อยู่ภายใต้การบังคับของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อยู่แล้ว

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 หมวด 3 ได้มีบทบัญญัติที่กำหนดหลักเกณฑ์และแนวทางที่ให้หน่วยงานต่างๆ ของรัฐ จะต้องถือปฏิบัติเกี่ยวเนื่องกับการจัดเก็บ การรวบรวม และการนำไปใช้ซึ่งข้อมูลข่าวสารส่วนบุคคล โดยมีหลักเกณฑ์หรือมาตรการสำคัญที่กำหนดให้หน่วยงานของรัฐต้องถือปฏิบัติ ซึ่งเป็นไปตามหลักปฏิบัติทางสากลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ได้แก่

(1) การกำหนดวัตถุประสงค์การจัดเก็บที่ชัดเจน (Identifying purposes) ตามมาตรา 23(5) วรรคสอง

(2) การจัดให้มีระบบหรือจัดเก็บเท่าที่จำเป็น รวมทั้งยกเลิกระบบดังกล่าวเมื่อหมดความจำเป็น (Limiting Collection and Retention) ตามมาตรา 23 (1)

(3) ข้อมูลข่าวสารส่วนบุคคลที่จัดเก็บจะต้องตรวจแก้ไขให้ถูกต้องอยู่เสมอ (Accuracy) ตามมาตรา 23 (4)

(4) การนำข้อมูลข่าวสารส่วนบุคคลไปใช้หรือไปเปิดเผยจะต้องอยู่ในกรอบวัตถุประสงค์และตามที่กฎหมายกำหนด มิฉะนั้นจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน (Consent, Limiting Use, Disclosure) ตามมาตรา 24

(5) จะต้องมีระบบรักษาความปลอดภัยของข้อมูลข่าวสารส่วนบุคคลเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสม (Safeguards) ตามมาตรา 23 (5)

(6) การกำหนดให้หน่วยงานของรัฐต้องประกาศในราชกิจจานุเบกษาเกี่ยวกับระบบข้อมูลข่าวสารส่วนบุคคลของหน่วยงานของตน เช่น ประเภทของบุคคลและของระบบข้อมูลข่าวสารส่วน

[33] เรื่องเดียวกัน, น. 15.

บุคคลที่จัดเก็บ ลักษณะของการใช้ข้อมูล วิธีการขอตรวจดู วิธีการขอแก้ไขและแหล่งที่มาของข้อมูล (Openness) ตามมาตรา 23 (3)

ในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลนี้ ได้มีการพัฒนาบทบัญญัติและมีการบังคับใช้กฎหมายดังกล่าวในนานาประเทศ โดยเฉพาะในยุโรปและสหรัฐอเมริกา เช่น กรณีสหภาพยุโรปได้มีการออกกฎหมายโดยรัฐสภายุโรป กำหนดแนวทางและหลักเกณฑ์ในการคุ้มครองปกป้องความเป็นส่วนตัวของบุคคลในส่วนที่เกี่ยวกับกระบวนการจัดเก็บ การรวบรวมและการนำไปใช้ซึ่งข้อมูลข่าวสารส่วนบุคคล ตลอดจนมาตรการที่จะทำให้การเชื่อมโยงข้อมูลส่วนบุคคลโดยเสรีที่จะไม่กระทบต่อมาตรการคุ้มครองความเป็นส่วนตัวของบุคคล (Directive 95/46/EU of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) ทั้งนี้ EU Directive มีหลักสำคัญ คือ กำหนดให้ประเทศสมาชิกในสหภาพยุโรปจะต้องมีมาตรฐานการคุ้มครองสิทธิและเสรีภาพของบุคคลในเรื่องที่เกี่ยวกับความเป็นส่วนตัว ในส่วนที่เกี่ยวกับกระบวนการจัดเก็บ การรวบรวมและการนำไปใช้ซึ่งข้อมูลข่าวสารส่วนบุคคล รวมทั้งกำหนดเงื่อนไขที่จะไม่ให้ประเทศสมาชิก ยินยอมให้มีการส่งผ่านข้อมูลข่าวสารส่วนบุคคลไปยังประเทศ อื่น ๆ นอกสหภาพยุโรป ที่มีมาตรฐานในการคุ้มครองข้อมูลข่าวสารส่วนบุคคลต่ำกว่ามาตรฐานที่สหภาพยุโรปกำหนด เช่น ข้อมูลข่าวสารที่เกี่ยวกับธุรกิจการบิน เป็นต้น

ด้วยเหตุผลดังกล่าวข้างต้น คณะกรรมการข้อมูลข่าวสารของราชการได้มอบหมายให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ทำการศึกษาและเตรียมการดำเนินงานเพื่อการคุ้มครองข้อมูลข่าวสารส่วนบุคคลของประเทศไทย ให้เป็นไปตามมาตรฐานสหภาพยุโรป และมาตรฐานนานาชาติในหลาย ๆ ประการ เช่น การส่งเจ้าหน้าที่ไปร่วมประชุมด้านการคุ้มครองข้อมูลข่าวสารส่วนบุคคลและความเป็นส่วนตัวในระดับนานาชาติ (International Conference of Personal Data and Privacy Protection) ตลอดจนการจัดประชุมสัมมนาเรื่องดังกล่าวขึ้นในประเทศไทยหลายครั้ง รวมทั้งได้มอบหมายให้สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ ให้ศึกษาและจัดทำความเห็นทางวิชาการเกี่ยวกับหลักเกณฑ์และแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งคณะผู้วิจัยได้ยกร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... อีกฉบับ และได้ผ่านการระดมความคิดเห็นจากนักวิชาการและหน่วยงานต่างๆ ในชั้นต้นเมื่อวันที่ 28 มกราคม พ.ศ. 2547

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ได้เสนอร่างกฎหมายดังกล่าวให้ที่ประชุมสัมมนาร่วมระหว่างคณะกรรมการข้อมูลข่าวสารของราชการและคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารพิจารณา ในระหว่างวันที่ 27 - 29 กุมภาพันธ์ พ.ศ. 2547 ณ โรงแรมมิชชั่นฮิลล์กอล์ฟคลับ เขาใหญ่ จังหวัดนครราชสีมา ซึ่งที่ประชุมสัมมนาได้มีการพิจารณาให้ความเห็นเพื่อให้ผู้ศึกษานำไปปรับปรุงแก้ไขร่างกฎหมายหลายประการ

หลังจากนั้นสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการได้นำเสนอร่างกฎหมายซึ่งมีการปรับปรุงแก้ไขตามข้อเสนอของที่ประชุมสัมมนาดังกล่าวข้างต้นเพื่อให้คณะกรรมการข้อมูลข่าวสารของราชการพิจารณาให้ความเห็นชอบในหลักการของร่างกฎหมายในการประชุมครั้งที่ 1/2547 เมื่อวันที่ 27 เมษายน 2547 ซึ่งที่ประชุมมีมติให้จัดประชุมสัมมนาทางวิชาการระหว่างคณะกรรมการข้อมูลข่าวสารของราชการ คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร ผู้แทนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ผู้แทนกระทรวงวิทยาศาสตร์และเทคโนโลยี และผู้แทนหน่วยงานที่เกี่ยวข้อง เพื่อร่วมกันพิจารณาเกี่ยวกับนโยบายและร่างกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้จัดทำร่าง และร่างที่คณะผู้วิจัยแห่งสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์ ที่มีรองศาสตราจารย์ สมยศ เชื้อไทย เป็นหัวหน้าคณะผู้วิจัย เป็นผู้จัดทำร่างขึ้นรวม 2 ฉบับ เพื่อหาข้อยุติในการดำเนินการที่เหมาะสมและสอดคล้องกับสถานการณ์ในปัจจุบันอีกครั้ง

ในการสัมมนาดังกล่าวมีข้อสังเกตให้มีการปรับปรุงแก้ไขร่างกฎหมายหลายประการ อย่างไรก็ตาม เนื่องจากร่างกฎหมาย 2 ฉบับ ที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารและคณะกรรมการข้อมูลข่าวสารของราชการ ต่างมีจุดมุ่งหมายที่ต้องการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของเอกชนเหมือนกัน แม้จะมีบทบัญญัติในรายละเอียดที่แตกต่างกันบ้าง ซึ่งผลจากการสัมมนามีความชัดเจนว่าควรมีกฎหมายเพื่อวัตถุประสงค์ดังกล่าวนี้เพียงฉบับเดียว และการจัดตั้งสำนักงานใหม่ควรดำเนินการเฉพาะเท่าที่จำเป็น เพื่อมิให้เกิดความซ้ำซ้อนและประหยัดโดยให้นำผลจากการสัมมนาไปปรับปรุงร่างกฎหมายให้สมบูรณ์เหมาะสมที่สุดต่อไป ดังนั้น จึงมีมติให้รายงานคณะกรรมการกลั่นกรองเรื่องเสนอคณะรัฐมนตรี คณะที่ 5 (ฝ่ายสังคม วิจัย วิทยาศาสตร์และเทคโนโลยี) เพื่อมีมติให้คณะกรรมการข้อมูลข่าวสารของราชการและกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรับร่างกฎหมายทั้งสองฉบับมาปรับปรุงแก้ไขให้เป็นฉบับเดียวเพื่อเสนอคณะกรรมการกลั่นกรองฯ พิจารณาอีกครั้งหนึ่งก่อนนำเสนอคณะรัฐมนตรี

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการได้สรุปรายงานให้คณะกรรมการข้อมูลข่าวสารของราชการพิจารณาว่า แม้ว่าในการสัมมนามิได้มีการหารืออย่างชัดเจนในประเด็นที่ว่าหน่วยงานใดสมควรจะเป็นผู้ที่รับผิดชอบการดำเนินการตามที่ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... แต่สามารถสรุปเป็นความเห็นเสนอเพื่อพิจารณาได้ ดังนี้

(1) ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายกลางด้านการคุ้มครองข้อมูลส่วนบุคคล มิใช่กฎหมายที่เกี่ยวกับเทคโนโลยีเฉพาะด้าน ดังนั้นที่ประชุมสัมมนาจึงไม่มีผู้หนึ่งผู้ใดโต้แย้งหรือมีข้อสังเกตในทางไม่เห็นด้วยกรณีที่สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการจะเป็นหน่วยงานที่รับผิดชอบตามร่างกฎหมายที่เสนอโดยให้ถือว่าเป็นประเด็นที่จะต้องตัดสินใจในระดับนโยบาย

(2) เนื่องจากคณะรัฐมนตรีได้มีมติเห็นชอบในหลักการการแก้ไขพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 โดยยกฐานะของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการให้

มีฐานะเทียบเท่ากรม สังกัดสำนักนายกรัฐมนตรี ซึ่งขณะนี้ร่างกฎหมายดังกล่าวอยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา ประกอบกับสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการได้รับผิดชอบเป็นฝ่ายธุรการและวิชาการของคณะกรรมการข้อมูลข่าวสารของราชการ ในการดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล ที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐอยู่แล้ว ดังนั้น จึงเห็นว่าสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการควรเป็นหน่วยงานผู้รับผิดชอบการดำเนินการตามร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลนี้ด้วย เพราะการบังคับใช้กฎหมายในด้านนี้จะมีเอกภาพโดยมีการบูรณาการด้านบุคลากรแผนงานและแนวปฏิบัติเพื่อประหยัดค่าใช้จ่ายและมีประสิทธิภาพยิ่งขึ้น และเนื่องจากสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการมีความพร้อมในเรื่องประสบการณ์ ความรู้ ความเข้าใจ สอดคล้องกับหลักสากลที่ถือปฏิบัติกันในการมีมาตรการคุ้มครองข้อมูลส่วนบุคคลภาครัฐและภาคเอกชนอยู่ในหน่วยงานเดียวกัน

คณะกรรมการข้อมูลข่าวสารของราชการในการประชุม ครั้งที่ 3/2547 เมื่อวันจันทร์ที่ 2 กรกฎาคม 2547 ได้มีมติให้แจ้งมติคณะกรรมการฯ รวม 2 ประเด็น ให้คณะกรรมการกลั่นกรองเรื่องเสนอคณะรัฐมนตรี คือให้พิจารณามอบหมายให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการรวมร่างกฎหมายทั้งสองฉบับให้เป็นฉบับเดียว และให้พิจารณามีมติกำหนดให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ เป็นหน่วยงานที่มีหน้าที่รับผิดชอบทางธุรการและวิชาการตามร่างกฎหมายฉบับใหม่นี้

สำนักเลขาธิการคณะรัฐมนตรีได้แจ้งไปยังกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเพื่อขอความเห็นเกี่ยวกับมติของคณะกรรมการข้อมูลข่าวสารของราชการใน 2 ประเด็นดังกล่าว และเมื่อได้รับทราบความเห็นแล้วก็จะเชิญผู้แทนของกระทรวงเทคโนโลยีสารสนเทศ และผู้แทนของคณะกรรมการข้อมูลข่าวสารของราชการไปร่วมชี้แจงต่อคณะกรรมการกลั่นกรองเรื่องเสนอต่อคณะรัฐมนตรี ซึ่งคณะรัฐมนตรีก็ได้มีมติให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นเจ้าภาพในการดำเนินงาน ซึ่งร่างกฎหมายดังกล่าวอยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา

การยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยภายหลังได้มีการยกจัดทำขึ้น ซึ่งร่างแรกเป็นร่างดั่งเดิมตามโครงการปฏิรูปกฎหมายเทคโนโลยีสารสนเทศของรัฐบาล โดยเจ้าภาพคือ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารซึ่งรับโอนภารกิจหน้าที่มาจากศูนย์เทคโนโลยีอีเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) กระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม ซึ่งได้โอนภารกิจในส่วนนี้มาเป็นของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารภายหลังการปฏิรูปราชการเมื่อเดือนตุลาคม 2545 ต่อมาจากความเห็นที่ไม่ตรงกันของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ทำให้ได้มีการยกร่างกฎหมายฉบับที่สองขึ้นอีกร่างหนึ่งโดยสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งเกิดจากการไม่เห็นด้วยในรายละเอียดบางประการของร่างฉบับแรก ทั้งนี้ประเด็นที่สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการไม่เห็นด้วย ได้แก่[34]

[34]หนังสือที่ นร 1405/1416 วันที่ 18 กุมภาพันธ์ พ.ศ. 2545.

1. การใช้ถ้อยคำหรือภาษาในการร่างกฎหมายยังไม่มีความชัดเจนเพียงพอ หรือมีขอบเขเพียงใด (มาตรา 8(3) มาตรา 9 มาตรา 10 มาตรา 11 มาตรา 12 มาตรา 13 มาตรา 15 มาตรา 18 และมาตรา 19)

2. การที่มาตรา 28 และมาตรา 41 กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจในการพิจารณาทั้งในเรื่องการกำกับดูแล หรือกำหนดมาตรการในการปฏิบัติตามกฎหมายและพิจารณาวินิจฉัยข้อขัดแย้งเกี่ยวกับข้อมูลส่วนบุคคลของฝ่ายต่างๆด้วยนั้น เห็นว่า ควรที่จะแยกอำนาจหน้าที่ออกจากกันโดยให้มีคณะกรรมการ 2 คณะรับผิดชอบ คือ คณะกรรมการด้านนโยบายและคณะกรรมการวินิจฉัย

3. หลักในเรื่องความรับผิดทางแพ่งมีข้อยกเว้นให้ผู้กระทำละเมิดไม่ต้องรับผิดเมื่อพิสูจน์ได้ว่างานดำเนินการครบถ้วนตามประมวลจริยธรรมที่จัดทำขึ้นแล้วนั้น อาจเป็นช่องทางที่จะใช้หลีกเลี่ยงความรับผิดได้ (มาตรา 47)

4. บทกำหนดโทษควรให้มีความสัมพันธ์กับลักษณะของคดีที่มีความแตกต่างกัน หรือมีระดับเรื่องเล็กหรือใหญ่แตกต่างกัน ไม่ควรจะกำหนดบทลงโทษเหมือนกันทั้งหมด (มาตรา 50 และมาตรา 42)

5. การจัดตั้งสำนักงานคณะกรรมการข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้ให้เป็นหน่วยงานของรัฐขึ้นใหม่ เพื่อทำหน้าที่เป็นหน่วยงานงานธุรการของคณะกรรมการข้อมูลข่าวสารส่วนบุคคล โดยมีฐานะเป็นนิติบุคคลอยู่ในกำกับของกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมนั้น เห็นว่า น่าจะเหมาะสม ในเรื่องนี้ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ได้จัดตั้งสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการในสังกัดสำนักงานปลัดสำนักนายกรัฐมนตรีอยู่แล้ว จึงสมควรกำหนดให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอีกหน้าที่หนึ่งจะเหมาะสมกว่า โดยมีเหตุผล ดังนี้

5.1 พระราชบัญญัติข้อมูลข่าวสารของราชการฯ ครอบคลุมข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานรัฐ เช่น ข้อมูลประกันสังคม ข้อมูลคนป่วยในโรงพยาบาลของรัฐ ข้อมูลทะเบียนราษฎร์ ข้อมูลเกี่ยวกับทะเบียนขนส่ง และข้อมูลของกรมทะเบียนการค้า เป็นต้น

5.2 พระราชบัญญัติข้อมูลข่าวสารของราชการฯ กำหนดให้มีคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร ซึ่งปัจจุบันมี 5 สาขา นอกจากจะทำหน้าที่วินิจฉัยการเปิดเผยข้อมูลข่าวสารของราชการแล้ว ยังทำหน้าที่พิจารณาปัญหาการเปิดเผยข้อมูลส่วนบุคคลรวมอยู่ด้วย และได้ปฏิบัติหน้าที่ดังกล่าวมาเป็นเวลาเกือบ 4 ปีแล้ว จึงมีความเชี่ยวชาญในการใช้หลักพิจารณาวินิจฉัย และหากนำเรื่องข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ในส่วนของการวินิจฉัยร้องทุกข์ให้อยู่ภายใต้การดำเนินการของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารก็สามารถกระทำได้โดยการแต่งตั้งคณะกรรมการวินิจฉัยฯ ในสาขาข้อมูลส่วนบุคคลนี้เพิ่มขึ้นตามความจำเป็น

5.3 คณะกรรมการข้อมูลข่าวสารของราชการ มีอำนาจหน้าที่ในการกำหนดนโยบายและกำกับดูแล เกี่ยวกับข้อมูลข่าวสารส่วนบุคคลอยู่ด้วย สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการซึ่งทำหน้าที่เป็นหน่วยธุรการและวิชาการให้กับคณะกรรมการข้อมูลข่าวสารของราชการ จึงมีประสบการณ์ที่จะปฏิบัติงานในฐานะหน่วยงานสนับสนุนให้กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ทันที เนื่องจากมีหลักการสำคัญคล้ายคลึงกันกับพระราชบัญญัติข้อมูลข่าวสารของราชการฯ ในส่วนที่เกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล

5.4 การให้มีหน่วยธุรการอยู่ในหน่วยงานเดียวกันทั้งในส่วนของกฎหมายข้อมูลข่าวสารของราชการและกฎหมายคุ้มครองข้อมูลส่วนบุคคล จะช่วยทำให้การประสานงานการดำเนินการและการกำหนดมาตรฐานหลักเกณฑ์ต่าง ๆ ไปในทิศทางเดียวกันโดยเฉพาะอย่างยิ่งในส่วนของข้อมูลข่าวสารส่วนบุคคลของภาครัฐและเอกชน

5.5 สำหรับการประมวลผลข้อมูลส่วนบุคคล ซึ่งต้องมีเทคโนโลยีเข้ามาเกี่ยวข้องนั้น สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการสามารถตรวจสอบ และควบคุมการดำเนินการได้เนื่องจากมีเจ้าหน้าที่ด้านนี้อยู่แล้ว หรืออาจแต่งตั้งคณะอนุกรรมการด้านเทคโนโลยีการประมวลผลข้อมูลเพื่อช่วยการพิจารณาได้

6. ร่างพระราชบัญญัติฉบับนี้ควรให้นายกรัฐมนตรีเป็นผู้รักษาการ และควรอยู่ในความรับผิดชอบของสำนักงานปลัดสำนักนายกรัฐมนตรี

ความเห็นที่ไม่ลงรอยกันดังกล่าวนำมาสู่การชะลอเรื่องในการพิจารณาร่างพระราชบัญญัติฯ ของ NECTEC ที่เสนอให้คณะรัฐมนตรีพิจารณาซึ่งสำนักเลขาธิการคณะรัฐมนตรีขอให้หน่วยงานที่เกี่ยวข้องไปตกลงกันในรายละเอียดที่ขัดแย้งกันเสียก่อน และก็ก่อให้เกิดการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นอีกฉบับโดยสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ

เมื่อพิจารณาถึงร่างพระราชบัญญัติทั้งสองฉบับของสองหน่วยงาน ก็มีความแตกต่างกันในเนื้อหาหลายประการซึ่งมีความจำเป็นที่จะต้องศึกษาวิเคราะห์ลงไปในความไม่เหมือนกันนั้น เพื่อให้ได้ข้อสรุปถึงแนวทางที่เหมาะสมที่สุดกับการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นในประเทศไทย ทั้งนี้ความแตกต่างของร่างกฎหมายทั้งสองฉบับเริ่มต้นที่จำนวนมาตรา ที่ร่างของกระทรวง ICT มีจำนวน 59 มาตรา ร่างของ สขร. มี 51 มาตรา ขณะที่จำนวนหมวดร่างของ สขร. มีมากกว่าคือ 9 ต่อ 7 โดยไม่รวมบทเฉพาะกาล

ตารางเปรียบเทียบความแตกต่างร่างพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..ที่มีการเสนอในอดีต

ร่างของ สขร.	ร่างของกระทรวง ICT
หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หมวด 2 สำนักงานคณะกรรมการข้อมูลข้าวสารแห่งชาติ หมวด 3 การประมวลผลข้อมูลส่วนบุคคล ส่วนที่ 1 การเก็บรวบรวมข้อมูลส่วนบุคคล ส่วนที่ 2 การใช้และการเปิดเผยข้อมูลส่วนบุคคล ส่วนที่ 3 การเก็บรักษา การแก้ไข และการโอนข้อมูลส่วนบุคคล หมวด 4 สิทธิของเจ้าของข้อมูลส่วนบุคคล หมวด 5 อำนาจและหน้าที่นายทะเบียน หมวด 6 พนักงานเจ้าหน้าที่ หมวด 7 มาตรการส่งเสริม หมวด 8 ความรับผิดทางแพ่ง หมวด 9 บทกำหนดโทษ บทเฉพาะกาล	หมวด 1 การให้ความคุ้มครองข้อมูลส่วนบุคคล ส่วนที่ 1 การเก็บรวบรวมข้อมูลส่วนบุคคล ส่วนที่ 2 การประมวลผลข้อมูลส่วนบุคคล ส่วนที่ 3 สิทธิของเจ้าของข้อมูล ส่วนที่ 4 การใช้หรือโอนข้อมูลส่วนบุคคล หมวด 2 นโยบายการคุ้มครองข้อมูลส่วนบุคคล หมวด 3 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หมวด 4 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หมวด 5 การร้องเรียนและการอุทธรณ์ หมวด 6 ความรับผิดทางแพ่ง หมวด 7 บทกำหนดโทษ บทเฉพาะกาล

ทั้งนี้หากพิจารณาถึงสาระสำคัญของเนื้อหาตามกฎหมายนั้นทั้งสองร่างมีความต่างกันอย่างเห็นได้ชัดในหลายประเด็นต่อไปนี้

1. การให้คำนิยามศัพท์และขอบเขตข้อยกเว้นการบังคับใช้กฎหมาย
2. ผู้รักษาการตามกฎหมาย
3. การจัดโครงสร้างองค์กรและองค์ประกอบของคณะกรรมการคุ้มครองข้อมูลฯ
4. การจัดองค์กรหน่วยงานธุรการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
5. รายละเอียดมาตรการการคุ้มครองข้อมูลส่วนบุคคล
6. ประเด็นเรื่องความรับผิดทางแพ่ง
7. ประเด็นเรื่องบทกำหนดโทษ

โดยรายละเอียดความแตกต่างในร่างพระราชบัญญัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลระหว่างสำนักงานปลัดสำนักนายกรัฐมนตรีและกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ในประเด็นที่กล่าวมาข้างต้น มีดังนี้

1. ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลควรบัญญัติอย่างกว้างและครอบคลุม

เนื่องจากร่างกฎหมายคุ้มครองข้อมูลข่าวสารเป็นกฎหมายซึ่งเป็นกฎหมายซึ่งเจตนารมณ์ของการร่างเพื่อให้เป็นบทบัญญัติทั่วไป ดังนั้น บทบัญญัติดังกล่าวจึงควรมีลักษณะกว้างและครอบคลุมเพื่อสามารถปรับใช้กับสถานการณ์ที่หลากหลายและสถานการณ์ใหม่ๆที่อาจเกิดขึ้นในอนาคต ในส่วนของรายละเอียดเกี่ยวกับการปฏิบัติการตามพระราชบัญญัตินี้โดยออกเป็นกฎหมายลำดับรอง ประมวลจริยธรรมเพื่อเป็นแนวปฏิบัติ หรือกฎเกณฑ์ เพื่อกำหนดหลักเกณฑ์หรือรายละเอียดต่อไป

ในร่างของกระทรวง ICT มีลักษณะเป็นการกำหนดมาตรฐานขั้นต่ำ และเป็นการเปิดโอกาสให้องค์กรสามารถแนวทางปฏิบัติเพื่อคุ้มครองความเป็นส่วนตัวภายในหน่วยงานของตน ซึ่งเป็นไปตามแนวทางระบบ self –regulation ซึ่งการเปิดโอกาสให้หน่วยงานสามารถออกแนวทางปฏิบัติเพื่อใช้ในการควบคุมและคุ้มครองข้อมูลข่าวสารส่วนบุคคลภายในหน่วยงานของตน

2. คณะกรรมการคุ้มครองความเป็นส่วนตัว

ในส่วนของคณะกรรมการฯและอำนาจหน้าที่ของคณะกรรมการทั้งร่างของ สขร. และร่างของ ICT ได้บัญญัติเนื้อหาไว้ค่อนข้างละเอียดและมีอำนาจหน้าที่กว้างขวางเช่นเดียวกับบทบัญญัตินานาประเทศทั่วไป เช่น การกำหนดนโยบาย มาตรการและแผนงานต่างๆเพื่อการคุ้มครองข้อมูลส่วนบุคคล ให้คำแนะนำ ส่งเสริม และตรวจสอบการให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานหรือองค์กร พิจารณาร้องทุกข์ ออกระเบียบ ข้อบังคับ หรือกฎเกณฑ์ต่างๆเพื่อดำเนินการให้บรรลุวัตถุประสงค์ตามกฎหมายนี้ เสนอแนะ ปรับปรุงและทบทวนบทบัญญัติกฎหมาย จัดทำรายงานประจำปี เป็นต้น

3. การจดทะเบียน

ร่างของ สขร. กำหนดให้มีการดำเนินการจดทะเบียนขององค์กรที่มีการดำเนินการเก็บประมวลผลข้อมูลข่าวสาร ในขณะที่ร่างของ ICT กำหนดให้หากคณะกรรมการฯเห็นว่าสมควรให้มีการลงทะเบียนในธุรกิจกิจบางอย่างบางประเภทในกรณีที่จำเป็นเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือในระบบบริหารจัดการข้อมูลส่วนบุคคล หรือเพื่อป้องกันความเสียหายต่อสาธารณชน (มาตรา 18)

ซึ่งมาตรานี้องค์กรเอกชนได้แสดงความเห็นต่อร่างของ สขร ว่า เอกชนเป็นห่วงว่าการดำเนินการจดทะเบียนจะเป็นการสร้างภาระให้กับภาคเอกชนเองที่จะต้องจัดทำเอกสารเพื่อใช้ในการจดทะเบียน หรือแม้กระทั่งต่อภาครัฐต้องเกิดภาระหน้าที่ในการจัดทำระบบทะเบียนและการเก็บรักษาข้อมูลข่าวสารในการจดทะเบียนดังกล่าว ซึ่งอาจเป็นการสร้างภาระเกินความจำเป็น

ระบบการจดทะเบียนเป็นระบบที่ใช้ในภาคพื้นยุโรปซึ่งได้กำหนดให้องค์กรที่ดำเนินการประมวลผลข้อมูลต้องจดทะเบียนต่อนายทะเบียนเพื่อประโยชน์ในการควบคุมตรวจสอบ ซึ่งการใช้

ระบบจดทะเบียนนี้เห็นว่ามีประโยชน์ในการควบคุมตรวจสอบแต่ต้องมีการจัดระบบการลงทะเบียนและระบบการจัดเก็บและมาตรการต่างๆในการดำเนินการจดทะเบียน แก้ไขข้อมูลข่าวสารในส่วนนี้อย่างดีและอำนวยความสะดวกแก่องค์กรผู้ดำเนินการประมวลข้อมูลข่าวสารระดับหนึ่ง เพราะองค์กรเอกชนแสดงความเป็นห่วงมากเรื่องความคล่องตัวในการดำเนินการจดทะเบียน นอกจากนี้ยังรวบถึงความคล่องตัวในการปรับปรุงข้อมูลด้วย

4. บุคคลที่ได้รับการคุ้มครองและสิทธิของเจ้าของข้อมูล

ร่างของ สขร บุคคลรวมถึงบุคคลธรรมดาและนิติบุคคลเว้นแต่มีบทบัญญัติแห่งกฎหมายในการประมวลผลข้อมูลส่วนบุคคลเรื่องหนึ่งเรื่องใดไว้เป็นการเฉพาะ

ความเห็น : ถึงแม้ว่าความเห็นส่วนหนึ่งจะเห็นว่าบุคคลธรรมดาและนิติบุคคลพึงได้รับการคุ้มครองข้อมูลข่าวสารเท่าเทียมกันในฐานะที่เป็นบุคคลตามกฎหมายเหมือนกัน แต่หากพิจารณาวัตถุประสงค์ที่แท้จริงของกฎหมายนี้เพื่อคุ้มครองสิทธิส่วนตัวของบุคคลธรรมดาและเกี่ยวกับสิทธิมนุษยชน และศักดิ์ศรีความเป็นมนุษย์ ซึ่งเป็นสิทธิซึ่งมีได้เฉพาะบุคคลธรรมดาเป็นสำคัญ ดังนั้น เห็นว่า การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายนี้ควรมีขอบเขตเฉพาะการคุ้มครองข้อมูลข่าวสารของบุคคลธรรมดาเท่านั้น ส่วนข้อมูลข่าวสารของนิติบุคคลนั้นย่อมได้รับความคุ้มครองตามประมวลกฎหมายแพ่งและพาณิชย์ ประมวลกฎหมายอาญา และกฎหมายเฉพาะอื่นๆที่เกี่ยวข้องอยู่แล้ว

5. สำนักงาน

ร่างฯ สขร. เสนอให้มีองค์กรเดียว คือ สำนักงานคณะกรรมการข้อมูลข่าวสารแห่งชาติโดยให้เป็นส่วนราชการที่ไม่สังกัดสำนักนายกรัฐมนตรี กระทรวงหรือทบวง มีฐานะเป็นกรม อยู่ในบังคับบัญชาและขึ้นตรงต่อนายกรัฐมนตรี ให้เลขาธิการเป็นผู้บังคับบัญชาและรับผิดชอบในการปฏิบัติราชการของสำนักงาน

ร่างฯของ ICTให้จัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยให้สำนักงานมีฐานะเป็นนิติบุคคลในกำกับของกระทรวงเทคโนโลยีสนเทศและการสื่อสาร โดยมีระบบที่แตกต่างจากระบบราชการเพื่อให้เกิดความคล่องตัวภายใต้นโยบายคณะกรรมการ และให้สำนักงานนี้ปฏิบัติหน้าที่ตามหลักเกณฑ์ ระเบียบ ข้อบังคับตามที่คณะกรรมการกำหนด

ร่างฯทั้งสองฉบับนี้ตั้งใจให้สำนักงานฯ เป็นหน่วยงานธุรการของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยเน้นว่าสำนักงานต้องมีการดำเนินงานที่เป็นอิสระไม่อยู่ภายใต้อำนาจขององค์กรหรือหน่วยงานราชการใด ซึ่งเห็นว่า การที่จะทำให้สำนักงานมีความอิสระอย่างแท้จริงและสามารถดำเนินงานได้อย่างคล่องตัวได้อย่างแท้จริงนั้น ร่างของ สขร. น่าจะสามารถปฏิบัติงานได้อย่างมีอิสระและมีความคล่องตัวมากกว่า เนื่องจากเป็นหน่วยงานที่ไม่สังกัดหน่วยราชการใดขึ้นตรงต่อนายกฯและมีสถานะที่เป็นกรมซึ่งมีอำนาจหน้าที่สูงพอแก่การดำเนินงานอย่างเป็นอิสระ ในขณะที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในร่างของ ICT ถึงแม้จะบัญญัติให้มีการดำเนินงานที่แตกต่าง

จากระบบราชการทั่วไปแต่ก็อยู่ภายใต้กำกับของกระทรวงเทคโนโลยีสนเทศและการสื่อสาร ดังนั้น การปฏิบัติงานอาจติดอยู่กับระบบราชการและอาจไม่มีความเป็นอิสระอย่างแท้จริง

ร่างของ สขร. ให้นายกเป็นผู้รักษาการตามพระราชบัญญัตินี้ และมีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้ ในขณะที่ร่างของ ICT ให้รัฐมนตรีว่ากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามกฎหมายนี้

ในการคุ้มครองสิทธิในความเป็นอยู่ส่วนตัว ในประเทศสหรัฐอเมริกาซึ่งมีการคุ้มครองในรูปแบบของคณะกรรมาธิการขึ้นตรงต่อประธานาธิบดี ซึ่งถือว่าเป็นองค์กรที่มีความเป็นกลางและไม่ตกอยู่ภายใต้อำนาจทางการเมือง แต่อย่างไรก็ตามคณะกรรมาธิการดังกล่าวไม่มีสำนักงานฯคอยปฏิบัติงานให้เป็นไปตามวัตถุประสงค์ การดำเนินการคุ้มครองโดยคณะกรรมาธิการจึงไม่ประสบความสำเร็จ ในขณะที่ประเทศในภาคพื้นยุโรปส่วนใหญ่สำนักงานฯเป็นองค์กรที่มีความเป็นอิสระขึ้นตรงต่อผู้ว่าการรัฐฯหรือต่อนายกรัฐมนตรีเป็นส่วนใหญ่

6. คณะกรรมการข้อมูลส่วนบุคคล

คณะกรรมการข้อมูลส่วนบุคคลร่าง สขร. ประกอบไปด้วย

1. ข้าราชการฝ่ายบริหาร 7 คน ประกอบไปด้วยปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงกลาโหม ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร อธิบดีกรมการปกครอง อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ อัยการสูงสุดและเลขาธิการสำนักงานคณะกรรมการคุ้มครองผู้บริโภค ซึ่งเป็นคณะกรรมการโดยตำแหน่ง

2. กรรมการ 7 คนโดยพิจารณาจากบุคลภายนอก ได้แก่ภาคเอกชนที่มีการประมวลผลข้อมูลข่าวสารจำนวนมาก ปัญหา คือ แค่ไหน อย่างไร เรียกว่ามีการประมวลผลข้อมูลข่าวสารจำนวนมาก ต้องจัดแบ่งระดับหรือขนาดของการเก็บ แบ่งจากอะไร ซึ่งมีจำนวนมากถึง 7 คน

3. กรรมการผู้เชี่ยวชาญซึ่งเป็นผู้ทรงคุณวุฒิ จำนวน 7 คน

ร่าง สขร. แม้ว่าคณะกรรมการฯจะประกอบไปด้วยสายข้าราชการ บุคคลภายนอก และผู้ทรงคุณวุฒิ ในอัตราส่วนเท่าๆกัน แต่จะเห็นได้ว่า กรรมการผู้ทรงคุณวุฒิเป็นกรรมการซึ่งได้รับคัดเลือกจากคณะรัฐมนตรีแต่งตั้ง ดังนั้น อาจได้รับอิทธิพลทางการเมืองเข้ามาเกี่ยวข้อง

ขณะที่ร่างฯของ ICT คณะกรรมการข้อมูลส่วนบุคคลประกอบไปด้วย

1. ผู้ทรงคุณวุฒิซึ่งคณะรัฐมนตรีแต่งตั้งโดยการเสนอชื่อของรัฐมนตรีอีกจำนวนเก้าคน

2. ผู้ซึ่งมีความเชี่ยวชาญในสาขาวิชานิติศาสตร์ พาณิชย์อิเล็กทรอนิกส์หรือวิทยาการคอมพิวเตอร์

3. ผู้ซึ่งเป็นหรือเคยเป็นอาจารย์ในสาขาวิชานิติศาสตร์ พาณิชย์อิเล็กทรอนิกส์หรือวิทยาการคอมพิวเตอร์ ในสถาบันการศึกษาของรัฐในระดับมหาวิทยาลัย

4. คณะกรรมการข้อมูลข่าวสารของราชการเสนอรายชื่อจำนวนหนึ่งคนและหนึ่งคนจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

5. ผู้ซึ่งสมาคมสมาพันธ์เทคโนโลยีสารสนเทศเสนอรายชื่อจำนวนหนึ่งคน ผู้ซึ่งหอการค้านานาชาติแห่งประเทศไทยเสนอรายชื่อจำนวน1 คน และผู้ซึ่งสภาทนายความเสนอรายชื่อจำนวน 1คน

6. คณะกรรมการสิทธิมนุษยชนเสนอรายชื่อจำนวนหนึ่งคน และผู้ซึ่งคณะกรรมการคุ้มครองผู้บริโภคเสนอรายชื่อจำนวนหนึ่งคน

เมื่อพิจารณาถึงร่างของ ICT จะเห็นได้ว่ามาจากสายการเมืองเป็นจำนวน 9 คน และผู้เชี่ยวชาญ ข้าราชการและบุคคลภายนอก 10 คน ซึ่งอยู่ในสัดส่วนที่ใกล้เคียงกัน ซึ่งคิดว่าการที่ ICT กำหนดให้คณะกรรมการมีองค์ประกอบดังกล่าวน่าจะมาจากเห็นว่าปัญหาจริงในการละเมิดข้อมูลข่าวสารส่วนบุคคลเกิดจากการใช้เทคโนโลยีและคอมพิวเตอร์ ซึ่งผู้ที่มีความรู้และมีประสบการณ์จริงๆมาเป็นคณะกรรมการน่าจะรู้ปัญหามากกว่า ทั้งนี้ในส่วนของการคุ้มครองสิทธิของประชาชนการมีคณะกรรมการ ซึ่งประกอบไปด้วยผู้มีความเชี่ยวชาญในด้านสาขาวิชานิติศาสตร์ คณะกรรมการสิทธิมนุษยชนและตัวแทนจากคณะกรรมการคุ้มครองผู้บริโภค มาร่วมในการคุ้มครองสิทธิของประชาชน ดังนั้นตามความเห็นจึงเห็นว่า คณะกรรมการชุดที่กระทรวง ICT เสนอเป็นคณะกรรมการที่เป็นผู้มีความเกี่ยวข้องกับการใช้ข้อมูลข่าวสารและมีประสบการณ์โดยตรงซึ่งมาจากหลายสายและมีความหลากหลายจึงน่าจะมีการดำเนินงานที่มีประสิทธิภาพมากกว่า แต่กระนั้นคณะกรรมการในชุดนี้ประกอบไปด้วยผู้ทรงคุณวุฒิซึ่งคณะรัฐมนตรีแต่งตั้งโดยการเสนอชื่อของรัฐมนตรี ซึ่งอาจมีอำนาจทางการเมืองเข้ามาเกี่ยวข้องถึงจำนวนเก้าคนซึ่งเกือบครึ่งหนึ่งของคณะกรรมการทั้งหมดซึ่งถือว่ามีจำนวนมากพอสมควร

อย่างไรก็ตามคณะกรรมการของร่างทั้งสองจะเห็นว่าไม่มีลักษณะเป็นคณะกรรมการที่เป็นงานประจำ ดังนั้น การทำงานหรือการดำเนินงานต่างๆอาจมีข้อจำกัดในเรื่องเวลาทำงาน ซึ่งไม่สามารถทุ่มเทอย่างเต็มที่เนื่องจากมีภาระหน้าที่ในงานประจำอยู่แล้ว หากมีคณะกรรมการบางส่วนหรือส่วนมากที่ทำงานในรูปแบบของงานประจำ น่าจะทำให้การดำเนินงานของคณะกรรมการประสบความสำเร็จมาก

7. การออกใบรับรองการประมวลผล

ทั้งสองร่างมีแนวความคิดให้มีการออกใบรับรองผลการประมวลข้อมูลข่าวสารซึ่งถือว่าเป็นมาตรการส่งเสริมประการหนึ่งที่นานาประเทศยอมรับและมีการใช้การออกใบรับรองการประมวลผลอย่างกว้างขวาง

8. บทลงโทษ

บทลงโทษโดยกำหนดให้ผู้ที่ละเมิดข้อมูลส่วนบุคคลต้องมีความรับผิดทางแพ่งโดยกำหนดโทษทั้งจำทั้งปรับ

ในส่วนขององค์กรผู้ดำเนินการประมวลผลข้อมูลข่าวสาร ร่างฯของ ICT กำหนดผู้ที่ดำเนินการฝ่าฝืนตามกฎหมายนี้ให้รับโทษปรับทางปกครอง คือ ปรับไม่เกินสองหมื่นบาท

ต่อวันสำหรับการฝ่าฝืนหรือไม่ปฏิบัติตาม โดยในการกำหนดอัตราโทษปรับทางปกครองให้คำนึงถึงความร้ายแรงแห่งพฤติกรรมที่กระทำผิดและในกรณีที่เห็นสมควรคณะกรรมการ และให้นำบทบัญญัติเกี่ยวกับการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับโดยอนุโลมและในกรณีที่ไม่มีเจ้าหน้าที่ดำเนินการบังคับตามคำสั่ง ให้คณะกรรมการมีอำนาจฟ้องคดีต่อศาลปกครองเพื่อบังคับชำระค่าปรับ

9. ภาระการพิสูจน์

ร่างทั้งสองฉบับกำหนดให้เป็นของผู้เก็บรวบรวมถ้าผู้เก็บรวบรวมข้อมูลหรือผู้ควบคุมข้อมูลเป็นผู้พิสูจน์ในกรณีที่มีการกล่าวหาว่าผู้เก็บรวบรวมข้อมูลหรือผู้ควบคุมข้อมูลไม่ดำเนินการพิสูจน์การดำเนินการนั้นหรือดำเนินการล่าช้าโดยไม่มีเหตุผลอันสมควร ซึ่งเป็นไปตามหลักสากล

10. หลักการทั่วไป

1. หลักการทั่วไปของการเก็บและการประมวลผลข้อมูล คือ กระทำภายใต้วัตถุประสงค์ที่กำหนด เท่าที่จำเป็นภายใต้หลักความยินยอมเป็นสำคัญ และเก็บจากเจ้าของข้อมูลโดยตรงเว้นแต่ในกรณีที่กฎหมายกำหนด

2. หลักการรักษาความปลอดภัยของข้อมูลข่าวสาร

3. หลักข้อมูลต้องถูกต้องและทันสมัย

4. สิทธิในการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลข่าวสาร รวมถึงสิทธิในการเรียกร้องให้มีการแก้ไข ปรับปรุง ลบ หรือยกเลิก การเก็บข้อมูลข่าวสารของตน รวมทั้งสิทธิที่จะได้รับการเยียวยาความเสียหายที่เกิดจากการประมวลผลที่ผิดพลาดด้วย

5. หลักการคุ้มครองข้อมูลข่าวสารที่มีความละเอียดอ่อน

6. หลักการโอนข้อมูล

ร่าง ICT ห้ามมิให้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศซึ่งมิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมกันในสาระสำคัญเช่นเดียวกับบทบัญญัติแห่งพระราชบัญญัตินี้ เว้นแต่

1. ได้รับความยินยอมจากเจ้าของข้อมูล

2. เป็นความจำเป็นเพื่อชำระหนี้ตามความผูกพันที่เป็นผลของสัญญา ซึ่งเจ้าของข้อมูลเป็นคู่สัญญาหรือเป็นสัญญาระหว่างหน่วยงานกับบุคคลอื่นที่เป็นเพื่อประโยชน์ของเจ้าของข้อมูล

3. กระทำเพื่อประโยชน์ของบุคคลซึ่งไม่สามารถให้ความยินยอมได้

4. กรณีอื่นใดตามที่คณะกรรมการประกาศกำหนด

ร่าง สขร. มาตรา 29 การส่งหรือโอนข้อมูลส่วนบุคคลออกไปนอกราชอาณาจักรโดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลส่วนบุคคลจะกระทำมิได้ เว้นแต่เป็นการกระทำตามบทบัญญัติแห่งกฎหมาย หรือเพื่อการดำเนินคดีนอกราชอาณาจักร หรือเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคลนั้น

ร่างของ ICT บัญญัติไว้ตามแนวทางที่ EU กำหนด เนื่องจากต้องการแสดงให้เห็นว่าประเทศไทยมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลเทียบเท่ากับนานาประเทศและขณะเดียวกันก็ต้องการคุ้มครองข้อมูลส่วนบุคคลซึ่งอาจถูกส่งไปยังประเทศที่ไม่มีมาตรการในการคุ้มครองข้อมูลข่าวสารอย่างพอเพียง ดังนั้น เพื่อให้เท่าเทียมและได้รับการยอมรับจากนานาประเทศและ EU ซึ่งเป็นภูมิภาคที่เป็นตลาดการค้าที่สำคัญของเรา ดังนั้น เห็นว่า มาตรการดังกล่าวของร่าง ICT น่าจะมีประสิทธิภาพมากกว่า

11. หลักการจดทะเบียน

ร่างของ สขร. กำหนดให้ผู้ควบคุมและผู้ประมวลผลข้อมูลต้องจดทะเบียนต่อเจ้าหน้าที่ แต่ในร่างของ ICT ไม่บังคับแต่ให้เป็นดุลยพินิจของคณะกรรมการฯที่เห็นว่าในกรณีที่จำเป็นเพื่อประโยชน์ในการเสริมสร้างความเชื่อถือในระบบบริหารจัดการข้อมูลส่วนบุคคล หรือเพื่อป้องกันความเสียหายต่อสาธารณชน คณะกรรมการอาจกำหนดประเภทหรือขนาดธุรกิจที่ต้องขึ้นทะเบียนต่อคณะกรรมการก็ได้

ในกรณีนี้เห็นว่า หากจะมีการใช้ระบบการจดทะเบียนควรกำหนดมาตรฐานเดียวกัน คือ ถ้าจะจดทะเบียนก็จอทั้งหมด หรือถ้าไม่จดทะเบียนก็ไม่จดทั้งหมด ทั้งนี้เพื่อไม่ต้องประสพปัญหาการแบ่งประเภทหรือการกำหนดขนานของธุรกิจที่ต้องมีการจดทะเบียน แค่ไหนอย่างไร

12. การทำ privacy policy

ร่างทั้งสองฉบับสนับสนุนให้มีการทำ privacy policy ซึ่งสอดคล้องกับประเทศอื่นๆที่มีการพัฒนาการคุ้มครองข้อมูลส่วนบุคคล

13. ความรับผิดของเจ้าหน้าที่

ร่างของ สขร. กำหนดให้นายทะเบียนผู้ใดไม่ดำเนินการตามกฎหมาย มีโทษปรับ และนายทะเบียนผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของคณะกรรมการ ระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำ ทั้งปรับ

ร่างของ ICT นอกจาก กำหนดบทลงโทษไว้ทำนองเดียวกับกฎหมายเฉพาะ เช่น พระราชบัญญัติวิธีปฏิบัติราชการทางปกครอง หรือ พระราชบัญญัติวิชาชีพเวชกรรม คือ ผู้ใดล่วงรู้กิจการของผู้อื่นเนื่องจากการปฏิบัติตามอำนาจหน้าที่ ต้องระวางโทษจำคุกไม่เกิน 1ปี หรือปรับไม่เกินสอง หมื่นบาท หรือทั้งจำทั้งปรับ เว้นแต่ การเปิดเผยในกรณีดังต่อไปนี้

1) เป็นการกระทำตามหน้าที่

2) เพื่อประโยชน์แก่การสอบสวนหรือการพิจารณาคดี

3) เกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้

4) เพื่อประโยชน์ในการแก้ไข ให้สอดคล้องกับมาตรฐานหรือมาตรการที่คณะกรรมการประกาศกำหนด

5) การเปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่เกี่ยวข้องกับเรื่องดังกล่าว

6) ได้รับความเห็นชอบจากบุคคลดังกล่าวเป็นลายลักษณ์อักษร

โดยรายละเอียดของประเด็นที่มีความแตกต่างกันซึ่งเป็นสาระสำคัญมากที่สุดใน 7 ประเด็นข้างต้นที่น่าจะส่งผลกระทบถึงความสัมฤทธิ์ผลในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยต่อไปนั้น จากการวิเคราะห์พบว่าคือเรื่องการจัดโครงสร้างองค์กร องค์ประกอบการได้มาซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล และการจัดหน่วยงานธุรการ

เหตุผลที่สามารถสรุปได้เช่นนั้นเนื่องจากกฎหมายคุ้มครองข้อมูลส่วนบุคคล อาจกล่าวได้ว่ายังคงเป็นเรื่องใหม่สำหรับสังคมไทย ซึ่งมีความจำเป็นต้องผลักดันอีกหลายๆเรื่องในอนาคตโดยเฉพาะการสร้างองค์ความรู้และความเชี่ยวชาญให้เกิดขึ้น ดังนั้นองค์กรที่เข้ามาดูแลทิศทางกำหนดนโยบายต่างๆ ตลอดจนควบคุมกำกับดูและหน่วยงานธุรการจะต้องมีการออกแบบโครงสร้างองค์กรที่ดีและเหมาะสม ขณะเดียวกันจะต้องไม่ลืมว่าอันที่จริงตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ก็เป็นกฎหมายที่กล่าวถึงการคุ้มครองข้อมูลส่วนบุคคลไว้แล้วแต่ก็เฉพาะข้อมูลส่วนบุคคลในความครอบครองของหน่วยงานของรัฐเท่านั้น ดังนั้นการตรากฎหมายที่เกี่ยวด้วยการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนขึ้นใหม่ ก็น่าจะต้องพิจารณาถึงความเป็นเอกภาพ และสอดคล้องกับกฎหมายข้อมูลข่าวสารของราชการด้วย เพื่อให้การบังคับใช้กฎหมายทั้งสองฉบับบรรลุถึงประสิทธิภาพประสิทธิผล

ในประเด็นเรื่องการจัดโครงสร้างองค์กรของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและหน่วยงานธุรการนั้นตามร่างของกระทรวง ICT ในมาตรา 28 กำหนดให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ประกอบด้วยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นประธานกรรมการ และผู้ทรงคุณวุฒิซึ่งคณะรัฐมนตรีแต่งตั้งโดยการเสนอชื่อของรัฐมนตรีอีกจำนวน 9 คนเป็นกรรมการ[35]

[35]คณะกรรมการผู้ทรงคุณวุฒิตามร่างพระราชบัญญัติฯมาตรา 28 จำนวน 9 คนประกอบด้วย

(1) ผู้ซึ่งมีความเชี่ยวชาญในสาขาวิชานิติศาสตร์ พาณิชย์อิเล็กทรอนิกส์หรือวิทยาการคอมพิวเตอร์และมีคุณสมบัติรับราชการหรือเคยรับราชการในตำแหน่งไม่ต่ำกว่ารองอธิบดีหรือเทียบเท่า หรือปฏิบัติงานในหน่วยงานของรัฐมาแล้วไม่น้อยกว่าเจ็ดปีหรือเป็นรองหัวหน้าหน่วยงาน จำนวนหนึ่งคน

(2) ผู้ซึ่งเป็นหรือเคยเป็นอาจารย์ในสาขาวิชานิติศาสตร์ พาณิชย์อิเล็กทรอนิกส์หรือวิทยาการคอมพิวเตอร์ ในสถาบันการศึกษาของรัฐในระดับมหาวิทยาลัยมาแล้วไม่น้อยกว่าห้าปี จำนวนหนึ่งคน

(3) ผู้ซึ่งคณะกรรมการข้อมูลข่าวสารของราชการเสนอรายชื่อจำนวนหนึ่งคน และผู้ซึ่งคณะกรรมการธุรกรรมทารงอิเล็กทรอนิกส์เสนอรายชื่อจำนวนหนึ่งคน

(4) ผู้ซึ่งสมาคมสมาพันธ์เทคโนโลยีสารสนเทศเสนอรายชื่อจำนวนหนึ่งคน ผู้ซึ่งหอการค้านานาชาติแห่งประเทศไทยเสนอรายชื่อจำนวนหนึ่งคน และผู้ซึ่งสภาทนายความเสนอรายชื่อจำนวนหนึ่งคน

(5) ผู้ซึ่งคณะกรรมการสิทธิมนุษยชนเสนอรายชื่อจำนวนหนึ่งคน และผู้ซึ่งคณะกรรมการคุ้มครองผู้บริโภคเสนอรายชื่อจำนวนหนึ่งคน

ในส่วนหน่วยงานธุรการตามร่างของICT มาตรา 45 กำหนดให้จัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการ และให้สักงานมีฐานะเป็นนิติบุคคลในกำกับดูแลของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารโดยมีระบบที่แตกต่างจากระบบราชการเพื่อให้เกิดความคล่องตัวภายใต้นโยบายคณะกรรมการ และให้สำนักงานนี้ปฏิบัติหน้าที่ตามหลักเกณฑ์ ระเบียบ ข้อบังคับตามที่คณะกรรมการกำหนด

สำหรับร่างของ สขร. ก็กำหนดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเช่นกัน แต่องค์ประกอบของคณะกรรมการมีความต่างกันออกไป โดยมาตรา 7 ของร่างกฎหมายกำหนดให้นายกรัฐมนตรีหรือรัฐมนตรีซึ่งนายกรัฐมนตรีมอบหมายเป็นประธานกรรมการ โดยมีกรรมการสามประเภท ได้แก่

1. กรรมการโดยตำแหน่งประกอบด้วย ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงกลาโหม ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร อธิบดีกรมการปกครอง อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ อัยการสูงสุดและเลขาธิการสำนักงานคณะกรรมการคุ้มครองผู้บริโภค

2. กรรมการซึ่งเป็นผู้แทนของผู้ประมวลข้อมูลส่วนบุคคลจำนวน 7 คน โดยพิจารณาจากภาคเอกชนด้านต่างๆที่มีการดำเนินการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก และ

3. กรรมการผู้ทรงคุณวุฒิซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญด้านการประมวลผลข้อมูลส่วนบุคคล จำนวน 7 คน

ซึ่งการได้มาของกรรมการประเภทผู้แทนและผู้ทรงคุณวุฒิ ร่างพระราชบัญญัติฯมาตรา 7 วรรคท้ายกำหนดให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะรัฐมนตรีกำหนดและประกาศในราชกิจจานุเบกษา

สำหรับหน่วยงานธุรการในร่างกฎหมายนี้ มาตรา 15 กำหนดให้มีสำนักงานคณะกรรมการข้อมูลข่าวสารแห่งชาติเป็นส่วนราชการไม่สังกัดสำนักนายกรัฐมนตรี กระทรวงหรือทบวง มีฐานะเป็นกรม อยู่ในบังคับบัญชาและขึ้นตรงต่อนายกรัฐมนตรี

สำนักงานคณะกรรรมการข้อมูลข่าวสารแห่งชาติที่จัดตั้งขึ้น ดังกล่าวมีอำนาจหน้าที่ปฏิบัติงานเกี่ยวกับงานวิชาการและธุรการให้แก่คณะกรรมการตามพระราชบัญญัตินี้ และคณะกรรมการตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ (มาตรา 16) โดยตามบทเฉพาะกาลมาตรา 50 กฎหมายได้ให้โอนบรรดากิจการ อำนาจหน้าที่ ทรัพย์สิน งบประมาณ หนี้ สิทธิ และภาระผูกพันทั้งปวง ตลอดจน โอนข้าราชการ ลูกจ้าง ตำแหน่งและอัตรากำลังของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการไปเป็นของสำนักงานคณะกรรมกรข้อมูลข่าวสารแห่งชาติ หากกล่าวโดยสรุปการจัดตั้งสำนักงานคณะกรรรมการข้อมูลข่าวสารแห่งชาติ ก็คือการเปลี่ยนสถานภาพมาจากสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการนั้นเอง

เมื่อพิจารณาถึงสาระสำคัญของร่างพระราชบัญญัติทั้งสองในประเด็นการจัดโครงสร้างองค์กรของกลไกที่ขับเคลื่อนการดำเนินงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามที่นำเสนอมาข้างต้นจะเห็นว่า ร่างของ สขร. จะมีความเชื่อมโยงกับกฎหมายข้อมูลข่าวสารของราชการมากกว่า และ

มีองค์ประกอบของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่ผสมผสานทั้งที่มาจากภาครัฐและเอกชน ตลอดจนมีการกำหนดให้มีหลักเกณฑ์การได้มาที่กำหนดโดยคณะรัฐมนตรี ขณะที่ร่างของICT บทบาทหลักจะอยู่ที่กระทรวง เทคโนโลยีสารสนเทศและการสื่อสาร โดยรัฐมนตรีว่าการกระทรวงเป็นทั้งรัฐมนตรีรักษาการตามพระราชบัญญัติและประธานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ทั้งนี้องค์ประกอบของคณะกรรมการตามร่างของICT ก็มีกรรมการน้อยกว่าร่างของ สขร. คือมีจำนวนกรรมการรวมประธานเพียง 11 คน ขณะที่ร่างของ สขร. มีจำนวน กรรมการโดยตำแหน่ง 7 คน กรรมการผู้แทนของผู้ประมวลข้อมูลส่วนบุคคลภาคเอกชน 7 คน และกรรมการผู้ทรงคุณวุฒิที่คณะรัฐมนตรีแต่งตั้ง 7 คน เมื่อรวมประธานก็จะมีจำนวนกรรมการ 22 คน นอกจากนั้นที่มาของกรรมการตามร่างของICT ก็ขาดหลักเกณฑ์ขั้นตอนวิธีการได้มา เพียงกำหนดให้เป็นการเสนอชื่อจากองค์กร ในแต่ละฝ่ายฝ่ายละหนึ่งคน

ในส่วนหน่วยงานธุรการก็เป็นการจัดตั้งสำนักงานคณะกรรมการขึ้นใหม่เป็นอีกองค์กรต่างหาก ต่างจากร่างของ สขร. ที่มีการบูรการงานตามกฎหมายข้อมูลข่าวสารของราชการไว้ด้วย โดยเปลี่ยนสถานภาพของ สขร. มาทำหน้าที่ตามกฎหมายใหม่ และปรับปรุงโครงสร้างการทำงานของ สขร. ให้เหมาะสมกับภารกิจ

ดังนั้นแล้วจากการวิเคราะห์ถึงข้อแตกต่างของร่างทั้งสองฉบับจะเห็นว่าการจัดโครงสร้างองค์กรหน่วยงานที่เกี่ยวข้องในการดำเนินงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามร่างของ สขร. มีความเหมาะสมมากกว่าร่างของICT ที่สามารถสะท้อนความเป็นเอกภาพระหว่างการคุ้มครองข้อมูลส่วนบุคคลทั้งในภาครัฐและเอกชนได้ดีกว่าอย่างเห็นได้ชัด เมื่อพิจารณาถึงการดำเนินงานต่อไปในอนาคตความสำเร็จในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย หากปล่อยให้เป็นตามโครงสร้างของร่าง ICT น่าจะก่อให้เกิดปัญหาอุปสรรคข้อขัดแย้งระหว่างการทำงาน ซึ่งเป็นความแตกต่างในแนวทางการวินิจฉัย และการปฏิบัติงานต่างๆ ของหน่วยงานรับผิดชอบที่แยกจากกันเป็นคนละองค์กรระหว่างข้อมูลส่วนบุคคลในภาครัฐกับภาคเอกชน ทั้งนี้ไม่จำเป็นต้องกล่าวถึงการขาดความคำนึงถึงการพัฒนางานในภาพรวมของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ที่ร่างของICT ได้เป็นการจัดตั้งองค์กรที่เป็นหน่วยงานธุรการขึ้นใหม่ โดยละเลยงานของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการทั้งที่เป็นองค์กรที่สมควรได้รับการพัฒนาปรับปรุงในฐานะที่เป็นผู้ดูแลงานด้านข้อมูลส่วนบุคคลมาตั้งแต่ต้น หากปล่อยให้มีการตรากฎหมายเช่นนี้ ก็จะก่อให้เกิดช่องว่างในโอกาสการพัฒนางานสนับสนุนการคุ้มครองข้อมูลส่วนบุคคลที่เป็นระบบซึ่งไม่สามารถละเลยไปได้

ภายหลังจากความขัดแย้งที่เกิดขึ้นระหว่างการพิจารณาร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ด้วยกันสองฉบับ ในที่สุดคณะรัฐมนตรีได้มีมติให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นเจ้าภาพหลักที่รับผิดชอบดูแลร่างกฎหมาย โดยให้ถือร่างของสำนักงานเป็นหลัก ซึ่งเมื่อได้ปรับปรุงเนื้อหาบางส่วนแล้วก็เข้าสู่การพิจารณาของคณะกรรมการกฤษฎีกา ซึ่งปรากฏหลักการและเหตุผลในร่างพระราชบัญญัติฯ ดังนี้

“ด้วยที่ผ่านมาปัญหาการล่วงละเมิดสิทธิส่วนบุคคลมีมาก โดยเฉพาะการนำข้อมูลส่วนบุคคลของเจ้าของข้อมูลไปใช้ประโยชน์หรือเปิดเผยหรือเผยแพร่จนทำให้เกิดความเสียหาย ซึ่งนับวัน

จะมีจำนวนมากขึ้นเรื่อย ๆ แม้ว่าจะได้มีการตรากฎหมายขึ้นใช้บังคับเพื่อคุ้มครองเกี่ยวกับข้อมูลต่าง ๆ ซึ่งบางเรื่องรวมไปถึงข้อมูลส่วนบุคคลด้วยก็ตาม แต่การคุ้มครองดังกล่าวมุ่งที่จะให้คามคุ้มครองเรื่องใดเรื่องหนึ่งเป็นหลักตามวัตถุประสงค์ของกฎหมายฉบับนั้น หาได้มีการตรากฎหมายในลักษณะที่เป็นการให้ความคุ้มครองเป็นการทั่วไปในสิทธิเกี่ยวกับข้อมูลส่วนบุคคล และโดยที่ในปัจจุบันรัฐธรรมนูญได้บัญญัติรับรองและให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลไว้ด้วย ดังนั้น เพื่อให้การคุ้มครองสิทธิในข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและเป็นกฎหมายหลักในการให้ความคุ้มครอง ไม่ว่าจะเป็นการเก็บ รวบรวม บันทึก ใช้ประโยชน์ การเปิดเผย หรือการอื่นใดที่เกี่ยวข้อง รวมตลอดถึงการกำหนดมาตรการและกระบวนการในการคุ้มครองและรักษาข้อมูลส่วนบุคคลดังกล่าว จึงเห็นสมควรที่จะได้มีการตรากฎหมายเพื่อให้การคุ้มครองสิทธิส่วนบุคคลขึ้นใช้บังคับ”

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ..... นี้ มีวัตถุประสงค์ที่จะบัญญัติขึ้นเพื่อเป็นกฎหมายกลางในการให้ความคุ้มครองสิทธิข้อมูลส่วนบุคคล ซึ่งจะกำหนดหลักเกณฑ์ กระบวนการและมาตรการต่าง ๆ ที่เป็นมาตรฐานทั่วไปในการให้การดูแลและคุ้มครองสิทธิส่วนบุคคลไว้เป็นการเฉพาะแล้ว การดำเนินการในการให้การดูแลและคุ้มครองสิทธิข้อมูลส่วนบุคคลในเรื่องนั้นก็จะเป็นไปตามหลักเกณฑ์ กระบวนการและมาตรการที่กฎหมายเฉพาะนั้นกำหนด แต่หากเป็นกรณีที่กฎหมายอื่นใดที่บัญญัติเกี่ยวกับข้อมูลส่วนบุคคลแล้วหาได้กำหนดหรือกำหนดไว้แต่เพียงเรื่องหนึ่งเรื่องใดเท่านั้น กรณีดังกล่าวร่างพระราชบัญญัติฉบับนี้กำหนดให้นำหลักเกณฑ์ กระบวนการและมาตรการตามที่กำหนดไว้ในร่างพระราชบัญญัตินี้ไปใช้บังคับในส่วนที่กฎหมายอื่นนั้นมิได้กำหนด อย่างไรก็ดี ด้วยวัตถุประสงค์ของร่างพระราชบัญญัติฉบับนี้ประสงค์ที่จะให้ความคุ้มครองสิทธิข้อมูลส่วนบุคคลในความครอบครองของเอกชนและหน่วยงานของรัฐที่มีวัตถุประสงค์ในการดำเนินงานเชิงธุรกิจหรือการพาณิชย์เป็นหลัก

ดังนั้น บทบัญญัติต่าง ๆ ตามร่างพระราชบัญญัตินี้จึงกำหนดมิให้นำไปใช้บังคับกับการประมวลข้อมูลส่วนบุคคลของหน่วยงานของรัฐซึ่งอยู่ภายใต้บังคับตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และเพื่อให้บรรลุวัตถุประสงค์แห่งร่างพระราชบัญญัตินี้ที่จะให้เป็นกฎหมายกลางใช้บังคับกับหน่วยงานทั้งหลายที่เกี่ยวข้อง รวมถึงการบริหารกฎหมายให้เป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้นายกรัฐมนตรีเป็นผู้รักษาการตามพระราชบัญญัตินี้

นอกจากหลักการดังกล่าวแล้ว ร่างพระราชบัญญัตินี้ได้กำหนดสาระสำคัญในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคล ดังต่อไปนี้

ตามร่างพระราชบัญญัติฯในมาตรา 7 ได้กำหนดให้มีคณะกรรมการคณะหนึ่งทำหน้าที่ดูแลคุ้มครองข้อมูลข่าวสารส่วนบุคคลตามกฎหมาย และวางนโยบายและมาตรการในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคล เรียกว่า “คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล” ประกอบด้วยนายกรัฐมนตรีหรือรัฐมนตรีซึ่งนายกรัฐมนตรีมอบหมายเป็นประธานกรรมการ และกรรมการจากส่วนราชการ ภาคเอกชน รวมถึงผู้ทรงคุณวุฒิเพื่อให้การใช้อำนาจเป็นไปอย่างมีประสิทธิภาพ ได้แก่

- กรรมการโดยตำแหน่งจากส่วนราชการ ประกอบด้วย ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เลขาธิการคณะกรรมการกฤษฎีกา อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ

- กรรมการซึ่งเป็นผู้แทนของหอการค้าไทย สมาคมธนาคารไทย คณะกรรมการสิทธิมนุษยชน คณะกรรมการคุ้มครองผู้บริโภค

- กรรมการผู้ทรงคุณวุฒิซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้ที่มีความรู้ความเชี่ยวชาญด้านกฎหมายและด้านการประมวลผลอิเล็กทรอนิกส์ จำนวน 4 คน

คณะกรรมการชุดนี้ นอกจากอำนาจหน้าที่ที่กล่าวข้างต้นแล้ว ยังมีอำนาจหน้าที่ในการควบคุม ดูแลและส่งเสริมการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคล ดังนี้ (ร่างมาตรา 11)

1) กำหนดนโยบาย มาตรการ หรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

2) เสนอความเห็นต่อนายกรัฐมนตรีเพื่อออกกฎกระทรวงตามพระราชบัญญัตินี้

3) ให้คำแนะนำและให้คำปรึกษาเกี่ยวกับการดำเนินการใด ๆ ในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมในการพัฒนาเทคโนโลยีที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

4) กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประมวลผล

5) กำหนดหลักเกณฑ์และเงื่อนไขในการได้รับเครื่องหมายรับรองการประมวลผล

6) ติดตาม ตรวจสอบและประเมินผลการดำเนินการของผู้ประมวลผลข้อมูลส่วนบุคคล

7) พิจารณาดำเนินการเกี่ยวกับเรื่องร้องเรียนตามพระราชบัญญัตินี้

8) ออกระเบียบ ข้อบังคับ คำสั่งหรือปฏิบัติการอื่นเพื่อให้เป็นไปตามวัตถุประสงค์ของพระราชบัญญัตินี้

9) แต่งตั้งคณะอนุกรรมการ เพื่อดำเนินการใด ๆ ตามพระราชบัญญัตินี้ตามความจำเป็นและเหมาะสม

10) ปฏิบัติการอื่นตามที่บัญญัติไว้ในพระราชบัญญัตินี้หรือตามที่กฎหมายอื่นกำหนดให้เป็นอำนาจของคณะกรรมการหรือตามที่นายกรัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย

11) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงแก้ไขกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องและเหมาะสม

12) จัดทำรายงานเกี่ยวกับการปฏิบัติการตามพระราชบัญญัตินี้เสนอต่อคณะรัฐมนตรี รัฐสภา หรือสาธารณชนเป็นครั้งคราวตามความเหมาะสมอย่างน้อยปีละหนึ่งครั้ง

เพื่อประโยชน์ในการดำเนินการของคณะกรรมการและเพื่อให้เป็นไปตามวัตถุประสงค์แห่งร่างพระราชบัญญัตินี้ ตลอดจนเพื่อให้เกิดประสิทธิภาพในการดำเนินการตามอำนาจหน้าที่ของคณะกรรมการร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้มีหน่วยงานธุรการของคณะกรรมการขึ้นเพื่อรับผิดชอบในการปฏิบัติงานด้านธุรการและด้านวิชาการให้แก่คณะกรรมการ ได้แก่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นสำนักงานในสังกัดของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งจะมีฐานะเป็นกรม โดยมีเลขาธิการสำนักงานคณะกรรมการข้อมูลข่าวสารของ

ราชการเป็นผู้บังคับบัญชาและรับผิดชอบในการปฏิบัติราชการของสำนักงาน โดยจะมีรองเลขาธิการเป็นผู้ช่วยสั่งและปฏิบัติราชการตามที่ได้รับมอบหมายก็ได้ (ร่างมาตรา 16)

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล นอกจากจะมีหน้าที่เป็นหน่วยงานธุรการที่ปฏิบัติหน้าที่ด้านธุรการและวิชาการให้แก่คณะกรรมการแล้ว สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลยังมีอำนาจหน้าที่ ดังนี้ (ร่างมาตรา 17)

1) ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชนและหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

2) ให้คำปรึกษาแก่องค์กรภาครัฐและภาคเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

3) วางระเบียบรวมถึงการกำหนดหลักสูตรฝึกอบรมการปฏิบัติหน้าที่ของนายทะเบียน

4) จัดทำบัญชีรายชื่อผู้ประมวลผลข้อมูลส่วนบุคคล

5) ติดตามและประเมินผลในการปฏิบัติตามพระราชบัญญัตินี้

6) ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการมอบหมาย

กรณีของความหมายของข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้มีความหมายกว้างกว่าข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 เนื่องจากเป็นข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือดำเนินการของภาคเอกชนและของหน่วยงานของรัฐที่ดำเนินงานเชิงธุรกิจหรือการพาณิชย์ ดังนั้นในการให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคล จึงได้แก่ การเก็บรวบรวม การบันทึก การจัดหมวดหมู่ การใช้ประโยชน์ การเก็บรักษา การแก้ไข การโอนและการเปิดเผย ฯลฯ ซึ่งตามร่างพระราชบัญญัตินี้เรียกว่า *“การประมวลผล”*

การประมวลผลตามร่างพระราชบัญญัตินี้ ได้กำหนดหลักการในการคุ้มครองสิทธิในข้อมูลส่วนบุคคลไว้ ได้แก่ “หลักความยินยอม” หลักการ “ปกปิด” เป็นหลักการทั่วไป “การเปิดเผย” เป็นข้อยกเว้น นอกจากนี้ ในการประมวลผลจะต้องเป็นไปตามวัตถุประสงค์ของกิจการของผู้ดำเนินการประมวลผลด้วย (ร่างมาตรา 21)

สำหรับหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลนั้น นอกจากผู้ดำเนินการประมวลผลข้อมูลส่วนบุคคลจะต้องดำเนินการประมวลผลข้อมูลส่วนบุคคลตามหลักเกณฑ์ วิธีการและเงื่อนไขตามที่บัญญัติไว้ในร่างพระราชบัญญัตินี้ และจะต้องจัดให้มีนายทะเบียนขึ้นเพื่อทำหน้าที่ในการควบคุมดูแลและรับผิดชอบในการประมวลผลข้อมูลส่วนบุคคล

ตามร่างพระราชบัญญัตินี้ ได้แบ่งการประมวลผลข้อมูลส่วนบุคคลออกเป็นส่วนต่าง ๆ ดังนี้

1) <u>การเก็บรวบรวมข้อมูลส่วนบุคคล</u>

การเก็บรวบรวมข้อมูลส่วนบุคคลถือเป็นสิ่งแรกที่ร่างพระราชบัญญัตินี้ได้ให้ความคุ้มครองสิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยกำหนดให้เก็บรวบรวมข้อมูลส่วนบุคคลได้เพียงเท่าที่เกี่ยวข้องและจำเป็นแก่การดำเนินกิจการตามวัตถุประสงค์ของผู้ประมวลข้อมูลส่วนบุคคลเท่านั้น ทั้งนี้ ตามร่างพระราชบัญญัติฉบับนี้ได้กำหนดห้ามการเก็บรวบรวมข้อมูลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ข้อมูลทางพันธุกรรม ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา ฯลฯ เว้นแต่ได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูลและเพื่อให้สอดคล้องกับหลักการในการให้ความคุ้มครอง

สิทธิในข้อมูลส่วนบุคคลของเจ้าของข้อมูล ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลได้ทราบถึงรายละเอียดก่อนหรือในขณะเก็บรวบรวมข้อมูล ดังนี้ (ร่างมาตรา 22)

(1) ชื่อ สถานที่ทำการและสถานภาพของผู้ประมวลข้อมูลส่วนบุคคล

(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล

(3) ประเภทของข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(4) วิธีการเก็บรวบรวมข้อมูลส่วนบุคคล

(5) ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

(6) เงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล

(7) รายละเอียดอื่นตามที่คณะกรรมการกำหนด

นอกจากนี้ เมื่อได้ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลแล้ว ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้นายทะเบียนจัดทำรายการการจัดเก็บข้อมูลเพื่อให้เจ้าของข้อมูลสามารถตรวจสอบได้ด้วย อย่างไรก็ดี โดยที่กฎหมายเกี่ยวกับการพิมพ์จัดได้ว่าเป็นกฎหมายเฉพาะกฎหมายหนึ่ง ดังนั้น ร่างพระราชบัญญัติฉบับนี้จึงกำหนดเป็นข้อยกเว้นไม่ใช้บังคับถึง (ร่างมาตรา 23)

2) <u>การใช้และการเปิดเผยข้อมูล</u>

ตามร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ผู้ประมวลข้อมูลส่วนบุคคลต้องใช้ข้อมูลส่วนบุคคลที่อยู่ในความครอบครองดูแลตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลเท่านั้น การใช้นอกเหนือจากวัตถุประสงค์จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน อย่างไรก็ดี ในกรณีที่มีเหตุจำเป็นที่มีผลประทบต่อชีวิต ร่างกาย อนามัยของเจ้าของข้อมูลส่วนบุคคล ร่างพระราชบัญญัติฉบับนี้ได้กำหนดเป็นข้อยกเว้นให้สามารถเปิดเผยข้อมูลได้ในกรณี ดังต่อไปนี้ (ร่างมาตรา 26)

(1) เจ้าหน้าที่ของรัฐร้องขอเพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวนการสอบสวนหรือการฟ้องคดี ไม่ว่าจะเป็นคดีประเภทใดก็ตาม

(2) ศาลและเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐที่มีอำนาจตามกฎหมายที่จะขอข้อมูลส่วนบุคคล

(3) เพื่อป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(4) หน่วยงานอื่นที่มีบทบัญญัติของกฎหมายให้อำนาจ

(5) เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุหรือมีส่วนใดที่ทำให้รู้ว่าเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับบุคคลใด

(6) ปรากฏโดยชัดแจ้งว่าเพื่อประโยชน์ของเจ้าของข้อมูลและการขอความยินยอมไม่สามารถกระทำได้ในเวลาจำเป็นนั้น

(7) เพื่อรักษาพยาบาลเจ้าของข้อมูลและในขณะนั้นเจ้าของข้อมูลไม่อยู่ในสภาวะตามกฎหมายที่จะให้คำยินยอมได้

ทั้งนี้ การเปิดเผยนั้นจะกระทำได้เท่าที่จำเป็น และเมื่อได้เปิดเผยแล้วให้แจ้งให้เจ้าของข้อมูลทราบ รวมทั้งผู้ซึ่งได้รับข้อมูลต้องใช้ข้อมูลตามวัตถุประสงค์เท่านั้น และผู้ประมวลข้อมูลต้องบันทึกการเปิดเผยข้อมูลนั้นเพื่อการตรวจสอบด้วย

3) การเก็บรักษา การแก้ไข และการโอนข้อมูลส่วนบุคคล

ในส่วนร่างพระราชบัญญัติได้แบ่งการคุ้มครองข้อมูลส่วนบุคคลออกเป็น 3 ส่วน คือ ของเจ้าของข้อมูลส่วนบุคคลได้เท่าระยะเวลาที่กำหนด หรือเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูล และเมื่อพ้นกำหนดระยะเวลา หรือหมดความจำเป็น หรือเจ้าของข้อมูลเพิกถอนความยินยอม ผู้ประมวลข้อมูลส่วนบุคคลต้องลบทำลายข้อมูลนั้นโดยเร็ว เว้นแต่ในกรณีที่ผู้ประมวลข้อมูลส่วนบุคคลมีความจำเป็นต้องเก็บรักษาข้อมูลนั้นไว้เพื่อเป็นสถิติการศึกษาวิจัย ผู้ประมวลข้อมูลส่วนบุคคลอาจไม่ลบทำลายข้อมูลนั้นก็ได้ แต่ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น (ร่างมาตรา 27)

4) การแก้ไขข้อมูลส่วนบุคคล

ร่างพระราชบัญญัติฉบับนี้กำหนดให้ผู้ประมวลข้อมูลส่วนบุคคลมีหน้าที่ต้องแก้ไขข้อมูลส่วนบุคคลให้ทันสมัยถูกต้องตามที่เจ้าของข้อมูลร้องขอ ในกรณีที่จำเป็นต้องจัดทำข้อมูลใหม่ให้ผู้ประมวลข้อมูลส่วนบุคคลทำลายข้อมูลเดิม และจัดทำข้อมูลใหม่ตามที่เจ้าของข้อมูลร้องขอ โดยแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบล่วงหน้าไม่น้อยกว่า 7 วัน (ร่างมาตรา 28)

5) การโอนข้อมูลส่วนบุคคล

กำหนดห้ามมิให้ผู้ประมวลข้อมูลส่วนบุคคลโอนข้อมูลส่วนบุคคลที่อยู่ในความดูแลไปให้บุคคลอื่น เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากเจ้าของข้อมูล อย่างไรก็ดีในกรณีมีความจำเป็นเร่งด่วนซึ่งหากรอรับความยินยอมก่อนอาจเกิดความเสียหายแก่ส่วนรวม หรือชีวิต ร่างกาย หรืออนามัยของบุคคล ผู้ประมวลข้อมูลส่วนบุคคลอาจส่งหรือโอนข้อมูลนั้นได้โดยให้นายทะเบียนแจ้งให้เจ้าของข้อมูลทราบภายใน 15 วัน(ร่างมาตรา 29)

ตามร่างพระราชบัญญัติยังมีบทบัญญัติในการห้ามส่งหรือโอนข้อมูลส่วนบุคคลไปนอกราชอาณาจักร โดยเฉพาะในประเทศที่ยังไม่มีบทบัญญัติของกฎหมายในการคุ้มครองข้อมูลส่วนบุคคลหรือมี แต่บทบัญญัติของกฎหมายนั้นมีมาตรฐานต่ำกว่าบทบัญญัติตามร่างพระราชบัญญัตินี้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (ร่างมาตรา 30 และมาตรา31)

โดยที่ตามร่างพระราชบัญญัตินี้มีวัตถุประสงค์ที่จะให้การคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นหลัก ดังนั้น จึงกำหนดให้เจ้าของข้อมูลส่วนบุคคล รวมถึงผู้ที่เกี่ยวข้องอื่น ๆ ไม่ว่าจะเป็น ผู้ปกครอง ผู้อนุบาลหรือผู้พิทักษ์ รวมตลอดถึงทายาท มีสิทธิในข้อมูลส่วนบุคคล ดังนี้ (ร่างมาตรา 32)

1) เข้าตรวจดู ขอสำเนา หรือขอสำเนารับรองถูกต้อง

2) ขอแก้ไขหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลที่เกี่ยวข้องกับตนให้ถูกต้องสมบูรณ์

3) ขอให้ระงับการใช้การเปิดเผยในกรณีที่ข้อมูลไม่ถูกต้องเป็นจริง

4) ขอให้ลบทำลายข้อมูลส่วนบุคคลที่พ้นกำหนดระยะเวลาการเก็บรวบรวมข้อมูลหรือไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมข้อมูลนั้น

ร่างพระราชบัญญัติฉบับนี้ยังกำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิเรียกร้องให้ผู้ที่ได้รับข้อมูลมาจากผู้อื่นโดยมิได้รับความยินยอมจากเจ้าของข้อมูลเปิดเผยถึงแหล่งที่มาของข้อมูลได้ หากผู้ได้รับข้อมูลมาโดยมิได้รับความยินยอมจากเจ้าของข้อมูลไม่ยอมเปิดเผย เจ้าของข้อมูลมีสิทธิเรียกร้องค่าสินไหมทดแทนได้ นอกจากนี้ ยังให้สิทธิเจ้าของข้อมูลร้องเรียนต่อคณะกรรมการได้อีกทางหนึ่งด้วย (ร่างมาตรา 34)

ทั้งนี้ร่างพระราชบัญญัติฉบับนี้กำหนดให้สิทธิเจ้าของข้อมูลส่วนบุคคลที่จะร้องเรียนต่อคณะกรรมการในกรณีที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอให้นายทะเบียนแก้ไขการดำเนินการให้เป็นไปตามพระราชบัญญัตินี้ แล้วนายทะเบียนมิได้แก้ไขให้ถูกต้องภายในสิบห้าวัน และเมื่อเจ้าของข้อมูลส่วนบุคคลได้ร้องเรียนต่อคณะกรรมการแล้ว คณะกรรมการมีหน้าที่จะต้องพิจารณาเรื่องดังกล่าวโดยเร็ว หากคณะกรรมการเห็นว่าการไม่ดำเนินการตามพระราชบัญญัตินี้ของ ผู้ประมวลข้อมูลส่วนบุคคล และก่อให้เกิดความเสียหายอย่างร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล คณะกรรมการอาจสั่งให้หยุดกิจการ หรือพักใช้ หรือเพิกถอนใบอนุญาตก็ได้ตามความร้ายแรงที่เกิดขึ้น (ร่างมาตรา 37 ถึง มาตรา 40)

เพื่อให้การบังคับใช้กฎหมายมีประสิทธิภาพ ร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้ ผู้ประมวลข้อมูลส่วนบุคคลแต่งตั้งนายทะเบียนขึ้นเพ่อรับผิดชอบในการดูแลข้อมูลส่วนบุคคลที่อยู่ในความครอบครอง รวมถึงการกำหนดให้นายทะเบียนจะต้องรายงานการประมวลผลข้อมูลส่วนบุคคลต่อคณะกรรมการด้วย (ร่างมาตรา 35 และมาตรา 36)

นอกจากนั้นยังกำหนดให้มีการแต่งตั้งพนักงานเจ้าหน้าที่ขึ้น โดยกำหนดให้พนักงานเจ้าหน้าที่มีอำนาจหน้าที่ ดังนี้ (ร่างมาตรา 41)

1) เรียกให้บุคคลมาให้ถ้อยคำหรือส่งวัตถุ เอกสาร หรือพยานหลักฐานมาเพื่อประกอบการพิจารณาเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

2) เข้าไปในอาคารสถานที่ที่เกี่ยวกับการประมวลผลในระหว่างเวลาทำการของผู้ประมวลผลเพื่อตรวจสอบการกระทำอันเป็นการฝ่าฝืนพระราชบัญญัตินี้

3) ตรวจสอบสถานที่ในกรณีที่มีเรื่องร้องเรียน โดยแจ้งให้เจ้าของหรือ ผู้ครอบครองสถานที่ทราบในเวลาอันควร

4) ยึดหรืออายัดทรัพย์สิน เอกสาร หรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิด

โดยที่การประมวลผลข้อมูลส่วนบุคคลมีเป็นจำนวนมาก และการประมวลผลสมควรที่จะได้มีการแบ่งแยกประเภทให้ชัดเจนเพื่อประโยชน์ในการตรวจติดตามการดำเนินการเพื่อให้เป็นไปตามพระราชบัญญัตินี้ ร่างพระราชบัญญัตินี้จึงกำหนดมาตรการส่งเสริมขึ้นเพื่อให้ผู้ประมวลข้อมูลส่วนบุคคลขอรับการสนับสนุนจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการขอคำปรึกษาในการดำเนินการประมวลผล การอบรมพัฒนา นอกจากนี้ ตามร่างพระราชบัญญัติได้กำหนดให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลนำเสนอต่อคณะกรรมการเพื่อพิจารณาในการออก

ใบรับรองมาตรฐานให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลด้วย ทั้งนี้เพื่อให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพ (ร่างมาตรา 44 ถึง มาตรา 46)

ร่างพระราชบัญญัติฉบับนี้มีข้อกำหนดที่ชัดเจนในความรับผิดทางแพ่ง บทกำหนดโทษและบทเฉพาะกาลให้ผู้ประมวลข้อมูลส่วนบุคคล ผู้ครอบครองหรือควบคุมดูแลข้อมูลส่วนบุคคลต้องรับผิดชดใช้ค่าสินไหมทดแทนให้แก่เจ้าของข้อมูลส่วนบุคคล ในกรณีที่บุคคลดังกล่าวกระทำการใด ๆ ที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลหรือบุคคลที่เกี่ยวข้องด้วย (ร่างมาตรา 47)

เนื่องจากข้อมูลส่วนบุคคลถือเป็นสิทธิของเจ้าของข้อมูล ดังนั้น การละเมิดสิทธิในข้อมูลส่วนบุคคลจึงเป็นสิ่งต้องห้าม หากผู้ใดละเมิดสิทธิของเจ้าของข้อมูลแล้วผู้นั้นสมควรอย่างยิ่งที่จะได้รับโทษ โดยเฉพาะโทษในทางอาญา ร่างพระราชบัญญัติฉบับนี้จึงกำหนดให้ผู้ใดก็ตาม และนายทะเบียนที่กระทำโดยการเผยแพร่ข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ผู้นั้นต้องได้รับโทษทางอาญา เช่น ผู้ใดกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อันไม่ชอบด้วยกฎหมาย หรือให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ การเผยแพร่ข้อมูลส่วนบุคคลโดยเฉพาะเจาะจงหรือโดยเปิดเผยซึ่งข้อมูลส่วนบุคคลผู้กระทำต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ(ร่างมาตรา 48 ถึง มาตรา 51)

ทั้งนี้เพื่อให้การดำเนินการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นโดยเร็วจึงกำหนดให้มีการแต่งตั้งคณะกรรมการขึ้นเพื่อปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ภายใน 90 วัน นับแต่วันที่พระราชบัญญัตินี้มีผลใช้บังคับ นอกจากนี้ โดยที่ตามร่างพระราชบัญญัติฉบับนี้ได้กำหนดให้มีสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นในสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ประกอบกับในขณะนี้พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 อยู่ระหว่างการพิจารณา แก้ไขเพื่อยกสถานะของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งมีสถานะเป็นกองในสำนักงานปลัดสำนักนายกรัฐมนตรี ให้มีสถานะเป็นกรมในสังกัดสำนักนายกรัฐมนตรี ดังนั้น จึงจำเป็นต้องกำหนดบทเฉพาะกาลให้ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการปฏิบัติหน้าที่เลขาธิการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการตามพระราชบัญญัตินี้ด้วย (ร่างมาตรา 51 และมาตรา 52)

เมื่อพิจารณาถึงบทบัญญัติตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...ที่ได้มีการผลักดันโดยรัฐบาลมาหลายชุดนี้ นับว่าเป็นร่างกฎหมายที่สำคัญที่จะส่งผลต่อการพัฒนาการคุ้มครองข้อมูลข่าวสารส่วนบุคคลในภาคเอกชนของประเทศไทยในอนาคตเป็นอย่างมาก เพราะจะช่วยแก้ไขข้อจำกัดที่มีอยู่ในการคุ้มครองตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่ใช้บังคับเฉพาะข้อมูลส่วนบุคคลที่อยู่ในภาครัฐเท่านั้น ให้ครอบคลุมถึงข้อมูลที่จัดเก็บโดยเอกชน ทั้งนี้พระราชบัญญัติฉบับนี้จะช่วยสร้างมาตรฐานกลางในการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนให้เกิดขึ้นในฐานเป็นกฎหมายทั่วไป แตกต่างจากพระราชบัญญัติฉบับอื่นๆที่เป็นการคุ้มครองในลักษณะเฉพาะเรื่องตามแต่ประเภทของข้อมูล เช่น พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 ซึ่งจะวางหลักการเฉพาะที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลเครดิต เป็นต้น

3.6.2 การคุ้มครองข้อมูลส่วนบุคคลในพ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540

ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540ได้กำหนดหน้าที่ให้หน่วยงานรัฐ[36] ต้องปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล [37]ในความครอบครอง ด้วยการต้องจัดระบบข้อมูลข่าวสารส่วนบุคคลของตน ซึ่งปรากฏเนื้อหาอยู่ในหมวด 3ตั้งแต่มาตรา 21-23 ซึ่งหน้าที่หลักของหน่วยงานรัฐได้รับการบัญญัติไว้ในมาตรา 23 มี 5 ประการ ดังนี้

(1) ต้องจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลเพียงเท่าที่เกี่ยวข้องและจำเป็นเพื่อการดำเนินงานของหน่วยงานของรัฐให้สำเร็จตามวัตถุประสงค์เท่านั้น และยกเลิกการจัดให้มีระบบดังกล่าวเมื่อหมดความจำเป็น

(2) พยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล โดยเฉพาะอย่างยิ่งในกรณีที่จะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลนั้น

(3) จัดให้มีการพิมพ์ในราชกิจจานุเบกษาและตรวจสอบแก้ไขให้ถูกต้องอยู่เสมอเกี่ยวกับสิ่งดังต่อไปนี้

(ก) ประเภทของบุคคลที่มีการเก็บข้อมูลไว้

(ข) ประเภทของระบบข้อมูลข่าวสารส่วนบุคคล

(ค) ลักษณะการใช้ข้อมูลตามปกติ

(ง) วิธีการขอตรวจดูข้อมูลข่าวสารของเจ้าของข้อมูล

(จ) วิธีการขอให้แก้ไขเปลี่ยนแปลงข้อมูล

(ฉ) แหล่งที่มาของข้อมูล

(4) ตรวจสอบแก้ไขข้อมูลข่าวสารส่วนบุคคลในความรับผิดชอบให้ถูกต้องอยู่เสมอ

(5) จัดระบบรักษาความปลอดภัยให้แก่ระบบข้อมูลข่าวสารส่วนบุคคลตามความเหมาะสมเพื่อป้องกันมิให้มีการนำไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

---

[36]**มาตรา 4** ได้ให้ความหมายของ *"หน่วยงานของรัฐ"* หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ ส่วนราชการสังกัดรัฐสภา ศาลเฉพาะในส่วนที่ไม่เกี่ยวกับการพิจารณาพิพากษาคดี องค์กรควบคุมการประกอบวิชาชีพ หน่วยงานอิสระของรัฐและหน่วยงานอื่นตามที่กำหนดในกฎกระทรวง.

[37]**มาตรา 4** ได้ให้ความหมายของ *" ข้อมูลข่าวสารส่วนบุคคล"* หมายความว่า ว่า "ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อของผู้นั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้หมายความรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย".

ในกรณีที่เก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูล ตามมาตรา 23 วรรคสอง กำหนดให้หน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบล่วงหน้าหรือพร้อมกับกับการขอข้อมูลถึงวัตถุประสงค์ที่จะนำข้อมูลมาใช้ ลักษณะการใช้ข้อมูลตามปกติ และกรณีที่ขอข้อมูลนั้นเป็นกรณีที่อาจให้ข้อมูลได้โดยความสมัครใจหรือเป็นกรณีมีกฎหมายบังคับ อีกทั้งหน่วยงานของรัฐต้องแจ้งให้เจ้าของข้อมูลทราบในกรณีมีการให้จัดส่งข้อมูลข่าวสารส่วนบุคคลไปยังที่ใดซึ่งจะเป็นผลให้บุคคลทั่วไปทราบข้อมูลข่าวสารนั้นได้ เว้นแต่เป็นไปตามลักษณะการใช้ข้อมูลตามปกติ (มาตรา 23 วรรคท้าย)

นอกเหนือจากมาตรา23 ในมาตรา24 ของพระราชบัญญัติฉบับนี้ก็ได้บัญญัติถึงการคุ้มครองในการเปิดเผยข้อมูลข่าวสารส่วนบุคคลเอาไว้ว่า หน่วยงานของรัฐจะเปิดเผยข้อมูลข่าวสารส่วนบุคคลที่อยู่ในความควบคุมดูแลของตนต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลที่ให้ไว้ล่วงหน้าหรือในขณะนั้นมิได้ เว้นแต่เป็นการเปิดเผยใน 9 กรณี ดังต่อไปนี้

(1) ต่อเจ้าหน้าที่ของรัฐในหน่วยงานของตนเพื่อการนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

(2) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดให้มีระบบข้อมูลข่าวสารส่วนบุคคลนั้น

(3) ต่อหน่วยงานของรัฐที่ทำงานด้านการวางแผนหรือการสถิติหรือสำมะโนต่างๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ไม่ให้เปิดเผยต่อไปยังผู้อื่น

(4) เป็นการให้เพื่อประโยชน์ในการศึกษาวิจัยโดยไม่ระบุชื่อหรือส่วนที่ทำให้รู้ว่าเป็นข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับบุคคลใด

(5) ต่อหอจดหมายเหตุแห่งชาติ กรมศิลปากร หรือหน่วยงานอื่นของรัฐตามมาตรา 26 วรรคหนึ่ง เพื่อการตรวจดูคุณค่าในการเก็บรักษา

(6) ต่อเจ้าหน้าที่ของรัฐเพื่อการป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

(7) เป็นการให้ซึ่งจำเป็นเพื่อการป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

(8) ต่อศาล และเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมายที่จะขอข้อเท็จจริงดังกล่าว

(9) กรณีอื่นตามที่กำหนดในพระราชกฤษฎีกา (นับจนถึงปัจจุบันนี้ พฤษภาคม 2549 ก็ยังไม่มีการตราพระราชกฤษฎีกาตามความในมาตรา 24 (9) ออกใช้บังคับแต่อย่างใด)

การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามวรรคหนึ่ง (3) (4) (5) (6) (7) (8) และ (9) มาตรา 24 วรรคท้ายได้กำหนดให้มีการจัดทำบัญชีแสดงการเปิดเผยกำกับไว้กับข้อมูลข่าวสารนั้น ตามหลักเกณฑ์และวิธีการที่กำหนดในกฎกระทรวงด้วย

ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งเป็นกฎหมายที่กำหนดรายละเอียดเพิ่มเติมในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานรัฐ นอกเหนือจากมาตรา 23และมาตรา 24แล้ว ก็ยังมีบทบัญญัติมาตรา 25 ที่รับรองถึงสิทธิในการรับทราบข้อมูลส่วนบุคคลเกี่ยวกับตนเองและสิทธิที่จะขอให้แก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคลนั้นให้ถูกต้องตรงตามความเป็นจริง โดยมาตรา 25 บัญญัติว่า

“ภายใต้บังคับมาตรา 14 และมาตรา 15 บุคคลย่อมมีสิทธิที่จะได้รู้ถึงข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตน และเมื่อบุคคลนั้นมีคำขอเป็นหนังสือ หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารนั้นจะต้องให้บุคคลนั้นหรือผู้กระทำการแทนบุคคลนั้นได้ตรวจดูหรือได้รับสำเนาข้อมูลข่าวสารส่วนบุคคลส่วนที่เกี่ยวกับบุคคลนั้น และให้นำมาตรา 9 วรรคสอง และวรรคสาม มาใช้บังคับโดยอนุโลม

การเปิดเผยรายงานการแพทย์ที่เกี่ยวกับบุคคลใด ถ้ากรณีมีเหตุอันควรเจ้าหน้าที่ของรัฐจะเปิดเผยต่อเฉพาะแพทย์ที่บุคคลนั้นมอบหมายก็ได้

ถ้าบุคคลใดเห็นว่าข้อมูลข่าวสารส่วนบุคคลที่เกี่ยวกับตนส่วนใดไม่ถูกต้องตามที่เป็นจริงให้มีสิทธิยื่นคำขอเป็นหนังสือให้หน่วยงานของรัฐที่ควบคุมดูแลข้อมูลข่าวสารแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารส่วนนั้นได้ ซึ่งหน่วยงานของรัฐจะต้องพิจารณาคำขอดังกล่าว และแจ้งให้บุคคลนั้นทราบโดยไม่ชักช้า

ในกรณีที่หน่วยงานของรัฐไม่แก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสารให้ตรงตามที่มีคำขอ ให้ผู้นั้นมีสิทธิอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารภายในสามสิบวันนับแต่วันได้รับแจ้งคำสั่งไม่ยินยอมแก้ไขเปลี่ยนแปลงหรือลบข้อมูลข่าวสาร โดยยื่นคำอุทธรณ์ต่อคณะกรรมการ และไม่ว่ากรณีใดๆ ให้เจ้าของข้อมูลมีสิทธิร้องขอให้หน่วยงานของรัฐหมายเหตุคำขอของตนแนบไว้กับข้อมูลข่าวสารส่วนที่เกี่ยวข้องได้

ให้บุคคลตามที่กำหนดในกฎกระทรวงมีสิทธิดำเนินการตามมาตรา 23 มาตรา 24 และมาตรานี้แทนผู้เยาว์ คนไร้ความสามารถ คนเสมือนไร้ความสามารถ หรือเจ้าของข้อมูลที่ถึงแก่กรรมแล้วได้”

เมื่อพิจารณาจากบทบัญญัติของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่เกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคลนี้ ก็จะพบว่ากฎหมายได้กำหนดหลักการสำคัญๆ ที่สามารถสรุปได้ 3 ประการ ดังต่อไปนี้

1) การกำหนดหน้าที่ต่าง ๆเกี่ยวกับการจัดระบบข้อมูลข่าวสารส่วนบุคคลให้กับหน่วยงานรัฐที่มีการจัดเก็บข้อมูล เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและปลอดภัย (มาตรา 23)

2) กำหนดข้อห้ามในการเปิดเผยข้อมูลข่าวสารส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล ยกเว้นแต่เข้าเงื่อนไขตามกฎหมายบัญญัติไว้ (มาตรา 24)

3) การให้สิทธิในการตรวจสอบข้อมูลข่าวสารส่วนบุคคลของตนเองที่จัดเก็บในหน่วยงานรัฐ และขอแก้ไขข้อมูลให้ถูกต้องตามความเป็นจริง รวมถึงสิทธิอุทธรณ์หากหน่วยงานรัฐไม่ปฏิบัติตาม

3.6.3 การคุ้มครองข้อมูลส่วนบุคคลในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดย สขร.

ปัจจุบัน(พ.ศ. 2557) ประเทศไทยได้มีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... บรรจุอยู่ในระเบียบวาระการประชุมของสภานิติบัญญัติแห่งชาติ ซึ่งเป็นร่างของคณะรัฐมนตรีที่ค้างการพิจารณามาตั้งแต่สมัยรัฐบาลนายกรัฐมนตรีอภิสิทธิ์ เวชชาชีวะ ต่อเนื่องมายังรัฐบาลนางสาวยิ่งลักษณ์ ชินวัตร ที่ได้เสนอเข้าสู่การพิจารณาของสภาผู้แทนราษฎรเมื่อวันพุธที่ 6 มีนาคม 2556 และผ่านการพิจารณาวาระที่ 1 ขั้นรับหลักการ และผ่านเข้าสู่การพิจารณาในวาระที่สอง การพิจารณาเรียงมาตราโดยคณะกรรมาธิการวิสามัญ แต่ร่างดังกล่าวก็ยังไม่ผ่านการให้ความเห็นชอบเนื่องจากเกิดเหตุการรัฐประหารเมื่อวันที่ 22 พฤษภาคม 2557 แต่ต่อมาคณะรักษาความสงบแห่งชาติได้เห็นความสำคัญของกฎหมายนี้ เมื่อได้มีการจัดตั้งรัฐบาลชุดใหม่ที่เข้ามาบริหารงานประเทศ คณะรัฐมนตรีโดยพลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรีจึงได้เสนอเข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติที่ทำหน้าที่รัฐสภาอีกครั้ง เมื่อวันที่ 7 ตุลาคม 2557 ตามหนังสือที่ นร 0503/188853

ร่างพระราชบัญญัติดังกล่าวเป็นร่างที่ผ่านการพิจารณาของคณะกรรมการกฤษฎีกา เป็นเรื่องเสร็จที่ 515/2552 ซึ่งได้รับอิทธิพลมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของต่างประเทศที่สำคัญ สามประเทศได้แก่

1. ประเทศแคนาดา คือ Privacy Act ที่ใช้กับข้อมูลส่วนบุคคลที่จัดเก็บในภาครัฐ และ Personal Information Protection and Electronic Documents Act (PIPEDA) ซึ่งใช้บังคับกับข้อมูลส่วนบุคคลในความดูแลของหน่วยงานภาคเอกชนและเอกสารอิเล็กทรอนิกส์

2. ประเทศสวีเดน คือ Personal Data Act (PDA) ซึ่งใช้บังคับกับข้อมูลส่วนบุคคลที่จัดเก็บทั้งในภาครัฐและภาคเอกชน

3. ประเทศสหพันธ์สาธารณรัฐเยอรมนีคือ Federal Data Protection Act ซึ่งใช้บังคับกับหน่วยงานของรัฐทั้งระดับสหพันธ์และมลรัฐที่ใช้อำนาจตามกฎหมายสหพันธ์หรือเป็นหน่วยงานของศาล และใช้บังคับกับหน่วยงานภาคเอกชนด้วย

หลักการและเหตุผลของความสำคัญในการเสนอร่างพระราชบัญญัติฉบับนี้ได้ระบุเหตุผลไว้อย่างชัดเจนว่า *“เนื่องจากปัจจุบันมีการล่วงละเมิดข้อมูลส่วนบุคคลเป็นจำนวนมาก*

โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผยโดยไม่ได้รับความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูลจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่บุคคลดังกล่าว แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป และโดยที่มาตรา 35 วรรคสาม และมาตรา 56 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน และการเปิดเผยข้อมูลส่วนบุคคล สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป เพื่อให้มีมาตรการคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลและการเปิดเผยข้อมูลส่วนบุคคลให้เป็นไปตามบทบัญญัติของรัฐธรรมนูญแห่งราชอาณาจักรไทย จึงจำเป็นต้องตราพระราชบัญญัตินี้”

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... มีทั้งหมด 61 มาตรา แบ่งออกเป็นหมวดต่างๆ 6 หมวด ได้แก่

หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (มาตรา 7-15)

หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล (มาตรา 16-40)

ส่วนที่ 1 บททั่วไป (มาตรา 16-21)

ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 22-24)

ส่วนที่ 3 การใช้และการเปิดเผยข้อมูลส่วนบุคคล(มาตรา 25-30)

ส่วนที่ 4 การเก็บรักษาและการแก้ไขเปลี่ยนแปลงข้อมูลส่วนบุคคล (มาตรา 31-33)

ส่วนที่ 5 ผู้ควบคุมข้อมูลส่วนบุคคลเชิงธุรกิจหรือการพาณิชย์(มาตรา 34-40)

หมวด 3 สิทธิของเจ้าของข้อมูลส่วนบุคคล (มาตรา 41-44)

หมวด 4 การร้องเรียน การตรวจสอบ และการอุทธรณ์ (มาตรา 45-48)

หมวด 5 มาตรการส่งเสริม (มาตรา 49-51)

หมวด 6 บทกำหนดโทษ (มาตรา 52-59)

ส่วนที่ 1 บททั่วไป (มาตรา 52)

ส่วนที่ 2 โทษปรับทางปกครอง (มาตรา 53-55)

ส่วนที่ 3 โทษอาญา (มาตรา 56-59)

บทเฉพาะกาล (มาตรา 60-61)

ร่างพระราชบัญญัติฉบับนี้ ได้กำหนดคำนิยามศัพท์ของ “ข้อมูลส่วนบุคคล” ไว้ในมาตรา 3 หมายความว่า *ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย*

เมื่อพิจารณาเปรียบเทียบความหมายของข้อมูลส่วนบุคคลที่ร่างกฎหมายฉบับนี้กำหนดไว้กับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ในมาตรา 4 ก็จะพบว่าเนื้อหาส่วนใหญ่มีความคล้ายคลึงกัน โดยมีความแตกต่างกันอยู่เล็กน้อยในสองประการกล่าวคือ

ประการที่ 1 การใช้ชื่อเรียกที่แตกต่างกัน กล่าวคือ ระหว่าง *"ข้อมูลข่าวสารส่วนบุคคล"* ในกฎหมายข้อมูลข่าวสารของราชการ *กับ"ข้อมูลส่วนบุคคล"* ในร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

ประการที่ 2 การยกตัวอย่างของข้อมูลส่วนบุคคล ซึ่งในร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล ได้เพิ่มตัวอย่างของประวัติกิจกรรมไว้ด้วย ขณะที่กฎหมายข้อมูลข่าวสารของราชการไม่ได้ระบุไว้

นอกเหนือจากนิยามดังกล่าวที่แตกต่างกัน ก็จะพบว่าร่างกฎหมายฯมีลักษณะที่น่าสนใจในมาตรา 4 ที่เป็นการกำหนดให้อำนาจนายกรัฐมนตรีโดยความเห็นชอบของคณะรัฐมนตรีอาจประกาศให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ซึ่งรวมถึงบทกำหนดโทษที่เกี่ยวข้องไปใช้บังคับเป็นการเพิ่มเติมหรือแทนที่กฎหมายว่าด้วยการนั้นได้ ขณะที่มาตรา 5 ได้กำหนดการไม่ใช้บังคับของพระราชบัญญัตินี้กับหน่วยงาน บุคคลและนิติบุคคลไว้สามกลุ่ม ได้แก่

(1) หน่วยงานของรัฐที่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ เว้นแต่รัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ

(2) บุคคลหรือนิติบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนของบุคคลหรือนิติบุคคลนั้นเท่านั้น โดยมิให้ผู้อื่นใช้ข้อมูลส่วนบุคคลนั้น หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อผู้อื่น

(3) บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวมรวมไว้เฉพาะเพื่อกิจการสื่อมวลชน งานศิลปกรรม หรือวรรณกรรมเท่านั้น

นอกจากนี้ยังสามารถยกเว้นแก่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะใดหรือกิจการใดได้โดยการตราเป็นพระราชกฤษฎีกาตามข้อเสนอของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอีกด้วย

สำหรับเนื้อหาของร่างพระราชบัญญัตินี้ได้สร้างให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 7 เป็นคณะกรรมการ โดยมีรัฐมนตรีซึ่งนายกรัฐมนตรีมอบหมายเป็นประธานกรรมการ และกรรมการอื่นๆประกอบด้วย

1. กรรมการโดยตำแหน่ง ได้แก่ ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เลขาธิการคณะกรรมการกฤษฎีกา อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ และผู้ว่าการธนาคารแห่งประเทศไทย

2. กรรมการซึ่งเป็นผู้แทนคณะกรรมการคุ้มครองผู้บริโภคหนึ่งคน ผู้แทนหอการค้าไทยหนึ่งคน และผู้แทนสมาคมธนาคารไทยหนึ่งคน

3. กรรมการผู้ทรงคุณวุฒิซึ่งนายกรัฐมนตรีแต่งตั้งจากผู้ซึ่งมีความรู้เชี่ยวชาญด้านกฎหมายและด้านเทคโนโลยีด้านละสองคน ซึ่งอย่างน้อยต้องแต่งตั้งจากภาคเอกชนไม่น้อยกว่ากึ่งหนึ่ง ซึ่งการได้มาให้เป็นไปตามหลักเกณฑ์และวิธีการที่นายกรัฐมนตรีประกาศกำหนด

4. ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นกรรมการและเลขานุการคณะกรรมการ

คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทำหน้าที่ดูเลรับผิดชอบกฎหมายนี้ตามมาตรา 11ทั้งหมด 8 ประการ ดังต่อไปนี้

(1) กำหนดนโยบาย มาตรการ หรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(2) เสนอความเห็นต่อนายกรัฐมนตรีเพื่อออกกฎกระทรวงหรือประกาศตามพระราชบัญญัตินี้

(3) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงแก้ไขกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(4) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆในการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งส่งเสริมการพัฒนาเทคโนโลยีที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(5) กำหนดหลักเกณฑ์ในการได้รับใบรับรองเพื่อมีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

(6) ออกระเบียบหรือประกาศเพื่อปฏิบัติการให้เป็นไปตามพระราชบัญญัตินี้

(7) จัดทำรายงานเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้เสนอต่อคณะรัฐมนตรีและรัฐสภาเป็นครั้งคราวตามความเหมาะสมอย่างน้อยปีละหนึ่งครั้ง และให้ประกาศรายงานดังกล่าวในราชกิจจานุเบกษาด้วย

(8) ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของคณะกรรมการหรือตามที่นายกรัฐมนตรีหรือคณะรัฐมนตรีมอบหมาย

ในส่วนหน่วยงานธุรการตามกฎหมายได้กำหนดให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการมีหน้าที่ปฏิบัติงานวิชาการและธุรการให้แก่คณะกรรมการและคณะอนุกรรมการในมาตรา 15 รวมทั้งให้มีอำนาจหน้าที่ ดังต่อไปนี้

1. ประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานอื่นของรัฐเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

2. ให้คำปรึกษาแก่องค์กรภาครัฐและเอกชนเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

3. กำหนดหลักสูตรและฝึกอบรมการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ลูกจ้าง หรือผู้รับจ้าง

4. จัดทำบัญชีรายชื่อผู้ควบคุมข้อมูลส่วนบุคคลเชิงธุรกิจหรือการพาณิชย์ตามมาตรา

5. ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้

6. ปฏิบัติการอื่นใดตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นอำนาจหน้าที่ของสำนักงาน หรือตามที่คณะกรรมการมอบหมาย

สาระสำคัญของร่างพระราชบัญญัตินี้ผู้ยกร่างและตรวจแก้ไขกฎหมายคือคณะกรรมการกฤษฎีกาได้กำหนดไว้เป็นดังนี้[38]

1) กำหนดให้มีลักษณะเป็นกฎหมายกลางเช่นเดียวกับกฎหมายว่าด้วยวัตถุอันตราย เนื่องจากข้อมูลส่วนบุคคลมีความหลากหลายเช่นเดียวกับวัตถุอันตราย โดยกำหนดให้การคุ้มครองข้อมูลส่วนบุคคลที่มีกฎหมายบัญญัติคุ้มครองไว้โดยเฉพาะแล้วให้บังคับตามบทบัญญัติแห่งกฎหมายว่าด้วยการนั้น แต่ถ้ามีเหตุอันควร นายกรัฐมนตรีโดยความเห็นชอบของคณะรัฐมนตรีอาจประกาศในราชกิจจานุเบกษาให้นำบทบัญญัติแห่งพระราชบัญญัตินี้ซึ่งรวมถึงบทกำหนดโทษที่เกี่ยวข้องไปใช้บังคับเป็นการเพิ่มเติมหรือแทนที่กฎหมายว่าด้วยการนั้นได้ ทั้งนี้โดยจะกำหนดระยะเวลาหรือเงื่อนไขอย่างใดไว้ในประกาศนั้นก็ได้ ตามร่างมาตรา 4

2) การคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัตินี้ ได้คำนึงถึงความสอดคล้องกับหลักสากล กล่าวคือ กำหนดห้ามการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ส่วนกรณีที่จะเก็บรวบรวม ใช้ หรือเปิดเผยได้นั้นเป็นข้อยกเว้น และการขอความยินยอมจะต้องปฏิบัติตามหลักเกณฑ์ที่กำหนดจึงจะถือว่าได้รับความยินยอมโดยชอบ เช่น ไม่ทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์หรือไม่หลอกหลวงและต้องแจ้งวัตถุประสงค์ รวมทั้งรายละเอียดของผู้เก็บรวบรวม โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจกำหนดแบบหรือข้อความในการขอความยินยอมได้และมีอำนาจประกาศกำหนดประมวลจริยธรรมเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้ปฏิบัติตามได้อีกด้วย (ร่างมาตรา 16 และมาตรา 18 ถึงมาตรา30)

3) กำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งหมายถึงผู้มีหน้าที่รับผิดชอบในการเก็บรวบรวม ควบคุมการใช้และการเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะหน้าที่ในการเก็บรักษาข้อมูลส่วนบุคคลตามระยะเวลาที่กำหนดหรือเท่าที่จำเป็นตามวัตถุประสงค์ หน้าที่ในการจัดให้มีระบบรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลส่วนบุคคล และหน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องครบถ้วน และเป็นปัจจุบันตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอหรือเมื่อจะใช้หรือเปิดเผยข้อมูลนั้น (ร่างมาตรา 17 และมาตรา 31 ถึงมาตรา 33)

4) กำหนดมาตรการควบคุมผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประกอบกิจการเชิงธุรกิจหรือการพาณิชย์ตามที่กำหนดในกฎกระทรวง ให้มีมาตรการเพิ่มเติมจากผู้ควบคุมข้อมูลส่วนบุคคลทั่วๆไป เช่น ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลจะต้องแจ้งข้อปฏิบัติเกี่ยวกับการเก็บ

[38] บันทึกวิเคราะห์สรุปสาระสำคัญของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....ที่คณะรัฐมนตรี(นางสาวยิ่งลักษณ์ ชินวัตร) เป็นผู้เสนอเมื่อวันที่ 27 กุมภาพันธ์ 2557 ต่อ ประธานสภาผู้แทนราษฎร

รวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลด้วย ต้องตั้งหน่วยรับเรื่องร้องเรียน กรณีลูกจ้างกระทำการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ หรือรับเรื่องร้องขอเพื่อแก้ไขข้อมูลส่วนบุคคลให้ถูกต้องครบถ้วน หรือเป็นปัจจุบัน นอกจากนี้ หากผู้ควบคุมข้อมูลส่วนบุคคลประเภทนี้เลิกกิจการจะต้องแจ้งให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการทราบและต้องจัดการข้อมูลส่วนบุคคลตามที่กำหนด (ร่างมาตรา 34 ถึงมาตรา 40)

5) กำหนดสิทธิของเจ้าของข้อมูลส่วนบุคคล เช่น ขอตรวจข้อมูลส่วนบุคคลที่เกี่ยวกับตน หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลที่เกี่ยวกับตนในกรณีที่เป็นข้อมูลซึ่งไม่ได้ให้ความยินยอมมาก่อน (มาตรา 41 ถึงมาตรา 44)

6) กำหนดให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายมีสิทธิร้องเรียนต่อคณะกรรมการตรวจสอบข้อมูลส่วนบุคคลซึ่งแต่งตั้งโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการดังกล่าวมีอำนาจตรวจสอบการกระทำใดๆ ที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล ไกล่เกลี่ยข้อพิพาทระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ควบคุมข้อมูลส่วนบุคคล รวมทั้งมีอำนาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลระงับการกระทำหรือแก้ไขการกระทำที่ก่อให้เกิดความเสียหายได้ นอกจากนี้ได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลหรือผู้ควบคุมข้อมูลส่วนบุคคลซึ่งไม่พอใจมีสิทธิอุทธรณ์ต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ (ร่างมาตรา 45 ถึงมาตรา 48)

7) กำหนดให้มีมาตรการส่งเสริมโดยผู้ควบคุมข้อมูลส่วนบุคคลอาจขอรับการส่งเสริมจากสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการได้ เช่น การขอคำแนะนำหรือคำปรึกษาในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล การอบรมและพัฒนาความรู้ความสามารถของบุคคลซึ่งปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล หรืออื่นๆตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด รวมทั้งหากผู้ควบคุมข้อมูลส่วนบุคคลประสงค์จะมีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลก็สามารถยื่นคำขอใบรับรองจากสำนักงานได้ เมื่อสำนักงานประเมินผลการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลว่ามีประสิทธิภาพและได้มาตรฐานสำนักงานจะเสนอคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลให้ความเห็นชอบ และออกใบรับรองแก่ผู้ควบคุมข้อมูลส่วนบุคคลนั้น เพื่อให้มีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐานฯ ซึ่งสำนักงานจะต้องตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลเป็นระยะๆ หากผู้ควบคุมข้อมูลส่วนบุคคลดำเนินงานต่ำกว่ามาตรฐาน สำนักงานก็อาจเพิกถอนใบรับรอง ซึ่งผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคืนใบรับรองที่ถูกเพิกถอนภายในสิบห้าวันนับแต่วันที่ถูกเพิกถอน

นอกจากนี้ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจประกาศยอมรับการตรวจสอบและรับรองเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลซึ่งกระทำโดยหน่วยงานอื่นไม่ว่าจะเป็นหน่วยงานของรัฐหรือเอกชนหรือจะตั้งอยู่ในต่างประเทศก็ได้ เมื่อคณะกรรมการประกาศยอมรับแล้วจะมีผลทำให้ผู้ควบคุมข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานดังกล่าวมีสิทธิใช้หรือแสดงเครื่องหมายรับรองมาตรฐาน (ร่างมาตรา 49ถึงมาตรา 51)

8) กำหนดให้มีบทลงโทษโยแบ่งออกเป็น สามส่วน ดังนี้

ส่วนที่ 1 บททั่วไป เป็นบทกำหนดโทษกรณีนิติบุคคลเป็นผู้กระทำความผิดซึ่งต้องรับโทษตามพระราชบัญญัตินี้ กรรมการผู้จัดการ ผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้นต้องระวางโทษตามที่บัญญัติไว้สำหรับความผิดนั้นๆด้วย เว้นแต่จะพิสูจน์ได้ว่าตนมิได้รู้เห็นหรือยินยอมในการกระทำผิดของนิติบุคคลนั้น (ร่างมาตรา 52)

ส่วนที่ 2 โทษปรับทางปกครอง โดยกำหนดให้ผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นผู้มีอำนาจลงโทษปรับทางปกครอง ซึ่งโทษปรับทางปกครองจะใช้กับความผิดเล็กน้อยหรือความผิดที่ไม่ใช่หลักการสำคัญของพระราชบัญญัตินี้ เช่น ความผิดฐานไม่มาให้ถ้อยคำ ความผิดฐานไม่จัดทำบัตรประจำตัวลูกจ้าง ความผิดฐานไม่แก้ไขข้อมูลส่วนบุคคลให้ถูกต้องก่อนใช้ ความผิดฐานไม่แจ้งวัตถุประสงค์ในการขอความยินยอม ความผิดฐานไม่จัดทำรายการแสดงการเก็บรวบรวมข้อมูลส่วนบุคคลหรือความผิดฐานไม่แจ้งรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นต้น ซึ่งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะประกาศกำหนดหลักเกณฑ์ในการพิจารณาโทษปรับทางปกครองและหากผู้ถูกลงโทษไม่ยอมชำระค่าปรับ ก็จะถูกมาตรการบังคับทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง (ร่างมาตรา 53 ถึงมาตรา 55)

ส่วนที่ 3 โทษอาญาซึ่งจะใช้กับความผิดสำคัญๆเช่น ความผิดฐานเก็บรวบรวมใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมหรือไม่เข้าข้อยกเว้นหรือความผิดฐานไม่จัดให้มีระบบรักษาความมั่นคงปลอดภัยแก่ข้อมูลส่วนบุคคล เป็นต้น โดยได้กำหนดให้มีบทเปรียบเทียบสำหรับความผิดที่มีโทษปรับสถานเดียวไว้ด้วย (ร่างมาตรา 56ถึงมาตรา 59)

9) บทเฉพาะกาล ได้กำหนดให้ในวาระเริ่มแรก คณะกรรมการข้อมูลส่วนบุคคลจะประกอบด้วยกรรมการโดยตำแหน่งเท่านั้น เนื่องจากคณะกรรมการชุดนี้มีความสำคัญในการออกระเบียบหรือประกาศตามพระราชบัญญัตินี้ หากมีข้อขัดข้องในการแต่งตั้งคณะกรรมการผู้ทรงคุณวุฒิคณะกรรมการชุดนี้ก็สามารถดำเนินการได้ไม่ส่งผลกระทบต่อการบังคับใช้กฎหมาย ทั้งนี้โดยมีบทเร่งรัดให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการดำเนินการให้มีการแต่งตั้งกรรมการผู้รงคุณวุฒิภายในเก้าสบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับด้วย (ร่างมาตรา 60) อีกทั้งกำหนดไม่ให้กฎหมายมีผลใช้บังคับย้อนหลังไว้อย่างชัดเจน สำหรับการปฏิบัติตามบทบัญญัติเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลที่อยู่ในความครอบครองก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ นอกจากนี้ได้กำหนดให้การปฏิบัติเกี่ยวกับการจัดให้มีระบบรักษาความมั่นคงปลอดภัยแก่ข้อมูลส่วนบุคคลไม่ต้องดำเนินการทันที เนื่องจากการปฏิบัติจะต้องมีภาระค่าใช้จ่ายจึงผ่อนเวลาให้อีกเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ (ร่างมาตรา 61)

หลักการสำคัญของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่นำเสนอมาข้างต้นมีประเด็นที่ต้องศึกษาวิเคราะห์ต่อไปในการเปรียบเทียบกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศในอาเซียนอื่นๆที่ได้ตราขึ้นบังคับใช้แล้ว โดยเฉพาะอย่างยิ่งมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลที่ปรากฏในกฎหมายของไทยว่ามีมาตรฐานเทียบเท่าของต่างประเทศนั้นๆหรือไม่ เพราะหากมีมาตรฐานไม่เทียบเท่าหรือมีลักษณะที่ต่ำกว่าก็จะเกิดผลกระทบอย่างสำคัญในการ

ที่ต่างประเทศจะสามารถส่งข้อมูลส่วนบุคคลมายังประเทศไทยได้ เพราะส่วนใหญ่กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศอาเซียนที่ได้ทำการศึกษาในรายงานวิจัยนี้จะมีข้อห้ามมิให้ส่งข้อมูลส่วนบุคคลของประเทศตนมายังประเทศที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ต่ำกว่า

ทั้งนี้หากศึกษาวิเคราะห์ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทย คณะผู้ศึกษาเห็นว่ามีมาตรฐานที่ทัดเทียมกับต่างประเทศในประชาคมอาเซียนไม่ว่าจะเป็นอินโดนีเซีย ฟิลิปปินส์ มาเลเซีย หรือสิงคโปร์ เนื่องจากร่างกฎหมายของไทยได้นำหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคลในทางระหว่างประเทศมาบัญญัติรับรองไว้ อีกทั้งยังมีเนื้อหาของบทบัญญัติที่ได้รับอิทธิผลมาจากต้นแบบกฎหมายของประเทศแคนาดา สวีเดนและเยอรมนี ที่มีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับความน่าเชื่อถือ โดยเฉพาะทั้งฝั่งกฎหมายในทวีปอเมริกาเหนือและกลุ่มประเทศสหภาพยุโรป (EU) ที่มีมาตรฐานในระดับสูงและเข้มงวด

อย่างไรก็ตาม คณะผู้ศึกษาก็มีข้อสังเกตและห่วงใยต่อความทันสมัยและการมีเนื้อหาที่ครอบคลุมปัญหาใหม่ๆของร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยซึ่งผ่านการพิจารณาจากคณะกรรมการกฤษฎีกามาตั้งแต่ปีพ.ศ. 2552 หรือ ค.ศ. 2009 ขณะที่เมื่อเปรียบเทียบกับประเทศในอาเซียนที่ได้ประกาศใช้กฎหมายนั้นก็เป็นในช่วงปี ค.ศ. 2010 เป็นต้นมาทั้งสิ้น ซึ่งถ้าพิจารณาดูเนื้อหาของกฎหมายต่างประเทศก็จะพบว่ามีหลายเรื่องที่ก้าวหน้าและครอบคลุมสถานการณ์ใหม่ๆ ของปัญหาการคุ้มครองข้อมูลส่วนบุคคลของประชาชน และที่สำคัญเจตนารมณ์ของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในต่างประเทศมีความพยายามในการรักษาสมดุลระหว่างการคุ้มครองสิทธิส่วนบุคคลกับการนำข้อมูลไปใช้ในทางเศรษฐกิจเพื่อพัฒนามูลค่าทางเศรษฐกิจของประเทศให้สูงขึ้นในโลกยุคข้อมูลสารสนเทศ ขณะที่ร่างกฎหมายของไทยเนื้อหาส่วนใหญ่เป็นการมุ่งคุ้มครองสิทธิเสรีภาพของประชาชนไม่ให้ถูกล่วงละเมิดจากการใช้ข้อมูลข่าวสารส่วนบุคคลในทางที่ผิด ฉะนั้นในประเด็นนี้คณะผู้ศึกษาจะนำเสนอให้เห็นถึงประสบการณ์ของต่างประเทศในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เป็นตัวอย่างที่ดีแก่ประเทศไทยนำมาทบทวนแก้ไขร่างกฎหมายให้ดีขึ้นในบทถัดไป

3.6.4 การคุ้มครองข้อมูลส่วนบุคคลในร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เมื่อพิจารณาถึงสถานการณ์ปัจจุบันของประเทศไทยเกี่ยวกับการตรากฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลนั้น จะพบถึงปัญหาที่ก่อให้เกิดความไม่ชัดเจนในการดำเนินงาน ด้วยเหตุที่แม้รัฐบาลพลเอกประยุทธ์ จันทร์โอชาจะได้เสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งเป็นร่างเดิมที่ผ่าการพิจารณาของคณะกรรมการกฤษฎีกาที่ค้างอยู่ในการพิจารณาของรัฐสภาชุดที่แล้วเข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติอีกครั้งเมื่อวันที่ 7 ตุลาคม พ.ศ. 2557 แต่ต่อมาคณะรัฐมนตรีก็ได้ให้ความเห็นชอบในหลักการของร่างกฎหมายเศรษฐกิจดิจิทัล จำนวน 10

ฉบับที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร[39] โดยหนึ่งในร่างกฎหมายเหล่านั้นก็มีร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ซึ่งมีหลักการและเหตุผลเช่นเดียวกับร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่อยู่ระหว่างการพิจารณาของสภานิติบัญญัติแห่งชาติ แต่ทั้งนี้ก็ยังมีความแตกต่างในหลายประเด็น โดยเฉพาะการเปลี่ยนแปลงหน่วยงานที่มีบทบาทรับผิดชอบตามกฎหมายจากสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการมาเป็นสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่จัดตั้งขึ้นใหม่

อย่างไรก็ตามการเสนอร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารก็ให้เกิดเสียงคัดค้านและไม่เห็นด้วยจากหลายฝ่าย เฉพาะอย่างยิ่งองค์กรพัฒนาภาคเอกชนและนักวิชาการที่เห็นว่าร่างกฎหมายดังกล่าวขาดความเหมาะสมในบทบัญญัติเมื่อเปรียบเทียบกับร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลเดิมที่ได้เสนอเข้าสู่สภานิติบัญญัติแห่งชาติ

นอกจากนี้คณะผู้ศึกษายังมีความเห็นว่า แม้เจตนารมณ์ของกระทรวงICT และรัฐบาลจะมีนโยบายที่ส่งเสริมเศรษฐกิจดิจิทัลในประเทศไทย จึงได้ดำเนินการผลักดันให้มีการตราชุดกฎหมายที่มีความจำเป็นในการรองรับ ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลก็เป็นหนึ่งในกฎหมายที่จำเป็นเพื่อให้เกิดการคุ้มครองข้อมูลส่วนบุคคลในการดำเนินงานทางธุรกิจที่เกิดขึ้นบนเครือข่ายของระบบคอมพิวเตอร์ที่มีการติดต่อสื่อสารถึงกันในภาคเอกชน อันเป็นเจตนารมณ์ที่ดี แต่การผลักดันร่างกฎหมายดังกล่าวก็ก่อให้เกิดปัญหาสำคัญในความเป็นเอกภาพของการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยเนื่องจากจะทำให้หน่วยงานของรัฐที่ดูแลการคุ้มครองข้อมูลส่วนบุคคลไม่ได้รวมอยู่ที่เดียวโดยแยกออกเป็นสององค์กรกล่าวคือ

---

1. [39] ร่างพระราชบัญญัติว่าด้วยคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ พ.ศ. ....
2. ร่างพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม เพื่อกำหนดให้มีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพ.ศ.....
3. ร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ....
4. ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. ....
5. ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ....
6. ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลพ.ศ. ....
7. ร่างพระราชบัญญัติว่าด้วยการส่งเสริมเศรษฐกิจดิจิทัลพ.ศ. ....
8. ร่างพระราชบัญญัติกองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมพ.ศ. ....
9. ร่างพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคมพ.ศ. ....
10. ร่างพระราชกฤษฎีกาจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. ....

1. การดูแลข้อมูลข่าวสารส่วนบุคคลในภาครัฐจะเป็นหน้าที่ของคณะกรรมการข้อมูลข่าวสารของราชการและสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

2. การดูแลข้อมูลข่าวสารส่วนบุคคลในภาคเอกชนจะเป็นหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดยกระทรวง ICT

ทั้งนี้ในห้วงเวลาปัจจุบัน (เมษายน 2558) ร่างพระราชบัญญัติดังกล่าวยังอยู่ระหว่างการพิจารณาตรวจร่างแก้ไขโดยคณะกรรมการกฤษฎีกา และได้มีการจัดรับฟังความคิดเห็นภาคส่วนต่างๆ ในสังคมไปครั้งหนึ่งแล้ว เมื่อวันที่ 11 มีนาคม 2558 โรงแรมรอยัลปริ๊นเซส ถนนหลานหลวง ซึ่งได้มีความเห็นของนายถนัดกิจ นิวาทวงษ์ ผอ.ฝ่ายกฎหมายยุติธรรมทางอาญา สำนักงานคณะกรรมการกฤษฎีกา ได้กล่าวถึงประเด็นการปรับปรุงแก้ไขร่างพ.ร.บ.ที่เสนอโดยกระทรวงICT อย่างน่าสนใจดังนี้

“การบังคับใช้กฎหมายได้มีการคุ้มครองข้อมูลส่วนบุคคลอยู่หลายฉบับ เช่น พ.ร.บ.สถิติ พ.ร.บ.ข้อมูลข่าวสารทางราชการ พ.ร.บ.การประกอบธุรกิจข้อมูลเครดิต หรือล่าสุดมี พ.ร.บ.การทวงถามหนี้ฯ พ.ร.บ.คุ้มครองสุขภาพแห่งชาติ เป็นต้น แต่ยังไม่มีกฎหมายที่ครอบคลุมธุรกิจอื่นๆ เช่น โรงแรม หรือสายการบิน จึงจำเป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลขึ้นมา และเมื่อมีกฎหมายนี้ขึ้นมาอาจผลมีกระทบไปยังกฎหมายที่มีอยู่แล้ว หากมีหลักเกณฑ์ที่ไม่ต่ำกว่า พ.ร.บ.ก็ให้ใช้กฎหมายนั้นๆไป แต่ในทางปฏิบัติก็ทำให้ลำบาก เพราะเจ้าหน้าที่ต้องนำกฎหมายมาเปรียบเทียบในเรื่องความเป็นธรรมตามกฎหมายต่างๆยากที่จะวินิจฉัย

นายถนัดกิจกล่าวอีกว่า คณะกรรมการกฤษฎีกาชุดที่ 11 จึงได้ปรับใช้หลักตัดกฎหมายทั่วไปในการร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลฯ ว่า หากจะใช้กฎหมายนี้บังคับก็ต้องไปดูว่ามีกฎหมายนั้นๆ บังคับอยู่หรือไม่ หากมีอยู่แล้วก็ให้ใช้กฎหมายนั้นๆ ไป เพื่อไม่ให้เกิดความยุ่งยาก แต่ก็ต้องยอมรับว่ากฎหมายเฉพาะนั้นได้เขียนไว้กว้างๆ เท่านั้น จึงได้เขียนไว้ในร่างกฎหมายนี้ว่าให้ออกประกาศให้นำบทบัญญัติใช้บังคับเพิ่มเติมตามกฎหมายฉบับนั้นๆ ได้ ขึ้นอยู่กับความเห็นของคณะกรรมการและรัฐมนตรี ส่วนเรื่องที่เกี่ยวกับสื่อมวลชนนั้นได้มีการยกเว้นให้ เพราะมีความจำเป็นต้องทำหน้าที่เพื่อประโยชน์สาธารณะ รวมไปถึงผู้ที่ทำงานด้านศิลปะด้านต่างๆ องค์กรทางศาสนา สภาผู้แทนราษฎร วุฒิสภา และอื่นๆ ที่กำหนดไว้ เป็นต้น อย่างไรก็ตาม สื่อมวลชนยังคงต้องรับผิดชอบกรณีที่ใช้ข้อมูลนั้นแล้วเกิดความเสียหายกับเจ้าของข้อมูลก็ต้องรับผิดชอบตามกฎหมายที่มีอยู่เดิม

“ร่างของกฤษฎีกาได้ตัดปลัดกระทรวงมหาดไทย และเลขาธิการสภาความมั่นคงแห่งชาติ (สมช.) ออกไปจากองค์ประกอบของคณะกรรมการ ขณะเดียวกัน เพื่อให้มีมิติการส่งเสริมและคุ้มครองสิทธิเสรีภาพ ได้ให้อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ กระทรวงยุติธรรม ผู้แทนหอการค้าไทย ผู้แทนสมาคมธนาคารไทยเข้ามาเป็นคณะกรรมการแทน”[40]

[40] ผู้จัดการออนไลน์ วันที่ 11 มีนาคม 2558 “กฤษฎีกาสัมมนา กม.เศรษฐกิจดิจิตอล รับร้อ่าง ครม.เพียบนักวิชาการ-TDRI สวดยับ รบ.” http://www.manager.co.th/Politics/ViewNews.aspx?NewsID =9580000028852

ดังนั้น จากการสัมมนารับฟังความคิดเห็นข้างต้นจะเห็นได้ว่า ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดยกระทรวง ICT คงต้องมีการปรับปรุงแก้ไขเนื้อหาให้มีความสมบูรณ์ในหลายส่วนในชั้นของคณะกรรมการกฤษฎีกา ซึ่งหากเปรียบเทียบเนื้อหาระหว่างร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งสองฉบับก็จะพบถึงความแตกต่างในประเด็นสำคัญถึง 19 ประเด็น ดังต่อไปนี้ [41]

ประเด็นที่หนึ่ง : แก้ไขความหมายของคำว่า “ข้อมูลส่วนบุคคล” ใหม่ให้สั้นแต่ตีความได้กว้าง

แก้ไขนิยามศัพท์ ของคำว่า **“ข้อมูลส่วนบุคคล”** จาก ข้อมูลส่วนบุคคลที่เกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม และเลขหมาย รหัส หรือสิ่งที่บอกลักษณะอื่นที่จะทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายนิ้วมือแผ่นบันทึกลักษณะเสียงของคน รูปถ่าย **เหลือเพียง “ข้อมูลเกี่ยวกับบุคคล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม”**

ประเด็นที่สอง : ลดนิยาม “เจ้าของข้อมูลส่วนบุคคล” ไม่ให้สิทธิทายาทและคู่สมรสเมื่อเจ้าของข้อมูลถึงแก่กรรม

แก้ไขนิยามคำว่า “เจ้าของข้อมูลส่วนบุคคล” ใหม่ เหลือเพียง บุคคลซึ่งเป็นเจ้าของข้อมูลเท่านั้น ทั้งที่ ในร่างกฎหมายเดิมถ้าเจ้าของข้อมูลเสียชีวิต ทายาทและคู่สมรส รวมถึงผู้ซึ่งมีหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคลจะถือว่าเป็นเจ้าของข้อมูลด้วย

ประเด็นที่สาม : เปลี่ยน “ผู้ควบคุมข้อมูลส่วนบุคคล” จากผู้มีหน้าที่รับผิดชอบเป็นผู้มีอำนาจตัดสินใจ

แก้ไขนิยามคำว่า **“ผู้ควบคุมข้อมูลส่วนบุคคล”** จากเดิมหมายความว่า **“ผู้ซึ่งมีหน้าที่รับผิดชอบ** ในการเก็บรวบรวม ควบคุมการใช้และการเปิดเผยข้อมูลส่วนบุคคล” กลายเป็น **“ผู้ซึ่งมีอำนาจตัดสินใจ** เกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคล ซึ่งรวมถึงการเก็บรวบรวม การใช้และเปิดเผยข้อมูลส่วนบุคคล”

ประเด็นที่สี่ : ย้ายงานข้อมูลส่วนบุคคลไปสังกัด "ความมั่นคงไซเบอร์"

จากเดิม “สำนักงาน” คือ สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ แต่ร่างกฎหมายใหม่เปลี่ยนเป็น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แทน และตัดคำว่า “ผู้อำนวยการ” หรือ ผู้อำนวยการคณะกรรมการข้อมูลข่าวสารของราชการ และเปลี่ยนเป็น “เลขาธิการ” ซึ่งก็คือ เลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

[41] i.law วันที่ 21 มกราคม 2558 “ 19 ประเด็นสำคัญที่เปลี่ยนแปลงในร่าง พ.ร.บ.คุ้มครอง Privacy (ฉบับความมั่นคงดิจิทัล) ” http://ilaw.or.th/node/3405

ประเด็นที่ห้า : สัดส่วนของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเปลี่ยนไปเน้นด้าน “ความมั่นคง”

ในร่างพ.ร.บ.ข้อมูลส่วนบุคคลฉบับใหม่ จะ**ตัดตัวแทนด้านคุ้มครองผู้บริโภค สิทธิเสรีภาพของประชาชน และข้อมูลข่าวสารของทางราชการ** ออกจากที่นั่งในคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแห่งชาติ และ**เพิ่มตัวแทนด้านความมั่นคง**เข้ามาแทน โดยกำหนดให้กรรมการจำนวน 6-7 คนมาจากการแต่งตั้งของคณะรัฐมนตรี กรรมการโดยตำแหน่งมาจาก ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงมหาดไทย เลขาธิการสภาความมั่นคงแห่งชาติ และ เลขาธิการสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นคณะกรรมการและเลขานุการด้วย

ในขณะที่สัดส่วนคณะกรรมการชุดเก่าประกอบไปด้วย ปลัดสำนักนายกฯ ปลัดกระทรวงไอซีที เลขากฤษฎีกา อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ ผู้ว่า ธปท. ตัวแทนคณะกรรมการคุ้มครองผู้บริโภค ตัวแทนหอการค้าไทย ตัวแทนสมาคมธนาคารไทย และ กรรมการผู้ทรงคุณวุฒิที่นายกฯ แต่งตั้งจากผู้เชี่ยวชาญด้านกฎหมายและเทคโนโลยี โดยมี ผู้อำนวยการคณะกรรมการข้อมูลข่าวสารของราชการ เป็นกรรมการและเลขานุการ

เมื่อเปรียบเทียบกับในร่างที่กระทรวงไอซีทีเคยเสนอเมื่อหลายปีก่อน จะมีตัวแทนจากคณะกรรมการข้อมูลข่าวสารของราชการ คณะกรรมการทางธุรกรรมอิเล็กทรอนิกส์ สมาคมสมาพันธ์เทคโนโลยีสารสนเทศ หอการค้านานาชาติแห่งประเทศไทย สภาทนายความ และคณะกรรมการสิทธิฯ อีกด้วย

ประเด็นที่หก : อำนาจหน้าที่ของกรรมการคุ้มครองข้อมูลส่วนบุคคลมีรายละเอียดมากขึ้น

สาระสำคัญเรื่องอำนาจหน้าที่ของคณะกรรมการตามร่างกฎหมายฉบับเดิม ได้แก่ เสนอความเห็นต่อนายกรัฐมนตรีในการวางมาตรการ ตรา หรือ ปรับปรุงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และกำหนดหลักเกณฑ์การได้ใบรับรองเพื่อมีสิทธิใช้เครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลแต่ในร่างกฎหมายฉบับใหม่ แม้ว่าเนื้อหาสาระไม่ได้แตกต่างกันมาก แต่ **เพิ่มอำนาจ การกำกับดูแลพนักงานเจ้าหน้าที่ หน่วยงานของรัฐ และผู้ควบคุมข้อมูลให้ทำงานภายใต้ขอบเขตที่กำหนด อำนาจพิจารณาคำร้องทุกข์ และมีอำนาจในการวินิจฉัยข้อพิพาทระหว่างบุคคลฝ่ายต่าง ๆ**

ประเด็นที่เจ็ด : เปลี่ยนบทบาทของสำนักงานคณะกรรมการข้อมูลข่าวสารของทางราชการ

ในร่างกฎหมายฉบับเดิม กำหนดอำนาจหน้าที่ของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ ในการประสานงานกับส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน และหน่วยงานรัฐอื่นๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล จัดทำบัญชีรายชื่อ "ผู้ควบคุมข้อมูล" และติดตามการประเมินผลการทำงานแต่ในร่างกฎหมายฉบับใหม่ ให้อำนาจในการกำกับดูแลพนักงานเจ้าหน้าที่

หน่วยงานของรัฐ และผู้ควบคุมข้อมูลให้ทำงานตามที่กำหนดไว้ สามารถพิจารณาคำร้องทุกข์ มีอำนาจวินิจฉัยข้อพิพาท และสามารถแต่งตั้งอนุกรรมการ พนักงานเจ้าหน้าที่ของรัฐ แต่จำกัดอำนาจเหล่านี้เฉพาะกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐ

ประเด็นที่แปด : เปลี่ยนแนวคิดจากการ "ขอความยินยอม" เป็น "แจ้งให้ทราบ"

ในร่างกฎหมายเดิม ผู้ควบคุมข้อมูลจะเก็บรวบรวมไม่ได้ หากเจ้าของไม่ได้ให้ความยินยอม **ในร่างกฎหมายใหม่ ไม่ได้มีบทบัญญัติเกี่ยวกับการขอความยินยอม**ในการเก็บรวบรวมข้อมูลส่วนบุคคลกับเจ้าของข้อมูลส่วนบุคคล แต่**บังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งให้เจ้าของข้อมูลทราบ** ก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคลถึงรายละเอียดดังต่อไปนี้ (มาตรา 22)

(1) วัตถุประสงค์ของการเก็บรวบรวม (2) ข้อมูลที่จะมีการเก็บรวบรวม (3) ประเภทของบุคคลหรือหน่วยงานที่ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย (4) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ (5) สิทธิของเจ้าของข้อมูลเท่ากับเปลี่ยนแนวคิดจากการ "ขอความยินยอม" เป็นการ "แจ้งให้ทราบ"

ประเด็นที่เก้า : เปิดช่องเก็บข้อมูลได้อิสระ โดยไม่ต้องขอและไม่ต้องแจ้ง

ในร่างกฎหมายเดิมกำหนดเก็บข้อมูลอย่างไรที่ไม่ต้องขอความยินยอม แต่ร่างกฎหมายใหม่กำหนดการเก็บข้อมูลแบบไหนที่ไม่ต้องแจ้งรายละเอียดตาม มาตรา22 หมายความว่า **ในร่างกฎหมายใหม่ นอกจากไม่ต้องขอความยินยอม ยังมีการเก็บข้อมูลที่ไม่ต้องแจ้งวัตถุประสงค์ในการเก็บข้อมูลที่จะเก็บ บุคลหรือหน่วยงานที่จะเข้าถึงข้อมูลส่วนบุคคล หรือข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล และสิทธิของเจ้าของข้อมูล** ซึ่งเหตุผลการเก็บข้อมูลที่ได้รับการยกเว้นไม่ต้องแจ้งรายละเอียดตามมาตรา 22 ได้แก่

(1) เพื่อประโยชน์ที่เกี่ยวกับการวางแผนหรือการสถิติหรือสำมะโนต่าง ๆ ของหน่วยงานของรัฐ (2) เพื่อประโยชน์แก่การสืบสวน สอบสวนของพนักงานเจ้าหน้าที่ตามกฎหมาย หรือการพิจารณาพิพากษาคดีของศาล (3) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคล (4) เป็นข้อมูลที่เปิดเผยต่อสาธารณะโดยชอบด้วยกฎหมาย (5) เป็นการปฏิบัติตามที่กฎหมายกำหนด หรือตามคำสั่งศาล (6) กรณีอื่นตามที่กำหนดในกฎกระทรวง

อย่างไรก็ดี สิ่งที่หายไปจากกฎหมายฉบับเดิม คือ การเก็บข้อมูลเพื่อการศึกษาวิจัย และสถิติที่ผู้เก็บจะเก็บข้อมูลเป็นความลับถ้าจะเปิดเผยให้แจ้งสำนักงานข้อมูลข่าวสารของทางราชการ กับตัดเรื่องการเก็บข้อมูลที่เป็นประโยชน์ต่อเจ้าของ และ กรณีไม่สามารถขอความยินยอมได้ทันออกไป

ประเด็นที่สิบ : การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูล แค่แจ้งให้ทราบก็พอ

เมื่อหลักการของร่างกฎหมายใหม่ ไม่เน้นเรื่องการขอความยินยอม เพราะฉะนั้นในร่างกฎหมายใหม่กำหนดให้การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูล ผู้เก็บเพียงแค่แจ้งให้เจ้าของข้อมูลทราบก่อนจะเก็บหรือในขณะเก็บก็ได้ ซึ่งการเก็บข้อมูลที่ได้รับการยกเว้นไม่ต้องแจ้งให้เจ้าของข้อมูลทราบ มาตรา 22 ถือเป็นเหตุในการเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลได้เลยทันที หมายความว่า **การเก็บข้อมูลบางประเภทจะได้รับการยกเว้นไม่ต้องแจ้งให้เจ้าของข้อมูลทราบ**

และยังเก็บข้อมูลจากที่ไหนก็ได้ด้วย ในขณะที่ร่างกฎหมายเดิมการจะเก็บข้อมูลจากแหล่งอื่นโดยไม่ขอความยินยอมนั้น ต้องเป็นการเก็บที่ได้รับการยกเว้นไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด

ประเด็นที่สิบเอ็ด : การเก็บข้อมูลที่มีเนื้อหาอ่อนไหวต้องขอความยินยอมก่อน แต่มีข้อยกเว้น

ร่างกฎหมายทั้งสองฉบับยังให้การคุ้มครองข้อมูลที่มีความอ่อนไหว อย่างเช่น พฤติกรรมทางเพศ ประวัติอาชญากรรม การกระทำผิดหรือการรับโทษ ประวัติสุขภาพ เชื้อชาติ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา โดยระบุอย่างชัดเจนว่าข้อมูลเหล่านี้ห้ามเก็บโดยเด็ดขาด แต่ทั้งสองร่างต่างก็มีข้อยกเว้นที่ใกล้เคียงกัน

ในร่างกฎหมายเดิม กำหนดว่า ถ้าเหตุผลการเก็บเป็นไปตามข้อยกเว้นที่ไม่ต้องขอความยินยอมก็สามารถเก็บได้ หรือ เพื่อ จุดประสงค์ทางการแพทย์และการรักษาพยาบาลที่เก็บข้อมูลเป็นความลับก็สามารถเก็บได้แต่ร่างกฎหมายใหม่ ซึ่ง**การเก็บข้อมูลตามปกติไม่ต้องขอความยินยอมอยู่แล้ว มีข้อยกเว้นให้สามารถเก็บข้อมูลที่อ่อนไหวได้โดยไม่ต้องขอความยินยอม และไม่ต้องแจ้งรายละเอียดการเก็บให้เจ้าของข้อมูลทราบด้วย** ในกรณีที่เป็นการเก็บเพื่อการสอบสวน การพิจารณาคดีของศาล เพื่อป้องกันอันตรายหรือสุขภาพของเจ้าของข้อมูล

ประเด็นที่สิบสอง : ข้อมูลที่ตอนเก็บไม่ต้องแจ้งให้ทราบ ตอนใช้ต้องทำบันทึกหมายเหตุและแจ้งเจ้าของข้อมูล

ในร่างกฎหมายเดิม กำหนดให้การใช้หรือเปิดเผยข้อมูลจะทำไม่ได้ หากไม่มีการแสดงความยินยอมเป็นหนังสือจากเจ้าของข้อมูลส่วนบุคคล ยกเว้น เป็นข้อมูลที่ใช้ได้โดยไม่ต้องขอความยินยอมตามที่กฎหมายกำหนด หรือ เพื่อประโยชน์ทางการแพทย์และการรักษาพยาบาล หรือ เปิดเผยต่อทนาย เพื่อการเรียกเก็บหนี้ หรือ ผู้ควบคุมข้อมูลที่บันทึกเป็นข้อมูลทางประวัติศาสาตร์ หรือ เหตุผลด้านความมั่นคง

แต่ในร่างกฎหมายใหม่ กำหนดแค่เพียงว่า **การใช้หรือเปิดเผยข้อมูลกรณีปกติต้องได้รับความยินยอมและใช้ตามวัตถุประสงค์ที่เก็บรวบรวม หากเป็นการใช้หรือเปิดเผยข้อมูลที่ได้รับการยกเว้นไม่ต้องแจ้งรายละเอียด ให้ทำบันทึกหมายเหตุการณ์ใช้และแจ้งให้เจ้าของข้อมูลทราบ**

ประเด็นที่สิบสาม : เปลี่ยนวัตถุประสงค์ของการดำเนินการใดเกี่ยวกับข้อมูลส่วนบุคคล ไม่ต้องขอความยินยอม แต่ต้องแจ้งให้เจ้าของข้อมูลทราบ

ในร่างกฎหมายใหม่ กำหนดให้การดำเนินการใดๆ เกี่ยวกับข้อมูลจะกระทำได้ต่อเมื่อเป็นไปตามวัตถุประสงค์ หากมีการเปลี่ยนแปลงวัตถุประสงค์ต้องแจ้งให้เจ้าของข้อมูลทราบ หรือ ของความยินยอมจากเจ้าของข้อมูล แต่ในร่างกฎหมายเดิม หากหากมีการเปลี่ยนแปลงวัตถุประสงค์ต้องแจ้งให้เจ้าของข้อมูลทราบ และ ของความยินยอมจากเจ้าของข้อมูล

ประเด็นที่สิบสี่ : ตัดหน้าที่พิเศษของผู้ควบคุมข้อมูลส่วนบุคคลในเชิงธุรกิจหรือการพาณิชย์

ในร่างกฎหมายเดิม มีนิยามความหมายของผู้ควบคุมข้อมูลส่วนบุคคลในเชิงธุรกิจหรือการพาณิชย์ และกำหนดหลักเกณฑ์ทั่วไปเกี่ยวกับการเก็บรวมรวบ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยต้องมีมาตรการคุ้มครองไม่น้อยกว่าที่กำหนดไว้ตามประมวลจริยธรรมที่คณะกรรมการกำหนด

นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลในเชิงธุรกิจหรือการพาณิชย์ ต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคล มีรายงานการดำเนินงานเพื่อคุ้มครองข้อมูลส่วนบุคคล มีการฝึกอบรมเจ้าหน้าที่ และหากมีการเลิกกิจการหรือควบรวมกิจการต้องแจ้งให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบด้วย ซึ่งร่างกฎหมายใหม่ได้ตัดเนื้อหาในส่วนนี้ออกไป

ประเด็นที่สิบห้า : เจ้าของข้อมูลมีมีสิทธิขอตรวจดูข้อมูลที่เกี่ยวกับตน แต่มีข้อยกเว้น

ตามร่างกฎหมายเดิม กำหนดให้เจ้าของข้อมูลมีสิทธิขอตรวจดูข้อมูลที่เกี่ยวกับตน และขอให้แจ้งถึงการมีอยู่ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตน และขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่เกี่ยวกับตนในกรณีที่เป็นข้อมูลซึ่งตนไม่ได้ให้ความยินยอม หากผู้ควบคุมข้อมูลจะปฏิเสธ ต้องเป็นการดำเนินการที่เสียค่าใช้จ่ายสูงมาก และเป็นข้อมูลส่วนบุคคลที่ปฏิเสธคำขอได้

แต่**ร่างกฎหมายใหม่ ตัดสิทธิเรื่อง การขอให้แจ้งถึงการมีอยู่ การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตน** และขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลที่เกี่ยวกับตนในกรณีที่เป็นข้อมูลซึ่งตนไม่ได้ให้ความยินยอม และกำหนดข้อยกเว้นให้ผู้ควบคุมข้อมูลสามารถปฏิเสธการตรวจดูข้อมูลได้ หาก ขัดแย้งต่อบทบัญญัติทางกฎหมาย คำสั่งศาล กระทบความมั่นคง กระทบเศรษฐกิจ หรือมีผลต่อการสืบสวน สอบสวน และเพื่อคุ้มครองสิทธิเสรีภาพของบุคคลอื่น

ประเด็นที่สิบหก : คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีอำนาจเต็ม ไม่มีไกล่เกลี่ย ไม่มีอุทธรณ์คำสั่ง

ตามร่างกฎหมายเดิม คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องแต่งตั้งคณะกรรมการตรวจสอบข้อมูลขึ้นมา ทำหน้าที่ในการพิจาณาเรื่องร้องเรียน ตรวจสอบการกระทำที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยคณะกรรมการตรวจสอบต้องมีความเชี่ยวชาญในแต่ละเรื่องและมีหลายคณะก็ได้

เมื่อได้รับเรื่องร้องเรียนและเห็นว่าผู้ควบคุมข้อมูลทำความผิดจริง คณะกรรมการตรวจสอบข้อมูล สามารถให้ผู้ควบคุมข้อมูลและเจ้าของข้อมูลไกล่เกลี่ยกัน หากไม่เป็นผลสำเร็จ คณะกรรมการตรวจสอบข้อมูล อาจสั่งให้ผู้ควบคุมข้อมูลแก้ไข เปลี่ยนแปลงให้ถูกต้อง และถ้าเกิดความเสียหายให้ผู้ควบคุมข้อมูลระงับความเสียหายนั้น หากคณะกรรมการตรวจสอบข้อมูลไม่รับเรื่องร้องเรียน สามารถยื่นอุทธรณ์โดยให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้วินิจฉัยก็ได้

ในร่างกฎหมายใหม่ เพิ่มอำนาจให้กับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่จะรับเรื่องร้องทุกข์ และมีอำนาจวินิจฉัยข้อพิพาท **ตัดกระบวนการไกล่เกลี่ยและกระบวนการอุทธรณ์คำสั่งออก ให้คณะกรรมการมีอำนาจสั่งให้บุคคลมาให้ข้อมูลหรือส่งเอกสารเมื่อมีการร้องเรียน** และ

เมื่อมีเหตุสงสัยว่าการดำเนินการใดๆ ก่อให้เกิดความเสียหายกับเจ้าของข้อมูลที่พิสูจน์ได้ว่าก่อให้เกิดความเสียหายจริง คณะกรรมการมีอำนาจสั่งห้ามดำเนินการใดๆ แก้ไขเปลี่ยนแปลง รวมถึงทำลายข้อมูลนั้น นอกจากนี้ **ในกรณีเร่งด่วนสามารถสั่งให้ผู้ควบคุมข้อมูลแก้ไขเปลี่ยนแปลง รวมถึงทำลายข้อมูลนั้น โดยไม่ต้องพิสูจน์ก็ได้**

ประเด็นที่สิบเจ็ด : ให้เจ้าหน้าที่มีอำนาจตรวจค้นสถานที่ ยึดหรืออายัดทรัพย์

ในร่างกฎหมายใหม่ ให้อำนาจเจ้าพนักงานในการตรวจสถานที่ที่มีการร้องเรียนโดยให้เจ้าของหรือผู้ครอบครองสถานที่ทราบล่วงหน้า และให้อำนาจในการยึด หรือ อายัดทรัพย์ เอกสารที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคล แต่ในร่างกฎหมายเดิม อำนาจในการยึดหรือ อายัดทรัพย์เป็นของคณะกรรมการตรวจสอบข้อมูล และไม่มีอำนาจค้นสถานที่

ประเด็นที่สิบแปด : เพิ่มโทษปรับหนักกว่า โดยไม่แยกประเภทผู้ควบคุมข้อมูล

ในร่างกฎหมายฉบับใหม่ เปลี่ยนโทษปรับกรณีไม่ปฏิบัติตามคำสั่งของคณะกรรมการ เป็นไม่เกิน 200,000 บาท และปรับรายวันอีกไม่เกินวันละ 5,000 บาท ขณะที่ตามร่างกฎหมายเดิมกำหนดให้การปรับนั้นเป็นโทษปรับทางปกครองมีโทษสูงสุดปรับไม่เกินห้าหมื่นบาท นอกจากนี้ ยังไม่มีการแยกกรณีผู้ควบคุมข้อมูลส่วนบุคคลเชิงธุรกิจหรือการพาณิชย์

ประเด็นที่สิบเก้า : เปิดเผยข้อมูลส่วนบุคคลแก่หน่วยงานรัฐในประเทศหรือต่างประเทศ ไม่เป็นความผิด

ในร่างกฎหมายฉบับใหม่ กำหนดว่า ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากปฏิบัติตามอำนาจหน้าที่ที่กำหนดในพระราชบัญญัตินี้ และนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือ ปรับไม่เกินสองหมื่นบาท **ยกเว้นว่า** (1) เป็นการกระทำตามหน้าที่ (2) เพื่อประโยชน์แก่การสืบสวน สอบสวน หรือการพิจารณาคดีของศาล (3) เพื่อประโยชน์ในการดำเนินความผิดตามกฎหมายนี้ (4) เพื่อประโยชน์ในการแก้ไขข้อมูล (5) **เปิดเผยแก่หน่วยงานของรัฐในประเทศหรือต่างประเทศที่เกี่ยวข้องกับเรื่องดังกล่าว** และ (6) ได้รับความเห็นชอบจากบุคคลดังกล่าวเป็นหนังสือ

สำหรับเนื้อหาของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดยกระทรวง ICT ซึ่งอยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกา มีจำนวน 50 มาตรา โดยมีหลักการและเหตุผล ตลอดจนแบ่งสาระสำคัญออกเป็น 6 หมวด และบทเฉพาะกาล ดังต่อไปนี้

บันทึกหลักการและเหตุผลประกอบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....ได้ระบุเหตุผลในการเสนอร่างกฎหมายฉบับนี้ไว้ได้แก่ *“โดยที่ความก้าวหน้าของเทคโนโลยีสารสนเทศรวมทั้งระบบสื่อสารทำให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย สะดวก และรวดเร็ว อันอาจนำมาซึ่งความเดือดร้อนรำคาญ หรือความเสียหายในกรณีที่มีการนำไปแสวงหาประโยชน์หรือเปิดเผยโดยไม่ได้รับความยินยอมหรือแจ้งล่วงหน้า ที่แม้ว่าจะได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง แต่ก็ยังไม่มีหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้”*

ร่างพระราชบัญญัติฉบับนี้ได้แบ่งเป็น 6 หมวด ได้แก่ หมวด 1 คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตั้งแต่ มาตรา 7 ถึง มาตรา 18 หมวด 2 การคุ้มครองข้อมูลส่วนบุคคล แบ่งเป็น ส่วนที่ 1 บททั่วไป (มาตรา 19-20) ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 21-25) ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 26-27) ส่วนที่ 4 สิทธิของเจ้าของข้อมูล (มาตรา 28-32) หมวด 3 ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ตั้งแต่มาตรา 33 ถึงมาตรา 35 หมวด 4 การร้องเรียน ตั้งแต่มาตรา 36 ถึง41 หมวด 5 ความรับผิดทางแพ่ง (มาตรา 42) หมวด 6 บทกำหนดโทษ ตั้งแต่มาตรา 43 ถึงมาตรา 46 และบทเฉพาะกาล (มาตรา47-50) สำหรับสาระสำคัญของร่างกฎหมายนี้มีประเด็นที่น่าสนใจซึ่งสามารถสรุปได้ดังนี้

1) ขอบเขตของการบังคับใช้กฎหมาย

ร่างกฎหมายฉบับนี้มีความพยายามทำให้เป็นกฎหมายกลางในการคุ้มครองข้อมูลส่วนบุคคลเว้นแต่จะมีกฎหมายอื่นกำหนดการคุ้มครองไว้เป็นการเฉพาะแต่ก็ต้องไม่มีหลักประกันต่ำกว่าที่กำหนดไว้ในร่างกฎหมายฉบับนี้ แต่ก็มีบทบัญญัติที่สามารถยกเว้นการบังคับใช้ได้ ดังปรากฏในร่างมาตรา 3และ4 ดังนี้

ร่างมาตรา 3 บุคคลย่อมได้รับการคุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดในพระราชบัญญัตินี้ เว้นแต่ในกรณีที่มีกฎหมายหรือกฎเกณฑ์ใดกำหนดหลักเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เรื่องใดเรื่องหนึ่งไว้เป็นการเฉพาะ และมีหลักประกันความเป็นธรรมและมาตรฐานไม่ต่ำกว่าที่กำหนดในพระราชบัญญัตินี้ ส่วนร่างมาตรา 4 กำหนดให้ พระราชบัญญัตินี้ให้ใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ผู้ควบคุมข้อมูลส่วนบุคคลในลักษณะหรือกิจกรรมใดที่มีพระราชกฤษฎีกากำหนดมิให้นำพระราชบัญญัตินี้ทั้งหมดหรือแต่บางส่วนมาใช้บังคับ

2) การกำหนดนิยามของข้อมูลส่วนบุคคล

ร่างกฎหมายนี้ได้นิยามความหมายของข้อมูลส่วนบุคคลไว้ในมาตรา 5 โดยระบุเพียงสั้นๆให้หมายความว่า “ข้อมูลเกี่ยวกับบุคลล ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม” ซึ่งนิยามนี้ไม่ได้มีการยกตัวอย่างและมีขอบเขตที่กว้างไม่ครอบคลุมถึงข้อมูลผู้ถึงแก่กรรมไปแล้ว

3) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ตามร่างมาตรา 7 ได้กำหนดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่ประกอบด้วยประธานกรรมการซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล หรือด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล ในส่วนกรรมการอื่นๆจะแบ่งเป็น

ก. กรรมการโดยตำแหน่งจำนวน 4 คน ได้แก่ ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงมหาดไทย และเลขาธิการสภาความมั่นคงแห่งชาติ

ข. กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกิน 4 คน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญด้านสังคมศาสตร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือด้านนิติศาสตร์ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล

ค. กรรมการและเลขานุการโดยตำแหน่ง คือเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

4) อำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เมื่อพิจารณาเปรียบเทียบอำนาจหน้าที่ของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลระหว่างร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลทั้งสองฉบับ จะพบว่าร่างของกระทรวงICT จะกำหนดอำนาจหน้าที่ไว้มากกว่าร่างของ สขร. ซึ่งมีเพียง 8 ข้อ โดยมีอำนาจหน้าที่ของคณะกรรมการถึง 14 ประการตามร่างมาตรา13 ดังต่อไปนี้

(1) จัดทำแผนยุทธศาสตร์การดำเนินงานด้านการส่งเสริม และการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องตามนโยบายและแผนระดับชาติที่เกี่ยวข้อง รวมทั้งเสนอมาตรการแก้ไขปัญหาอุปสรรคการปฏิบัติการตามนโยบายและแผนยุทธศาสตร์ดังกล่าว

(2) ส่งเสริมและสนับสนุนหน่วยงานของรัฐ ภาคเอกชน และภาคประชาชนดำเนินกิจกรรมตามนโยบายและแผนยุทธศาสตร์ตาม(1) รวมทั้งจัดให้มีการประเมินผลการดำเนินงานตามนโยบายและแผนยุทธศาสตร์ดังกล่าวเพื่อเสนอต่อคณะกรรมการ

(3) กำหนดมาตรการ หรือแนวทางการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

(4) ติดตามให้การคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัตินี้

(5) ให้เครื่องหมายรับรองข้อปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

(6) ออกประกาศหรือระเบียบเพื่อให้การดำเนินการเป็นไปตามพระราชบัญญัตินี้

(7) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราหรือปรับปรุงกฎหมายหรือกฎที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(8) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการดำเนินการใดๆเพื่อให้ความคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานทั้งภาครัฐและเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(9) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(10) ส่งเสริมและสนับสนุนการวิจัย เพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(11) กำกับและติดตามดูแลให้พนักงานเจ้าหน้าที่ หน่วยงานของรัฐ หรือผู้ควบคุมข้อมูลส่วน บุคคลปฏิบัติการตามอำนาจและหน้าที่ที่กฎหมายกำหนด

(12) พิจารณาคำร้องทุกข์ต่างๆ ของบุคคลที่เกี่ยวข้องตามพระราชบัญญัตินี้ รวมทั้งวินิจฉัยข้อพิพาทระหว่างบุคคลฝ่ายต่างๆที่เกี่ยวข้อง

(13) แต่งตั้งคณะอนุกรรมการคณะทำงานหรือพนักงานเจ้าหน้าที่เพื่อพิจารณาหรือปฏิบัติการอย่างหนึ่งอย่างใดตามที่คณะกรรมการมอบหมาย

(14) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามวัตถุประสงค์ของพระราชบัญญัตินี้

ทั้งนี้ในการปฏิบัติหน้าที่ตามมาตรานี้ของคณะกรรมการ อาจมอบหมายให้สำนักงานเป็นผู้ปฏิบัติการหรือเตรียมข้อเสนอมายังคณะกรรมการเพื่อพิจารณาดำเนินการต่อไปได้ อย่างไรก็ตามในร่างมาตรา 14 ได้บัญญัติให้คณะกรรมการข้อมูลข่าวสารของทางราชการมีอำนาจตามมาตรา 13(11) ถึง (13) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐที่อยู่ภายใต้กฎหมายว่าด้วยข้อมูลข่าวสารราชการ เว้นแต่รัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ

5) การคุ้มครองข้อมูลส่วนบุคคลที่กำหนดไว้ในร่างกฎหมาย

ในร่างพระราชบัญญัติฉบับนี้ได้กำหนดหลักการทั่วไปในการคุ้มครองข้อมูลส่วนบุคคลไว้ในหมวด 2 การคุ้มครองข้อมูลส่วนบุคคลตั้งแต่มาตรา 19 ถึง มาตรา 32 โดยแบ่งเป็น ส่วนที่ 1 บททั่วไป (มาตรา 19-20) ส่วนที่ 2 การเก็บรวบรวมข้อมูลส่วนบุคคล (มาตรา 21-25) ส่วนที่ 3 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล (มาตรา 26-27) ส่วนที่ 4 สิทธิของเจ้าของข้อมูล (มาตรา 28-32) การกำหนดข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ในหมวด 3 ตั้งแต่มาตรา 33 ถึงมาตรา 35 การกำหนดสิทธิในการร้องเรียนขอประชาชนตาม หมวด 4 การร้องเรียน ตั้งแต่มาตรา 36 ถึง41 นอกจากนี้หากมีการกระทำความผิดฝ่าฝืนกฎหมายที่บัญญัติไว้ก็จะมีความรับผิดทางแพ่งในหมวด 5 ความรับผิดทางแพ่ง (มาตรา 42) และบทกำหนดโทษตาม หมวด 6 บทกำหนดโทษ ตั้งแต่มาตรา 43 ถึงมาตรา 46 ซึ่งเมื่อพิจารณาจากหลักการคุ้มครองข้อมูลส่วนบุคคลในร่างพระราชบัญญัติฉบับนี้จะพบว่ามีปัญหาในหลายส่วนซึ่งแตกต่างไปจากร่างพระราชบัญญัติที่เสนอโดย สขร. ดังที่กล่าวมาตอนต้นในหัวข้อนี้แล้ว

หากกล่าวโดยสรุปถึงกระบวนการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยปัจจุบันได้เดินทางมาถึงทางแยกที่สำคัญ ซึ่งรัฐบาล สขร. และกระทรวงICTตลอดจนสภานิติบัญญัติแห่งชาติ จะต้องตัดสินใจในทางนโยบายเพื่อเลือกร่างกฎหมายที่เหมาะสมซึ่งจะตราขึ้นให้เป็นกฎหมายที่มีผลบังคับใช้อย่างสมบูรณ์ต่อไป ทั้งนี้ในการศึกษาวิเคราะห์เปรียบเทียบร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ที่เสนอโดยกระทรวง ICT และร่างที่เสนอโดยคณะรัฐมนตรีที่เป็นร่างดั่งเดิมที่ผ่านการพิจารณาปรับปรุงแก้ไขโดยคณะกรรมการกฤษฎีกา ในมุมมองของคณะที่ปรึกษาเห็นว่าร่างพระราชบัญญัติที่มีความเหมาะสมคือร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....ซึ่งเป็นร่างเดิมที่ผ่านการผลักดันมาหลายรัฐบาลท้ายที่สุดก็ได้เสนอเข้าสู่การพิจารณาของสภานิติบัญญัติแห่งชาติ เนื่องจากเป็นร่างที่ได้มีการศึกษาอย่างรอบคอบสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลในทางระหว่างประเทศ ขณะเดียวกันได้ช่วยทำให้เกิดความเป็นเอกภาพในระบบการคุ้มครองข้อมูลส่วนบุคคลทั้งในภาครัฐและภาคเอกชนที่จะอยู่ภายใต้การควบคุมดูแลของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเพียงองค์กรเดียว

บทที่ 4
กรณีศึกษาการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสิงคโปร์กับการนำมาปรับใช้ในประเทศไทย

ปัจจุบัน (พ.ศ. 2557)ประเทศไทยยังไม่มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่บังคับใช้กับข้อมูลส่วนบุคคลที่อยู่ในภาคเอกชนทั่วไป คงมีแต่พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่เป็นบทบัญญัติในการดูแลคุ้มครองข้อมูลข่าวสารส่วนบุคคลเฉพาะที่อยู่ในความควบคุมดูแลของหน่วยงานภาครัฐ ซึ่งในอนาคตอันใกล้นี้เป็นที่น่าเชื่อว่าจะมีการตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ขึ้นบังคับใช้ ซึ่งจะส่งผลให้มีกฎหมายที่ทำหน้าที่คุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในภาคเอกชน ความเปลี่ยนแปลงของกฎหมายฉบับนี้ย่อมส่งผลอย่างกว้างขวางในภาคเอกชนที่มีการดำเนินงานเก็บรวบรวมข้อมูลส่วนบุคคลและใช้ประโยชน์จากข้อมูลที่ต้องมีหน้าที่ปฏิบัติตามพระราชบัญญัติอย่างเคร่งครัด ทั้งนี้เรื่องดังกล่าวถือเป็นเรื่องใหม่อย่างมากสำหรับสังคมไทยซึ่งไม่เคยมีการกำหนดหลักเกณฑ์กลางในการดูแลคุ้มครองความมั่นคงปลอดภัยข้อมูลส่วนบุคคลในภาคเอกชน

ดังนั้น เพื่อเป็นการเตรียมความพร้อมก่อนการบังคับใช้กฎหมายข้อมูลส่วนบุคคลในประเทศไทย อีกทั้งในปี พ.ศ. 2558 ประเทศต่างๆในภูมิภาคเอเชียตะวันออกเฉียงใต้จะได้เข้าสู่การรวมตัวเป็นประชาคมอาเซียนอย่างสมบูรณ์ ซึ่งแน่นอนว่าประเด็นของการคุ้มครองข้อมูลส่วนบุคคลก็จะทวีความสำคัญมากยิ่งขึ้น หากกล่าวเจาะจงลงไปก็คือ “มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของกฎหมายแต่ละประเทศ” จะอยู่ในระดับเดียวกันหรือไม่ซึ่งจะส่งผลไปยังการส่งข้อมูลส่วนบุคคลไปยังประเทศอื่นในประชาคมอาเซียนจะสามารถกระทำได้ตามบทกฎหมายของประเทศนั้นๆได้หรือไม่เพราะหลักการสำคัญในทางระหว่างประเทศในเรื่องการส่งข้อมูลส่วนบุคคลไปยังประเทศอื่นนั้น ต้องมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลไม่ต่ำกว่าที่กำหนดไว้ในกฎหมายของประเทศต้นทาง

เนื่องจากการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิกอาเซียนที่ได้นำเสนอในรายงานวิจัยฉบับนี้ล้วนแต่มีประสบการณ์การบังคับใช้มาก่อนประเทศไทยหลายปีจึงเป็นเรื่องที่สมควรในการศึกษาประสบการณ์การปฏิบัติตามกฎหมายของหน่วยงานรัฐเพื่อนำมาประยุกต์ใช้กับประเทศไทย ซึ่งในการศึกษาเปรียบเทียบทั้งสี่ประเทศได้แก่ อินโดนีเซีย ฟิลิปปินส์ มาเลเซียและสิงคโปร์ คณะผู้ศึกษาเห็นว่าประเทศที่สามารถถือว่าเป็นตัวอย่างกรณีศึกษาที่ดีในการนำประสบการณ์มาเป็นบทเรียนในการเตรียมความพร้อมสำหรับการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในอนาคต คือ ประเทศสิงคโปร์ ด้วยเหตุที่มีการวางระบบกลไกการบังคับใช้กฎหมาย การเตรียมความพร้อมให้กับหน่วยงานเอกชนที่ต้องปฏิบัติตามกฎหมาย และการให้ความรู้แก่ประชาชนเกี่ยวกับสิทธิที่ได้รับการคุ้มครองตามกฎหมายเป็นอย่างดี ขณะเดียวกันในมุมมองของบริษัทต่างชาติที่ดำเนินธุรกิจในประเทศต่างๆในภูมิภาคอาเซียนซึ่งคณะผู้ศึกษาได้สัมภาษณ์ ก็มองว่าประเทศสิงคโปร์เป็นตัวอย่างที่ดีในการออกแบบกฎหมายและประสบความสำเร็จในก้าวแรกของการบังคับใช้

ดังนั้น เพื่อให้ได้ข้อมูลเกี่ยวกับการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ในทางการดำเนินงานของหน่วยงานรัฐที่ดูแล คณะผู้ศึกษาพร้อมคณะเจ้าหน้าที่ของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการประกอบด้วยผู้อำนวยการและหัวหน้าฝ่ายต่าง ๆของสำนักงาน นำโดยรองปลัดสำนักนายกรัฐมนตรี (นายกมล สุขสมบูรณ์) ได้เดินทางไปศึกษาดูงานและรับฟังการบรรยายสรุปจาก สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Commission Singapore) ระหว่างวันที่ 25 -27 กันยายน 2557 โดยมีโอกาสได้พบปะแลกเปลี่ยนพูดคุยกับกรรมการคุ้มครองข้อมูลส่วนบุคคลท่านหนึ่ง คือ Ms Aileen Chia ตลอดจนผู้บริหารของสำนักงานท่านอื่นๆ ได้แก่ ผู้อำนวยการ รองผู้อำนวยการ ผู้จัดการฝ่ายบริหารของสำนักงานซึ่งได้รับข้อมูลที่เป็นประโยชน์อย่างยิ่ง สำหรับรายละเอียดผลการศึกษาดูงานในแต่ละประเด็นที่น่าสนใจในการนำมาปรับใช้กับประเทศไทยมีดังต่อไปนี้

4.1 ข้อมูลพื้นฐานเกี่ยวกับสำนักงานคณะกรรมคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Commission Singapore) เป็นหน่วยงานของรัฐอยู่ภายใต้สังกัดกระทรวงการสื่อสารและข้อมูลข่าวสาร จัดตั้งขึ้นโดย Personal Data Protection Act 2012 ซึ่งได้เริ่มดำเนินการอย่างเป็นทางการในการแต่งตั้งคณะกรรมการและจัดตั้งสำนักงานเมื่อ 2 มกราคม ค.ศ.2013 มีพันธกิจสำคัญของคณะกรรมการที่ปรากฏในรายงานประจำปี 2013/2014 ว่า “การส่งเสริมและบังคับใช้การคุ้มครองข้อมูลส่วนบุคคล โดยดูแลสภาพแวดล้อมให้เกิดความไว้วางใจทั้งภาคธุรกิจและผู้บริโภค เพื่อนำไปสู่การมีส่วนร่วมในการสร้างความเติบโตให้กับเศรษฐกิจของสิงคโปร์”

ปัจจุบัน(พ.ศ. 2557/ค.ศ.2014)นับแต่กฎหมายนี้ประกาศใช้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์มีทั้งหมด 5 ท่าน ซึ่งตามกฎหมายPDPA มาตรา 5 กำหนดให้รัฐมนตรีกระทรวงการสื่อสารและข้อมูลข่าวสารเป็นผู้แต่งตั้งโดยกำหนดจำนวนน้อยที่สุด คือ 3 คน และมากที่สุดห้ามเกิน 17 คน โดยรายชื่อกรรมการทั้ง 5 ท่านในชุดปัจจุบัน มีดังนี้

1. **ประธานกรรมการ** คือ Mr.Leong Keng Thai ซึ่งดำรงตำแหน่ง Deputy Chief Excutive and Director-General (Telecoms and Post), Infocomm Development Authority of Singpore

กรรมการอีก 4 ท่าน ได้แก่

2. Ms.Aileen Chia ซึ่งดำรงตำแหน่ง Assistant Chief Excutive and Director-General (Telecoms and Post), Infocomm Development Authority of Singpore

3. Mr. Ong Tong San ซึ่งดำรงตำแหน่ง Cluster Director (Competition and Resource Development), Infocomm Development Authority of Singpore

4. Mr. Amos Tan ซึ่งดำรงตำแหน่ง Director (Strategy and Innovation), Infocomm Development Authority of Singpore

5. Ms. Koh Li-Na ซึ่งดำรงตำแหน่ง Assistant Chief Excutive, Early Childhood Development Agency

นอกเหนือจากคณะกรรมการ PDPC ข้างต้น ในกฎหมายPDPA มาตรา 7 ยังกำหนดให้รัฐมนตรีสามารถแต่งตั้งคณะกรรมการที่ปรึกษาเพื่อทำหน้าที่เป็นที่ปรึกษาของคณะกรรมการPDPC และปฏิบัติหน้าที่อื่นตามที่กฎหมายกำหนด ซึ่งจะมีหนึ่งคนหรือหลายคนก็ได้ โดยในปัจจุบันได้มีการแต่งตั้งทั้งหมด 8 คน ดังนี้

1. ประธานกรรมการ คือ Ms.Liew Woon Yin (Director ,Abundanti)

กรรมการที่ปรึกษาอีก 7 ท่าน ได้แก่

2. Mr. Tan Kai Hoe (Chief Executive Officer, SPRING Singapore)

3. Mr.Ho Meng Kit (Chief Executive Officer, Singapore Business Federation)

4. Mr. Arun Mahizhnan (Special Research Adviser at the Institute of Policy Studies)

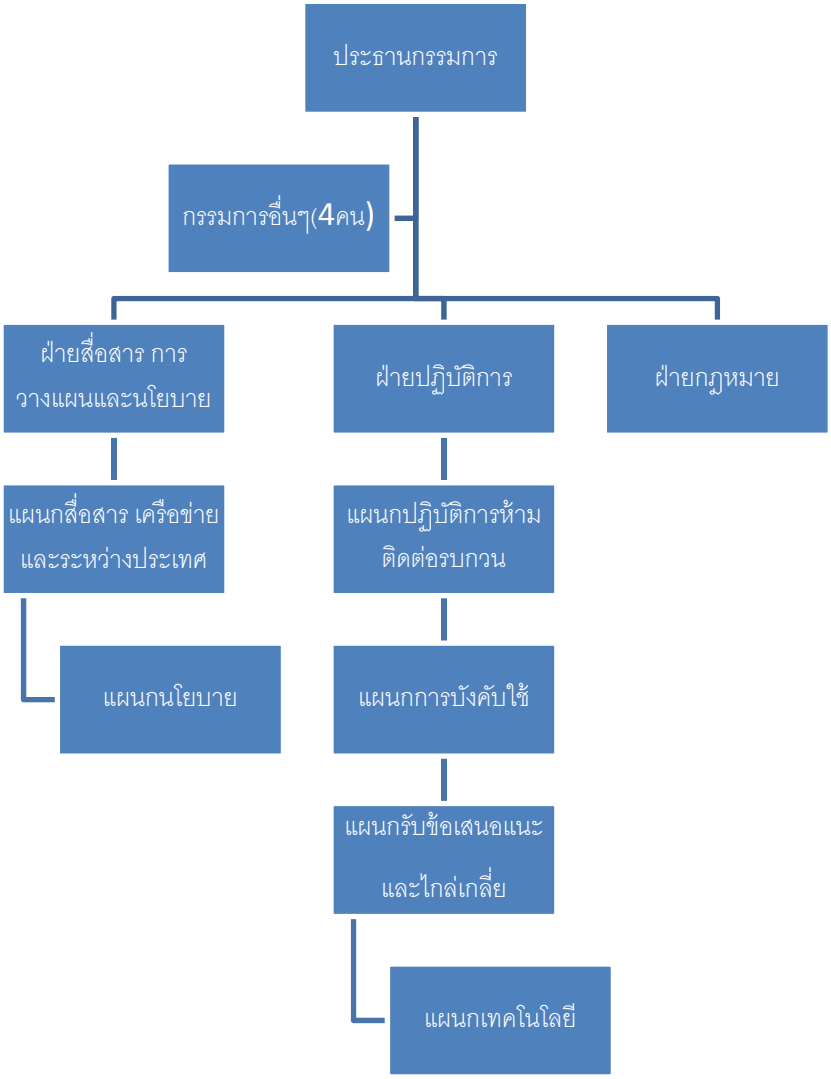
5. Mr.Lim Biow Chuan (President .Consumers Association of Singapore)

6. Ms.Hoo Sheau Peng (Deputy Chief Counsel(Advisory and Administration), Civil Division, Attorney General'sChambers)

7. Professor Simon Chesterman (Dean and Professor of Law, National University of Singapore)

8. Mr. Lim Chin Hu (Managing Partner, Stream Global Pte Ltd)

การดูแลการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของคณะกรรมการPDPCนั้น คือการทำหน้าที่รักษาสมดุลระหว่างความต้องการในการปกป้องความเป็นส่วนตัวของบุคคล และความต้องการขององค์กรในการใช้ข้อมูลเพื่อวัตถุประสงค์ที่ชอบด้วยกฎหมาย ซึ่งคณะกรรมการจะต้องเป็นผู้นำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไปปฏิบัติ รวมถึงการพัฒนาข้อกำหนด แนวทางการให้คำปรึกษาเพื่อช่วยเหลือให้องค์กรมีความเข้าใจและปฏิบัติตามกฎหมาย PDPA ได้อย่างถูกต้อง นอกเหนือจากการออกกฎระเบียบในการคุ้มครองข้อมูลของคณะกรรมการแล้ว คณะกรรมการยังทำหน้าที่ให้สาธารณทั่วไปและภาคส่วนที่เจาะจงได้เกิดความรู้ และมีกิจกรรมที่จะช่วยให้องค์กรนำการปฏิบัติของการคุ้มครองข้อมูลส่วนบุคคลที่ดีมาใช้ และดูแลให้แต่ละบุคคลทราบว่าจะทำอย่างไรในการปกป้องการใช้ข้อมูลที่ผิด ซึ่งการดำเนินงานตามกฎหมายของคณะกรรมการและสำนักงานนั้นจะแบ่งภาระงานออกเป็นสองด้านใหญ่ คือ 1.ด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection) และ 2. ด้านการห้ามติดต่อรบกวน (Do Not Call) ซึ่งครอบคลุมถึง การโทรด้วยเสียง SMS MMS Texts และ Faxes ที่ส่งไปยังหมายเลขโทรศัพท์ในสิงคโปร์ ทั้งนี้จำนวนบุคลากรของสำนักงานปัจจุบันมีประมาณ 40 คน ในส่วนโครงสร้างของการจัดองค์กรของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์เป็นดังนี้



4.2 การเตรียมความพร้อมก่อนการบังคับใช้กฎหมายของสิงคโปร์

แม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Act 2012 จะได้ประกาศใช้ตั้งแต่วันที่ 7 ธันวาคม 2012 แต่การมีผลบังคับใช้กฎหมายทุกบทบัญญัติก็ยังไม่เกิดขึ้นทันที กฎหมายฉบับนี้เพิ่งมีผลบังคับใช้อย่างสมบูรณ์เมื่อวันที่ 2 กรกฎาคม 2014 ที่ผ่านมา ซึ่งจะเห็นได้ว่าระยะเวลาที่หน่วยงานรัฐของสิงคโปร์ได้ใช้เตรียมพร้อมกินเวลานานถึง 18 เดือน ทั้งนี้การใช้เวลานานเช่นนี้มักจะไม่พบในการประกาศใช้กฎหมายของประเทศไทย เพราะที่ผ่านมาระยะเวลาที่พบส่วนใหญ่ก็ประมาณ 90 วัน หรือสามเดือน ซึ่งการให้เวลาเตรียมพร้อมนานขนาดนี้เหตุผลสำคัญของกฎหมาย เห็นว่าเรื่องนี้เป็นเรื่องใหม่ที่กระทบกับองค์กรธุรกิจจำนวนมาก ไม่ใช่เพียงที่ตั้งอยู่ประเทศสิงคโปร์เท่านั้น แต่รวมถึงบริษัทต่างชาติอื่นๆที่อยู่ในต่างประเทศที่อาจมีการส่งต่อข้อมูลจากสิงคโปร์ไปยังประเทศที่สาม ก็ต้องปฏิบัติตามมาตรการของกฎหมายPDPA ด้วย

สำหรับการดำเนินงานในช่วงเตรียมความพร้อมของสำนักงาน PDPC นั้นมีกิจกรรมที่น่าสนใจที่ปรากฏในรายงานประจำปีของสำนักงานที่รายงานไว้ ได้แก่

เดือนมกราคม 2013

เป็นช่วงเวลาของการแต่งตั้งคณะกรรมการตามกฎหมาย เมื่อวันที่ 2 มกราคม พ.ศ. 2556 และก่อตั้งสำนักงานคณะกรรมการ มีการสร้างเว็บไซต์เพื่อเผยแพร่ข้อมูลกฎหมายให้กับประชาชนและองค์กรต่าง ๆ

เดือนพฤษภาคม 2013

สำนักงานได้จัดให้มีการสัมมนาคณะกรรมการในการเริ่มเปิดตัวอย่างเป็นทางการในการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย โดยเน้นไปยังมุมมองระดับโลกและภายในประเทศเกี่ยวกับการดำเนินงานคุ้มครองข้อมูลส่วนบุคคล

เดือนมิถุนายน 2013

มีการประชุมเชิงปฏิบัติการสำหรับเจ้าหน้าที่ของสำนักงานทุกคนเพื่อให้มีความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ประกาศใช้ให้ตรงกันโดยเฉพาะบทบาทอำนาจหน้าที่ของสำนักงาน การให้บริการแก่ประชาชน และข้อมูลที่ประชาชนควรรู้ในการปกป้องสิทธิของตน

เดือนกันยายน 2013

คณะกรรมการได้มีการออกแนวทางในการให้คำปรึกษากลุ่มแรกเกี่ยวกับความมุ่งหมายของกฎหมาย และหัวข้อสำคัญในการปฏิบัติตามกฎหมายที่ใช้เก็บข้อมูลที่เป็นความลับ การจ้างงาน และกิจกรรมผ่านเครือข่ายออนไลน์ นอกจากนี้คณะกรรมการยังได้ออกกฎสำหรับองค์กรธุรกิจในการปฏิบัติตามกฎหมายเรื่องห้ามโทรรบกวนบุคคล เพื่อช่วยเหลือให้องค์กรสามารถปฏิบัติได้อย่างถูกต้องโดยเฉพาะกระบวนการที่เกี่ยวข้องกับการขายทางไกล (Telemarketing Processes)

เดือนธันวาคม 2013

เริ่มต้นเปิดให้ลงทะเบียนตามบทบัญญัติกฎหมายในเรื่องการห้ามโทรรบกวน (Do Not Call Registry) สำหรับประชาชนทั่วไป ซึ่งทางสำนักงานก็ดำเนินงานสร้างบัญชี และสถานะเพื่อการตรวจสอบ

เดือนมกราคม 2014

สำนักงานได้จัดให้มีการประชุมอย่างเป็นทางการเกี่ยวกับการลงทะเบียนการห้ามโทรรบกวน ซึ่งในวันที่ 2 มกราคม 2014 บทบัญญัติในส่วน Do Not Call (DNC)ของกฎหมายมีผลบังคับใช้

เดือนกุมภาพันธ์ 2014

สำนักงานได้มีการให้คำปรึกษาแก่สาธารณะในแนวทางข้อกำหนดที่ออกโดยคณะกรรมการซึ่งเป็นกลุ่มแรกขององค์กรธุรกิจที่ต้องปฏิบัติตามกฎหมายให้ถูกต้องในกลุ่มอสังหาริมทรัพย์ และโทรคมนาคม

เดือนกรกฎาคม 2014

บทกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์มีผลบังคับใช้ทุกบทบัญญัติ

เมื่อพิจารณาถึงการเตรียมพร้อมก่อนการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยสำนักงานและคณะกรรมการPDPC ข้างต้นจะเห็นได้ว่ามีการให้ความสำคัญอย่างมาก แม้ในปัจจุบันที่กฎหมายมีผลบังคับใช้ในทุกบทบัญญัติแล้ว งานในการให้ความรู้แก่ประชาชนและองค์กรเอกชนที่ต้องปฏิบัติตามกฎหมาย ยังคงดำเนินงานอย่างต่อเนื่อง ซึ่งข้อมูลส่วนนี้จะเห็นได้จากเนื้อหาภายในเว็บไซต์ของสำนักงานที่สามารถเข้าไปเยี่ยมชมได้ที่ www.pdpc.gov.sg โดยจะมีทั้งเอกสารเผยแพร่ให้คำแนะนำปรึกษาต่างๆ ข้อมูลแนวทางการปฏิบัติตามกฎหมาย ซึ่งเอกสารเหล่านี้จะมีการจัดทำทั้งในรูปที่เป็นทางการ หนังสือการ์ตูน แผ่นพับ รวมถึงหลักสูตรการเรียนรู้ผ่านระบบe-learning นอกจากนี้ยังมีการจัดประชุมสัมมนาเป็นครั้งคราว รวมถึงการประชุมในลักษณะฝึกอบรมเชิงปฏิบัติในหัวข้อการปฏิบัติให้ถูกต้องตามกฎหมายแก่องค์กรธุรกิจอีกด้วย

ข้อมูลการจัดกิจกรรมในช่วงการเตรียมความพร้อมของการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในสิงคโปร์มีความน่าสนใจหลายประการ ไม่ว่าจะเป็นการจัดสัมมนาในการสถาปนาคณะกรรมการในช่วงแรกของการจัดตั้งคณะกรรมการเมื่อวันที่ 15 พฤษภาคม 2013 ที่มีผู้เข้าร่วมทั้งจากต่างประเทศกว่า 400 คนและผู้ที่ได้รับเชิญภายในประเทศอีกจำนวนมาก ทั้งภาคธุรกิจ นักวิชาการ เพื่อแลกเปลี่ยนมุมมองทางกฎหมายและการปฏิบัติในทางระหว่างประเทศ ประเทศอื่นและภายในสิงคโปร์เอง โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์และเจ้าหน้าที่ก็ได้เข้าร่วมประชุมครั้งนี้ด้วย ซึ่งถือว่าการจัดประชุมเช่นนี้จะเป็นการสัมมนาวิชาการประจำปีที่สำนักงาน PDPC จะได้จัดต่อเนื่องเป็นประจำทุกปี

หัวข้อที่เป็นประเด็นหลักในการสัมมนาครั้งนี้ได้ตั้งไว้อย่างน่าสนใจคือ “Data Protection Trends, Challenges and Benefits for Business Today” (แนวโน้มการคุ้มครองข้อมูล ความท้าทาย และ ประโยชน์สำหรับ ธุรกิจในปัจจุบัน) ซึ่งได้มีการเชิญองค์ปาฐก จากคณะกรรมการความเป็นส่วนตัวของออสเตรเลีย (Australia’s Privacy Commissioner) Mr.Timothy Pilgrim ที่เป็นผู้นำเสนอมุมมองการคุ้มครองข้อมูลส่วนบุคคลในระดับโลก และการจะทำอย่างไรให้การคุ้มครองข้อมูลส่วนบุคคลที่ดีสามารถไปได้ด้วยกันกับธุรกิจ ซึ่งจะสร้างความไว้วางใจแก่ผู้บริโภคให้เกิดขึ้น ซึ่งผู้เข้าร่วมฟังปาฐกถาครั้งนี้ทางคณะกรรมการได้เชิญตัวแทนผู้ประกอบการอุตสาหกรรม เช่น Microsoft Singapore สมาคมผู้ประกอบการธุรกิจขายตรง(The Direct Marketing Association of Singapore) มาร่วมแลกเปลี่ยนประสบการณ์ด้วย

4.3 การสร้างเครือข่ายความร่วมมือกับกลุ่มองค์กรทางการค้าและอุตสาหกรรม

เพื่อให้เกิดความสำเร็จในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ ทางคณะกรรมการ PDPC ได้ขยายหุ้นส่วนความร่วมมือไปยังสมาคมทางการค้าและองค์กรภายนอก รวมแล้วมากถึง 57 สมาคม ซึ่งมีสมาชิกของแต่ละองค์กรดังกล่าวประมาณ 27,000 องค์กร เพื่อสร้างความเข้าใจที่ถูกต้องให้เกิดขึ้นในการปฏิบัติตามกฎหมายที่ได้ประกาศใช้ใหม่และเกิดความตระหนักใน

ความจำเป็นของการคุ้มครองข้อมูลส่วนบุคคล ซึ่งได้มีการประชุมระหว่างองค์กรต่างๆไปถึงสองรอบก่อนการบังคับใช้กฎหมายในเดือนกุมภาพันธ์ 2012

สำหรับรายชื่อกลุ่มองค์กรที่ได้เข้าร่วมเป็นเครือข่ายกับคณะกรรมการข้อมูลส่วนบุคคลของสิงคโปร์มีหลายองค์กร อาทิเช่น The Association of Banks in Singapore ,Singapore Business Federation , Life Insurance Association, Singapore Association Estate Agencies, Direct Marketing Association of Singapore , Singapore Retailers Association และ Singpore Medical Association

นอกจากความร่วมมือที่เกิดกับสมาคมองค์กรธุรกิจข้างต้น คณะกรรมการPDPC ได้เห็นความสำคัญในการสร้างความเข้าใจให้เกิดขึ้นกับธุรกิจขนาดกลางและขนาดย่อม (SME) ซึ่งมีข้อจำกัดในการปฏิบัติตามกฎหมายเมื่อเทียบกับธุรกิจขนาดใหญ่ที่มีความพร้อมมากกว่า จึงได้ร่วมมือกับ SPRING Singapore ที่เป็นหน่วยงานในกระทรวงอุตสาหกรรมและการค้าที่ดูแลธุรกิจ SME ทำหน้าที่เป็นคลินิกช่วยให้คำปรึกษาการปฏิบัติตามกฎหมายอีกทางหนึ่ง

ตัวอย่างการสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานรัฐและสมาคมทางธุรกิจต่างๆของประเทศสิงคโปร์นับเป็นตัวอย่างที่ประเทศไทยจำเป็นต้องเรียนรู้และสร้างให้เกิดขึ้นในการเตรียมความพร้อมสร้างความเข้าใจให้เกิดขึ้นสำหรับภาคเอกชนก่อนการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย ซึ่งสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการก็น่าจะนำมาใช้ในการสร้างความเข้าใจให้เกิดขึ้นในภาคเอกชนของไทย ที่มีขนาดจำนวนบริษัทและองค์กรธุรกิจมากกว่าสิงคโปร์ที่น่าจะเกิดผลกระทบวงกว้างในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลหากมีการประกาศใช้ในอนาคต

4.4 การเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายไปยังประชาชนและองค์กรเอกชน

การดำเนินงานดังกล่าวสำหรับการประกาศใช้กฎหมายใหม่ ซึ่งมีผลกระทบในการปฏิบัติขององค์กรเอกชนในการทำหน้าที่ตามที่กฎหมายกำหนด และการให้ประชาชนได้รับรู้ถึงสิทธิต่างๆที่ได้รับการคุ้มครองตามกฎหมายในเรื่องข้อมูลส่วนบุคคล นับว่าเป็นเรื่องที่สำคัญอย่างยิ่งต่อความสำเร็จในการบังคับใช้กฎหมายฉบับนี้ ซึ่งทางสำนักงาน PDPC ก็ได้ให้ความสำคัญเป็นอย่างมาก โดยมีตัวเลขข้อมูลระหว่างเดือนกรกฎาคม 2013 ถึงเดือนมีนาคม 2014 มีพนักงานบริษัทด้านการดูแลข้อมูลส่วนบุคคลมากกว่า 2,000 คนได้ผ่านการฝึกอบรมเชิงปฏิบัติการ ขณะเดียวกันก็มีองค์กรถึง2,000 แห่ง ได้เข้าร่วมรับฟังการบรรยายสรุปและสัมมนาเกี่ยวกับการปฏิบัติตามกฎหมายนี้ มีจำนวนผู้เข้าร่วมสัมมนารวมทั้งหมดมากกว่า 11,000 คน ทั้งนี้ผลของการสัมมนาได้รับการต้อนรับเป็นอย่างดีจากผู้ที่เข้าร่วม

การสัมมนาในครั้งแรกๆที่ได้จัดขึ้นของสำนักงานมีเนื้อหามุ่งเน้นไปยังการสร้างความรู้ความเข้าใจในเชิงลึกเกี่ยวกับการปฏิบัติตามกฎหมายที่ถูกต้อง การพัฒนาแผนปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องของตัวองค์กรธุรกิจที่เข้าร่วม

ในส่วนการให้ความรู้แก่ผู้บริโภคที่เป็นประชาชนทั่วไปทางสำนักงานPDPC ก็ได้ให้ความสำคัญไม่แพ้กันโดยได้ร่วมมือกับสมาคมผู้บริโภคของสิงคโปร์ (The Consumers Association of Singapore :CASE) the Infocomm Development Authority of Singapore และ The National Library Board Singapore เพื่อจัดชุดกิจกรรมที่เผยแพร่แก่สาธารณะ โดยในวันสิทธิผู้บริโภคโลก ที่จัดในเดือนมีนาคม 2014 โดย CASE ทางคณะกรรมการก็ได้สนับสนุนในการจัดนิทรรศการและเผยแพร่เอกสารความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีผู้เข้าร่วมงานถึง2,000 คน ซึ่งนิทรรศการนี้ก็สามารถนำไปจัดที่สถานศึกษาและที่ชุมชนต่างๆได้ ขณะเดียวกันคณะกรรการ PDPC ก็ได้ผลิตเอกสารความรู้ในรูปแบบต่างๆในการเรียนรู้กฎหมายด้วยตนเองไม่ว่าจะเป็นเอกสารแนะนำ ภาพเคลื่อนไหว (Video Clips) ถึง 4 ภาษา ซึ่งประชาชนสามารถเข้าถึงได้จากเว็บไซต์สำนักงาน โดยตั้งแต่เดือนมีนาคม2014 มีผู้เข้าชมเว็บไซต์มากกว่า 350,000 ครั้ง ซึ่งในประเด็นนี้หากย้อนกลับมาดูการสร้างความตื่นตัวและความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยก็ไม่ปรากฏชัดเจนถึงการดำเนินงานอย่างเป็นระบบโดยหน่วยงานรัฐแม้แต่การปฏิบัติในส่วนของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการที่เป็นอยู่ปัจจุบันก็ตาม

สำหรับตัวอย่างเอกสารเผยแพร่ที่สำนักงาน PDPC ได้จัดทำเผยแพร่แก่ประชาชนทั่วไปนั้น ทางสำนักงานได้มีการพิจารณาถึงกลุ่มเป้าหมายและเนื้อหาที่มีความสำคัญซึ่งต้องมีการเผยแพร่เพื่อให้บรรลุวัตถุประสงค์ในการเสริมสร้างความรู้ความเข้าใจที่ถูกต้องตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์กำหนดไว้ ซึ่งเอกสารดังกล่าวจะแบ่งออกเป็นสองกลุ่มหลักๆ คือ

กลุ่มที่ 1 เอกสารที่เผยแพร่ให้กับประชาชนทั่วไป เช่น Your Personal Data , Your Choice A quick guide to the Personal Data Protection Act for individuals, Registering with the Do Not Call Registry

กลุ่มที่ 2 เอกสารที่เผยแพร่ให้กับกลุ่มผู้ประกอบการธุรกิจเอกชน เช่น WHEN BUSINESS GETS PERSONAL: A QUICK GUIDE TO THE PERSONAL DATA PROTECTION ACT 2012 FOR ORGANISATIONS

นอกเหนือจากการจัดทำเอกสารเผยแพร่ประชาสัมพันธ์ต่างๆข้างต้นของสำนักงาน PDPC แล้ว ทางสำนักงานยังได้จัดให้โครงการฝึกอบรมหลักสูตรให้ความรู้แก่ผู้ประกอบการในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในเรื่องต่างๆทั้งหลักสูตรทั่วไปและหลักสูตรเฉพาะเรื่อง อาทิเช่น การอบรมหลักสูตรความรู้เบื้องต้นเกี่ยวกับกฎหมายเป็นเวลา 2 วัน ในเรื่อง An Introduction to the Fundamentals of the Personal Data Protection Act (PDPA) for Non – Legal Personnel ซึ่งหลักสูตรดังกล่าวจะมีการฝึกอบรมในเรื่องที่สำคัญ แบ่งเป็นสองส่วน คือ ส่วนแรก เป็นข้อความคิดพื้นฐานและหน้าที่ของ PAPA ส่วนที่สอง คือ ข้อแนะนำและกระบวนการปฏิบัติสำหรับองค์กรที่ถูกต้อง และเมื่ออบรมครบตามหลักสูตรก็จะได้รับประกาศนียบัตรรับรองว่าเป็นผู้ผ่านการฝึกอบรม

ทั้งนี้ทางสำนักงาน PDPC ยังได้สร้างช่องทางการให้ความช่วยเหลือผ่านการแนะนำ การให้คำปรึกษาต่างๆจากเจ้าหน้าที่ของสำนักงาน แก่ประชาชนทั่วไปและบริษัทเอกชนที่เป็นผู้ประกอบการทั้งรายใหญ่และ SMEs ไม่ว่าจะเป็นเว็บไซต์ของสำนักงาน ทางโทรศัพท์ ทางอีเมล์

ขณะเดียวกันในส่วนของผู้ประกอบการขนาดกลางและขนาดเล็กทางสำนักงาน PDPC ยังได้สร้างความร่วมมือกับ องค์กรภายนอกที่เป็นสมาคมของผู้ประกอบการต่างๆจัดตั้งแผนกคลินิกให้คำปรึกษาในเรื่องการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ซึ่งสามารถขอคำปรึกษาได้โดยตรงอีกด้วย

จากตัวอย่างการดำเนินงานตามภารกิจของสำนักงาน PDPC ที่นำเสนอมาข้างต้น จะเห็นได้ว่าบทบาทของสำนักงานนี้มีส่วนอย่างสำคัญในการผลักดันให้การบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์สามารถบรรลุวัตถุประสงค์ของกฎหมายได้ โดยการดำเนินงานของสำนักงานมีบทบาทนับแต่ขั้นตอนการเตรียมการเพื่อสร้างการรับรู้ของประชาชนและภาคธุรกิจก่อนที่กฎหมายจะมีผลบังคับใช้อย่างสมบูรณ์ และแม้ภายหลังจากกฎหมายได้มีผลบังคับแล้วก็ยังมีบทบาทอย่างต่อเนื่องในการขับเคลื่อนการบังคับใช้กฎหมาย ทั้งในส่วนเป็นเจ้าหน้าที่ผู้ต้องปฏิบัติหน้าที่ตามกฎหมายในการบังคับใช้กับภาคเอกชน การเป็นผู้ให้คำปรึกษา การจัดฝึกอบรมเผยแพร่ความรู้ความเข้าใจในการปฏิบัติที่ถูกต้อง นอกจากนี้สำนักงานยังทำหน้าที่ด้านวิชาการเพื่อพัฒนาการบังคับใช้กฎหมาย ดังจะเห็นจากการจัดให้มีการประชุมวิชาการนานาชาติประจำปีอีกด้วย

ดังนั้น คณะผู้ศึกษาจึงเห็นว่า การประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยในอนาคต มีความจำเป็นที่ต้องเตรียมการวางแผนในกิจกรรมต่างๆที่จะเข้ามาช่วยส่งเสริมและสนับสนุนให้เกิดความรู้ความเข้าใจที่ถูกต้องในการปฏิบัติตามกฎหมายอย่างมาก ทั้งในส่วนภาคเอกชนที่มีหน้าที่ต้องปฏิบัติตามกฎหมาย ตลอดจนการสร้างความตระหนักรับรู้ถึงการคุ้มครองสิทธิในข้อมูลส่วนบุคคลของประชาชนทั่วไป ซึ่งงานทั้งหลายเหล่านี้นับเป็นภารกิจที่ท้าทายเป็นอย่างมาก อย่างไรก็ตามเราสามารถเรียนรู้จากประสบการณ์ของสำนักงาน PDPC ของสิงคโปร์เพื่อนำไปใช้กำหนดแนวทางการดำเนินงานที่เหมาะสมกับประเทศไทยต่อไปได้ ขณะเดียวกันก็มีความจำเป็นอย่างยิ่งที่ประเทศไทยและประเทศต่างๆในภูมิภาคอาเซียนต้องแลกเปลี่ยนเรียนรู้ในเรื่องกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศเพื่อเอื้ออำนวยให้สิทธิในข้อมูลส่วนบุคคลของประชาชนได้รับการดูแลปกป้องอย่างเต็มที่ และรวมถึงยังจะช่วยส่งเสริมให้กิจกรรมทางเศรษฐกิจที่มีการติดต่อระหว่างกันเจริญเติบโตก้าวหน้ามากยิ่งขึ้น

บทที่ 5
ข้อเสนอแนะในการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยและการเตรียมความพร้อมของ สขร.

การศึกษาเปรียบเทียบกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลของประเทศสมาชิกประชาคมอาเซียนทั้ง 4 ประเทศ คือ อินโดนีเซีย ฟิลิปปินส์ มาเลเซียและสิงคโปร์ นั้น จะพบประเด็นที่น่าสนใจว่าประเทศทั้งหลายต่างก็ได้ยอมรับเอามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ มาบัญญัติไว้เป็นเนื้อหาของกฎหมายของประเทศนั้นๆ ซึ่งรูปแบบกฎหมายและขอบเขตการบังคับใช้กฎหมายยังมีความแตกต่างกัน ได้แก่ รูปแบบที่มีลักษณะเป็นกฎหมายกลางใช้ในการคุ้มครองข้อมูลส่วนบุคคลทุกประเภท จะเป็นกฎหมายของประเทศฟิลิปปินส์ มาเลเซียและสิงคโปร์ ขณะที่ประเทศอินโดนีเซียจะมีลักษณะเป็นกฎหมายเฉพาะเรื่อง ในส่วนขอบเขตของการบังคับใช้กฎหมายนั้น ประเทศฟิลิปปินส์จะใช้บังคับกับข้อมูลส่วนบุคคลที่จัดเก็บทั้งในภาครัฐและภาคเอกชน ส่วนประเทศอินโดนีเซีย มาเลเซียและสิงคโปร์ จะใช้บังคับเฉพาะข้อมูลส่วนบุคคลในภาคเอกชน

สำหรับรูปแบบโครงสร้างของกลไกในกฎหมายที่พบส่วนใหญ่ก็จะมีการออกแบบให้มีคณะกรรมการตามกฎหมายเพื่อทำหน้าที่ขับเคลื่อนการบังคับใช้กฎหมาย การกำหนดสิทธิของบุคคลที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคล การกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคล หลักความยินยอมของผู้เป็นเจ้าของข้อมูล ข้อยกเว้นความยินยอม ข้อกำหนดการส่งข้อมูลไปต่างประเทศที่ต้องมีมาตรฐานที่ไม่ต่ำกว่าของประเทศตน การร้องเรียนจากการดำเนินงานขององค์กรธุรกิจซึ่งเป็นผู้ที่มีหน้าที่ต้องปฏิบัติหลักเกณฑ์เงื่อนไขที่ปรากฏอยู่ในกฎหมายและบทลงโทษสำหรับผู้ที่กระทำผิด โดยจากการศึกษาตามโครงการคณะที่ปรึกษามีข้อเสนอแนะ ดังต่อไปนี้

5.1 ข้อเสนอแนะการพัฒนากฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทย

ประเด็นสำคัญในการพิจารณาศึกษาเปรียบเทียบกฎหมายคุ้มครองข้อมูลส่วนบุคคลใน 4 ประเทศที่เป็นกรณีศึกษานั้นก็จะพบว่าไม่มีประเทศใดที่มีเนื้อหาซึ่งครบถ้วนสมบูรณ์ทั้งหมด บางเรื่องอาจบัญญัติไว้กว้างๆ บางเรื่องอาจบัญญัติไว้อย่างละเอียด ซึ่งขึ้นอยู่เจตนารมณ์ในการยกร่างกฎหมายมาตั้งแต่ต้น อย่างไรก็ตามเมื่อพิจารณาถึงประเด็นนี้จะพบว่ามีข้อแตกต่างอย่างชัดเจนในที่มาของการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศไทยกับประเทศที่เป็นกรณีศึกษาด้วยเหตุที่แรงผลักดันที่ทำให้มีกฎหมายในประเทศนั้นๆ คือปัจจัยทางเศรษฐกิจโดยเฉพาะอย่างยิ่งเศรษฐกิจระหว่างประเทศที่ต้องมีการส่งข้อมูลส่วนบุคคลข้ามประเทศ ซึ่งตามมาตรฐานสากลไม่ว่าจะเป็นของประเทศในกลุ่ม OECD สหภาพยุโรป (EU) หรือ ประเทศที่เข้าร่วมกับAPEC Privacy Frame work ก็จะมีข้อกำหนดในเรื่องมาตรฐานของการคุ้มครองข้อมูลส่วนบุคคลเข้ามาเกี่ยวข้องว่าจะต้องไม่มีมาตรฐานที่ต่ำกว่าประเทศของตน

ดังนั้นเมื่อนำข้อเท็จจริงที่เป็นที่มาที่ไปของการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศสมาชิกประชาคมอาเซียน จึงเป็นเรื่องที่น่าคิดว่าร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ของประเทศไทยได้ตระหนักถึงความจำเป็นดังกล่าวมากน้อยเพียงใด ทั้งจากความก้าวหน้าในเรื่องเทคโนโลยีสารสนเทศของโลกยุคปัจจุบัน การเปลี่ยนแปลงกิจกรรมทางเศรษฐกิจที่มีลักษณะโลกาภิวัตน์ ส่งผลให้มีการเคลื่อนย้ายข้อมูลส่วนบุคคลในปริมาณมหาศาลไม่ว่าจะเป็นด้านอุตสาหกรรม การค้าหรือการบริการ ทั้งนี้การใช้ประโยชน์จากข้อมูลส่วนบุคคลจึงกลายเป็นประเด็นที่น่าสนใจมากยิ่งขึ้นในทางธุรกิจโดยเฉพาะอย่างยิ่ง ธุรกิจที่เกิดขึ้นบนโลกออนไลน์ มีนวัตกรรมความก้าวหน้าใหม่ๆเกิดขึ้น ข้อมูลส่วนบุคคลที่มีความจำเป็นต้องได้รับการปกป้องคุ้มครอง อาจไม่ใช่ข้อมูลส่วนบุคคลตามที่เคยเข้าใจในอดีต ดังจะเห็นได้จากเรื่องของ “Big Data”[42] ตลอดจนความล้ำหน้าในเรื่องเทคโนโลยีต่างๆ เช่น Cloud Computing[43] เป็นต้น

ในส่วนข้อวิพากษ์วิจารณ์ต่อร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลของไทยนั้นก็มีอยู่หลายประการ ดังจะเห็นได้จากข้อเสนอแนะจากโครงการปรับปรุงกระบวนการนิติบัญญัติของประเทศไทยเพื่อส่งเสริมการมีส่วนร่วมของประชาชน โดยสถาบันวิจัยเพื่อการพัฒนาประเทศไทย (TDRI) ดังนี้[44]

1) ความสอดคล้องกับหลัก 8 ประการในการคุ้มครองข้อมูลส่วนบุคคลตามแนวทาง OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

2) ขอบเขตของ “ข้อมูลส่วนบุคคล” ของประเทศไทยนั้นมีการคุ้มครองที่แคบกว่ากฎหมายของประเทศอื่น เพราะควบคุมไว้เฉพาะ “สิ่งเฉพาะตัว” ของบุคคลเท่านั้น ไม่รวมถึงข้อมูลใดๆที่สามารถระบุตัวตนของบุคคลได้ (Identifiable) จึงควรมีการแก้ไขให้ชัดเจนมากขึ้น ขณะเดียวกันข้อมูลส่วนบุคคลควรครอบคลุมถึงข้อมูลส่วนบุคคลประเภทการเก็บข้อมูลที่เป็นพฤติกรรมของบุคคล อันเป็นกิจกรรมที่บุคคลนั้นทำเป็นประจำ (routine activity) ในช่วงเวลาหนึ่งๆ เช่นข้อมูลรายการใช้โทรศัพท์ ข้อมูลรายการซื้อสินค้าหรือบริการผ่านบัตรเครดิต หรือข้อมูลการเข้าถึงเว็บไซต์หรือการดาวน์โหลดต่างๆ ซึ่งอาจจะเป็นข้อมูลที่นำไปใช้ประโยชน์เชิงพาณิชย์หรือนำไปใช้ก่ออาชญากรรมได้

3) ยังมีข้อถกเถียงว่าขอบเขตการให้การยกเว้นที่เหมาะสมควรจะเป็นอย่างไร เช่น กรณีที่สื่อมวลชนจัดเก็บข้อมูลข่าวสารส่วนบุคคลที่มีลักษณะต้องห้ามผ่านการทำข่าวหรือสัมภาษณ์

---

[42]Big Data ก็คือ กลุ่มข้อมูลขนาดใหญ่ ซึ่งสามารถจะนำข้อมูลมหาศาลมาสรุปประมวลผลเพื่อทำความเข้าใจอย่างลึกซึ้ง และนำเสนอในรูปแบบที่ง่ายต่อการทำความเข้าใจอันจะเป็นประโยชน์กับธุรกิจ ซึ่งก็อาจนำไปสู่การละเมิดได้.

[43]Cloud Computing เป็นลักษณะของการทำงานของผู้ใช้งานคอมพิวเตอร์ผ่านอินเทอร์เน็ต ที่ให้บริการใดบริการหนึ่งกับผู้ใช้ โดยผู้ให้บริการจะแบ่งปันทรัพยากรให้กับผู้ต้องการใช้งานนั้น การประมวลผลแบบกลุ่มเมฆเป็นลักษณะที่พัฒนาขึ้นต่อมาจากความคิดและบริการของเวอร์ชัวไลเซชันและเว็บเซอร์วิส โดยผู้ใช้งานนั้นไม่จำเป็นต้องมีความรู้ในเชิงเทคนิคสำหรับตัวพื้นฐานการทำงานนั้น.

[44]รายงานสรุปและวิเคราะห์ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.... โดย คุปต์ พันธ์หินกอง www.thailawwatch.org

4) คณะกรรมการมีสัดส่วนผู้ทรงคุณวุฒิน้อยภาครัฐค่อนข้างน้อย และไม่มีตัวแทนขององค์กรปกครองส่วนท้องถิ่น ในคณะกรรมการ ควรปรับปรุงองค์ประกอบคณะกรรมการให้มีภาคเอกชนด้านอื่นๆมีส่วนร่วมมากยิ่งขึ้นนอกเหนือจากภาคธนาคาร เช่น ด้านเทคโนโลยีคอมพิวเตอร์

5) วิธีการและกระบวนการดำเนินการพิจารณาเรื่องร้องเรียนยังไม่ชัดเจน ควรแก้ไขขั้นตอนและวิธีการดำเนินการรับเรื่องร้องเรียน การพิจารณาเรื่องร้องเรียน หรือการขยายเวลาพิจารณาเรื่องร้องเรียนให้มีความชัดเจนมากขึ้น

6) บทกำหนดโทษควรมีการแก้ไขปรับปรุงโดยกำหนดเพิ่มโทษปรับเป็นรายวันไว้ด้วยนอกเหนือจากการคิดค่าปรับเป็นรายคดี เพื่อปรับแรงจูงใจของผู้ควบคุมข้อมูลให้ปฏิบัติตามกฎหมายอย่างเคร่งครัด

7) ควรให้มีการจัดตั้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลขึ้นมาเมื่อถึงระยะเวลาหนึ่ง เพื่อแบ่งเบาภาระการรับเรื่องร้องเรียนของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการที่มีแนวโน้มจะเพิ่มมากขึ้นภายหลังจากการบังคับใช้กฎหมายไประยะหนึ่งแล้ว

นอกจากข้อเสนอของสถาบันวิจัยเพื่อการพัฒนาประเทศไทย (TDRI) ข้างต้น ยังมีข้อเสนอแนะที่เป็นความเห็นของ รศ.ดร.นนทวัชร์ นวตระกูลพิสุทธ์ อาจารย์ประจำภาควิชากฎหมายพาณิชย์และธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ซึ่งได้เสนอไว้ในบทความเรื่อง “สิทธิในความเป็นส่วนตัวเกี่ยวกับ “ข้อมูลส่วนบุคคล” กับมาตรการคุ้มครองตาม “ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”อย่างน่าสนใจดังนี้ [45]

ในบทความดังกล่าว ได้ชี้ให้เห็นถึงปัญหาของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ของรัฐบาลซึ่งมีกลไกและมาตรการที่ขัดแย้งกับการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลหลายกรณี โดยเฉพาะอย่างยิ่งในสามกรณีใหญ่ๆได้แก่ การกำหนดมาตรการอันเป็น “การจำกัดสิทธิ” ของเจ้าของข้อมูลส่วนบุคคล การกำหนดมาตรการอันเป็นการ “ยกเว้นหลักความยินยอม” และ“ยกเว้นหลักการปฏิบัติตามสิทธิ” ของเจ้าของข้อมูลส่วนบุคคลโดยไม่สมเหตุสมผล และการกำหนดมาตรการอันเป็นการ “ยกเว้นความรับผิด” ของผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่สมควร ซึ่งสามารถแยกออกเป็นปัญหาตามรายมาตราของร่างพระราชบัญญัติ ได้แก่

1) การคุ้มครองเสรีภาพในการแสดงความคิดเห็นของสื่อมวลชนยิ่งกว่าสิทธิในความเป็นส่วนตัวของบุคคล ตามร่างมาตรา 5 ที่กำหนดข้อยกเว้นของการบังคับใช้กฎหมายนี้ไว้

2) การเปิดโอกาสให้เอกชนใช้สัญญาจำกัดสิทธิมนุษยชนของเจ้าของข้อมูลส่วนบุคคลได้ตามร่างมาตรา 16 วรรคสามได้ ซึ่งขัดต่อลักษณะของการคุ้มครองข้อมูลส่วนบุคคลที่เป็นสิทธิมนุษยชน

[45] รายละเอียดข้อเสนอทั้งหมดโปรดดูเพิ่มเติมใน นนทวัชร์ นวตระกูลพิสุทธ์, “สิทธิในความเป็นส่วนตัวเกี่ยวกับ “ข้อมูลส่วนบุคคล” กับมาตรการคุ้มครองตาม “ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....”, **วารสารนิติศาสตร์** ปีที่ 43 ฉบับที่ 4 (ธันวาคม 2557), น. 732-771.

3) การเปิดโอกาสให้เอกชนเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนตามร่างมาตรา 22

4) การเปิดโอกาสให้เอกชนเก็บรักษาข้อมูลส่วนบุคคลแม้จะพ้นกำหนดเวลา หมดความจำเป็น หรือเจ้าของข้อมูลส่วนบุคคลเพิกถอนความยินยอมได้ตามร่างมาตรา 31 วรรคสอง

5) การไม่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประกอบกิจการเชิงธุรกิจหรือการพาณิชย์ลบหรือทำลายข้อมูลส่วนบุคคลเมื่อเลิกกิจการตามร่างมาตรา 40 วรรคหนึ่ง

6) การกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถปฏิเสธที่จะปฏิบัติตามคำขอของเจ้าของข้อมูลส่วนบุคคลโดยไม่มีเหตุผลโดยชอบ ตามร่างมาตรา 42

7) การกำหนดเหตุยกเว้นความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่สมควร ตามร่างมาตรา 43

ทั้งนี้อาจารย์ นนทวัชร์ นวตระกูลพิสุทธ์ ยังได้มีข้อเสนอแนะเพิ่มเติมเพื่อการปรับปรุงกลไกและมาตรการคุ้มครองข้อมูลส่วนบุคคลให้มีความเหมาะสมยิ่งขึ้นในหลายประการ ดังต่อไปนี้

1) การกำหนดการปฏิบัติตามหลักความได้สัดส่วนสำหรับกรณีที่เป็นข้อยกเว้นการปฏิบัติตามสิทธิของเจ้าของข้อมูลส่วนบุคคล

2) การกำหนดหลักเกณฑ์และเงื่อนไขเกี่ยวกับการเก็บรวบรวมข้อมูลส่วนบุคคลอันมีลักษณะต้องห้าม

3) การกำหนดหลักเกณฑ์และเงื่อนไขเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประกอบกิจการเชิงธุรกิจหรือการพาณิชย์ให้มีความเข้มงวดมากขึ้น ได้แก่ กำหนดให้มีการขึ้นทะเบียนผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประกอบกิจการเชิงธุรกิจกับ สขร. การประกาศข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งประกอบกิจการเชิงธุรกิจ ตลอดจนรายละเอียดเกี่ยวกับการจัดทำระบบข้อมูลส่วนบุคคลเป็นการทั่วไป การกำหนดคุณสมบัติของผู้ควบคุมข้อมูลส่วนบุคคลอย่างเคร่งครัดและชัดเจนเพื่อให้เกิดความเชื่อมั่นในการรับรองและคุ้มครองสิทธิของเจ้าของข้อมูล การกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลจัดทำรายงานการดำเนินการตามกฎหมายประจำปีเสนอต่อ สขร. และกำหนดบทลงโทษผู้ควบคุมข้อมูลส่วนบุคคลในกรณีนี้ให้รุนแรงยิ่งกว่าการกระทำความผิดของผู้ควบคุมข้อมูลส่วนบุคคลกรณีทั่วไป โดยเฉพาะการกำหนด “ค่าสินไหมทดแทนเพื่อการลงโทษ” (punitive damages) แก่ผู้ควบคุมข้อมูลส่วนบุคคลในกรณีนี้ โดยคำนึงถึงพฤติการณ์ของการกระทำการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายประกอบกับความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ

ข้อเสนอแนะต่างๆเกี่ยวกับการแก้ไขปรับปรุงร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่นำเสนอมาข้างต้นคณะผู้ศึกษามีความเห็นด้วยว่ามีเหตุผลที่น่ารับฟังซึ่งทาง สขร. ควรรับไปพิจารณานำเสนอเพื่อปรับปรุงแก้ไขในกระบวนการพิจารณาของสภานิติบัญญัติแห่งชาติต่อไป อย่างไรก็ตามในสถานการณ์ปัจจุบันได้มีประเด็นสำคัญที่ส่งผลต่อการผลักดันร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลให้ได้รับการประกาศใช้บังคับเป็นกฎหมายต่อไปเพราะได้มีการนำเสนอร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอีกฉบับ โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารซึ่งมีเนื้อหาที่แตกต่างไปจากร่างพระราชบัญญัติที่อยู่ในการพิจารณาของสภานิติบัญญัติแห่งชาติในประเด็น

หลักการ คือการเปลี่ยนแปลงหน่วยงานรัฐผู้ดูแลจากสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการมาเป็นสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อีกทั้งได้เปลี่ยนผู้รักษาการตามกฎหมายจากนายกรัฐมนตรีมาเป็นรมต.กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

รวมถึงได้มีการเปลี่ยนแปลงองค์ประกอบของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่ได้ตัดตัวแทนของภาคประชาชนและเอกชนออกไป ถ้าเปรียบเทียบกับองค์ประกอบของคณะกรรมการในร่างกฎหมายทั้งสองฉบับก็จะพบความแตกต่างในการกำหนดองค์ประกอบอย่างมีนัยสำคัญ ซึ่งคณะผู้ศึกษาเห็นว่าองค์ประกอบคณะกรรมการนับว่าเป็นเรื่องสำคัญที่ส่งผลต่อการขับเคลื่อนการบังคับใช้กฎหมายว่าจะประสบความสำเร็จตามวัตถุประสงค์หรือไม่ ทั้งนี้จากการวิเคราะห์คณะผู้ศึกษาเห็นว่าองค์ประกอบตามร่างกฎหมายของกระทรวงกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารนั้นขาดความเหมาะสมเนื่องจากขาดการมีส่วนร่วมจากภาคส่วนต่างๆที่ครอบคลุมครบถ้วนโดยเฉพาะตัวแทนจากภาคเอกชนที่เป็นผู้ต้องจัดเก็บข้อมูลส่วนบุคคลและปฏิบัติตามบทบัญญัติกฎหมายให้ถูกต้องและที่สำคัญ ผู้อำนวยการ สขร. ได้ถูกตัดออกจากกรรมการชุดนี้ ทำให้งานของกฎหมายนี้ขาดความเชื่อมโยงกับการคุ้มครองข้อมูลส่วนบุคคลในกฎหมายข้อมูลข่าวสารราชการซึ่งไม่ถูกต้อง

ตารางเปรียบเทียบองค์ประกอบของคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในร่างกฎหมาย

ร่างของคณะรัฐมนตรีที่เสนอ สนช.	ร่างของกระทรวงICT
ประธานกรรมการ คือ รัฐมนตรีซึ่งนายกฯมอบหมาย **กรรมการโดยตำแหน่ง**ได้แก่ 1.ปลัดสำนักนายกรัฐมนตรี 2.ปลัดกระทรวง ICT 3.เลขาธิการคณะกรรมการกฤษฎีกา 4.อธิบดีกรมคุ้มครองสิทธิและเสรีภาพ 5.ผู้ว่าการธนาคารแห่งประเทศไทย **กรรมการที่เป็นผู้แทนองค์กรภายนอก** ได้แก่ 6.ผู้แทนคณะกรรมการคุ้มครองผู้บริโภค 7.ผู้แทนหอการค้าไทย 8.ผู้แทนสมาคมธนาคารไทย กรรมการผู้ทรงคุณวุฒิซึ่งนายกรัฐมนตรีแต่งตั้งจากผู้ซึ่งมีความรู้ความเชี่ยวชาญด้านกฎหมายและด้านเทคโนโลยีด้านละ2คนอย่างน้อยต้องแต่งตั้งจากภาคเอกชนไม่น้อยกว่ากึ่งหนึ่ง ผู้อำนวยการ สขร. เป็นกรรมการและเลขานุการ	ประธานกรรมการ คือบุคคลซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล หรือด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล **กรรมการโดยตำแหน่ง** ไม่เกิน 4 คน ได้แก่ ปลัดสำนักนายกรัฐมนตรี ปลัดกระทรวงดิจิทัลฯ ปลัดกระทรวงมหาดไทย และเลขาธิการสภาความมั่นคงแห่งชาติ กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกิน 4 คน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญเป็นที่ประจักษ์ในด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านการคุ้มครองผู้บริโภค ด้านสังคมศาสตร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือด้านนิติศาสตร์ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล ให้เลขาธิการสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นกรรมการและเลขานุการโดยตำแหน่ง

5.2 การเตรียมความพร้อมของ สขร. ในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

จากการศึกษาในรายงานฉบับนี้โดยเฉพาะประสบการณ์ของประเทศสิงคโปร์ก็แสดงให้เห็นว่าความสำเร็จของการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้น มิได้เกิดจากการบัญญัติกฎหมายที่ดีในส่วนเนื้อหาเท่านั้น แต่ต้องมีการเตรียมความพร้อมก่อนการบังคับใช้กฎหมายด้วย เพราะกฎหมายดังกล่าวหากประกาศใช้ย่อมส่งผลกระทบต่อองค์กรธุรกิจจำนวนมาก ขณะเดียวกันในด้านประชาชนถ้าไม่รู้ถึงสิทธิที่ได้รับการคุ้มครองตามกฎหมายก็คงไม่สามารถเรียกร้องสิทธิและรู้ว่าตนเองถูกละเมิดข้อมูลส่วนบุคคลอย่างไร

ดังนั้นคณะผู้ศึกษาเห็นว่าทางสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการมีความจำเป็นต้องเตรียมการวางแผนรองรับการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทย ไม่ว่าจะเป็นการสร้างการรับรู้ร่วมกันของสังคมไทยทุกภาคส่วนทั้งภาคเอกชน ภาครัฐและประชาชนทั่วไปให้รับทราบถึงข้อกำหนดสำคัญตามกฎหมาย การสร้างความตระหนักในความสำคัญของข้อมูลส่วนบุคคล การเผยแพร่องค์ความรู้และความเข้าใจที่ถูกต้องผ่านช่องทางสื่อสารต่างๆ ทั้งสื่อสิ่งพิมพ์ สื่อใหม่ และสื่อมวลชน ซึ่งก่อนหน้าที่กฎหมายจะผ่านสภานิติบัญญัติแห่งชาติก็ควรที่จะมีการดำเนินงานอย่างเป็นขั้นตอนในแต่ละช่วงเวลา เพราะถ้ารอให้กฎหมายประกาศใช้ก่อนก็อาจจะไม่ทันกาลซึ่งประสบการณ์ของกิจกรรมต่างๆของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (PDPC) ที่ได้นำเสนอมาเป็นกรณีศึกษาก็สามารถนำมาปรับใช้กับประเทศไทยได้เป็นอย่างดี

ทั้งนี้เพื่อให้เห็นเป็นรูปธรรมถึงแนวทางการเผยแพร่กฎหมาย/หลักการคุ้มครองข้อมูลส่วนบุคคลขอประเทศสมาชิกอาเซียนให้ประชาชนไทยเตรียมพร้อมการเข้าสู่ประชาคมอาเซียนนั้น คณะผู้ศึกษามีข้อเสนอแนะต่อการเตรียมการของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการในแต่ละเรื่องดังต่อไปนี้

1. การกำหนดกลุ่มเป้าหมายในการเผยแพร่องค์ความรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

ในที่นี้ทางคณะผู้ศึกษามีข้อเสนอแนะให้ทาง สขร. กำหนดกลุ่มเป้าหมายไว้สามกลุ่ม ได้แก่ ประชาชนทั่วไป กลุ่มองค์กรธุรกิจภาคเอกชน และกลุ่มนักเรียนนักศึกษา ซึ่งการกำหนดเป็นสามกลุ่มจะทำให้การเผยแพร่ด้านเนื้อหาที่จะเกิดขึ้นสอดคล้องกับลักษณะเฉพาะแต่ละกลุ่ม ทำให้เกิดประสิทธิภาพ ความสำเร็จในการสร้างความรู้ความเข้าใจได้มากขึ้นและเหมาะสมกับแต่ละกลุ่ม โดยเนื้อหาก็จะมีความยากง่ายแตกต่างกัน

2. การออกแบบลักษณะเนื้อหาในการเผยแพร่ให้เหมาะสมกับกลุ่มเป้าหมายแต่ละกลุ่ม

สืบเนื่องจากการแบ่งกลุ่มเป้าหมายในข้อ 1 ซึ่งมีความสนใจไม่เหมือนกัน การออกแบบเนื้อหาในการเผยแพร่ควรมีการจัดทำให้สอดคล้องกับลักษณะเฉพาะแต่ละกลุ่ม โดยคณะผู้ศึกษาให้ความสำคัญกับกลุ่มที่ต้องปฏิบัติตามกฎหมายได้แก่องค์กรธุรกิจภาคเอกชน และ

กลุ่มประชาชนทั่วไปเป็นเบื้องต้น ขณะที่ในกลุ่มนักเรียนนักศึกษาก็เป็นกลุ่มคนรุ่นใหม่ที่ต้องปลูกฝังความรู้ความเข้าใจในเรื่องนี้ต่อไปด้วย

สำหรับเนื้อหาที่ทาง สขร. ควรเตรียมการจัดทำขึ้นสำหรับกลุ่มองค์กรธุรกิจ คือการสร้างความเข้าใจเกี่ยวกับเจตนารมณ์ของกฎหมายและประโยชน์แก่องค์กรธุรกิจที่จะเกิดขึ้น ตลอดจนหน้าที่ซึ่งกฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ต้องปฏิบัติ และจะปฏิบัติอย่างไรให้ถูกต้องตามกฎหมาย อีกทั้งช่องทางในการติดต่อขอคำปรึกษาแนะนำต่างๆจะติดต่อได้อย่างไรบ้าง สุดท้ายหากมีการฝ่าฝืนกฎหมายจะต้องรับผิดมีบทลงโทษอะไรบ้าง โดยรูปแบบเนื้อหาควรทำออกมาเป็นคู่มือการปฏิบัติหน้าที่ตามกฎหมายขององค์กรธุรกิจ การจัดทำในลักษณะคำถามคำตอบที่พบบ่อยๆ Q&A แผ่นพับอธิบายกฎหมายอย่างง่ายๆ เป็นต้น ซึ่งรูปแบบนี้ประเทศสิงคโปร์ก็ได้ใช้ปฏิบัติอยู่ รวมถึงการออกแบบจัดทำหลักสูตรฝึกอบรมการปฏิบัติตามกฎหมายทั้งระยะสั้นและระยะยาวแก่องค์กรธุรกิจ

ในส่วนกลุ่มประชาชน จำเป็นต้องให้ทราบถึงสิทธิที่จะได้รับการคุ้มครองตามกฎหมายและหน้าที่ซึ่งองค์กรธุรกิจต้องปฏิบัติ รวมถึงช่องทางในการขอความช่วยเหลือในเวลาที่เกิดปัญหา ซึ่งเนื้อหาในส่วนนี้สามารถนำไปใช้กับกลุ่มนักเรียนนักศึกษาได้โดยจัดรูปแบบนำเสนอให้ง่ายขึ้นได้

3. การใช้ช่องทางการเผยแพร่ข้อมูลข่าวสารที่มีประสิทธิภาพและกิจกรรมที่ควรจัดให้เกิดขึ้น

เมื่อพิจารณาถึงการเผยแพร่ข้อมูลข่าวสารเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายให้แก่ประชาชน องค์กรธุรกิจ และนักเรียนนักศึกษาที่ได้ออกแบบไว้แล้ว ประเด็นที่ สขร. จะต้องดำเนินการต่อไป คือการใช้ช่องทางและการจัดกิจกรรมที่เหมาะสมเพื่อให้เข้าถึงกลุ่มเป้าหมายให้มากที่สุด ซึ่งในยุคปัจจุบันสื่อที่มีบทบาทอย่างมาก คือ สื่อใหม่ (New Media)ได้แก่ สื่อออนไลน์ต่างๆ แต่อย่างไรก็ตามการผลิตสื่อสิ่งพิมพ์ก็ยังมีความสำคัญเนื่องจากเป็นเอกสารที่ทุกกลุ่มสามารถจับต้องและใช้ประโยชน์ได้โดยตรง และยังมีคนจำนวนมากที่ไม่สามารถเข้าถึงเนื้อหาในสื่อออนไลน์ได้ง่าย

ดังนั้น คณะผู้ศึกษาจึงขอเสนอให้ทาง สขร. นำเนื้อหาที่ได้จัดทำซึ่งเหมาะสมแต่ละกลุ่มในลักษณะแผ่นพับ คู่มืออธิบายและบรรจุไว้ในเว็บไซต์ของหน่วยงาน โดยควรมีเนื้อหาต่างๆ ดังต่อไปนี้

1) ความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลและสิทธิของประชาชนที่ควรรู้

2) สาระสำคัญของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในลักษณะเข้าใจง่าย (ฉบับประชาชน)

3) ข้อควรปฏิบัติขององค์กรธุรกิจให้ถูกต้องตามกฎหมายในเรื่องการคุ้มครองข้อมูลส่วนบุคคล

4) กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับนักเรียนนักศึกษา โดยอาจจัดทำในรูปแบบการ์ตูน

5) คำถามคำตอบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย 20 คำถามที่พบบ่อย (Q&A)

อย่างไรก็ตามเนื่องจากในขณะนี้กฎหมายคุ้มครองข้อมูลส่วนบุคคลยังไม่ผ่านการพิจารณาของรัฐสภาและยังไม่มีผลเป็นกฎหมายสมบูรณ์ ดังนั้นการนำเสนอข้อมูลต่างๆมีความจำเป็นที่ต้องรอความชัดเจนตามกฎหมายก่อน แม้กระนั้นก็ตาม สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการก็สามารถจัดทำเอกสารเผยแพร่ในส่วนร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล และการรณรงค์ให้ประชาชนเกิดความตระหนักถึงสิทธิส่วนบุคคลที่ได้รับการคุ้มครองตามกฎหมายเป็นเบื้องต้นได้ในระหว่างกฎหมายยังไม่ได้ประกาศใช้เพื่อเป็นการสร้างการรับรู้แก่ประชาชนและองค์กรธุรกิจที่ต้องปฏิบัติตามกฎหมายในอนาคตได้

นอกจากการจัดทำเอกสารและข้อมูลเผยแพร่ผ่านทางเว็บไซต์ของสำนักงานแล้ว คณะผู้ศึกษามีข้อเสนอแนะถึงการเปิดช่องทางการติดต่อสื่อสารให้ความรู้ผ่านสื่อเครือข่ายสังคมออนไลน์ คือ Face book ที่เป็นสื่อที่ได้รับความนิยมอยู่ในปัจจุบันโดยเปิดหน้าเพจของสำนักงานขึ้นเพื่อเข้าถึงเยาวชนคนรุ่นใหม่และประชาชนทั่วไปโดยตรง ขณะเดียวกันหากพิจารณาถึงแนวทางการดำเนินเพื่อรองรับการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ ที่ได้มีการจัดกิจกรรมประชุมสัมมนาให้ความรู้และการฝึกอบรมในลักษณะกลุ่มเฉพาะ ซึ่งถือว่าประสบความสำเร็จอย่างมาก ก็นับเป็นกรณีศึกษาที่สำนักงาน สขร. ควรใช้รูปแบบกิจกรรมเช่นนี้มาจัดขึ้นด้วย โดยเฉพาะในช่วงเวลานี้ซึ่งกฎหมายอยู่ระหว่างการพิจารณาของสภานิติบัญญัติแห่งชาติก็จะเป็นการสร้างความรู้ความเข้าใจให้เกิดขึ้นเป็นวงกว้างและตรงกับกลุ่มเป้าหมายที่มีหน้าที่ปฏิบัติตามกฎหมายอีกด้วย

4. การแสวงหาความร่วมมือกับองค์กรภายนอกทั้งในภาครัฐและภาคเอกชน

เนื่องจากภารกิจของการขับเคลื่อนกฎหมายคุ้มครองข้อมูลส่วนบุคคล เป็นเรื่องที่มีความสำคัญในสถานการณ์ที่กฎหมายกำลังพิจารณาอยู่ในฝ่ายนิติบัญญัติ ซึ่งต้องดำเนินการหลายด้านเพื่อเป็นการเตรียมความพร้อมล่วงหน้า ในประเด็นนี้ถ้าพิจารณาศักยภาพของหน่วยงานคือ สขร. ก็อาจมีข้อจำกัดหลายเรื่องทั้ง งบประมาณและบุคลากร ดังนั้นผู้ศึกษาจึงขอเสนอให้ สขร. ทำความตกลงร่วมมือกันระหว่างหน่วยงานต่างๆทั้งภาครัฐและเอชน เพื่อเข้ามาเป็นหุ้นส่วนช่วยเหลือกันในการทำงานไม่ว่าจะเป็นการเผยแพร่ความรู้ความเข้าใจ การให้คำแนะนำให้คำปรึกษาการปฏิบัติตามกฎหมายที่ถูกต้อง และครอบคลุมกลุ่มเป้าหมายต่างๆ โดยการดำเนินการเช่นนี้มีตัวอย่างความสำเร็จในการเตรียมการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสิงคโปร์ที่ได้จัดกิจกรรมประชุมสัมมนาและการฝึกอบรมเผยแพร่ความรู้หลายครั้งก่อนกฎหมายมีผลบังคับอย่างเป็นทางการ

ในส่วนองค์กรภายนอกรัฐทาง สขร. มีความจำเป็นต้องสื่อสารสร้างความเข้าใจในกฎหมายแก่ตัวแทนสมาคมของภาคเอกชนต่างๆ ไม่ว่าจะเป็นหอการค้าแห่งประเทศไทย สมาคมธนาคารไทย สมาคมผู้ประกอบการที่รวมตัวกัน โดยเฉพาะการเจาะกลุ่มเป้าหมายที่มีหน้าที่ปฏิบัติและกลุ่มธุรกิจขนาดกลางและขนาดเล็กซึ่งจะมีภาระและข้อจำกัดในการปฏิบัติมากกว่ากลุ่มธุรกิจขนาดใหญ่ที่มีความพร้อมมากกว่า ทั้งนี้จากกรณีต่างประเทศจะพบว่ากลุ่มธุรกิจ SME คือ กลุ่มที่ทุกประเทศให้ความสนใจที่ต้องเข้าไปดูแลให้คำปรึกษาเป็นพิเศษ นอกจากจำนวนที่มีมากแล้วยังมีประเด็น

ท้ายที่สุดคณะผู้ศึกษาเห็นว่าสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการต้องเร่งเตรียมความพร้อมให้กับบุคลากรของสำนักงานในการรองรับภารกิจใหม่ที่จะเพิ่มขึ้นจากการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ตลอดจนทำการปฏิรูปสำนักงานในด้านต่างๆและสร้างเครือข่ายความร่วมมือกับองค์กรภายนอกทั้งภายในและภายนอกประเทศ ภารกิจข้างหน้าเป็นความท้าทายอย่างยิ่งของสำนักงาน ขณะเดียวกันก็มีส่วนสัมพันธ์กับการพัฒนาเติบโตทางเศรษฐกิจของประเทศในยุคข้อมูลข่าวสารสารสนเทศอีกทางหนึ่งด้วย ประเด็นทั้งหมดนี้กล่าวมานี้ การนำเสนอให้ฝ่ายนโยบายคือคณะรัฐมนตรี และฝ่ายสภานิติบัญญัติแห่งชาติได้รับทราบความสำคัญและมีความเข้าใจที่ถูกต้องก็จำเป็นต้องดำเนินการในช่วงระยะเวลานี้ควบคู่กันไปเพื่อไม่ให้การตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยล่าช้าออกไปอย่างเช่นอดีตที่ผ่านมา

อย่างไรก็ตามนอกเหนือจากการผลักดันให้กฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคลผ่านการพิจารณาของสภานิติบัญญัติแห่งชาติมีผลเป็นกฎหมายแล้ว คณะผู้ศึกษายังมีความเห็นเพิ่มเติมว่า สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการยังมีความจำเป็นอีกประการหนึ่งที่ควรดำเนินงานยกระดับการคุ้มครองข้อมูลส่วนบุคคลของประเทศไทยให้ได้มาตรฐานสากล โดยพิจารณาจัดทำเอกสารเพื่อเสนอแนะต่อคณะกรรมการข้อมูลข่าวสารของราชการที่จะได้มีมติเสนอแนะต่อคณะรัฐมนตรีให้ความเห็นชอบในการที่ประเทศไทยจะสมัครเข้าร่วมกรอบข้อตกลงการคุ้มครองข้อมูลส่วนบุคคลของเอเปค (APEC Privacy Framework) ซึ่งประเทศไทยจะได้รับประโยชน์หลายประการดังที่ปรากฏในรายงานโครงการพัฒนามาตรการในการดำเนินการ การพิจารณาความเหมาะสม ความเป็นไปได้ เพื่อจัดทำแนวทาง ขั้นตอนและวิธีการในการเข้าร่วมหรือทำความตกลงตามกรอบว่าด้วยการคุ้มครองความเป็นส่วนตัวของ APEC (APEC Privacy Framework) ที่จัดทำโดยสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

แม้ประเทศไทยยังไม่มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในปัจจุบัน ก็ยังสามารถแสดงความจำนงถึงการเข้าร่วมกรอบการคุ้มครองข้อมูลส่วนบุคคลของเอเปคได้ โดยแสดงให้เห็นถึงบรรดากฎหมายระดับพระราชบัญญัติหรือกฎหมายระดับรองที่เกี่ยวข้องซึ่งมีการคุ้มครองข้อมูลส่วนบุคคลภายในประเทศไว้ โดยเฉพาะอย่างยิ่งการคุ้มครองในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ขณะเดียวหากบทกฎหมายใดที่ยังมีปัญหาก็สามารถดำเนินการแก้ไขปรับปรุงภายหลังให้สมบูรณ์ต่อไป ซึ่งในกรณีนี้จะคล้ายกับประเทศญี่ปุ่นโดยเมื่อเข้าร่วมแล้วก็ได้ดำเนินการปรับปรุงกฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศให้มีประสิทธิภาพสอดคล้องกับมาตรฐานเอเปค

ขณะเดียวกัน สขร. มีความจำเป็นในการสร้างความชัดเจนของการมีเจ้าภาพและบูรณาการทุกภาคส่วนทั้งรัฐและเอกชนให้มีความตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล การปฏิบัติที่ถูกต้องเหมาะสม ตลอดจนการเผยแพร่ความรู้ความเข้าใจในสิทธิส่วนบุคคลและหน้าที่ของหน่วยงานเอกชนและรัฐที่ต้องปฏิบัติตามกฎหมาย และการเตรียมการปรับปรุงแก้ไขกฎหมายต่างๆที่เกี่ยวข้องนั้น เป็นบทบาทที่สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการจะต้องวางแผนกำหนดยุทธศาสตร์และลงมือปฏิบัติซึ่งมีรายละเอียดดังนี้

1) ที่ปรึกษามีข้อเสนอแนะให้ สขร. จัดทำข้อเสนอแนะเชิงนโยบายในการเตรียมการเข้าร่วม APEC Privacy Framework ต่อคณะรัฐมนตรีโดยผ่านความเห็นชอบจากคณะกรรมการข้อมูลข่าวสารของราชการ ซึ่งเป็นอำนาจหน้าที่ตามมาตรา 6 ประกอบกับมาตรา 8 โดยชี้ให้เห็นถึงความจำเป็นและประโยชน์ที่จะเกิดขึ้น และระบุถึงการให้ สขร. เป็นหน่วยงานหลักในการดูแลและประสานงานระหว่างหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องทั้งหมดเพื่อให้เกิดการทำงานเชิงบูรณาการ

2) ในข้อเสนอดังกล่าว คณะที่ปรึกษาเห็นว่า สขร. ควรเสนอให้นายกรัฐมนตรีใช้อำนาจตามพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. 2534 มาตรา 11 (6) แต่งตั้งคณะกรรมการระดับชาติเพื่อดูแลการเข้าร่วม APEC Privacy Framework และทำหน้าที่เตรียมการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้ สขร. ทำหน้าที่เป็นหน่วยงานเลขานุการและธุรการ

3) สำหรับองค์ประกอบของคณะกรรมการระดับชาติที่จะจัดตั้งขึ้น ควรประกอบด้วยรัฐมนตรีประจำสำนักนายกรัฐมนตรีเป็นประธาน และกรรมการอื่นๆที่มีส่วนร่วมจากภาคส่วนที่เกี่ยวข้อง ได้แก่ หน่วยงานของรัฐ ได้แก่ปลัดกระทรวงหรือผู้แทนจากกระทรวงการต่างประเทศ กระทรวงกลาโหม กระทรวงพาณิชย์ กระทรวงอุตสาหกรรม กระทรวงมหาดไทย ธนาคารแห่งประเทศไทย ตัวแทนภาคเอกชน ได้แก่ หอการค้าแห่งประเทศไทย สมาคมธนาคารไทย และผู้ทรงคุณวุฒิที่ซึ่งเป็นผู้เชี่ยวชาญด้านกฎหมายระหว่างประเทศ กฎหมายมหาชน และข้อมูลส่วนบุคคล โดยมีผู้อำนวยการสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเป็นกรรมการและเลขานุการ ทั้งนี้การที่ที่ปรึกษาไม่ได้เสนอแนะให้นายกรัฐมนตรีมอบหมายภารกิจนี้ให้กับคณะกรรมการข้อมูลข่าวสารของราชการรับผิดชอบโดยตรงนั้นเนื่องจากองค์ประกอบของคณะกรรมการข้อมูลข่าวสารของราชการจะจำกัดเฉพาะหน่วยงานภาครัฐ ไม่มีกรรมการตัวแทนของภาคเอกชน

4) สำหรับการเตรียมการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่ปรึกษาเห็นว่าในข้อเสนอที่นำเสนอต่อคณะรัฐมนตรีนั้นควรกำหนดเป็นแผนปฏิบัติการในการจัดประชุมสัมมนาระดับชาติ เพื่อสร้างความรู้ความเข้าใจแก่สังคม การจัดทำเอกสารเผยแพร่ข้อมูลข่าวสารเกี่ยวกับเนื้อหากฎหมาย การจัดประชุมชี้แจงและฝึกอบรมให้กับภาคเอกชน และการผลิตสื่อประชาสัมพันธ์

ทั้งนี้ในสถานการณ์ปัจจุบันนับว่ามีความยุ่งยากมากขึ้นสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการเนื่องจากไม่ได้มีเพียงร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ฉบับเดียวที่เป็นการผลักดันโดยสำนักงานอยู่ในการพิจารณาของสภานิติบัญญัติแห่งชาติ โดยยังมีร่างพระราชบัญญัติอีกฉบับที่มีการเสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะเป็นส่วนหนึ่งของชุดร่างกฎหมายเพื่อผลักดันเศรษฐกิจดิจิทัลตามนโยบายของรัฐบาลพลเอกประยุทธ์ จันทร์โอชา ซึ่งร่างกฎหมายฉบับนี้คณะรัฐมนตรีได้มีมติให้ความเห็นชอบและอยู่ระหว่างการพิจารณาของคณะกรรมการกฤษฎีกาขณะนี้ หากเปรียบเทียบร่างกฎหมายทั้งสองฉบับนับว่ามีความแตกต่างกันในเรื่องสำคัญหลายประการตามที่คณะผู้ศึกษาได้นำเสนอมาในบทที่ 3 แล้ว

เมื่อพิจารณาถึงเนื้อหาของร่างพระราชบัญญัติทั้งสองฉบับ ร่างกฎหมายที่เสนอโดยกระทรวงICT นับว่าถูกวิพากษ์วิจารณ์จากสาธารชนรวมถึงนักวิชาการเป็นอย่างมากในประเด็นความบกพร่องที่ไม่เหมาะสมสอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลที่ควรจะเป็น ซึ่งคณะผู้ศึกษาก็เห็นด้วยเช่นกัน ดังนั้นในสถานการณ์เช่นนี้จึงไม่เป็นผลดีต่อสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการหากท้ายที่สุดร่างกฎหมายของกระทรวงICT ได้กลายเป็นร่างหลักในการพิจารณาของสภานิติบัญญัติแห่งชาติ เพราะจะส่งผลทำให้งานการคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนจะถูกดึงออกไปจากสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการไปอยู่ที่หน่วยงานใหม่ซึ่งจะเกิดขึ้น คือ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ฉะนั้นในทัศนะของคณะผู้ศึกษาเห็นว่าทาง สขร. มีความจำเป็นที่ต้องช่วงชิงบทบาทนำในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลกลับมา ซึ่งจะต้องสร้างความเข้าใจและการสนับสนุนจากฝ่ายบริหาร และสาธารณชนทั่วไปเพื่อเป็นแรงสนับสนุนสำคัญในการคงบทบาทดูแลการบังคับใช้กฎหมายฉบับนี้ที่ สขร. โดยเริ่มต้นจากการเผยแพร่ความรู้ความเข้าใจผ่านการจัดเวทีสัมมนาทางวิชาการอย่างต่อเนื่องและจัดทำข้อมูลเผยแพร่ผ่านสื่อมวลชนในช่องทางต่างๆโดยเริ่มจากเว็บไซต์ของ สขร. แน่นอนว่าทางสำนักงานอาจมีข้อจำกัดเรื่องงบประมาณและบุคลากรที่มีความพร้อม แต่ก็สามารถแก้ไขปัญหาดังกล่าวได้จากการแสวงหาความร่วมมือทางวิชาการกับสถาบันการศึกษา นักวิชาการและสมาคมขององค์กรธุรกิจเอกชนที่มีอยู่ในประเทศไทย ซึ่งทั้งหมดนี้ทางสำนักงานควรเริ่มต้นอย่างทันทีและจัดเป็นความสำคัญเร่งด่วนที่ไม่อาจรอช้าได้ เพราะมิเช่นนั้น สขร. ก็จะสูญเสียบทบาทนำในเรื่องการคุ้มครองข้อมูลส่วนบุคคลไป โดยทั้งหมดนี้ คณะผู้ศึกษาเห็นว่าจะเป็นจุดเปลี่ยนที่ส่งผลต่อการพัฒนาของสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการในอนาคตที่ควรคว้าโอกาสนี้มาให้ได้

บรรณานุกรม

หนังสือและบทความในหนังสือ

กิตติศักดิ์ ปรกติ. ความรู้เบื้องต้นเกี่ยวกับสิทธิรับรู้ข้อมูลข่าวสาร ตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ 2540. กรุงเทพมหานคร: วิญญูชน, 2541.

เกรียงไกร เจริญธนาวัฒน์ . หลักกฎหมายว่าด้วยสิทธิเสรีภาพ. กรุงเทพมหานคร : วิญญูชน, 2547.

กลุ่มงานนโยบาย สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ. เอกสารแปลกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล, แปลโดย ศิริกุล ภู่พันธ์ และนคร เสรีรักษ์, 2544.

ชาญชัย แสวงศักดิ์. สาระน่ารู้ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540. กรุงเทพมหานคร : วิญญูชน, 2540.

นคร เสรีรักษ์ . ความเป็นส่วนตัว. กรุงเทพมหานคร: พี.เพรส, 2557.

นนทวัชร์ นวตระกูลพิสุทธ์ . “สิทธิในความเป็นส่วนตัวเกี่ยวกับ “ข้อมูลส่วนบุคคล” กับมาตรการคุ้มครองตาม “ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....” วารสารนิติศาสตร์ ปีที่ 43 ฉบับที่ 4 (ธันวาคม 2557).

นพนิธิ สุริยะ. สิทธิมนุษยชน. กรุงเทพมหานคร: วิญญูชน, 2537.

บุญรักษ์ บุญญะเขตมาลา. “สิทธิที่จะรู้ในมาตรา 58 สู่รัฐโปร่งใส.” ในระหว่างกระจกกับตะเกียง. โครงการจัดพิมพ์คบไฟ, 2542.

บรรเจิด สิงคะเนติ. หลักพื้นฐานของ สิทธิ เสรีภาพ และศักดิ์ศรีความเป็นมนุษย์ตามรัฐธรรมนูญใหม่. กรุงเทพมหานคร: วิญญูชน, 2543.

พิชิตพล ศรียานนท์ และ สมศักดิ์ นวตระกูลพิสุทธิ์. “สิทธิในการรับรู้ข้อมูลข่าวสารของราชการตามกฎหมายฝรั่งเศส เยอรมัน และสหรัฐอเมริกา.” วารสารกฎหมายปกครอง 17 (2541).

ฤทัย หงส์สิริและมานิตย์ จุมปา . คำอธิบายกฎหมายและข้อมูลข่าวสารของทางราชการ. กรุงเทพมหานคร: นิติธรรม, 2542.

วัชรา ไชยสาร. สิทธิรับรู้ข้อมูลข่าวสารของราชการ. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: นิติธรรม, 2544.

สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ. โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ. พิมพ์ครั้งที่ 3. กรุงเทพมหานคร, 2544.

สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์. แนวทางการจัดทำกฎหมายคุ้มครองข้อมูลส่วนบุคคล. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547.

อธิป จิตตฤกษ์ และปวรรัตน์ ผลาสิทธุ์ (ผู้แปล) . ความเป็นส่วนตัว ความรู้ฉบับพกพา . กรุงเทพฯ : โอเพ่นเวิลด์ส, 2556.

อุดม รัฐอมฤต, นพนิธิ สุริยะ และ บรรเจิด สิงคะเนติ. การอ้างศักดิ์ศรีความเป็นมนุษย์เพื่อใช้สิทธิเสรีภาพของบุคคลตามมาตรา 28 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2540. กรุงเทพมหานคร: นานาสิ่งพิมพ์, 2544.

<u>วิทยานิพนธ์</u>

กงจักร โพธิ์พร้อม. “ปัญหาทางกฎหมายมหาชนบางประการเกี่ยวด้วยการควบคุมการใช้ข่าวสารโดยเครื่องคอมพิวเตอร์.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2529.

กิตติพงศ์ กมลธรรมวงศ์ . “การคุ้มครองข้อมูลข่าวสารส่วนบุคคลในระบบกฎหมายไทย : ปัญหาและแนวทางการแก้ไข” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ , 2548.

กิตติพันธุ์ เกียรติสุนทร. “มาตรการทางอาญาในการคุ้มครองข้อมูลส่วนบุคคล.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2538.

กมลา สุวรรณธรรมา. “ความคิดเห็นเกี่ยวกับสิทธิในการรับรู้และสิทธิส่วนบุคคลและอิทธิพลของภาพลักษณ์ต่อการประเมินเหตุการณ์ละเมิดสิทธิส่วนบุคคล.” วิทยานิพนธ์นิเทศศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2538.

ชื่นอารี มาลีศรีประเสริฐ. “การคุ้มครองสิทธิส่วนตัวกับสื่อสารสนเทศ.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2539.

ชูชีพ ปิณฑะศิริ. “การละเมิดสิทธิส่วนตัว.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2525.

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

นพรัตน์ สนั่นพานิชกุล. “สิทธิอย่างใดอย่างหนึ่งตามบทบัญญัติมาตรา 420.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2538.

ปฏิวัติ อุ่นเรือน. “ปัญหาการคุ้มครองข้อมูลส่วนบุคคลในการโอนข้อมูลระหว่างประเทศ.” สารนิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2547.

มณฑนา สีตสุวรรณ. “การกระทำของมนุษย์บนอินเตอร์เน็ตที่เป็นภัยต่อมนุษย์ในสังคม: แนวคิดและการจัดการ.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2546.

วีรพงษ์ บึงไกร. “การเปิดเผยข้อมูลข่าวสารส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2543.

ศิริกุล ภู่พันธ์. “ข้อความคิดว่าด้วยข้อมูลข่าวสารส่วนบุคคล” วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

ศศิพร ต่ายคำ. “การศึกษาเปรียบเทียบกรณีที่ปกปิด และเปิดเผยข้อมูลข่าวสารตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540, วิทยานิพนธ์นิเทศศาสตร์มหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย, 2543.

หิรัญญา บุญจำรูญ. “สิทธิของประชาชนตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. 2540: กรณีศึกษาปัญหาและอุปสรรคที่ก่อให้เกิดจาการใช้สิทธิอุทธรณ์และร้องเรียน.” สารนิพนธ์สังคมสงเคราะห์ศาสตร์มหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์, 2542.

อังธิดา ลิมป์ปัทมปาณี. “การละเมิดสิทธิส่วนบุคคลของนักหนังสือพิมพ์ต่อนักการเมือง ศิลปิน นักแสดง นักธุรกิจ และประชาชนทั่วไป.” วิทยานิพนธ์นิติศาสตร์มหาบัณฑิตจุฬาลงกรณ์มหาวิทยาลัย, 2540.

เอกอิศร์ ทองเนื้อดี. “การเปิดเผยเอกสารเกี่ยวกับการสอบของรัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.” วิทยานิพนธ์นิติศาสตรมหาบัณฑิตจุฬาลงกรณ์มหาวิทยาลัย, 2543.

<u>เอกสารอื่น ๆ</u>

กิตติศักดิ์ ปรกติ. แนวทางการปฏิบัติงานของ กขร. 41-45., ม.ป.ท., ม.ป.ป.

คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารสาขาสังคม การบริหารราชการแผ่นดินและการบังคับใช้กฎหมาย, คำวินิจฉัยที่ สค.1/2541.

ปทีป เมธาคุณวุฒิ และ อภิรัตน์ เพชรศิริ. “แนวทางในการออกกฎหมายคุ้มครองข้อมูลและสารสนเทศส่วนบุคคลในประเทศไทย.” เสนอต่อสำนักงานคณะกรรมการวิจัยแห่งชาติ, 2539.

สำนักกฎหมาย สำนักงานเลขาธิการวุฒิสภา. เอกสารประกอบการพิจารณาเบื้องต้นร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... . (อัดสำเนา) พฤศจิกายน 2556.

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประมวลกฎหมายแพ่งและพาณิชย์

ประมวลกฎหมายอาญา

มหาวิทยาลัยสุโขทัยธรรมาธิราช. สาขาวิชารัฐศาสตร์ “รายงานการศึกษาวิจัยและพัฒนาองค์ความรู้เกี่ยวกับข้อมูลข่าวสารส่วนบุคคล.” 2545.

มารค ตามไท. เอกสารประกอบการสัมมนาเชิงปฏิบัติการ คณะกรรมการข้อมูลข่าวสารของราชการ. (อัดสำเนา)

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550

รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2557

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....ที่เสนอโดยคณะรัฐมนตรี

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....ที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศฯ

ศูนย์เทคโนโลยีอีเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และ “ร่าง พ.ร.บ.ข้อมูลข่าวสารส่วนบุคคล พ.ศ. ...., เอกสารเผยแพร่โครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศ สำนักงานเลขานุการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, 2544.

สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์. “รายงานการวิจัยโครงการจัดทำความเห็นทางวิชาการเพื่อจัดทำรายงานเกี่ยวกับหลักเกณฑ์และแนวทางการพิจารณาและดำเนินการตามกฎหมายคุ้มครองข้อมูลข่าวสารส่วนบุคคล และจัดทำคู่มือการปฏิบัติงานเกี่ยวกับข้อมูลข่าวสารส่วนบุคคลภาครัฐตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.” 2547.

_____. “รายงานการศึกษาวิจัยฉบับสมบูรณ์ โครงการศึกษาวิจัยเรื่องการคุ้มครองข้อมูลส่วนบุคคลที่จัดเก็บในบัตรประจำตัวแบบอเนกประสงค์ (Smart Card) เสนอต่อสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ, 2549.

สมคิด เลิศไพฑูรย์ . รายงานวิจัยเรื่องกฎหมายข้อมูลข่าวสารทางปกครองของประเทศฝรั่งเศส เสนอ ต่อสำนักงานคณะกรรมการกฤษฎีกา , กรกฎาคม 2545.

Books

Alderman Ellen and Kennedy Caroline. The Right to Privacy. New York: Alfred A. Knopf, 1995.

Birkinshaw Patrick. Citizenship and Privacy: Right of Citizenship. Mansell Publishing, 1993.

Chang Winnie .Practical Guide to Singapore Data Protection Law.Singapore:LexisNexis,2013

Chesterman Simon.Data Protection Law in Singapore. Singapore: Academy Publishing,2014.

Flaherty H. David. Privacy Edition. Privacy and Data Protection: An International Bibliography. Knowledge Industry Publication Inc, 1984.

Littman Mark and Carter-Ruck Peter. Privacy and the Law. Stevens & Sons Limited, 1970.

Miller LeRoy Roger and Jentz A. Caylord. Law for E-Commerce. West Legal Studies in Business, 2002.

Nugter A.C.M., Transborder Flow of Personal Data within the EC: Computer / Law Series. Deventer-Boston: Kluwer Law and Taxation Publishers, 1990.

Passerin d'Entrèves Maurizio and Vogel Ursula, Editor. Public and Private: Legal, political and philosophical perspectives. Routledge, 2000.

Wacks Raymond. Personal Information: Privacy and the Law. Oxford Clarendon Press, 1989.

Wagner Judith. In Pursuit of Privacy Law, Ethic, and the Rise of Technology. Cornell University Press, 1997.

Articles

Kelly Paul. "Recent Development in Private-Sector Personal Data Protection in Australia: Will There be An Upside Down Under?." John Marshall Journal of Computer and Information Law 71 19 (2000).

Murray J. Patrick. "The Adequacy Standard under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?." 21 Fordham International Law Journal 932 (1998).

Schwartz M. Paul. "Privacy and Participation: Personal Information and Public Sector Regulation in the United States." Iowa Law Review 80 IALR (1995).

Shaffer Gregory. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting of U.S. Privacy Standard." 25 Yale Journal of International Law 1 25 (2000).

Turkel Gerald. "The Public/Private distinction: Approaches to the critique of legal Ideology." Law and Society Review 22 LSOCR (1988)

Voss S. Andreas. "The Right to Privacy & Assisted Reproductive Technologies: A Comparative Study of Law Of Germany and the U.S." New York Law Journal of International & Comparative Law Volume 21 (2002).

Other Materials

ANNUAL REPORT PDPC SINGAPORE 2013/2014

APEC Privacy Framework

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

Data Privacy Act of 2012 (Philippines)

Law of The Republic of Indonesia Number 11 of 2008 Electronic Information and Transactions (Indonesia)

Banking Law No.7 of 1992 and The Capital Market Law No. 8 of 1995 contain data privacy provisions. (Indonesia)

Personal Data Protection Act 2010 (Malaysia)

Personal Data Protection Act 2012 (Singapore)

ข้อมูลอิเล็กทรอนิกส์

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (PDPC) www.pdpc.gov.sg

สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ www.oic.go.th

ภาพผนวก

ภาคผนวก ก.
ฐานข้อมูลกฎหมายคุ้มครองข้อมูลส่วนบุคคล ในกลุ่มอาเซียนเพื่อใช้ในการเผยแพร่ของ สขร.

เนื้อหาในส่วนนี้ คณะผู้ศึกษาได้เรียบเรียงขึ้นจากข้อมูลที่ได้ศึกษาตามโครงการนี้เพื่อให้สำนักงานคณะกรรมการข้อมูลข่าวสารของราชการ นำไปไว้ในระบบคอมพิวเตอร์ของสำนักงานเพื่อเป็นการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน

ภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน

ปัจจุบันในปีพ.ศ. 2557 (คศ.2014) หลายประเทศในอาเซียนได้มีการตรากฎหมายที่ใช้ในการคุ้มครองข้อมูลส่วนบุคคลแล้ว ได้แก่ อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ สิงคโปร์[46] ซึ่งเป็นเรื่องที่น่าสนใจว่าหากย้อนกลับไปก่อนปี ค.ศ.2000 ยังไม่มีประเทศใดในอาเซียนที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นการเฉพาะ แต่หากมาถึงในช่วงปีค.ศ. 2010 เป็นต้นมา 4 ประเทศในภูมิภาคนี้คือ อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์ ได้ผ่านกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีความทันสมัย สอดคล้องกับมาตรฐานสากลต่างๆ และประกอบด้วยรายละเอียดชัดเจน โดยเริ่มมีผลบังคับใช้จริงในระยะใกล้เคียงกันคือช่วงปี ค.ศ.2012-2013 ซึ่งต่างก็มุ่งคุ้มครอบข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวม ใช้ และเผยแพร่โดยภาคเอกชน โดยกำหนดมาตรการที่สอดคล้องกับหลักสากล เช่น หลักความยินยอม หลักการแจ้งวัตถุประสงค์ หลักความปลอดภัย โดยเฉพาะมาตรการเกี่ยวกับการส่งข้อมูลไปต่างประเทศ (transfer of data) ต่างมีการจำกัดประเภทของข้อมูลที่สามารถส่งต่อไปต่างประเทศและกำหนดเงื่อนไขให้ต้องได้รับความยินยอมหรือให้มีหลักประกันว่าประเทศปลายทางนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลไม่ด้อยไปกว่าประเทศตน

ประเทศเพื่อนบ้านเหล่านี้ นอกจะมีความสัมพันธ์กับไทยในแง่ของการค้าอย่างมากแล้ว ยังต่างเป็นผู้เล่นที่สำคัญในการพัฒนาระบบเศรษฐกิจและสังคมของภูมิภาคอาเซียนอีกด้วย ประเทศมาเลเซียเป็นกรณีศึกษาที่น่าสนใจ เนื่องจากการผลักดันกฎหมายคุ้มครองข้อมูลส่วนบุคคลนั้นมีความเชื่อมโยงอย่างชัดเจนกับแผนเศรษฐกิจของประเทศที่ต้องการให้มาเลเซียเป็นศูนย์กลางการบริการด้าน

[46]สำหรับประเทศอื่นๆในภูมิภาคอาเซียนมีข้อพิจารณาที่น่าสนใจว่าบางประเทศแม้ยังไม่มีการตรากฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะแต่ก็มีกฎหมายที่มีบทบัญญัติคุ้มครองข้อมูลส่วนบุคคลในบางเรื่อง ได้แก่ ประเทศไทยมีพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ที่บัญญัติการคุ้มครองข้อมูลส่วนบุคคลในภาครัฐ ประเทศเวียดนามในปีค.ศ.2010 ได้มีการประกาศใช้ Law 59 ที่ถือว่าเป็นการคุ้มครองข้อมูลของผู้บริโภค Consumer Rights Protection Law ซึ่งมีผลวันที่ 1 กรกฎาคม 2011 ในประเทศบูรไนมีการคุ้มครองในส่วนกฎหมายทรัพย์สินทางปัญญา เครื่องหมายการค้า กฎหมายลิขสิทธ์ ในส่วนที่เป็นข้อมูลความลับทั่วไปก็ได้รับการคุ้มครองตามหลักกฎหมายCommon Law และหลัก Equity ขณะที่ประเทศในกลุ่มอาเซียนที่ยังไม่มีความคืบหน้าในการเตรียมการออกกฎหมายคือ เมียร์มาร์ ลาวและกัมพูชา

เทคโนโลยีโทรคมนาคม (IT Hub) เห็นได้จากการจัดตั้งองค์กร The Multimedia Development Corporation (MDeC) เพื่อสนับสนุนการพัฒนาของอุตสาหกรรม ICT ตั้งแต่ขนาดกลางและขนาดเล็ก (SMEs) ให้สามารถเติบโตเป็นธุรกิจระดับโลกได้และมีเป้าหมายการแข่งขันกับประเทศในภูมิภาคเช่น สิงคโปร์อย่างชัดเจน นอกจากนี้ยังได้กำหนดให้มีคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Commission) เป็นองค์กรอิสระที่กำกับดูแลการบังคับใช้กฎหมายและออกแนวปฏิบัติ (guidelines) ต่างๆ ด้วย แสดงให้เห็นว่ามีความพยายามของภาครัฐที่จะทำให้กฎและข้อบังคับต่างๆ สามารถบังคับใช้ได้จริง และเป็นไปในทางที่ไม่เป็นอุปสรรคกีดขวางการเจริญเติบโตทางเศรษฐกิจ

หากยกตัวอย่างที่น่าสนใจของการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียนก็จะพบอยู่สองประเทศที่มีความก้าวหน้าอย่างมาก ได้แก่ประเทศมาเลเซียและสิงคโปร์

โดยมาเลเซียอยู่ในระยะเริ่มต้นบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล หน่วยงานต่างๆ โดยเฉพาะภาคเอกชนมีความตื่นตัวในการแลกเปลี่ยนข้อมูลเพื่อหาแนวทางปฏิบัติตามกฎหมายกันอย่างมาก องค์กรในภาคการเงินที่มีมาตรฐานการคุ้มครองข้อมูลค่อนข้างสูงอยู่แล้วเป็นแนวหน้าในการปฏิบัติตามกฎหมายและแบ่งปันแนวปฏิบัติให้ภาคธุรกิจส่วนอื่นๆ ด้วย อนึ่ง แต่เดิมองค์กรที่มีความเชื่อมโยงกับบริษัทในต่างประเทศโดยเฉพาะประเทศใน EU ต่างก็มีแนวปฏิบัติที่เป็นมาตรฐานสากลซึ่งสูงกว่ามาตรฐานใหม่ตามกฎหมายของมาเลเซียอยู่แล้ว เนื่องจากบริษัทเหล่านี้มักจะต้องเพิ่มเติม Standard Contractual Clauses หรือ Binding Corporate Rules เพื่อให้ปฏิบัติตามมาตรฐานของประเทศต้นทางข้อมูลอยู่แล้ว จึงไม่ค่อยมีปัญหาในการปฏิบัติตามกฎหมายใหม่ ข้อสำคัญคือการแบ่งปันความรู้และประสบการณ์ไปสู่ผู้ประกอบการขนาดกลางและขนาดเล็กอื่นๆ ที่เริ่มต้องเกี่ยวข้องกับการรับส่งข้อมูลไปต่างประเทศ

ขณะเดียวกันในประเทศสิงคโปร์ก็นับว่าเป็นประเทศล่าสุดที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพิ่งมีผลบังคับใช้อย่างเป็นทางการเมื่อเดือนกรกฎาคม 2557 ที่ผ่านมาแม้กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสิงคโปร์ (Personal Data Protection Act 2012) จะได้ประกาศใช้ตั้งแต่วันที่ 7 ธันวาคม 2012 แต่การมีผลบังคับใช้กฎหมายทุกบทบัญญัติก็ยังไม่เกิดขึ้นทันที กฎหมายฉบับนี้เพิ่งมีผลบังคับใช้อย่างสมบูรณ์เมื่อวันที่ 2 กรกฎาคม 2014 ที่ผ่านมา ซึ่งจะเห็นได้ว่าระยะเวลาที่หน่วยงานรัฐของสิงคโปร์ได้ใช้เตรียมพร้อมกินเวลานานถึง 18 เดือน ทั้งนี้การใช้เวลานานเช่นนี้มักจะไม่พบในการประกาศใช้กฎหมายของประเทศไทย ซึ่งการให้เวลาเตรียมพร้อมนานขนาดนี้เหตุผลสำคัญของกฎหมาย เห็นว่าเรื่องนี้เป็นเรื่องใหม่ที่กระทบกับองค์กรธุรกิจจำนวนมาก ไม่ใช่เพียงที่ตั้งอยู่ประเทศสิงคโปร์เท่านั้น แต่รวมถึงบริษัทต่างชาติอื่นๆที่อยู่ในต่างประเทศที่อาจมีการส่งต่อข้อมูลจากสิงคโปร์ไปยังประเทศที่สาม ก็ต้องปฏิบัติตามมาตรการของกฎหมายPDPA ด้วย

บรรดากฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มประเทศอาเซียน 4 ประเทศ ที่มีการประกาศใช้กฎหมายแล้ว ได้แก่ประเทศอินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์ มีลักษณะสำคัญที่ร่วมกันดังต่อไปนี้

1. การปฏิบัติตามมาตรฐานสากล (standardization)

เราสามารถสรุปท่าทีของประเทศต่างๆ ในภูมิภาคเอเชียแปซิฟิคต่อการคุ้มครองข้อมูลส่วนบุคคลนั้นเป็นไปในทิศทางเดียวกัน คือจำเป็นต้องมีการยกระดับมาตรฐานการคุ้มครองให้มากขึ้น มิใช่เพื่อรักษาสิทธิของบุคคลเพียงอย่างเดียว แต่การมีมาตรฐานที่ชัดเจนนั้นเป็นการเพิ่มพูนโอกาสทางเศรษฐกิจให้กับเอกชนของประเทศตนด้วย กล่าวคือ ทั้งภาครัฐและเอกชนต่างตระหนักถึงความจำเป็นในการสร้างสมดุล (balance) ระหว่าง “การคุ้มครองความเป็นส่วนตัว (privacy protection)” กับ “การส่งเสริมการเคลื่อนไหวเสรีของข้อมูล (free flow of information)” ซึ่งนำไปสู่ในการการสร้างโอกาสทางการแข่งขันเชิงเศรษฐกิจ เนื่องจากการเพิ่มความไว้วางใจของผู้บริโภคทั้งในประเทศตนเองและในต่างประเทศเป็นกุญแจสำคัญในการเพิ่มขีดความสามารถในการแข่งขันสำหรับธุรกิจที่ต้องจัดการกับข้อมูลส่วนบุคคลจำนวนมาก ไม่ว่าจะเป็นธุรกิจเชิงไอทีที่มีจุดขายอยู่ที่การเคลื่อนย้ายข้อมูลอย่างยืดหยุ่นและเสรี หรือธุรกิจบริการที่เกี่ยวข้องกับการตอบสนองความต้องการของลูกค้ารายคนที่จำเป็นจะต้องล่วงรู้และรักษาข้อมูลที่อาจจะเกี่ยวข้องกับข้อมูลที่เป็นข้อมูลส่วนตัวโดยเฉพาะ (sensitive data) ของลูกค้าด้วย

แม้ว่าแต่ละประเทศต่างมีความจำเป็นในการคุ้มครองข้อมูลส่วนบุคคลต่างๆ กันไปตามสภาพเศรษฐกิจและสังคม ประชากรในแต่ละประเทศก็อาจมีทัศนคติและความไว้วางใจในการเปิดเผยข้อมูลแตกต่างกัน หากแต่ทุกประเทศก็คำนึงถึงความสอดคล้องระหว่างมาตรการภายในประเทศกับมาตรฐานสากล พยายามปรับปรุงให้ระบบการคุ้มครองนั้นมีความทันสมัยอยู่เสมอทั้งในเชิงของกฎหมาย และในเชิงของเทคโนโลยี

2. การคุ้มครองข้อมูลส่วนบุคคลและการพัฒนาทางเศรษฐกิจ

การพัฒนาทางเศรษฐกิจอย่างยั่งยืนจำเป็นจะต้องดำเนินไปโดยคำนึงถึงผลกระทบในด้านอื่นๆ เช่นเดียวกับการลงทุนในภาคอุตสาหกรรมที่ไม่ควรจะต้องแลกมาด้วยการทำลายสภาพแวดล้อม การลงทุนในภาคการบริการที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเพื่อสร้างคุณภาพชีวิตที่ดีขึ้นก็ไม่ควรจะต้องสละแลกกับความเป็นส่วนตัว จนนำมาซึ่งความหวาดระแวงเทคโนโลยีอันไม่จำเป็นและอาจจะกลายเป็นอุปสรรคต่อการพัฒนานวัตกรรมใหม่ๆ ได้

การสร้างมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลในระดับที่ไม่ด้อยไปกว่าประเทศอื่นๆ และสอดคล้องกับมาตรฐานสากลจึงเป็นพื้นฐานที่จำเป็นต่อการพัฒนาธุรกิจบริการในอนาคตให้มีความสามารถแข่งขันกับนานาชาติ นอกจากนี้ยังช่วยสร้างวัฒนธรรมการเคารพสิทธิส่วนบุคคลให้เกิดขึ้นในสังคม รวมทั้งจะช่วยสร้างความตระหนักรู้ในสิทธิที่จะเข้าถึง ปกป้อง และควบคุมข้อมูลส่วนบุคคลของเอกชนให้เกิดขึ้น ทำให้เกิดความเข้าใจระหว่างผู้ประกอบการและผู้บริโภค ลดต้นทุนของผู้ประกอบการในการสร้างภาพเพื่อเรียกความน่าเชื่อถือ และมีความคล่องตัวในการใช้ข้อมูลที่เก็บมาให้เป็นประโยชน์อย่างแท้จริง

3. การยอมรับมาตรฐานสากล และกรอบความร่วมมือระหว่างประเทศ

ปัจจุบัน มีมาตรฐานสากลหลากหลายที่กำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ทั้ง OECD Guidelines ที่ไม่มีผลผูกพันทางกฎหมายแต่มีอิทธิพลต่อการร่างกฎหมายของหลายประเภท และ EU Directive ที่สร้างมาตรฐานอันเคร่งครัดของยุโรปซึ่งส่งผลกระทบให้คู่ค้าของยุโรปต้องเร่งจัดทำกฎเกณฑ์ภายในของตนให้มีมาตรฐานไม่ต่ำกว่าของยุโรปด้วย ขณะเดียวกันก็มีกรอบข้อตกลง APEC Privacy Framework ที่ก็ได้รับกันอย่างกว้างขวาง ซึ่งในกลุ่มประเทศอาเซียนก็ได้นำหลักการที่ยอมรับเป็นสากลเหล่านี้มาบัญญัติไว้ในกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศด้วย

ประเทศทั้งหลายต่างก็ได้ยอมรับเอามาตรฐานการคุ้มครองข้อมูลส่วนบุคคลระหว่างประเทศ มาบัญญัติไว้เป็นเนื้อหาของกฎหมายของประเทศนั้นๆ ซึ่งรูปแบบกฎหมายและขอบเขตการบังคับใช้กฎหมายยังมีความแตกต่างกัน ได้แก่ รูปแบบที่มีลักษณะเป็นกฎหมายกลางใช้ในการคุ้มครองข้อมูลส่วนบุคคลทุกประเภท จะเป็นกฎหมายของประเทศฟิลิปปินส์ มาเลเซียและสิงคโปร์ ขณะที่ประเทศอินโดนีเซียจะมีลักษณะเป็นกฎหมายเฉพาะเรื่อง ในส่วนขอบเขตของการบังคับใช้กฎหมายนั้น ประเทศฟิลิปปินส์จะใช้บังคับกับข้อมูลส่วนบุคคลที่จัดเก็บทั้งในภาครัฐและภาคเอกชน ส่วนประเทศอินโดนีเซีย มาเลเซียและสิงคโปร์ จะใช้บังคับเฉพาะข้อมูลส่วนบุคคลในภาคเอกชน

สำหรับรูปแบบโครงสร้างของกลไกในกฎหมายที่พบส่วนใหญ่ก็จะมีการออกแบบให้มีคณะกรรมการตามกฎหมายเพื่อทำหน้าที่ขับเคลื่อนการบังคับใช้กฎหมาย การกำหนดสิทธิของบุคคลที่จะได้รับการคุ้มครองข้อมูลส่วนบุคคล การกำหนดหลักการคุ้มครองข้อมูลส่วนบุคคล หลักความยินยอมของผู้เป็นเจ้าของข้อมูล ข้อยกเว้นความยินยอม ข้อกำหนดการส่งข้อมูลไปต่างประเทศที่ต้องมีมาตรฐานที่ไม่ต่ำกว่าของประเทศตน การร้องเรียนจากการดำเนินงานขององค์กรธุรกิจซึ่งเป็นผู้ที่มีหน้าที่ต้องปฏิบัติหลักเกณฑ์เงื่อนไขที่ปรากฏอยู่ในกฎหมายและบทลงโทษสำหรับผู้ที่กระทำผิด

ทั้งนี้ภาพรวมของกฎหมายคุ้มครองข้อมูลส่วนบุคคลของอินโดนีเซีย มาเลเซีย ฟิลิปปินส์ และสิงคโปร์สามารถสรุปได้ ดังนี้

ตารางสรุปข้อมูลเกี่ยวกับกฎหมายคุ้มครองข้อมูลส่วนบุคคลในกลุ่มอาเซียน 4ประเทศ

ประเด็น/ประเทศ	อินโดนีเซีย	มาเลเซีย	ฟิลิปปินส์	สิงคโปร์
กฎหมายที่บังคับใช้	กฎหมายที่เกี่ยวข้องกับ data privacy protection ของประเทศอินโดนีเซีย คือ Provision of Electronic System and Transaction ซึ่งมีผลใช้บังคับเมื่อวันที่ 15 ตุลาคม 2555 ซึ่งนอกจากกฎหมายฉบับนี้ดังกล่าวแล้วยังมี กฎหมายอื่น ที่เกี่ยวข้อง เช่น ● Telecommunications Sector ● Public Information Sector ● Banking and Capital Market Sector	Personal Data Protection Act 2013 (PDPA) ได้มีการประกาศลงในราชกิจจานุเบกษาและมีผลใช้บังคับแล้ว เมื่อวันที่ 15 พฤศจิกายน 2556กฎหมายฉบับนี้ใช้บังคับกับหน่วยงานของรัฐบาล	Data Privacy Act of 2012 มีผลใช้บังคับเมื่อวันที่ 8 กันยายน 2555	สิงคโปร์มี Personal Data Protection Act 2012 (No 26 0f 2012) เรียกโดยย่อว่า PDPA เป็นกฎหมายที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ในภาคเอกชนซึ่งประกาศใช้เมื่อเดือนธันวาคม 2012 และมีผลบังคับใช้กฎหมายทั้งฉบับเมื่อ 2 กรกฎาคม 2557
คำจำกัดความของข้อมูลส่วนบุคคล (Definition of personal data)	ข้อมูลส่วนบุคคล ซึ่งถูกเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ ถูกต้องตรงตามความจริงเสมอ	-ได้มีการให้คำจำกัดความข้อมูลส่วนบุคคลไว้โดยเน้นในเรื่องของการส่งข้อมูลทางธุรกิจ -มีการกำหนดเรื่องการให้ความยินยอมของเจ้าข้อมูลไว้ว่า ในกรณีที่เจ้าของข้อมูลมีอายุต่ำกว่า 18 ปี ผู้ให้ความยินยอมได้ต้องเป็นผู้ปกครองหรือผู้ดูแลเจ้าของข้อมูลนั้น	ได้มีการกำหนดคำจำกัดความของข้อมูลส่วนบุคคลไว้โดยละเอียด	ข้อมูลส่วนบุคคลตามกฎหมายของประเทศสิงคโปร์นั้นได้มีการให้คำนิยามไว้อย่างกว้างๆว่าคือข้อมูลส่วนบุคคลซึ่งไม่ว่าจริงหรือไม่ โดยสามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าจะจากข้อมูลๆ เอง หรือจากข้อมูลอื่นๆ ที่นำมาประกอบกัน

ประเด็น/ประเทศ	อินโดนีเซีย	มาเลเซีย	ฟิลิปปินส์	สิงคโปร์
คำจำกัดความของข้อมูลส่วนตัวโดยเฉพาะ (Definition of sensitive data)	ยังมิได้มีการให้คำจำกัดความไว้ในกฎหมายฉบับนี้	มีการให้คำนิยามของ ข้อมูลส่วนบุคคลโดยเฉพาะ (sensitive data) หมายถึง ข้อมูลส่วนบุคคลซึ่งประกอบไปด้วยข้อมูลที่เกี่ยวข้องกับสุขภาพ (ร่างกาย,จิตใจ) ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา หรือความเชื่ออื่นๆ	มีการให้คำจำกัดความของข้อมูลส่วนตัวโดยเฉพาะไว้ว่าเป็นข้อมูลส่วนบุคคลซึ่งเกี่ยวกับเชื้อชาติ สถานะ อายุ ศาสนา ความคิดเห็นทางการเมือง ประวัติสุขภาพหรือพฤติกรรมทางเพศ หรือข้อมูลอื่นๆที่หน่วยงานชองรัฐเป็นผู้กำหนดเพิ่มเติม	ไม่ได้มีให้คำนิยามของข้อมูลส่วนตัวโดยเฉพาะไว้ในกฎหมายฉบับนี้
หน่วยงานที่รับผิดชอบในการปฏิบัติตามหลักกฎหมายนี้	มิได้มีการกำหนดหน่วยงานที่รับผิดชอบ	ปัจจุบันมี Abu Hassan bin Ismail เป็น Personal Data Protection Commissioner	ตามกฎหมายฉบับนี้ได้มีการกำหนดให้มีการจัดตั้งคณะกรรมการดูแลข้อมูลส่วนบุคคลแห่งชาติ แต่ปัจจุบันยังมิได้มีการจัดตั้งขึ้น	กฎหมายของสิงคโปร์กำหนดให้แต่ละองค์กรมีผู้ดูแล/ควบคุมข้อมูลส่วนบุคคล โดยมีหน้าที่ดูแลรับผิดชอบการดำเนินการต่างๆที่เกี่ยวข้องกับข้อมูลส่วนบุคคลขององค์กรนั้นๆ ว่าเป็นไปตามที่กฎหมายกำหนดหรือไม่

ประเด็น/ประเทศ	อินโดนีเซีย	มาเลเซีย	ฟิลิปปินส์	สิงคโปร์
การเก็บและการใช้ข้อมูลส่วนบุคคลตามกฎหมาย	ผู้ดำเนินการ (data controller) สามารถเก็บและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลได้ภายใต้เงื่อนไขดังต่อไปนี้ เช่น ●เจ้าของข้อมูลให้ความยินยอม ●ผู้ดำเนินการจัดเก็บข้อมูลตามหลักเกณฑ์ที่กฎหมายกำหนด ●เป็นการจัดเก็บข้อมูลตามที่กฎหมายหรือรัฐบาลของประเทศอินโดนีเซียกำหนดและ/หรือเพื่อประโยชน์สาธารณะ	ผู้ดำเนินการ (data controller) มีหน้าที่ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยในการจัดเก็บข้อมูล	การเก็บและใช้ข้อมูลต้องเป็นไปตามหลักการทั่วไปของข้อมูลส่วนบุคคล a ต้องมีการแจ้งถึงวัตถุประสงค์ของการจัดเก็บข้อมูลก่อนหรือเร็วที่สุดเท่าที่จะทำได้แก่เจ้าของของข้อมูล b การดำเนินการต่างๆ ต้องเป็นไปด้วยชอบด้วยกฎหมาย c ….. นอกจากนี้แล้ว การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลต้องเป็นไปตามเงื่อนไขที่กำหนด มิเช่นนั้น ก็จะต้องห้ามมิให้มีการดำเนินการดังกล่าว a ต้องได้รับความยินยอมจากเจ้าของข้อมูล ….. d การจัดเก็บข้อมูลมีความจำเป็นเพื่อปกป้องชีวิต หรือสุขภาพของเจ้าของข้อมูล ตามกฎหมายของประเทศฟิลิปฟินส์ ห้ามมิให้มีการจัดเก็บข้อมูลส่วนตัวโดยเฉพาะ (sensitive data) เว้นแต่กรณีดังต่อไปนี้	กำหนดให้แต่ละองค์กรเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคลได้ในกรณีที่ -มีการให้ความยินยอมโดยเจ้าของข้อมูลก่อนดำเนินการใดๆ -เจ้าของข้อมูลสามารถปฏิเสธหรือยกเลิกความยินยอมได้หากมีเหตุผลจำเป็น

ประเด็น/ประเทศ	อินโดนีเซีย	มาเลเซีย	ฟิลิปปินส์	สิงคโปร์
			a เจ้าของข้อมูลได้ให้ความยินยอมก่อนการจัดเก็บข้อมูลและมีการแจ้งถึงวัตถุประสงค์ในการจัดเก็บข้อมูลอย่างชัดเจน .... c ในกรณีที่เจ้าของข้อมูลไม่มีสิทธิหรือไม่สามารถแสดงออกซึ่งความยินยอมได้ แต่จำเป็นต้องดำเนินการกับข้อมูลเพื่อปกป้องชีวิต สุขภาพของเจ้าของข้อมูล หรือบุคคลอื่น	
การส่งข้อมูล(Transfer)	ในกรณีที่มีการส่งข้อมูลทางอิเล็กทรอนิกส์ที่หรือเอกสารอิเล็กทรอนิกส์ ผู้ให้บริการ (provider) ต้องอธิบายให้ผู้ดำเนินการ (data controller) และผู้ครอบครองข้อมูลทราบว่ามีการส่งข้อมูล		การส่งข้อมูลส่วนบุคคลนั้นสามารถกระทำได้ตามกฎหมายของประเทศฟิลิปฟินส์ แต่ผู้ดำเนินการ (data controller) ยังคงมีหน้าที่รับผิดชอบข้อมูลซึ่งอยู่ในความดูแลของตนในกรณีที่มีการส่งข้อมูลไปยังหน่วยงานอื่น อย่างไรก็ดี ข้อมูลส่วนตัวโดยเฉพาะนั้นกฎหมายห้ามมิให้มีการส่งต่อข้อมูลในส่วนนี้ไม่ว่ากรณีใดๆ	การส่งข้อมูลออกไปยังประเทศอื่นนั้นสามารถกระทำได้หากองค์กร (ผู้ดูแลข้อมูล) สามารถพิสูจน์ได้ว่าประเทศอื่นที่มีการส่งออกข้อมูลนั้นมีมาตรฐานด้านความปลอดภัยเทียบเท่าหรือสูงกว่าสิงคโปร์

ประเด็น/ประเทศ	อินโดนีเซีย	มาเลเซีย	ฟิลิปปินส์	สิงคโปร์
การบังคับใช้ (Enforcement)	บทลงโทษกรณีที่มีการไม่ปฏิบัติตามกฎหมาย คือ มีการกำหนดโทษปรับ และหากมีการพิสูจน์ได้ว่าการฝ่าฝืนกฎหมายนั้นมีขึ้นด้วยความตั้งใจ ผู้กระทำผิดอาจได้รับโทษถึงจำคุก	ตามกฎหมายฉบับนี้ อนุญาตให้เจ้าของข้อมูลยกเลิกความยินยอมให้การจัดเก็บข้อมูลได้ซึ่งหากผู้ดำเนินการฝ่าฝืนอาจได้รับโทษปรับเป็นเงินถึง RM 100,000 หรือต้องโทษจำคุกเป็นไม่เกิน 1 ปี หรือทั้งจำทั้งปรับ	คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ตรวจสอบว่าผู้ควบคุมดำเนินการตามกฎหมายหรือไม่ อย่างไรก็ดีคณะกรรมการฯ ไม่สามารถฟ้องร้องหรือดำเนินคดีกับผู้ควบคุมข้อมูลได้เอง ในกรณีนี้เป็นหน้าที่ของกระทรวงยุติธรรมในการดำเนินการ	การบังคับใช้กฎหมายนั้น เป็นหน้าที่ของคณะกรรมการโดยที่คณะกรรมการมีอำนาจดังต่อไปนี้ - สั่งให้หยุดการเก็บ การใช้ การเปิดเผยข้อมูล ส่วนบุคคลหากพบการกระทำที่ฝ่าฝืนต่อบทบัญญัติของกฎหมาย - ทำลายข้อมูลส่วนบุคคลที่มีการเก็บไว้โดยฝ่าฝืนต่อกฎหมาย
การรักษาความปลอดภัยของข้อมูล (Security)			ผู้ดำเนินการต้องจัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลทั้งทางด้านกายภาพและด้านเทคนิค รวมทั้งต้องมีมาตรการรักษาความปลอดภัยจากอุบัติภัยและการเข้าใช้ข้อมูลโดยผิดกฎหมาย และที่สำคัญคือต้องมีมาตรการรักษาความปลอดภัยตามที่คณะกรรมการกำหนด	องค์กรมีหน้าที่ในการรักษาความปลอดภัยของข้อมูลที่อยู่ในความครอบครอง ทั้งนี้ตามกฎหมายของสิงคโปร์ไม่ได้มีการกำหนดมาตรการด้านความปลอดภัยไว้เป็นพิเศษ จึงเป็นหน้าที่ขององค์กรที่ต้องจัดให้มีมาตรการในการรักษาความปลอดภัยที่เหมาะสม

ประเด็น/ประเทศ	อินโดนีเซีย	มาเลเซีย	ฟิลิปปินส์	สิงคโปร์
การแจ้งว่ามีการกระทำผิด (Breach of notification) อื่นๆ		ตามกฎหมายฉบับนี้กำหนดให้ผู้ครอบครองข้อมูลต่างๆ ต่อไปนี้จดทะเบียน(มีใบอนุญาตในการดำเนินการ) เช่น -องค์กรที่เกี่ยวข้องกับการสื่อสาร -ธนาคารและสถาบันทางการเงิน -ธุรกิจประกันภัย -ธุรกิจที่เกี่ยวข้องกับสุขภาพ -การศึกษา -การขายตรง	ผู้ควบคุมต้องแจ้งให้คณะกรรมการข้อมูลส่วนบุคคลทราบทันทีเมื่อพบว่ามีการกระทำความผิดเกี่ยวกับข้อมูลส่วนบุคคล หรือมีเหตุอันควรเชื่อได้มีการกระทำผิดดังกล่าว	

ภาพผนวก ข.
กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศสมาชิกอาเซียน ที่เป็นกรณีศึกษา

1. Law of The Republic of Indonesia Number 11 of 2008 Electronic Information and Transactions (Indonesia)

2. Personal Data Protection Act 2010 (Malaysia)

3. Data Privacy Act of 2012 (Philippines)

4. Personal Data Protection Act 2012 (Singapore)

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008
TENTANG
INFORMASI DAN TRANSAKSI ELEKTRONIK

LAW OF THE REPUBLIC OF INDONESIA
NUMBER 11 OF 2008
CONCERNING
ELECTRONIC INFORMATION AND TRANSACTIONS

Daftar Isi / Table of Contents

	Pasal / Article	
Bab I: Ketentuan Umum	1 – 2	Chap. I: General Provisions
Bab II: Asas dan Tujuan	3 – 4	Chap. II: Principles and Objectives
Bab III: Informasi, Dokumen, dan Tanda Tangan Elektronik	5 – 12	Chap. III: Electronic Information, Records, and Signatures
Bab IV: Penyelenggaraan Sertifikasi Elektronik dan Sistem Elektronik	13 – 16	Chap. IV: Provision of Electronic Certification and Electronic Systems
Bab V: Transaksi Elektronik	17 – 22	Chap. V: Electronic Transactions
Bab VI: Nama Domain, Hak Kekayaan Intelektual dan Perlindungan Hak Pribadi	23 – 26	Chap. VI: Domain Names, Intellectual Property Rights and Protection of Privacy Rights
Bab VII: Perbuatan Yang Dilarang	27 – 37	Chap. VII: Prohibited Acts
Bab VIII: Penyelesaian Sengketa	38 – 39	Chap. VIII: Dispute Resolution
Bab IX: Peran Pemerintah dan Peran Masyarakat	40 – 41	Chap. IX: Role of the Government and Role of the Public
Bab X: Penyidikan	42 – 44	Chap. X: Investigation
Bab XI: Ketentuan Pidana	45 – 52	Chap. XI: Penal Provisions
Bab XII: Ketentuan Peralihan	53	Chap. XII: Transitional Provisions
Bab XIII: Ketentuan Penutup	54	Chap. XIII: Concluding Provisions

Please note that the format of this text differs from the official text. For example, in this version, the elucidation of the law is placed right below the respective articles, which is, in the official version, placed separately after the text of the law (or as a supplement). This version is intended as a convenience for the readers and not a substitute for the official text.

Translated by Wishnu Basuki (ABNR)
wbasuki@abnrlaw.com

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 11 TAHUN 2008
TENTANG
INFORMASI DAN TRANSAKSI ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang:

a. bahwa pembangunan nasional adalah suatu proses yang berkelanjutan yang harus senantiasa tanggap terhadap berbagai dinamika yang terjadi di masyarakat;

b. bahwa globalisasi informasi telah menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia sehingga mengharuskan dibentuknya pengaturan mengenai pengelolaan informasi dan Transaksi Elektronik di tingkat nasional sehingga pembangunan Teknologi Informasi dapat dilakukan secara optimal, merata, dan menyebar ke seluruh lapisan masyarakat guna mencerdaskan kehidupan bangsa;

c. bahwa perkembangan dan kemajuan Teknologi Informasi yang demikian pesat telah menyebabkan perubahan kegiatan kehidupan manusia dalam berbagai bidang yang secara langsung telah memengaruhi lahirnya bentuk-bentuk perbuatan hukum baru;

d. bahwa penggunaan dan pemanfaatan Teknologi Informasi harus terus dikembangkan untuk menjaga, memelihara, dan memperkukuh persatuan dan kesatuan nasional berdasarkan peraturan perundang-undangan demi kepentingan nasional;

e. bahwa pemanfaatan Teknologi Informasi berperan penting dalam perdagangan dan pertumbuhan perekonomian nasional untuk mewujudkan kesejahteraan masyarakat;

f. bahwa Pemerintah perlu mendukung pengembangan Teknologi Informasi melalui infrastruktur hukum dan pengaturannya

LAW OF THE REPUBLIC OF INDONESIA
NUMBER 11 OF 2008
CONCERNING
ELECTRONIC INFORMATION AND TRANSACTIONS

WITH THE BLESSING OF GOD ALMIGHTY

THE PRESIDENT OF THE REPUBLIC OF INDONESIA,

Considering:

a. that the national development is a sustainable process that should at all times be responsive to the varying dynamics among the public;

b. that globalization of information has placed Indonesia as part of the world's information community, therefore the making of regulation concerning organization of Electronic Information and transactions at the national level is required in order that the development of Information Technology can be carried out in an optimal, distributive, and widespread manner throughout all levels of society to advance the intellectual life of the people;

c. that the very rapid development and advance of Information Technology have contributed to changes in the people's life activities in the various fields that have had direct effect on the emergence of new forms of legal acts;

d. that the use and usage of Information Technology must continuously be developed to foster, maintain, and strengthen the national union and unity under laws and regulations in the national interest;

e. that usage of Information Technology has important role in national trade and economic growth in order to achieve public prosperity;

f. that the Government of necessity supports the development of Information Technology through infrastructure of law and its regulation

sehingga pemanfaatan Teknologi Informasi dilakukan secara aman untuk mencegah penyalahgunaannya dengan memperhatikan nilai-nilai agama dan sosial budaya masyarakat Indonesia;

g. bahwa berdasarkan pertimbangan-pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, huruf d, huruf e, dan huruf f perlu membentuk Undang-undang tentang Informasi dan Transaksi Elektronik.

Mengingat:
Pasal 5 ayat (1) dan Pasal 20 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

Dengan Persetujuan Bersama
DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA
dan
PRESIDEN REPUBLIK INDONESIA

MEMUTUSKAN:

Menetapkan: UNDANG-UNDANG TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK.

PENJELASAN UMUM

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum siber atau hukum telematika. Hukum siber atau cyber law secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi (law of information technology), hukum dunia maya

in order that the Information Technology usage is carried out securely to prevent its misuse with due regard to religious and social-cultural values of the Indonesian society;

g. that based on consideration as intended by point a, point b, point c, point d, point e, and point f, it is necessary to make Law concerning Electronic Information and Transactions.

Bearing in Mind:
Article 5 section (1) and Article 20 of the 1945 Constitution of the Republic of Indonesia;

With the Joint Consent of
THE HOUSE OF REPRESENTATIVES OF
THE REPUBLIC OF INDONESIA
and
THE PRESIDENT OF THE REPUBLIC OF INDONESIA

HAS DECIDED:

To enact: LAW CONCERNING ELECTRONIC INFORMATION AND TRANSACTIONS.

GENERAL ELUCIDATION

Usage of Information Technology, media, and communications has globally changed both public behavior and human civilization. The development of information technology and communications has also contributed to the borderlessness of world connection and has significantly made social, economic, and cultural changes rapidly. Today, Information Technology becomes a double-edged sword, that is, to give contributions to the improvement of human welfare, advance, and civilization, and at the same time, becomes effective means for unlawful acts.

Today, a regime of a new law is born, known as hukum siber *or telematics law.* Hukum siber *or cyber law is internationally used as a legal term concerning the usage of information technology and communications. Likewise, telematics law is the embodiment of the convergence of telecommunications law, media law, and informatics law. Other terms also used are* hukum teknologi informasi *(law of information technology),* hukum dunia maya *(virtual world law) and* hukum mayantara. *Such terms were*

(virtual world law) dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

coined after activities carried out through computer system networks and communications systems in the scope of both local and global (Internet) by taking advantage of computer system-based information technology that constitutes virtually-visible electronic systems. Legal issues frequently faced are when those involve the conveyance of information, communications, and/or transactions in an electronic manner, especially a matter of proof and matters that concern legal acts committed via electronic means.

Yang dimaksud dengan sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut.

Electronic systems mean computer systems in a broad sense that include not only computer hardware and software, but also telecommunications networks and/or electronic communications systems. Software or a computer program is a collection of instructions embodied in the form of language, code, scheme, or other forms when interfaced with computer-readable media is able to make computers work to execute special functions or to deliver special results, including preparation in writing such instructions.

Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi input, process, output, storage, dan communication.

Electronic systems are also used to explain the existence of information systems that constitute application of telecommunications network-based information technology and electronic media, functioning to write, process, analyze, display, and send or distribute electronic information. Technically or in management respect, information systems are in effect the embodiment of application of information technology products in some form of organization and management fitting the typical needs within such organization and conforming to the purpose of the functions. On the other hand, technically and functionally speaking, information systems are an integrated system between human and machines with hardware components, software, procedures, human resources, and substance of information that in their usage include functions of input, process, output, storage, and communications.

Sehubungan dengan itu, dunia hukum sebenarnya sudah sejak lama memperluas penafsiran asas dan normanya ketika menghadapi persoalan kebendaan yang tidak berwujud, misalnya dalam kasus pencurian listrik sebagai perbuatan pidana. Dalam kenyataan kegiatan siber tidak lagi sederhana karena kegiatannya tidak lagi dibatasi oleh teritori suatu negara, yang mudah diakses kapanpun dan dari manapun. Kerugian dapat terjadi baik pada pelaku transaksi maupun pada orang lain yang tidak pernah melakukan transaksi, misalnya pencurian dana kartu kredit melalui pembelanjaan di Internet. Di samping itu, pembuktian merupakan faktor yang sangat penting, mengingat informasi elektronik bukan saja belum terakomodasi dalam sistem hukum acara Indonesia secara komprehensif, melainkan juga ternyata sangat rentan untuk diubah, disadap, dipalsukan dan dikirim ke berbagai penjuru dunia dalam waktu hitungan detik. Dengan demikian, dampak yang diakibatkannyapun bisa demikian kompleks dan rumit.

As aforesaid, it is true the world of law has long since broadened its interpretation of principles and values when facing intangible issues, for example, the criminalization of electricity theft. Facts of cyber activities are no longer that simple in that such activities can no longer be bordered by a state's territory, the Access to which is easily made at any time and from wherever. Loss may be sustained by both transacting actors and other persons who never enter transactions, for example, credit card frauds by internet shopping. In addition, proof is a crucial factor since not only has electronic information been unaccommodated comprehensively by the Indonesian law of civil procedure, but in fact, also vulnerable to alteration, interception, forge and transmission to various places worldwide in second. So, the impacts as consequence may be very complex and complicated.

*Permasalahan yang lebih luas terjadi pada bidang keperdataan karena transaksi elektronik untuk kegiatan perdagangan melalui sistem elektronik (*electronic commerce*) telah menjadi bagian dari perniagaan nasional dan internasional. Kenyataan ini menunjukkan bahwa konvergensi di bidang teknologi informasi, media, dan informatika (telematika) berkembang terus tanpa dapat dibendung, seiring dengan ditemukannya perkembangan baru di bidang teknologi informasi, media, dan komunikasi.*

Broader issues also appear in the private sphere in which electronic transactions for trade via electronic systems (electronic commerce) have made a part of national and international trade. This fact shows that the convergence in the field of information technology, media, and informatics (telematics), inevitably, keeps developing in line with the invention in the field of information technology, media, and communications.

*Kegiatan melalui media sistem elektronik, yang disebut juga ruang siber (*cyber space*), meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada ruang siber tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam ruang siber adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.*

Activities via electronic media systems also called cyber (cyberspace), despite being virtual, can be categorized as actual legal acts and actions. Speaking judicially, activities in cyberspace cannot be approached by parameters and qualifications of conventional law only, and if adopted such conventional method, it is too complicated and many would evade the law. Activities in cyberspace are virtual activities that have actual impacts even if the means of proof is electronic in nature.

Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai Orang yang telah melakukan perbuatan hukum secara nyata. Dalam kegiatan e-commerce *antara lain dikenal adanya dokumen elektronik yang kedudukannya*

Therefore, the subject actor must be qualified as a Person who has committed an actual legal act. In e-commerce activities, there are such things known as, inter alia, electronic records, the position of which is held equivalent to documents

disetarakan dengan dokumen yang dibuat di atas kertas.

Berkaitan dengan hal itu, perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, terdapat tiga pendekatan untuk menjaga keamanan di cyber space, yaitu pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Undang-Undang ini yang dimaksud dengan:

1. "Informasi Elektronik" adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI) surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya..
2. "Transaksi Elektronik" adalah perbuatan hukum yang dilakukan dengan menggunakan Komputer, jaringan Komputer, dan/atau media elektronik lainnya.
3. "Teknologi Informasi" adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
4. "Dokumen Elektronik" adalah setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang

made on paper.

In connection therewith, attention to security and legal certainy in the usage of information technology, media, and communications is necessary to be paid in order to develop in an optimal manner. There are accordingly three approaches to maintain cyberspace security, i.e., approaches of legal aspect, technological aspect, and social, cultural, and ethics aspect. To address security threats in the provision of electronic systems, a legal approach is absolute since without legal certainty the problems of the usage of information technology cannot be addressed optimally.

CHAPTER I
GENERAL PROVISIONS
Article 1

In this Law:

1. "Electronic Information" means one cluster or clusters of electronic data, including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them.
2. "Electronic Transaction" means a legal act that is committed by the use of Computers, Computer networks, and/or other electronic media.
3. "Information Technology" means a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information.
4. "Electronic Record" means any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical form, or the like, visible, displayable and/or audible via Computers or Electronic Systems, including but not limited to writings, sounds, images, maps, drafts, photographs or the like, letters, signs, figures, Access Codes, symbols or perforations having certain meaning or

memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

5. "Sistem Elektronik" adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

6. "Penyelenggaraan Sistem Elektronik" adalah pemanfaatan Sistem Elektronik oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.

7. "Jaringan Sistem Elektronik" adalah terhubungnya dua Sistem Elektronik atau lebih, yang bersifat tertutup ataupun terbuka.

8. "Agen Elektronik" adalah perangkat dari suatu Sistem Elektronik yang dibuat untuk melakukan suatu tindakan terhadap suatu Informasi Elektronik tertentu secara otomatis yang diselenggarakan oleh Orang.

9. "Sertifikat Elektronik" adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukan status subyek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.

10. "Penyelenggara Sertifikasi Elektronik" adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.

11. "Lembaga Sertifikasi Keandalan" adalah lembaga independen yang dibentuk oleh profesional yang diakui, disahkan, dan diawasi oleh Pemerintah dengan kewenangan mengaudit dan mengeluarkan sertifikat keandalan dalam Transaksi Elektronik.

12. "Tanda Tangan Elektronik" adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

13. "Penanda Tangan" adalah subyek hukum yang terasosiasikan atau terkait dengan Tanda Tangan Elektronik.

14. "Komputer" adalah alat untuk memproses data elektronik, magnetik, optikal, atau sistem yang melaksanakan fungsi logika, aritmatika, dan

definition or understandable to persons qualified to understand them.

5. "Electronic System" means a set of electronic devices and procedures that functions to prepare, collect, process, analyze, store, display, announce, send, and/or disseminate Electronic Information.

6. "Provision of Electronic System" means an Electronic System usage by the state administrators, Persons, Business Entities, and/or the public.

7. "Electronic System Network" means a closed or open connection of two Electronic Systems or more.

8. "Electronic Agent" means an automated electronic means that is used to initiate an action to certain Electronic Information, which is operated by Persons.

9. "Electronic Certificate" means a certificate in electronic nature that bears an Electronic Signature and identity, demonstrating a status of a legal subject of parties to an Electronic Transaction issued by Certification Service Providers.

10. "Electronic Certification Service Provider" means a legal entity that acts as a reliable party, issues and audits Electronic Certificates.

11. "Trustworthiness Certification Body" means an independent institution that is formed by professionals acknowledged, certified, and supervised by the Government, whose authority is to audit and issue trustworthiness certificates for Electronic Transactions.

12. "Electronic Signature" means a signature that contains Electronic Information that is attached to, associated or linked with other Electronic Information that is used for means of verification and authentication.

13. "Signatory/Signer" means a legal subject associated or linked with an Electronic Signature.

14. "Computer" means an electronic, magnetic, optical data processing device, or a system that performs logic, arithmetic, and storage

penyimpanan.

15. "Akses" adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
16. "Kode Akses" adalah angka, huruf, simbol, karakter lainnya atau kombinasi di antaranya yang merupakan kunci untuk dapat mengakses Komputer dan/atau Sistem Elektronik lainnya.
17. "Kontrak Elektronik" adalah perjanjian para pihak yang dibuat melalui Sistem Elektronik.
18. "Pengirim" adalah subyek hukum yang mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik.
19. "Penerima" adalah subyek hukum yang menerima Informasi Elektronik dan/atau Dokumen Elektronik dari Pengirim.
20. "Nama Domain" adalah alamat internet penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
21. "Orang" adalah orang perseorangan, baik warga negara Indonesia, warga negara asing maupun badan hukum.
22. "Badan Usaha" adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
23. "Pemerintah" adalah Menteri atau pejabat lainnya yang ditunjuk oleh Presiden.

Penjelasan Pasal 1: Cukup jelas

Pasal 2

Undang-Undang ini berlaku untuk setiap Orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Penjelasan Pasal 2:
Undang-Undang ini memiliki jangkauan

functions.

15. "Access" means an activity to make interaction with independent or network Electronic Systems.
16. "Access Code" means a figure, letter, symbol, other character or a combination thereof, which is a key to enable Access to Computers and/or other Electronic Systems.
17. "Electronic Contract" means an agreement of parties entered into by means of Electronic Systems.
18. "Sender/Originator" means a legal subject that sends Electronic Information and/or Electronic Records.
19. "Recipient/Addressee" means a legal subject that receives Electronic Information and/or Electronic Records from Senders/Originators.
20. "Domain Name" means an internet address of a state administrator, Person, Business Entity, and/or the public that can be used for communication over the internet, in the form of unique character code or set to identify a certain location on the internet.
21. "Person" means an individual, whether an Indonesian citizen, foreign citizen, or legal entity.
22. "Business Entity" means a sole proprietorship or partnership of both legal entity and nonlegal entity.
23. "Government" means a Minister(s) or other official(s) the President designates.

Elucidation of Article 1: Sufficiently clear

Article 2

This Law shall apply to any Person who commits legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, having legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia.

Elucidation of Article 2:
Since Information Technology usage for

yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun oleh warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal.

Electronic Information and Electronic Transactions is cross-territorial or universal in nature, this law shall have jurisdiction over legal acts applicable not only in Indonesia and/or committed by Indonesian citizens, but also applicable to legal acts committed outside jurisdiction of Indonesia by both Indonesian citizens and foreign citizens or Indonesian legal entities and foreign legal entities having legal effect in Indonesia.

Yang dimaksud dengan "merugikan kepentingan Indonesia" adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

"Detrimental to the interest of Indonesia" shall include but not limited to detrimental to the interests of national economy, strategic data protection, nation's dignity and degree, state defense and security, sovereignty, citizens as well as Indonesian legal entities.

BAB II
ASAS DAN TUJUAN
Pasal 3

CHAPTER II
PRINCIPLES AND OBJECTIVES
Article 3

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Information Technology and Electronic Transaction usage shall be implemented under the principles of legal certainty, benefit, prudence, good faith, and freedom to choose technology or technology neutrality.

Penjelasan Pasal 3:

Elucidation of Article 3:

"Asas kepastian hukum" berarti landasan hukum bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.

"Principle of legal certainty" means a legal foundation on which Information Technology and Electronic Transaction usage as well as anything that supports its application shall be legally recognized inside and outside the court.

"Asas manfaat" berarti asas bagi pemanfaatan Teknologi Informasi dan Transaksi Elektronik diupayakan untuk mendukung proses berinformasi sehingga dapat meningkatkan kesejahteraan masyarakat.

"Principle of benefit" means a principle that Information Technology and Electronic Transaction usage shall be attempted to support the process of using information in order to enable improvement of public welfare.

"Asas kehati-hatian" berarti landasan bagi pihak yang bersangkutan harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian, baik bagi dirinya maupun pihak lain dalam pemanfaatan Teknologi Informasi dan Transaksi Elektronik.

"Principle of prudence" means a foundation on which the parties concerned must address themselves to any aspect with potential for causing damage to both himself/herself and other party in the usage of Information Technology and Electronic Transactions.

"Asas iktikad baik" berarti asas yang digunakan para pihak dalam melakukan Transaksi Elektronik tidak bertujuan untuk secara sengaja dan tanpa hak atau melawan hukum mengakibatkan kerugian bagi pihak lain tanpa sepengetahuan pihak lain tersebut.

"Asas kebebasan memilih teknologi atau netral teknologi" berarti asas pemanfaatan Teknologi Informasi dan Transaksi Elektronik tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

"Principle of good faith" means a principle that parties to an Electronic Transaction shall not aim at knowingly, without authority or unlawfully causing damage to other parties without the other parties' knowledge.

"Principle of freedom to choose technology or technology neutrality" means a principle that the usage of Information Technology and Electronic Transactions shall not focus on the use of certain technology in order to follow the development of future technology.

Pasal 4

Pemanfaatan Teknologi Informasi dan Transaksi Elektronik dilaksanakan dengan tujuan untuk:

a. mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
b. mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
c. meningkatkan efektifitas dan efisiensi pelayanan publik;
d. membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
e. memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

Penjelasan Pasal 4: Cukup jelas

Article 4

Information Technology and Electronic Transaction usage shall be implemented with the objectives to:

a. advance the intellectual life of the people as part of the world information community;
b. develop the national trade and economy in order to improve public welfare;
c. improve the effectiveness and efficiency of public services;
d. give as wide opportunities as possible to any Person to cultivate his/her insight and capability in the optimal and responsible use and usage of Information Technology; and
d. give senses of security, justice, and legal certainty for Information Technology users and providers.

Elucidation of Article 4: Sufficiently clear

BAB III
INFORMASI, DOKUMEN, DAN TANDA TANGAN ELEKTRONIK

Pasal 5

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

Penjelasan Pasal 5 Ayat (1): Cukup jelas

(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1)

CHAPTER III
ELECTRONIC INFORMATION, RECORDS, AND SIGNATURES

Article 5

(1) Electronic Information and/or Electronic Records and/or the printouts thereof shall be lawful means of proof.

Elucidation of Article 5 Section (1): Sufficiently clear

(2) Electronic Information and/or Electronic Records and/or the printouts thereof as intended by section (1) shall be the expansion

merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Penjelasan Pasal 5 Ayat (2):
Cukup jelas

(3) Informasi Elektronik dan/atau Dokumen Elektronik dinyatakan sah apabila menggunakan Sistem Elektronik sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

Penjelasan Pasal 5 Ayat (3):
Cukup jelas

(4) Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan

Penjelasan Pasal 5 Ayat (4) Huruf a:
Surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Penjelasan Pasal 5 Ayat (4) Huruf b:
Cukup jelas

Pasal 6

Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Penjelasan Pasal 6:
Selama ini bentuk tertulis identik dengan informasi dan/atau dokumen yang tertuang di atas kertas semata, padahal pada hakikatnya informasi dan/atau dokumen dapat dituangkan ke dalam media apa saja, termasuk media

of lawful means of proof in accordance with the Law of Procedure applicable in Indonesia.

Elucidation of Article 5 Section (2):
Sufficiently clear

(3) Electronic Information and/or Electronic Records shall be declared to be lawful if using Electronic Systems in accordance with provisions as governed by this Law.

Elucidation of Article 5 Section (3):
Sufficiently clear

(4) Provisions on Electronic Information and/or Electronic Records as intended by section (1) shall not apply to:

a. certificates that under Laws must be made in writing form; and

Elucidation of Article 5 Section (4) Point a:
Certificates that under laws must be made in writing form shall include but not limited to negotiable instruments, valuable documents, and documents used in the process of law enforcement of civil procedure, criminal procedure, and state administration.

b. certificates together with their papers that under Laws must be made in notarial deed or deed made by land conveyancers.

Elucidation of Article 5 Section (4) Point b:
Sufficiently clear

Article 6

Where other provisions are in place other than those regulated in Article 5 section (4) requiring that information must be in writing or original form, Electronic Information and/or Electronic Records shall be deemed to be lawful to the extent information contained therein is accessible, displayable, assured as to its integrity, and accountable in order to be explanatory.

Elucidation of Article 6:
Until the present, a writing form is identical to information and/or records contained on paper only; in effect, information and/or records can essentialy be inscribed on any medium, including electronic media. Within the context

elektronik. Dalam lingkup Sistem Elektronik, informasi yang asli dengan salinannya tidak relevan lagi untuk dibedakan sebab Sistem Elektronik pada dasarnya beroperasi dengan cara penggandaan yang mengakibatkan informasi yang asli tidak dapat dibedakan lagi dari salinannya.

of Electronic Systems, it is no longer relevant to distinguish the original information from its copies in that Electronic Systems can typically generate copies that make the original information can no longer be distinguished from them.

Pasal 7

Setiap Orang yang menyatakan hak, memperkuat hak yang telah ada, atau menolak hak Orang lain berdasarkan adanya Informasi Elektronik dan/atau Dokumen Elektronik harus memastikan bahwa Informasi Elektronik dan/atau Dokumen Elektronik yang ada padanya berasal dari Sistem Elektronik yang memenuhi syarat berdasarkan Peraturan Perundang-undangan.

Article 7

Any Person who asserts rights, affirms existing rights, or denies other Persons' rights with respect to the existence of Electronic Information and/or Electronic Records must ensure that Electronic Information and/or Electronic Records with him/her originate in Electronic Systems eligible under Laws and Regulations.

Penjelasan Pasal 7:

Ketentuan ini dimaksudkan bahwa suatu Informasi Elektronik dan/atau Dokumen Elektronik dapat digunakan sebagai alasan timbulnya suatu hak.

Elucidation of Article 7:

This provision is intended that Electronic Information and/or Electronic Records may be used as grounds from which rights accrue.

Pasal 8

(1) Kecuali diperjanjikan lain, waktu pengiriman suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik telah dikirim dengan alamat yang benar oleh Pengirim ke suatu Sistem Elektronik yang ditunjuk atau dipergunakan Penerima dan telah memasuki Sistem Elektronik yang berada di luar kendali Pengirim.

(2) Kecuali diperjanjikan lain, waktu penerimaan suatu Informasi Elektronik dan/atau Dokumen Elektronik ditentukan pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik di bawah kendali Penerima yang berhak.

(3) Dalam hal Penerima telah menunjuk suatu Sistem Elektronik tertentu untuk menerima Informasi Elektronik, penerimaan terjadi pada saat Informasi Elektronik dan/atau Dokumen Elektronik memasuki Sistem Elektronik yang ditunjuk.

(4) Dalam hal terdapat dua atau lebih sistem informasi yang digunakan dalam pengiriman atau penerimaan Informasi Elektronik dan/atau

Article 8

(1) Unless agreed otherwise, time of sending of Electronic Information and/or Electronic Records shall be determined at the time the Electronic Information and/or Electronic Records have been sent to the proper address by the Senders/Originators to Electronic Systems the Recipients/Addressees designate or use, and have entered Electronic Systems outside the control of the Senders/Originators.

(2) Unless agreed otherwise, the time of receipt of Electronic Information and/or Electronic Records shall be determined at the time the Electronic Information and/or Electronic Records enter Electronic Systems under the control of the authorized Recipients/ Addressees.

(3) Where Recipients/Addressees have designated certain Electronic Systems to receive Electronic Information, reception shall occur at the time Electronic Information and/or Electronic Records enter designated Electronic Systems.

(4) Where there are two or more information systems used in the sending or reception of Electronic Information and/or Electronic

Dokumen Elektronik, maka:

a. waktu pengiriman adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi pertama yang berada di luar kendali Pengirim.

b. waktu penerimaan adalah ketika Informasi Elektronik dan/atau Dokumen Elektronik memasuki sistem informasi terakhir yang berada di bawah kendali Penerima.

Penjelasan Pasal 8: Cukup jelas

Pasal 9

Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan.

Penjelasan Pasal 9:
Yang dimaksud dengan "informasi yang lengkap dan benar" meliputi:

a. Informasi yang memuat identitas serta status subjek hukum dan kompetensinya, baik sebagai produsen, pemasok, penyelenggara maupun perantara;

b. Informasi lain yang menjelaskan hal tertentu yang menjadi syarat sahnya perjanjian serta menjelaskan barang dan/atau jasa yang ditawarkan, seperti nama, alamat, dan deskripsi barang/jasa.

Pasal 10

(1) Setiap pelaku usaha yang menyelenggarakan Transaksi Elektronik dapat disertifikasi oleh Lembaga Sertifikasi Keandalan.

Penjelasan Pasal 10 Ayat (1):
*Sertifikasi Keandalan dimaksudkan sebagai bukti bahwa pelaku usaha yang melakukan perdagangan secara elektronik layak berusaha setelah melalui penilaian dan audit dari badan yang berwenang. Bukti telah dilakukan Sertifikasi Keandalan ditunjukkan dengan adanya logo sertifikasi berupa trust mark pada laman (*home page*) pelaku usaha tersebut.*

(2) Ketentuan mengenai pembentukan Lembaga Sertifikasi Keandalan sebagaimana dimaksud

Records, then:

a. the time of sending shall be the time when Electronic Information and/or Electronic Records enter a first information system outside the control of the Senders/ Originators.

b. the time of receipt shall be the time when Electronic Information and/or Electronic Records enter a last information system under the control of the Recipients/Addressees.

Elucidation of Article 8: Sufficiently clear

Article 9

Business actors that offer products through Electronic Systems must make available full and true information about contractual conditions, producers, and offered products.

Elucidation of Article 9:
"Full and true information" includes:

a. Information that contains the identity as well as the status of legal subject and its competency, whether as producers, suppliers, providers or intermediaries;

a. Other information that explains certain matters of requirements for validity of agreements, as well as explains offered goods and/or services, such as names, addresses, and descriptions of goods/services;

Article 10

(1) Any business actor who conducts Electronic Transactions may be certified by Trustworthniness Certification Bodies.

Elucidation of Article 10 section (1):
Trustworthiness Certification is intended as proof that business actors conducting trade electronically are eligible to do business upon assessment and audits by authorized bodies. Proof that Trustworthiness Certification has been made shall be demonstrated by a trustmark certification logo on the homepage of the business actor.

(2) Provisions on formation of Trustworthiness Certification Bodies as intended by section (1)

dalam ayat (1) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 10 Ayat (2):
Cukup jelas

Pasal 11

(1) Tanda Tangan Elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

a. data pembuatan Tanda Tangan Elektronik terkait hanya kepada Penanda Tangan;

b. data pembuatan Tanda Tangan Elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa Penanda Tangan;

c. Segala perubahan terhadap Tanda Tangan Elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;

d. Segala perubahan terhadap Informasi Elektronik yang terkait dengan Tanda Tangan Elektronik tersebut setelah waktu penandatanganan dapat diketahui;

e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa Penandatangannya; dan

f. Terdapat cara tertentu untuk menunjukkan bahwa Penanda Tangan telah memberikan persetujuan terhadap Informasi Elektronik yang terkait.

Penjelasan Pasal 11 Ayat (1):
Undang-Undang ini memberikan pengakuan secara tegas bahwa meskipun hanya merupakan suatu kode, Tanda Tangan Elektronik memiliki kedudukan yang sama dengan tanda tangan manual pada umumnya yang memiliki kekuatan hukum dan akibat hukum.
Persyaratan sebagaimana dimaksud dalam Pasal ini merupakan persyaratan minimum yang harus dipenuhi dalam setiap Tanda Tangan Elektronik. Ketentuan ini membuka kesempatan seluas-luasnya kepada siapapun untuk mengembangkan metode, teknik, atau proses pembuatan Tanda Tangan Elektronik.

(2) Ketentuan lebih lanjut mengenai Tanda Tangan Elektronik sebagaimana dimaksud pada ayat

shall be regulated by Government Regulation.

Elucidation of Article 10 section (2):
Sufficiently clear

Article 11

(1) Electronic Signatures shall have lawful legal force and legal effect to the extent satisfying the following requirements:

a. Electronic Signature-creation data shall be associated only with the Signatories/ Signers;

b. Electronic Signature-creation data at the time the electronic signing process shall be only in the power of the Signatories/ Signers;

c. Any alteration in Electronic Signatures that occur after the signing time is knowable;

d. Any alteration in Electronic Information associated with the Electronic Signatures after the signing time is knowable;

e. There are certain methods adopted to identify the identity of the Signatories/ Signers; and

f. There are certain methods to demonstrate that the Signatories/Signers have given consent to the associated Electronic Information;

Elucidation of Article 11 Section (1):
This Law grants recognition definitely that despite codes, Electronic Signatures have an equal position to manual signatures in general, with legal force and legal effect.

The requirements as intended by this Article shall be the requirements that minimally any Electronic Signature must satisfy. This provision gives as wide opportunities as possible to anyone to develop methods, techniques, or process for creating Electronic Signatures.

(2) Further provisions on Electronic Signatures as intended by section (1) shall be regulated by

(1) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 11 Ayat (2):
Peraturan Pemerintah dimaksud, antara lain, mengatur tentang teknik, metode, sarana, dan proses pembuatan Tanda Tangan Elektronik.

Pasal 12

(1) Setiap Orang yang terlibat dalam Tanda Tangan Elektronik berkewajiban memberikan pengamanan atas Tanda Tangan Elektronik yang digunakannya;

(2) Pengamanan Tanda Tangan Elektronik sebagaimana dimaksud pada ayat (1) sekurang-kurangnya meliputi:

a. sistem tidak dapat diakses oleh Orang lain yang tidak berhak;

b. Penanda Tangan harus menerapkan prinsip kehati-hatian untuk menghindari penggunaan secara tidak sah terhadap data terkait pembuatan Tanda Tangan Elektronik;

c. Penanda Tangan harus tanpa menunda-nunda, menggunakan cara yang dianjurkan oleh penyelenggara Tanda Tangan Elektronik ataupun cara lain yang layak dan sepatutnya harus segera memberitahukan kepada seseorang yang oleh Penanda Tangan dianggap memercayai Tanda Tangan Elektronik atau kepada pihak pendukung layanan Tanda Tangan Elektronik jika:

1. Penanda Tangan mengetahui bahwa data pembuatan Tanda Tangan Elektronik telah dibobol; atau

2. keadaan yang diketahui oleh Penanda Tangan dapat menimbulkan risiko yang berarti, kemungkinan akibat bobolnya data pembuatan Tanda Tangan Elektronik; dan

d. dalam hal Sertifikat Elektronik digunakan untuk mendukung Tanda Tangan Elektronik, Penanda Tangan harus memastikan kebenaran dan keutuhan semua informasi yang terkait dengan Sertifikat Elektronik tersebut.

(3) Setiap Orang yang melakukan pelanggaran ketentuan sebagaimana dimaksud pada ayat

Government Regulation.

Elucidation of Article 11 Section (2):
The Government Regulation concerned shall govern, inter alia, techniques, methods, means or process for creating Electronic Signatures.

Article 12

(1) Any Person involved in electronic signing is required to provide security of Electronic Signatures he/she uses;

(2) Security of Electronic Signatures as intended by section (1) shall include at least:

a. the systems are not accessible to unauthorized Persons;

b. the Signatories/Signers must apply the principle of prudence to avoid unauthorized uses of Electronic Signature-creation data;

c. the Signatories/Signers must without delay adopt methods recommended by Electronic Signature providers, or other appropriate methods and should promptly notify Persons whom the Signatories/Signers consider to be relying on the Electronic Signatures or notify parties that support Electronic Signature services if:

1. the Signatories/Signers know that the Electronic Signature-creation data has been compromised; or

2. circumstances known to the Signatories/Signers may pose considerable risks due likely to the compromised Electronic Signature-creation data; and

d. where Electronic Certificates are used to support Electronic Signatures, the Signatories/Signers must confirm the truth and integrity of all information in connection with the Electronic Certificates.

(3) Any Person in violation of the provisions as intended by section (1) shall be responsible for

(1), bertanggung jawab atas segala kerugian dan konsekuensi hukum yang timbul.

Penjelasan Pasal 12: Cukup jelas

any damage and legal consequence incurred.

Elucidation of Article 12: Sufficiently clear

BAB IV
PENYELENGGARAAN SERTIFIKASI ELEKTRONIK DAN SISTEM ELEKTRONIK

Bagian Kesatu
Penyelenggaraan Sertifikasi Elektronik
Pasal 13

(1) Setiap Orang berhak menggunakan jasa Penyelenggara Sertifikasi Elektronik untuk pembuatan Tanda Tangan Elektronik.

(2) Penyelenggara Sertifikasi Elektronik harus memastikan keterkaitan suatu Tanda Tangan Elektronik dengan pemiliknya.

(3) Penyelenggara Sertifikasi Elektronik terdiri atas:

a. Penyelenggara Sertifikasi Elektronik Indonesia; dan

b. Penyelenggara Sertifikasi Elektronik asing.

(4) Penyelenggara Sertifikasi Elektronik Indonesia berbadan hukum Indonesia dan berdomisili di Indonesia.

(5) Penyelenggara Sertifikasi Elektronik asing yang beroperasi di Indonesia harus terdaftar di Indonesia.

(6) Ketentuan lebih lanjut mengenai Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 13: Cukup jelas

CHAPTER IV
PROVISION OF ELECTRONIC CERTIFICATION AND ELECTRONIC SYSTEMS

Part One
Provision of Electronic Certification
Article 13

(1) Any Person shall be entitled to engage the service of Electronic Certification Service Providers for creating Electronic Signatures.

(2) Electronic Certification Service Providers must confirm the attribution of an Electronic Signature to the owner.

(3) Electronic Certification Service Providers shall include:

a. Indonesian Electronic Certification Service Providers; and

b. foreign Electronic Certification Service Providers.

(4) Indonesian Electronic Certification Service Providers shall be an Indonesian legal entity and domiciled in Indonesia.

(5) Foreign Electronic Certification Service Providers that operate in Indonesia must be registered in Indonesia.

(6) Further provisions on Electronic Certification Service Providers as intended by section (3) shall be regulated by Government Regulation.

Elucidation of Article 13: Sufficiently clear

Pasal 14

Penyelenggara Sertifikasi Elektronik sebagaimana dimaksud pada Pasal 13 ayat (1) sampai dengan ayat (5) harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa, yang meliputi:

a. metode yang digunakan untuk mengidentifikasi Penanda Tangan;

b. hal yang dapat digunakan untuk mengetahui data diri pembuatan Tanda Tangan Elektronik;

Article 14

Electronic Certification Service Providers as intended by Article 13 section (1) through section (5) must make available to any service user accurate, clear, and definite information that includes:

a. methods that are adopted to identify the Signatories/Signers;

b. things that can be used to recognize Electronic Signature-creation personal data;

c. hal yang dapat menunjukkan keberlakuan dan keamanan Tanda Tangan Elektronik;

Penjelasan Pasal 14:
Informasi sebagaimana dimaksud dalam Pasal ini adalah informasi yang minimum harus dipenuhi oleh setiap penyelenggara Tanda Tangan Elektronik.

Bagian Kedua
Penyelenggaraan Sistem Elektronik
Pasal 15

(1) Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

Penjelasan Pasal 15 Ayat (1):
"Andal" artinya Sistem Elektronik memiliki kemampuan yang sesuai dengan kebutuhan penggunaannya.
"Aman" artinya Sistem Elektronik terlindungi secara fisik dan nonfisik.

"Beroperasi sebagaimana mestinya" artinya Sistem Elektronik memiliki kemampuan sesuai dengan spesifikasinya.

(2) Penyelenggara Sistem Elektronik bertanggung jawab terhadap Penyelenggaraan Sistem Elektroniknya.

Penjelasan Pasal 15 Ayat (2):
"Bertanggung jawab" artinya ada subjek hukum yang bertanggung jawab secara hukum terhadap Penyelenggaraan Sistem Elektronik tersebut.

(3) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Penjelasan Pasal 15 Ayat (3):
Cukup jelas

Pasal 16

(1) Sepanjang tidak ditentukan lain oleh undang-undang tersendiri, setiap Penyelenggara Sistem Elektronik wajib mengoperasikan Sistem Elektronik yang memenuhi persyaratan minimum sebagai berikut:

c. things that can demonstrate the validity and security of Electronic Signatures;

Elucidation of Article 14:
Information as intended by this Article shall be the information that minimally any Electronic Signature service provider must satisfy.

Part Two
Provision of Electronic Systems
Article 15

(1) Any Electronic System Provider must provide Electronic Systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems.

Elucidation of Article 15 Section (1):
"Reliable" means the Electronic Systems shall have capabilities that match the needs of the users.
"Secure" means the Electronic Systems shall be protected in a physical and nonphysical manner.
"Proper operation" means the Electronic Systems shall have capabilities that match their specifications.

(2) Electronic System providers shall be responsible for their Provision of Electronic Systems.

Elucidation of Article 15 Section (2):
"Responsible" means there shall be legal subjects that are legally responsible for such Provision of Electronic Systems.

(3) The provision as intended by section (2) shall not apply where it is verifiable that there occur compelling circumstances, fault, and/or negligence on the part of the Electronic System users.

Elucidation of Article 15 Section (3):
Sufficiently clear

Article 16

(1) To the extent not provided otherwise by separate laws, any Electronic System Provider is required to operate Electronic Systems in compliance with the following minimal requirements:

a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan, Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;

c. dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelenggaraan Sistem Elektronik tersebut;

d. dilengkapi dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau simbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelenggaraan Sistem Elektronik tersebut; dan

e. memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk;

(2) Ketentuan lebih lanjut tentang Penyelenggaraan Sistem Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 16: Cukup jelas

BAB V
TRANSAKSI ELEKTRONIK
Pasal 17

(1) Penyelenggaraan Transaksi Elektronik dapat dilakukan dalam lingkup publik atau privat.

Penjelasan Pasal 17 Ayat (1):
Undang-Undang ini memberikan peluang terhadap pemanfaatan Teknologi Informasi oleh penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat.
Pemanfaatan Teknologi Informasi harus dilakukan secara baik, bijaksana, bertanggung jawab, efektif, dan efisien agar dapat diperoleh manfaat yang sebesar-besarnya bagi masyarakat.

(2) Para pihak yang melakukan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) wajib beriktikad baik dalam melakukan

a. can redisplay Electronic Information and/or Electronic Records in their entirety in accordance with the retention period as provided for by Laws and Regulations;

b. can protect the availability, entirety, authenticity, confidentiality, and accessibility of Electronic Information in the Provision of Electronic Systems;

c. can operate in compliance with procedures or guidelines for the Provision of Electronic Systems;

d. are furnished with procedures or guidelines that are announced with languages, information, or symbols that are understandable to parties attributed to the Provision of Electronic Systems; and

e. adopt sustainable mechanism in order to maintain updates, clarity, and accountability for the procedures or guidelines;

(2) Further provisions on Provision of Electronic Systems as intended by section (1) shall be regulated by Government Regulation.

Elucidation of Article 16: Sufficiently clear

CHAPTER V
ELECTRONIC TRANSACTIONS
Article 17

(1) Provision of Electronic Transactions may be carried out within a public or private scope.

Elucidation of Article 17 Section (1):
This Law allows opportunities of Information Technology usage to state administrators, Persons, Business Entities, and/or the public.

Information Technology usage must be implemented in a proper, responsible, effective, and efficient manner in order that the public can reap as much benefits as possible.

(2) Parties that conduct Electronic Transactions as intended by section (1) must be in good faith in making interaction and/or exchange

interaksi dan/atau pertukaran Informasi Elektronik dan/atau Dokumen Elektronik selama transaksi berlangsung.

Penjelasan Pasal 17 Ayat (2):
Cukup jelas

(3) Ketentuan lebih lanjut mengenai penyelenggaraan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 17 Ayat (3):
Cukup jelas

Pasal 18

(1) Transaksi Elektronik yang dituangkan ke dalam Kontrak Elektronik mengikat para pihak.

Penjelasan Pasal 18 Ayat (1)
Cukup jelas

(2) Para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi Transaksi Elektronik internasional yang dibuatnya.

Penjelasan Pasal 18 Ayat (2):
Pilihan hukum yang dilakukan oleh para pihak dalam kontrak internasional termasuk yang dilakukan secara elektronik dikenal dengan choice of law. *Hukum ini mengikat sebagai hukum yang berlaku bagi kontrak tersebut.*
Pilihan hukum dalam Transaksi Elektronik hanya dapat dilakukan jika dalam kontraknya terdapat unsur asing dan penerapannya harus sejalan dengan prinsip-prinsip hukum perdata internasional (HPI).

(3) Jika para pihak tidak melakukan pilihan hukum dalam Transaksi Elektronik internasional, hukum yang berlaku didasarkan pada asas Hukum Perdata Internasional.

Penjelasan Pasal 18 Ayat (3):
Dalam hal tidak ada pilihan hukum, penetapan hukum yang berlaku berdasarkan prinsip atau asas hukum perdata internasional yang akan ditetapkan sebagai hukum yang berlaku pada kontrak tersebut.

(4) Para pihak memiliki kewenangan untuk menetapkan forum pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari Transaksi Elektronik

of Electronic Information and/or Electronic Records during the transactions.

Elucidation of Article 17 Section (2):
Sufficiently clear

(3) Further provisions on provision of Electronic Transactions as intended by section (1) shall be regulated by Government Regulation.

Elucidation of Article 17 Section (3):
Sufficiently clear

Article 18

(1) Electronic Transactions that are stated in Electronic Contracts shall bind on parties.

Elucidation of Article 18 Section (1)
Sufficiently clear

(2) Parties shall have the power to choose law applicable to international Electronic Transactions they enter.

Elucidation of Article 18 Section (2):
Pilihan hukum *made by parties in the international contracts, including electronically-made contracts, is known as choice of law. This law shall bind as law applicable to such contracts.*
Choice of law in Electronic Transactions may be made only if the contracts contain foreign elements and their applicability must be in harmony with the principles of the Private International Law.

(3) If parties do not make choice of law in international Electronic Transactions, the applicable law shall be under the principles of the Private International Law.

Elucidation of Article 18 Section (3):
Where there is no choice of law, the law determined applicable to the contracts shall be under the principles or tenets of the private international law.

(4) Parties shall have the powers to determine forums of court, arbitration, or other alternative dispute resolution institutions with jurisdiction to handle disputes that may arise from international Electronic Transactions they

internasional yang dibuatnya.

Penjelasan Pasal 18 Ayat (4):
Forum yang berwenang mengadili sengketa kontrak internasional, termasuk yang dilakukan secara elektronik, adalah forum yang dipilih oleh para pihak. Forum tersebut dapat berbentuk pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya.

(5) Jika para pihak tidak melakukan pilihan forum sebagaimana dimaksud pada ayat (4), penetapan kewenangan pengadilan, arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya yang berwenang menangani sengketa yang mungkin timbul dari transaksi tersebut, didasarkan pada asas Hukum Perdata Internasional.

Penjelasan Pasal 18 Ayat (5):
*Dalam hal para pihak tidak melakukan pilihan forum, kewenangan forum berlaku berdasarkan prinsip atau asas hukum perdata internasional. Asas tersebut dikenal dengan asas tempat tinggal tergugat (*the basis of presence*) dan efektivitas yang menekankan pada tempat harta harta tergugat berada (*principle of effectiveness*).*

Pasal 19

Para pihak yang melakukan Transaksi Elektronik harus menggunakan Sistem Elektronik yang disepakati.

Penjelasan Pasal 19:
Yang dimaksud dengan "disepakati" dalam pasal ini juga mencakup disepakatinya prosedur yang terdapat dalam Sistem Elektronik yang bersangkutan.

Pasal 20

(1) Kecuali ditentukan lain oleh para pihak, Transaksi Elektronik terjadi pada saat penawaran transaksi yang dikirim Pengirim telah diterima dan disetujui Penerima.

Penjelasan Pasal 20 Ayat (1):
*Transaksi Elektronik terjadi pada saat kesepakatan antara para pihak yang dapat berupa, antara lain pengecekan data, identitas, nomor identifikasi pribadi (*personal

enter.

Elucidation of Article 18 Section (4):
Forums with jurisdiction to adjudicate international contract disputes, including electronically-made contracts, shall be forums chosen by parties. Such forums may be in the form of court, arbitration, or other alternative dispute resolution institution.

(5) If parties do not make choice of forum as intended by section (4), the jurisdiction of court, arbitration, or other alternative dispute resolution institution with jurisdiction to handle disputes that may arise from such transactions shall be determined under the principles of the Private International Law.

Elucidation of Article 18 Section (5):
Where parties do not make choice of forum, jurisdiction of forum under the principles of the Private International Law shall apply. Such principles are known as the principle of the residence of the defendants (the basis of presence) and the principle of effectiveness that emphasizes the place of assets of the defendants (principle of effectiveness).

Article 19

Parties that conduct Electronic Transactions must adopt agreed-on Electronic Systems.

Elucidation of Article 19:
"Agreed-on" in this article shall also include agreements with respect to procedures contained in such Electronic Systems.

Article 20

(1) Unless provided otherwise by parties, Electronic Transactions shall occur at the time the transaction offers sent by Senders/Originators have been received and accepted by Recipients/Addressees.

Elucidation of Article 20 Section (1):
Electronic Transactions shall occur at the time of the agreements between parties, which can be in the form of, inter alia, verification of data, identity, personal identification

identification number/PIN*) atau sandi lewat (*password*).*

number/PIN or password.

(2) Persetujuan atas penawaran Transaksi Elektronik sebagaimana dimaksud pada ayat (1) harus dilakukan dengan pernyataan penerimaan secara elektronik.

(2) Acceptance on the Electronic Transaction offers as intended by section (1) must be made with an electronic acknowledgement of receipt.

Penjelasan Pasal 20 Ayat (2):
Cukup jelas

Elucidation of Article 20 Section (2):
Sufficiently clear

Pasal 21

(1) Pengirim atau Penerima dapat melakukan Transaksi Elektronik sendiri, melalui pihak yang dikuasakan olehnya, atau melalui Agen Elektronik.

Article 21

(1) Senders/Originators or Recipients/Addressees may conduct Electronic Transactions in person, or by his/her proxy, or by Electronic Agents.

Penjelasan Pasal 21 Ayat (1):
Yang dimaksud dengan "dikuasakan" dalam ketentuan ini sebaiknya dinyatakan dalam surat kuasa.

Elucidation of Article 21 Section (1):
It is advisable to authorize "proxy" by virtue of a power of attorney.

(2) Pihak yang bertanggung jawab atas segala akibat hukum dalam pelaksanaan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) diatur sebagai berikut:

(2) Parties responsible for any legal effect in the conduct of Electronic Transactions as intended by section (1) shall be regulated as follows:

a. jika dilakukan sendiri, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab para pihak yang bertransaksi;

a. if conducted in person, any legal effect in the conduct of Electronic Transactions shall become the responsibility of parties to a transaction;

b. jika dilakukan melalui pemberian kuasa, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab pemberi kuasa; atau

b. if conducted by proxy, any legal effect in the conduct of Electronic Transactions shall become the responsibility of the grantors of the proxy; or

c. jika dilakukan melalui Agen Elektronik, segala akibat hukum dalam pelaksanaan Transaksi Elektronik menjadi tanggung jawab penyelenggara Agen Elektronik.

c. if conducted by Electronic Agents, any legal effect in the conduct of Electronic Transactions shall become the responsibility of Electronic Agent providers.

Penjelasan Pasal 21 Ayat (2):
Cukup jelas

Elucidation of Article 21 Section (2):
Sufficiently clear

(3) Jika kerugian Transaksi Elektronik disebabkan gagal beroperasinya Agen Elektronik akibat tindakan pihak ketiga secara langsung terhadap Sistem Elektronik, segala akibat hukum menjadi tanggung jawab penyelenggara Agen Elektronik.

(3) If damage of Electronic Transactions is occasioned by failure of the operation of Electronic Agents due to third parties' direct measures against Electronic Systems, any legal effect shall become the responsibility of Electronic Agents.

Penjelasan Pasal 21 Ayat (3):
Cukup jelas

Elucidation of Article 21 Section (3):
Sufficiently clear

(4) Jika kerugian Transaksi Elektronik

(4) If damage of Electronic Transactions is

disebabkan gagal beroperasinya Agen Elektronik akibat kelalaian pihak pengguna jasa layanan, segala akibat hukum menjadi tanggung jawab pengguna jasa layanan.

Penjelasan Pasal 21 Ayat (4):
Cukup jelas

(5) Ketentuan sebagaimana dimaksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna Sistem Elektronik.

Penjelasan Pasal 21 Ayat (5):
Cukup jelas

Pasal 22

(1) Penyelenggara Agen Elektronik tertentu harus menyediakan fitur pada Agen Elektronik yang dioperasikannya yang memungkinkan penggunanya melakukan perubahan informasi yang masih dalam proses transaksi.

Penjelasan Pasal Pasal 22 Ayat (1):
Yang dimaksud dengan "fitur" adalah fasilitas yang memberikan kesempatan kepada pengguna Agen Elektronik untuk melakukan perubahan atas informasi yang disampaikannya, misalnya fasilitas pembatalan (cancel), edit, dan konfirmasi ulang.

(2) Ketentuan lebih lanjut mengenai penyelenggara Agen Elektronik tertentu sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 22 Ayat (2):
Cukup jelas

BAB VI
NAMA DOMAIN, HAK KEKAYAAN INTELEKTUAL, DAN PERLINDUNGAN HAK PRIBADI

Pasal 23

(1) Setiap penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat berhak memiliki Nama Domain berdasarkan prinsip pendaftar pertama.

Penjelasan Pasal 23 Ayat (1):
Nama Domain berupa alamat atau jati diri penyelenggara negara, Orang, Badan Usaha, dan/atau masyarakat, yang perolehannya

occasioned by failure of the operation of Electronic Agents due to negligence of service users, any legal effect shall become the responsibility of the service users.

Elucidation of Article 21 Section (4):
Sufficiently clear

(5) The provision as intended by section (2) shall not apply if provable that there occur compelling circumstances, fault and/or negligence on the part of the Electronic System users.

Elucidation of Article 21 Section (5):
Sufficiently clear

Article 22

(1) Certain Electronic Agent Providers must provide features to Electronic Agents they operate to enable their users to alter information still in the process of transaction.

Elucidation of Article 22 Section (1):
"Features" means facilities that are provided for Electronic Agent users to alter information conveyed to them, for example, facilities: cancel, edit, and confirm.

(2) Further provisions on certain Electronic Agent providers as intended by section (1) shall be regulated by Government Regulation.

Elucidation of Article 22 Section (2):
Sufficiently clear

CHAPTER VI
DOMAIN NAMES, INTELLECTUAL PROPERTY RIGHTS AND PROTECTION OF PRIVACY RIGHTS

Article 23

(1) Any state administrator, Person, Business Entity, and/or the public shall be entitled to hold Domain Names on a first applicant principle basis.

Elucidation of Article 23 Section (1):
Domain Names shall be addresses or identity of state administrators, Persons, Business Entities and/or the public obtained on a first

didasarkan pada prinsip pendaftar pertama (first come first serve).
Prinsip pendaftar pertama berbeda antara ketentuan dalam Nama Domain dan dalam bidang hak kekayaan intelektual karena tidak diperlukan pemeriksaan substantif, seperti pemeriksaan dalam pendaftaran merek dan paten.

applicant principle basis (first-come, first-served).
The first applicant principle in Domain Name policy is different from one in the field of Intellectual Property Rights in that no substantive examination is required while it is in the registration of trademarks and patents.

(2) Pemilikan dan penggunaan Nama Domain sebagaimana dimaksud pada ayat (1) harus didasarkan pada iktikad baik, tidak melanggar prinsip persaingan usaha secara sehat, dan tidak melanggar hak Orang lain.

(2) Holding and use of Domain Names as intended by section (1) must be on the basis of good faith, nonviolation of fair business competition, and noninfringement of the rights of other Persons.

Penjelasan Pasal 23 Ayat (2):
Yang dimaksud dengan "melanggar hak Orang lain", misalnya melanggar merek terdaftar, nama badan hukum terdaftar, nama Orang terkenal, dan sejenisnya yang pada intinya merugikan Orang lain.

Elucidation of Article 23 Section (2):
"Infringement of the rights of other Persons" means, for example, infringement of registered trademarks, registered names of legal entities, names of famous Persons, and the like, in sum, detrimental to other Persons.

(3) Setiap penyelenggara negara, Orang, Badan Usaha, atau masyarakat yang dirugikan karena penggunaan Nama Domain secara tanpa hak oleh Orang lain, berhak mengajukan gugatan pembatalan Nama Domain dimaksud.

(3) Any state administrator, Person, Business Entity, or the public damaged by other Persons' unauthorized use of Domain Names shall be entitled to lodge a claim for canceling such Domain Names.

Penjelasan Pasal 23 Ayat (3):
Yang dimaksud dengan "penggunaan Nama Domain secara tanpa hak" adalah pendaftaran dan penggunaan Nama Domain yang semata-mata ditujukan untuk menghalangi atau menghambat Orang lain untuk menggunakan nama yang intuitif dengan keberadaan nama dirinya atau nama produknya, atau untuk mendompleng reputasi Orang yang sudah terkenal atau ternama, atau untuk menyesatkan konsumen.

Elucidation of Article 23 Section (3):
"Unauthorized use of Domain Names" means registration and use of Domain Names only aimed at inhibiting or preventing other Persons to use a name which is intuitively their proper name or product names, or cashing in on the reputation of famous or well-known Persons, or misleading consumers.

Pasal 24

(1) Pengelola Nama Domain adalah Pemerintah dan/atau masyarakat.

(2) Dalam hal terjadi perselisihan pengelolaan Nama Domain oleh masyarakat, Pemerintah berhak mengambil alih sementara pengelolaan Nama Domain yang diperselisihkan.

(3) Pengelola Nama Domain yang berada di luar wilayah Indonesia dan Nama Domain yang diregistrasinya diakui keberadaannya sepanjang tidak bertentangan dengan Peraturan

Article 24

(1) Domain Name administrators shall be the Government and/or the public.

(2) Where a dispute on Domain Name administration by the public occurs, the Government shall be entitled to take over temporarily the Domain Name administration in dispute.

(3) Domain Name administrators residing outside the territory of Indonesia and Domain Names they have registered shall be recognized as to its existence to the extent not against Laws and

Perundang-undangan.

(4) Ketentuan lebih lanjut mengenai pengelolaan Nama Domain sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 24: Cukup jelas

Pasal 25

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.

Penjelasan Pasal 25:

Informasi Elektronik dan/atau Dokumen Elektronik yang disusun dan didaftarkan sebagai karya intelektual, hak cipta, paten, merek, rahasia dagang, desain industri, dan sejenisnya wajib dilindungi oleh Undang-Undang ini dengan memperhatikan ketentuan Peraturan Perundang-undangan.

Pasal 26

(1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.

Penjelasan Pasal 26 Ayat (1):

*Dalam pemanfaatan Teknologi Informasi, perlindungan data pribadi merupakan salah satu bagian dari hak pribadi (*privacy right*s). Hak pribadi mengandung pengertian sebagai berikut:*

a. Hak pribadi merupakan hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan.
b. Hak pribadi merupakan hak untuk dapat berkomunikasi dengan Orang lain tanpa tindakan memata-matai.
c. Hak pribadi merupakan hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang.

(2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat

Regulations.

(4) Further provisions on Domain Name administration as intended by section (1), section (2), and section (3) shall be regulated by Government Regulation.

Elucidation of Article 24: Sufficiently clear

Article 25

Electronic Information and/or Electronic Records that are created into intellectual works, internet sites, and intellectual works contained therein shall be protected as Intellectual Property Rights under provisions of Laws and Regulations.

Elucidation of Article 25:

Electronic Information and/or Electronic Records created into and registered as intellectual works, copyrights, patents, trademarks, trade secret, industrial designs, and the like must be protected by this Law with due regard to provisions of laws and regulations.

Article 26

Unles provided otherwise by Laws and Regulations, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned.

Elucidation of Article 26 Section (1):

In the usage of Information Technology, personal data shall be a part of the privacy rights to be protected. Privacy rights shall contain the following meaning:

a. A privacy right shall be the right to enjoy personal life and be free from any invasion.
b. A privacy right shall be the right to communicate with other Persons without surveillance.
c. A privacy right shall be the right to inspect access to information about personal life of and data on individuals.

(2) Any Person whose rights are infringed as intended by section (1) may lodge a claim for

mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Penjelasan Pasal 26 Ayat (2):
Cukup jelas

BAB VII
PERBUATAN YANG DILARANG
Pasal 27

(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

(2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Penjelasan Pasal 27: Cukup jelas

Pasal 28

(1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

(2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

Penjelasan Pasal 28: Cukup jelas

Pasal 29

damages incurred under this Law.

Elucidation of Article 26 Section (2):
Suficiently clear

CHAPTER VII
PROHIBITED ACTS
Article 27

(1) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents against propriety.

(2) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of gambling.

(3) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of affronts and/or defamation.

(4) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of extortion and/or threats.

Elucidation of Article 27: Sufficiently clear

Article 28

(1) Any Person who knowingly and without authority disseminates false and misleading information resulting in consumer loss in Electronic Transactions.

(2) Any Person who knowingly and without authority disseminates information aimed at inflicting hatred or dissension on individuals and/or certain groups of community based on ethnic groups, religions, races, and intergroups (SARA).

Elucidation of Article 28: Sufficiently clear

Article 29

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

Penjelasan Pasal 29: Cukup jelas

Pasal 30

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun.

Penjelasan Pasal 30 Ayat (1):
Cukup jelas

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

Penjelasan Pasal 30 Ayat (2):
Secara teknis perbuatan yang dilarang sebagaimana dimaksud pada ayat ini dapat dilakukan, antara lain dengan:

a. melakukan komunikasi, mengirimkan, memancarkan atau sengaja berusaha mewujudkan hal-hal tersebut kepada siapapun yang tidak berhak untuk menerimanya; atau

b. sengaja menghalangi agar informasi dimaksud tidak dapat diterima atau gagal diterima oleh yang berwenang menerimanya di lingkungan pemerintah dan/atau pemerintah daerah.

(3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Penjelasan Pasal 30 Ayat (3):
Sistem pengamanan adalah sistem yang membatasi akses komputer atau melarang akses ke dalam komputer dengan berdasarkan kategorisasi atau klasifikasi pengguna beserta tingkatan kewenangan yang ditentukan.

Any Person who knowingly and without authority sends Electronic Information and/or Electronic Records that contain violence threats or scares aimed personally.

Elucidation of Article 29: Sufficiently clear

Article 30

(1) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems of other Persons in any manner whatsoever.

Elucidation of Article 30 Section (1):
Sufficiently clear

(2) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever with the intent to obtain Electronic Information and/or Electronic Records.

Elucidation of Article 30 Section (2):
Technically, such prohibited acts as intended by this section may be committed through, inter alia:

a. communicating, sending, transmitting or attempting such information to be received by any Person whomsoever unauthorized to receive it; or

b. knowingly inhibiting such information from being received or making it fail to be received by the authorized to receive it within the government and/or regional governments.

(3) Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever by breaching, hacking into, trespassing into, or breaking through security systems.

Elucidation of Article 30 Section (3):
Security systems are systems that restrict access to computers or prohibit access to computers by category or classification of users and specified levels of the authority.

Pasal 31

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.

Penjelasan Pasal 31 Ayat (1):
Yang dimaksud dengan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apapun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Penjelasan Pasal 31 Ayat (2):
Cukup jelas

(3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.

Penjelasan Pasal 31 Ayat (3):
Cukup jelas

(4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 31 Ayat (4):
Cukup jelas

Article 31

(1) Any Person who knowingly and without authority or unlawfully carries out interception or wiretapping of Electronic Information and/or Electronic Records in certain Computers and/or Electronic Systems of other Persons.

Elucidation of Article 31 Section (1):
"Interception or wiretapping" means activities to listen, record, reroute, alter, block, and/or log transmission of nonpublic Electronic Information and/or Electronic Records, whether communications cable networks or wireless networks, such as electromagnetic waves or frequency radio.

(2) Any Person who knowingly and without authority or unlawfully carries out interception of the transmission of nonpublic Electronic Information and/or Electronic Records from, to, and in certain Computers and/or Electronic Systems of other Persons, whether or not causing alteration, deletion, and/or termination of Electronic Information and/or Electronic Records in transmission.

Elucidation of Article 31 Section (2):
Sufficiently clear

(3) Interception excepted from one as intended by section (1) and section (2) shall be interception carried out in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as stated by laws.

Elucidation of Article 31 Section (3):
Sufficiently clear

(4) Further provisions on procedures for interception as intended by section (3) shall be regulated by Government Regulation.

Elucidation of Article 31 Section (4):
Sufficiently clear

Pasal 32

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

Penjelasan Pasal 32: Cukup jelas

Pasal 33

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Penjelasan Pasal 33: Cukup jelas

Pasal 34

(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:

a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi

Article 32

(1) Any Person who knowingly and without authority or unlawfully in any manner whatsoever alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Records of other Persons or of the public.

(2) Any Person who knowingly and without authority or unlawfully in any manner whatsoever, moves or transfers Electronic Information and/or Electronic Records to Electronic Systems of unauthorized Persons.

(3) Acts as intended by section (1) shall be acts that result in any confidential Electronic Information and/or Electronic Record being compromised such that the data becomes accessible to the public in its entirety in an improper manner.

Elucidation of Article 32: Sufficiently clear

Article 33

Any Person who knowingly and without authority or unlawfully commits any act resulting in faults on Electronic Systems and/or resulting in Electronic Systems working improperly.

Elucidation of Article 33: Sufficiently clear

Article 34

(1) Any Person who knowingly and without authority or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns:

a. Computer hardware or software that is designed or specifically developed to facilitate acts as intended by Article 27 through Article 33;

b. Computer passwords, Access Codes, or the like to make Electronic Systems accessible with the intent to facilitate acts as intended by Article 27 through Article 33;

perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.

Penjelasan Pasal 34 Ayat (1):
Cukup jelas

(2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

Penjelasan Pasal 34 Ayat (2):
Yang dimaksud dengan "kegiatan penelitian" adalah penelitian yang dilaksanakan oleh lembaga penelitian yang memiliki izin.

Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Penjelasan Pasal 35: Cukup jelas

Pasal 36

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

Penjelasan Pasal 36: Cukup jelas

Pasal 37

Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Penjelasan Pasal 37: Cukup jelas

BAB VIII
PENYELESAIAN SENGKETA

Pasal 38

(1) Setiap Orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi

Elucidation of Article 34 Section (1):
Sufficiently clear

(2) Acts as intended by section (1) are not criminal acts if aimed at carrying out research activities, testing of Electronic Systems, protection of Electronic Systems themselves in a legal and lawful manner.

Elucidation of Article 34 Section (2):
"Research activities" shall be research that is conducted by authorized research institutions.

Article 35

Any Person who knowingly and without authority or unlawfully manipulates, creates, alters, deletes, tampers with Electronic Information and/or Electronic Records with the intent that such Electronic Information and/or Electronic Records would seem to be authentic data.

Elucidation of Article 35: Sufficiently clear

Article 36

Any Person who knowingly and without authority or unlawfully commits acts as intended by Article 27 through Article 34 to other Persons' detriment.

Elucidation of Article 36: Sufficiently clear

Article 37

Any Person who knowingly commits prohibited acts as intended by Article 27 through Article 36 outside the territory of Indonesia towards Electronic Systems residing within jurisdiction of Indonesia.

Elucidation of Article 37: Sufficiently clear

CHAPTER VIII
DISPUTE RESOLUTION

Article 38

(1) Any Person may institute actions against parties that provide Electronic Systems and/or using Information Technology to his/her

Informasi yang menimbulkan kerugian.

(2) Masyarakat dapat mengajukan gugatan secara perwakilan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang berakibat merugikan masyarakat, sesuai dengan ketentuan Peraturan Perundang-undangan.

Penjelasan Pasal 38: Cukup jelas

Pasal 39

(1) Gugatan perdata dilakukan sesuai dengan ketentuan Peraturan Perundang-undangan.

(2) Selain penyelesaian gugatan perdata sebagaimana dimaksud pada ayat (1), para pihak dapat menyelesaikan sengketa melalui arbitrase, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan Peraturan Perundang-undangan.

Penjelasan Pasal 39: Cukup jelas

BAB IX
PERAN PEMERINTAH DAN PERAN MASYARAKAT

Pasal 40

(1) Pemerintah memfasilitasi pemanfaatan Teknologi Informasi dan Transaksi Elektronik sesuai dengan ketentuan Peraturan Perundang-undangan.

(2) Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum, sesuai dengan ketentuan Peraturan Perundang-undangan.

(3) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi.

(4) Instansi atau institusi sebagaimana dimaksud pada ayat (3) harus membuat Dokumen Elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.

(5) Instansi atau institusi lain selain diatur pada ayat (3) membuat Dokumen Elektronik dan rekam cadang elektroniknya sesuai dengan keperluan perlindungan data yang dimilikinya.

detriment.

(2) The public in accordance with provisions of laws and regulations may bring class action lawsuits against parties that provide Electronic Systems and/or using Information Technology to the public detriment.

Elucidation of Article 38: Sufficiently clear

Article 39

(1) Civil actions shall be instituted in accordance with provisions of laws and regulations.

- (2) In addition to resolution by civil actions as intended by section (1) parties may resolve disputes through arbitration or other alternative dispute resolution institutions in accordance with provisions of Laws and Regulations.

Elucidation of Article 39: Sufficiently clear

CHAPTER IX
ROLE OF THE GOVERNMENT AND ROLE OF THE PUBLIC

Article 40

(1) The Government shall facilitate the Information Technology and Electronic Transaction usage in accordance with provisions of prevailing laws and regulations.

(2) The Government shall protect the public interest from any type of threat as a result of misusing Electronic Information and Electronic Transactions that offends public order, in accordance with provisions of Laws and Regulations.

(3) The Government shall specify agencies or institutions holding strategic electronic data that must be protected.

(4) Agencies or institutions as intended by section (3) must create Electronic Records and the electronic backups thereof, and connect them with specified data centers in the interest of data security.

(5) Other agencies or institutions other than those regulated by section (3) shall create Electronic Records and their electronic backups as necessary to protect data they hold.

(6) Ketentuan lebih lanjut mengenai peran Pemerintah sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) diatur dengan Peraturan Pemerintah.

Penjelasan Pasal 40: Cukup jelas

Pasal 41

(1) Masyarakat dapat berperan meningkatkan pemanfaatan Teknologi Informasi melalui penggunaan dan Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik sesuai dengan ketentuan Undang-Undang ini

Penjelasan Pasal 41 Ayat (1):
Cukup jelas

(2) Peran masyarakat sebagaimana dimaksud pada ayat (1) dapat diselenggarakan melalui lembaga yang dibentuk oleh masyarakat.

Penjelasan Pasal 41 Ayat (2):
Yang dimaksud dengan "lembaga yang dibentuk oleh masyarakat" merupakan lembaga yang bergerak di bidang teknologi informasi dan transaksi elektronik.

(3) Lembaga sebagaimana dimaksud pada ayat (2) dapat memiliki fungsi konsultasi dan mediasi.

Penjelasan Pasal 41 Ayat (3):
Cukup jelas

BAB X
PENYIDIKAN
Pasal 42

Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Penjelasan Pasal 42: Cukup jelas

Pasal 43

(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Teknologi Informasi dan Transaksi Elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam Undang-Undang tentang Hukum Acara Pidana untuk melakukan penyidikan tindak pidana di

(6) Further provisions on role of the Government as intended by section (1), section (2), and section (3) shall be regulated by Regulation of the Government.

Elucidation of Article 40: Sufficiently clear

Article 41

(1) The public may play role in the improvement of the Information Technology usage through the use and Provision of Electronic Systems and Electronic Transactions in accordance with the provisions of this Law.

Elucidation of Article 41 Section (1):
Sufficiently clear

(2) Role of the public as intended by section (1) may be played via institutions the public forms.

Elucidation of Article 41 Section (2):
"Institutions the public forms" shall be institutions engaged in the field of information technology and electronic transactions.

(3) Institutions as intended by section (2) may have the functions of consultation and mediation.

Elucidation of Article 41 Section (3):
Sufficiently clear

CHAPTER X
INVESTIGATION
Article 42

Investigation of criminal acts as intended by this Law shall be made under the provisions of the Law of Criminal Procedure and the provisions of this Law.

Elucidation of Article 42: Sufficiently clear

Article 43

(1) In addition to Investigators of the State Police of the Republic of Indonesia, certain Civil Service Officials within the Government whose scope of duties and responsibilities is in the field of Information Technology and Electronic Transactions shall be granted special authority as investigators as intended by the Law of Criminal Procedure to make investigation of criminal acts of Information Technology and

bidang Teknologi Informasi dan Transaksi Elektronik.

Penjelasan Pasal 43 Ayat (1):
Cukup jelas

(2) Penyidikan di bidang Teknologi Informasi dan Transaksi Elektronik sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data sesuai dengan ketentuan Peraturan Perundang-undangan.

Penjelasan Pasal 43 Ayat (2):
Cukup jelas

(3) Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat.

Penjelasan Pasal 43 Ayat (3):
Cukup jelas

(4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

Penjelasan Pasal 43 Ayat (4):
Cukup jelas

(5) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:

a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana berdasarkan ketentuan Undang-Undang ini;

Penjelasan Pasal 43 Ayat (5) Huruf a:
Cukup jelas

b. memanggil setiap Orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang terkait dengan ketentuan Undang-Undang ini;

Penjelasan Pasal 43 Ayat (5) Huruf b:
Cukup jelas

c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana berdasarkan ketentuan Undang-Undang ini;

Electronic Transactions.

Elucidation of Article 43 Section (1):
Sufficiently clear

(2) Investigation of Information Technology and Electronic Transactions as intended by section (1) shall be made with due regard to privacy protection, secrecy, smooth public services, data integrity, or data entirety in accordance with provisions of laws and regulations.

Elucidation of Article 43 Section (2):
Sufficiently clear

(3) Searches and/or seizures of electronic systems suspiciously involved in criminal acts must be carried out with the permission of the local chief justice of the district court.

Elucidation of Article 43 Section (3):
Sufficiently clear

(4) In carrying out searches and/or seizures as intended by section (3), investigators are required to maintain the public service interests.

Elucidation of Article 43 Section (4):
Sufficiently clear

(5) Civil Service Investigators as intended by section (1) shall have the authority:

a. to receive reports or complaints from Persons of the occurrence of criminal acts under the provisions of this Law;

Elucidation of Article 43 Section (5) Point a:
Sufficiently clear

b. to summons any Person or other party for hearing and/or examination as suspects or witnesses in connection with suspected criminal acts in the field related to the provisions of this Law;

Elucidation of Article 43 Section (5) Point b:
Sufficiently clear

c. to make examination of the truth of reports or inquiries into criminal acts under the provisions of this Law;

Penjelasan Pasal 43 Ayat (5) Huruf c:
Cukup jelas

d. melakukan pemeriksaan terhadap Orang dan/atau Badan Usaha yang patut diduga melakukan tindak pidana berdasarkan Undang-Undang ini;

Penjelasan Pasal 43 Ayat (5) Huruf d:
Cukup jelas

e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan Teknologi Informasi yang diduga digunakan untuk melakukan tindak pidana berdasarkan Undang-Undang ini;

Penjelasan Pasal 43 Ayat (5) Huruf e:
Cukup jelas

f. melakukan penggeledahan terhadap tempat tertentu yang diduga digunakan sebagai tempat untuk melakukan tindak pidana berdasarkan ketentuan Undang-Undang ini;

Penjelasan Pasal 43 Ayat (5) Huruf f:
Cukup jelas

g. melakukan penyegelan dan penyitaan terhadap alat dan/atau sarana kegiatan Teknologi Informasi yang diduga digunakan secara menyimpang dari ketentuan Peraturan Perundang-undangan;

Penjelasan Pasal 43 Ayat (5) Huruf g:
Cukup jelas

h. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana berdasarkan Undang-Undang ini; dan/atau

Penjelasan Pasal 43 Ayat (5) Huruf h:
Yang dimaksud "ahli" adalah seseorang yang memiliki keahlian khusus di bidang Teknologi Informasi yang dapat dipertanggungjawabkan secara akademis maupun praktis mengenai pengetahuannya tersebut.

i. mengadakan penghentian penyidikan tindak pidana berdasarkan Undang-Undang ini sesuai dengan ketentuan hukum acara pidana yang berlaku.

Penjelasan Pasal 43 Ayat (5) Huruf i:
Cukup jelas

(6) Dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum

Elucidation of Article 43 Section (5) Point c:
Sufficiently clear

d. to make examination of Persons and/or Business Entities that should be suspected of having committed criminal acts under this Law;

Elucidation of Article 43 Section (5) Pont d:
Sufficiently clear

e. to make inspection of equipment and/or facilities in connection with the activities of Information Technology suspected of having been used to commit criminal acts under this Law;

Elucidation of Article 43 Section (5) Point e:
Sufficiently clear

f. to search certain places suspected of having been used as the place to commit criminal acts under the provisions of this Law;

Elucidation of Article 43 Section (5) Point f:
Sufficiently clear

g. to seal and seize equipment and/or facilities of Information Technology activities suspected of having been used in a manner departing from provisions of Laws and Regulations;

Elucidation of Article 43 Section (5) Point g:
Sufficiently clear

h. to solicit assistance of experts necessary for investigation of criminal acts under this Law; and/or

Elucidation of Article 43 Section (5) Point h:
"Expert" means a Person who has special expertise in the field of Information Technology, and whose knowledge thereof is reliable, whether academically or practically.

i. to cease investigation of criminal acts under this Law in accordance with the provisions of the prevailing law of criminal procedure.

Elucidation of Article 43 Section (5) Point i:
Sufficiently clear

(6) To make arrest and detention, investigators through public prosecutors are required to seek

wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

Penjelasan Pasal 43 Ayat (6):
Cukup jelas

(7) Penyidik Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Penyidik Pejabat Polisi Negara Republik Indonesia memberitahukan dimulainya penyidikan dan menyampaikan hasilnya kepada penuntut umum.

Penjelasan Pasal 43 Ayat (7):
Cukup jelas

(8) Dalam rangka mengungkap tindak pidana Informasi Elektronik dan Transaksi Elektronik, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti.

Penjelasan Pasal 43 Ayat (8):
Cukup jelas

Pasal 44

Alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ini adalah sebagai berikut:

a. alat bukti sebagaimana dimaksud dalam ketentuan Perundang-undangan; dan

b. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3).

Penjelasan Pasal 44: Cukup jelas

BAB XI
KETENTUAN PIDANA

Pasal 45

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat

order of the local chief justice of the district court within a period of twenty-four hours.

Elucidation of Article 43 Section (6):
Sufficiently clear

(7) Civil Service Investigators as intended by section (1) shall coordinate with Investigators of the State Police of the Republic of Indonesia to notify the commencement of investigation and deliver the results thereof to public prosecutors.

Elucidation of Article 43 Section (7):
Sufficiently clear

(8) To uncover criminal acts of Electronic Information and Electronic Transactions, investigators may cooperate with investigators of other countries to share information and means of proof.

Elucidation of Article 43 Section (8):
Sufficiently clear

Article 44

Means of proof on the investigation, prosecution and examination at court under the provisions of this Law shall be as follows:

a. means of proof as intended by provisions of laws and regulations; and

b. other means of proof in the form of Electronic Information and/or Electronic Records as intended by Article 1 point 1 and point 4 as well as Article 5 section (1), section (2), and section (3).

Elucidation of Article 44: Sufficiently clear

CHAPTER XI
PENAL PROVISIONS

Article 45

(1) Any Person who satisfies the elements as intended by Article 27 section (1), section (2), section (3), or section (4) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp1,000,000,000 (one billion rupiah).

(2) Any Person who satisfies the elements as intended by Article 28 section (1) or section (2)

(1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Penjelasan Pasal 45: Cukup jelas

Pasal 46

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Penjelasan Pasal 46: Cukup jelas

Pasal 47

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Penjelasan Pasal 47: Cukup jelas

Pasal 48

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar

shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp1,000,000,000,- (one billion rupiah).

(3) Any Person who satisfies the elements as intended by Article 29 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp2,000,000,000 (two billion rupiah).

Elucidation of Article 45: Sufficiently clear

Article 46

(1) Any Person who satisfies the elements as intended by Article 30 section (1) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding Rp600,000,000 (six hundred million rupiah).

(2) Any Person who satisfies the elements as intended by Article 30 section (2) shall be sentenced to imprisonment not exceeding 7 (seven) years and/or a fine not exceeding Rp700,000,000 (seven hundred million rupiah).

(3) Any Person who satisfies the elements as intended by Article 30 section (3) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding Rp800,000,000 (eight hundred million rupiah).

Elucidation of Article 46: Sufficiently clear

Article 47

Any Person who satisfies the elements as intended by Article 31 section (1) or section (2) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp800,000,000 (eight hundred million rupiah).

Elucidation of Article 47: Sufficiently clear

Article 48

(1) Any Person who satisfies the elements as intended by Article 32 section (1) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding Rp2,000,000,000 (two billion rupiah).

rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

Penjelasan Pasal 48: Cukup jelas

Pasal 49

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Penjelasan Pasal 49: Cukup jelas

Pasal 50

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Penjelasan Pasal 50: Cukup jelas

Pasal 51

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Penjelasan Pasal 51: Cukup jelas

(2) Any Person who satisfies the elements as intended by Article 32 section (2) shall be sentenced to imprisonment not exceeding 9 (nine) years and/or a fine not exceeding Rp3,000,000,000 (three billion rupiah).

(3) Any Person who satisfies the elements as intended by Article 32 section (3) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp5,000,000,000 (five billion rupiah).

Elucidation of Article 48: Sufficiently clear

Article 49

Any Person who satisfies the elements as intended by Article 33 shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp10,000,000,000 (ten billion rupiah).

Elucidation of Article 49: Sufficiently clear

Article 50

Any Person who satisfies the elements as intended by Article 34 section (1) shall be sentenced to imprisonment not exceeding 10 (ten) years and/or a fine not exceeding Rp10,000,000,000 (ten billion rupiah).

Elucidation of Article 50: Sufficiently clear

Article 51

(1) Any Person who satisfies the elements as intended by Article 35 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp12,000,000,000 (twelve billion rupiah).

(2) Any Person who satisfies the elements as intended by Article 36 shall be sentenced to imprisonment not exceeding 12 (twelve) years and/or a fine not exceeding Rp12,000,000,000 (twelve billion rupiah).

Elucidation of Article 51: Sufficiently clear

Pasal 52

(1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.

Penjelasan Pasal 52 Ayat (1):
Cukup jelas

(2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.

Penjelasan Pasal 52 Ayat (2):
Cukup jelas

(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.

Penjelasan Pasal 52 Ayat (3):
Cukup jelas

(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

Penjelasan Pasal 52 Ayat (4):
Ketentuan ini dimaksudkan untuk menghukum setiap perbuatan melawan hukum yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 yang dilakukan oleh korporasi (corporate crime) dan/atau oleh pengurus dan/atau staf yang memiliki kapasitas untuk:

a. mewakili korporasi;
b. mengambil keputusan dalam korporasi;
c. melakukan pengawasan dan pengendalian dalam korporasi;

Article 52

(1) Criminal acts as intended by Article 27 section (1) involving propriety or sexual exploitation of children shall be subject to an increase in the sentence by one third of the basic sentence.

Elucidation of Article 52 Section (1):
Sufficiently clear

(2) Criminal acts as intended by Article 30 through Article 37 aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Records of the Government and/or used for public services shall be sentenced to the basic sentence plus one third.

Elucidation of Article 52 Section (2):
Sufficiently clear

(3) Criminal acts as intended by Article 30 through Article 37 aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Records of the Government and/or strategic bodies including and not limited to defense institutions, the central bank, banking, finance, international institutions, aviation authority shall be subject to a sentence of maximally the basic sentence for the respective Articles plus two-thirds.

Elucidation of Article 52 Section (3):
Sufficiently clear

(4) Criminal acts as intended by Article 27 through Article 37 committed by corporations shall be sentenced to the basic sentence plus two-thirds.

Elucidation of Article 52 Section (4):
This provision is intended to sentence any unlawful act that satisfies the elements as intended by Article 27 through Article 37 committed by corporations (corporate crimes) and/or by the management and/or staff with capacity to:

a. represent the corporations;
b. make decisions for the corporations;
c. make supervision and control over the corporations;

d. melakukan kegiatan demi keuntungan korporasi.

BAB XII
KETENTUAN PERALIHAN
Pasal 53

Pada saat berlakunya Undang-Undang ini, semua Peraturan Perundang-undangan dan kelembagaan yang berhubungan dengan pemanfaatan Teknologi Informasi yang tidak bertentangan dengan Undang-Undang ini dinyatakan tetap berlaku.

Penjelasan Pasal 53: Cukup jelas

BAB XIII
KETENTUAN PENUTUP
Pasal 54

(1) Undang-undang ini mulai berlaku pada tanggal diundangkan.

(2) Peraturan Pemerintah harus sudah ditetapkan paling lama 2 (dua) tahun setelah diundangkannya Undang-Undang ini.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Penjelasan Pasal 54: Cukup jelas

Disahkan di Jakarta
pada tanggal 21 April 2008
PRESIDEN REPUBLIK INDONESIA

ttd.

DR. H. SUSILO BAMBANG YUDHOYONO

Diundangkan di Jakarta
Pada tanggal 21 April 2008
MENTERI HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA,

ttd

ANDI MATTALATTA

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN 2008 NOMOR 58

TAMBAHAN LEMBARAN NEGARA REPUBLIK INDONESIA NOMOR 4843

d. carry out activities for the benefit of the corporations.

CHAPTER XII
TRANSITIONAL PROVISIONS
Article 53

Upon effectiveness of this Law, all Laws and Regulations and institutions in connection with Information Technology usage that are not against this Law are declared to remain valid.

Elucidation of Article 53: Sufficiently clear

CHAPTER XIII
CONCLUDING PROVISIONS
Article 54

(1) This law shall take effect from the date it is promulgated.

(2) Government Regulations must have been enacted not longer than 2 (two) years upon promulgation of this Law.

In order that any person may know of it, the promulgation of this Law is ordered by placement in the State Gazette of the Republic of Indonesia.

Elucidation of Article 54: Sufficiently clear

Ratified in Jakarta
on April 21, 2008
PRESIDENT OF THE REPUBLIC OF INDONESIA

sgd.

DR. H. SUSILO BAMBANG YUDHOYONO

Promulgated in Jakarta
on April 21, 2008
MINISTER OF LAW AND HUMAN RIGHTS OF THE REPUBLIC OF INDONESIA,

sgd

ANDI MATTALATTA

STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 58 OF 2008

SUPPLEMENT TO STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER 4843

***

LAWS OF MALAYSIA

ACT 709
PERSONAL DATA PROTECTION ACT 2010

Date of Royal Assent : **2 June 2010**

Date of publication in the Gazette : **10 June 2010**

ARRANGEMENT OF SECTIONS

Preamble

An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto.

[ ]

ENACTED by the Parliament of Malaysia as follows:

PART I – PRELIMINARY

Section 1. Short title and commencement

(1) This Act may be cited as the Personal Data Protection Act 2010.

(2) This Act comes into operation on a date to be appointed by the Minister by notification in the *Gazette*, and the Minister may appoint different dates for different provisions of this Act.

Section 2. Application

(1) This Act applies to—

(a) any person who processes; and

(b) any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions.

(2) Subject to subsection (1), this Act applies to a person in respect of personal data if—

(a) the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or

(b) the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.

(3) A person falling within paragraph (2)*(b)* shall nominate for the purposes of this Act a representative established in Malaysia.

(4) For the purposes of subsections (2) and (3), each of the following is to be treated as established in Malaysia:

(a) an individual whose physical presence in Malaysia shall not be less than one hundred and eighty days in one calendar year;

(b) a body incorporated under the Companies Act 1965 [*Act 125*];

(c) a partnership or other unincorporated association formed under any written laws in Malaysia; and

(d) any person who does not fall within paragraph *(a)*, *(b)* or *(c)* but maintains in Malaysia—

(i) an office, branch or agency through which he carries on any activity; or

(ii) a regular practice.

Section 3. Non-application

(1) This Act shall not apply to the Federal Government and State Governments.

(2) This Act shall not apply to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia.

Section 4. Interpretation

In this Act, unless the context otherwise requires—

“credit reporting agency” has the meaning assigned to it in the Credit Reporting Agencies Act 2010 [*Act 710*];

“this Act” includes regulations, orders, notifications and other subsidiary legislation made under this Act;

“register” means the Register of Data Users, Register of Data User Forums or Register of Codes of Practice;

“personal data” means any information in respect of commercial transactions, which—

(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010;

“sensitive personal data” means any personal data consisting of information as to the physical or

mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the *Gazette*;

"prescribed" means prescribed by the Minister under this Act and where no mode is mentioned, means prescribed by order published in the *Gazette*;

"Advisory Committee" means the Personal Data Protection Advisory Committee established under section 70;

"vital interests" means matters relating to life, death or security of a data subject;

"Fund" means the Personal Data Protection Fund established under section 61;

"use", in relation to personal data, does not include the act of collecting or disclosing such personal data;

"collect", in relation to personal data, means an act by which such personal data enters into or comes under the control of a data user;

"Minister" means the Minister charged with the responsibility for the protection of personal data;

"disclose", in relation to personal data, means an act by which such personal data is made available by a data user;

"relevant person", in relation to a data subject, howsoever described, means—

(a) in the case of a data subject who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject;

(b) in the case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the data subject to act on behalf of the data subject; or

(c) in any other case, a person authorized in writing by the data subject to make a data access request, data correction request, or both such requests, on behalf of the data subject;

"authorized officer" means any officer authorized in writing by the Commissioner under section 110;

"correction", in relation to personal data, includes amendment, variation, modification or deletion;

"requestor", in relation to a data access request or data correction request, means the data subject or the relevant person on behalf of the data subject, who has made the request;

"data processor", in relation to personal data, means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes;

"processing", in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including—

(a) the organization, adaptation or alteration of personal data;

(b) the retrieval, consultation or use of personal data;

(c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making

available; or

(d) the alignment, combination, correction, erasure or destruction of personal data;

"registration" means the registration of a data user under section 16;

"data user" means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor;

"relevant data user", in relation to—

(a) an inspection, means the data user who uses the personal data system which is the subject of the inspection;

(b) a complaint, means the data user specified in the complaint;

(c) an investigation—

(i) in the case of an investigation initiated by a complaint, means the data user specified in the complaint;

(ii) in any other case, means the data user who is the subject of the investigation;

(d) an enforcement notice, means the data user on whom the enforcement notice is served;

"credit reporting business" has the meaning assigned to it in the Credit Reporting Agencies Act 2010;

"Commissioner" means the Personal Data Protection Commissioner appointed under section 47;

"third party", in relation to personal data, means any person other than—

(a) a data subject;

(b) a relevant person in relation to a data subject;

(c) a data user;

(d) a data processor; or

(e) a person authorized in writing by the data user to process the personal data under the direct control of the data user;

"relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

"data subject" means an individual who is the subject of the personal data;

"appointed date" means the relevant date or dates, as the case may be, on which this Act comes into operation;

"code of practice" means the personal data protection code of practice in respect of a specific class of data users registered by the Commissioner pursuant to section 23 or issued by the

Commissioner under section 24;

"commercial transactions" means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.

PART II - PERSONAL DATA PROTECTION

Division 1 - *Personal Data Protection Principles*

Section 5. Personal Data Protection Principles

(1) The processing of personal data by a data user shall be in compliance with the following Personal Data Protection Principles, namely—

(a) the General Principle;

(b) the Notice and Choice Principle;

(c) the Disclosure Principle;

(d) the Security Principle;

(e) the Retention Principle;

(f) the Data Integrity Principle; and

(g) the Access Principle,

as set out in sections 6, 7, 8, 9, 10, 11 and 12.

(2) Subject to sections 45 and 46, a data user who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Section 6. General Principle

(1) A data user shall not—

(a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or

(b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions of section 40.

(2) Notwithstanding paragraph (1)*(a)*, a data user may process personal data about a data subject if the processing is necessary—

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

(c) for compliance with any legal obligation to which the data user is the subject, other than an

obligation imposed by a contract;

(d) in order to protect the vital interests of the data subject;

(e) for the administration of justice; or

(f) for the exercise of any functions conferred on any person by or under any law.

(3) Personal data shall not be processed unless—

(a) the personal data is processed for a lawful purpose directly related to an activity of the data user;

(b) the processing of the personal data is necessary for or directly related to that purpose; and

(c) the personal data is adequate but not excessive in relation to that purpose.

Section 7. Notice and Choice Principle

(1) A data user shall by written notice inform a data subject—

(a) that personal data of the data subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject;

(b) the purposes for which the personal data is being or is to be collected and further processed;

(c) of any information available to the data user as to the source of that personal data;

(d) of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;

(e) of the class of third parties to whom the data user discloses or may disclose the personal data;

(f) of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;

(g) whether it is obligatory or voluntary for the data subject to supply the personal data; and

(h) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.

(2) The notice under subsection (1) shall be given as soon as practicable by the data user—

(a) when the data subject is first asked by the data user to provide his personal data;

(b) when the data user first collects the personal data of the data subject; or

(c) in any other case, before the data user—

(i) uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected; or

(ii) discloses the personal data to a third party.

(3) A notice under subsection (1) shall be in the national and English languages, and the individual shall be provided with a clear and readily accessible means to exercise his choice, where necessary, in the national and English languages.

Section 8. Disclosure Principle

Subject to section 39, no personal data shall, without the consent of the data subject, be disclosed—

(a) for any purpose other than—

(i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or

(ii) a purpose directly related to the purpose referred to in subparagraph (i); or

(b) to any party other than a third party of the class of third parties as specified in paragraph 7(1)*(e)*.

Section 9. Security Principle

(1) A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard—

(a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) to the place or location where the personal data is stored;

(c) to any security measures incorporated into any equipment in which the personal data is stored;

(d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

(e) to the measures taken for ensuring the secure transfer of the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction, ensure that the data processor—

(a) provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and

(b) takes reasonable steps to ensure compliance with those measures.

Section 10. Retention Principle

(1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

(2) It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

Section 11. Data Integrity Principle

A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

Section 12. Access Principle

A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.

Division 2 – *Registration*

Section 13. Application of this Division

(1) This Division shall apply to a data user who belongs to a class of data users as specified in the order made under subsection 14(1).

(2) A data user who belongs to a class of data users not specified in the order made under subsection 14(1) shall comply with all the provisions of this Act other than the provisions of this Division relating to the registration of data users and matters connected thereto.

Section 14. Registration of data users

(1) The Minister may, upon the recommendation of the Commissioner, by order published in the *Gazette*, specify a class of data users who shall be required to be registered as data users under this Act.

(2) The Commissioner shall, before making his recommendation under subsection (1), consult with—

(a) such bodies representative of data users belonging to that class; or

(b) such other interested persons.

Section 15. Application for registration

(1) A person who belongs to the class of data users as specified in the order made under subsection 14(1) shall submit an application for registration to the Commissioner in the manner and form as determined by the Commissioner.

(2) Every application for registration shall be accompanied with the prescribed registration fee and such documents as may be required by the Commissioner.

(3) The Commissioner may in writing at any time after receiving the application and before it is determined, require the applicant to provide such additional documents or information within the time as specified by the Commissioner.

(4) If the requirement under subsection (3) is not complied with, the application for registration shall be deemed to have been withdrawn by the applicant and shall not be further proceeded with by the Commissioner, but without prejudice to a fresh application being made by the applicant.

Section 16. Certificate of registration

(1) After having given due consideration to an application under subsection 15(1), the Commissioner may—

(a) register the applicant and issue a certificate of registration to the applicant in such form as determined by the Commissioner; or

(b) refuse the application.

(2) The certificate of registration may be issued subject to such conditions or restrictions as the Commissioner may think fit to impose.

(3) Where the Commissioner refuses the application for registration in pursuance of subsection (1), he shall inform the applicant by a written notice that the application has been refused and the reasons for the refusal.

(4) A person who belongs to the class of data users as specified in the order made under subsection 14(1) and who processes personal data without a certificate of registration issued in pursuance of paragraph 16(1)*(a)* commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

Section 17. Renewal of certificate of registration

(1) A data user may make an application for the renewal of the certificate of registration not later than ninety days before the date of expiry of the certificate of registration in the manner and form as determined by the Commissioner and the application shall be accompanied with the prescribed renewal fee and such documents as may be required by the Commissioner, but no application for renewal shall be allowed where the application is made after the date of expiry of the certificate of registration.

(2) When renewing a certificate of registration, the Commissioner may vary the conditions or restrictions imposed upon the issuance of the certificate of registration or impose additional conditions or restrictions.

(3) The Commissioner may refuse to renew a certificate of registration—

(a) if the data user has failed to comply with any of the provisions of this Act;

(b) if the data user has failed to comply with any conditions or restrictions imposed upon the issuance of the certificate of registration; or

(c) if he is satisfied that the data user is unable to continue the processing of personal data in accordance with this Act.

Section 18. Revocation of registration

(1) The Commissioner may revoke the registration of a data user if the Commissioner is satisfied that—

(a) the data user has failed to comply with any of the provisions of this Act;

(b) the data user has failed to comply with any conditions or restrictions imposed upon the issuance of the certificate of registration;

(c) the issuance of the certificate of registration was induced by a false representation of fact by the data user; or

(d) the data user has ceased to carry on the processing of personal data.

(2) Notwithstanding subsection (1), the Commissioner shall not revoke the registration of a data user unless the Commissioner is satisfied that, after giving the data user an opportunity of making

any representation in writing he may wish to make, the registration should be revoked.

(3) Where the registration of the data user is revoked, the Commissioner shall issue a notice of revocation of registration to the data user, and the certificate of registration issued in respect of such registration shall have no effect upon service of the notice of revocation of registration.

(4) A data user whose registration has been revoked under this section and who continues to process personal data thereafter commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

Section 19. Surrender of certificate of registration

(1) Where the certificate of registration is revoked in pursuance of section 18, the holder of the certificate shall, within seven days from the date of service of the notice of revocation of registration, surrender the certificate to the Commissioner.

(2) A person who fails to comply with subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Section 20. Register of Data Users

(1) The Commissioner shall maintain a Register of Data Users in accordance with section 128.

(2) The Register of Data Users shall contain the names of data users who have been registered in pursuance of this Division and any other particulars regarding such data users as may be determined by the Commissioner.

Division 3 - *Data user forum and code of practice*

Section 21. Data user forum

(1) The Commissioner may designate a body as a data user forum in respect of a specific class of data users for the purposes of this Act by notifying that body in writing, if the Commissioner is satisfied that—

(a) the membership of the body is open to all data users of that class;

(b) the body is capable of performing as required under the relevant provisions of this Act; and

(c) the body has a written constitution.

(2) The body shall agree in writing to be a data user forum before the designation is registered by the Commissioner in the Register of Data User Forums.

(3) The Commissioner may decide that an existing body that was previously designated as a data user forum under subsection (1) is no longer a data user forum for the purposes of this Act, if he is satisfied that the body no longer meets the requirements as set out in that subsection.

(4) Where the Commissioner decides that an existing body which has been designated as a data user forum is no longer a data user forum for the purposes of this Act, he shall withdraw the designation and subsequently cancel the registration of the designation in the Register of Data User Forums.

(5) A designation or withdrawal of designation under this section shall take effect from the date of registration of the designation or the date of cancellation of the registration of the designation, as the case may be, or such later date as specified by the Commissioner.

Section 22. Register of Data User Forums

(1) The Commissioner shall maintain a Register of Data User Forums in accordance with section 128.

(2) The Register of Data User Forums shall contain the names of data user forums which have been designated and registered in pursuance of this Division and any other particulars regarding such data user forums as may be determined by the Commissioner.

Section 23. Code of practice

(1) A data user forum may prepare a code of practice—

(a) on its own initiative; or

(b) upon request by the Commissioner.

(2) The data user forum shall, in preparing a code of practice under subsection (1), consider matters including—

(a) the purpose for the processing of personal data by the data user or class of data users;

(b) the views of the data subjects or groups representing data subjects;

(c) the views of the relevant regulatory authority, if any, to which the data user is subject to; and

(d) that the code of practice, upon having regard to all of the matters in paragraphs *(a)*, *(b)* and *(c)* and any other matters, offers an adequate level of protection for the personal data of the data subjects concerned.

(3) The Commissioner may register the code of practice prepared pursuant to subsection (1), if the Commissioner is satisfied that—

(a) the code of practice is consistent with the provisions of this Act; and

(b) the matters as set out in subsection (2) have been given due consideration.

(4) The code of practice under subsection (1) shall take effect on the date of registration of the code of practice by the Commissioner in the Register of Codes of Practice.

(5) If the Commissioner refuses to register the code of practice, the Commissioner shall notify the relevant data user forum of his decision in writing and provide the reasons for it.

(6) If the Commissioner neither registers nor refuses to register a code of practice within thirty days from the date of receipt of the code of practice by him for registration, he shall be deemed to have refused the registration of the code of practice.

(7) The Commissioner may register different codes of practice for different classes of data users.

(8) The Commissioner and data user shall make available to the public any code of practice registered under subsection (3).

Section 24. Commissioner may issue code of practice

(1) The Commissioner may issue a code of practice, if—

(a) a code of practice is not prepared under paragraph 23(1)*(a)*;

(b) the Commissioner is satisfied that a code of practice for a specific class of data users is unlikely to be prepared by the relevant data user forum within the period as specified by the Commissioner; or

(c) there is no data user forum to develop the relevant code of practice for the class of data users.

(2) The Commissioner shall, before issuing a code of practice under subsection (1), consider matters including—

(a) the purpose for the processing of personal data by the data user or class of data users;

(b) the views of the data users or groups representing data users, to which the code of practice is applicable;

(c) the views of the data subjects or groups representing data subjects;

(d) the views of the relevant regulatory authority, if any, to which the data user is subject to; and

(e) that the code of practice, upon having regard to all of the matters in paragraphs *(a)*, *(b)* and *(c)* and any other matters, offers an adequate level of protection for the personal data of the data subjects concerned.

(3) The Commissioner may issue different codes of practice for different classes of data users.

(4) The code of practice issued by the Commissioner under subsection (1) shall be registered in the Register of Codes of Practice.

(5) The code of practice under subsection (1) shall take effect on the date of registration of the code of practice by the Commissioner.

(6) The Commissioner shall make available to the public any code of practice issued by him under subsection (1).

Section 25. Applicable code of practice

(1) The Commissioner shall ensure that there is only one code of practice registered for a class of data users at a given time.

(2) All data users belonging to a class of data users shall comply with the relevant registered code of practice that is applicable to that class of data users at a given time.

(3) Where a code of practice is registered by the Commissioner under section 23 or 24, the Commissioner shall notify, in such manner as he may determine, the relevant class of data users to whom the code of practice is applicable—

(a) of the identity of the code of practice concerned and the date on which the code of practice is to take effect; and

(b) of the specific requirements under this Act for which the code of practice is issued and registered.

(4) If there is any uncertainty or ambiguity as to which code of practice is applicable to a particular data user or class of data users, the data user or person concerned may apply to the Commissioner for his opinion on which code of practice is the applicable code of practice in

relation to the circumstances of such data user or person.

(5) The Commissioner shall provide his opinion within thirty days from the date of receipt of an application made under subsection (4).

(6) The Commissioner shall, when making his opinion under subsection (5), take into account any relevant previous opinions, if any.

(7) The Commissioner may withdraw an opinion made under this section if the Commissioner is satisfied that the nature of the activity engaged by the data user has changed materially.

Section 26. Revocation, etc., of code of practice

(1) The Commissioner may revoke, amend or revise, whether in whole or in part, any code of practice registered under this Act—

(a) on his own accord; or

(b) upon an application by the data user forum or such bodies representing the data users.

(2) The Commissioner shall, before revoking, amending or revising a code of practice under subsection (1), consult with—

(a) such data users or bodies representative of data users to which the code of practice shall apply, whether in whole or in part; and

(b) such other interested persons,

as the Commissioner thinks fit.

(3) Where any code of practice has been revoked, amended or revised under subsection (1), the Commissioner—

(a) shall enter the particulars of such revocation, amendment or revision in the Register of Codes of Practice; and

(b) shall notify the relevant data user forum, class of data users, data users and the public of such revocation, amendment or revision in such manner as may be determined by him.

(4) The Commissioner shall make available to the public any code of practice as amended or revised by him under this section.

Section 27. Submission of new code of practice by data user forum

(1) A data user forum may submit a new code of practice to replace an existing code of practice.

(2) The new code of practice submitted in pursuance of subsection (1) shall be subject to the provisions of this Division.

Section 28. Register of Codes of Practice

(1) The Commissioner shall maintain a Register of Codes of Practice in accordance with section 128.

(2) The Register of Codes of Practice shall contain—

(a) particulars of codes of practice registered under section 23 or 24 and any revocation,

amendment or revision to such codes of practice under section 26; and

(b) any opinion made by the Commissioner under section 25, including particulars of withdrawal of previous opinions.

Section 29. Non-compliance with code of practice

A data user who fails to comply with any provision of the code of practice that is applicable to the data user commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Division 4 - *Rights of data subject*

Section 30. Right of access to personal data

(1) An individual is entitled to be informed by a data user whether personal data of which that individual is the data subject is being processed by or on behalf of the data user.

(2) A requestor may, upon payment of a prescribed fee, make a data access request in writing to the data user—

(a) for information of the data subject's personal data that is being processed by or on behalf of the data user; and

(b) to have communicated to him a copy of the personal data in an intelligible form.

(3) A data access request for any information under subsection (2) shall be treated as a single request, and a data access request for information under paragraph (2)*(a)* shall, in the absence of any indication to the contrary, be treated as extending also to such request under paragraph (2)*(b)*.

(4) In the case of a data user having separate entries in respect of personal data held for different purposes, a separate data access request shall be made for each separate entry.

(5) Where a data user does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data user who holds the personal data from complying, whether in whole or part, with the data access request under subsection (2) which relates to the personal data, the firstmentioned data user shall be deemed to hold the personal data and the provisions of this Act shall be construed accordingly.

Section 31. Compliance with data access request

(1) Subject to subsection (2) and section 32, a data user shall comply with a data access request under section 30 not later than twenty-one days from the date of receipt of the data access request.

(2) A data user who is unable to comply with a data access request within the period specified in subsection (1) shall before the expiration of that period—

(a) by notice in writing inform the requestor that he is unable to comply with the data access request within such period and the reasons why he is unable to do so; and

(b) comply with the data access request to the extent that he is able to do so.

(3) Notwithstanding subsection (2), the data user shall comply in whole with the data access request not later than fourteen days after the expiration of the period stipulated in subsection (1).

Section 32. Circumstances where data user may refuse to comply with data

access request

(1) A data user may refuse to comply with a data access request under section 30 if—

(a) the data user is not supplied with such information as he may reasonably require—

(i) in order to satisfy himself as to the identity of the requestor; or

(ii) where the requestor claims to be a relevant person, in order to satisfy himself—

(A) as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and

(B) that the requestor is the relevant person in relation to the data subject;

(b) the data user is not supplied with such information as he may reasonably require to locate the personal data to which the data access request relates;

(c) the burden or expense of providing access is disproportionate to the risks to the data subject's privacy in relation to the personal data in the case in question;

(d) the data user cannot comply with the data access request without disclosing personal data relating to another individual who can be identified from that information, unless—

(i) that other individual has consented to the disclosure of the information to the requestor; or

(ii) it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual;

(e) subject to subsection (3), any other data user controls the processing of the personal data to which the data access request relates in such a way as to prohibit the first-mentioned data user from complying, whether in whole or in part, with the data access request;

(f) providing access would constitute a violation of an order of a court;

(g) providing access would disclose confidential commercial information; or

(h) such access to personal data is regulated by another law.

(2) In determining for the purposes of subparagraph (1)*(d)*(ii) whether it is reasonable in all the circumstances to comply with the data access request without the consent of the other individual, regard shall be had, in particular, to—

(a) any duty of confidentiality owed to the other individual;

(b) any steps taken by the data user with a view to seeking the consent of the other individual;

(c) whether the other individual is capable of giving consent; and

(d) any express refusal of consent by the other individual.

(3) Paragraph (1)*(e)* shall not operate so as to excuse the data user from complying with the data access request under subsection 30(2) to any extent that the data user can comply with the data access request without contravening the prohibition concerned.

Section 33. Notification of refusal to comply with data access request

Where a data user who pursuant to section 32 refuses to comply with a data access request under section 30, he shall, not later than twenty-one days from the date of receipt of the data access request, by notice in writing, inform the requestor—

(a) of the refusal and the reasons for the refusal; and

(b) where paragraph 32(1)*(e)* is applicable, of the name and address of the other data user concerned.

Section 34. Right to correct personal data

(1) Where—

(a) a copy of the personal data has been supplied by the data user in compliance with the data access request under section 30 and the requestor considers that the personal data is inaccurate, incomplete, misleading or not up-to-date; or

(b) the data subject knows that his personal data being held by the data user is inaccurate, incomplete, misleading or not up-to-date,

the requestor or data subject, as the case may be, may make a data correction request in writing to the data user that the data user makes the necessary correction to the personal data.

(2) Where a data user does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data user who holds the personal data from complying, whether in whole or in part, with the data correction request under subsection (1) which relates to the personal data, the first-mentioned data user shall be deemed to be the data user to whom such a request may be made and the provisions of this Act shall be construed accordingly.

Section 35. Compliance with data correction request

(1) Subject to subsections (2), (3) and (5) and section 36, where a data user is satisfied that the personal data to which a data correction request relates is inaccurate, incomplete, misleading or not up-to-date, he shall, not later than twenty-one days from the date of receipt of the data correction request—

(a) make the necessary correction to the personal data;

(b) supply the requestor with a copy of the personal data as corrected; and

(c) subject to subsection (4), where—

(i) the personal data has been disclosed to a third party during the twelve months immediately preceding the day on which the correction is made; and

(ii) the data user has no reason to believe that the third party has ceased using the personal data for the purpose, including any directly related purpose, for which the personal data was disclosed to the third party,

take all practicable steps to supply the third party with a copy of the personal data as so corrected accompanied by a notice in writing stating the reasons for the correction.

(2) A data user who is unable to comply with a data correction request within the period specified in subsection (1) shall before the expiration of that period—

(a) by notice in writing inform the requestor that he is unable to comply with the data correction

request within such period and the reasons why he is unable to do so; and

(b) comply with the data correction request to the extent that he is able to do so.

(3) Notwithstanding subsection (2), the data user shall comply in whole with the data correction request not later than fourteen days after the expiration of the period stipulated in subsection (1).

(4) A data user is not required to comply with paragraph (1)*(c)* in any case where the disclosure of the personal data to a third party consists of the third party's own inspection of a register—

(a) in which the personal data is entered or otherwise recorded; and

(b) which is available for inspection by the public.

(5) Where a data user is requested to correct personal data under subsection 34(1) and the personal data is being processed by another data user that is in a better position to respond to the data correction request—

(a) the first-mentioned data user shall immediately transfer the data correction request to such data user, and notify the requestor of this fact; and

(b) sections 34, 35, 36 and 37 shall apply as if the references therein to a data user were references to such other data user.

Section 36. Circumstances where data user may refuse to comply with data correction request

(1) A data user may refuse to comply with a data correction request under section 34 if—

(a) the data user is not supplied with such information as he may reasonably require—

(i) in order to satisfy himself as to the identity of the requestor; or

(ii) where the requestor claims to be a relevant person, in order to satisfy himself—

(A) as to the identity of the data subject in relation to whom the requestor claims to be the relevant person; and

(B) that the requestor is the relevant person in relation to the data subject;

(b) the data user is not supplied with such information as he may reasonably require to ascertain in what way the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date;

(c) the data user is not satisfied that the personal data to which the data correction request relates is inaccurate, incomplete, misleading or not up-to-date;

(d) the data user is not satisfied that the correction which is the subject of the data correction request is accurate, complete, not misleading or up-to-date; or

(e) subject to subsection (2), any other data user controls the processing of the personal data to which the data correction request relates in such a way as to prohibit the first-mentioned data user from complying, whether in whole or in part, with the data correction request.

(2) Paragraph (1)*(e)* shall not operate so as to excuse the data user from complying with subsection 35(1) in relation to the data correction request to any extent that the data user can comply with that subsection without contravening the prohibition concerned.

Section 37. Notification of refusal to comply with data correction request

(1) Where a data user who pursuant to section 36 refuses to comply with a data correction request under section 34, he shall, not later than twenty-one days from the date of receipt of the data correction request, by notice in writing, inform the requestor—

(a) of the refusal and the reasons for the refusal; and

(b) where paragraph 36(1)*(e)* is applicable, of the name and address of the other data user concerned.

(2) Without prejudice to the generality of subsection (1), where personal data to which the data correction request relates is an expression of opinion and the data user is not satisfied that the expression of opinion is inaccurate, incomplete, misleading or not up-to-date, the data user shall—

(a) make a note, whether annexed to the personal data or elsewhere—

(i) of the matters in respect of which the expression of opinion is considered by the requestor to be inaccurate, incomplete, misleading or not up-to-date; and

(ii) in such a way that the personal data cannot be used by any person without the note being drawn to the attention of and being available for inspection by that person; and

(b) attach a copy of the note to the notice referred to in subsection (1) which relates to the data correction request.

(3) In this section, "expression of opinion" includes an assertion of fact which is unverifiable or in all circumstances of the case is not practicable to verify.

(4) A data user who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Section 38. Withdrawal of consent to process personal data

(1) A data subject may by notice in writing withdraw his consent to the processing of personal data in respect of which he is the data subject.

(2) The data user shall, upon receiving the notice under subsection (1), cease the processing of the personal data.

(3) The failure of the data subject to exercise the right conferred by subsection (1) does not affect any other rights conferred on him by this Part.

(4) A data user who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Section 39. Extent of disclosure of personal data

Notwithstanding section 8, personal data of a data subject may be disclosed by a data user for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances:

(a) the data subject has given his consent to the disclosure;

(b) the disclosure —

(i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or

(ii) was required or authorized by or under any law or by the order of a court;

(c) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;

(d) the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or

(e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister.

Section 40. Processing of sensitive personal data

(1) Subject to subsection (2) and section 5, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions:

(a) the data subject has given his explicit consent to the processing of the personal data;

(b) the processing is necessary—

(i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;

(ii) in order to protect the vital interests of the data subject or another person, in a case where—

(A) consent cannot be given by or on behalf of the data subject; or

(B) the data user cannot reasonably be expected to obtain the consent of the data subject;

(iii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

(iv) for medical purposes and is undertaken by—

(A) a healthcare professional; or

(B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

(v) for the purpose of, or in connection with, any legal proceedings;

(vi) for the purpose of obtaining legal advice;

(vii) for the purposes of establishing, exercising or defending legal rights;

(viii) for the administration of justice;

(ix) for the exercise of any functions conferred on any person by or under any written law;

or

(x) for any other purposes as the Minister thinks fit; or

(c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

(2) The Minister may by order published in the *Gazette* exclude the application of subparagraph (1)*(b)*(i), (viii) or (ix) in such cases as may be specified in the order, or provide that, in such cases as may be specified in the order, the condition in subparagraph (1)*(b)*(i), (viii) or (ix) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

(3) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

(4) For the purposes of this section—

"medical purposes" includes the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services;

"healthcare services" has the meaning assigned to it in the Private Healthcare Facilities and Services Act 1998 [*Act 586*];

"healthcare professional" means a medical practitioner, dental practitioner, pharmacist, clinical psychologist, nurse, midwife, medical assistant, physiotherapist, occupational therapist and other allied healthcare professionals and any other person involved in the giving of medical, health, dental, pharmaceutical and any other healthcare services under the jurisdiction of the Ministry of Health.

Section 41. Repeated collection of personal data in same circumstances

(1) Where a data user—

(a) has complied with the provisions of the Notice and Choice Principle under section 7 in respect of the collection of personal data from the data subject, referred to as the "first collection"; and

(b) on any subsequent occasion again collects personal data from that data subject, referred to as the "subsequent collection",

the data user is not required to comply with the provisions of the Notice and Choice Principle in respect of the subsequent collection if—

(A) to comply with those provisions in respect of that subsequent collection would be to repeat, in the same circumstances, what was done to comply with that principle in respect of the first collection; and

(B) not more than twelve months have elapsed between the first collection and the subsequent collection.

(2) For the avoidance of doubt, it is declared that subsection (1) shall not operate to prevent a subsequent collection from becoming a first collection if the data user concerned has complied with the provisions of the Notice and Choice Principle in respect of the subsequent collection.

Section 42. Right to prevent processing likely to cause damage or distress

(1) Subject to subsection (2), a data subject may, at any time by notice in writing to a data user, referred to as the "data subject notice", require the data user at the end of such period as is reasonable in the circumstances, to—

(a) cease the processing of or processing for a specified purpose or in a specified manner; or

(b) not begin the processing of or processing for a specified purpose or in a specified manner,

any personal data in respect of which he is the data subject if, based on reasons to be stated by him—

(A) the processing of that personal data or the processing of personal data for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another person; and

(B) the damage or distress is or would be unwarranted.

(2) Subsection (1) shall not apply where—

(a) the data subject has given his consent;

(b) the processing of personal data is necessary—

(i) for the performance of a contract to which the data subject is a party;

(ii) for the taking of steps at the request of the data subject with a view to entering a contract;

(iii) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by contract; or

(iv) in order to protect the vital interests of the data subject; or

(c) in such other cases as may be prescribed by the Minister by order published in the *Gazette*.

(3) The data user shall, within twenty-one days from the date of receipt of the data subject notice under subsection (1), give the data subject a written notice—

(a) stating that he has complied or intends to comply with the data subject notice; or

(b) stating his reasons for regarding the data subject notice as unjustified, or to any extent unjustified, and the extent, if any, to which he has complied or intends to comply with it.

(4) Where the data subject is dissatisfied with the failure of the data user to comply with the data subject notice, whether in whole or in part, under paragraph (3)*(b)*, the data subject may submit an application to the Commissioner to require the data user to comply with the data subject notice.

(5) Where the Commissioner is satisfied that the application of the data subject under subsection (4) is justified or justified to any extent, the Commissioner may require the data user to take such steps for complying with the data subject notice.

(6) A data user who fails to comply with the requirement of the Commissioner under subsection (5) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Section 43. Right to prevent processing for purposes of direct marketing

(1) A data subject may, at any time by notice in writing to a data user, require the data user at the end of such period as is reasonable in the circumstances to cease or not to begin processing his personal data for purposes of direct marketing.

(2) Where the data subject is dissatisfied with the failure of the data user to comply with the notice, whether in whole or in part, under subsection (1), the data subject may submit an application to the Commissioner to require the data user to comply with the notice.

(3) Where the Commissioner is satisfied that the application of the data subject under subsection (2) is justified or justified to any extent, the Commissioner may require the data user to take such steps for complying with the notice.

(4) A data user who fails to comply with the requirement of the Commissioner under subsection (3) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

(5) For the purposes of this section, "direct marketing" means the communication by whatever means of any advertising or marketing material which is directed to particular individuals.

Section 44. Record to be kept by data user

(1) A data user shall keep and maintain a record of any application, notice, request or any other information relating to personal data that has been or is being processed by him.

(2) The Commissioner may determine the manner and form in which the record is to be maintained.

PART III – EXEMPTION

Section 45. Exemption

(1) There shall be exempted from the provisions of this Act personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

(2) Subject to section 46, personal data—

(a) processed for—

(i) the prevention or detection of crime or for the purpose of investigations;

(ii) the apprehension or prosecution of offenders; or

(iii) the assessment or collection of any tax or duty or any other imposition of a similar nature,

shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act;

(b) processed in relation to information of the physical or mental health of a data subject shall be exempted from the Access Principle and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;

(c) processed for preparing statistics or carrying out research shall be exempted from the

General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;

(d) that is necessary for the purpose of or in connection with any order or judgement of a court shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act;

(e) processed for the purpose of discharging regulatory functions shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or

(f) processed only for journalistic, literary or artistic purposes shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle, Retention Principle, Data Integrity Principle and Access Principle and other related provisions of this Act, provided that—

(i) the processing is undertaken with a view to the publication by any person of the journalistic, literary or artistic material;

(ii) the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the publication would be in the public interest; and

(iii) the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.

Section 46. Power to make further exemptions

(1) The Minister may, upon the recommendation of the Commissioner, by order published in the *Gazette* exempt—

(a) the application of any of the Personal Data Protection Principles under this Act to any data user or class of data users; or

(b) any data user or class of data users from all or any of the provisions of this Act.

(2) The Minister may impose any terms or conditions as he thinks fit in respect of any exemption made under subsection (1).

(3) The Minister may at any time, on the recommendation of the Commissioner, by order published in the *Gazette,* revoke any order made under subsection (1).

PART IV - APPOINTMENT, FUNCTIONS AND POWERS OF COMMISSIONER

Section 47. Appointment of Commissioner

(1) The Minister shall appoint any person as the “Personal Data Protection Commissioner” for the purposes of carrying out the functions and powers assigned to the Commissioner under this Act on such terms and conditions as he thinks desirable.

(2) The appointment of the Commissioner shall be published in the *Gazette*.

(3) The Commissioner appointed under subsection (1) shall be a body corporate having perpetual succession and a common seal.

(4) The Commissioner may sue and be sued in his corporate name.

Section 48. Functions of Commissioner

The Commissioner shall have the following functions:

(a) to advise the Minister on the national policy for personal data protection and all other related matters;

(b) to implement and enforce the personal data protection laws, including the formulation of operational policies and procedures;

(c) to promote and encourage associations or bodies representing data users to prepare codes of practice and to disseminate to their members the codes of practice for the purposes of this Act;

(d) to cooperate with bodies corporate or government agencies for the purpose of performing his functions;

(e) to determine in pursuance of section 129 whether any place outside Malaysia has in place a system for the protection of personal data that is substantially similar to that as provided for under this Act or that serves the same purposes as this Act;

(f) to undertake or cause to be undertaken research into and monitor developments in the processing of personal data, including technology, in order to take account any effects such developments may have on the privacy of individuals in relation to their personal data;

(g) to monitor and supervise compliance with the provisions of this Act, including the issuance of circulars, enforcement notices or any other instruments to any person;

(h) to promote awareness and dissemination of information to the public about the operation of this Act;

(i) to liaise and cooperate with persons performing similar personal data protection functions in any place outside Malaysia in respect of matters of mutual interest, including matters concerning the privacy of individuals in relation to their personal data;

(j) to represent Malaysia through participation in events that relate to personal data protection as authorized by the Minister, whether within or outside Malaysia; and

(k) to carry out such activities and do such things as are necessary, advantageous and proper for the administration of this Act, or such other purposes consistent with this Act as may be directed by the Minister.

Section 49. Powers of Commissioner

(1) The Commissioner shall have all such powers to do all things necessary or expedient for or in connection with the performance of his functions under this Act.

(2) Without prejudice to the generality of subsection (1), the powers of the Commissioner shall include the power—

(a) to collect such fees as may be prescribed by the Minister;

(b) to appoint such agents, experts, consultants or any other persons as he thinks fit to assist him in the performance of his functions;

(c) to formulate human resource development and cooperation programmes for the proper and effective performance of his functions;

(d) to enter into contracts;

(e) to acquire, purchase, take, hold and enjoy any movable or immovable property of every description for the performance of his functions, and to convey, assign, surrender, yield up, charge, mortgage, demise, transfer or otherwise dispose of, or deal with such property or any interest therein vested in him;

(f) to perform such other functions as the Minister may assign from time to time; and

(g) to do all such things as may be incidental to or consequential upon the performance of his functions.

Section 50. Appointment of Deputy Commissioners and Assistant Commissioners

(1) The Commissioner may, with the approval of the Minister, from time to time, appoint such number of public officers as Deputy Commissioners and such number of persons as Assistant Commissioners as are necessary to assist the Commissioner in the performance of his functions and the exercise of his powers under this Act.

(2) The Deputy Commissioners and Assistant Commissioners appointed under subsection (1) shall hold office for such periods, receive such remuneration, allowances or benefits, and shall be subject to such terms and conditions of service as the Commissioner, with the approval of the Minister, may determine.

(3) The Deputy Commissioners and Assistant Commissioners appointed under subsection (1) shall be subject to the supervision, direction and control of the Commissioner.

Section 51. Appointment of other officers and servants

The Commissioner may employ on such terms and conditions as he thinks desirable such officers and servants as may be necessary to assist him in the performance of his functions and the exercise of his powers under this Act.

Section 52. Loans and advances to officers and servants

The Commissioner may grant loans and advances to the officers and servants under section 51 for such purposes and on such terms and conditions as the Commissioner may determine.

Section 53. Tenure of office

Subject to such conditions as may be specified in his instrument of appointment, the Commissioner shall, unless he sooner resigns or vacates his office or his appointment is sooner revoked, hold office for a term not exceeding three years and may be eligible for reappointment.

Section 54. Revocation of appointment and resignation

(1) The Minister may at any time revoke the appointment of the Commissioner and shall state the reason for such revocation.

(2) The Commissioner may at any time resign his office by giving a written notice addressed to the Minister fourteen days prior to the intended date of resignation.

Section 55. Temporary exercise of functions and powers of Commissioner

(1) The Minister may temporarily appoint a Deputy Commissioner to perform the functions and powers of the Commissioner for the period when—

(a) the Commissioner is by reason of illness, leave of absence or any other cause unable to perform his functions for any substantial period; or

(b) the office of the Commissioner is vacant.

(2) A person appointed under subsection (1) shall, during the period in which he is performing the functions and exercising the powers of the Commissioner under this section, be deemed to be the Commissioner.

Section 56. Vacation of office

The office of the Commissioner shall be vacated—

(a) if he dies;

(b) if there has been proved against him, or he has been convicted of, a charge in respect of—

(i) an offence involving fraud, dishonesty or moral turpitude;

(ii) an offence under any law relating to corruption; or

(iii) any other offence punishable with imprisonment (in itself only or in addition to or in lieu of a fine) for more than two years;

(c) if his conduct, whether in connection with his duties as a Commissioner or otherwise, has been such as to bring discredit on the office of the Commissioner;

(d) if he becomes bankrupt;

(e) if he is of unsound mind or is otherwise incapable of discharging his duties;

(f) if his appointment is revoked by the Minister; or

(g) if his resignation is accepted by the Minister.

Section 57. Remuneration and allowances

The Commissioner shall be paid such remuneration and allowances as the Minister may determine after consultation with the Minister of Finance.

Section 58. Delegation of Commissioner’s functions and powers

(1) The Commissioner may, subject to such conditions, limitations or restrictions as he may think fit to impose, delegate any of his functions or powers imposed or conferred upon him under this Act, except his power of delegation, to the Deputy Commissioners or Assistant Commissioners, and any function or power so delegated may be performed and exercised by the officer in the name and on behalf of the Commissioner.

(2) The delegation under subsection (1) shall not preclude the Commissioner himself from performing or exercising at any time the delegated functions or powers.

Section 59. Direction by Minister

(1) The Commissioner shall be responsible to the Minister.

(2) The Minister may give to the Commissioner directions of a general character consistent with

the provisions of this Act relating to the performance of the functions and powers of the Commissioner and the Commissioner shall give effect to such directions.

Section 60. Returns, reports, accounts and information

(1) The Commissioner shall furnish to the Minister and any such public authority as may be directed by the Minister, the returns, reports, accounts and information with respect to his activities as the Minister may require or direct.

(2) Without prejudice to the generality of subsection (1), the Commissioner shall, as soon as practicable after the end of each financial year, cause to be made and transmitted to the Minister and if so directed by the Minister to any other public authority, a report dealing with the activities of the Commissioner during the preceding financial year, and the report shall be in such form and shall contain such information relating to the proceedings and policies of the Commissioner as the Minister may specify.

PART V - PERSONAL DATA PROTECTION FUND

Section 61. Establishment of Fund

(1) For the purposes of this Act, a fund to be known as the “Personal Data Protection Fund” is established.

(2) The Fund shall be controlled, maintained and operated by the Commissioner.

(3) The Fund shall consist of—

(a) such sums as may be provided by Parliament for the purposes of this Act from time to time;

(b) fees, costs and any other charges imposed by or payable to the Commissioner under this Act;

(c) all monies derived from the sale, disposal, lease, hire or any other dealings with the movable or immovable property vested in or acquired by the Commissioner;

(d) all monies as may be paid to the Commissioner from time to time for loans given by the Commissioner; and

(e) all other monies or property which may in any manner become payable to or vested in the Commissioner in respect of any matter incidental to his functions and powers.

Section 62. Expenditure to be charged on Fund

The Fund may be expended for the following purposes:

(a) paying any expenditure lawfully incurred by the Commissioner;

(b) paying any expenses incurred for organizing campaigns, research, studies and publication of materials for the protection of personal data;

(c) paying the remuneration, allowances, benefits and other expenses of the Commissioner, Deputy Commissioners, Assistant Commissioners, members of the Advisory Committee, members, officers and servants of the Appeal Tribunal and officers and servants of the Commissioner, including the granting of loans and advances, superannuation allowances, retirement benefits and gratuities;

(d) paying any other expenses, expenditure, fees and costs, including fees for the engagement of consultants, and legal fees and costs, properly incurred or accepted, or deemed fit by the Commissioner in the performance of his functions and the exercise of his powers;

(e) purchasing or hiring equipment and materials, acquiring land and any assets, and carrying out any other works and undertakings in the performance of his functions and the exercise of his powers; and

(f) generally, paying any expenses for carrying into effect the provisions of this Act.

Section 63. Conservation of Fund

It shall be the duty of the Commissioner to conserve the Fund by so performing his functions and exercising his powers under this Act as to secure that the total revenues of the Commissioner are sufficient to meet all sums properly chargeable to its revenue account, including depreciation and interest on capital, taking one year with another.

Section 64. Reserve fund

The Commissioner shall establish and maintain a reserve fund within the Fund.

Section 65. Financial year

The financial year of the Commissioner shall begin on 1 January and end on 31 December of each year.

Section 66. Limitation on contracts

The Commissioner shall not, without the approval of the Minister and the concurrence of the Minister of Finance, enter into any contract under which the Commissioner is to pay or receive an amount exceeding two million ringgit.

Section 67. Bank accounts

The Commissioner shall open and maintain an account or accounts with such financial institution or financial institutions in Malaysia as the Commissioner, after consulting with the Minister, thinks fit; and every such account shall be operated upon as far as practicable by cheques signed by such persons as may be authorized by the Minister.

Section 68. Accounts and audit

The Commissioner shall cause proper accounts to be kept and maintained in respect of the Fund and in compliance with the provisions of the Statutory Bodies (Accounts and Annual Reports) Act 1980 [*Act 240*].

Section 69. Expenditure and preparation of estimates

(1) The expenditure of the Commissioner up to such amount as may be authorized by the Minister for any one year shall be defrayed out of the Fund.

(2) Before 1 June of each year, the Commissioner shall submit to the Minister an estimate of the expenditure for the following year in such form and containing such particulars as the Minister may direct.

(3) The Minister shall, before 1 January of the following year, notify the Commissioner of the amount authorized for expenditure generally or of the amounts authorized for each description of expenditure based on the estimate prepared under subsection (2).

(4) The Commissioner may at any time submit to the Minister a supplementary estimate of its expenditure for any one year and the Minister may allow the whole or any part of the additional expenditure to be included in the supplementary estimate.

PART VI - PERSONAL DATA PROTECTION ADVISORY COMMITTEE

Section 70. Establishment of Advisory Committee

There is established a Personal Data Protection Advisory Committee.

Section 71. Functions of Advisory Committee

(1) The functions of the Advisory Committee shall be—

(a) to advise the Commissioner on all matters relating to personal data protection, and the due administration and enforcement of this Act; and

(b) to advise the Commissioner on any matter referred by him to the Advisory Committee.

(2) The Commissioner shall not be bound to act upon the advice of the Advisory Committee.

Section 72. Members of Advisory Committee

The Advisory Committee shall consist of the following members to be appointed by the Minister:

(a) a Chairman;

(b) three members from the public sector; and

(c) at least seven but not more than eleven other members.

Section 73. Tenure of office

A member appointed under section 72 shall, unless he sooner resigns or vacates his office or his appointment is sooner revoked, hold office for such period not exceeding three years as the Minister may determine at the time of his appointment, and shall be eligible for reappointment; but no member shall hold office for more than two consecutive terms.

Section 74. Revocation of appointment and resignation

(1) The Minister may at any time revoke the appointment of any member of the Advisory

Committee and shall state the reason for such revocation.

(2) A member of the Advisory Committee appointed under section 72 may at any time resign from his office by giving a written notice addressed to the Minister fourteen days prior to the intended date of resignation.

Section 75. Temporary exercise of functions of Chairman

(1) The Minister may temporarily appoint any member of the Advisory Committee to act as the Chairman for the period when—

(a) the Chairman is by reason of illness, leave of absence or any other cause unable to perform his functions for any substantial period; or

(b) the office of the Chairman is vacant.

(2) A member appointed under subsection (1) shall, during the period in which he is performing the functions of the Chairman under this section, be deemed to be the Chairman.

Section 76. Vacation of office

The office of a member of the Advisory Committee shall be vacated—

(a) if he dies;

(b) if there has been proved against him, or he has been convicted of, a charge in respect of—

(i) an offence involving fraud, dishonesty or moral turpitude;

(ii) an offence under any law relating to corruption; or

(iii) any other offence punishable with imprisonment (in itself only or in addition to or in lieu of a fine) for more than two years;

(c) if his conduct, whether in connection with his duties as a member of the Advisory Committee or otherwise, has been such as to bring discredit on the Advisory Committee;

(d) if he becomes bankrupt;

(e) if he is of unsound mind or is otherwise incapable of discharging his duties;

(f) in the case of the Chairman, if he absents himself from a meeting of the Advisory Committee without leave in writing of the Minister;

(g) in the case of a member of the Advisory Committee other than the Chairman, if he absents himself from three consecutive meetings of the Advisory Committee without leave in writing of the Chairman;

(h) if his appointment is revoked by the Minister; or

(i) if his resignation is accepted by the Minister.

Section 77. Allowances

The Chairman and all other members of the Advisory Committee may be paid such allowances as the Minister may determine after consultation with the Minister of Finance.

Section 78. Time and place of meetings

(1) The Advisory Committee is to hold as many meetings as are necessary for the efficient performance of its functions and such meetings are to be held at such places and times as the Chairman may decide, provided that the Chairman shall not allow more than two months to lapse between meetings.

(2) The Chairman shall call for a meeting if requested to do so in writing by the Minister or by at least four members of the Advisory Committee.

Section 79. Advisory Committee may invite others to attend meetings

(1) The Advisory Committee may invite any person to attend any meeting or deliberation of the Advisory Committee for the purpose of assisting it on any matter under discussion.

(2) A person invited under subsection (1) shall be paid such allowances as may be determined by the Commissioner.

Section 80. Minutes

(1) The Advisory Committee shall cause minutes of all its meetings to be maintained and kept in a proper form.

(2) Minutes made of meetings of the Advisory Committee shall, if duly signed, be admissible in evidence in all legal proceedings without further proof.

(3) Every meeting of the Advisory Committee in respect of the proceedings of which minutes have been so made shall be deemed to have been duly convened and held and all members thereat to have been duly qualified to act.

Section 81. Procedure

The Advisory Committee may regulate its own procedure.

Section 82. Members to devote time to business of Advisory Committee

The members of the Advisory Committee shall devote such time to the business of the Advisory Committee as is necessary to discharge their duties effectively.

PART VII - APPEAL TRIBUNAL

Section 83. Establishment of Appeal Tribunal

There is established an Appeal Tribunal for the purpose of reviewing any of the matters on appeal as set out in section 93.

Section 84. Powers of Appeal Tribunal

(1) The Appeal Tribunal shall have the power—

(a) to summon parties to the proceedings or any other person to attend before it to give evidence in respect of an appeal;

(b) to procure and receive evidence on oath or affirmation, whether written or oral, and examine all such persons as witnesses as the Appeal Tribunal considers necessary;

(c) where a person is so summoned, to require the production of any information, document or other thing in his possession or under his control which the Appeal Tribunal considers necessary for the purposes of the appeal;

(d) to administer any oath, affirmation or statutory declaration, as the case may require;

(e) where a person is so summoned, to allow the payment for any reasonable expenses incurred in connection with his attendance;

(f) to admit evidence or reject evidence adduced, whether oral or documentary, and whether admissible or inadmissible under the provisions of any written law relating to the admissibility of evidence;

(g) to adjourn the hearing of an appeal from time to time, including the power to adjourn to consider its decision; and

(h) generally to direct and do all such matters as may be necessary or expedient for the expeditious decision of the appeal.

(2) The Appeal Tribunal shall have the powers of a subordinate court with regard to the enforcement of attendance of witnesses, hearing evidence on oath or affirmation and punishment for contempt.

Section 85. Members of Appeal Tribunal

(1) The Appeal Tribunal shall consist of the following members who shall be appointed by the Minister:

(a) a Chairman; and

(b) at least two other members, or such greater number of members as the Minister thinks necessary.

(2) The Minister shall appoint a person who is a member of the Judicial and Legal Service of the Federation for at least ten years to be the Chairman of the Appeal Tribunal.

(3) The appointment of the members of the Appeal Tribunal shall be published by notification in the *Gazette*.

Section 86. Secretary to Appeal Tribunal and other officers, etc.

(1) The Minister shall appoint a Secretary to the Appeal Tribunal on such terms and conditions as he thinks desirable.

(2) The Secretary to the Appeal Tribunal shall be responsible for the administration and management of the functions of the Appeal Tribunal.

(3) The Minister may appoint such number of officers and servants as the Minister thinks fit to assist the Secretary to the Appeal Tribunal in carrying out his functions under subsection (2).

(4) The Secretary to the Appeal Tribunal shall have the general control of the officers and servants of the Appeal Tribunal.

(5) For the purposes of this Act, the Secretary to the Appeal Tribunal and the officers appointed under subsection (3) shall be deemed to be officers of the Appeal Tribunal.

Section 87. Tenure of office

A member of the Appeal Tribunal appointed under subsection 85(1) shall, unless he sooner resigns or vacates his office or his appointment is sooner revoked—

(a) hold office for a term not exceeding three years; and

(b) shall be eligible for reappointment upon the expiry of his term of office, but shall not be appointed for more than two consecutive terms.

Section 88. Resignation and revocation of appointment

(1) The Minister may at any time revoke the appointment of a member of the Appeal Tribunal and shall state the reason for such revocation.

(2) A member of the Appeal Tribunal appointed under subsection 85(1) may at any time resign from his office by giving a written notice addressed to the Minister fourteen days prior to the intended date of resignation.

Section 89. Temporary exercise of functions of Chairman

(1) The Minister may temporarily appoint any member of the Appeal Tribunal to act as the Chairman for the period when—

(a) the Chairman is by reason of illness, leave of absence or any other cause unable to perform his functions for any substantial period; or

(b) the office of the Chairman is vacant.

(2) A member appointed under subsection (1) shall, during the period in which he is performing the functions of the Chairman under this section, be deemed to be the Chairman.

Section 90. Vacation of office

The office of a member of the Appeal Tribunal shall be vacated—

(a) if he dies;

(b) if there has been proved against him, or he has been convicted of, a charge in respect of—

(i) an offence involving fraud, dishonesty or moral turpitude;

(ii) an offence under any law relating to corruption; or

(iii) any other offence punishable with imprisonment (in itself only or in addition to or in lieu of a fine) for more than two years;

(c) if his conduct, whether in connection with his duties as a member of the Appeal Tribunal or otherwise, has been such as to bring discredit on the Appeal Tribunal;

(d) if he becomes bankrupt;

(e) if he is of unsound mind or otherwise incapable of discharging his duties;

(f) if he fails to comply with his obligations under section 92;

(g) if his performance as a member of the Appeal Tribunal has been unsatisfactory for a

significant period of time;

(h) if his appointment is revoked by the Minister; or

(i) if his resignation is accepted by the Minister.

Section 91. Allowances

(1) The Chairman of the Appeal Tribunal appointed under paragraph 85(1)*(a)* shall be paid such fixed allowances and other allowances as the Minister may determine.

(2) The other members of the Appeal Tribunal appointed under paragraph 85(1)*(b)* shall be paid—

(a) daily sitting allowances during the sitting of the Appeal Tribunal; and

(b) lodging, travelling and subsistence allowances,

as the Minister may determine.

Section 92. Disclosure of interest

(1) A member of the Appeal Tribunal shall disclose, as soon as practicable, to the Chairman any interest, whether substantial or not, which might conflict with the member's duties as a member of the Appeal Tribunal in a particular matter.

(2) If the Chairman is of the opinion that the member's interest is in conflict with his duties as a member of the Appeal Tribunal, the Chairman shall inform all the parties to the matter of the conflict.

(3) If none of the parties to the matter objects to the conflict, the member may continue to execute his duties as a member of the Appeal Tribunal in relation to that matter.

(4) If a party to the matter objects to the conflict, the member of the Appeal Tribunal shall not continue to execute his duties as a member of the Appeal Tribunal in relation to that matter.

(5) The failure by the member to disclose his interest under subsection (1) shall—

(a) invalidate the decision of the Appeal Tribunal, unless all parties agree to be bound by the decision; and

(b) subject the member to the revocation of his appointment under section 88.

Section 93. Appeal to Appeal Tribunal

(1) Any person who is aggrieved by the decision of the Commissioner under this Act relating to matters, including—

(a) the registration of a data user under Division 2 of Part II;

(b) the refusal of the Commissioner to register a code of practice under subsection 23(5);

(c) the failure of the data user to comply with a data access request or data correction request under Division 4 of Part II;

(d) the issuance of an enforcement notice under section 108;

(e) the refusal of the Commissioner to vary or revoke an enforcement notice under section

109; and

(f) the refusal of the Commissioner to carry out or continue an investigation initiated by a complaint under Part VIII,

may appeal to the Appeal Tribunal by filing a notice of appeal with the Appeal Tribunal.

(2) The notice of appeal shall be made in writing to the Appeal Tribunal within thirty days from the date of the decision of the Commissioner, or in the case of an enforcement notice, within thirty days after the enforcement notice is served upon the relevant data user, and the appellant shall serve a copy of the notice of appeal upon the Commissioner.

(3) The notice of appeal shall state briefly the substance of the decision of the Commissioner against which an appeal is filed with the Appeal Tribunal, contain an address at which any notice or document connected with the appeal may be served upon the appellant or his advocate, and shall be signed by the appellant or his advocate.

Section 94. Record of decision of Commissioner

(1) The aggrieved person referred to in subsection 93(1) may, on his own initiative, request in writing from the Commissioner a statement of the grounds for his decision.

(2) Subject to subsection (3), the Commissioner shall, upon receiving the written request under subsection (1), provide to the aggrieved person, upon the payment of a prescribed fee, a copy of a statement of the grounds for his decision.

(3) Where a notice of appeal has been filed with the Appeal Tribunal under subsection 93(1), the Commissioner shall, if he has not already written the grounds for his decision in respect of the matter stated in the notice under subsection 93(1), record in writing the grounds for his decision, and the written grounds shall form part of the record of proceedings before the Appeal Tribunal.

Section 95. Stay of decision pending appeal

(1) A decision of the Commissioner shall be valid, binding and enforceable pending the decision of an appeal by the Appeal Tribunal, except where an appeal against an enforcement notice has been made to the Appeal Tribunal in accordance with subsection 93(2), or a stay of the decision of the Commissioner has been applied for under subsection (2) and granted by the Appeal Tribunal.

(2) An aggrieved person may apply in writing to the Appeal Tribunal for a stay of the decision of the Commissioner on or after the notice of appeal has been filed with the Appeal Tribunal.

Section 96. Composition of Appeal Tribunal

(1) Every proceeding of the Appeal Tribunal shall be heard and disposed of by three members or such greater uneven number of members of the Appeal Tribunal as the Chairman may in any particular case determine.

(2) In the absence of the Chairman, the senior member of the Appeal Tribunal shall preside.

Section 97. Sitting of Appeal Tribunal

(1) The Appeal Tribunal shall sit on such dates and at such places as the Chairman may appoint.

(2) The Chairman may cancel or postpone any sitting of the Appeal Tribunal or change the place of the sitting which has been appointed under subsection (1).

(3) The Secretary to the Appeal Tribunal shall by written notice inform the parties to the appeal of any change to the date or place of any sitting of the Appeal Tribunal.

Section 98. Procedure of Appeal Tribunal

The Appeal Tribunal may regulate its own procedure.

Section 99. Decision of Appeal Tribunal

(1) The decision of the Appeal Tribunal on any matter shall be decided on a majority of members of the Appeal Tribunal.

(2) A decision of the Appeal Tribunal shall be final and binding on the parties to the appeal.

Section 100. Enforcement of decision of Appeal Tribunal

A decision given by the Appeal Tribunal may, by leave of the Sessions Court, be enforced in the same manner as a judgment or order to the same effect, and where leave is so given, judgment may be entered in terms of the decision.

PART VIII - INSPECTION, COMPLAINT AND INVESTIGATION

Section 101. Inspection of personal data system

(1) The Commissioner may carry out an inspection of—

(a) any personal data system used by data users for the purpose of ascertaining information to assist the Commissioner in making recommendations to the relevant data user relating to the promotion of compliance with the provisions of this Act, in particular the Personal Data Protection Principles, by the relevant data user; or

(b) any personal data system used by data users belonging to a class of data users for the purpose of ascertaining information to assist the Commissioner in making recommendations to the class of data users to which the relevant data user belongs relating to the promotion of compliance with the provisions of this Act, in particular the Personal Data Protection Principles, by the class of data users to which the relevant data user belongs.

(2) For the purposes of this section—

“data user” includes a data processor;

“personal data system” means any system, whether automated or otherwise, which is used, whether in whole or in part, by a data user for the processing of personal data, and includes the record maintained under section 44 and any document and equipment forming part of the system.

Section 102. Relevant data user, etc., to be informed of result of inspection

Where the Commissioner has completed an inspection of a personal data system, he shall in such manner and at such time as he thinks fit inform the relevant data user or class of data users to which the relevant data user belongs of—

(a) the results of the inspection;

(b) any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Act, in particular the Personal Data Protection Principles, by the relevant data user or the class of data users to which the relevant data user belongs; and

(c) such other comments arising from the inspection as he thinks fit.

Section 103. Reports by Commissioner

(1) The Commissioner may, after completing the inspection of any personal data system used by data users belonging to a class of data users, publish a report—

(a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Act, in particular the Personal Data Protection Principles, by the class of data users to which the relevant data users belong; and

(b) in such manner as he thinks fit.

(2) A report published under subsection (1) shall be so framed as to prevent the identity of any individual from being ascertained.

Section 104. Complaint

Any individual or relevant person may make a complaint in writing to the Commissioner about an act, practice or request—

(a) specified in the complaint;

(b) that has been done or engaged in, or is being done or engaged in, by the data user specified in the complaint;

(c) that relates to personal data of which the individual is the data subject; and

(d) that may be a contravention of the provisions of this Act, including any codes of practice.

Section 105. Investigation by Commissioner

(1) Where the Commissioner receives a complaint under section 104, the Commissioner shall, subject to section 106, carry out an investigation in relation to the relevant data user to ascertain whether the act, practice or request specified in the complaint contravenes the provisions of this Act.

(2) Where the Commissioner has reasonable grounds to believe that an act, practice or request has been done or engaged in, or is being done or engaged in, by the relevant data user that relates to personal data and such act, practice or request may be a contravention of the provisions of this Act, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act, practice or request contravenes the provisions of this Act.

(3) The provisions of Part IX shall apply in respect of investigations carried out by the Commissioner under this Part.

Section 106. Restriction on investigation initiated by complaint

(1) The Commissioner may refuse to carry out or continue an investigation initiated by a complaint if he is of the opinion that, having regard to all the circumstances of the case—

(a) the complaint, or a complaint of a substantially similar nature, has previously initiated an investigation as a result of which the Commissioner was of the opinion that there has been no contravention of the provisions of this Act;

(b) the act, practice or request specified in the complaint is trivial;

(c) the complaint is frivolous, vexatious or is not made in good faith; or

(d) any investigation or further investigation is for any other reason unnecessary.

(2) Notwithstanding the generality of the powers conferred on the Commissioner by this Act, the Commissioner may refuse to carry out or continue an investigation initiated by a complaint—

(a) if—

(i) the complainant; or

(ii) in the case where the complainant is a relevant person in relation to a data subject, the data subject or relevant person, as the case may be,

has had actual knowledge of the act, practice or request specified in the complaint for more than two years immediately preceding the date on which the Commissioner received the complaint, unless the Commissioner is satisfied that in all the circumstances of the case it is proper to carry out or continue the investigation;

(b) if the complaint is made anonymously;

(c) if the complainant cannot be identified or traced;

(d) if the Commissioner is satisfied that the relevant data user has not been a data user for a period of not less than two years immediately preceding the date on which the Commissioner received the complaint; or

(e) in any other circumstances as he thinks fit.

(3) Where the Commissioner refuses under this section to carry out or continue an investigation initiated by a complaint, he shall, as soon as practicable but in any case not later than thirty days after the date of receipt of the complaint, by notice in writing served on the complainant inform the complainant of the refusal and of the reasons for the refusal.

(4) An appeal may be made to the Appeal Tribunal against any refusal specified in the notice under subsection (3) by the complainant on whom the notice was served or if the complainant is a relevant person, by the data subject in respect of whom the complainant is the relevant person.

Section 107. Commissioner may carry out or continue investigation initiated by complaint notwithstanding withdrawal of complaint

Where the Commissioner is of the opinion that it is in the public interest so to do, he may carry out or continue an investigation initiated by a complaint notwithstanding that the complainant has withdrawn the complaint and, in any such case, the provisions of this Act shall apply to the complaint and the complainant as if the complaint had not been withdrawn.

Section 108. Enforcement notice

(1) Where, following the completion of an investigation about an act, practice or request specified in the complaint, the Commissioner is of the opinion that the relevant data user—

(a) is contravening a provision of this Act; or

(b) has contravened such a provision in circumstances that make it likely that the contravention will continue or be repeated,

then the Commissioner may serve on the relevant data user an enforcement notice—

(A) stating that he is of that opinion;

(B) specifying the provision of this Act on which he has based that opinion and the reasons why he is of that opinion;

(C) directing the relevant data user to take such steps as are specified in the enforcement notice to remedy the contravention or, as the case may be, the matters occasioning it within such period as is specified in the enforcement notice; and

(D) directing, where necessary, the relevant data user to cease processing the personal data pending the remedy of the contravention by the relevant data user.

(2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention or the matter to which the enforcement notice relates has caused or is likely to cause damage or distress to the data subject of the personal data to which the contravention or matter relates.

(3) The steps as specified in the enforcement notice to remedy the contravention or matter to which the enforcement notice relates may be framed—

(a) to any extent by reference to any approved code of practice; or

(b) so as to afford the relevant data user a choice between different ways of remedying the contravention or matter.

(4) The period specified in the enforcement notice under subsection (1) for taking the steps specified in it shall not expire before the end of the period specified in subsection 93(2) within which an appeal against the enforcement notice may be made and, if such an appeal is made, those steps need not be taken pending the determination or withdrawal of the appeal.

(5) Notwithstanding subsection (4), if the Commissioner is of the opinion that by reason of special circumstances the steps specified in the enforcement notice should be taken as a matter of urgency—

(a) he may include a statement to that effect in the enforcement notice together with the reasons why he is of that opinion; and

(b) where such a statement is so included, subsection (4) shall not apply but the enforcement notice shall not require those steps to be taken before the end of the period of seven days from the date on which the enforcement notice was served.

(6) An appeal may be made to the Appeal Tribunal against an enforcement notice by the relevant data user in accordance with section 93.

(7) Where the Commissioner—

(a) forms an opinion referred to in subsection (1) in respect of the relevant data user at any

time before the completion of an investigation; and

(b) is also of the opinion that, by reason of special circumstances, an enforcement notice should be served on the relevant data user as a matter of urgency,

he may so serve the enforcement notice notwithstanding that the investigation has not been completed and, in any such case—

(A) the Commissioner shall, without prejudice to any other matters to be included in the enforcement notice, specify in the enforcement notice the reasons as to why he is of the opinion referred to in paragraph *(b)*; and

(B) the other provisions of this Act, including this section, shall be construed accordingly.

(8) A person who fails to comply with an enforcement notice commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Section 109. Variation or cancellation of enforcement notice

The Commissioner may, on his own initiative or on the application of a relevant data user, vary or cancel the enforcement notice served under subsection 108(1) by notice in writing to the relevant data user if the Commissioner is satisfied with the action taken by the relevant data user to remedy the contravention.

PART IX – ENFORCEMENT

Section 110. Authorized officers

The Commissioner may in writing authorize any officer appointed under sections 50 and 51 or any public officer to exercise the powers of enforcement under this Act.

Section 111. Authority card

(1) The Commissioner shall issue to each authorized officer an authority card which shall be signed by the Commissioner.

(2) Whenever the authorized officer exercises any of the powers of enforcement under this Act, he shall produce on demand to the person against whom the power is being exercised the authority card issued to him under subsection (1).

Section 112. Power of investigation

(1) An authorized officer may investigate the commission of any offence under this Act.

(2) For the avoidance of doubt, it is declared that for the purposes of this Act, the authorized officer shall have all or any of the special powers of a police officer of whatever rank in relation to police investigations in seizable cases as provided for under the Criminal Procedure Code [*Act 593*], and such powers shall be in addition to the powers provided for under this Act and not in derogation thereof.

Section 113. Search and seizure with warrant

(1) If it appears to a Magistrate, upon written information on oath from the authorized officer and after

such inquiry as the Magistrate considers necessary, that there is reasonable cause to believe that—

(a) any premises has been used for; or

(b) there is in any premises evidence necessary to the conduct of an investigation into,

the commission of an offence under this Act, the Magistrate may issue a warrant authorizing the authorized officer named in the warrant at any reasonable time by day or night and with or without assistance, to enter the premises and if need be by force.

(2) Without affecting the generality of subsection (1), the warrant issued by the Magistrate may authorize the search and seizure of—

(a) any computer, book, account, computerized data or other document which contains or is reasonably suspected to contain information as to any offence suspected to have been committed;

(b) any signboard, card, letter, pamphlet, leaflet or notice representing or implying that the person is registered under this Act; or

(c) any equipment, instrument or article that is reasonably believed to furnish evidence of the commission of the offence.

(3) An authorized officer conducting a search under subsection (1) may, for the purpose of investigating into the offence, search any person who is in or on the premises.

(4) An authorized officer making a search of a person under subsection (3) or section 114 may seize or take possession of, and place in safe custody all things other than the necessary clothing found upon the person, and any of those things which there is reason to believe were the instruments or other evidence of the offence may be detained until the discharge or acquittal of the person.

(5) Whenever it is necessary to cause a woman to be searched, the search shall be made by another woman with strict regard to decency.

(6) If, by the reason of its nature, size or amount, it is not practicable to remove any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized under this section, the authorized officer shall by any means seal such computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article in the premises or container in which it is found.

(7) A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (6) or removes any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so commits an offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding six months or to both.

Section 114. Search and seizure without warrant

If an authorized officer is satisfied upon information received that he has reasonable cause to believe that by reason of delay in obtaining a search warrant under section 113 the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed, the authorized officer may enter the premises and exercise in, upon and in respect of the premises all the powers referred to in section 113 in as full and ample a manner as if he were authorized to do so by a warrant issued under that section.

Section 115. Access to computerized data

(1) An authorized officer conducting a search under sections 113 and 114 shall be given access to computerized data whether stored in a computer or otherwise.

(2) For the purposes of this section, “access”—

(a) includes being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerized data; and

(b) has the meaning assigned to it by subsections 2(2) and (5) of the Computer Crimes Act 1997 [*Act 563*].

Section 116. Warrant admissible notwithstanding defects

A search warrant issued under this Act shall be valid and enforceable notwithstanding any defect, mistake or omission therein or in the application for such warrant, and any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized under such warrant shall be admissible in evidence in any proceedings under this Act.

Section 117. List of computer, book, account, etc., seized

(1) Except as provided in subsection (2), where any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article is seized pursuant to this Act, the authorized officer making the seizure—

(a) shall prepare—

(i) a list of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized and shall sign the list; and

(ii) a written notice of the seizure containing the grounds for the seizure and shall sign the notice; and

(b) shall as soon as practicable serve a copy of the list of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized and the written notice of the seizure to the occupier of the premises which have been searched, or to his agent or servant at those premises.

(2) The written notice of the seizure shall not be required to be served in pursuance of paragraph (1)*(b)* where the seizure is made in the presence of the person against whom proceedings under this Act are intended to be taken, or in the presence of the owner of such property or his agent, as the case may be.

(3) If the premises are unoccupied, the authorized officer shall post a copy of the list of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized conspicuously on the premises.

Section 118. Release of computer, book, account, etc., seized

(1) If any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article has been seized under this Act, the authorized officer who effected the seizure may, after referring to the Public Prosecutor, release the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article to the person as he determines to be lawfully entitled to it, if the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article is not liable to forfeiture under this Act, and is not otherwise required for the purpose of any proceedings under this Act or for the purpose of any prosecution under any other written law, and in such event neither the authorized officer effecting the seizure, nor the Federal Government, Commissioner or any person acting on behalf of the Federal Government or Commissioner shall be liable to any proceedings by any person if the seizure and the release of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article had been effected in good faith.

(2) A record in writing shall be made by the authorized officer effecting the release of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under subsection (1) specifying in detail the circumstances of and the reason for the release, and he shall send a copy of the record to the Public Prosecutor within seven days of the release.

Section 119. No cost or damages arising from seizure to be recoverable

No person shall, in any proceedings before any court in respect of any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized in the exercise or the purported exercise of any power conferred under this Act, be entitled to the costs of such proceedings or to any damages or other relief unless such seizure was made without reasonable cause.

Section 120. Obstruction to search

Any person who—

(a) refuses any authorized officer access to any premise which the authorized officer is entitled to have under this Act or in the execution of any duty imposed or power conferred by this Act;

(b) assaults, obstructs, hinders or delays any authorized officer in effecting any entry which the authorized officer is entitled to effect under this Act, or in the execution of any duty imposed or power conferred by this Act; or

(c) refuses any authorized officer any information relating to an offence or suspected offence under this Act or any other information which may reasonably be required of him and which he has in his knowledge or power to give,

commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding two years or to a fine not exceeding ten thousand ringgit or to both.

Section 121. Power to require production of computer, book, account, etc.

An authorized officer shall, for the purposes of the execution of this Act, have the power to do all or any of the following:

(a) to require the production of any computer, book, account, computerized data or other document kept by the data user or any other person and to inspect, examine and to download from them, make copies of them or take extracts from them;

(b) to require the production of any identification document from any person in relation to any act or offence under this Act;

(c) to make such enquiries as may be necessary to ascertain whether the provisions of this Act have been complied with.

Section 122. Power to require attendance of persons acquainted with case

(1) An authorized officer making an investigation under this Act may by order in writing require the attendance before himself of any person who appears to the authorized officer to be acquainted with the facts and circumstances of the case, and such person shall attend as so required.

(2) If any person refuses or fails to attend as so required, the authorized officer may report such refusal or failure to a Magistrate who shall issue a summons to secure the attendance of such person as may be required by the order made under subsection (1).

Section 123. Examination of persons acquainted with case

(1) An authorized officer making an investigation under this Act may examine orally any person supposed to be acquainted with the facts and circumstances of the case and shall reduce into writing any statement made by the person so examined.

(2) Such person shall be bound to answer all questions relating to the case put to him by the authorized officer:

Provided that such person may refuse to answer any question the answer to which would have a tendency to expose him to a criminal charge or penalty or forfeiture.

(3) A person making a statement under this section shall be legally bound to state the truth, whether or not such statement is made wholly or partly in answer to questions.

(4) The authorized officer examining a person under subsection (1) shall first inform that person of the provisions of subsections (2) and (3).

(5) A statement made by any person under this section shall, whenever possible, be taken down in writing and signed by the person making it or affixed with his thumb print, as the case may be, after it has been read to him in the language in which he made it and after he has been given an opportunity to make any corrections he may wish.

Section 124. Admission of statements in evidence

(1) Except as provided in this section, no statement made by any person to an authorized officer in the course of an investigation made under this Act shall be used in evidence.

(2) When any witness is called for the prosecution or for the defence, other than the accused, the court shall, on the request of the accused or the prosecutor, refer to any statement made by that witness to the authorized officer in the course of the investigation under this Act and may then, if the courts thinks fit in the interest of justice, direct the accused to be furnished with a copy of it and the statement may be used to impeach the credit of the witness in the manner provided by the Evidence

Act 1950 [*Act 56*].

(3) Where the accused had made a statement during the course of an investigation, such statement may be admitted in evidence in support of his defence during the course of the trial.

(4) Nothing in this section shall be deemed to apply to any statement made in the course of an identification parade or falling within section 27 or paragraphs 32(1)*(a)*, *(i)* and *(j)* of the Evidence Act 1950.

(5) When any person is charged with any offence in relation to—

(a) the making; or

(b) the contents,

of any statement made by him to an authorized officer in the course of an investigation made under this Act, that statement may be used as evidence in the prosecution's case.

Section 125. Forfeiture of computer, book, account, etc., seized

(1) Any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized shall be liable to forfeiture.

(2) An order for the forfeiture of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized and liable to forfeiture under this Act shall be made by the court before which the prosecution with regard thereto has been held if it is proved to the satisfaction of the court that an offence under this Act has been committed and that the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized was the subject matter of or was used in the commission of the offence, notwithstanding that no person has been convicted of such offence.

(3) If there is no prosecution with regard to any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized under this Act, such computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article shall be taken and deemed to be forfeited at the expiration of a period of one calendar month from the date of service of a notice to the last-known address of the person from whom the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article was seized indicating that there is no prosecution in respect of such computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article, unless before the expiration of that period a claim thereto is made in the manner set out in subsections (4), (5) and (6).

(4) Any person asserting that he is the owner of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article referred to in subsection (3) and that it is not liable to forfeiture may, personally or by his agent authorized in writing, give written notice to the authorized officer in whose possession such computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article is held that he claims the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article.

(5) On receipt of the notice under subsection (4), the authorized officer shall refer the matter to a Magistrate for his decision.

(6) The Magistrate to whom the matter is referred under subsection (5) shall issue a summons requiring the person asserting that he is the owner of the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article and the person from whom it was seized to appear before the Magistrate, and upon their appearance or default to appear, due service of the summons having been proved, the Magistrate shall proceed to the examination of the matter and, on proof that an offence under this Act has been committed and that the computer, book, account, computerized data or other

document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized was the subject matter of or was used in the commission of such offence, the Magistrate shall order the computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article to be forfeited, and shall, in the absence of such proof, order its release.

(7) Any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article forfeited or deemed to be forfeited shall be delivered to the Commissioner and shall be disposed of in such manner as the Commissioner thinks fit

Section 126. Joinder of offences

Notwithstanding anything contained in section 164 of the Criminal Procedure Code, where a person is accused of more than one offence under this Act, he may be charged with and tried at one trial for any number of such offences committed within the space of any length of time.

Section 127. Power of arrest

(1) An authorized officer or police officer may arrest without warrant any person whom he reasonably believes has committed or is attempting to commit an offence under this Act.

(2) An authorized officer making an arrest under subsection (1) shall without unnecessary delay make over the person so arrested to the nearest police officer or, in the absence of a police officer, take such person to the nearest police station, and thereafter the person shall be dealt with as is provided for by the law relating to criminal procedure for the time being in force as if he had been arrested by a police officer.

PART X – MISCELLANEOUS

Section 128. Register

(1) The Commissioner shall maintain in both physical and electronic forms a register as required under this Act.

(2) A person may on payment of the prescribed fee—

(a) inspect the register; or

(b) make a copy of or take extracts from an entry in the register.

(3) Where a person requests that a copy of an entry in the register be provided in an electronic form, the Commissioner may provide the relevant information by way of electronic means.

Section 129. Transfer of personal data to places outside Malaysia

(1) A data user shall not transfer any personal data of a data subject to a place outside Malaysia unless to such place as specified by the Minister, upon the recommendation of the Commissioner, by notification published in the *Gazette*.

(2) For the purposes of subsection (1), the Minister may specify any place outside Malaysia if—

(a) there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act; or

(b) that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act.

(3) Notwithstanding subsection (1), a data user may transfer any personal data to a place outside Malaysia if—

(a) the data subject has given his consent to the transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the data user;

(c) the transfer is necessary for the conclusion or performance of a contract between the data user and a third party which—

(i) is entered into at the request of the data subject; or

(ii) is in the interests of the data subject;

(d) the transfer is for the purpose of any legal proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights;

(e) the data user has reasonable grounds for believing that in all circumstances of the case—

(i) the transfer is for the avoidance or mitigation of adverse action against the data subject;

(ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and

(iii) if it was practicable to obtain such consent, the data subject would have given his consent;

(f) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Malaysia, would be a contravention of this Act;

(g) the transfer is necessary in order to protect the vital interests of the data subject; or

(h) the transfer is necessary as being in the public interest in circumstances as determined by the Minister.

(4) Where the Commissioner has reasonable grounds for believing that in a place as specified under subsection (1) there is no longer in force any law which is substantially similar to this Act, or that serves the same purposes as this Act—

(a) the Commissioner shall make such recommendations to the Minister who shall, either by cancelling or amending the notification made under subsection (1), cause that place to cease to be a place to which personal data may be transferred under this section; and

(b) the data user shall cease to transfer any personal data of a data subject to such place with effect from the time as specified by the Minister in the notification.

(5) A data user who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

(6) For the purposes of this section, “adverse action”, in relation to a data subject, means any action that may adversely affect the data subject’s rights, benefits, privileges, obligations or interests.

Section 130. Unlawful collecting, etc., of personal data

(1) A person shall not knowingly or recklessly, without the consent of the data user—

(a) collect or disclose personal data that is held by the data user; or

(b) procure the disclosure to another person of personal data that is held by the data user.

(2) Subsection (1) shall not apply to a person who shows—

(a) that the collecting or disclosing of personal data or procuring the disclosure of personal data—

(i) was necessary for the purpose of preventing or detecting a crime or for the purpose of investigations; or

(ii) was required or authorized by or under any law or by the order of a court;

(b) that he acted in the reasonable belief that he had in law the right to collect or disclose the personal data or to procure the disclosure of the personal data to the other person;

(c) that he acted in the reasonable belief that he would have had the consent of the data user if the data user had known of the collecting or disclosing of personal data or procuring the disclosure of personal data and the circumstances of it; or

(d) that the collecting or disclosing of personal data or procuring the disclosure of personal data was justified as being in the public interest in circumstances as determined by the Minister.

(3) A person who collects or discloses personal data or procures the disclosure of personal data in contravention of subsection (1) commits an offence.

(4) A person who sells personal data commits an offenceif he has collected the personal data in contravention of subsection (1).

(5) A person who offers to sell personal data commits an offence if—

(a) he has collected the personal data in contravention of subsection (1); or

(b) he subsequently collects the personal data in contravention of subsection (1).

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale is an offer to sell the personal data.

(7) A person who commits an offence under this section shall, upon conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

Section 131. Abetment and attempt punishable as offences

(1) A person who abets the commission of or who attempts to commit any offence under this Act shall be guilty of that offence and shall, on conviction, be liable to the punishment provided for that offence.

(2) A person who does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall, on conviction, be liable to the punishment provided for the offence:

Provided that any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence.

Section 132. Compounding of offences

(1) The Commissioner may, with the consent in writing of the Public Prosecutor, compound any offence committed by any person under this Act and prescribed to be a compoundable offence by making a written offer to the person suspected to have committed the offence to compound the offence upon payment to the Commissioner of an amount of money not exceeding fifty per centum of the amount of maximum fine for that offence within such time as may be specified in his written offer.

(2) An offer under subsection (1) may be made at any time after the offence has been committed but before any prosecution for it has been instituted, and if the amount specified in the offer is not paid within the time specified in the offer or such extended time as the Commissioner may grant, prosecution for the offence may be instituted at any time after that against the person to whom the offer was made.

(3) Where an offence has been compounded under subsection (1), no prosecution shall be instituted in respect of the offence against the person to whom the offer to compound was made, and any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article seized in connection with the offence may be released or forfeited by the Commissioner, subject to such terms and conditions as he thinks fit to impose in accordance with the conditions of the compound.

(4) All sums of money received by the Commissioner under this section shall be paid into the Federal Consolidated Fund.

Section 133. Offences by body corporate

(1) If a body corporate commits an offence under this Act, any person who at the time of the commission of the offence was a director, chief executive officer, chief operating officer, manager, secretary or other similar officer of the body corporate or was purporting to act in any such capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management—

(a) may be charged severally or jointly in the same proceedings with the body corporate; and

(b) if the body corporate is found to have committed the offence, shall be deemed to have committed that offence unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves—

(i) that the offence was committed without his knowledge, consent or connivance; and

(ii) that he had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

(2) If any person would be liable under this Act to any punishment or penalty for his act, omission, neglect or default, he shall be liable to the same punishment or penalty for every such act, omission, neglect or default of any employee or agent of his, or of the employee of the agent, if the act, omission, neglect or default was committed—

(a) by that person's employee in the course of his employment;

(b) by the agent when acting on behalf of that person; or

(c) by the employee of the agent in the course of his employment by the agent or otherwise on behalf of then agent acting on behalf of that person.

Section 134. Prosecution

No prosecution for an offence under this Act shall be instituted except by or with the written consent of the Public Prosecutor.

Section 135. Jurisdiction to try offences

Notwithstanding any other written law to the contrary, a Sessions Court shall have jurisdiction to try any offence under this Act and to impose full punishment for any such offence under this Act.

Section 136. Service of notices or other documents

(1) Service of a notice or any other document upon any person shall be effected—

(a) by the delivering the notice or other document to the person;

(b) by leaving the notice or other document at the last-known address of residence or place of business of the person in a cover addressed to that person; or

(c) by forwarding the notice or other document by post in an A.R. registered letter addressed to the person at his last-known address of residence or place of business.

(2) Where the person to whom there has been addressed an A.R. registered letter containing any notice or other document which may be given under this Act is informed of the fact that there is an A.R. registered letter awaiting him at a post office, and such person refuses or neglects to take delivery of such A.R. registered letter, such notice or other document shall be deemed to have been served upon him on the date on which he was so informed.

Section 137. Public Authorities Protection Act 1948

The Public Authorities Protection Act 1948 [*Act 198*] shall apply to any action, suit, prosecution or proceedings against the Commissioner, Deputy Commissioner, Assistant Commissioner, any officer or servant of the Commissioner, any member of the Advisory Committee, any member, officer or servant of the Appeal Tribunal, or any authorized officer in respect of any act, neglect or default done or omitted by him or it in such capacity.

Section 138. Public servant

The Commissioner, Deputy Commissioner, Assistant Commissioner, any officer or servant of the Commissioner, any member of the Advisory Committee, any member, officer or servant of the Appeal Tribunal, or any authorized officer while discharging his duty or performing his functions or exercising his powers under this Act in such capacity shall be deemed to be a public servant within the meaning of the Penal Code [*Act 574*].

Section 139. Protection against suit and legal proceedings

No action, suit, prosecution or other proceedings shall lie or be brought, instituted or maintained in any court against—

(a) the Commissioner, Deputy Commissioner, Assistant Commissioner or any officer or servant of the Commissioner;

(b) any member of the Advisory Committee;

(c) any member, officer or servant of the Appeal Tribunal; or\

(d) any authorized officer,

in respect of any act or omission done or omitted by him or it in good faith in such capacity.

Section 140. Protection of informers

(1) Except as provided in subsections (2) and (3), no witness in any civil or criminal proceedings pursuant to this Act shall be obliged or permitted to disclose the name or address of any informer or the substance and nature of the information received from him or state any matter which might lead to his discovery.

(2) If any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article which is in evidence or is liable to inspection in any civil or criminal proceedings whatsoever contains any entry in which any informer is named or described or which might lead to his discovery, the court shall cause all such entries to be concealed from view or to be obliterated in so far as may be necessary to protect the informer from discovery.

(3) If in a trial for any offence under this Act the court, after full inquiry into the case, is of the opinion that the informer wilfully made in his complaint a material statement which he knew or believed to be false or did not believe to be true, or if in any other proceedings the court is of the opinion that justice cannot be fully done between the parties in the proceeding without the discovery of the informer, the court may require the production of the original complaint, if in writing, and permit an inquiry and require full disclosure concerning the informer.

Section 141. Obligation of secrecy

(1) Except for any of the purposes of this Act or for the purposes of any civil or criminal proceedings under any written law or where otherwise authorized by the Minister—

(a) the Commissioner, Deputy Commissioner, Assistant Commissioner, any officer or servant of the Commissioner, any member of the Advisory Committee, any member, officer or servant of the Appeal Tribunal, any authorized officer or any person attending any meeting or deliberation of the Advisory Committee, whether during or after his tenure of office or employment, shall not disclose any information obtained by him in the course of his duties; and

(b) no other person who has by any means access to any information or documents relating to the affairs of the Commissioner shall disclose such information or document.

(2) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both.

Section 142. Things done in anticipation of the enactment of this Act

All acts and things done by any person in preparation for or in anticipation of the enactment of this Act and any expenditure incurred in relation thereto shall be deemed to have been authorized under this Act, provided that the acts and things done are consistent with the general intention and purposes of this Act; and all rights and obligations acquired or incurred as a result of the doing of those acts or things including any expenditure incurred in relation thereto, shall on the coming into operation of this Act be deemed to be the rights and obligations of the Commissioner.

Section 143. Power to make regulation

(1) The Minister may make such regulations as may be necessary or expedient for the purpose of carrying into effect the provisions of this Act.

(2) Without prejudice to the generality of the powers conferred by subsection (1), the Minister may make regulations for all or any of the following purposes:

(a) to regulate all matters relating to the registration of data users under this Act, including to prescribe the registration fees and renewal fees;

(b) to regulate all matters necessary for the implementation of the Personal Data Protection Principles;

(c) to regulate procedures in respect of the inspection of personal data systems, investigation of complaints and issuance of enforcement notices, and all other matters related to it;

(d) to prescribe the offences which may be compounded and the forms to be used and the method and procedure for compounding the offences;

(e) to provide and prescribe for any fees payable in connection with the provision of any service or any matter under this Act;

(f) to prescribe any matter for which this Act makes express provision to be made by regulations;

(g) to prescribe all other matters as are necessary or expedient to be prescribed for giving effect to this Act.

(3) The regulations made under this section or any other subsidiary legislation made under this Act may prescribe for any act or omission in contravention of the regulations or other subsidiary legislation to be an offence and may prescribe for penalties of a fine not exceeding two hundred and fifty thousand ringgit or imprisonment for a term not exceeding two years or to both.

Section 144. Prevention of anomalies

(1) The Minister may, by order published in the *Gazette*, make such modifications to the provisions of this Act as may appear to him to be necessary or expedient for the purpose of removing any difficulties or preventing anomalies in consequence of the coming into operation of this Act.

(2) The Minister shall not exercise the powers conferred by subsection (1) after the expiration of one year from the appointed date.

(3) In this section, "modifications" means amendments, additions, deletions and substitutions of any provisions of this Act.

PART XI - SAVINGS AND TRANSITIONAL PROVISIONS

Section 145. Personal data processed before the date of coming into operation of this Act

Where a data user has collected personal data from the data subject or any third party before the date of coming into operation of this Act, he shall comply with the provisions of this Act within three months from the date of coming into operation of this Act.

Section 146. Registration of persons who process personal data before the date of coming into operation of this Act

(1) Subject to subsection (2), any person who at the date of coming into operation of this Act either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, shall within three months from the date of coming into operation of this Act be registered as a data user in accordance with the provisions of this Act.

(2) Subsection (1) shall not apply to a data user who does not belong to the class of data users who shall be required to be registered as data users in pursuance of the provisions of Division 2 of Part II.

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the "Data Privacy Act of 2012".

SEC. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *Consent of the data subject* refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

(e) *Filing system* refers to any act of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

(f) *Information and Communications System* refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.

(g) *Personal information* refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained

by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:
(1) A person or organization who performs such functions as instructed by another person or organization; and
(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.
(i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
(j) *Processing* refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
(k) *Privileged information* refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
(l) *Sensitive personal information* refers to personal information:
(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
(4) Specifically established by an executive order or an act of Congress to be kept classified.
SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: *Provided*, That the requirements of Section 5 are complied with.
This Act does not apply to the following:
(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:
(1) The fact that the individual is or was an officer or employee of the government institution;
(2) The title, business address and office telephone number of the individual;
(3) The classification, salary range and responsibilities of the position held by the individual; and
(4) The name of the individual on a document prepared by the individual in the course of employment with the government;
(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;
(d) Personal information processed for journalistic, artistic, literary or research purposes;
(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and
(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.
SEC. 5. *Protection Afforded to Journalists and Their Sources.* – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter.
SEC. 6. *Extraterritorial Application.* – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:
(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;
(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:
(1) A contract is entered in the Philippines;
(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and
(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and
(c) The entity has other links in the Philippines such as, but not limited to:
(1) The entity carries on business in the Philippines; and
(2) The personal information was collected or held by an entity in the Philippines.

CHAPTER II
THE NATIONAL PRIVACY COMMISSION

SEC. 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent body to be known as the National Privacy Commission, winch shall have the following functions:
(a) Ensure compliance of personal information controllers with the provisions of this Act;

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;
(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;
(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;
(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;
(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;
(g) Publish on a regular basis a guide to all laws relating to data protection;
(h) Publish a compilation of agency system of records and notices, including index and other finding aids;
(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;
(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers: *Provided,* That the privacy codes shall adhere to the underlying data privacy principles embodied in this Act: *Provided, further,* That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: *Provided, finally.* That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;
(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;
(l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;
(m) Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;
(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;
(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and
(q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.
SEC. 8. *Confidentiality.* – The Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.
SEC. 9. *Organizational Structure of the Commission.* – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as Chairman of the Commission. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be responsible for Data Processing Systems and one to be responsible for Policies and Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years, and may be reappointed for another term of three (3) years. Vacancies in the Commission shall be filled in the same manner in which the original appointment was made.
The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary.
The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.
The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: *Provided*, That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.
SEC. 10. *The Secretariat.* – The Commission is hereby authorized to establish a Secretariat. Majority of the members of the Secretariat must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

CHAPTER III
PROCESSING OF PERSONAL INFORMATION

SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
Personal information must, be:

(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
(b) Processed fairly and lawfully;
(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;
(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and
(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.
The personal information controller must ensure implementation of personal information processing principles set out herein.
SEC. 12. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
(a) The data subject has given his or her consent;
(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.
SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required

by law or regulation permitting the processing of the sensitive personal information or the privileged information;
(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally*, That consent of the data subject was obtained prior to processing;
(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.
SEC. 14. *Subcontract of Personal Information.* – *A* personal information controller may subcontract the processing of personal information: *Provided*, That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.
SEC. 15. *Extension of Privileged Communication.* – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

SEC. 16. *Rights of the Data Subject.* – The data subject is entitled to:
(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;
(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:
(1) Description of the personal information to be entered into the system;
(2) Purposes for which they are being or are to be processed;
(3) Scope and method of the personal information processing;
(4) The recipients or classes of recipients to whom they are or may be disclosed;
(5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
(6) The identity and contact details of the personal information controller or its representative;
(7) The period for which the information will be stored; and
(8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided,* That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena* or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

(c) Reasonable access to, upon demand, the following:

(1) Contents of his or her personal information that were processed;

(2) Sources from which personal information were obtained;

(3) Names and addresses of recipients of the personal information;

(4) Manner by which such data were processed;

(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

SEC. 17. *Transmissibility of Rights of the Data Subject.* – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

SEC. 18. *Right to Data Portability*. – The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

SEC. 19. *Non-Applicability*. – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the

data subject: *Provided*, That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

CHAPTER V
SECURITY OF PERSONAL INFORMATION

SEC. 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

(2) A security policy with respect to the processing of personal information;

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.
(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.
(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

CHAPTER VI
ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.
(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.
(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

CHAPTER VII
SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

SEC 22. *Responsibility of Heads of Agencies.* – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.
SEC. 23. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.* – (a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.
(b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:
(1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;
(2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and

(3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act.

SEC. 24. *Applicability to Government Contractors.* – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

CHAPTER VIII
PENALTIES

SEC. 25. *Unauthorized Processing of Personal Information and Sensitive Personal Information.* – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

SEC. 26. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

SEC. 27. *Improper Disposal of Personal Information and Sensitive Personal Information.* – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information

of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

SEC. 28. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

SEC. 29. *Unauthorized Access or Intentional Breach.* – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

SEC. 30. *Concealment of Security Breaches Involving Sensitive Personal Information.* – The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.

SEC. 31. *Malicious Disclosure.* – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

SEC. 35. *Large-Scale.* – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied.

SEC. 37. *Restitution.* – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

CHAPTER IX
MISCELLANEOUS PROVISIONS

SEC. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

SEC. 39. *Implementing Rules and Regulations (IRR).* – Within ninety (90) days from the effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 40. *Reports and Information.* – The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

SEC. 41. *Appropriations Clause.* – The Commission shall be provided with an initial appropriation of Twenty million pesos (Php20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (Php10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government.

SEC. 42. *Transitory Provision.* – Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transitory period from the effectivity of the IRR or such other period as may be determined by the Commission, to comply with the requirements of this Act.

In case that the DICT has not yet been created by the time the law takes full force and effect, the National Privacy Commission shall be attached to the Office of the President.

SEC. 43. *Separability Clause.* – If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid and subsisting.

SEC. 44. *Repealing Clause.* – The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

SEC. 45. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

Approved,

(Sgd.) **FELICIANO BELMONTE JR.** *Speaker of the House* *of Representatives*	(Sgd.) **JUAN PONCE ENRILE** *President of the Senate*

This Act which is a consolidation of Senate Bill No. 2965 and House Bill No. 4115 was finally passed by the Senate and the House of Representatives on June 6, 2012.

(Sgd.) **MARILYN B. BARUA-YAP** *Secretary General* *House of Representatives*	(Sgd.) **EMMA LIRIO-REYES** *Secretary of the Senate*

Approved: **AUG 15 2012**

(Sgd.) **BENIGNO S. AQUINO III** *President of the Philippines*

REPUBLIC OF SINGAPORE

GOVERNMENT GAZETTE

ACTS SUPPLEMENT

Published by Authority

NO. 25] **FRIDAY, DECEMBER 7** **[2012**

First published in the Government *Gazette*, Electronic Edition, on 3rd December 2012 at 5:00 pm.

The following Act was passed by Parliament on 15th October 2012 and assented to by the President on 20th November 2012:—

PERSONAL DATA PROTECTION ACT 2012

(No. 26 of 2012)

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

1. Short title and commencement
2. Interpretation
3. Purpose
4. Application of Act

PART II

PERSONAL DATA PROTECTION COMMISSION AND ADMINISTRATION

Section
5. Personal Data Protection Commission
6. Functions of Commission
7. Advisory committees
8. Delegation
9. Administration Body
10. Co-operation agreements

PART III

GENERAL RULES WITH RESPECT TO PROTECTION OF PERSONAL DATA

11. Compliance with Act
12. Policies and practices

PART IV

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Division 1 — Consent

13. Consent required
14. Provision of consent
15. Deemed consent
16. Withdrawal of consent
17. Collection, use and disclosure without consent

Division 2 — Purpose

18. Limitation of purpose and extent
19. Personal data collected before appointed day
20. Notification of purpose

PART V

ACCESS TO AND CORRECTION OF PERSONAL DATA

21. Access to personal data
22. Correction of personal data

PART VI

CARE OF PERSONAL DATA

Section
23. Accuracy of personal data
24. Protection of personal data
25. Retention of personal data
26. Transfer of personal data outside Singapore

PART VII

ENFORCEMENT OF PARTS III TO VI

27. Alternative dispute resolution
28. Power to review
29. Power to give directions
30. Enforcement of directions of Commission in District Court
31. Reconsideration of directions or decisions
32. Right of private action

PART VIII

APPEALS TO DATA PROTECTION APPEAL COMMITTEE, HIGH COURT AND COURT OF APPEAL

33. Data Protection Appeal Panel and Data Protection Appeal Committees
34. Appeal from direction or decision of Commission
35. Appeals to High Court and Court of Appeal

PART IX

DO NOT CALL REGISTRY

Division 1 — Preliminary

36. Interpretation of this Part
37. Meaning of "specified message"
38. Application of this Part

Division 2 — Administration

39. Register
40. Applications
41. Evidence
42. Information on terminated Singapore telephone number

Division 3 — Specified message to Singapore telephone number

Section

43. Duty to check register
44. Contact information
45. Calling line identity not to be concealed
46. Consent
47. Withdrawal of consent
48. Defence for employee

PART X

GENERAL

49. Advisory guidelines
50. Powers of investigation
51. Offences and penalties
52. Offences by bodies corporate, etc.
53. Liability of employers for acts of employees
54. Jurisdiction of court
55. Composition of offences
56. General penalties
57. Public servants
58. Evidence in proceedings
59. Preservation of secrecy
60. Protection from personal liability
61. Symbol of Commission
62. Power to exempt
63. Certificate as to national interest
64. Amendment of Schedules
65. Power to make regulations
66. Rules of Court
67. Related and consequential amendments
68. Savings and transitional provision

First Schedule — Constitution and proceedings of Personal Data Protection Commission

Second Schedule — Collection of personal data without consent

Third Schedule — Use of personal data without consent

Fourth Schedule — Disclosure of personal data without consent

Fifth Schedule — Exceptions from access requirement
Sixth Schedule — Exceptions from correction requirement
Seventh Schedule — Constitution and proceedings of Data Protection Appeal Panel and Data Protection Appeal Committees
Eighth Schedule — Exclusion from meaning of "specified message"
Ninth Schedule — Powers of investigation of Commission and inspectors

REPUBLIC OF SINGAPORE

No. 26 of 2012.

I assent.

TONY TAN KENG YAM,
President.
20th November 2012.

LS

An Act to govern the collection, use and disclosure of personal data by organisations, and to establish the Personal Data Protection Commission and Do Not Call Register and to provide for their administration, and for matters connected therewith, and to make related and consequential amendments to various other Acts.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

PART I

PRELIMINARY

Short title and commencement

1. This Act may be cited as the Personal Data Protection Act 2012 and shall come into operation on such date as the Minister may, by notification in the *Gazette*, appoint.

Interpretation

2.—(1) In this Act, unless the context otherwise requires —

"Administration Body" means the Administration Body appointed under section 9;

"advisory committee" means an advisory committee appointed under section 7;

"Appeal Committee" means a Data Protection Appeal Committee nominated under section 33(4);

"Appeal Panel" means the Data Protection Appeal Panel established under section 33(1);

"appointed day" means the date of commencement of Parts III to VI;

"authorised officer", in relation to the exercise of any power or performance of any function or duty under any provision of this Act, means a person to whom the exercise of that power or performance of that function or duty under that provision has been delegated under section 8(2);

"benefit plan" means an insurance policy, a pension plan, an annuity, a provident fund plan or other similar plan;

"business" includes the activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity;

"business contact information" means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax

number and any other similar information about the individual, not provided by the individual solely for his personal purposes;

"Chairman" means the Chairman of the Commission appointed under paragraph 1(1) of the First Schedule;

"Commission" means the Personal Data Protection Commission established under section 5;

"credit bureau" means an organisation which —

(*a*) provides credit reports for gain or profit; or

(*b*) provides credit reports on a routine, non-profit basis as an ancillary part of a business carried on for gain or profit;

"credit report" means a communication, whether in written, oral or other form, provided to an organisation to assess the creditworthiness of an individual in relation to a transaction between the organisation and the individual;

"data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation;

"document" includes information recorded in any form;

"domestic" means related to home or family;

"education institution" means any organisation that provides education, including instruction, training or teaching, whether by itself or in association or collaboration with or by affiliation with any other person;

"employee" includes a volunteer;

"employment" includes working under an unpaid volunteer work relationship;

"evaluative purpose" means —

(*a*) for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates —

(i) for employment or for appointment to office;

(ii) for promotion in employment or office or for continuance in employment or office;

(iii) for removal from employment or office;

(iv) for admission to an education institution;

(v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits;

(vi) for selection for an athletic or artistic purpose; or

(vii) for grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;

(*b*) for the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;

(*c*) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or

(*d*) for such other similar purposes as may be prescribed by the Minister;

"individual" means a natural person, whether living or deceased;

"investigation" means an investigation relating to —

(*a*) a breach of an agreement;

(*b*) a contravention of any written law, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(*c*) a circumstance or conduct that may result in a remedy or relief being available under any law;

"national interest" includes national defence, national security, public security, the maintenance of essential services and the conduct of international affairs;

"organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not —

(*a*) formed or recognised under the law of Singapore; or

(*b*) resident, or having an office or a place of business, in Singapore;

"personal data" means data, whether true or not, about an individual who can be identified —

(*a*) from that data; or

(*b*) from that data and other information to which the organisation has or is likely to have access;

"prescribed healthcare body" means a healthcare body, prescribed for the purposes of the Fourth Schedule by the Minister charged with the responsibility for health;

"prescribed law enforcement agency" means an authority charged with the duty of investigating offences or charging offenders under written law, prescribed for the purposes of section 21(4) and the Fourth Schedule by the Minister charged with the responsibility for that authority;

"private trust" means a trust for the benefit of one or more designated individuals who are friends, or members of the family, of the settlor;

"proceedings" means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of —

(*a*) a breach of an agreement;

(*b*) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(*c*) a wrong or a breach of a duty for which a remedy is claimed under any law;

"processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

(*a*) recording;

(*b*) holding;

(*c*) organisation, adaptation or alteration;

(*d*) retrieval;

(*e*) combination;

(*f*) transmission;

(*g*) erasure or destruction;

"public agency" includes —

(*a*) the Government, including any ministry, department, agency, or organ of State;

(*b*) any tribunal appointed under any written law; or

(*c*) any statutory body specified under subsection (2);

"publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event —

(*a*) at which the individual appears; and

(*b*) that is open to the public;

"relevant body" means the Commission, the Administration Body, the Appeal Panel or any Appeal Committee;

"tribunal" includes a judicial or quasi-judicial body or a disciplinary, an arbitral or a mediatory body.

(2) The Minister may, by notification in the *Gazette*, specify any statutory body established under a public Act for a public function to be a public agency for the purposes of this Act.

Purpose

3. The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

Application of Act

4.—(1) Parts III to VI shall not impose any obligation on —

(*a*) any individual acting in a personal or domestic capacity;

(*b*) any employee acting in the course of his employment with an organisation;

(*c*) any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data; or

(*d*) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of this provision.

(2) Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data)) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

(3) An organisation shall have the same obligation under this Act in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

(4) This Act shall not apply in respect of —

(*a*) personal data about an individual that is contained in a record that has been in existence for at least 100 years; or

(*b*) personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) shall apply in respect

of personal data about an individual who has been dead for 10 years or fewer.

(5) Except where business contact information is expressly referred to, Parts III to VI shall not apply to business contact information.

(6) Unless otherwise expressly provided in this Act —

(*a*) nothing in Parts III to VI shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening this Act; and

(*b*) the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law.

PART II

PERSONAL DATA PROTECTION COMMISSION AND ADMINISTRATION

Personal Data Protection Commission

5.—(1) There shall be established a Personal Data Protection Commission consisting of not fewer than 3 but not more than 17 members appointed by the Minister.

(2) The First Schedule shall have effect with respect to the Commission, its members and its proceedings.

Functions of Commission

6. The functions of the Commission shall be —

(*a*) to promote awareness of data protection in Singapore;

(*b*) to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection;

(*c*) to advise the Government on all matters relating to data protection;

(*d*) to represent the Government internationally on matters relating to data protection;

(*e*) to conduct research and studies and promote educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities;

(*f*) to manage technical co-operation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or inter-governmental organisations, on its own behalf or on behalf of the Government;

(*g*) to administer and enforce this Act;

(*h*) to carry out functions conferred on the Commission under any other written law; and

(*i*) to engage in such other activities and perform such functions as the Minister may permit or assign to the Commission by order published in the *Gazette*.

Advisory committees

7.—(1) The Minister may appoint one or more advisory committees to provide advice to the Commission with regard to the performance of any of its functions under this Act.

(2) The Commission may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Act but shall not be bound by such consultation.

Delegation

8.—(1) The Commission may appoint by name or office such number of inspectors and other officers, being public officers or employees of a statutory body, as the Commission thinks fit.

(2) The Commission may delegate the exercise of all or any of its functions, duties and powers under this Act (except the power of delegation conferred by this subsection) to any officer appointed

under subsection (1), subject to such conditions or limitations as the Commission may specify.

(3) In exercising any of the powers of enforcement under this Act, an authorised officer shall on demand produce to the person against whom he is acting the authority issued to him by the Commission.

(4) Any decision of the Commission or of any person to whom any function, duty or power has been delegated by the Commission may be signified under the hand of the Chairman or any person authorised by the Chairman to sign on his behalf.

Administration Body

9.—(1) The Minister may, by notification in the *Gazette*, appoint an Administration Body.

(2) The Administration Body —

(*a*) may advise the Minister on any matter relating to the management and administration of the Commission that the Administration Body considers appropriate or that is referred to the Administration Body by the Minister;

(*b*) may enter into agreements for the purposes of the Commission, including any co-operation agreement;

(*c*) shall manage the budget for the Commission, and accounts and records of transactions and affairs relating to the Commission;

(*d*) shall submit such reports relating to the affairs of the Commission as the Minister may require; and

(*e*) may provide the Commission with such administrative and other support as may be required.

(3) Proceedings in respect of an offence under this Act may, with the authorisation of the Public Prosecutor, be conducted by an officer of the Administration Body who is authorised in writing in that behalf by the Chairman.

(4) Notwithstanding the provisions of any written law, a legal counsel (by whatever name called) of the Administration Body who

has been admitted as an advocate and solicitor under the Legal Profession Act (Cap. 161) may —

(*a*) appear in any civil proceedings involving the Commission in the performance of its functions or duties under any written law; and

(*b*) make and do all acts and applications in respect of the civil proceedings on behalf of the Commission.

Co-operation agreements

10.—(1) For the purposes of sections 9 and 59, a co-operation agreement is an agreement for the purposes of —

(*a*) facilitating co-operation between the Commission and another regulatory authority in the performance of their respective functions in so far as those functions relate to data protection; and

(*b*) avoiding duplication of activities by the Commission and another regulatory authority, being activities involving the enforcement of data protection laws.

(2) A co-operation agreement may include provisions —

(*a*) to enable the Commission and the other regulatory authority to furnish to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;

(*b*) to provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and

(*c*) to enable the Commission and the other regulatory authority to forbear to perform any of their respective functions in relation to a matter in circumstances where it is satisfied that the other is performing functions in relation to that matter.

(3) The Commission shall not furnish any information to a foreign data protection body pursuant to a co-operation agreement unless it requires of, and obtains from, that body an undertaking in writing by it that it will comply with terms specified in that requirement, including

terms that correspond to the provisions of any written law concerning the disclosure of that information by the Commission.

(4) The Commission may give an undertaking to a foreign data protection body that it will comply with terms specified in a requirement made of the Commission by the foreign data protection body to give such an undertaking where —

(*a*) those terms correspond to the provisions of any law in force in the country or territory in which the foreign data protection body is established, being provisions which concern the disclosure by the foreign data protection body of the information referred to in paragraph (*b*); and

(*b*) compliance with the requirement is a condition imposed by the foreign data protection body for furnishing information in its possession to the Commission pursuant to a co-operation agreement.

(5) In this section —

"foreign data protection body" means a body in whom there are vested functions under the law of another country or territory with respect to the enforcement or the administration of provisions of law of that country or territory concerning data protection;

"regulatory authority" includes the Commission and any foreign data protection body.

PART III

GENERAL RULES WITH RESPECT TO PROTECTION OF PERSONAL DATA

Compliance with Act

11.—(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.

(2) An organisation is responsible for personal data in its possession or under its control.

(3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.

(4) An individual designated under subsection (3) may delegate to another individual the responsibility conferred by that designation.

(5) An organisation shall make available to the public the business contact information of at least one of the individuals designated under subsection (3) or delegated under subsection (4).

(6) The designation of an individual by an organisation under subsection (3) shall not relieve the organisation of any of its obligations under this Act.

Policies and practices

12. An organisation shall —

(*a*) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act;

(*b*) develop a process to receive and respond to complaints that may arise with respect to the application of this Act;

(*c*) communicate to its staff information about the organisation's policies and practices referred to in paragraph (*a*); and

(*d*) make information available on request about —

(i) the policies and practices referred to in paragraph (*a*); and

(ii) the complaint process referred to in paragraph (*b*).

PART IV

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Division 1 — Consent

Consent required

13. An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —

(*a*) the individual gives, or is deemed to have given, his consent under this Act to the collection, use or disclosure, as the case may be; or

(*b*) the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or any other written law.

Provision of consent

14.—(1) An individual has not given consent under this Act for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless —

(*a*) the individual has been provided with the information required under section 20; and

(*b*) the individual provided his consent for that purpose in accordance with this Act.

(2) An organisation shall not —

(*a*) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or

(*b*) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices.

(3) Any consent given in any of the circumstances in subsection (2) is not validly given for the purposes of this Act.

(4) In this Act, references to consent given, or deemed to have been given, by an individual for the collection, use or disclosure of personal data about the individual shall include consent given, or deemed to have been given, by any person validly acting on behalf of that individual for the collection, use or disclosure of such personal data.

Deemed consent

15.—(1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if —

(*a*) the individual, without actually giving consent referred to in section 14, voluntarily provides the personal data to the organisation for that purpose; and

(*b*) it is reasonable that the individual would voluntarily provide the data.

(2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation.

Withdrawal of consent

16.—(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

(2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of the likely consequences of withdrawing his consent.

(3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal.

(4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the

consent of the individual is required or authorised under this Act or other written law.

Collection, use and disclosure without consent

17.—(1) An organisation may collect personal data about an individual, without consent or from a source other than the individual, only in the circumstances and subject to any condition in the Second Schedule.

(2) An organisation may use personal data about an individual, without the consent of the individual, only in the circumstances and subject to any condition in the Third Schedule.

(3) An organisation may disclose personal data about an individual, without the consent of the individual, only in the circumstances and subject to any condition in the Fourth Schedule.

Division 2 — Purpose

Limitation of purpose and extent

18. An organisation may collect, use or disclose personal data about an individual only for purposes —

(*a*) that a reasonable person would consider appropriate in the circumstances; and

(*b*) that the individual has been informed of under section 20, if applicable.

Personal data collected before appointed day

19. Notwithstanding the other provisions in this Part, an organisation may use personal data about an individual collected before the appointed day for the purposes for which the personal data was collected unless —

(*a*) consent for such use is withdrawn in accordance with section 16; or

(*b*) the individual, whether before, on or after the appointed day, has otherwise indicated to the organisation that he does not consent to the use of the personal data.

Notification of purpose

20.—(1) For the purposes of sections 14(1)(*a*) and 18(*b*), an organisation shall inform the individual of —

(*a*) the purposes for the collection, use or disclosure of the personal data, as the case may be, on or before collecting the personal data;

(*b*) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph (*a*), before the use or disclosure of the personal data for that purpose; and

(*c*) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data.

(2) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act.

(3) Subsection (1) shall not apply if —

(*a*) the individual is deemed to have consented to the collection, use or disclosure, as the case may be, under section 15; or

(*b*) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 17.

(4) Notwithstanding subsection (3), an organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship between the organisation and that individual, shall inform the individual of —

(*a*) that purpose; and

(*b*) on request by the individual, the business contact information of a person who is able to answer the individual's questions

about that collection, use or disclosure on behalf of the organisation.

PART V

ACCESS TO AND CORRECTION OF PERSONAL DATA

Access to personal data

21.—(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with —

(*a*) personal data about the individual that is in the possession or under the control of the organisation; and

(*b*) information about the ways in which the personal data referred to in paragraph (*a*) has been or may have been used or disclosed by the organisation within a year before the date of the request.

(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.

(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —

(*a*) threaten the safety or physical or mental health of an individual other than the individual who made the request;

(*b*) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

(*c*) reveal personal data about another individual;

(*d*) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

(*e*) be contrary to the national interest.

(4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(*f*) or (*n*) of the Fourth Schedule or under any other written law.

(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4).

Correction of personal data

22.—(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation.

(2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall —

(*a*) correct the personal data as soon as practicable; and

(*b*) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

(3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made.

(4) When an organisation is notified under subsection (2)(*b*) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made.

(5) If no correction is made under subsection (2)(*a*) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made.

(6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion.

(7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule.

PART VI

CARE OF PERSONAL DATA

Accuracy of personal data

23. An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data —

(*a*) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or

(*b*) is likely to be disclosed by the organisation to another organisation.

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Retention of personal data

25. An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —

(*a*) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(*b*) retention is no longer necessary for legal or business purposes.

Transfer of personal data outside Singapore

26.—(1) An organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under this Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Act.

(2) The Commission may, on the application of any organisation, by notice in writing exempt the organisation from any requirement prescribed pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2) —

(*a*) may be granted subject to such conditions as the Commission may specify in writing; and

(*b*) need not be published in the *Gazette* and may be revoked at any time by the Commission.

(4) The Commission may at any time add to, vary or revoke any condition imposed under this section.

PART VII

ENFORCEMENT OF PARTS III TO VI

Alternative dispute resolution

27.—(1) If the Commission is of the opinion that any complaint by an individual against an organisation may more appropriately be resolved by mediation, the Commission may, with the consent of the complainant and the organisation, refer the matter for mediation.

(2) Subject to subsection (1), the Commission may, with or without the consent of the complainant and the organisation, direct a complainant or the organisation or both to attempt to resolve the complaint of the individual in the way directed by the Commission.

Power to review

28.—(1) On the application of a complainant, the Commission may review —

(*a*) a refusal to provide access to personal data requested by the complainant under section 21, or a failure to provide such access within a reasonable time;

(*b*) a fee required from the complainant by an organisation in relation to a request by the complainant under section 21 or 22; or

(*c*) a refusal to correct personal data in accordance with a request by the complainant under section 22, or a failure to make such correction within a reasonable time.

(2) Upon completion of its review under subsection (1), the Commission may —

(*a*) confirm the refusal to provide access to the personal data, or direct the organisation to provide access to the personal data, within such time as the Commission may specify;

(*b*) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant; or

(*c*) confirm the refusal to correct the personal data, or direct the organisation to correct the personal data, in such manner and within such time as the Commission may specify.

Power to give directions

29.—(1) The Commission may, if it is satisfied that an organisation is not complying with any provision in Parts III to VI, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision.

(2) Without prejudice to the generality of subsection (1), the Commission may, if it thinks fit in the circumstances to ensure compliance with Parts III to VI, give the organisation all or any of the following directions:

(*a*) to stop collecting, using or disclosing personal data in contravention of this Act;

(*b*) to destroy personal data collected in contravention of this Act;

(*c*) to comply with any direction of the Commission under section 28(2);

(*d*) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

(3) Subsection (2)(*d*) shall not apply in relation to any failure to comply with a provision of this Act, the breach of which is an offence under this Act.

(4) The Commission shall, in any direction requiring the payment of a financial penalty, specify the date before which the financial penalty is to be paid, being a date not earlier than the end of the period within which an application for reconsideration of the direction, or an appeal against the direction, may be brought under section 31 or 34, respectively.

(5) The interest payable on the outstanding amount of any financial penalty imposed under subsection (2)(*d*) and for payment by instalment (as may be directed by the Commission in its discretion) of any financial penalty imposed under subsection (2)(*d*) shall be at such rate as the Commission may direct, which shall not exceed the rate prescribed in the Rules of Court in respect of judgment debts.

(6) Any interest ordered to be paid under subsection (5) shall form part of the penalty payable and be enforced in accordance with section 30.

Enforcement of directions of Commission in District Court

30.—(1) For the purposes of enforcement of any direction made by the Commission under section 28(2) or 29, the Commission may apply for the direction to be registered in a District Court in accordance with the Rules of Court and the District Court shall register the direction in accordance with the Rules of Court.

(2) From the date of registration of any direction under subsection (1), the direction shall be of the same force and effect, and all proceedings may be taken on the direction, for the purposes of enforcement as if it had been an order originally obtained in the District Court which shall have power to enforce it accordingly.

(3) A District Court shall have jurisdiction to enforce any direction in accordance with subsection (2) regardless of the monetary amount involved and may, for the purpose of enforcing such direction, make any order —

(*a*) to secure compliance with the direction; or

(*b*) to require any person to do anything to remedy, mitigate or eliminate any effects arising from —

(i) anything done which ought not, under the direction, to have been done; or

(ii) anything not done which ought, under the direction, to have been done,

which would not have occurred had the direction been complied with.

Reconsideration of directions or decisions

31.—(1) An organisation or individual aggrieved by —

(*a*) any direction made by the Commission under section 27(2) or section 29(1) or (2); or

(*b*) any direction or decision made under section 28(2),

may, within 28 days after the issue of the direction or decision concerned, make a written application to the Commission to reconsider the direction or decision.

(2) Unless the Commission decides otherwise in any particular case, an application for reconsideration shall not suspend the effect of the direction or decision to be reconsidered except in the case of an application for reconsideration of a direction to pay a financial penalty or of the amount thereof.

(3) The application for reconsideration shall be made in such form and manner as the Commission may require and shall set out the grounds on which the applicant is requesting the reconsideration.

(4) If any application for reconsideration is made in accordance with this section, the Commission shall —

(*a*) reconsider the direction or decision;

(*b*) affirm, revoke or vary the direction or decision as the Commission thinks fit; and

(*c*) notify the applicant in writing of the result of the reconsideration.

(5) There shall be no application for reconsideration of a decision made under subsection (4)(*b*).

Right of private action

32.—(1) Any person who suffers loss or damage directly as a result of a contravention of any provision in Part IV, V or VI by an organisation shall have a right of action for relief in civil proceedings in a court.

(2) If the Commission has made a decision under this Act in respect of a contravention specified in subsection (1), no action accruing under subsection (1) may be brought in respect of that contravention until after the decision has become final as a result of there being no further right of appeal.

(3) The court may grant to the plaintiff in an action under subsection (1) all or any of the following:

(*a*) relief by way of injunction or declaration;

(*b*) damages;

(*c*) such other relief as the court thinks fit.

PART VIII

APPEALS TO DATA PROTECTION APPEAL COMMITTEE, HIGH COURT AND COURT OF APPEAL

Data Protection Appeal Panel and Data Protection Appeal Committees

33.—(1) There shall be established a Data Protection Appeal Panel.

(2) The Minister shall appoint the members of the Appeal Panel.

(3) The Chairman of the Appeal Panel shall be appointed by the Minister from among the members of the Appeal Panel.

(4) For the purpose of hearing any appeal under section 34, the Chairman of the Appeal Panel may nominate a Data Protection Appeal Committee comprising 3 or more members of the Appeal Panel.

(5) The Seventh Schedule shall have effect with respect to the Appeal Panel, Appeal Committees and their members and the proceedings of Appeal Committees, as the case may be.

Appeal from direction or decision of Commission

34.—(1) Any organisation or individual aggrieved by —

(*a*) any direction made by the Commission under section 27(2) or section 29(1) or (2);

(*b*) any direction or decision made by the Commission under section 28(2); or

(*c*) any decision made by the Commission under section 31(4)(*b*),

may, within 28 days after the issue of the direction or decision concerned, appeal to the Chairman of the Appeal Panel against that direction or decision.

(2) Where any application for reconsideration has been made under section 31, every appeal in respect of the same direction or decision which is the subject of the application for reconsideration shall be deemed to be withdrawn.

(3) Unless the Appeal Committee decides otherwise in any particular case, the making of an appeal under this section shall not suspend the effect of the direction or decision to which the appeal relates except in the case of an appeal against the imposition of a financial penalty or the amount thereof.

(4) An Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal, and, in particular, may —

(*a*) remit the matter to the Commission;

(*b*) impose or revoke, or vary the amount of, a financial penalty;

(*c*) give such direction, or take such other step, as the Commission could itself have given or taken; or

(*d*) make any other direction or decision which the Commission could itself have made.

(5) Any direction or decision of an Appeal Committee on an appeal has the same effect, and may be enforced in the same manner, as a direction or decision of the Commission, except that there shall be no application for further reconsideration under section 31 and no further appeal under this section from any direction or decision of the Appeal Committee.

(6) If an Appeal Committee confirms the direction or decision which is the subject of the appeal, it may nevertheless set aside any finding of fact on which the direction or decision was based.

Appeals to High Court and Court of Appeal

35.—(1) An appeal against, or with respect to, a direction or decision of an Appeal Committee shall lie to the High Court —

(*a*) on a point of law arising from a direction or decision of the Appeal Committee; or

(*b*) from any direction of the Appeal Committee as to the amount of a financial penalty.

(2) An appeal under this section may be made only at the instance of —

(*a*) the organisation aggrieved by the direction or decision of the Appeal Committee;

(*b*) if the decision relates to a complaint, the complainant; or

(*c*) the Commission.

(3) The High Court shall hear and determine any such appeal and may —

(*a*) confirm, modify or reverse the direction or decision of the Appeal Committee; and

(*b*) make such further or other order on such appeal, whether as to costs or otherwise, as the Court may think fit.

(4) There shall be such further right of appeal from decisions of the High Court under this section as exists in the case of decisions made by that Court in the exercise of its original civil jurisdiction.

PART IX

DO NOT CALL REGISTRY

Division 1 — Preliminary

Interpretation of this Part

36.—(1) In this Part, unless the context otherwise requires —

"calling line identity" means the telephone number or information identifying the sender;

"financial services" has the same meaning as in section 2 of the Consumer Protection (Fair Trading) Act (Cap. 52A);

"goods" means any personal property, whether tangible or intangible, and shall be deemed to include —

(*a*) chattels that are attached or intended to be attached to real property on or after delivery;

(*b*) financial products and credit, including credit extended solely on the security of land;

(*c*) any residential property; or

(*d*) a voucher;

"message" means any message, whether in sound, text, visual or other form;

"register" means any Do Not Call Register kept and maintained under section 39;

"send", in relation to a message, means —

(*a*) to send the message, cause the message to be sent, or authorise the sending of the message; or

(*b*) to make a voice call containing the message, cause a voice call containing the message to be made, or

authorise the making of a voice call containing the message;

"sender", in relation to a message, means a person —

(*a*) who sends the message, causes the message to be sent, or authorises the sending of the message; or

(*b*) who makes a voice call containing the message, causes a voice call containing the message to be made, or authorises the making of a voice call containing the message;

"services" includes —

(*a*) a service offered or provided that involves the addition to or maintenance, repair or alteration of goods or any residential property;

(*b*) a membership in any club or organisation if the club or organisation is a business formed to make a profit for its owners;

(*c*) the right to use time share accommodation under a time share contract; and

(*d*) financial services;

"Singapore telephone number" means —

(*a*) a telephone number, with 8 digits beginning with the digit "3", "6", "8" or "9", that is in accordance with the National Numbering Plan referred to in regulation 12A of the Telecommunications (Class Licences) Regulations (Cap. 323, Rg 3); or

(*b*) any other telephone numbers as may be prescribed;

"subscriber", in relation to a Singapore telephone number, means the subscriber of the telecommunications service to which the Singapore telephone number is allocated;

"time share accommodation" means any living accommodation, in Singapore or elsewhere, used or intended to be used (wholly or partly) for leisure purposes by a class of persons all of whom have rights to use, or participate in arrangements

under which they may use, that accommodation or accommodation within a pool of accommodation to which that accommodation belongs;

"time share contract" means a contract which confers or purports to confer on an individual time share rights that are exercisable during a period of not less than 3 years;

"voice call" includes —

(*a*) a call that involves a recorded or synthetic voice; or

(*b*) in the case of a recipient with a disability (for example, a hearing impairment), a call that is equivalent to a voice call,

whether or not the recipient responds by way of pressing buttons on a telephone handset or similar telecommunications device.

(2) For the purposes of this Part, a telecommunications service provider who merely provides a service that enables a specified message to be sent shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorised the message to be sent.

(3) For the purposes of this Part, if a specified message is sent and at the relevant time the telecommunications device, service or network from which it was sent was controlled by a person without the knowledge of the owners or authorised users of the telecommunications device, service or network, the owners or authorised users shall, unless the contrary is proved, be presumed not to have sent the message and not to have authorised the sending of the message.

(4) In subsection (3), "control" means either physical control or control through the use of software or other means.

Meaning of "specified message"

37.—(1) Subject to subsection (5), for the purposes of this Part, a specified message is a message, where, having regard to —

(*a*) the content of the message;

(*b*) the presentational aspects of the message;

(*c*) the content that can be obtained using the numbers, URLs or contact information (if any) mentioned in the message; and

(*d*) if the telephone number from which the message is made is disclosed to the recipient (whether by calling line identity or otherwise), the content (if any) that can be obtained by calling that number,

it would be concluded that the purpose, or one of the purposes, of the message is —

(i) to offer to supply goods or services;

(ii) to advertise or promote goods or services;

(iii) to advertise or promote a supplier, or prospective supplier, of goods or services;

(iv) to offer to supply land or an interest in land;

(v) to advertise or promote land or an interest in land;

(vi) to advertise or promote a supplier, or prospective supplier, of land or an interest in land;

(vii) to offer to provide a business opportunity or an investment opportunity;

(viii) to advertise or promote a business opportunity or an investment opportunity;

(ix) to advertise or promote a provider, or prospective provider, of a business opportunity or an investment opportunity; or

(x) any other prescribed purpose related to obtaining or providing information.

(2) For the purposes of subsection (1)(i) to (x), it is immaterial whether —

(*a*) the goods, services, land, interest or opportunity exist; or

(*b*) it is lawful to acquire the goods, services, land or interest or take up the opportunity.

(3) Subject to subsection (4), a person who authorises another person to offer, advertise or promote the first person's goods, services, land, interest or opportunity shall be deemed to have authorised the sending of any message sent by the second person that offers, advertises or promotes that first person's goods, services, land, interest or opportunity.

(4) For the purposes of subsection (3), a person who takes reasonable steps to stop the sending of any message referred to in that subsection shall be deemed not to have authorised the sending of the message.

(5) For the purposes of this Part, a specified message shall not include any message referred to in the Eighth Schedule.

Application of this Part

38. This Part shall apply to a specified message addressed to a Singapore telephone number where —

(*a*) the sender of the specified message is present in Singapore when the specified message is sent; or

(*b*) the recipient of the specified message is present in Singapore when the specified message is accessed.

Division 2 — Administration

Register

39.—(1) The Commission shall cause to be kept and maintained one or more registers of Singapore telephone numbers, each known as a Do Not Call Register, for the purposes of this Part.

(2) Each register shall be kept in such form and shall contain such particulars as the Commission thinks fit.

(3) The Commission may authorise another person to maintain any register, on its behalf, subject to such conditions or restrictions as the Commission may think fit.

Applications

40.—(1) A subscriber may apply to the Commission, in the form and manner prescribed —

(*a*) to add his Singapore telephone number to a register; or

(*b*) to remove his Singapore telephone number from a register.

(2) Any person may apply to the Commission, in the form and manner required by the Commission, to confirm whether any Singapore telephone number is listed in a register.

Evidence

41. A certificate purporting to be signed by the Chairman or an authorised officer and stating that a Singapore telephone number was or was not listed in a register at a date specified in the certificate shall be admissible as evidence of its contents in any proceedings.

Information on terminated Singapore telephone number

42.—(1) Every telecommunications service provider shall report to the Commission, in the form and manner prescribed, all terminated Singapore telephone numbers.

(2) A telecommunications service provider which contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000.

(3) In this section, "terminated Singapore telephone number" means —

(*a*) a Singapore telephone number to which the following apply:

(i) the Singapore telephone number which has been allocated to a subscriber;

(ii) the telecommunications service associated with the Singapore telephone number has been terminated by the subscriber or telecommunications service provider; and

(iii) the Singapore telephone number has not been allocated to a different subscriber; or

(*b*) any other telephone numbers and circumstances as may be prescribed.

(4) For the purpose of subsection (1), where —

(*a*) a Singapore telephone number has been allocated to a subscriber by a telecommunications service provider (referred to in this subsection as the first provider);

(*b*) the telecommunications service associated with the Singapore telephone number has been terminated by the subscriber;

(*c*) the subscriber contracts for a telecommunications service associated with the Singapore telephone number with another telecommunications service provider (referred to in this subsection as the subsequent provider);

(*d*) the telecommunications service referred to in paragraph (*c*) has been terminated by the subscriber or the subsequent provider; and

(*e*) the Singapore telephone number has not subsequently been allocated to any subscriber,

it shall be the responsibility of the first provider to satisfy subsection (1).

(5) Without prejudice to the obligations of the telecommunications service provider under subsections (1) to (4), the Commission shall pay the prescribed fees to the telecommunications service provider for each terminated Singapore telephone number reported to the Commission in accordance with this section.

Division 3 — Specified message to Singapore telephone number

Duty to check register

43.—(1) No person shall, on or after the prescribed date, send a specified message addressed to a Singapore telephone number unless the person had within the prescribed duration (which may include a duration before the prescribed date) before sending the specified message —

(*a*) applied to the Commission under section 40(2) to confirm whether that Singapore telephone number is listed in the relevant register; and

(*b*) received confirmation from the Commission that that Singapore telephone number is not listed in the relevant register.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000.

(3) In any proceedings for an offence under subsection (1), it shall be a defence for the person charged to prove that the subscriber or user of the telephone number —

(*a*) gave clear and unambiguous consent to the sending of the specified message to that Singapore telephone number; and

(*b*) the consent is evidenced in written or other form so as to be accessible for subsequent reference.

(4) For the purpose of this section —

(*a*) where there is only one register kept or maintained under section 39, the relevant register shall refer to that one register; and

(*b*) where there are 2 or more registers kept or maintained under section 39 for different types of specified messages, the relevant register shall refer to the register relevant for the particular type of specified message.

Contact information

44.—(1) No person shall, on or after the prescribed date, send a specified message addressed to a Singapore telephone number unless —

(*a*) the specified message includes clear and accurate information identifying the individual or organisation who sent or authorised the sending of the specified message;

(*b*) the specified message includes clear and accurate information about how the recipient can readily contact that individual or organisation;

(*c*) the specified message includes such information and complies with such conditions as is or are specified in the regulations, if any; and

(*d*) the information included in the specified message in compliance with this subsection is reasonably likely to be valid for at least 30 days after the message is sent.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000.

Calling line identity not to be concealed

45.—(1) A person who, on or after the prescribed date, makes a voice call containing a specified message or causes a voice call containing a specified message to be made or authorises the making of a voice call containing a specified message, addressed to a Singapore telephone number from a telephone number or facsimile number, shall not do any of the following:

(*a*) conceal or withhold from the recipient the calling line identity of the sender;

(*b*) perform any operation or issue any instruction in connection with the sending of the specified message for the purpose of, or that has the effect of, concealing or withholding from the recipient the calling line identity of the sender.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000.

Consent

46.—(1) A person shall not, as a condition for supplying goods, services, land, interest or opportunity, require a subscriber or user of a Singapore telephone number to give consent for the sending of a specified message to that Singapore telephone number or any other

Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity to that subscriber or user, and any consent given in such circumstance is not validly given.

(2) If a person obtains or attempts to obtain consent for sending a specified message to a Singapore telephone number —

(*a*) by providing false or misleading information with respect to the sending of the specified message; or

(*b*) by using deceptive or misleading practices,

any consent given in such circumstances is not validly given.

Withdrawal of consent

47.—(1) On giving notice, a subscriber or user of a Singapore telephone number may at any time withdraw any consent given to a person for the sending of any specified message to that Singapore telephone number.

(2) A person shall not prohibit a subscriber or user of a Singapore telephone number from withdrawing his consent to the sending of a specified message to that Singapore telephone number, but this section shall not affect any legal consequences arising from such withdrawal.

(3) If a subscriber or user of a Singapore telephone number gives notice withdrawing consent given to a person for the sending of any specified message to that Singapore telephone number, the person shall cease (and cause its agent to cease) sending any specified message to that Singapore telephone number after the expiry of the prescribed period.

(4) For the purposes of this Part, a subscriber or user of a Singapore telephone number shall be deemed to have given his consent to a person to send a specified message to that Singapore telephone number if the subscriber or user —

(*a*) consents to the sending of the specified message before the date of commencement of this Part; and

(*b*) that consent has not been withdrawn on or after the date of commencement of this Part.

(5) For the purposes of this Part, where a subscriber or user of a Singapore telephone number —

(*a*) consents to a person sending a specified message to that Singapore telephone number before, on or after the date of commencement of this Part; and

(*b*) subsequently applies to add or adds that Singapore telephone number to the register on or after the date of commencement of this Part,

the application to add or the addition of that Singapore telephone number shall not be regarded as a withdrawal of the consent.

(6) For the avoidance of doubt, a subscriber of a Singapore telephone number may, at any time on or after the date of commencement of this Part, withdraw any consent given for the sending of a specified message to that Singapore telephone number.

Defence for employee

48.—(1) In any proceedings for an offence under this Part brought against any employee in respect of an act or conduct alleged to have been done or engaged in, as the case may be, by the employee, it is a defence for the employee to prove that he did the act or engaged in the conduct in good faith —

(*a*) in the course of his employment; or

(*b*) in accordance with instructions given to him by or on behalf of his employer in the course of his employment.

(2) Subsection (1) does not apply to an employee who, at the time the act was done or the conduct was engaged in, was an officer and it is proved —

(*a*) the act was done or the conduct was engaged in with the consent or connivance of that officer; or

(*b*) the act done or the conduct engaged in was attributable to any neglect on the part of that officer.

(3) In subsection (2), "officer" has the same meaning as in section 52(5).

PART X

GENERAL

Advisory guidelines

49.—(1) The Commission may, from time to time, issue written advisory guidelines indicating the manner in which the Commission will interpret the provisions of this Act.

(2) Guidelines issued under this section may, from time to time, be varied, amended or revoked by the Commission.

(3) The Commission shall publish the guidelines in any way the Commission thinks fit, but failure to comply with this subsection in respect of any guidelines shall not invalidate the guidelines.

Powers of investigation

50.—(1) The Commission may, upon complaint or of its own motion, conduct an investigation under this section to determine whether an organisation is not complying with this Act.

(2) The powers of investigation under this section of the Commission and the inspectors shall be as set out in the Ninth Schedule.

(3) The Commission may suspend, discontinue or refuse to conduct an investigation under this section if it thinks fit, including but not limited to any of the following circumstances:

(*a*) the complainant has not complied with a direction under section 27(2);

(*b*) the parties involved in the matter have mutually agreed to settle the matter;

(*c*) any party involved in the matter has commenced legal proceedings against another party in respect of any contravention or alleged contravention of this Act by the other party;

(*d*) the Commission is of the opinion that the matter may be more appropriately investigated by another regulatory authority and has referred the matter to that authority; or

(*e*) the Commission is of the opinion that —

(i) a complaint is frivolous or vexatious or is not made in good faith; or

(ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation.

(4) An organisation shall retain records relating to an investigation under this section for one year after the conclusion of the investigation or any longer period specified in writing by the Commission.

Offences and penalties

51.—(1) A person shall be guilty of an offence if he makes a request under section 21 or 22, as the case may be, to obtain access to or to change the personal data about another individual without the authority of that individual.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 12 months or to both.

(3) An organisation or person commits an offence if the organisation or person —

(*a*) with an intent to evade a request under section 21 or 22, disposes of, alters, falsifies, conceals or destroys, or directs another person to dispose of, alter, falsify, conceal or destroy, a record containing —

(i) personal data; or

(ii) information about the collection, use or disclosure of personal data;

(*b*) obstructs or impedes the Commission or an authorised officer in the exercise of their powers or performance of their duties under this Act; or

(*c*) knowingly or recklessly makes a false statement to the Commission, or knowingly misleads or attempts to mislead the Commission, in the course of the performance of the duties or powers of the Commission under this Act.

(4) An organisation or person that commits an offence under subsection (3)(*a*) is liable —

(*a*) in the case of an individual, to a fine not exceeding $5,000; and

(*b*) in any other case, to a fine not exceeding $50,000.

(5) An organisation or person that commits an offence under subsection (3)(*b*) or (*c*) is liable —

(*a*) in the case of an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and

(*b*) in any other case, to a fine not exceeding $100,000.

Offences by bodies corporate, etc.

52.—(1) Where an offence under this Act committed by a body corporate is proved —

(*a*) to have been committed with the consent or connivance of an officer; or

(*b*) to be attributable to any neglect on his part,

the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

(3) Where an offence under this Act committed by a partnership is proved —

(*a*) to have been committed with the consent or connivance of a partner; or

(*b*) to be attributable to any neglect on his part,

the partner as well as the partnership shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(4) Where an offence under this Act committed by an unincorporated association (other than a partnership) is proved —

(*a*) to have been committed with the consent or connivance of an officer of the unincorporated association or a member of its governing body; or

(*b*) to be attributable to any neglect on the part of such an officer or member,

the officer or member as well as the unincorporated association shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(5) In this section —

"body corporate" includes a limited liability partnership;

"officer" —

(*a*) in relation to a body corporate, means any director, partner, member of the committee of management, chief executive, manager, secretary or other similar officer of the body corporate and includes any person purporting to act in any such capacity; or

(*b*) in relation to an unincorporated association (other than a partnership), means the president, the secretary, or any member of the committee of the unincorporated association, or any person holding a position analogous to that of president, secretary or member of such a committee and includes any person purporting to act in any such capacity;

"partner" includes a person purporting to act as a partner.

(6) Regulations may be made to provide for the application of any provision of this section, with such modifications as the Minister considers appropriate, to any body corporate or unincorporated association formed or recognised under the law of a territory outside Singapore.

Liability of employers for acts of employees

53.—(1) Any act done or conduct engaged in by a person in the course of his employment (referred to in this section as the employee) shall be treated for the purposes of this Act as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) In any proceedings for an offence under this Act brought against any person in respect of an act or conduct alleged to have been done or engaged in, as the case may be, by an employee of that person, it is a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing the act or engaging in the conduct, or from doing or engaging in, in the course of his employment, acts or conduct, as the case may be, of that description.

Jurisdiction of court

54. Notwithstanding any provision to the contrary in the Criminal Procedure Code (Cap. 68), a District Court shall have jurisdiction to try any offence under this Act and shall have power to impose the full penalty or punishment in respect of the offence.

Composition of offences

55.—(1) The Commission may, in its discretion, compound any offence under this Act (except Part IX) which is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding the lower of the following sums:

(*a*) one half of the amount of the maximum fine that is prescribed for the offence;

(*b*) a sum of $5,000.

(2) The Commission may, in its discretion, compound any offence under Part IX which is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding $1,000.

(3) On payment of such sum of money, no further proceedings shall be taken against that person in respect of the offence.

(4) The Minister may make regulations prescribing the offences which may be compounded.

General penalties

56. Any person guilty of an offence under this Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part thereof during which the offence continues after conviction.

Public servants

57. All members and officers of the Commission and persons authorised or appointed to exercise the powers of the Commission shall be deemed to be public servants for the purposes of the Penal Code (Cap. 224).

Evidence in proceedings

58.—(1) The Commission, the Appeal Panel, an Appeal Committee, their members and anyone acting for or under the direction of the Commission shall not give or be compelled to give evidence in a court or in any other proceedings in respect of any information obtained in performing their duties or exercising their powers or functions under this Act, except —

(*a*) in a prosecution for perjury or for the furnishing of false information;

(*b*) in a prosecution for an offence under this Act; or

(*c*) in an application for judicial review or an appeal from a decision with respect to such an application.

(2) Subsection (1) applies also in respect of evidence of the existence of proceedings conducted before the Commission.

Preservation of secrecy

59.—(1) Subject to subsection (5), every specified person shall preserve, and aid in the preservation of, secrecy with regard to —

(*a*) any personal data an organisation would be required or authorised to refuse to disclose if it were contained in personal data requested under section 21;

(*b*) whether information exists, if an organisation in refusing to provide access under section 21 does not indicate whether the information exists;

(*c*) all matters that have been identified as confidential under subsection (3); and

(*d*) all matters relating to the identity of persons furnishing information to the Commission,

that may come to his knowledge in the performance of his functions and discharge of his duties under this Act and shall not communicate any such matter to any person, except in so far as such communication —

(i) is necessary for the performance of any such function or discharge of any such duty; or

(ii) is lawfully required by any court, or lawfully required or permitted under this Act or any other written law.

(2) Any person who fails to comply with subsection (1) shall be guilty of an offence.

(3) Any person, when furnishing any information to the Commission, may identify information that he claims to be confidential information.

(4) Every claim made under subsection (3) shall be supported by a written statement giving reasons why the information is confidential.

(5) Notwithstanding subsection (1), the Commission may disclose, or authorise any specified person to disclose, any information relating to any matter referred to in subsection (1) in any of the following circumstances:

(*a*) where the consent of the person to whom the information relates has been obtained;

(*b*) if the Commission considers there is evidence of an offence, disclose information relating to the commission of an offence

to the Public Prosecutor, any police officer and other law enforcement authorities;

(*c*) to give effect to any provision of this Act;

(*d*) for the purposes of a prosecution, an application or an appeal referred to in section 58(1)(*a*), (*b*) or (*c*);

(*e*) to comply with any provision of a co-operation agreement entered into under section 10, where the conditions specified in subsection (6) are satisfied; or

(*f*) to a public body in such circumstances as may be prescribed by the Minister.

(6) The conditions referred to in subsection (5)(*e*) are —

(*a*) that the information or documents requested by the foreign country are in the possession of the Commission;

(*b*) that unless the Government otherwise allows, the foreign country undertakes to keep the information given confidential at all times; and

(*c*) that the disclosure of the information is not likely to be contrary to the public interest.

(7) In this section, "specified person" means a person who is or has been —

(*a*) a member or an officer of a relevant body;

(*b*) a member of a committee of a relevant body or any person authorised, appointed or employed to assist the relevant body; or

(*c*) an inspector or a person authorised, appointed or employed to assist an inspector.

Protection from personal liability

60. No liability shall be incurred by —

(*a*) any member or officer of a relevant body;

(*b*) any person authorised, appointed or employed to assist a relevant body;

(*c*) any person who is on secondment or attachment to a relevant body;

(*d*) any person authorised or appointed by a relevant body to exercise the relevant body's powers, perform the relevant body's functions or discharge the relevant body's duties or to assist the relevant body in the exercise of its powers, the performance of its functions or the discharge of its duties under this Act or any other written law; or

(*e*) any inspector or any person authorised, appointed or employed to assist him in connection with any function or duty of the inspector under this Act,

as a result of anything done (including any statement made) or omitted to be done with reasonable care and in good faith in the course of or in connection with —

(i) the exercise or purported exercise of any power under this Act or any other written law;

(ii) the performance or purported performance of any function or the discharge or purported discharge of any duty under this Act or any other written law; or

(iii) the compliance or purported compliance with this Act or any other written law.

Symbol of Commission

61.—(1) The Commission shall have the exclusive right to the use of such symbol or representation as may be prescribed in connection with its activities or affairs.

(2) Any person who, without the authority of the Commission, uses a symbol or representation identical with that of the Commission, or which so resembles the symbol or representation of the Commission as to deceive or cause confusion, or to be likely to deceive or to cause confusion, shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $2,000 or to imprisonment for a term not exceeding 6 months or to both.

Power to exempt

62. The Commission may, with the approval of the Minister, by order published in the *Gazette*, exempt any person or organisation or any class of persons or organisations from all or any of the provisions of this Act, subject to such terms or conditions as may be specified in the order.

Certificate as to national interest

63. For the purposes of this Act, if any doubt arises as to whether anything is necessary for the purpose of, or could be contrary to, the national interest, a certificate signed by the Minister charged with responsibility for that matter shall be conclusive evidence of the matters stated therein.

Amendment of Schedules

64.—(1) The Minister may, by order published in the *Gazette*, amend any of the Schedules, except the Ninth Schedule.

(2) An order under this section shall be presented to Parliament as soon as possible after publication in the *Gazette*.

Power to make regulations

65.—(1) The Minister may make such regulations as may be necessary or expedient for carrying out the purposes and provisions of this Act and for prescribing anything that may be required or authorised to be prescribed by this Act.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations for or with respect to all or any of the following matters:

(*a*) the keeping and audit of accounts and records, and submission of reports, relating to the transactions and affairs of the Commission by the Administration Body, including the powers of the auditor;

(*b*) the form, manner and procedures, relating to the making and responding to requests under section 21 or 22, including the content of responses to such requests, the period for such

responses, the circumstances in which an organisation may refuse to provide a response or refuse to confirm or deny the existence of any matter and the fees that an organisation may charge in respect of such requests;

(*c*) the classes of persons who may act under this Act for minors, deceased persons or any other individuals who lack capacity to act under this Act and regulating the manner in which, and the extent to which, any rights or powers of individuals under this Act may be exercised on their behalf;

(*d*) the form, manner and procedures relating to applications and complaints under this Act;

(*e*) the conduct of reviews by the Commission under section 28;

(*f*) the form, manner and procedures for applications for reconsideration by the Commission under section 31, including the fees to be paid in respect of such applications;

(*g*) the form, manner and procedures for appeals to an Appeal Committee, including the fees to be paid in respect of such appeals;

(*h*) the award of costs of or incidental to any proceedings before the Commission or Appeal Committee, and the award of expenses, including any allowances payable to persons in connection with their attendance before the Commission or Appeal Committee;

(*i*) the criteria for determining whether a Singapore telephone number is eligible to be listed in a register;

(*j*) the manner in which entries in the register are to be made, corrected or removed;

(*k*) the manner and form of giving or withdrawing consent for the sending of a specified message;

(*l*) any other matter relating to the establishment, operation or administration of the register;

(*m*) the fees to be paid in respect of applications, and services provided by or on behalf of the Commission, under this Act, including applications to confirm whether a Singapore

telephone number is listed in the relevant register for the purposes of section 43(1)(*a*).

(3) Regulations made under this section may provide differently for different organisations, individuals, classes of organisations or classes of individuals.

Rules of Court

66. Rules of Court may be made to provide for the practice and procedure relating to actions under section 32 and appeals under section 35, including the requirement that the plaintiff notify the Commission upon commencing any such action or appeal, and for matters related thereto.

Related and consequential amendments

67.—(1) Part II of the Third Schedule to the Banking Act (Cap. 19) is amended by deleting item 9.

(2) Section 26 of the Electronic Transactions Act (Cap. 88) is amended by inserting, immediately after subsection (1), the following subsection:

"(1A) Subject to subsection (2), a network service provider shall not be subject to any liability under the Personal Data Protection Act 2012 in respect of third-party material in the form of electronic records to which he merely provides access.".

(3) The Info-communications Development Authority of Singapore Act (Cap. 137A) is amended —

(*a*) by deleting the word "and" at the end of section 6(1)(*t*);

(*b*) by deleting the full-stop at the end of paragraph (*u*) of section 6(1) and substituting the word "; and", and by inserting immediately thereafter the following paragraph:

"(*v*) to support the Personal Data Protection Commission in the performance of its functions and duties and exercise of its powers under the Personal Data Protection Act 2012."; and

(*c*) by inserting, immediately after paragraph 31 of the Second Schedule, the following paragraphs:

"31A. To provide administrative support, including the provision of premises, office supplies and equipment and manpower and premises to the Personal Data Protection Commission in the performance of its functions under the Personal Data Protection Act 2012.

31B. To perform the functions and duties and exercise the powers of the Administration Body under the Personal Data Protection Act 2012, if so appointed.".

Savings and transitional provision

68. The Minister may, in relation to any provision of this Act, for a period of 2 years after the date of commencement of that provision, prescribe by regulations published in the *Gazette*, such provisions of a savings or transitional nature consequent on the enactment of that provision as he considers necessary or expedient.

FIRST SCHEDULE

Sections 2 and 5(2)

CONSTITUTION AND PROCEEDINGS OF PERSONAL DATA PROTECTION COMMISSION

Appointment of Chairman and Deputy Chairman

1.—(1) The Chairman and the Deputy Chairman shall be appointed by the Minister from among the members of the Commission.

(2) The Deputy Chairman may, subject to such directions as may be given by the Chairman, exercise all or any of the powers exercisable by the Chairman under this Act, including the power under section 8(4).

Temporary Chairman or Deputy Chairman

2. The Minister may appoint any member to be a temporary Chairman or temporary Deputy Chairman during the temporary incapacity from illness or otherwise or during the temporary absence from Singapore of the Chairman or the Deputy Chairman, as the case may be.

Revocation of appointment

3. The Minister may revoke the appointment of the Chairman, the Deputy Chairman or any member without assigning any reason.

FIRST SCHEDULE — *continued*

Tenure of office of appointed member

4. The Chairman, the Deputy Chairman or a member, unless his appointment is revoked by the Minister or unless he resigns during his term of office, shall hold office for such period as the Minister may determine and shall be eligible for re-appointment.

Filling of vacancies

5. If a member resigns, dies or has his appointment revoked before the expiry of the term for which he has been appointed, the Minister may appoint a person to fill the vacancy for the remainder of the term for which his predecessor was appointed.

Meetings of Commission

6.—(1) The Commission shall meet for the despatch of business at such times and places as the Chairman may from time to time appoint.

(2) At every meeting of the Commission, one half of the number of members shall form a quorum.

(3) A decision at a meeting of the Commission shall be adopted by a simple majority of the members present and voting except that, in the case of an equality of votes, the Chairman or member presiding shall have a casting vote in addition to his original vote.

(4) The Chairman or, in his absence, the Deputy Chairman shall preside at meetings of the Commission.

(5) Where both the Chairman and the Deputy Chairman are absent at a meeting, such member as the members present may elect shall preside at that meeting.

(6) Subject to the provisions of this Act, the Commission may regulate its own procedures generally and, in particular, regarding the holding of meetings, the notice to be given of such meetings, the proceedings thereat, the keeping of minutes and the custody, production and inspection of such minutes.

Commission may act notwithstanding vacancy

7. The Commission may act notwithstanding any vacancy in its membership.

SECOND SCHEDULE

Section 17(1)

COLLECTION OF PERSONAL DATA WITHOUT CONSENT

1. An organisation may collect personal data about an individual without the consent of the individual or from a source other than the individual in any of the following circumstances:

(*a*) the collection is necessary for any purpose that is clearly in the interest of the individual, if consent for its collection cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

(*b*) the collection is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

(*c*) the personal data is publicly available;

(*d*) the collection is necessary in the national interest;

(*e*) the collection is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;

(*f*) the collection is necessary for evaluative purposes;

(*g*) the personal data is collected solely for artistic or literary purposes;

(*h*) subject to paragraph 2, the personal data is collected by a news organisation solely for its news activity;

(*i*) the personal data is collected for the organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;

(*j*) the collection is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;

(*k*) the personal data is collected by a credit bureau from a member of the credit bureau to create a credit report, or by a member of the credit bureau from a credit report provided by the credit bureau to that member in relation to a transaction between the member and the individual;

(*l*) the personal data is collected to confer an interest or a benefit on the individual under a private trust or a benefit plan, and to administer such trust or benefit plan, at the request of the settlor or the person establishing the benefit plan, as the case may be;

SECOND SCHEDULE — *continued*

(*m*) the personal data was provided to the organisation by another individual to enable the organisation to provide a service for the personal or domestic purposes of that other individual;

(*n*) the personal data is included in a document —

(i) produced in the course, and for the purposes, of the individual's employment, business or profession; and

(ii) collected for purposes consistent with the purposes for which the document was produced;

(*o*) the personal data is collected by the individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual;

(*p*) subject to the conditions in paragraph 3, the personal data —

(i) is collected by an organisation, being a party or a prospective party to a business asset transaction with another organisation, from that other organisation;

(ii) is about an employee, customer, director, officer or shareholder of the other organisation; and

(iii) relates directly to the part of the other organisation or its business assets with which the business asset transaction is concerned;

(*q*) the personal data was disclosed by a public agency, and the collection is consistent with the purpose of the disclosure by the public agency; or

(*r*) the personal data —

(i) was disclosed to the organisation in accordance with section 17(3); and

(ii) is collected by the organisation for purposes consistent with the purpose of that disclosure.

2. In this paragraph and paragraph 1(*h*) —

"broadcasting service" has the same meaning as in section 2 of the Broadcasting Act (Cap. 28);

"news activity" means —

(*a*) the gathering of news, or the preparation or compilation of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or

SECOND SCHEDULE — *continued*

(*b*) the dissemination, to the public or any section of the public, of any article or programme of or concerning —

(i) news;

(ii) observations on news; or

(iii) current affairs;

"news organisation" means —

(*a*) any organisation —

(i) the business of which consists, in whole or in part, of news activity carried out in relation to a relevant broadcasting service, a newswire service or the publication of a newspaper; and

(ii) which, if the organisation publishes a newspaper in Singapore within the meaning of section 8(1) of the Newspaper and Printing Presses Act (Cap. 206), is required to be a newspaper company within the meaning of Part III of that Act; or

(*b*) any organisation which provides a broadcasting service in or from Singapore and holds a broadcasting licence granted under section 8 of the Broadcasting Act;

"newspaper" has the same meaning as in section 2 of the Newspaper and Printing Presses Act;

"relevant broadcasting service" means any of the following licensable broadcasting services within the meaning of the Broadcasting Act:

(*a*) Free-to-air nationwide television services;

(*b*) Free-to-air localised television services;

(*c*) Free-to-air international television services;

(*d*) Subscription nationwide television services;

(*e*) Subscription localised television services;

(*f*) Subscription international television services;

(*g*) Special interest television services;

(*h*) Free-to-air nationwide radio services;

(*i*) Free-to-air localised radio services;

(*j*) Free-to-air international radio services;

SECOND SCHEDULE — *continued*

(*k*) Subscription nationwide radio services;

(*l*) Subscription localised radio services;

(*m*) Subscription international radio services;

(*n*) Special interest radio services.

3.—(1) The conditions in this paragraph shall apply if the personal data is collected under paragraph 1(*p*).

(2) If the organisation is a prospective party to a business asset transaction —

(*a*) the personal data collected must be necessary for the organisation to determine whether to proceed with the business asset transaction; and

(*b*) the organisation and the other organisation must have entered into an agreement that requires the prospective party to use or disclose the personal data solely for purposes related to the business asset transaction.

(3) If an organisation enters into the business asset transaction with another organisation —

(*a*) the organisation shall only use or disclose the personal data collected for the same purposes for which the other organisation would have been permitted to use or disclose the data;

(*b*) if any of the personal data collected does not relate directly to the part of the other organisation or its business assets with which the business asset transaction entered into is concerned, the organisation shall destroy, or return to the other organisation, any such personal data; and

(*c*) the employees, customers, directors, officers and shareholders whose personal data is disclosed shall be notified that —

(i) the business asset transaction has taken place; and

(ii) the personal data about them has been disclosed to the organisation.

(4) If a business asset transaction does not proceed or is not completed, the organisation shall destroy, or return to the other organisation, all the personal data collected.

(5) In this paragraph and paragraph 1(*p*), "business asset transaction" has the same meaning as in paragraph 3(4) of the Fourth Schedule.

4. For the avoidance of doubt, personal data disclosed before the appointed day in the circumstances and conditions set out in the Fourth Schedule shall satisfy paragraph 1(*r*), notwithstanding that section 17(3) was not in force at the time of the disclosure.

THIRD SCHEDULE

Section 17(2)

USE OF PERSONAL DATA WITHOUT CONSENT

1. An organisation may use personal data about an individual without the consent of the individual in any of the following circumstances:

(*a*) the use is necessary for any purpose which is clearly in the interests of the individual, if consent for its use cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent;

(*b*) the use is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

(*c*) the personal data is publicly available;

(*d*) the use is necessary in the national interest;

(*e*) the use is necessary for any investigation or proceedings;

(*f*) the use is necessary for evaluative purposes;

(*g*) the personal data is used for the organisation to recover a debt owed to the organisation by the individual or for the organisation to pay to the individual a debt owed by the organisation;

(*h*) the use is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;

(*i*) subject to the conditions in paragraph 2, the personal data is used for a research purpose, including historical or statistical research; or

(*j*) the data was collected by the organisation in accordance with section 17(1), and is used by the organisation for purposes consistent with the purpose of that collection.

2. Paragraph 1(*i*) shall not apply unless —

(*a*) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

(*b*) it is impracticable for the organisation to seek the consent of the individual for the use;

(*c*) the personal data will not be used to contact persons to ask them to participate in the research; and

(*d*) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

3. For the avoidance of doubt, personal data collected before the appointed day in the circumstances and conditions set out in the Second Schedule shall satisfy

THIRD SCHEDULE — *continued*

paragraph 1(*j*) notwithstanding that section 17(1) was not in force at the time of the collection.

FOURTH SCHEDULE

Sections 2, 17(3) and 21(4)

DISCLOSURE OF PERSONAL DATA WITHOUT CONSENT

1. An organisation may disclose personal data about an individual without the consent of the individual in any of the following circumstances:

(*a*) the disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way;

(*b*) the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

(*c*) subject to the conditions in paragraph 2, there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way;

(*d*) the personal data is publicly available;

(*e*) the disclosure is necessary in the national interest;

(*f*) the disclosure is necessary for any investigation or proceedings;

(*g*) the disclosure is to a public agency and such disclosure is necessary in the public interest;

(*h*) the disclosure is necessary for evaluative purposes;

(*i*) the disclosure is necessary for the organisation to recover a debt owed by the individual to the organisation or for the organisation to pay to the individual a debt owed by the organisation;

(*j*) the disclosure is necessary for the provision of legal services by the organisation to another person or for the organisation to obtain legal services;

(*k*) the personal data is disclosed by a member of a credit bureau to the credit bureau for the purpose of preparing credit reports, or in a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual;

(*l*) the personal data about the current or former students of the organisation, being an education institution, is disclosed to a public agency for the purposes of policy formulation or review;

FOURTH SCHEDULE — *continued*

(*m*) the personal data about the current or former patients of a healthcare institution licensed under the Private Hospitals and Medical Clinics Act (Cap. 248) or any other prescribed healthcare body is disclosed to a public agency for the purposes of policy formulation or review;

(*n*) the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer;

(*o*) the disclosure is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual;

(*p*) subject to the conditions in paragraph 3, the personal data —

(i) is disclosed to a party or a prospective party to a business asset transaction with the organisation;

(ii) is about an employee, customer, director, officer or shareholder of the organisation; and

(iii) relates directly to the part of the organisation or its business assets with which the business asset transaction is concerned;

(*q*) subject to the conditions in paragraph 4, the disclosure is for a research purpose, including historical or statistical research;

(*r*) the disclosure is for archival or historical purposes if a reasonable person would not consider the personal data to be too sensitive to the individual to be disclosed at the proposed time; or

(*s*) subject to the conditions in paragraph 5, the personal data —

(i) was collected by the organisation in accordance with section 17(1); and

(ii) is disclosed by the organisation for purposes consistent with the purpose of that collection.

2. In the case of disclosure under paragraph 1(*c*), the organisation shall, as soon as may be practicable, notify the individual whose personal data is disclosed of the disclosure and the purposes of the disclosure.

3.—(1) The conditions in this paragraph shall apply to personal data disclosed under paragraph 1(*p*).

(2) In the case of disclosure to a prospective party to a business asset transaction —

FOURTH SCHEDULE — *continued*

(*a*) the personal data must be necessary for the prospective party to determine whether to proceed with the business asset transaction; and

(*b*) the organisation and prospective party must have entered into an agreement that requires the prospective party to use or disclose the personal data solely for purposes related to the business asset transaction.

(3) If the organisation enters into the business asset transaction, the employees, customers, directors, officers and shareholders whose personal data is disclosed shall be notified that —

(*a*) the business asset transaction has taken place; and

(*b*) the personal data about them has been disclosed to the party.

(4) In this paragraph and paragraph 1(*p*) —

"business asset transaction" means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation or of any of the business or assets of an organisation other than the personal data to be disclosed under paragraph 1(*p*);

"party" means another organisation that enters into the business asset transaction with the organisation.

4. Paragraph 1(*q*) shall not apply unless —

(*a*) the research purpose cannot reasonably be accomplished without the personal data being provided in an individually identifiable form;

(*b*) it is impracticable for the organisation to seek the consent of the individual for the disclosure;

(*c*) the personal data will not be used to contact persons to ask them to participate in the research;

(*d*) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest; and

(*e*) the organisation to which the personal data is to be disclosed has signed an agreement to comply with —

(i) this Act;

(ii) the policies and procedures relating to the confidentiality of personal data of the organisation that collected the personal data;

(iii) security and confidentiality conditions of the organisation disclosing the personal data;

FOURTH SCHEDULE — *continued*

(iv) a requirement to remove or destroy individual identifiers at the earliest reasonable opportunity; and

(v) a requirement not to use the personal data for any other purpose or to disclose the personal data in individually identifiable form without the express authorisation of the organisation that disclosed the personal data.

5. For the avoidance of doubt, personal data collected before the appointed day in the circumstances and conditions set out in the Second Schedule shall satisfy paragraph 1(*s*) notwithstanding that section 17(1) was not in force at the time of the collection.

FIFTH SCHEDULE

Section 21(2)

EXCEPTIONS FROM ACCESS REQUIREMENT

1. An organisation is not required to provide information under section 21(1) in respect of —

(*a*) opinion data kept solely for an evaluative purpose;

(*b*) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

(*c*) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

(*d*) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

(*e*) a document related to a prosecution if all proceedings related to the prosecution have not been completed;

(*f*) personal data which is subject to legal privilege;

(*g*) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

(*h*) personal data collected, used or disclosed without consent, under paragraph 1(*e*) of the Second Schedule, paragraph 1(*e*) of the Third Schedule or paragraph 1(*f*) of the Fourth Schedule, respectively, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed;

FIFTH SCHEDULE — *continued*

(*i*) the personal data was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he was appointed to act —

(i) under a collective agreement under the Industrial Relations Act (Cap. 136) or by agreement between the parties to the mediation or arbitration;

(ii) under any written law; or

(iii) by a court, arbitral institution or mediation centre; or

(*j*) any request —

(i) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;

(ii) if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;

(iii) for information that does not exist or cannot be found;

(iv) for information that is trivial; or

(v) that is otherwise frivolous or vexatious.

SIXTH SCHEDULE

Section 22(7)

EXCEPTIONS FROM CORRECTION REQUIREMENT

1. Section 22 shall not apply in respect of —

(*a*) opinion data kept solely for an evaluative purpose;

(*b*) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

(*c*) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

(*d*) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or

(*e*) a document related to a prosecution if all proceedings related to the prosecution have not been completed.

SEVENTH SCHEDULE

Section 33(5)

CONSTITUTION AND PROCEEDINGS OF DATA PROTECTION APPEAL PANEL AND DATA PROTECTION APPEAL COMMITTEES

Data Protection Appeal Panel

1.—(1) The Data Protection Appeal Panel shall consist of not more than 30 members appointed, from time to time, by the Minister on the basis of their ability and experience in industry, commerce or administration or their professional qualifications or their suitability otherwise for appointment.

(2) Members of the Appeal Panel shall be appointed for such period as may be determined by the Minister and shall be eligible for re-appointment.

(3) The Minister may at any time revoke the appointment of any member of the Appeal Panel without assigning any reason.

(4) A member of the Appeal Panel may resign by giving notice in writing to the Minister.

Chairman of Appeal Panel or temporary Chairman of Appeal Panel

2.—(1) The Chairman of the Appeal Panel, unless his appointment is revoked by the Minister or unless he resigns during his term of office, shall hold office for such period as the Minister may determine and shall be eligible for re-appointment.

(2) The Minister may appoint any member to be a temporary Chairman of the Appeal Panel during the temporary incapacity from illness or otherwise or during the temporary absence from Singapore of the Chairman of the Appeal Panel.

Proceedings of Appeal Committees

3.—(1) Subject to sub-paragraph (2), where the Chairman of the Appeal Panel is nominated as a member of an Appeal Committee under section 33(4), he shall preside at every meeting of the Appeal Committee, and where the Chairman of the Appeal Panel is not nominated as a member of the Appeal Committee, the Chairman of the Appeal Panel shall determine which member of the Appeal Committee shall preside at every meeting of that Appeal Committee.

(2) All matters coming before an Appeal Committee at any sitting thereof shall be decided by a majority of votes of those members present and, in the event of an equality of votes, the Chairman of the Appeal Panel (if he is nominated as a member of the Appeal Committee) or any other member presiding shall have a second or casting vote.

(3) Any member of the Appeal Panel whose term of appointment expires in the course of proceedings by an Appeal Committee to which he has been appointed

SEVENTH SCHEDULE — *continued*

shall continue as a member of that Appeal Committee until the Committee has completed its work.

Powers of Appeal Committees

4.—(1) An Appeal Committee shall have all the powers and duties of the Commission that are necessary to perform its functions and discharge its duties under this Act.

(2) An Appeal Committee shall have the powers, rights and privileges vested in a District Court on the hearing of an action, including —

(*a*) the enforcement of the attendance of witnesses and their examination on oath or otherwise;

(*b*) the compelling of the production of documents; and

(*c*) the award of such costs or expenses as may be prescribed under section 65.

(3) A summons signed by such member of an Appeal Committee as may be authorised by the Appeal Committee shall be equivalent to any formal procedure capable of being issued in an action for enforcing the attendance of witnesses and compelling the production of documents.

(4) Where any person being duly summoned to attend before an Appeal Committee does not so attend, that person shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both.

(5) A witness before an Appeal Committee shall be entitled to the same immunities and privileges as if he were a witness before a District Court.

(6) All appeals under section 34 shall be determined, having regard to the nature and complexity of the appeal, as soon as reasonably practicable.

(7) An Appeal Committee shall notify the Commission and the parties to the appeal of the date on and the place at which the appeal shall be heard.

(8) An Appeal Committee shall notify the Commission and the parties to the appeal of its decision in respect of the appeal and the reasons for its decision.

Allowances

5. Members of the Appeal Committee may receive such remuneration and such travelling and subsistence allowances as the Minister may determine.

EIGHTH SCHEDULE

Section 37(5)

EXCLUSION FROM MEANING OF "SPECIFIED MESSAGE"

1. For the purposes of Part IX, a specified message shall not include any of the following:

(*a*) any message sent by a public agency under, or to promote, any programme carried out by any public agency which is not for a commercial purpose;

(*b*) any message sent by an individual acting in a personal or domestic capacity;

(*c*) any message which is necessary to respond to an emergency that threatens the life, health or safety of any individual;

(*d*) any message the sole purpose of which is —

(i) to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender;

(ii) to provide warranty information, product recall information or safety or security information with respect to a product or service purchased or used by the recipient of the message; or

(iii) to deliver goods or services, including product updates or upgrades, that the recipient of the message is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender;

(*e*) any message the sole purpose of which is to provide —

(i) notification concerning a change in the terms or features of;

(ii) notification of a change in the standing or status of the recipient of the message with respect to; or

(iii) at regular periodic intervals, account balance information or other type of account statement with respect to,

a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of goods or services offered by the sender;

(*f*) any message the sole purpose of which is to conduct market research or market survey; or

(*g*) any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation.

EIGHTH SCHEDULE — *continued*

2. In this Schedule, "individual" does not include a sole proprietor registered under the Business Registration Act (Cap. 32).

NINTH SCHEDULE

Section 50(2)

POWERS OF INVESTIGATION OF COMMISSION AND INSPECTORS

Power to require documents or information

1.—(1) For the purposes of an investigation under section 50, the Commission or an inspector may, by notice in writing to any organisation, require the organisation to produce to the Commission or the inspector a specified document or specified information, which the Commission or inspector considers relates to any matter relevant to such investigation.

(2) A notice under sub-paragraph (1) shall indicate the purpose for which the specified document or specified information is required by the Commission.

(3) The Commission may specify in the notice —

(*a*) the time and place at which any document is to be produced or any information is to be provided; and

(*b*) the manner and form in which it is to be produced or provided.

(4) The power under this paragraph to require an organisation to produce a document includes the power —

(*a*) if the document is produced —

(i) to take copies of it or extracts from it; and

(ii) to require such organisation, or any person who is a present or past officer of the organisation, or is or was at any time employed by the organisation, to provide an explanation of the document; or

(*b*) if the document is not produced, to require such organisation or person to state, to the best of his knowledge and belief, where it is.

(5) In sub-paragraphs (1) and (2), "specified" means —

(*a*) specified or described in the notice; or

(*b*) falling within a category which is specified or described in the notice.

Power to enter premises without warrant

2.—(1) In connection with an investigation under section 50, an inspector, and such other persons as the inspector may require to assist him, may enter any premises.

NINTH SCHEDULE — *continued*

(2) No inspector or person assisting the inspector shall enter any premises in exercise of the powers under this paragraph unless the inspector has given the occupier of the premises a written notice which —

(*a*) gives at least 2 working days' notice of the intended entry; and

(*b*) indicates the subject-matter and purpose of the investigation.

(3) Sub-paragraph (2) shall not apply if the inspector has reasonable grounds for suspecting that the premises are, or have been, occupied by an organisation which is being investigated in relation to a contravention of this Act and if the inspector has taken all such steps as are reasonably practicable to give written notice under that sub-paragraph but has not been able to do so.

(4) Where sub-paragraph (3) applies, the power of entry conferred by sub-paragraph (1) shall be exercised upon production of —

(*a*) evidence of the inspector's appointment; and

(*b*) a document containing the information referred to in sub-paragraph (2)(*b*).

(5) An inspector or a person assisting the inspector entering any premises under this paragraph may —

(*a*) take with him such equipment as appears to him to be necessary;

(*b*) require any person on the premises —

(i) to produce any document which he considers relates to any matter relevant to the investigation; and

(ii) if the document is produced, to provide an explanation of it;

(*c*) require any person to state, to the best of the person's knowledge and belief, where any such document is to be found;

(*d*) take copies of, or extracts from, any document which is produced;

(*e*) require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter relevant to the investigation, to be produced in a form —

(i) in which it can be taken away; and

(ii) in which it is visible and legible; and

(*f*) take any step which appears to be necessary for the purpose of preserving or preventing interference with any document which he considers relates to any matter relevant to the investigation.

NINTH SCHEDULE — *continued*

Power to enter premises under warrant

3.—(1) The Commission or any inspector may apply to a court for a warrant and the court may issue such a warrant if it is satisfied that —

(*a*) there are reasonable grounds for suspecting that there are, on any premises, documents —

(i) the production of which has been required under paragraph 1 or 2; and

(ii) which have not been produced as required;

(*b*) there are reasonable grounds for suspecting that —

(i) there are, on any premises, documents which the Commission or the inspector has power under paragraph 1 to require to be produced; and

(ii) if the documents were required to be produced, they would not be produced but would be concealed, removed, tampered with or destroyed; or

(*c*) an inspector or a person assisting the inspector has attempted to enter the premises in the exercise of his powers under paragraph 2 but has been unable to do so and that there are reasonable grounds for suspecting that there are, on the premises, documents the production of which could have been required under that paragraph.

(2) A warrant under this paragraph shall authorise a named officer, and such other persons as the inspector may require to assist him, to do all or any of the following:

(*a*) to enter the premises specified in the warrant, using such force as is reasonably necessary for the purpose;

(*b*) to search any person on those premises if there are reasonable grounds for believing that that person has in his possession any document, equipment or article which has a bearing on the investigation;

(*c*) to search the premises and take copies of, or extracts from, any document appearing to be of a kind in respect of which the application under sub-paragraph (1) was granted (the relevant kind);

(*d*) to take possession of any document appearing to be of the relevant kind if —

(i) such action appears to be necessary for preserving the document or preventing interference with it; or

(ii) it is not reasonably practicable to take copies of the document on the premises;

NINTH SCHEDULE — *continued*

(*e*) to take any other step which appears to be necessary for the purpose mentioned in sub-paragraph (*d*)(i);

(*f*) to require any person to provide an explanation of any document appearing to be of the relevant kind or to state, to the best of his knowledge and belief, where it may be found;

(*g*) to require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter relevant to the investigation, to be produced in a form —

(i) in which it can be taken away; or

(ii) in which it is visible and legible; and

(*h*) to remove from those premises for examination any equipment or article which relates to any matter relevant to the investigation.

(3) If, in the case of a warrant under sub-paragraph (1)(*b*), the court is satisfied that it is reasonable to suspect that there are also on the premises other documents relating to the investigation concerned, the warrant shall also authorise the actions mentioned in sub-paragraph (2) to be taken in relation to any such document.

(4) Where possession of any document is taken under sub-paragraph (2)(*d*) or (3), the named officer may, at the request of the person from whom possession of the document was taken, provide such person with a copy of the document.

(5) A named officer may allow any equipment or article which has a bearing on an investigation and which may be removed from any premises for examination under sub-paragraph (2)(*h*) to be retained on those premises subject to such conditions as the named officer may require.

(6) A warrant issued under this paragraph shall —

(*a*) indicate the subject-matter and purpose of the investigation; and

(*b*) continue in force until the end of the period of one month beginning from the day on which it is issued.

(7) The powers conferred by this paragraph shall not be exercised except upon production of a warrant issued under this paragraph.

(8) Any person entering any premises by virtue of a warrant under this paragraph may take with him such equipment as appears to him to be necessary.

(9) If there is no one at the premises when the named officer proposes to execute such a warrant, he shall, before executing it —

(*a*) take such steps as are reasonable in all the circumstances to inform the occupier of the intended entry; and

NINTH SCHEDULE — *continued*

(*b*) if the occupier is informed, afford him or his legal or other representative a reasonable opportunity to be present when the warrant is executed.

(10) If the named officer is unable to inform the occupier of the intended entry, he shall, when executing the warrant, leave a copy of the warrant in a prominent place on the premises.

(11) On leaving any premises which he has entered by virtue of a warrant under this paragraph, the named officer shall, if the premises are unoccupied or the occupier is temporarily absent, leave them as effectively secured as he found them.

(12) Any document of which possession is taken under sub-paragraph (2)(*d*) or (3) may be retained for a period of not more than 3 months.

(13) In this paragraph —

"named officer" means an inspector named in the warrant;

"occupier", in relation to any premises, means a person whom the inspector reasonably believes is the occupier of those premises.