ภาคผนวก

ภาคผนวก ก.

ร่าง

พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...

โดยที่เป็นการสมควรให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 1 พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ...

มาตรา 2 พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนด 120 วัน นับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา 3 พระราชบัญญัตินี้ให้ใช้บังคับแก่ประมวลผลข้อมูลส่วนบุคคลแม้เพียงส่วนหนึ่งส่วนใดหรือทั้งหมดโดยวิธีการทางอิเลคทรอนิกส์ หรือวิธีการอัตโนมัติ หรือโดยวิธีการอื่นใดที่ไม่ใช่วิธีการทางอิเลคทรอนิกส์หรือวิธีการอัตโนมัติซึ่งกระทำขึ้นในราชอาณาจักร รวมทั้งที่มีการจัดเก็บไว้นอกราชอาณาจักร

ความในวรรคหนึ่ง มิให้ใช้บังคับการประมวลผลข้อมูลส่วนบุคคลเพียงเพื่อวัตถุประสงค์ในการใช้ส่วนบุคคลเว้นแต่จะมีวัตถุประสงค์ในการเปิดเผยข้อมูลนั้นโดยทั่วไปหรือโดยเฉพาะเจาะจง

มาตรา 4 ในพระราชบัญญัตินี้ "ข้อมูลข่าวสาร" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงข้อมูลหรือสิ่งใดๆไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆและไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีการอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ข้อมูลส่วนบุคคล" หมายความว่า ข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม หรือประวัติการทำงาน บรรดาที่มีชื่อเสียงของผู้นั้นหรือมีเลขหมาย รหัสหรือสิ่งบอกลักษณะอื่นที่ทำให้รู้ตัวผู้นั้นได้ เช่นลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคนหรือรูปถ่าย และให้ความหมายรวมถึงข้อมูลข่าวสารเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย

"ข้อมูลห้ามประมวลผล" หมายความว่า ข้อมูลส่วนบุคคลซึ่งกระทบต่อความรู้สึกหรือสิทธิเสรีอันอาจก่อให้เกิดความเสียหายต่อผู้เป็นเจ้าของข้อมูลตามที่คณะกรรมการประกาศกำหนด

"คลังข้อมูล" หมายความว่า สถานที่หรือระบบเครือข่ายหรือระบบข้อมูลซึ่งใช้ในการ

จัดเก็บข้อมูลส่วนบุคคลที่มีการประมวลผลไว้ในหมวดหมู่

"การประมวลผลข้อมูล" หมายความว่า การดำเนินการใดๆกับข้อมูลส่วนบุคคลโดยวิธีทางการอิเล็กทรอนิกส์ วิธีการอัตโนมัติ หรือวิธีอื่นใด ในการเก็บรวบรวม บันทึก จัดหมวดหมู่ เก็บรักษา ให้รายละเอียด แก้ไขเปลี่ยนแปลง คัดเลือก เรียกข้อมูลจากระบบ เปรียบเทียบ ใช้ประโยชน์ เชื่อมโยง ระงับการใช้ชั่วคราว เปิดเผยข้อมูลโดยเฉพาะเจาะจงหรือโดยทั่วไป ลบหรือทำลายข้อมูล เว้นแต่ข้อความจะกำหนดไว้เป็นอย่างอื่น

"ผู้ควบคุมข้อมูล" หมายความว่า บุคคลธรรมดา คณะบุคคล นิติบุคคล หรือหน่วยงานของรัฐ ซึ่งกำหนดการประมวลข้อมูลส่วนบุคคล หรือควบคุมและกำกับการประมวลผลข้อมูลส่วนบุคคลของผู้ประมวลข้อมูล โดยการกำหนดวัตถุประสงค์ หรือวิธีการในการประมวลผลข้อมูลนั้น

"ผู้ประมวลผลข้อมูล" หมายความว่า บุคคลธรรมดา คณะบุคคล นิติบุคคล หรือหน่วยงานของรัฐ ซึ่งดำเนินการประมวลผลข้อมูลเอง หรือดำเนินการในนามหรือแทนผู้ควบคุมข้อมูล หรือผู้ทำหน้าที่กำกับการประมวลผลข้อมูล

"เจ้าของข้อมูล" หมายความว่า บุคคลธรรมดา คณะบุคคล หรือนิติบุคคล ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล

"การเปิดเผยโดยเฉพาะเจาะจง" หมายความว่า การเปิดเผยข้อมูลส่วนบุคคลเป็นการเฉพาะให้กับบุคคลซึ่งไม่ได้เป็นเจ้าของข้อมูล รวมถึงการทำให้บุคคลดังกล่าวได้รับข้อมูลหรือสามารถสืบค้นข้อมูลส่วนบุคคลนั้นได้

"การเปิดเผยโดยทั่วไป" หมายความว่า การเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้กับบุคคลโดยทั่วไปรวมถึงการทำให้บุคคลดังกล่าวได้รับข้อมูล หรือสามารถสืบค้นข้อมูลข่าวสารส่วนบุคคลนั้น

"ข้อมูลซึ่งไม่ระบุชื่อ" หมายความว่า ข้อมูลใดๆซึ่งยังไม่มีการประมวลผลหรือมีการประมวลผลแล้วโดยไม่ระบุชื่อหรือทำให้รู้ว่าเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับบุคคลใด

"หน่วยงานของรัฐ" หมายความว่า กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรมราชการส่วนท้องถิ่น รัฐวิสาหกิจที่จัดตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคลคณะบุคคล หรือบุคคลซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใดๆและหน่วยงานตามที่กำหนดในกระทรวง

"คณะกรรมการ" หมายความว่า คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีรักษาการตามพระราชบัญญัตินี้

มาตรา 5 ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้

หมวดที่ 1
หลักการประมวลผลข้อมูล

มาตรา 6 การประมวลผลข้อมูลส่วนบุคคล โดยวิธีการทางอิเล็กทรอนิกส์ วิธีการอัตโนมัติหรือวิธีการอื่นใด ในการเก็บรวบรวมบันทึก จัดหมวดหมู่ เก็บรักษา ให้รายละเอียด แก้ไขเปลี่ยนแปลง คัดเลือก เรียกข้อมูลจากระบบ เปรียบเทียบ ใช้ประโยชน์เชื่อมโยง ระงับการใช้ชั่วคราว เปิดเผยข้อมูลโดยเฉพาะเจาะจงหรือโดยทั่วไป ลบหรือทำลายข้อมูลจะ กระทำมิได้ เว้นแต่จะได้รับความเห็นชอบจากเจ้าของข้อมูล และภายใต้วัตถุประสงค์ของการประมวลผลข้อมูลโดยชัดแจ้ง โดยมีการรักษาความปลอดภัยของข้อมูล และต้องตรวจสอบนั้นให้ถูกต้องอยู่เสมอ

หมวดที่ 2
ผู้ควบคุมข้อมูล

มาตรา 7 ผู้ใดประสงค์จะทำการเป็นผู้ควบคุมข้อมูลต้องแจ้งให้คณะกรรมการทราบหลักเกณฑ์วิธีการแจ้งและการดำเนินตามวรรคหนึ่งให้เป็นไปตามที่กำหนดในพระราชกฤษฎีกาและตามที่คณะกรรมการประกาศกำหนด

หลักเกณฑ์และวิธีการที่ต้องแจ้งให้คณะกรรมการทราบในวรรคสองอย่างน้อยต้องมีรายการ ดังต่อไปนี้

(1) ชื่อ ที่อยู่ หรือสำนักงานของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

(2) วัตถุประสงค์และวิธีการประมวลผลข้อมูล

(3) ลักษณะและประเภทของข้อมูลข่าวสารส่วนบุคคลที่จะประมวล

(4) ประเภทของเจ้าของข้อมูล

(5) วัตถุประสงค์ในการโอนข้อมูลไปนอกราชอาณาจักร

(6) คลังข้อมูลซึ่งใช้ในการจัดเก็บข้อมูลที่ได้ประมวลผลข้อมูล หรือที่เชื่อมโยงกับการประมวลผลข้อมูลอื่นหรือคลังข้อมูลอื่นทั้งที่อยู่ในและนอกราชอาณาจักร

(7) เงื่อนไขการเปิดเผยข้อมูลส่วนบุคคลโดยทั่วไปหรือโดยเฉพาะเจาะจง

(8) มาตรการในการรักษาความปลอดภัยของข้อมูล

มาตรา 8 ภายใต้บังคับบทบัญญัติแห่งมาตรา 7 ผู้ควบคุมข้อมูลไม่ต้องการแสดงรายการตามที่กำหนดไว้ใน (2) ถึง (6)

หากเป็นการประมวลผลข้อมูลในกรณี ดังต่อไปนี้

(1) การประมวลผลข้อมูลโดยหน่วยงานของรัฐซึ่งมีวัตถุประสงค์เพื่อประโยชน์สาธารณะ

(2) การประมวลผลข้อมูลโดยผู้ประกอบวิชาชีพเกี่ยวกับหนังสือพิมพ์เกี่ยวกับการเขียนข่าว

(3) การประมวลผลข้อมูลชั่วคราวโดยไม่ใช้วิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติอื่นใดเพียงเพื่อใช้ใน

กิจกรรมภายในของผู้ควบคุมข้อมูลซึ่งไม่ได้บันทึกไว้ในระบบคลังข้อมูล

(4) การประมวลผลข้อมูลซึ่งมีวัตถุประสงค์ในการวิจัยทางประวัติศาสตร์ ทางวิทยาศาสตร์ และทางสถิติศาสตร์

(5) กรณีอื่นตามที่กำหนดในกฎกระทรวง

มาตรา 9 ผู้ควบคุมข้อมูลไม่ต้องแจ้งหรือยื่นแบบแสดงรายการตามที่กำหนดไว้ในมาตรา 7 หากเป็นการประมวลผลข้อมูลในกรณีดังต่อไปนี้

(1) การประมวลผลข้อมูลตามที่กำหนดในกฎหมายอื่นเป็นการเฉพาะ

(2) การประมวลผลข้อมูลจากเอกสารมหาชนหรือเอกสารที่สามารถได้โดยทั่วไป

(3) การประมวลผลข้อมูลเพื่อจัดทำสมุดโทรศัพท์หรือสิ่งอื่นใดที่มีลักษณะคล้ายกันเพื่อใช้เฉพาะภายในหน่วยงาน

(4) การประมวลผลข้อมูลเกี่ยวกับบัญชี เงินเดือน ผลกำไร รายงานประจำปี เพื่อใช้ภายในหน่วยงานหรือเฉพาะกลุ่มบุคคล

(5) กรณีอื่นตามที่กำหนดในกฎกระทรวง

มาตรา 10 ในกรณีที่ผู้ควบคุมประสงค์จะประมวลผลข้อมูลเอง หรือแต่งตั้งหรือมอบหมายให้บุคคลใดประมวลผลข้อมูลบุคคลซึ่งทำหน้าที่ประมวลผลข้อมูลนั้น จะต้องเป็นผู้ที่มีความรู้ประสบการณ์และเป็นผู้ที่มีความน่าเชื่อถือในการดำเนินการประมวลผลข้อมูลนั้น

ผู้ควบคุมข้อมูลต้องกำหนดแนวทางปฏิบัติเพื่อให้ผู้ประมวลผลข้อมูลใช้เป็นแนวทางทางปฏิบัติเพื่อให้ผู้ประมวลผลข้อมูลใช้เป็นแนวทางปฏิบัติ และเพื่อใช้เป็นแนวทางในการติดตามและตรวจสอบการดำเนินงานของผู้ประมวลผล

มาตรา 11 ผู้ควบคุมข้อมูลต้องจัดให้ผู้พิการ คนชรา และผู้ด้อยโอกาส สามารถเข้าถึงและตรวจสอบข้อมูลส่วนบุคคลของตนได้

มาตรา 12 การประมวลผลข้อมูลนอกวัตถุประสงค์ที่ได้แจ้งให้เจ้าของข้อมูลทราบตามมาตรา 16 จะกระทำมิได้ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล

หมวดที่ 3
การประมวลผลข้อมูล

มาตรา 13 ภายใต้บังคับบทบัญญัติแห่งมาตรา 6 ผู้ควบคุมข้อมูลต้องประมวลผลโดยชอบ และกำหนดวัตถุประสงค์ ขอบเขตระยะเวลา ข้อกำหนดการใช้งาน คุณภาพ ความปลอดภัย และการเปิดเผยข้อมูลที่มีการประมวลผลนั้นโดยชัดแจ้งการประมวลผลตามความในวรรคหนึ่ง

ผู้ควบคุมหรือผู้ประมวลผลข้อมูลจะต้องพยายามจัดเก็บหรือรวบรวมข้อมูลส่วนบุคคลโดยตรงจากเจ้าของข้อมูลเพียงเท่าที่จำเป็นและเกี่ยวข้องต่อการดำเนินงาน โดยต้องตรวจสอบและแก้ไขให้ถูกต้องอยู่เสมอ และยกเลิกการดำเนินการนั้นเมื่อหมดความจำเป็น

ในกรณีที่มิได้มีการจัดเก็บหรือรวบรวมข้อมูลส่วนจากเจ้าของข้อมูลโดยตรง ผู้ควบคุมข้อมูลหรือประมวลผลข้อมูลส่วนบุคคลจากเจ้าของข้อมูลทราบโดยมิชักช้าหรือในทันทีที่มีการเปิดเผยข้อมูลนั้น

มาตรา 14 ห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล หากมิได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล เว้นแต่การประมวลผลในกรณีดังต่อไปนี้

(1) การประมวลผลตามที่กำหนดในกฎหมายอื่นเป็นการเฉพาะ

(2) การประมวลผลเท่าที่จำเป็นอันเกิดจากความผูกพันตามสัญญา หรือก่อนจะผูกพันตามสัญญาหรือเพื่อ ชำระหนี้ตามสัญญา

(3) การประมวลผลเพื่อประโยชน์ต่อการศึกษา วิจัยทางวิทยาศาสตร์หรือเป็นข้อมูลทางสถิติ

(4) การประมวลผลสาขาวิชาชีพเกี่ยวกับหนังสือพิมพ์หรือการเขียนข่าว

(5) การประมวลผลเพื่อประโยชน์ในเชิงพาณิชย์อันไม่ขัดต่อกฎหมายว่าด้วยความลับทางการค้า

(6) การประมวลผลเพื่อประโยชน์ในการคุ้มครองหรือประกันชีวิต หรือสุขภาพในกรณีที่เจ้าของ ข้อมูลไม่สามารถให้ข้อมูลได้ เนื่องจากเป็นบุคคลไร้ความสามารถหรือเสมือนไร้ความสามารถ

(7) การประมวลผลเพื่อประโยชน์ในการสืบสวน สอบสวนของเจ้าพนักงานภายใต้ประมวลกฎหมายวิธีพิจารณาความอาญาเท่าที่จำเป็น

มาตรา 15 การประมวลผลข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐที่มิได้มีวัตถุประสงค์เพื่อแสวงหากำไรจะทำได้ต่อเมื่อมีกฎหมายกำหนดไว้โดยชัดแจ้ง หรือกระทบต่อประโยชน์สาธารณะ กรณีเป็นที่สงสัยให้ยื่นต่อคณะกรรมการเพื่อพิจารณา

หมวดที่ 4
การคุ้มครองเจ้าของข้อมูล

มาตรา 16 ภายใต้บทบัญญัติแห่งมาตรา 6 และมาตรา 13 ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลต้องแจ้งรายละเอียดให้แก่เจ้าของข้อมูลทราบ โดยอย่างน้อยต้องมีรายการดังต่อไปนี้

(1) วัตถุประสงค์ของการประมวลผลข้อมูล

(2) แสดงหลักฐานที่ระบุตัวผู้ประมวลผลข้อมูลหรือผู้ควบคุมข้อมูล

(3) สิทธิของเจ้าของข้อมูล

(4) ข้อมูลอื่นตามที่คณะกรรมการประกาศกำหนด

มาตรา 17 เจ้าของข้อมูลมีสิทธิ ขอให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลดำเนินการโดยไม่ชักช้า ในกรณีดังต่อไปนี้

(1) แจ้งข้อมูลของตนที่จัดเก็บไว้

(2) ยืนยันข้อมูลส่วนบุคคลของตน

(3) ลบหรือระงับการใช้ชั่วคราวหรือแปลงข้อมูลให้อยู่ในรูปแบบข้อมูลที่ไม่ระบุชื่อ ในกรณีที่มีการประมวลผลโดยมิชอบหรือฝ่าฝืนต่อบทบัญญัติแห่งพระราชบัญญัติหรือมีการจัดเก็บข้อมูลไว้เกินกว่าที่เกี่ยวข้องและจำเป็น

(4) ตรวจสอบและแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ

(5) แจ้งการดำเนินการตาม (3) หรือ (4) ไปยังบุคคลที่ได้มีการเปิดเผยข้อมูลทั้งโดยเฉพาะเจาะจงหรือโดยทั่วไป เว้นแต่การดำเนินการนั้นจะกระทบถึงประโยชน์ได้เสียโดยตรงของบุคคลผู้เป็นเจ้าของข้อมูล

มาตรา 18 เจ้าของข้อมูลมีสิทธิโต้แย้งคัดค้านว่าข้อมูลของตนไม่ถูกต้อง แต่ทั้งนี้ต้องไม่ช้ากว่าเวลาที่การเปิดเผยข้อมูลนั้นโดยเฉพาะเจาะจง หรือโดยทั่วไป

มาตรา 19 เจ้าของข้อมูลมีสิทธิขอให้ผู้ประมวลผลข้อมูล หรือผู้ควบคุมข้อมูลแจ้งเหตุผลที่ไม่แจ้งหรือไม่เปิดเผยให้ทราบเกี่ยวกับการจัดเก็บ รวบรวม หรือประมวลผล

หากผู้มีสิทธิตามวรรคหนึ่งถึงแก่ชีวิต บรรดาผู้มีส่วนได้เสียสามารถใช้สิทธิดังกล่าวที่เกี่ยวกับข้อมูลส่วนบุคคลของผู้นั้นได้

มาตรา 20 เจ้าของข้อมูลมีสิทธิได้รับแจ้ง การประมวลผลข้อมูลของตน และสามารถเข้าถึงและตรวจสอบข้อมูลนั้นได้โดยไม่เสียค่าใช้จ่าย

บทบัญญัติในวรรคหนึ่งมิให้ใช้บังคับถ้าการเข้าถึงและตรวจสอบข้อมูลนั้น อาจทำให้มีการเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่น เว้นแต่ข้อมูลส่วนบุคคลของบุคคลอื่นจะสามารถแยก ตัดทอนหรือทำโดยประการใดที่ไม่ทำให้เกิดผลกระทบต่อข้อมูลส่วนของบุคคลอื่น หรือบุคคลอื่นได้ให้ความยินยอมในการเข้าถึงและตรวจสอบข้อมูลนั้น หรือจำเป็นต้องให้มีการเข้าถึงและตรวจสอบข้อมูลส่วนบุคคลของบุคคลอื่น เนื่องจากข้อมูลนั้นมีผลกระทบต่อชีวิต อนามัย และความปลอดภัยของเจ้าของข้อมูล

ความในวรรคสองมิให้ใช้บังคับในกรณี ดังต่อไปนี้

(1) ข้อมูลอันเป็นของตัวความหรือของประชาชนผู้มีอรรถคดีอันได้มาจากการประกอบวิชาชีพทนายความ

(2) ข้อมูลอันเป็นความลับทางการค้า

(3) ข้อมูลอันกระทบต่อชีวิต ร่างกาย อนามัย และความปลอดภัยของผู้อื่น อันได้มาโดยปราศจากการรับรู้หรือยินยอมของผู้อื่น เว้นแต่ข้อมูลที่รวบรวมนั้นกระทำไปเพื่อประโยชน์ในการสืบสวนหรือพิจารณาคดีอันเกิดจากผิดสัญญาหรือการฝ่าฝืนกฎหมาย

(4) ข้อมูลที่ได้จากข้อพิพาทที่อยู่ระหว่างการพิจารณาคดีหรือดำเนินคดี

(5) ข้อมูลประเภทอื่นๆ ที่คณะกรรมการกำหนด

การเข้าถึงหรือตรวจสอบข้อมูลตามความในวรรคสาม อนุมาตรา (2) และอนุมาตรา (3) หากสามารถแยก ตัดทอนหรือทำโดยประการอื่นใดออกได้จากข้อมูลของบุคคลซึ่งยื่นคำร้องขอ ให้ผู้ควบคุมข้อมูลแยกข้อมูลส่วนบุคคลของบุคคลอื่นออกเสียก่อน

ความในวรรคสามมิให้ใช้บังคับหากการเข้าถึงและตรวจสอบทำให้ต้องเปิดเผยข้อมูลส่วนบุคคลของบุคคลอื่นเนื่องจากข้อมูลนั้นมีผลกระทบต่อชีวิต ร่างกาย อนามัย และความปลอดภัยของผู้ยื่นคำร้อง

มาตรา 21 ในกรณีที่ได้รับคำร้องจากเจ้าของข้อมูลในการขอเข้าถึงและตรวจสอบข้อมูลบุคคล ผู้ควบคุมจะต้องดำเนินการตามคำร้องนั้นโดยไม่คิดค่าธรรมเนียม เว้นแต่กรณีที่ข้อมูลส่วนบุคคลถูกประมวลผลเพื่อใช้ในการเปิดเผยโดยเฉพาะเจาะจงและเจ้าของข้อมูลนำข้อมูลดังกล่าวไปใช้ในกิจกรรมเชิงพาณิชย์กับบุคคลอื่น ผู้ควบคุมข้อมูลอาจจัดเก็บค่าธรรมเนียมใน

อัตราที่ไม่สูงเกินกว่าค่าใช้จ่ายปกติในการให้ข้อมูลนั้น

ผู้ควบคุมข้อมูลอาจจัดเก็บค่าธรรมเนียมในกรณีที่เจ้าของข้อมูลยื่นคำร้องขอเข้าถึงหรือตรวจสอบข้อมูลส่วนบุคคลของตนเกินกว่าหนึ่งครั้ง ในอัตราที่ไม่สูงเกินกว่าค่าใช้จ่ายปกติในการให้ข้อมูลนั้น

คำร้องในการเข้าถึงหรือตรวจสอบข้อมูลส่วนบุคคลจะต้องทำเป็นหนังสือ

มาตรา 22 เมื่อเจ้าของข้อมูลใช้สิทธิในการตรวจสอบหรือขอแก้ไขของตนที่อยู่ในความควบคุมข้อมูล ให้ผู้ควบคุมข้อมูลพิจารณาคำขอและตรวจสอบข้อมูลนั้นโดยเร็วและให้แจ้งผลการตรวจสอบพร้อมเหตุผลให้เจ้าของข้อมูลทราบภายใน 30 วันนับแต่วันที่ได้รับคำขอ ถ้ามีเหตุจำเป็นไม่อาจแจ้งผลการตรวจสอบได้ทันกำหนดระยะเวลาดังกล่าว ในการนี้ให้ขยายระยะเวลาการแจ้งผลการตรวจสอบออกไปได้อีกไม่เกิน 30 วัน นับแต่วันที่ครบกำหนดนั้น

ในกรณีที่ยังไม่มีการปฏิบัติการใดๆ ให้เป็นไปตามความเหมาะสมภายในสามสิบวันนับแต่วันที่ยื่นคำร้อง ให้ผู้ยื่นคำร้องยื่นอุทธรณ์ต่อคณะกรรมการ

ในกรณีที่ผู้ควบคุมข้อมูลเห็นว่าข้อมูลไม่ถูกต้องไม่ว่าด้วยเหตุใด ให้ผู้ควบคุมข้อมูลแก้ไขข้อมูลให้ถูกต้องโดยเร็ว รวมทั้งต้องแจ้งข้อมูลที่ต้องแก้ไขกับผู้ที่เกี่ยวข้องเพื่อนำไปแก้ไขข้อมูลให้ถูกต้องต่อไปด้วย

มาตรา 23 ในกรณีที่ข้อโต้แย้งระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลเกี่ยวกับความถูกต้องของข้อมูลและไม่อาจหาข้อยุติได้ให้ผู้ควบคุมข้อมูลบันทึกข้อโต้แย้งพร้อมหลักฐานประกอบของเจ้าของข้อมูลไว้ ในการนี้เจ้าของข้อมูลอาจอุทธรณ์ข้อโต้แย้งต่อคณะกรรมการ

หมวดที่ 5
ความปลอดภัยของข้อมูลมีการประมวลผล

มาตรา 24 ข้อมูลส่วนบุคคลต้องได้รับการประมวลผล จัดเก็บและควบคุมโดยคำนึงถึงมาตรฐานทางเทคโนโลยีและมาตรการความปลอดภัยที่เหมาะสม เพื่อป้องกันการทำลายข้อมูลหรือการทำให้ข้อมูลสูญหายหรือเสียหาย หรือการเข้าถึงข้อมูลโดยปราศจากอำนาจ และเพื่อมิให้มีการนำข้อมูลที่มีการประมวลผลนั้นไปใช้โดยไม่เหมาะสมหรือเป็นผลร้ายต่อเจ้าของข้อมูล

มาตรฐานทางเทคโนโลยีและมาตรการความปลอดภัยขั้นต่ำของข้อมูลวรรคหนึ่ง ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

มาตรา 25 การประมวลผลข้อมูลถือว่าสิ้นสุดลงเมื่อผู้ประมวลผลข้อมูลหยุดการประมวลผลข้อมูลไม่ว่าด้วยเหตุใดก็ตามและผู้ควบคุมข้อมูลได้แจ้งให้คณะกรรมการทราบล่วงหน้าแล้ว

ในกรณีตามวรรคหนึ่งให้ผู้ควบคุมข้อมูลดำเนินการดังต่อไปนี้

(1) ทำลายข้อมูลที่มีการประมวลผลนั้น

(2) โอนข้อมูลที่มีการประมวลผลให้ผู้ควบคุมข้อมูลอื่นซึ่งดำเนินการประมวลผลข้อมูลโดยมีวัตถุประสงค์ทำนองเดียวกัน

(3) จัดเก็บข้อมูลเพียงแค่วัตถุประสงค์ในการนำไปใช้ส่วนบุคคลเท่านั้น และห้ามมิให้นำไปเปิดเผยโดยเฉพาะเจาะจงหรือโดยทั่วไป

(4) จัดเก็บหรือโอนข้อมูลที่มีการประมวลผล เพื่อวัตถุประสงค์ในการวิจัยทางประวัติศาสตร์ วิทยาศาสตร์ และสถิติศาสตร์ให้ผู้ควบคุมข้อมูลอื่นทั้งนี้ ตามบทบัญญัติมาตรา 8 และมาตรา 14

หมวดที่ 6
การเปิดเผยข้อมูลโดยทั่วไปและการเปิดเผยโดยเฉพาะเจาะจง

มาตรา 26 ห้ามมิให้เปิดเผยข้อมูลที่มีการประมวลผลทั้งโดยทั่วไปและเฉพาะเจาะจง โดยปราศจากความยินยอมจากเจ้าของข้อมูลโดยชัดแจ้ง เว้นแต่กรณีดังต่อไปนี้

(1) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการประมวลผลข้อมูลนั้น

(2) เป็นข้อมูลที่คัดย่อ ตัดตอน หรือนำมาจากเอกสารมหาชน การลงทะเบียนเอกสารหรือบันทึกใดๆ ซึ่งหาได้ทั่วไปโดยมิได้ฝ่าฝืนบทบัญญัติแห่งกฎหมาย ประกาศหรือระเบียบเกี่ยวกับการเปิดเผยหรือการเผยแพร่ข้อมูลนั้น

(3) เปิดเผยตามบทบัญญัติของกฎหมาย หรือประกาศ ระเบียบหรือกฎที่ออกตามความในบทบัญญัติแห่งกฎหมาย

(4) เปิดเผยในขอบเขตของวิชาชีพหนังสือพิมพ์หรือการเขียนข่าวสื่อสารมวลชนโดยไม่ฝ่าฝืนบทบัญญัติของกฎหมายว่าด้วยเสรีภาพของสิ่งพิมพ์ หรือกระทบต่อการให้ความคุ้มครองความเป็นส่วนตัว หรือประโยชน์สาธารณะ

(5) ฝ่าฝืนต่อบทบัญญัติแห่งกฎหมายว่าด้วยความลับทางการค้า

(6) เป็นการจำเป็นเพื่อป้องกันหรือระงับอันตรายต่อชีวิตหรือสุขภาพของเจ้าของข้อมูลหรือบุคคลอื่น ในกรณีที่เจ้าของข้อมูลไม่สามารถให้ความยินยอมได้เนื่องจากเป็นบุคคลไร้ความสามารถ กายพิการ หรือจิตฟั่นเฟือน

(7) เป็นการจำเป็นเพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวนหรือการฟ้องคดีประเภทใดก็ตาม

(8) เป็นการจำเป็นในการรักษาความมั่นคงของรัฐ

(9) กรณีอื่นตามที่คณะกรรมการประกาศกำหนด

ความตามในมาตรานี้มิให้นำไปใช้บังคับแก่กรณีที่มีบทบัญญัติอื่นกำหนดไว้เป็นการเฉพาะ

มาตรา 27 ภายใต้บทบัญญัติมาตรา 26 การเปิดเผยข้อมูลโดยเฉพาะเจาะจงให้บุคคลอื่นซึ่งมิใช่เจ้าของข้อมูล ต้องกระทำภายใต้การควบคุมของผู้ประมวลผลข้อมูลหรือผู้ควบคุมข้อมูลโดยตรง

มาตรา 28 ห้ามทำการเปิดเผยข้อมูลโดยเฉพาะเจาะจงและเปิดเผยข้อมูลโดยทั่วไปเพื่อวัตถุประสงค์อื่น นอกเหนือจากที่ได้แจ้งไว้ต่อคณะกรรมการตามมาตรา 7 หรือเมื่อคณะกรรมการได้มีคำสั่งให้ลบข้อมูลนั้นในกรณีที่พ้นกำหนดระยะเวลาการจัดเก็บข้อมูลตามมาตรา 13

คณะกรรมการอาจกำหนดหลักเกณฑ์ห้ามเปิดเผยข้อมูลโดยทั่วไป หากว่าส่วนหนึ่งส่วนใดของข้อมูลนั้นกระทบต่อประโยชน์สาธารณะ

บทบัญญัติตามความในวรรคสองไม่ต้องตัดสิทธิของเจ้าของข้อมูลในการยื่นคัดค้านต่อคณะกรรมการ

หมวดที่ 7
ข้อมูลห้ามประมวลผล

มาตรา 29 ข้อมูลห้ามประมวลผล ได้แก่ข้อมูลเกี่ยวกับ

(1) เชื้อชาติ เผ่าพันธุ์

(2) ความเชื่อทางศาสนา ปรัชญาหรือลัทธิความเชื่อ

(3) ความคิดเห็นทางการเมือง

(4) สุขภาพ

(5) ข้อมูลอื่นที่คณะกรรมการประกาศกำหนด

การประมวลผลข้อมูลตามวรรคหนึ่งจะทำได้ต่อเมื่อได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลและได้รับอนุญาตจากคณะกรรมการ ทั้งนี้ ตามหลักเกณฑ์ในกฎกระทรวงและตามที่คณะกรรมการกำหนด

มาตรา 30 ห้ามมิให้เปิดเผยข้อมูลห้ามประมวลผล เว้นแต่ได้รับอนุญาตจากคณะกรรมการ คณะกรรมการจะต้องแจ้งผลการอนุญาตให้ผู้ขอทราบภายใน 30 วัน

มาตรา 31 การประมวลผลข้อมูลด้านสุขภาพของเจ้าของข้อมูลโดยหน่วยงานหรือผู้ประกอบการวิชาชีพเวชกรรมเพื่อรักษาความปลอดภัยในชีวิต ร่างกาย และอนามัยของเจ้าของข้อมูลไม่ต้องได้รับอนุญาตจากคณะกรรมการ

หากการประมวลผลข้อมูลตามวรรคหนึ่งเกี่ยวข้องกับบุคคลอื่นหรือสาธารณชนและเจ้าของข้อมูลไม่อาจให้ความยินยอมได้ จะต้องได้รับอนุญาตจากคณะกรรมการ

ห้ามมิให้เปิดเผยโดยทั่วไปเกี่ยวกับข้อมูลด้านสุขภาพ เว้นแต่ในกรณีที่มีความจำเป็นเพื่อป้องกันและปราบปรามการกระทำความผิด

มาตรา 32 การประมวลผลหรือการหยุดประมวลผลข้อมูลของนิติบุคคลไม่อยู่ภายใต้บทบัญญัติว่าด้วยเรื่องการแจ้ง ตามมาตรา 7 ความในมาตรา 33 ไม่นำมาบังคับใช้กับข้อมูลของนิติบุคคล

หมวดที่ 8
การส่งหรือโอนข้อมูลไปประเทศอื่น

มาตรา 33 การส่งหรือโอนข้อมูลข่าวสารส่วนบุคคลที่ถูกประมวลผลหรือข้อมูลห้ามประมวลผลตามหรือข้อมูลใดที่คณะกรรมการประกาศกำหนด ไปนอกราชอาณาจักรจะกระทำมิได้ เว้นแต่ผู้ควบคุมข้อมูลจะได้แจ้งให้คณะกรรมการทราบล่วงหน้าเป็นระยะเวลาพอสมควร

ห้ามมิให้ส่งข้อมูลตามวรรคหนึ่งไปยังประเทศซึ่งมิได้มีบทบัญญัติในการให้ความคุ้มครองข้อมูลข่าวสารส่วนบุคคลวิธีการประมวลผลข้อมูล และระดับความน่าเชื่อของมาตรการในการรักษาความปลอดภัย หรือมีมาตรฐานน้อยกว่าที่กำหนดตามพระราชบัญญัตินี้

ให้นำบทบัญญัติว่าด้วยการแจ้งต่อคณะกรรมการมาใช้บังคับโดยอนุโลม

มาตรา 34 บทบัญญัติมาตรา 33 มิให้ใช้บังคับการส่งหรือโอนข้อมูลข่าวสารส่วนบุคคลไปนอกราชอาณาจักรอาจทำได้ หากเป็นกรณีดังต่อไปนี้

(1) การส่งหรือโอนข้อมูลโดยเจ้าของข้อมูลให้ความยินยอมโดยชัดแจ้ง

(2) การส่งหรือโอนข้อมูลเท่าที่จำเป็นอันเกิดจากความผูกพันตามสัญญา หรือก่อนจะผูกพันตามสัญญาหรือเพื่อชำระหนี้ตามสัญญา

(3) การส่งหรือโอนข้อมูลเท่าที่จำเป็นเพื่อรักษาผลประโยชน์สาธารณะ

(4) การส่งหรือโอนข้อมูลเท่าที่จำเป็นเพื่อประโยชน์ในการสืบสวน สอบสวนของเจ้า

พนักงานภายใต้กฎหมายวิธีพิจารณาความอาญาเท่าที่จำเป็น

(5) การส่งหรือโอนข้อมูลเพื่อประโยชน์ในการคุ้มครองหรือประกันชีวิต หรือสุขภาพในกรณีที่เจ้าของข้อมูลไม่สามารถให้ข้อมูลได้ เนื่องจากเป็นบุคคลไร้ความสามารถหรือเสมือนไร้ความสามารถ

(6) การส่งหรือโอนข้อมูลเพื่อประโยชน์ต่อการศึกษา วิจัยทางวิทยาศาสตร์หรือเป็นข้อมูลทางสถิติ

หมวดที่ 9
คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 35 ให้มีคณะกรรมการคณะหนึ่งเรียกว่า "คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล" ประกอบด้วยประธานกรรมการคนหนึ่ง และกรรมการอีกสี่คน ซึ่งคณะรัฐมนตรีแต่งตั้งตามคำแนะนำของคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติจากผู้ทรงคุณวุฒิด้านวิศวกรรมศาสตร์ ด้านวิทยาการคอมพิวเตอร์ ด้านเศรษฐศาสตร์หรือพาณิชย์ศาสตร์หรือการเงินการธนาคาร ด้านสังคมศาสตร์ และด้านนิติศาสตร์ด้านละหนึ่งคน เพื่อให้ปฏิบัติหน้าที่ของตนอย่างเป็นอิสระและเป็นกลาง รวมทั้งต้องคำนึงถึงผลประโยชน์ส่วนรวมของประเทศชาติและประชาชนประกอบด้วย

ให้ผู้อำนวยการสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นกรรมการและเลขานุการ

การคัดเลือกกรรมการเพื่อเสนอแนะต่อคณะรัฐมนตรีให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติกำหนด

มาตรา 36 ให้มีคณะกรรมการคณะหนึ่งเรียกว่า "คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล" ประกอบด้วยรัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม เป็นประธานกรรมการ ปลัดกระทรวงพาณิชย์ ปลัดกระทรวงมหาดไทย เลขาธิการคณะกรรมการกฤษฎีกา เลขาธิการคณะกรรมการข้อมูลข่าวสารของราชการ โดยในจำนวนนี้ต้องแต่งตั้งจากผู้ทรงคุณวุฒิด้านวิศวกรรมศาสตร์หรือวิทยาการคอมพิวเตอร์ ด้านเศรษฐศาสตร์หรือพาณิชยศาสตร์หรือการเงินการธนาคาร และด้านนิติศาสตร์ด้านละหนึ่งคน และให้รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม เสนอคณะรัฐมนตรีเพื่อแต่งตั้งพนักงานของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยี แห่งชาติหนึ่งคน เป็นกรรมการและเลขานุการ

ให้คณะกรรมการแต่งตั้งผู้ช่วยเลขานุการอีกไม่เกินสองคน

มาตรา 37 กรรมการมีวาระการดำรงตำแหน่งคราวละสี่ปี

กรรมการซึ่งพ้นจากตำแหน่งตามวาระต้องปฏิบัติหน้าที่ต่อไปจนกว่ากรรมการซึ่งได้รับแต่งตั้งใหม่จะเข้ารับหน้าที่ เพื่อให้ได้มาซึ่งกรรมการ กรรมการชุดใหม่จะเข้ามาปฏิบัติหน้าที่เมื่อสิ้นสุดวาระของกรรมการชุดเดิม ให้ดำเนินการสรรหาและเลือกกรรมการชุดใหม่ก่อนครบวาระของกรรมการชุดเดิมเป็นระยะเวลาหกสิบวัน

กรรมการซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้แต่จะดำรงตำแหน่งติดต่อกันเกินสองวาระไม่ได้

มาตรา 39 นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา 37 กรรมการพ้นจากตำแหน่งเมื่อ

(1) ตาย

(2) ลาออก

(3) รัฐมนตรีให้ออก

(4) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 38

มาตรา 40 ในการประชุมคณะกรรมการ ถ้าประธานกรรมการไม่มาประชุมหรือไม่อยู่ในที่ประชุม ให้กรรมการที่มาประชุมเลือกกรรมการคนหนึ่งเป็นประธานในที่ประชุม

การประชุมคณะกรรมการทุกคราวต้องมีกรรมการมาประชุมมาต่ำกว่ากึ่งหนึ่งของจำนวนกรรมการทั้งหมดจึงจะเป็นองค์ประชุม

การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก กรรมการคนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกเสียงหนึ่งเป็นเสียงชี้ขาด

มาตรา 41 ให้คณะกรรมการมีอำนาจหน้าที่ ดังต่อไปนี้

(1) กำหนดนโยบาย มาตรการและมาตรฐานในการประมวลผลและรักษาความปลอดภัยของข้อมูลส่วนบุคคล

(2) ตรวจสอบเพื่อให้การดำเนินการของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลเป็นไปตามพระราชบัญญัตินี้

(3) เสนอแนะต่อคณะรัฐมนตรีให้มีการตราพระราชกฤษฎีกาตามพระราชบัญญัตินี้ ปรับปรุงแก้ไขกฎหมาย กฎข้อบังคับ ระเบียบ ประกาศคำสั่งที่ใช้บังคับอยู่ในส่วนที่เกี่ยวข้องและเหมาะสม

(4) ให้คำแนะนำและปรึกษาเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลของหน่วยงานภาครัฐและเอกชนในการปฏิบัติตามพระราชบัญญัตินี้

(5) ส่งเสริมและสนับสนุนให้เกิดทักษะการเรียนรู้และความเข้าใจเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้แก่ประชาชน

(6) ส่งเสริมและสนับสนุนการวิจัยเพื่อพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(7) แจ้งหรือโฆษณาข่าวสารเกี่ยวกับการประมวลผลที่อาจก่อให้เกิดความเสียหายหรือเสื่อมเสียแก่สิทธิของเจ้าของข้อมูล ในการนี้จะระบุชื่อผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลด้วยก็ได้

(8) สอดส่องเร่งรัดพนักงานเจ้าหน้าที่ ส่วนราชการ หรือหน่วยงานอื่นของรัฐให้ปฏิบัติการตามอำนาจหน้าที่ที่กฎหมายกำหนด ตลอดจนเร่งรัดพนักงานเจ้าหน้าที่ให้ดำเนินคดีในความผิดเกี่ยวกับการละเมิดสิทธิของเจ้าของข้อมูล

(9) พิจารณาคำร้องทุกข์ต่างๆของบุคคลที่เกี่ยวข้องตามพระราชบัญญัตินี้รวมทั้งวินิจฉัยข้อพิพาทระหว่างบุคคลฝ่ายต่างๆที่เกี่ยวข้อง

(10) ดำเนินคดีเกี่ยวกับการละเมิดสิทธิของเจ้าของข้อมูลหรือเกี่ยวกับการให้ความคุ้มครองข้อมูล ส่วนบุคคลที่คณะกรรมการเห็นสมควรหรือมีผู้ร้องขอ

(11) จัดทำรายงานเกี่ยวกับการปฏิบัติการตามพระราชบัญญัตินี้เสนอต่อคณะรัฐมนตรีเป็นครั้งคราวตามความเหมาะสม

(12) แต่งตั้งคณะอนุกรรมการ เพื่อดำเนินการใดๆตามพระราชบัญญัตินี้ตามความจำเป็นและเหมาะสม

(13) ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามวัตถุประสงค์ของพระราชบัญญัตินี้

ในการปฏิบัติหน้าที่ตามมาตรนี้ คณะกรรมการอาจมอบหมายให้สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ปฏิบัติการหรือเตรียมข้อเสนอมายังคณะกรรมการเพื่อพิจารณาดำเนินการต่อไป

มาตรา 42 คณะกรรมการจะแต่งตั้งคณะอนุกรรมการเพื่อพิจารณาหรือปฏิบัติการอย่างใดอย่างหนึ่งตามที่คณะกรรมการ หรือคณะกรรมการเฉพาะเรื่องมอบหมายก็ได้

มาตรา 43 ให้ประธานกรรมการและกรรมการเป็นผู้ปฏิบัติงานประจำเต็มเวลาโดยได้รับค่าตอบแทนเป็นรายเดือนและค่าใช้จ่ายในการเดินทางไปปฏิบัติงาน ตามหลักเกณฑ์และอัตราที่กำหนดในพระราชกฤษฎีกา

ให้อนุกรรมการได้รับค่าตอบแทนเป็นเบี้ยประชุมการใช้จ่ายในการเดินทางไปปฏิบัติงานตามหลักเกณฑ์และอัตราที่กำหนดในพระราชกฤษฎีกา

มาตรา 44 คณะกรรมการและคณะกรรมการเฉพาะเรื่องมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลที่เกี่ยวกับเรื่องที่มีผู้ร้องทุกข์หรือเรื่องอื่นใดที่เกี่ยวข้องกับการคุ้มครองมิทธิของเจ้าของข้อมูลได้ ในการนี้จะเรียกบุคคลที่เกี่ยวข้องมาชี้แจงด้วยก็ได้

มาตรา 45 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ คณะกรรมการต้องให้โอกาสแก่ผู้ถูกกล่าวหาหรือสงสัยว่ากระทำการอันเป็นการละเมิดสิทธิของเจ้าของข้อมูล เพื่อชี้แจงข้อเท็จจริงและแสดงความคิดเห็นตามสมควร เว้นแต่ในกรณีจำเป็นและเร่งด่วน

การกำหนดหรือการออกคำสั่งในเรื่องใดตามพระราชบัญญัตินี้ ให้คณะกรรมการคำนึงถึงความเสียหายที่อาจจะเกิดขึ้นแก่เจ้าของข้อมูล และในกรณีที่เห็นสมควรคณะกรรมการหรือคณะกรรมการเฉพาะเรื่องจะกำหนดเงื่อนไขหรือวิธีการบังคับให้เป็นไปตามการกำหนดหรือการออกคำสั่งนั้นก็ได้

หมวด 10
สำนักงาน

มาตรา 46 ให้มีสำนักงานคณะกรรมการข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐซึ่งทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการ และให้มีสำนักงานมีฐานะเป็นนิติบุคคลในกำกับของกระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมโดยมีระบบที่แตกต่างจากระบบราชการเพื่อให้เกิดความคล่องตัวภายใต้นโยบายคณะกรรมการ และให้สำนักงานนี้ปฏิบัติหน้าที่ตามหลักเกณฑ์ ระเบียบ ข้อบังคับตามที่คณะกรรมการกำหนด

มาตรา 47 ให้สำนักงานมีอำนาจและหน้าที่ปฏิบัติการใดๆเพื่อให้เป็นไปตามมติของคณะกรรมการและปฏิบัติงานอื่นตามวัตถุประสงค์ของพระราชบัญญัตินี้ อันรวมถึง

(1) รับผิดชอบงานธุรการและคณะกรรมการ

(2) ดำเนินการจัดการ ใช้งบประมาณซึ่งได้จัดสรรให้โดยรัฐบาลเพื่อให้เป็นประโยชน์สูงสุดในการบริหารงานหรือตามระเบียบที่คณะกรรมการกำหนดขึ้น

(3) จัดให้ได้มา ถือกรรมสิทธิ์ เช่า ให้เช่า เช่าซื้อ ยืม ให้ยืม และแลกเปลี่ยน โอน รับโอนและขายหรือจำหน่ายด้วยวิธีใดๆซึ่งอสังหาริมทรัพย์หรืออสังหาริมทรัพย์ รวมทั้งหลักทรัพย์และทรัพย์สินทางปัญญาต่างๆตลอดจนทรัพย์สินที่มีผู้มอบหรืออุทิศให้

(4) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานในประเทศและต่างประเทศใน

กิจการที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

(5) รับเรื่องร้องเรียนหรืออุทธรณ์เกี่ยวกับการคุ้มครองสิทธิของเจ้าของข้อมูลและการประมวลผลข้อมูลส่วนบุคคลเพื่อเสนอต่อคณะกรรมการ

(6) ศึกษา รวบรวม และวิเคราะห์จัดการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลรวมทั้งข้อมูลอื่นๆ อันจะเป็นประโยชน์ต่อการปฏิบัติงานของคณะกรรมการ รวมทั้งช่วยเหลือและให้คำแนะนำเกี่ยวกับข้อมูลดังกล่าว และดำเนินการเผยแพร่วิชาการ และให้ความรู้และการศึกษาแก่ประชาชน

(7) ติดตามและสอดส่องพฤติการณ์ของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล ซึ่งกระทำการใดอันมีลักษณะเป็นการละเมิดสิทธิของเจ้าของข้อมูลและจัดให้มีการทดสอบหรือพิสูจน์เกี่ยวกับมาตรการและมาตรฐานในการประมวลผลและรักษาความปลอดภัยของข้อมูลตามที่เห็นสมควรและจำเป็นเพื่อคุ้มครองสิทธิของเจ้าของข้อมูล

(8) ปฏิบัติอื่นใดตามที่คณะกรรมการมอบหมาย

มาตรา 48 ให้สำนักงานมีผู้อำนวยการซึ่งคณะกรรมการแต่งตั้งด้วยความเห็นชอบของคณะรัฐมนตรีเป็นผู้มีหน้าที่บริหารของสำนักงานตามมาตรา 47 และดำเนินงานอื่นๆตามนโยบายและมติของคณะกรรมการการมอบหมาย

มาตรา 49 ให้ผู้อำนวยการอยู่ในตำแน่งได้คราวละสี่ปี และอาจได้แต่งตั้งอีกได้แต่ไม่เกินสองวาระติดต่อกัน

ให้นำความในมาตรา 37 มาใช้บังคับกับการพ้นจากตำแหน่งของเลขาธิการโดยอนุโลม และให้เลขาธิการพ้นจากตำแหน่งเมื่อขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา 38

มาตรา 50 ผู้อำนวยการต้องมีคุณสมบัติและไม่มีลักษณะต้องห้ามตามมาตรา 38 รวมถึงให้มีลักษณะดังต่อไปนี้

(1) เป็นผู้สามารถปฏิบัติงานเต็มเวลาให้แก่สำนักงาน

(2) มีอายุไม่เกินหกสิบห้าปีบริบูรณ์

(3) ไม่เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่น ผู้บริหารท้องถิ่นกรรมการหรือผู้ดำรงตำแหน่งที่รับผิดชอบในการบริหารพรรคการเมือง หรือเจ้าหน้าที่ในพรรคการเมือง

(4) เป็นข้าราชการซึ่งมีตำแหน่งหรือเงินเดือนประจำ พนักงานหรือลูกจ้างของรัฐวิสาหกิจหรือหน่วยงานของรัฐอื่นหรือของส่วนราชการท้องถิ่น

(5) ไม่ดำรงตำแหน่งหรือหน้าที่ใดหรือมีผลประโยชน์เกี่ยวข้องกับการประมวลผลข้อมูลข่าวสารส่วนบุคคล

มาตรา 51 มีให้นำกฎหมายว่าด้วยการคุ้มครองแรงงานในส่วนที่เกี่ยวกับการจ่ายค่าชดเชยและการเงินสมทบกองทุนเงินทดแทนกฎหมายว่าด้วยแรงงานสัมพันธ์ และกฎหมายว่าด้วยพนักงานรัฐวิสาหกิจสัมพันธ์มาใช้บังคับกับเลขาธิการ พนักงาน และลูกจ้างของสำนักงาน

หมวดที่ 11
การร้องเรียนและการอุทธรณ์

มาตรา 52 ในกรณีที่สิทธิของผู้เป็นเจ้าของข้อมูล ตามมาตร 17 ถูกกระทบกระเทือนหรืออาจถูกกระทบกระเทือนให้ยื่นคำร้องต่อคณะกรรมการเพื่อบังคับให้เป็นไปตามสิทธิของเจ้าของข้อมูล

หลักเกณฑ์และวิธีการยื่นคำร้องตามวรรคหนึ่งให้เป็นไปตามระเบียบที่คณะการกำหนด

มาตรา 53 เมื่อมีการยื่นคำร้องแล้วคณะกรรมการต้องพิจารณาให้แล้วเสร็จภายในสามสิบวัน ในกรณีที่ผู้เป็นเจ้าของข้อมูลไม่เห็นด้วยกับคำสั่งของคณะกรรมการหรือยังไม่มีการปฏิบัติการใดๆให้เป็นไปตามความเหมาะสมภายในสามสิบวันนับแต่วันที่คณะกรรมการมีคำสั่งหรือนับแต่วันที่ยื่นคำร้อง ให้ผู้ยื่นคำร้องอุทธรณ์ต่อคณะกรรมการได้

หลักเกณฑ์และวิธีการยื่นคำร้องหรือการอุทธรณ์ตามวรรคหนึ่งให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด

ในกรณีที่มีการอุทธรณ์ต่อคณะกรรมการตามวรรคหนึ่ง คณะกรรมการต้องพิจารณาให้แล้วเสร็จภายในสามสิบวันนับแต่วันที่ได้รับอุทธรณ์ ในกรณีที่มีเหตุจำเป็นให้ขยายเวลาออกไปได้แต่ต้องแสดงเหตุผลและรวมเวลาทั้งหมดแล้วต้องไม่เกินหกสิบวัน

คำวินิจฉัยของคณะกรรมการให้เป็นที่สุด

มาตรา 54 คณะกรรมการมีอำนาจสั่งให้บุคคลหนึ่งบุคคลใดส่งเอกสารหรือข้อมูลที่เกี่ยวข้องกับเรื่องที่มีผู้ร้องทุกข์ หรือเรื่องอื่นใดที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและสิทธิของเจ้าของข้อมูล ในการนี้จะเรียกบุคคลที่เกี่ยวข้องมาชี้แจงด้วยก็ได้

มาตรา 55 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ คณะกรรมการต้องกำหนดระยะเวลาพอสมควรเพื่อให้ผู้ถูกกล่าวหาหรือสงสัยว่ากระทำการอันเป็นการละเมิดสิทธิของเจ้าของข้อมูลเพื่อชี้แจงข้อเท็จจริงและแสดงความคิดเห็นตามสมควร เว้นแต่ในกรณีที่จำเป็นและเร่งด่วน

การกระทำหรือออกคำสั่งในเรื่องใดตามพระราชบัญญัตินี้ ให้คณะกรรมการคำนึงถึงความเสียหายที่อาจเกิดขึ้นแก่ทั้งเจ้าของข้อมูล ผู้ควบคุมข้อมูลหรือบุคคลอื่นที่เกี่ยวข้องและในกรณีที่เห็นสมควร และคณะกรรมการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขเป็นการชั่วคราวในการบังคับให้เป็นไปตามการกำหนดหรือออกคำสั่งนั้นก็ได้

มาตรา 56 ในการปฏิบัติการตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้ามีมีอำนาจหน้าที่ดังนี้

(1) เข้าไปในสถานที่ประมวลผลข้อมูลของผู้ควบคุมข้อมูลกซหรือผู้ประมวลผลข้อมูล

(2) เข้าไปในสถานที่ใดๆ ที่มีเหตุอันควรสงสัยว่ามีการกระทำอันเป็นความผิด หรือมีหลักฐานหรือเอกสารที่เกี่ยวกับการกระทำความผิดเพื่อตรวจสอบได้ในระหว่างพระอาทิตย์ขึ้นจนถึงพระอาทิตย์ตก หรือในระหว่างเวลาทำการของสถานที่นั้น

(3) ยึดหรืออายัดทรัพย์สิน เอกสารหรือสิ่งของที่เกี่ยวข้องกับการกระทำความผิดพลาดตามพระราชบัญญัตินี้เพื่อประโยชน์ในการตรวจสอบหรือดำเนินคดี

(4) ปฏิบัติการอื่นใดตามที่คณะกรรมการมอบหมาย

มาตรา 57 ให้คณะกรรมการและพนักงานเจ้าหน้าที่ที่ปฏิบัติการตามพระราชบัญญัตินี้เป็นเจ้าพนักงานตามประมวลกฎหมายอาญา

ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลที่เกี่ยวข้องทุกครั้ง

หมวดที่ 12
บทกำหนดโทษ

มาตรา 58 ผู้ใดประมวลผลข้อมูลส่วนบุคคลทำให้เกิดความเสียหาย บุคคลนั้นจะต้องรับผิดชดใช้ค่าสินไหมทดแทนเพื่อการนั้น

มาตรา 59 ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 7 หรือ แจ้งรายการอันเป็นเท็จต่อคณะกรรมการต้องระวางโทษจำคุกตั้งแต่.....ถึง.....

มาตรา 60 ผู้ใดทำการประมวลผลข้อมูลส่วนบุคคลเพื่อให้ตนเองหรือผู้อื่นได้รับผลกำไรหรือผลประโยชน์อันมิชอบด้วยกฎหมายหรือให้ผู้อื่นเสียหาย ต้องระวางโทษจำคุกไม่เกิน.....หรือปรับไม่เกิน....หรือทั้งจำทั้งปรับ

ถ้าเป็นการเผยแพร่ข้อมูลโดยเฉพาะเจาะจงหรือโดยเปิดเผยซึ่งข้อมูลดังกล่าว ผู้กระทำต้องระวางโทษจำคุกตั้งแต่....ถึง....ปี หรือปรับไม่เกิน.... หรือทั้งจำทั้งปรับ

ผู้ใดเพื่อให้ตนเองหรือบุคคลอื่นได้รับผลกำไรหรือผลประโยชน์ หรือเจตนาให้บุคคลอื่นเสียหาย ทำการเผยแพร่ข้อมูลส่วนบุคคลโดยเฉพาะเจาะจงหรือโดยเปิดเผยอันเป็นการฝ่าฝืนบทบัญญัติตามมาตรา....หรือเป็นการขัดต่อบทบัญญัติในมาตรา....ต้องระวางโทษจำคุกตั้งแต่....ถึง....ปี หรือปรับไม่เกิน....หรือทั้งจำทั้งปรับ เว้นแต่การกระทำความผิดนั้นเป็นความผิดที่ร้ายแรง

การกระความผิดตาม....หากทำให้เกิดความเสียหายแก่บุคคลอื่น ต้องระวางโทษตั้งแต่.....ถึง....หรือปรับไม่เกิน.....หรือทั้งจำทั้งปรับ

มาตรา 61 ผู้ใดละเลยหรือฝ่าฝืนหรือไม่ปฏิบัติตามมาตรา 22 ในการกำหนดหรือปรับเปลี่ยนมาตรการเพื่อรักษาความปลอดภัยของข้อมูล ต้องระวางโทษ.....

มาตรา 62 ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามมาตรการหรือประกาศที่กำหนดโดยคณะกรรมการตามบทบัญญัติในมาตรา.....ต้องระวางโทษจำคุก.....หรือปรับไม่เกิน.....หรือทั้งจำทั้งปรับ

มาตรา 63 ผู้ใดล่วงรู้กิจการของบุคคลใดเนื่องจากการปฏิบัติตามอำนาจหน้าที่ที่บัญญัติไว้ในพระราชบัญญัตินี้ อันเป็นกิจการที่ตามปกติวิสัยจะพึงสงวนไว้ไม่พึงเปิดเผย ถ้าผู้นั้นนำไปเปิดเผยแก่บุคคลอื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี และปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่ง มิให้นำมาใช้บังคับแก่การเปิดเผยในกรณีดังต่อไปนี้

(1) การเปิดเผยตามหน้าที่

(2) การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือการพิจารณาคดี

(3) การเปิดเผยเกี่ยวกับการกระทำความผิดตามพระราชบัญญัตินี้

(4) การเปิดเผยเพื่อประโยชน์ในการแก้ไขสอดคล้องกับมาตรฐานหรือมาตรการที่คณะกรรมการประกาศกำหนด

(5) การเปิดเผยแก่ทางการหรือหน่วยงานในประเทศและต่างประเทศที่เกี่ยวข้องกับเรื่องดังกล่าว

(6) การเปิดเผลเมื่อได้รับความเห็นชอบจากบุคคลดังกล่าวเป็นลายลักษณ์อักษร

มาตรา 64 ผู้ร้องขอแก้ไขข้อมูลข่าวสารส่วนบุคคลโดยเจตนาให้ข้อมูลผิด หรือทำให้เกิดความเข้าใจผิดในสาระสำคัญต้องระวางโทษจำคุกไม่เกิน...ปี หรือปรับไม่เกิน...บาท หรือทั้งจำทั้งปรับ

มาตรา 65 ผู้ใดให้ถ้อยคำอันเป็นเท็จหรือปกปิดข้อความจริงที่ควรบอกให้แกคณะกรรมการหรือพนักงาน เจ้าหน้าที่ซึ่งอาจทำให้เจ้าของข้อมูลหรือบุคคลอื่นเสียหาย ต้องระวางโทษจำคุกไม่เกินหกเดือน และปรับไม่เกินหกหมื่นบาท

ภาคผนวก ข.

Data Protection Act 1998

The *Data Protection Act 1998* is a United Kingdom Act of Parliament which defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in the UK. Although the Act itself does not mention privacy, it was enacted to bring UK law into line with the EU data protection directive of 1995 which required Member States to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. In practice it provides a way for individuals to control information about themselves. Most of the Act does not apply to domestic use,[1] for example keeping a personal address book. Anyone holding personal data for other purposes is legally obliged to comply with this Act, subject to some exemptions. The Act defines eight data protection principles. It also requires companies and individuals to keep personal information to themselves.

History

The 1998 Act replaced and consolidated earlier legislation such as the Data Protection Act 1984 and the Access to Personal Files Act 1987. At the same time it aimed to implement the European Data Protection Directive. In some aspects, notably electronic communication and marketing, it has been refined by subsequent legislation for legal reasons. The Privacy and Electronic Communications (EC Directive) Regulations 2003 altered the consent requirement for most electronic marketing to "positive consent" such as an opt in box. Exemptions remain for the marketing of "similar products and services" to existing customers and enquirers, which can still be permissioned on an opt out basis.

The Jersey data protection law was modeled on the UK law. [2]

Personal data

The Act covers any data about a living and identifiable individual. Anonymised or aggregated data is not regulated by the Act, providing the anonymisation or aggregation has not been done in a reversible way. Individuals can be identified by various means including their name and address, telephone number or Email address. The Act applies only to data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'.

In some cases even a paper address book can be classified as a 'relevant filing system', for example diaries used to support commercial activities such as a salesperson's diary.

The Freedom of Information Act 2000 modified the act for public bodies and authorities, and the Durant case modified the interpretation of the act by providing case law and precedent.[3]

Subject rights

The Data Protection Act creates rights for those who have their data stored, and responsibilities for those who store, process or The person who has their data processed has the right to[4]

- View the data an organisation holds on them, for a small fee, known as 'subject access fee'[5]
- Request that incorrect information be corrected. If the company ignores the request, a court can order the data to be corrected or destroyed, and in some cases compensation can be awarded.[6]
- Require that data is not used in any way that may potentially cause damage or distress.[7]
- Require that their data is not used for direct marketing.[8]

Data protection principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
    1. at least one of the conditions in Schedule 2 is met, and
    2. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. About the rights of individuals e.g.[9]
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Conditions relevant to the first principle

Personal data should only be processed fairly and lawfully. In order for data to be classed as 'fairly processed', at least one of these six conditions must be applicable to that data (Schedule 2).

1. The data subject (the person whose data is stored) has consented ("given their permission") to the processing;
2. Processing is necessary for the performance of, or commencing, a contract;
3. Processing is required under a legal obligation (other than one stated in the contract);
4. Processing is necessary to protect the vital interests of the data subject;
5. Processing is necessary to carry out any public functions;
6. Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).[10]

Consent

Except under the below mentioned exceptions, the individual needs to consent to the collection of their personal information and its use in the purpose(s) in question. The *European Data Protection Directive* defines consent as "...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed", meaning the individual may *signify* agreement other than in writing. However, non-communication should not be interpreted as consent.

Additionally, consent should be appropriate to the age and capacity of the individual and other circumstances of the case. E.g. if an organisation "intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this." And even when consent is given, it shouldn't be assumed to last forever. Although in most cases consent lasts for as long as the personal data needs to be processed, individuals may be able to withdraw their consent, depending on the nature of the consent and the circumstances in which the personal information is being collected and used.[11]

The *Data Protection Act* also specifies that sensitive personal data must be processed according to a stricter set of conditions, in particular any consent must be explicit.[11]

Exceptions

The Act is structured such that all processing of personal data is covered by the act, while providing a number of exceptions in Part IV.[1] Notable exceptions are:

- Section 28 - National security. Any processing for the purpose of safeguarding national security is exempt from all the data protection principles, as well as Part II (subject access rights), Part III (notification), Part V (enforcement), and Section 55 (Unlawful obtaining of personal data).
- Section 29 - Crime and taxation. Data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of taxes are exempt from the first data protection principle.
- Section 36 - Domestic purposes. Processing by an individual only for the purposes of that individual's personal, family or household affairs is exempt from all the data protection principles, as well as Part II (subject access rights) and Part III (notification).

Offences

The Act details a number of civil and criminal offences for which data controllers may be liable if a data controller has failed to gain appropriate consent from a data subject. However 'consent' is not specifically defined in the Act; consent is therefore a common law matter.

- Sub-section 21(1) - This sub-section makes it an offence to process personal information without registration.[12]
- Sub-section 21(2) - This sub-section makes it an offence to fail to comply with the notification regulations made by the Secretary of State[12] (proposed by the Information Commissioner under section 25 of the Act[13]).

- Section 55 - Unlawful obtaining of personal data. This section makes it an offence for people (Other Parties), such as hackers and impersonators, outside the organisation to obtain unauthorised access to the personal data.[14]
- Section 56 - This section makes it a criminal offence to require an individual to make a Subject Access Request relating to cautions or convictions for the purposes of recruitment, continued employment, or the provision of services.[15] This was brought into effect by the Data Protection Act 1998 (Commencement No. 2) Order 2008.[16]

Complexity

The UK Data Protection Act is a large Act that has a reputation for complexity.[17] While the basic principles are honoured for protecting privacy, interpreting the act is not always simple. Many companies, organisations and individuals seem very unsure of the aims, content and principles of the DPA. Some hide behind the Act and refuse to provide even very basic, publicly available material quoting the Act as a restriction.[18] The act also impacts on the way in which organisations conduct business in terms of who can be contacted for marketing purposes, not only by telephone and direct mail, but also electronically and has led to the development of permission based marketing strategies.

Problems of interpretation

Definition of personal data

The definition of personal data is data which relates to a living individual who can be identified

- from that data, or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller

Sensitive personal data concerns the subject's race, ethnicity, politics, religion, trade union status, health, sex life or criminal record.[19]

Subject access

Personal data which is normally held for under 40 days may be legitimately denied in subject access requests under the Act. This is a consequence of the time limit data controllers must meet in making their response. If the data has been deleted by the normal procedures of the business by the time the data controller responds to a request, that data cannot be supplied. For data such as closed-circuit television images which are routinely overwritten, it may be impossible for a subject to exercise their data access rights.

Regulation

Compliance with the Act is regulated and enforced by an independent authority, the Information Commissioner's Office, which maintains guidance relating to the Act. Full details can be found at http://www.ico.gov.uk[20][21]

ภาคผนวก ค.

Data Protection Directive

The Data Protection Directive (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) is a European Union directive which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law. On 25 January 2012, the European Commission unveiled a draft European General Data Protection Regulation that will supersede the Data Protection Directive.[1]

Context

The right to privacy is a highly developed area of law in Europe. All the member states of the European Union (EU) are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence," subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence.

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data."[2] The seven principles governing the OECD's recommendations for protection of personal data were:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent;
4. Security—collected data should be kept secure from any potential abuses;

5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles.[3]

The OECD Guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. The US, meanwhile, while endorsing the OECD's recommendations, did nothing to implement them within the United States.[4] However, all seven principles were incorporated into the EU Directive.[5] In 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did. The European Commission realised that diverging data protection legislation amongst EU member states impeded the free flow of data within the EU and accordingly proposed the Data Protection Directive.

Content

The directive regulates the processing of personal data regardless of whether such processing is automated or not.

Scope

Personal data are defined as "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;" (art. 2 a)

This definition is meant to be very broad. Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of "personal data" are: address, credit card number, bank statements, criminal record, etc.

The notion *processing* means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;" (art. 2 b)

The responsibility for compliance rests on the shoulders of the "controller", meaning the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; (art. 2 d)

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data. (art. 4) Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any online business trading with EU citizens would process some personal data and would be using equipment in the EU to process the data (i.e. the customer's computer). As a consequence, the website operator would have to comply with the European data protection rules. The directive was written before the breakthrough of the Internet, and to date there is little jurisprudence on this subject.

The proposed new European Union Data Protection Regulation (a draft for which was unveiled in January 2012) extends the scope of the EU data protection law to all foreign companies processing data of European Union residents.[1]

Principles

Personal data should not be processed at all, except when certain conditions are met. These conditions fall into three categories: transparency, legitimate purpose, and proportionality.

Transparency

The data subject has the right to be informed when his personal data is being processed. The controller must provide his name and address, the purpose of processing, the recipients of the data and all other information required to ensure the processing is fair. (art. 10 and 11)

Data may be processed only under the following circumstances (art. 7):

- when the data subject has given his consent
- when the processing is necessary for the performance of or the entering into a contract
- when processing is necessary for compliance with a legal obligation
- when processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules. (art. 12)

Legitimate purpose

Personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes. (art. 6 b)

Proportionality

Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. (art. 6)

When sensitive personal data (can be: religious beliefs, political opinions, health, sexual orientation, race, membership of past organisations) are being processed, extra restrictions apply. (art. 8)

The data subject may object at any time to the processing of personal data for the purpose of direct marketing. (art. 14)

A decision which produces legal effects or significantly affects the data subject may not be based solely on automated processing of data. (art. 15) A form of appeal should be provided when automatic decision making processes are used.

Supervisory authority and the public register of processing operations

Each member state must set up a supervisory authority, an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection regulation has been violated. (art. 28) Individuals may lodge complaints about violations to the supervisory authority or in a court of law.

The controller must notify the supervisory authority before he starts to process data. The notification contains at least the following information (art. 19):

- the name and address of the controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description of the measures taken to ensure security of processing.

This information is kept in a public register.

Transfer of personal data to third countries

Third countries is the term used in EU legislation to designate countries outside the European Union. Personal data may only be transferred to third countries if that country provides an adequate level of protection. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.

The Directive's Article 29 created the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party". The Working Party gives advice about the level of protection in the European Union and third countries.

The Working Party negotiated with U.S. representatives about the protection of personal data, the Safe Harbor Principles were the result. According to critics the Safe Harbor Principles do not provide for an adequate level of protection, because they contain fewer obligations for the controller and allow the contractual waiver of certain rights.

In July 2007, a new, controversial,[6] Passenger Name Record agreement between the US and the EU was undersigned.[7]

In February 2008, Jonathan Faull, the head of the EU's Commission of Home Affairs, complained about the US bilateral policy concerning PNR.[8] The US had signed in February 2008 a memorandum of understanding (MOU) with the Czech Republic in exchange of a visa waiver scheme, without first consulting Brussels.[6] The tensions between Washington and Brussels are mainly caused by the lower level of data protection in the US, especially since foreigners do not benefit from the US Privacy Act of 1974. Other countries approached for bilateral Memoranda of Understandings included the United Kingdom, Estonia, Germany and Greece.[9]

Implementation by the member states

EU directives are addressed to the member states, and aren't legally binding for citizens in principle. The member states must transpose the directive into internal law. Directive 95/46/EC on the protection of personal data had to be transposed by the end of 1998. All member states have enacted their own data protection legislation.

Comparison with US data protection law

The United States prefers what it calls a 'sectoral' approach to data protection legislation, which relies on a combination of legislation, regulation, and self-regulation, rather than governmental regulation alone.[10] Former U.S. President Bill Clinton and former Vice-President Al Gore explicitly recommended in their "Framework for Global Electronic Commerce" that the private sector should lead, and companies should implement self-regulation in reaction to issues brought on by Internet technology.[11] To date, the US has no single data protection law comparable to the EU's Data Protection

Directive.[12] Privacy legislation in the United States tends to be adopted on an *ad hoc* basis, with legislation arising when certain sectors and circumstances require (e.g., the Video Privacy Protection Act of 1988, the Cable Television Protection and Competition Act of 1992,[13] the Fair Credit Reporting Act, and the 2010 Massachusetts Data Privacy Regulations). Therefore, while certain sectors may already satisfy the EU Directive, at least in part, most do not.[14]

The reasoning behind this approach probably has as much to do with American laissez-faire economics as with different social perspectives. The First Amendment of the United States Constitution guarantees the right to free speech.[15] While free speech is an explicit right guaranteed by the United States Constitution, privacy is an implicit right guaranteed by the Constitution as interpreted by the United States Supreme Court,[16] although it is often an explicit right in many state constitutions.[17]

Extensive European privacy regulation is usually justified in Europe with reference to experiences under World War II-era fascist governments and post-War Communist regimes, and Europeans are said to be highly suspicious and fearful of unchecked use of personal information.[18] World War II and the post-War period was a time in Europe that disclosure of race or ethnicity led to secret denunciations and seizures that sent friends and neighbors to work camps and concentration camps.[5] In the age of computers, Europeans' guardedness of secret government files has translated into a distrust of corporate databases, and governments in Europe took decided steps to protect personal information from abuses in the years following World War II.[19] Germany and France, in particular, set forth comprehensive data protection laws.[20] However, European privacy directives contain explicit exemptions for many governmental organizations, including the EU itself, national security, taxation, and policing, and would not have protected citizens against the abuses suffered at the hands of fascist or communist governments.

ประวัติผู้เขียน

ชื่อ นามสกุล:	เจษฎา ชมภูจันทร์
วุฒิการศึกษา	
ระดับปริญญาตรี:	นิติศาสตรบัณฑิต มหาวิทยาลัยพายัพ 2550
ประสบการณ์การทำงาน:	
(พ.ศ. 2553 – ปัจจุบัน)	เทศบาลตำบลตลาดขวัญ อำเภอดอยสะเก็ด จังหวัดเชียงใหม่ ผู้ช่วยนิติกร
สถานที่ติดต่อ:	41 หมู่ 3 ต.ตลาดขวัญ อ.ดอยสะเก็ด จ.เชียงใหม่ 50220
E-mail:	sumo_jes@hotmail.com