คู่มือ
การจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
ของหน่วยงานของรัฐ

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
อาคารรัฐประศาสนภักดี ชั้น 6
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02-1416-991
โทรสาร 02-1438-036
www.etcommission.go.th

คู่มือ
การจัดทำนโยบายและแนวปฏิบัติ
ในการคุ้มครองข้อมูลส่วนบุคคล
ของหน่วยงานของรัฐ

พิมพ์ครั้งที่ 1	มิถุนายน 2557	500 เล่ม
พิมพ์ครั้งที่ 2	มิถุนายน 2558 ปรับปรุง	500 เล่ม
พิมพ์ครั้งที่ 3	เมษายน 2560 ปรับปรุงครั้งที่ 2	500 เล่ม

สงวนลิขสิทธิ์โดย สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

จัดพิมพ์และเผยแพร่โดย

Electronic Transactions Commission

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
อาคารรัฐประศาสนภักดี ชั้น 6
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02-1416-991
โทรสาร 02-1438-036
www.etcommission.go.th
www.mict.go.th

คำนำ

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่เกี่ยวกับงานวิชาการและเป็นหน่วยงานธุรการของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในการปฏิบัติตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เพื่อให้การบริหารจัดการธุรกรรมทางอิเล็กทรอนิกส์มีประสิทธิภาพ

ในการจัดทำคู่มือการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ มีวัตถุประสงค์ 2 ประการ กล่าวคือ เพื่อให้เจ้าหน้าที่ในหน่วยงานภาครัฐ ใช้เป็นแนวทางเบื้องต้นในการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐได้อย่างถูกต้องและเหมาะสม และเพื่อสร้างความตระหนักให้แก่หน่วยงานของรัฐเห็นถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล

คู่มือเล่มนี้ ได้รับการปรับปรุงเป็นฉบับที่ 2 ซึ่งแก้ไขเนื้อหาบางส่วน ปรับเปลี่ยนขั้นตอนการดำเนินการ เรียบเรียงถ้อยคำให้เข้าใจง่าย เพื่อเป็นแนวทางให้เกิดความชัดเจนยิ่งขึ้น

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หวังเป็นอย่างยิ่งว่า เนื้อหาสาระสำคัญต่างๆ ในคู่มือเล่มนี้ จะเป็นประโยชน์แก่เจ้าหน้าที่ในหน่วยงานของรัฐและผู้ที่เกี่ยวข้องสามารถจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ตามกฎหมายได้อย่างมีประสิทธิภาพยิ่งขึ้น

กลุ่มงานกำกับดูแลธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
มีนาคม 2560 ปรับปรุงครั้งที่ 2

สารบัญ

หน้า

บทที่ 1 บทนำ......1
ความเป็นส่วนตัว 1
ข้อมูลส่วนบุคคล 2
ขอบเขต 3
ผลการบังคับใช้ 5
บทที่ 2 หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล 6
บทที่ 3 การจัดการข้อมูลส่วนบุคคล 10
ประเด็นสำคัญจากทั้งนโยบายและแนวปฏิบัติ 11
บทที่ 4 การจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล 14
ขั้นตอนการดำเนินการจัดทำ 15
การสำรวจและเตรียมความพร้อมกับข้อมูลส่วนบุคคลที่มีอยู่ 16
ประเด็นพิจารณาในการจัดทำ 17
แนวทางการเขียน 18
สาระสำคัญของประกาศฯ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครอง
ข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 19
ตัวอย่างการจัดทำ 33
ขั้นตอนการจัดส่งนโยบายและแนวปฏิบัติฯ ของหน่วยงานให้คณะกรรมการธุรกรรม
ทางอิเล็กทรอนิกส์พิจารณา 40
วิธีการและช่องทางจัดส่งเอกสารให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณา 42
การดำเนินการอย่างไรหลังจากแนวนโยบายและแนวปฏิบัติฯ ผ่านความเห็นชอบแล้ว 43
ภาคผนวก
ก. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 และ แก้คำผิด 45
ข. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
พ.ศ. 2549 54

1

บทนำ

บทที่ 1 บทนำ

ความเป็นส่วนตัว

“ความเป็นส่วนตัว” หรือ *“สิทธิส่วนบุคคล”* เป็นสิทธิมนุษยชนขั้นพื้นฐานของมนุษย์ ในภาษาอังกฤษใช้คำว่า *“Privacy”* หมายถึง สิทธิของบุคคลที่ประกอบไปด้วยสิทธิของบุคคล ในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัว ในเรื่องดังกล่าวน่าจะจัดอยู่ในเรื่องของ ความเป็นอยู่ส่วนตัวซึ่งหมายความว่า สถานะที่บุคคลจะรอดพ้นจากการสังเกต การรู้เห็น การสืบ ความลับ การรบกวนต่างๆ และความมีสันโดษ ไม่ติดต่อสัมพันธ์กับสังคม โดยทั้งนี้ ขอบเขตที่บุคคล ควรได้รับการคุ้มครองและการเคารพในสิทธิส่วนบุคคลก็คือการดำรงชีวิตอย่างเป็นอิสระ ตามที่ต้องการ ตามวิถีทางที่อาจเป็นไปได้และเป็นความพอใจตราบเท่าที่ไม่ขัดต่อกฎหมาย ไม่ขัดต่อความสงบ เรียบร้อยและศีลธรรมอันดีของประชาชนและไม่เป็นการล่วงละเมิดสิทธิเสรีภาพของผู้อื่น ซึ่งสิทธิ ในความเป็นส่วนตัวหรือสิทธิส่วนบุคคลนี้เป็นสิทธิขั้นพื้นฐานโดยมีบัญญัติไว้ในรัฐธรรมนูญ แห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2557 มาตรา 4

ความเป็นส่วนตัว (Privacy) ในบรรดาสิทธิที่เกี่ยวข้องกับสิทธิมนุษยชนทั้งหมด “ความเป็นส่วนตัว” นับเป็น *“สิทธิ”* ลักษณะหนึ่งที่ยากที่สุดในการบัญญัติความหมาย เพราะต้อง พิจารณาเนื้อหา สภาพสังคม วัฒนธรรม และพฤติการณ์แวดล้อมประกอบด้วย ในบางประเทศแนวคิด ของ “ความเป็นส่วนตัว” ได้รวมถึงการคุ้มครองข้อมูลส่วนบุคคล ซึ่งเป็นการตีความคำว่า “ความเป็น ส่วนตัว” ในด้านการจัดการข้อมูลส่วนบุคคล อย่างไรก็ตาม คำว่า *“ความเป็นส่วนตัว”* เป็นคำที่มี ความหมายกว้างและครอบคลุมถึงสิทธิต่างๆ หลายประการ *อาทิ*

(1) ความเป็นส่วนตัวเกี่ยวกับข้อมูล (Information Privacy) เป็นการให้ความคุ้มครอง ข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูล ส่วนบุคคล

(2) ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy) เป็นการให้ความคุ้มครอง ในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใดๆ อันละเมิดความเป็นส่วนตัว อาทิ การทดลองทางพันธุกรรม การทดลองยา เป็นต้น

(3) ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy) เป็นการ ให้ความคุ้มครองในความปลอดภัย และความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใด ที่ผู้อื่นจะล่วงรู้มิได้

(4) ความเป็นส่วนตัวในเคหสถาน (Territorial Privacy) เป็นการกำหนดขอบเขต หรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้

ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2557 ได้กำหนดสิทธิและให้การคุ้มครองสิทธิส่วนบุคคล ดังนี้

มาตรา 4 ภายใต้บังคับบทบัญญัติแห่งรัฐธรรมนูญนี้ ศักดิ์ศรีความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาค บรรดาที่ชนชาวไทยเคยได้รับการคุ้มครองตามประเพณีการปกครองประเทศไทย ในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขและตามพันธกรณีระหว่างประเทศที่ประเทศไทย มีอยู่แล้ว ย่อมได้รับการคุ้มครองตามรัฐธรรมนูญนี้

ความก้าวหน้าทางเทคโนโลยีกับการละเมิดข้อมูลส่วนบุคคล

แม้ว่าการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลจะเกิดขึ้นมานานโดยผ่านกระบวนการปกติธรรมดา ซึ่งปัญหาการล่วงละเมิดสิทธิความเป็นส่วนตัวในข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลมีอยู่เป็นจำนวนมาก แต่อาจไม่รุนแรงมากนัก และเนื่องด้วยพัฒนาการที่ก้าวหน้าของเทคโนโลยีคอมพิวเตอร์และเครือข่าย ส่งผลให้มีการนำคอมพิวเตอร์และระบบเทคโนโลยีสารสนเทศมาใช้และให้บริการเพิ่มมากขึ้น รวมถึงการเจริญเติบโตของโลกไซเบอร์หรือโลกออนไลน์ ซึ่งเป็นโลกที่สุ่มเสี่ยงต่อการถูกล่วงละเมิดข้อมูลส่วนบุคคลได้โดยง่าย โดยเฉพาะการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์หรือเปิดเผย โดยไม่ได้รับความยินยอมจากบุคคลซึ่งเป็นเจ้าของข้อมูล จนสร้างความเดือดร้อนหรือความเสียหายให้แก่เจ้าของข้อมูล

ตัวอย่างของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลส่วนใหญ่เป็นข้อมูลขั้นพื้นฐาน *เช่น* ชื่อ นามสกุล เพศ ที่อยู่ วันเดือนปีเกิดอายุ สถานภาพ บิดามารดา การเสียภาษี ประวัติการศึกษา ประวัติการทำงาน

ขอบเขต

ปัจจุบันการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีการขยายตัวอย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ซึ่งมีความสำคัญต่อการพัฒนาประเทศ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐช่วยให้หน่วยงานของรัฐสามารถให้บริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว โดยหน่วยงานของรัฐมีการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ในกิจกรรมของหน่วยงานของรัฐเอง หรือเพื่อการให้บริการของรัฐนั้น แต่การดำเนินการดังกล่าว หน่วยงานอาจมีความไม่พร้อมด้านบุคลากร ด้านเทคโนโลยี ด้านกฎระเบียบ และด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่ให้บริการ อันอาจเป็นปัญหาและอุปสรรคสำคัญที่อาจก่อให้เกิดการละเมิดข้อมูลส่วนบุคคล ซึ่งนับเป็นความเสี่ยงที่สำคัญประการหนึ่งที่ทำให้ประชาชนหรือผู้ใช้บริการกับหน่วยงานของรัฐขาดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ และการละเมิดดังกล่าวอาจมีผลกระทบต่อสิทธิขั้นพื้นฐานในความเป็นส่วนตัวของประชาชน ด้วยเหตุนี้ จึงมีการตรา*พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐพ.ศ. 2549* โดยอาศัยอำนาจตาม*มาตรา 35 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ* ได้กำหนดให้การทำ *“คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใดๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผล โดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด”*

ทั้งนี้ เพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคล ของผู้ที่ติดต่อหรือทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ โดยใน*มาตรา 6 มาตรา 7 และมาตรา 8* กำหนดให้หน่วยงานของรัฐต้อง*จัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ* ในกรณีที่หน่วยงานของรัฐได้ให้บริการหรือดำเนินกิจกรรมใดๆ ในทางอิเล็กทรอนิกส์ ตาม*มาตรา 35* และได้มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงใดที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยตรงหรือโดยอ้อม ทั้งนี้ *ต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ก่อน จึงมีผลใช้บังคับได้* และเพื่อให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน รวมทั้งสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งทำหน้าที่ส่งเสริมความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง *แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ* เพื่อเป็นแนวทางและตัวอย่างเบื้องต้น ให้หน่วยงานของรัฐใช้เป็นกรอบในการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

จากที่กล่าวมาข้างต้น เนื่องจาก*มาตรา 35 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544* ได้กำหนดให้มีการตราพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ สำหรับกรณีของการทำคำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศ หรือการดำเนินการใดๆ ตามกฎหมาย ซึ่งที่ผ่านมาได้มีการนำประเด็นการตีความมาตรา 35 ว่า รองรับเฉพาะกรณีการดำเนินการตามกฎหมายเท่านั้น เช่น การอนุญาต หรือการยื่นคำขอตามกฎหมาย แต่ไม่ขยายครอบคลุมไปถึงการดำเนินการอื่นๆ ที่ไม่มีกฎหมายบัญญัติรองรับ ใช่หรือไม่ หรือตีความว่า ขยายครอบคลุมไปถึงการดำเนินการของหน่วยงานของรัฐทุกกรณีที่มีการทำด้วยวิธีการทางอิเล็กทรอนิกส์ อาทิ การให้บริการแก่ประชาชนของหน่วยงานรัฐที่ดำเนินการตามนโยบายรัฐบาล ซึ่งในการพิจารณาประเด็นนี้มีข้อสังเกตว่า การดำเนินการของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ในปัจจุบันมีหลายเรื่องซึ่งมีความสำคัญอย่างยิ่งต่อหน่วยงานของรัฐเองและรวมถึงผู้ใช้บริการ แม้ว่าการให้บริการในบางเรื่องกฎหมายไม่ได้ระบุไว้ชัดเจนแต่ก็ถือเป็นการดำเนินการตามภารกิจเพื่ออำนวยความสะดวก ลดขั้นตอนการดำเนินงาน ทั้งนี้เพื่อประโยชน์สูงสุดของการให้บริการของหน่วยงานของรัฐ เช่น การให้บริการสอบถามข้อมูล หรือการให้บริการประชาชน ซึ่งมิได้อยู่ในรูปของคำขอหรือการอนุญาต เป็นต้น ดังนั้นเมื่อพิจารณาจากเจตนารมณ์สำคัญประการหนึ่งในการจัดทำพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ในประเด็นความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และผลกระทบจากความเสียหายที่อาจจะเกิดขึ้นหากมีการล่วงละเมิดข้อมูลส่วนบุคคลแล้ว ประกอบกับแม้ในประเทศไทยจะมีกฎหมายหลายฉบับที่เกี่ยวข้องหรือควบคุมเกี่ยวกับข้อมูลส่วนบุคคล แต่ก็ยังไม่ครอบคลุมทั้งระบบ โดยในปัจจุบันกฎหมายสำคัญที่คุ้มครองข้อมูลส่วนบุคคลคือ*พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540* แต่พระราชบัญญัติดังกล่าวครอบคลุมเฉพาะข้อมูลส่วนบุคคลที่อยู่ในครอบครองของหน่วยงานของรัฐ ซึ่งมีหลักการสำคัญคือ *“เปิดเผยเป็นหลัก ยกเว้นข้อจำกัดเฉพาะข้อมูลข่าวสาร ที่หากเปิดเผยแล้วจะเกิดความเสียหายต่อประเทศชาติหรือต่อประโยชน์ที่สำคัญของสาธารณชน”* ในขณะที่ *พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 6* มีหลักการสำคัญคือเพื่อให้มีการคุ้มครองข้อมูลส่วนบุคคลของประชาชนโดยให้ความสำคัญกับ *“ปกปิด” เป็นหลักการทั่วไป ทั้งนี้ “การเปิดเผย” เป็นข้อยกเว้นหากมีการดำเนินการตามกฎหมายและได้รับความยินยอม* ประกอบกับขอบเขตการบังคับใช้มีความแตกต่างกันในประเด็นของความเป็นข้อมูลอิเล็กทรอนิกส์ และการรองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์

สำหรับ*ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ...(ฉบับที่ผ่านการตรวจพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา (เรื่องเสร็จที่ 1135/2558)* ซึ่งเป็นกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป (ครอบคลุมทั้งระบบ) เป็นกฎหมายที่คุ้มครองสิทธิเสรีภาพของประชาชนในข้อมูลส่วนบุคคล นอกจากนี้ยังเป็นไปตามหลักสากลก่อให้เกิดความเชื่อมั่นแก่นานาประเทศที่จะติดต่อกับประชาชนในประเทศ

ดังนั้น อย่างไรก็ดี หน่วยงานของรัฐหลายแห่งได้ตระหนักถึงความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานของรัฐเพื่อประโยชน์ในกิจกรรมของหน่วยงานของรัฐเองหรือเพื่อการให้บริการของรัฐนั้น จึงได้ให้ความสำคัญต่อการเตรียมความพร้อมของหน่วยงานโดยการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 เพื่อเป็นการปฏิบัติตามกฎหมายและเพื่อให้เกิดความสอดคล้องกับหลักปฏิบัติสากลในเรื่องการคุ้มครองข้อมูลส่วนบุคคลด้วย

ผลการบังคับใช้

ตามหลักการสำคัญของพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 หน่วยงานของรัฐใดที่ต้องการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐและประสงค์ให้ข้อมูลอิเล็กทรอนิกส์มีผลทางกฎหมายและบังคับใช้ได้ ให้ปฏิบัติตามหลักเกณฑ์และวิธีการที่กำหนดในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

2

หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล

บทที่ 2 หลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคล

กรอบในการคุ้มครองข้อมูลส่วนบุคคลของ OECD

องค์การความร่วมมือและการพัฒนาทางเศรษฐกิจ หรือ OECD (The Organization for Economic Co-operation and Development) ได้มีการออก Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data ซึ่งเป็นแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่หลายประเทศนิยมนำไปใช้เป็นแนวทางในการยกร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคลในประเทศของตน เพื่อใช้บังคับกับการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยวางหลักการสำคัญไว้ว่า ข้อมูลส่วนบุคคลต้องได้รับการคุ้มครองที่เหมาะสม ในทุกขั้นตอนตั้งแต่การเก็บรวบรวม การเก็บรักษา และการเปิดเผย โดยแนวทางดังกล่าวนี้ คณะกรรมการฯ ได้นำมาเป็นแนวทางในการยกร่าง ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ด้วยเช่นกัน

โดย *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data ของ OECD มีการกำหนดหลักพื้นฐาน 8 ประการ* ดังต่อไปนี้

ข้อ	กรอบ OECD	สาระสำคัญ
1	หลักข้อจำกัดในการเก็บรวบรวมข้อมูล	ในการเก็บรวบรวมข้อมูลนั้น ต้องชอบด้วยกฎหมายและต้องใช้วิธีการที่เป็นธรรมและเหมาะสม โดยในการเก็บรวบรวมข้อมูลนั้นต้องให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล
2	หลักคุณภาพของข้อมูล	ข้อมูลที่เก็บรวบรวมนั้น ต้องเกี่ยวข้องกับวัตถุประสงค์ที่กำหนดขึ้นว่า "จะนำไปใช้ทำอะไร" และเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานตามที่กฎหมายกำหนด นอกจากนั้นข้อมูลดังกล่าวจะต้องถูกต้อง สมบูรณ์ หรือทำให้เป็นปัจจุบัน หรือทันสมัยอยู่เสมอ
3	หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ	ต้องกำหนดวัตถุประสงค์ว่า ข้อมูลที่มีการเก็บรวบรวมนั้น เก็บรวบรวมไปเพื่ออะไร พร้อมทั้งกำหนดระยะเวลาที่เก็บรวบรวมหรือรักษาข้อมูลนั้นตลอดจนกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเช่นว่านั้น ไว้ให้ชัดเจน
4	หลักข้อจำกัดในการนำไปใช้	ข้อมูลส่วนบุคคลนั้น จะต้องไม่มีการเปิดเผย ทำให้มี หรือปรากฏในลักษณะอื่นใด ซึ่งไม่ได้กำหนดไว้โดยชัดแจ้งในวัตถุประสงค์ของการเก็บรวบรวมข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือโดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย

ข้อ	กรอบ OECD	สาระสำคัญ
5	หลักการรักษาความมั่นคงปลอดภัยข้อมูล	จะต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันความเสี่ยงภัยใดๆ ที่อาจจะทำให้ข้อมูลนั้นสูญหาย เข้าถึง ทำลาย ใช้ ดัดแปลง แก้ไข หรือเปิดเผยโดยมิชอบ
6	หลักการเปิดเผยข้อมูล	ควรมีการประกาศนโยบายฯ ให้ทราบโดยทั่วกัน หากมีการปรับปรุง แก้ไข หรือพัฒนาแนวนโยบาย หรือแนวปฏิบัติที่เกี่ยวกับข้อมูลส่วนบุคคล ก็ควรเปิดเผยหรือประกาศไว้ให้ชัดเจน รวมทั้งให้ข้อมูลใดๆ ที่สามารถระบุเกี่ยวกับหน่วยงานของรัฐผู้ให้บริการ ที่อยู่ผู้ควบคุมข้อมูลส่วนบุคคล ด้วย
7	หลักการมีส่วนร่วมของบุคคล	ให้บุคคลซึ่งเป็นเจ้าของข้อมูลได้รับแจ้งหรือยืนยันจากหน่วยงานของรัฐที่เก็บรวบรวม หรือจัดเก็บข้อมูลทราบว่า “หน่วยงานของรัฐนั้นๆ ได้รวบรวมข้อมูลหรือจัดเก็บข้อมูลส่วนบุคคลดังกล่าวหรือไม่ ภายในระยะเวลาที่เหมาะสม”
8	หลักความรับผิดชอบ	ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

Privacy Policy
Macro
Shift

3

การจัดการข้อมูลส่วนบุคคล

ประเด็นสำคัญจากทั้งนโยบายและแนวปฏิบัติ

ส่วนที่ 1 : นโยบายการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์ของการจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคล คือ เป็นการแจ้งให้กับผู้ที่ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐกับหน่วยงานได้ทราบว่า หน่วยงานมีแนวทางในการบริหารจัดการข้อมูลส่วนบุคคลของผู้ใช้บริการซึ่งเป็นเจ้าของข้อมูลอย่างไร เพื่อให้ผู้ใช้บริการทราบและสามารถตัดสินใจได้ว่าจะให้ข้อมูลส่วนบุคคลของตน หรือไม่

สาระสำคัญในนโยบาย

หัวข้อหลักที่เป็นสาระสำคัญในการจัดทำนโยบายที่มีความสอดคล้องกับประกาศคณะกรรมการฯ ประกอบด้วย

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด
2. คุณภาพของข้อมูลส่วนบุคคล
3. การระบุวัตถุประสงค์ในการเก็บรวบรวม
4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้
5. การรักษาความมั่นคงปลอดภัย
6. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล
7. การมีส่วนร่วมของเจ้าของข้อมูล
8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

<u>คำแนะนำ</u>
สาระสำคัญทั้ง 8 ข้อ เป็นรายการขั้นต่ำที่ต้องปรากฏในนโยบาย หน่วยงานสามารถกำหนดสาระสำคัญอื่นเพิ่มเติมนอกเหนือจากที่ประกาศไว้ด้วยก็ได้

ส่วนที่ 2 : แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

วัตถุประสงค์ของการจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล คือ เพื่อให้มีขั้นตอนในการปฏิบัติกับข้อมูลส่วนบุคคลเป็นไปตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ทั้งนี้หน่วยงานจะต้องกำหนดรายละเอียดให้ปรากฏในแต่ละข้อ โดยแนวปฏิบัติควรแสดงถึงขั้นตอนและวิธีการดำเนินการพอสังเขปเพื่อให้ทราบได้ว่าหน่วยงานมีแนวทางปฏิบัติกับข้อมูลส่วนบุคคลอย่างไร

2.1) สาระสำคัญในแนวปฏิบัติ

หัวข้อหลักที่เป็นสาระสำคัญการจัดทำแนวปฏิบัติที่มีความสอดคล้องกับประกาศคณะกรรมการฯ ประกอบด้วย

1. ข้อมูลเบื้องต้น
2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล
3. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น
4. การรวมข้อมูลจากที่มาหลายๆ แห่ง
5. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล
6. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ
7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน
8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
9. การติดต่อกับเว็บไซต์

คำแนะนำ

ก. หน่วยงานต้องระบุหัวข้อให้ครบทั้ง 9 ข้อ

ข. กรณีที่หน่วยงานไม่มีการดำเนินการในแนวปฏิบัติข้อใด ให้คงหัวข้อไว้ และระบุรายละเอียดของหัวข้อนั้นว่า “– ไม่มี –” พร้อมเหตุผลประกอบ

2.2) ในกรณีที่หน่วยงานมีระบบสารสนเทศที่ให้บริการธุรกรรมทางอิเล็กทรอนิกส์หลายระบบงาน โดยแต่ละระบบงานนั้นมีวิธีปฏิบัติในบางเรื่องที่อาจมีความแตกต่างกัน

ในกรณีที่หน่วยงานของรัฐมีระบบการให้บริการหลายระบบงาน ซึ่งแต่ละระบบงานอาจมีข้อปฏิบัติที่มีความแตกต่างกัน หน่วยงานควรมีการกำหนดแนวปฏิบัติของแต่ละระบบงาน โดยอาจจะกำหนดไว้เป็นระเบียบข้อบังคับแนบท้ายประกาศฉบับนี้ได้

หมายเหตุ

1. เพื่อความสะดวกในการปรับแก้ไขประกาศนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานในอนาคต ให้หน่วยงานจัดทำนโยบายและแนวปฏิบัติแยกออกจากกัน

2. ในกรณีที่หน่วยงานได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ด้วย

ทรัสต์มาร์ค (Trust Mark) ตามความในวรรคแรกหมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัสต์มาร์คให้กับผู้ขอรับการรับรอง

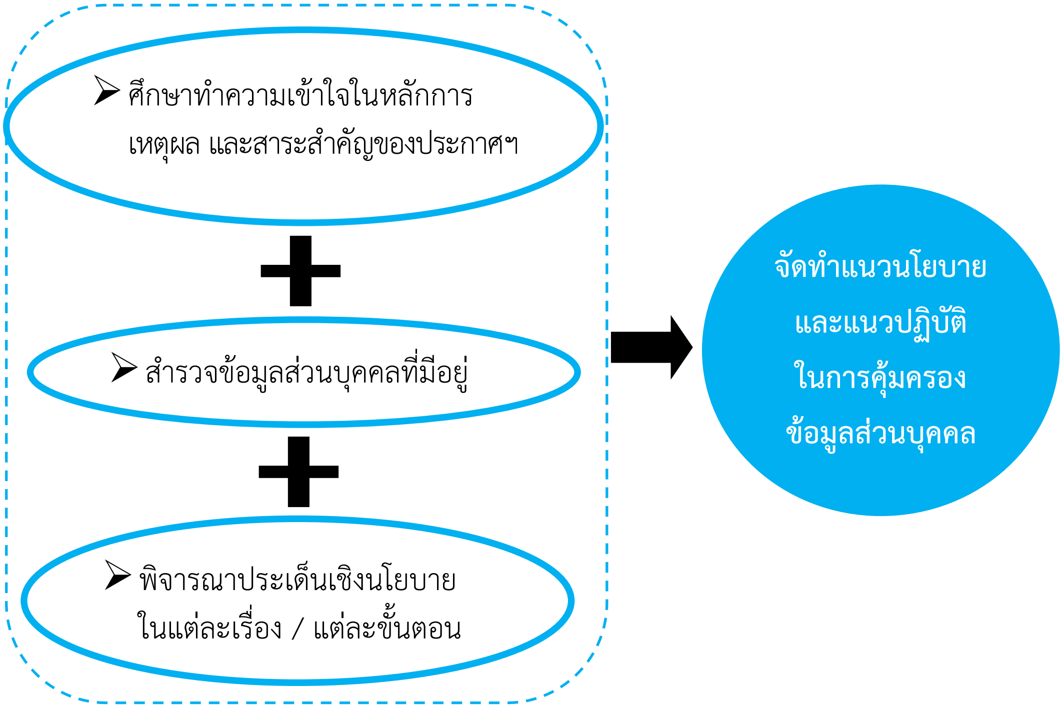
3. ในกรณีที่หน่วยงานได้มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ที่มีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

4

การจัดทำนโยบายและแนวปฏิบัติ
ในการคุ้มครองข้อมูลส่วนบุคคล

บทที่ 4 การจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ขั้นตอนการดำเนินการจัดทำ



- ดำเนินการศึกษาทำความเข้าใจในหลักการ เหตุผล และสาระสำคัญของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553
- ดำเนินการสำรวจและเตรียมความพร้อม เกี่ยวกับข้อมูลส่วนบุคคลที่มีอยู่ เพื่อตรวจสอบข้อมูลเบื้องต้นว่าหน่วยงานมีการรวบรวม จัดเก็บ ใช้ เผยแพร่ข้อมูลส่วนบุคคลที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ในระบบงานใดบ้าง ผู้ใช้บริการคือใคร (เจ้าของข้อมูล) ผู้ควบคุมข้อมูล (ผู้รับผิดชอบในการดูแลการจัดเก็บ การใช้ และการเปิดเผยข้อมูลส่วนบุคคล) วัตถุประสงค์ของการจัดเก็บข้อมูลส่วนบุคคลของแต่ละระบบงาน มีการจัดเก็บข้อมูลส่วนบุคคลประเภทใดบ้าง มีวิธีการจัดเก็บข้อมูลส่วนบุคคลอย่างไร มีการเชื่อมโยงข้อมูลส่วนบุคคลให้กับหน่วยงานอื่นหรือองค์กรอื่น หรือไม่ เป็นต้น
- ดำเนินการพิจารณาประเด็นเชิงนโยบายฯ ในแต่ละเรื่อง พร้อมทั้งพิจารณาในขั้นตอนการปฏิบัติของหน่วยงานที่ปฏิบัติแต่ละเรื่องนั้น
- ดำเนินการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล ทั้งนี้หน่วยงานควรพิจารณาจัดทำควบคู่ หรือหลังจากที่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์แล้ว พร้อมทั้งตรวจสอบความครบถ้วน ถูกต้อง

การสำรวจและเตรียมความพร้อมกับข้อมูลส่วนบุคคลที่มีอยู่

ก่อนจะเริ่มจัดทำนโยบายและแนวปฏิบัติฯ หน่วยงานควรมีการสำรวจความพร้อมของหน่วยงานเพื่อให้ทราบรายละเอียดเกี่ยวกับข้อมูลเบื้องต้นของข้อมูลส่วนบุคคลที่เป็นอยู่ในหน่วยงานเพื่อนำมาใช้กำหนดแนวนโยบายและแนวปฏิบัติฯ

ทั้งนี้ หน่วยงานสามารถกำหนดรายละเอียดข้อมูลเพื่อใช้ในการสำรวจความพร้อมตามตัวอย่าง

ที่	หัวข้อ	มี	ไม่มี	รายละเอียด
1	มีการเก็บรวบรวมข้อมูลส่วนบุคคล หรือไม่			
2	ข้อมูลส่วนบุคคลประเภทใดบ้างที่มีการเก็บรวมรวม			
3	มีการเก็บรวบรวมข้อมูลอย่างไร (เก็บจากเจ้าของข้อมูลโดยตรง หรือเก็บจากบุคคลที่สาม)			
4	ได้มีการเตือนให้เจ้าของข้อมูลทราบถึงการเก็บรวบรวมข้อมูล ส่วนบุคคลนั้น หรือไม่			
5	บุคคลใดเป็นผู้ตัดสินใจว่าจะเก็บรวบรวมข้อมูลส่วนบุคคลอะไรบ้าง และจะเก็บรวบรวมอย่างไร			
6	มีบุคคลอื่นนอกจากเว็บไซต์ที่เก็บรวบรวมข้อมูลส่วนบุคคลนี้หรือไม่			
7	เพราะเหตุใดจึงต้องมีการเก็บรวบรวมข้อมูลส่วนบุคคล และใครเป็นผู้ควบคุมข้อมูลส่วนบุคคลที่มีการเก็บรวบรวมนั้น			
8	ข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมไปมีการเปิดเผยต่อบุคคลที่สามหรือไม่ และหากมีการเปิดเผย เปิดเผยด้วยเหตุผลใด			
9	ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ ถูกเก็บรักษาไว้ที่ไหนและเก็บรักษาอย่างไร			
10	มีการใช้มาตรฐานหรือแนวทางปฏิบัติที่หน่วยงานอื่นกำหนดในการเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล หรือไม่			
11	เจ้าของข้อมูลมีทางเลือกอย่างไรบ้างเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล			
12	อนุญาตให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลของตนเองหรือไม่			
13	กรณีเจ้าของข้อมูลมีคำร้องขอใดๆ เกี่ยวกับข้อมูลส่วนบุคคล (ขอให้แก้ไข หรือขอให้ลบทิ้ง) จะต้องทำอย่างไรบ้าง			

ข้อสังเกตเพิ่มเติม หากหน่วยงานมีการเชื่อมโยงเพื่อใช้ข้อมูลประวัติจากหน่วยงานอื่นๆ เช่น ฐานข้อมูลทะเบียนราษฎร์ หรืออื่นๆ หรือให้หน่วยงานอื่นมาใช้ข้อมูลประวัติจากหน่วยงานเอง จะต้องพิจารณาในข้อ 2, 3 และ 11 ด้วย

ประเด็นพิจารณาในการจัดทำ

ในเบื้องต้นจากการสำรวจความพร้อมของหน่วยงานเพื่อให้ทราบรายละเอียดเกี่ยวกับข้อมูลเบื้องต้นของข้อมูลส่วนบุคคลที่เป็นอยู่ในหน่วยงาน ขอยกตัวอย่างประเด็นพิจารณาในบางหัวข้อ ดังนี้

หัวข้อ ข้อมูลส่วนบุคคลประเภทใดบ้างที่มีการเก็บรวมรวม

1. นิยาม ขอบเขตของคำว่า “ข้อมูลส่วนบุคคล” ตามประกาศคณะกรรมการฯ ไม่ได้กำหนดชัดเจน แต่กำหนดหลักการไว้ในมาตรา 6 ของพระราชกฤษฎีกาฯ ดังนี้ “มาตรา 6 ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม”

2. กำหนดขอบเขตการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งในเบื้องต้นหากพิจารณาจากหลักการตามมาตรา 35 และประกาศคณะกรรมการฯ มีข้อสังเกตว่า หน่วยงานควรพิจารณาข้อมูลส่วนบุคคลของผู้ใช้บริการที่อยู่ในความครอบครองของหน่วยงานที่ได้มาจากการให้บริการของหน่วยงานตามที่กฎหมายกำหนดและหรือตามภารกิจของหน่วยงาน ทั้งจากเว็บไซต์ของหน่วยงานโดยตรง หรือบริการอื่นใดผ่านรูปแบบของการกรอกข้อมูลทางกระดาษแล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่นด้วย

3. การพิจารณากำหนดประเภทของข้อมูล

- ข้อมูลธรรมดาทั่วไป (ขั้นพื้นฐาน) เช่น ชื่อ นามสกุล เพศ ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด อายุ สถานภาพ จดหมายอิเล็กทรอนิกส์
- ข้อมูลธรรมดาทั่วไป (เพิ่มรายละเอียดตามภารกิจของหน่วยงาน แล้วแต่กรณี) เช่น บิดามารดา หมู่โลหิต การเสียภาษี ประวัติการศึกษา ประวัติการทำงาน ประวัติการรักษาพยาบาล
- ข้อมูลห้ามประมวลผล หรือ ข้อมูลห้ามจัดเก็บ หรือข้อมูลลับ เช่น เผ่าพันธุ์ ความเชื่อทางศาสนา ความคิดเห็นทางการเมือง ลักษณะทางพันธุกรรม ข้อมูลที่อาจเป็นผลร้าย ทำให้เสียชื่อเสียง หรืออาจก่อให้เกิดความรู้สึกเกี่ยวกับการเลือกปฏิบัติโดยไม่เป็นธรรมหรือไม่เท่าเทียมกันแก่บุคคลใด
- ข้อมูลที่ได้รับหรือรวบรวมมา ว่ามาจากเจ้าของข้อมูลโดยตรง หรือได้รับมาจากแห่งอื่นใด ทั้งทางเว็บไซต์ หรือได้รับมาจากบุคคลอื่นด้วย
- ข้อมูลที่ได้มาจากเจ้าของข้อมูลโดยตรง จะต้องได้รับความยินยอมหรือแจ้งให้เจ้าของข้อมูลทราบก่อน
- ข้อมูลได้รับมาจากแห่งอื่นใด ทั้งทางเว็บไซต์ หรือได้รับมาจากบุคคลอื่น ได้มาด้วยวิธีการใด หรือเป็นไปตามกฎหมายใด หรือเก็บรวบรวมเพื่อการใด
- ข้อมูลผู้เยาว์ บุคคลซึ่งมีอายุต่ำกว่าสิบแปดปีบริบูรณ์ ต้องใช้วิธีการเฉพาะและเหมาะสมในการจัดเก็บ

- ข้อมูลสถิติเกี่ยวกับประชากร เป็นข้อมูลที่ประมวลผลเชิงสถิติแล้วยังสามารถเชื่อมโยงกลับมายังเจ้าของข้อมูลได้ในภายหลัง

4. การพิจารณา ใครคือ Data Subject ของข้อมูล
   1) เจ้าของข้อมูลบุคคล
   2) ผู้มีหน้าที่รวบรวมข้อมูลและประมวลผลข้อมูล
   3) ผู้ที่มีข้อมูลของเจ้าของข้อมูล

   Data subject คือ ผู้มีสิทธิในข้อมูลส่วนบุคคลที่เก็บรวบรวม

   (Data subject means an individual who is the subject of personal data)

5. การพิจารณา ใครคือ ผู้ควบคุมข้อมูล

   ผู้ควบคุมข้อมูล คือ ผู้ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ที่อยู่ในความรับผิดชอบของหน่วยงาน

แนวทางการเขียน

แนวทางการจัดทำนโยบายและแนวปฏิบัติฯ ตามที่คณะอนุกรรมการภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ที่เกี่ยวข้องกับการตรวจพิจารณา ได้กำหนดหลักการไว้ มีดังนี้

1. หน่วยงานของรัฐต้องกำหนดแนวนโยบายและแนวปฏิบัติฯ แยกออกจากกัน ให้ชัดเจน และเป็นไปตามประกาศคณะกรรมการฯ

2. การดำเนินการนั้น กฎหมายของหน่วยงาน ได้ให้อำนาจแก่หน่วยงานในการจัดเก็บข้อมูลส่วนบุคคลด้วยหรือไม่ โดยต้องมีการระบุไว้ในประกาศอย่างชัดเจน เนื่องจากเป็นประเด็นที่เกี่ยวข้องกับอำนาจหน้าที่ตามกฎหมาย ซึ่งหากหน่วยงานจัดเก็บข้อมูลส่วนบุคคลเกินกว่าอำนาจหน้าที่จะเป็นการไม่ถูกต้อง

3. ส่วนที่เกี่ยวข้องกับนโยบายฯ หน่วยงานจะต้องเขียนแยกเป็นข้อๆ ให้ครบทั้ง 8 ข้อตามที่ประกาศคณะกรรมการฯ กำหนด สำหรับส่วนที่เกี่ยวข้องกับแนวปฏิบัติฯ หน่วยงานจะต้องเขียนโดยให้มีหัวข้อแยกเป็นข้อๆ และให้ครบตามประกาศคณะกรรมการฯ กำหนดเช่นกัน โดยจะต้องระบุวิธีการ/ประเด็นที่ควบคุม รวมทั้งขั้นตอนการปฏิบัติที่ชัดเจนว่าหน่วยงานปฏิบัติอย่างไร หากเรื่องใดที่หน่วยงานไม่ได้ดำเนินการก็ให้ระบุไว้ด้วยว่า “ไม่มี” พร้อมทั้งแสดงเหตุผลที่มิได้ดำเนินการประกอบด้วย โดยห้ามตัดหัวข้อนั้นทิ้ง

4. การจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน (ประเด็นด้านเทคนิคฯ) ควรเน้นให้เห็นว่า “หน่วยงานมีการจัดเก็บข้อมูลส่วนบุคคลอย่างเป็นความลับและมีมาตรการรักษาความมั่นคงปลอดภัยตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน” ดังนั้น หน่วยงานควรเพิ่มข้อความดังกล่าวในนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้มีความเชื่อมโยงไปสู่การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สาระสำคัญของประกาศฯ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

การจัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคล จะต้องมีรายละเอียดอย่างน้อย ดังนี้

กำหนดขอบเขตการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งในเบื้องต้นหากพิจารณาจากหลักการตามมาตรา 35 และประกาศคณะกรรมการฯ มีข้อสังเกตว่า หน่วยงานควรพิจารณาข้อมูลส่วนบุคคลของผู้ใช้บริการที่อยู่ในความครอบครองของหน่วยงานที่ได้มาจากการให้บริการของหน่วยงานตามที่กฎหมายกำหนดและหรือตามภารกิจของหน่วยงาน ทั้งจากเว็บไซต์ของหน่วยงานโดยตรง หรือบริการอื่นใดผ่านรูปแบบของการกรอกข้อมูลทางกระดาษแล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์ หรือจัดเก็บโดยวิธีอื่นด้วย

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

- ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ควรระบุว่าเป็นไปตามกฎหมายใด และต้องระบุวิธีการที่ได้มาซึ่งข้อมูลส่วนบุคคลโดยให้เจ้าของข้อมูลรู้เห็น รับรู้ หรือได้รับความยินยอมจากเจ้าของข้อมูล
- ในกรณีที่การเก็บรวบรวมข้อมูลส่วนบุคคล เพื่อใช้ในการดำเนินการตามกฎหมาย เช่น หน่วยงานมีการประกาศแบบคำร้อง/คำขอต่างๆ หน่วยงานสามารถดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลตามแบบนั้นได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูล เนื่องจากเป็นการดำเนินงานตามกฎหมายของหน่วยงานอยู่แล้ว ทั้งนี้ หน่วยงานสามารถแจ้งให้กับผู้ใช้บริการทราบว่า การเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวเป็นไปตามแบบคำร้อง/คำขอ เลขที่ใด เรื่องอะไร เป็นต้น สำหรับข้อมูลส่วนบุคคลที่หน่วยงานต้องการเก็บรวบรวมนอกเหนือจากแบบดังกล่าวข้างต้น หน่วยงานต้องแจ้งให้ทราบว่ามีการเก็บข้อมูลอะไรเพิ่มเติมใช้เพื่อการใด ซึ่งจะต้องแจ้งให้เจ้าของข้อมูล รับรู้และได้รับความยินยอมก่อนเสมอ

<u>ตัวอย่าง</u>

...(หน่วยงาน).. มีภารกิจหน้าที่ดำเนินการเกี่ยวกับ *...(ระบุภารกิจของหน่วยงานตามกฎหมาย)...*ซึ่งเป็นไปตาม*....(ระบุชื่อกฎหมาย / กฎระเบียบที่เกี่ยวข้อง)..* กำหนด

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการ*...(หน่วยงาน)...*จะใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และจัดเก็บข้อมูลเท่าที่จำเป็นแก่การให้บริการธุรกรรมทางอิเล็กทรอนิกส์ตามวัตถุประสงค์ในการดำเนินงานของ*..(หน่วยงาน)...*ตามที่กฎหมายกำหนดเท่านั้น และ*...(หน่วยงาน)...*จะขอความยินยอมจากผู้ใช้บริการก่อนทำการเก็บรวบรวม เว้นแต่เป็นกรณีที่กฎหมายกำหนด และหรือ ในกรณีอื่นๆ ตามที่กำหนดไว้ในนโยบายฉบับนี้

2. คุณภาพของข้อมูลส่วนบุคคล

- ให้คำนึงถึงว่าการเก็บรวบรวมและจัดเก็บข้อมูลส่วนบุคคลนั้น ต้องเป็นไปตามกฎหมาย / อำนาจหน้าที่ของหน่วยงานที่กำหนดไว้ และรวมถึงการนำไปใช้เป็นสำคัญ
- ข้อมูลส่วนบุคคลที่จัดเก็บจะต้องคำนึงถึงความถูกต้องสมบูรณ์ และทำให้เป็นปัจจุบันและทันสมัยอยู่เสมอ เช่น (1) มีวิธีการตรวจสอบความถูกต้องของข้อมูลก่อนที่มีการจัดเก็บและนำไปประมวลผล (2) มีช่องทางสำหรับให้ผู้ใช้บริการสามารถปรับปรุงแก้ไขข้อมูลส่วนบุคคลของตน เช่น การตรวจสอบการกรอกข้อมูลเลขบัตรประชาชนครบ 13 หลัก หรือไม่ การตรวจสอบการกรอกอีเมล์เป็นไปตามรูปแบบ name@host.domain หรือไม่ เป็นต้น

ตัวอย่าง

*...(หน่วยงาน)...*มีการรวบรวมและจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการเพื่อนำไปใช้ประโยชน์ต่อการดำเนินงานตามภารกิจของหน่วยงานซึ่งเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของ*..(หน่วยงาน)..* ตามที่กฎหมายกำหนด โดยข้อมูลที่จัดเก็บ*...(หน่วยงาน)...*จะให้ความสำคัญถึงความถูกต้อง ครบถ้วน และเป็นปัจจุบันของข้อมูล

3. การระบุวัตถุประสงค์ในการเก็บรวบรวม

- ให้กำหนดวัตถุประสงค์ให้ชัดเจนว่า มีการรวมรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใด
- กรณีที่มีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลหน่วยงานควรจัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

ตัวอย่าง

*...(หน่วยงาน)...*มีการรวบรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคลเพื่อ*...(ระบุวัตถุประสงค์)...* ทั้งนี้ หากภายหลัง *...(หน่วยงาน)...* มีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล*...(หน่วยงาน)...*จะแจ้งให้ผู้ใช้บริการทราบและ/หรือขอความยินยอม พร้อมนี้*...(หน่วยงาน)...*ได้มีการกำหนดให้มีการบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐานด้วย

4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

- ให้แสดงถึงเจตนาการไม่นำไปเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดต่อผู้อื่นที่มิได้เกี่ยวข้อง
- ให้ระบุให้ทราบในกรณีที่มีการบังคับให้เปิดเผยข้อมูลตามกฎหมาย/ คำสั่งศาล (กรณีที่มีกฎหมายกำหนดให้กระทำได้ ให้มีการระบุกฎหมายที่เกี่ยวข้องนั้นด้วย)
- กรณีมีการว่าจ้างหน่วยงานอื่น (outsource) ที่ดำเนินการเกี่ยวกับข้อมูลของผู้ใช้บริการ หน่วยงานต้องกำหนดให้ผู้รับจ้างเก็บรักษาความลับและความปลอดภัยของข้อมูล โดยห้ามผู้รับจ้างนำข้อมูลดังกล่าวไปใช้นอกเหนือจากกิจการหรือกิจกรรมตามที่มอบหมายให้ดำเนินการ

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*จะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ นอกเหนือจากวัตถุประสงค์ในการรวบรวมและจัดเก็บข้อมูล เว้นแต่

- ได้รับความยินยอมจากเจ้าของข้อมูล

5. การรักษาความมั่นคงปลอดภัย

- ให้ระบุมาตรการ / วิธีการ ในการรักษาความมั่นคงปลอดภัยที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ ให้ผู้ใช้บริการทราบ

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*มีมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลอย่างเหมาะสม เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน*...(ระบุนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ)...*เพื่อป้องกันมิให้ข้อมูลสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

6. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

- ให้ระบุวิธีการเปิดเผยนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
- ให้ระบุวิธีการที่ให้ผู้ใช้บริการสามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคล / วัตถุประสงค์ของการนำข้อมูลไปใช้ / ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคลได้

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*จะเปิดเผยแนวปฏิบัติ และแนวนโยบายในการคุ้มครองข้อมูลส่วนบุคคลนี้ และ หากมีการปรับปรุงแก้ไข*...(หน่วยงาน)...*จะดำเนินการเผยแพร่ผ่านทางเว็บไซต์*....(ระบุเว็บไซต์)....*

ทั้งนี้ *...(หน่วยงาน)...*มีช่องทางที่ผู้ใช้บริการสามารถตรวจดูความมีอยู่ / ลักษณะของข้อมูลส่วนบุคคล / วัตถุประสงค์ของการนำข้อมูลไปใช้ / ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล ได้ที่*....(ระบุช่องทาง)..*

7. การมีส่วนร่วมของเจ้าของข้อมูล

- ให้ระบุถึงวิธีการ / รูปแบบและระยะเวลาในการยื่นคำร้องขอรายละเอียดของข้อมูลส่วนบุคคลของเจ้าของข้อมูล รวมถึงค่าใช้จ่าย (ถ้ามี) และระบุให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอดังกล่าวภายในระยะเวลาอันสมควร
- ให้ระบุถึงการห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย และให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใดๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*จะเปิดเผยรายละเอียดข้อมูลส่วนบุคคลต่อเมื่อได้รับคำร้องขอจากเจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย โดย*...(ระบุวิธีการ / รูปแบบการยื่นคำร้อง)...*ทั้งนี้ *...(หน่วยงาน)...*จะดำเนินการให้แล้วเสร็จภายในระยะเวลา*...(ระบุเวลาตามที่หน่วยงานกำหนด)....*

และในกรณีที่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย มีการคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใดๆ เช่น การแจ้งปรับปรุงแก้ไขข้อมูลส่วนบุคคล หรือลบข้อมูลส่วนบุคคลฯลฯ*...(หน่วยงาน)...*จะดำเนินการบันทึกหลักฐานคำคัดค้านดังกล่าวไว้เป็นหลักฐานด้วย

8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

- ให้แสดงให้เห็นถึงการกำหนดให้มีผู้ควบคุมข้อมูลส่วนบุคคลที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนี้

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*กำหนดให้เจ้าหน้าที่ของหน่วยงานซึ่งมีหน้าที่รับผิดชอบในการดูแลการจัดเก็บ การใช้ และการเปิดเผย ข้อมูลส่วนบุคคลของผู้ใช้บริการ ต้องปฏิบัติตาม*...(ระบุชื่อประกาศแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล)...*อย่างเคร่งครัด

<u>การจัดทำแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล จะต้องมีรายละเอียดอย่างน้อย ดังนี้</u>

1. ข้อมูลเบื้องต้น ประกอบด้วย

(ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด

- ต้องมีชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด

(ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคล ที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์

- ให้ระบุ “รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์ ทั้งนี้ให้เป็นไปตามขอบเขตที่กำหนดไว้ในนโยบายข้อ 1 การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด หน้า 19 และข้อ 3 การระบุวัตถุประสงค์ในการเก็บรวบรวม หน้า 20”

(ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคล ให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ

- ให้ระบุ “ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน 15 วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่นการขอความยินยอมจากเจ้าของข้อมูลนั้น ต้องให้มีความชัดเจนว่าหน่วยงานขอรับความยินยอมเพื่อวัตถุประสงค์ใด”

2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

- กำหนดช่องทาง / วิธีการ ของข้อมูลที่เก็บรวบรวมหรือได้รับมา เช่น จากผู้ใช้บริการเว็บไซต์โดยตรง หรือบริการอื่นใดผ่านรูปแบบของการกรอกข้อมูลทางกระดาษแล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่นด้วย ทั้งนี้ หากมีการเก็บรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์ จะต้องระบุว่าอยู่ในส่วนใดของเว็บไซต์หรือเว็บเพจที่มีการรวบรวมและจัดเก็บข้อมูล
- กำหนดประเภทของข้อมูลส่วนบุคคลที่มีการเก็บ รวบรวม ใช้ จากช่องทางข้างต้น กรณีที่หน่วยงานมีการเก็บรวบรวมข้อมูลส่วนบุคคลตามแบบคำร้อง / คำขอ ที่ประกาศกำหนดไว้ หน่วยงานสามารถแจ้งว่าจะจัดเก็บตามแบบคำร้อง / คำขอ เลขที่ใด เรื่องอะไร
- ระบุ / จัดแบ่ง ประเภทข้อมูลที่หน่วยงานจะไม่จัดเก็บ จะต้องแจ้งให้ทราบ ซึ่งตัวอย่างข้อมูลที่หน่วยงานอาจจะไม่จัดเก็บ เช่น เลขบัตรเครดิต ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

<u>ตัวอย่าง</u>

...(หน่วยงาน)... มีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการ เป็นไปตามอำนาจหน้าที่ตามกฎหมาย / ภารกิจหน้าที่ / วัตถุประสงค์ใดของหน่วยงาน ด้วยวิธีการใด / ผ่านช่องทางใดบ้าง / จัดเก็บอะไรบ้าง

(ก) การติดต่อระหว่างหน่วยงานของรัฐ

ให้ระบุ

- ให้ระบุว่าหน่วยงานจะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยวิธีการใด และมีการบอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้าอย่างไร
- ในกรณีที่ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้

ตัวอย่าง

*...(หน่วยงาน)...*จะติดต่อไปยังผู้ใช้บริการโดยทางโทรศัพท์*...(ระบุหมายเลข)...*หรือทาง *...(ระบุอีเมล์)...*ของหน่วยงานที่เกี่ยวข้องกับการให้บริการนั้นๆ

กรณีที่หน่วยงานไม่มีการติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้ระบุว่า "– ไม่มี – พร้อมระบุเหตุผลประกอบ"

ตัวอย่าง

...(หน่วยงาน)... ไม่มีนโยบายที่จะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์ และจะติดต่อกับผู้ใช้บริการเป็นหนังสือทางจดหมายเท่านั้น

(ข) การใช้คุกกี้ (Cookies)

ให้หน่วยงานพิจารณาว่ามีการใช้คุกกี้ที่สามารถเชื่อมโยงกับข้อมูลส่วนบุคคลของผู้ใช้ได้บริการได้ ซึ่งถ้ามี "ให้ระบุสิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้ด้วย"

ตัวอย่าง

เว็บไซต์ของ*...(หน่วยงาน)...* มีการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลได้ โดยใช้คุกกี้เพื่อ*...(ระบุวัตถุประสงค์การใช้คุกกี้)...* ซึ่งผู้ใช้บริการสามารถที่จะยอมรับหรือไม่รับคุกกี้ก็ได้ ในกรณีที่เลือกที่จะไม่รับคุกกี้ เว็บไซต์อาจจะไม่สามารถให้บริการนั้นได้

กรณีที่หน่วยงานไม่มีเว็บไซต์ที่ให้บริการ หรือมีเว็บไซต์แต่ไม่มีการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคล ให้ระบุว่า "– ไม่มี – พร้อมระบุเหตุผลประกอบ"

ตัวอย่าง

เว็บไซต์ของ*...(หน่วยงาน)...* ไม่มีการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลของผู้ใช้บริการ แต่ใช้คุกกี้เพื่อช่วยอำนวยความสะดวกให้บริการเว็บไซต์เท่านั้น ซึ่งผู้ใช้บริการสามารถที่จะยอมรับหรือไม่รับคุกกี้ได้ ในกรณีที่เลือกที่จะไม่รับคุกกี้ เว็บไซต์อาจจะไม่สามารถให้บริการนั้นได้

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

กรณีที่หน่วยงานมีเว็บไซต์ที่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ให้ระบุ ถึง

- วิธีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้
- วัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้

ตัวอย่าง

เว็บไซต์ของ*...(หน่วยงาน)...*มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ซึ่งมีการใช้งานสถิติเกี่ยวกับประชากรเพื่อ*...(ระบุวัตถุประสงค์การใช้)*

กรณีที่หน่วยงานไม่มีเว็บไซต์ที่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ให้ระบุว่า “– ไม่มี –”

(ง) บันทึกผู้เข้าชมเว็บ (Log Files)

ให้ระบุ ถึง

- วิธีการเก็บรวบรวมบันทึกการเข้าออกโดยอัตโนมัติที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้

ตัวอย่าง

*...(หน่วยงาน)...*ไม่มีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร

- วัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้บันทึกการเข้าออกโดยอัตโนมัติที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้

ตัวอย่าง

การให้บริการเว็บไซต์ของ*...(หน่วยงาน)...*มีการเก็บบันทึกการเข้าออกและระหว่างการเข้าใช้บริการของผู้ใช้บริการโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคล ทั้งนี้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อ*...(ระบุวัตถุประสงค์การนำไปใช้งาน)...*

<u>ตัวอย่าง</u>

เว็บไซต์ของ*...(หน่วยงาน)...*มีการเก็บบันทึกการเข้าออกและระหว่างการเข้าใช้บริการของผู้ใช้บริการโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคลได้ ทั้งนี้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า "จะให้หรือไม่ให้" ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

ให้หน่วยงานพิจารณาว่า การจัดเก็บข้อมูลส่วนบุคคล<u>ทางเว็บไซต์</u>ที่ให้บริการของหน่วยงาน มีลักษณะการจัดเก็บข้อมูลเป็นอย่างไร เช่น

๑) ข้อมูลที่ผู้ใช้บริการต้องให้ (Mandatory field) ซึ่งเป็นข้อมูลที่จำเป็นต่อการประมวลผลและการดำเนินการตามคำขอของผู้ใช้บริการ ถ้าไม่ให้ข้อมูล ผู้ใช้บริการจะไม่สามารถใช้บริการ e-Services นั้นได้ จะระบุด้วยอักษรสีแดง หรือกำกับด้วยเครื่องหมาย (*) เป็นต้น

๒) ข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้หรือไม่ให้ก็ได้ (Optional field) ถ้าผู้ใช้บริการไม่ประสงค์จะให้ข้อมูล ผู้ใช้บริการยังสามารถใช้บริการ e-Services นั้นได้ ทั้งนี้ผู้ใช้บริการสามารถให้ข้อมูลส่วนบุคคลดังกล่าว โดยติดต่อกับเจ้าหน้าที่ที่เกี่ยวข้องก็ได้

ในกรณีที่มีการจัดเก็บข้อมูลส่วนบุคคลในรูปแบบของการกรอกข้อมูลทางกระดาษแล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่นด้วย ให้ระบุว่า "*...(หน่วยงาน)...* ไม่มีการจัดเก็บข้อมูลส่วนบุคคลผ่านทางเว็บไซต์"

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*มีเว็บไซต์ให้บริการ ซึ่งผู้ใช้บริการต้องให้ข้อมูลที่จำเป็นต่อการประมวลผลและการดำเนินการตามคำขอนั้น โดยจะระบุด้วยอักษรสีแดง หรือกำกับด้วยเครื่องหมาย (*) เป็นต้น และในส่วนของข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้ หรือไม่ให้ ก็ได้ หากในกรณีที่ผู้ใช้บริการไม่ประสงค์จะให้ข้อมูลนั้น ผ่านเว็บไซต์สามารถติดต่อกับ*...(หน่วยงาน)...*โดยช่องทางอื่นๆ ได้แก่ *...(ระบุช่องทางการติดต่อ เช่น ทางจดหมาย โทรศัพท์ หรือที่ทำการของหน่วยงาน ฯลฯ)...* หรือเจ้าหน้าที่ที่เกี่ยวข้องโดยตรงก็ได้

3. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

ต้องกำหนดให้มีการระบุชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่ได้ให้กับหน่วยงานหรือองค์กรนั้นๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล และต้องกำหนดให้มีการแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น

ตัวอย่าง

เว็บไซต์ของ...*(หน่วยงาน A)*...มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับ...*(หน่วยงาน B)*... โดย..*(หน่วยงาน A)*..เป็นผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ และ..*(หน่วยงาน B)* ..เป็นผู้มีสิทธิเข้าถึงและใช้ข้อมูลดังกล่าว ซึ่งได้มีการใช้ข้อมูล..*(ประเภทข้อมูล)*...ร่วมกัน ทั้งนี้ ขอให้ผู้ใช้บริการได้โปรดตรวจสอบ นโยบายและแนวปฏิบัติของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน B ด้วย

กรณีที่หน่วยงานไม่มีการเชื่อมโยงให้ข้อมูลกับหน่วยงานหรือองค์กรอื่น ให้ระบุว่า "– ไม่มี –"

ตัวอย่าง

เว็บไซต์ของ...*(หน่วยงาน)*..ไม่มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น...(ระบุเหตุผลประกอบ)...

4. การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

ต้องกำหนดให้มีการแสดงเจตนาของการรวบรวมข้อมูลส่วนบุคคลจากผู้ใช้บริการผ่านทางเว็บไซต์ที่ให้บริการ และนำข้อมูลส่วนบุคคลนั้นไปรวมกับข้อมูลส่วนบุคคลที่ได้รับจากแห่งอื่นๆ นั้นเพื่ออะไร

ตัวอย่าง

...*(หน่วยงาน)*...นำข้อมูลส่วนบุคคลที่ได้รับมาจากผู้ใช้บริการผ่านทางเว็บไซต์ไปรวมเข้ากับข้อมูลของบุคคลที่ได้รับจากที่มาแห่งอื่น...*(ระบุวัตถุประสงค์การนำไปใช้)*...

กรณีที่หน่วยงานไม่มีการรับข้อมูลส่วนบุคคลมาจากผู้ใช้บริการผ่านทางเว็บไซต์ที่ให้บริการ ให้ระบุว่า "– ไม่มี –"

ตัวอย่าง

...*(หน่วยงาน)*...ไม่มีการนำข้อมูลส่วนบุคคลซึ่งได้รับมาจากผู้ใช้บริการผ่านทางเว็บไซต์ไปรวมเข้ากับข้อมูลของบุคคลที่ได้รับจากที่มาแห่งอื่น...*(ระบุเหตุผลประกอบ)*...

5. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

ต้องกำหนดให้มีการระบุไว้ในนโยบายในการคุ้มครองข้อมูล โดยให้ระบุว่า หน่วยงานได้มีการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลกับหน่วยงานใดหรือบุคคลใดบ้าง และสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานที่มีหน้าที่ในการดำเนินการดังกล่าวอย่างไร (เช่น ต้องปฏิบัติตามพระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน เป็นต้น)

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*มีการให้บุคคลอื่นเข้าถึง หรือใช้ข้อมูลที่หน่วยงานได้เก็บรวบรวมผ่านทางเว็บไซต์ ให้กับ*..(ระบุชื่อหน่วยงานอื่นที่เข้าถึง/ใช้)..*ซึ่งเป็นไปตามกฎหมาย *..(ระบุชื่อกฎหมาย)..*

กรณีที่หน่วยงานไม่มีการให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคลให้ระบุว่า "– ไม่มี –"

<u>ตัวอย่าง</u>

*...(หน่วยงาน)...*ไม่มีการให้บุคคลอื่นเข้าถึงหรือใช้ข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมมา *...(ระบุเหตุผลประกอบ)...*

6. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

ให้หน่วยงานระบุถึงสิทธิของผู้ใช้บริการ สำหรับในกรณีที่หน่วยงานมีความประสงค์จะนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้เพื่อวัตถุประสงค์อย่างอื่น<u>ที่แตกต่างหรือที่นอกเหนือ</u>จากที่ได้ระบุไว้ (ถ้ามี) ดังนี้

- หน่วยงานจะขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลก่อน
- หน่วยงานให้สิทธิกับผู้ใช้บริการสามารถปฏิเสธ "ไม่ให้" มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น
- ทั้งนี้ หน่วยงานต้องระบุรายละเอียดให้ผู้ใช้บริการทราบว่า หากต้องการใช้สิทธิ "ให้หรือไม่ให้" ผู้ใช้บริการจะต้องดำเนินการอย่างไร

กรณีที่ผู้ใช้บริการเลือกสิทธิห้ามไม่ให้ใช้ข้อมูลส่วนบุคคลนอกเหนือวัตถุประสงค์ที่ได้ระบุไว้ในครั้งแรก หน่วยงานต้องระบุช่องทางการติดต่อให้ผู้ใช้ทราบด้วยว่า หากจะติดต่อกับเว็บไซต์ในครั้งต่อไปจะมีวิธีการอย่างไร

ตัวอย่าง

โดยทั่วไป...(หน่วยงาน)...จะไม่เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการนอกเหนือจากวัตถุประสงค์ที่ได้กำหนดไว้ แต่ในบางกรณีหน่วยงานจำเป็นต้องนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้ เปิดเผย ต่อบุคคลอื่น ซึ่งการเปิดเผยดังกล่าว...(ระบุเหตุผล ความจำเป็น / เจตนาการนำไปใช้งาน)...

ทั้งนี้...(หน่วยงาน)...จะขอความยินยอมจากเจ้าของข้อมูลและให้สิทธิผู้ใช้บริการเลือกว่าจะให้ หรือไม่ให้ ใช้ หรือเปิดเผย ข้อมูลนั้นเพื่อวัตถุประสงค์...(ระบุวัตถุประสงค์)...นั้น

กรณีที่หน่วยงานไม่มีความประสงค์จะนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้เพื่อวัตถุประสงค์อย่างอื่นที่แตกต่างหรือที่นอกเหนือจากที่ได้ระบุไว้ ให้ระบุว่า “– ไม่มี –”

ตัวอย่าง

...(หน่วยงาน)...ไม่มีการนำข้อมูลส่วนบุคคลที่ได้รวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการไปดำเนินการอย่างอื่น นอกเหนือวัตถุประสงค์ที่ได้ระบุไว้

7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

- ให้หน่วยงานของรัฐกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานของรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง

ตัวอย่าง

ผู้ใช้บริการสามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลของท่านที่...(หน่วยงาน)...รวบรวม จัดเก็บไว้ ผ่านทางเว็บไซต์...(ระบุเว็บไซต์)...หรือช่องทางอื่นๆ ...(ระบุช่องทางอื่นๆ เช่น ที่ทำการ / เจ้าหน้าที่ที่เกี่ยวข้อง)...โดยเป็นไปตามระเบียบของ...(หน่วยงาน)...ที่กำหนดไว้

8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ให้ระบุว่ามีมาตรการ / วิธีการในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้อย่างเหมาะสม อย่างไร และเป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานที่ผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือเทียบเท่าหรือสูงกว่า

(ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสารให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

- กรณีที่หน่วยงานมีเอกสารรายละเอียดมาตรการการสร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้

(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงานหรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

- กรณีที่หน่วยงานมีเอกสารรายละเอียดการกำหนดสิทธิและข้อจำกัดสิทธิให้กับบุคคลากรที่เกี่ยวข้องในการเข้าถึงข้อมูลส่วนบุคคลแต่ละลำดับชั้นอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

- กรณีที่หน่วยงานมีเอกสารรายละเอียดการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้

(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

- กรณีที่หน่วยงานมีเอกสารรายละเอียดมาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจนอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้

(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม

- กรณีที่หน่วยงานมีเอกสารรายละเอียดการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้

9. การติดต่อกับเว็บไซต์

เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(ก) ชื่อและที่อยู่

(ข) หมายเลขโทรศัพท์

(ค) หมายเลขโทรสาร

(ง) ที่อยู่จดหมายอิเล็กทรอนิกส์

*** **<u>หมายเหตุ</u>***

- *มาตรการที่กำหนดไว้ในนโยบายเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลว่าจะดำเนินการอย่างไรที่จะป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ ให้ผู้ใช้บริการทราบและมั่นใจในบริการของหน่วยงานนั้น ให้หน่วยงานนำมาตรการดังกล่าวมาระบุขั้นตอนการปฏิบัติไว้ในแนวปฏิบัติด้วย ทั้งนี้ หากมาตรการดังกล่าวหน่วยงานได้มีเอกสารรายละเอียดเป็นข้อปฏิบัติ / แผนปฏิบัติในการดำเนินการดังกล่าวอยู่แล้ว หน่วยงานสามารถอ้างอิงไปยังเอกสารฉบับนั้นได้ (<u>ตัวอย่างเช่น</u> มาตรการการป้องกันการทำลายข้อมูลส่วนบุคคลให้เป็นไปตามวิธีปฏิบัติในประกาศ...(หน่วยงาน)...เรื่อง...(ชื่อเอกสารที่ต้องการอ้างอิง)...หน้าที่...ในหัวข้อ...(ระบุชื่อหัวข้อ)... เป็นต้น)*
- *ทั้งนี้ การจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน (ประเด็นด้านเทคนิคฯ) ควรเน้นให้เห็นว่า "หน่วยงานมีการจัดเก็บข้อมูลส่วนบุคคลอย่างเป็นความลับ และมีมาตรการรักษาความมั่นคงปลอดภัยตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน" ดังนั้น หน่วยงานควรเพิ่มข้อความดังกล่าวในนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้มีความเชื่อมโยงไปสู่การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ*

ตัวอย่างนโยบายในการคุ้มครองข้อมูลส่วนบุคคล

ประกาศ ....*(หน่วยงาน)*......................

เรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

บทนำ (ถ้ามี)

นโยบายฯ ฉบับนี้จัดทำขึ้นเพื่อให้ผู้ใช้บริการได้ทราบและเข้าใจในนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่*...(หน่วยงาน)...*ได้เก็บรวบรวม ใช้ เปิดเผยและเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยเป็นไปตามกฎหมาย / อำนาจหน้าที่ / ภารกิจ / (ระบุชื่อกฎหมาย) การดำเนินงานของ*...(หน่วยงาน)...*ซึ่งมีการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ทั้งทางเว็บไซต์และทางกระดาษเป็นไปตามแบบฟอร์มในการให้บริการของ*...(หน่วยงาน)...*แล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น

(หมายเหตุ กรณีที่หน่วยงานต้องการกำหนดนิยามศัพท์ขอให้ใส่ในบทนำ)....

1. ขอบเขตของการเก็บรวบรวมข้อมูลส่วนบุคคล

*...(หน่วยงาน)...*มีการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้บริการด้วยวิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และจัดเก็บข้อมูลเท่าที่จำเป็นในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของ*..(หน่วยงาน)...*ตามที่กฎหมายกำหนดเท่านั้น โดยแจ้งให้ผู้ใช้บริการทราบและขอความยินยอมก่อนเก็บรวบรวมข้อมูลนั้น เว้นแต่เป็นกรณีที่กฎหมายกำหนด และหรือ ในกรณีอื่นๆ ตามที่กำหนดไว้ในนโยบายฉบับนี้

2. คุณภาพของข้อมูลส่วนบุคคล

*...(หน่วยงาน)...*มีการรวบรวมและจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ เพื่อนำไปใช้ประโยชน์ต่อการดำเนินงานตามภารกิจของหน่วยงาน ซึ่งเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของ*...(หน่วยงาน)...*ตามที่กฎหมายกำหนด โดยข้อมูลที่จัดเก็บ*..(หน่วยงาน)..*จะให้ความสำคัญถึงความถูกต้อง ครบถ้วน และเป็นปัจจุบันของข้อมูล

3. วัตถุประสงค์ในการจัดเก็บข้อมูลส่วนบุคคล

*...(หน่วยงาน)...*มีการรวบรวม จัดเก็บ ใช้ ข้อมูลส่วนบุคคลเพื่อ*...(ระบุวัตถุประสงค์)...* ทั้งนี้หากภายหลัง *..(หน่วยงาน)...*มีการเปลี่ยนแปลงวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล*...(หน่วยงาน)...*จะแจ้งให้ผู้ใช้บริการทราบและ/หรือขอความยินยอม พร้อมนี้ *..(หน่วยงาน)...*ได้มีการกำหนดให้มีการบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐานด้วย

4. **ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้**

...(หน่วยงาน)... จะไม่เปิดเผยข้อมูลส่วนบุคคลที่ได้จัดเก็บรวบรวมไว้ นอกเหนือจากวัตถุประสงค์ในการรวบรวมและจัดเก็บข้อมูล เว้นแต่ได้รับความยินยอมจากเจ้าของข้อมูลหรือตามคำสั่งศาล และกำหนดให้ผู้รับจ้าง (outsource) เก็บรักษาความลับและความปลอดภัยของข้อมูลของผู้ใช้บริการ โดยห้ามนำข้อมูลไปใช้นอกเหนือจากที่กำหนดให้ดำเนินการ

5. **การรักษาความมั่นคงปลอดภัย**

...(หน่วยงาน)... มีมาตรการในการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลอย่างเหมาะสมอย่างเหมาะสม เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน *...(ระบุนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ)...*เพื่อป้องกันมิให้ข้อมูลสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

6. **การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล**

*...(หน่วยงาน)...*จะเปิดเผยแนวปฏิบัติและแนวนโยบายในการคุ้มครองข้อมูลส่วนบุคคลนี้ และหากมีการปรับปรุงแก้ไข *..(หน่วยงาน)...*จะดำเนินการเผยแพร่ทาง*.....(ระบุเว็บไซต์ / ที่ทำการ)....*

ทั้งนี้*...(หน่วยงาน)...*มีช่องทางที่ผู้ใช้บริการสามารถตรวจดูความมีอยู่ /ลักษณะของข้อมูลส่วนบุคคล / วัตถุประสงค์ของการนำข้อมูลไปใช้ / ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล ได้ที่*...(ระบุช่องทาง)....*

7. **การมีส่วนร่วมของเจ้าของข้อมูล**

*...(หน่วยงาน)...*จะเปิดเผยรายละเอียดข้อมูลส่วนบุคคลต่อเมื่อได้รับคำร้องขอจากเจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย โดย*...(ระบุวิธีการ / รูปแบบการยื่นคำร้อง)...*ทั้งนี้ *..(หน่วยงาน)...*จะดำเนินการให้แล้วเสร็จภายในระยะเวลา*..(ระบุเวลาตามที่หน่วยงานกำหนด)..*

และในกรณีที่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ตามกฎหมาย มีการคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใดๆ เช่น การแจ้งปรับปรุงแก้ไขข้อมูลส่วนบุคคล หรือลบข้อมูลส่วนบุคคล ฯลฯ *...(หน่วยงาน)...*จะดำเนินการบันทึกหลักฐานคำคัดค้านดังกล่าวไว้เป็นหลักฐานด้วย

8. **ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูลส่วนบุคคล**

*...(หน่วยงาน)...*กำหนดให้เจ้าหน้าที่ที่ของหน่วยงานซึ่งมีหน้าที่รับผิดชอบในการดูแลการจัดเก็บ การใช้ และเปิดเผย ข้อมูลส่วนบุคคลของผู้ใช้บริการ ต้องปฏิบัติตาม *..(ระบุชื่อประกาศแนวนโยบายฯ)..* อย่างเคร่งครัด

....

.......ผู้บริหารของหน่วยงานลงนาม......

วันที่ .. เดือน .... พ.ศ. ....

<u>ตัวอย่างแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล</u>

ประกาศ *.............(หน่วยงาน)......................*

เรื่อง แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

บทนำ (ถ้ามี)

แนวปฏิบัติฯ ฉบับนี้สอดคล้องกับนโยบายในการคุ้มครองข้อมูลส่วนบุคคลที่*...(หน่วยงาน)...* ได้เก็บรวบรวม ใช้ เปิดเผยและเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการ โดยเป็นไปตามกฎหมาย / อำนาจหน้าที่ / ภารกิจ / (ระบุชื่อกฎหมาย) การดำเนินงานของ*...(หน่วยงาน)...*ซึ่งมีการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ทั้งทางเว็บไซต์และทางกระดาษเป็นไปตามแบบฟอร์มในการให้บริการของ *...(หน่วยงาน)...*แล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น

(<u>หมายเหตุ</u> กรณีที่หน่วยงานต้องการกำหนดนิยามศัพท์ขอให้ใส่ในบทนำ)....

1. ข้อมูลเบื้องต้น

(ก) แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล จัดทำขึ้นเพื่อบังคับใช้ตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของ*....(หน่วยงาน)...*

(ข) ...(ระบุขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานรวบรวม จัดเก็บ หรือใช้ตามวัตถุประสงค์ ให้เป็นไปตามขอบเขตที่กำหนดไว้ในนโยบายข้อ 1 การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด หน้า 23 และข้อ 3 การระบุวัตถุประสงค์ในการเก็บรวบรวม หน้า 24)...

*(ค)...*ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้ง*...(ระบุวัตถุประสงค์)...*ตาม*...(ระบุวิธีการ)..*และ*..(ระบุระยะเวลาที่เหมาะสม)...*ผ่านทาง*...(ระบุช่องทาง)...*เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

2. การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

*...(หน่วยงาน)...*มีการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ ทั้งทางเว็บไซต์ (ถ้ามี)*...(ระบุเว็บไซต์)..* และทางกระดาษเป็นไปตามแบบฟอร์มในการให้บริการของ*...(ระบุกฎหมาย / อำนาจหน้าที่ / ภารกิจ / การดำเนินงานของหน่วยงาน)...*แล้วนำมาแปลงข้อมูลเข้าสู่ระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น

** ให้ระบุ / จัดแบ่ง ประเภทข้อมูลที่หน่วยงานจะไม่จัดเก็บ จะต้องแจ้งให้ทราบ

<u>ตัวอย่างข้อมูลที่หน่วยงานอาจจะไม่จัดเก็บ</u> เช่น ความเชื่อ ความคิดเห็นทางการเมือง เป็นต้น

(ก) การติดต่อระหว่างหน่วยงานของรัฐ

*...(หน่วยงาน)...*จะติดต่อไปยังผู้ใช้บริการ โดยทางโทรศัพท์*...(ระบุหมายเลข)...* หรือทางอีเมล์*...(ระบุอีเมล์)...*ของหน่วยงานที่เกี่ยวข้องกับการให้บริการนั้นๆ

(ข) การใช้คุกกี้ (Cookies)

เว็บไซต์ของ...*(หน่วยงาน)*...มีการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคลได้ โดยใช้คุกกี้เพื่อ...*(ระบุวัตถุประสงค์การใช้คุกกี้)*...ซึ่งผู้ใช้บริการสามารถที่จะยอมรับหรือไม่รับคุกกี้ก็ได้ ในกรณีที่เลือกที่จะไม่รับคุกกี้ เว็บไซต์อาจจะไม่สามารถให้บริการนั้นได้

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

กรณีมี

เว็บไซต์ของ...*(หน่วยงาน)*...มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ซึ่งมีการใช้งานสถิติเกี่ยวกับประชากรเพื่อ.....*(ระบุวัตถุประสงค์การใช้)*...

กรณีไม่มี ให้ระบุว่า “– ไม่มี –”

...*(หน่วยงาน)*...ไม่มีเว็บไซต์ที่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ หรือ

...*(หน่วยงาน)*...มีเว็บไซต์ให้บริการแต่ไม่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ หรือ

เว็บไซต์ของ...*(หน่วยงาน)*...ไม่มีการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากรที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้

(ง) บันทึกผู้เข้าชมเว็บ (Log Files)

ต้องมีเพราะต้องปฏิบัติตาม พ.ร.บ. คอมพิวเตอร์ฯ

การให้บริการเว็บไซต์ของ...*(หน่วยงาน)*...ต้องมีการเก็บบันทึกการเข้าออกและระหว่างการเข้าใช้บริการของผู้ใช้บริการโดยอัตโนมัติที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลที่ระบุตัวบุคคล ทั้งนี้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อ..*(ระบุวัตถุประสงค์การนำไปใช้งาน..*

(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า “จะให้หรือไม่ให้” ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

...*(หน่วยงาน)*...มีเว็บไซต์ให้บริการ ซึ่งผู้ใช้บริการต้องให้ข้อมูลที่จำเป็นต่อการประมวลผลและการดำเนินการตามคำขอนั้น โดยจะระบุด้วยอักษรสีแดง หรือกำกับด้วยเครื่องหมาย (*) เป็นต้น และในส่วนของข้อมูลที่ผู้ใช้บริการมีสิทธิเลือกว่าจะให้ หรือไม่ให้ ก็ได้ หากในกรณีที่ผู้ใช้บริการไม่ประสงค์จะให้ข้อมูลนั้น ผ่านเว็บไซต์สามารถติดต่อกับ...*(หน่วยงาน)*...โดยช่องทางอื่นๆ ได้แก่...(ระบุช่องทางการติดต่อ ตัวอย่างเช่น ทางจดหมาย โทรศัพท์ หรือที่ทำการของหน่วยงาน ฯลฯ)...หรือเจ้าหน้าที่ที่เกี่ยวข้องโดยตรงก็ได้

3. การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

เว็บไซต์ของ...*(หน่วยงาน A)*...มีการเชื่อมโยงให้ข้อมูลส่วนบุคคลกับ...*(หน่วยงาน B)*...โดย..*(หน่วยงาน A)*..เป็นผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ และ..*(หน่วยงาน B)* ..เป็นผู้มีสิทธิเข้าถึงและใช้ข้อมูลดังกล่าว ซึ่งได้มีการใช้ข้อมูล..*(ประเภทข้อมูล)*...ร่วมกัน ทั้งนี้ ขอให้ผู้ใช้บริการได้โปรดตรวจสอบ นโยบายและแนวปฏิบัติของนโยบายการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน B ด้วย

4. การรวมข้อมูลจากที่มาหลายๆ แห่ง

...*(หน่วยงาน)*...นำข้อมูลส่วนบุคคลที่ได้รับมาจากผู้ใช้บริการผ่านทางเว็บไซต์ไปรวมเข้ากับข้อมูลของบุคคลที่ได้รับจากที่มาแห่งอื่น...*(ระบุวัตถุประสงค์การนำไปใช้)*...

5. การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

...*(หน่วยงาน)*...มีการให้บุคคลอื่นเข้าถึง หรือใช้ข้อมูลที่หน่วยงานได้เก็บรวบรวมผ่านทางเว็บไซต์ ให้กับ..*(ระบุชื่อหน่วยงานอื่นที่เข้าถึง/ใช้)*..ซึ่งเป็นไปตามกฎหมาย ..*(ระบุชื่อกฎหมาย)*..

6. การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

โดยทั่วไป...*(หน่วยงาน)*...จะไม่เปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการนอกเหนือจากวัตถุประสงค์ที่ได้กำหนดไว้ แต่ในบางกรณีหน่วยงานจำเป็นต้องนำข้อมูลส่วนบุคคลของผู้ใช้บริการไปใช้ เปิดเผย ต่อบุคคลอื่น ซึ่งการเปิดเผยดังกล่าว...(ระบุเหตุผล ความจำเป็น / เจตนาการนำไปใช้งาน)...

ทั้งนี้...*(หน่วยงาน)*...จะขอความยินยอมจากเจ้าของข้อมูลและให้สิทธิผู้ใช้บริการเลือกว่าจะให้หรือไม่ให้ ใช้ หรือเปิดเผย ข้อมูลนั้นเพื่อวัตถุประสงค์...*(ระบุวัตถุประสงค์)*...นั้น

7. การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

ผู้ใช้บริการสามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลของท่านที่...*(หน่วยงาน)*... รวบรวม จัดเก็บไว้ ผ่านทางเว็บไซต์...*(ระบุเว็บไซต์)*...หรือช่องทางอื่นๆ...*(ระบุช่องทางอื่นๆ เช่น ที่ทำการ / เจ้าหน้าที่ที่เกี่ยวข้อง)*...โดยเป็นไปตามระเบียบของ...*(หน่วยงาน)*...ที่กำหนดไว้

8. การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

...*(หน่วยงาน)*..มีมาตรการ / วิธีการในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้อย่างเหมาะสม สอดคล้องตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ...*(ระบุนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือเทียบเท่าหรือสูงกว่า)*...

(ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสารให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

*...(หน่วยงาน)..*มีการจัดเผยแพร่ข้อมูลข่าวสารด้านความมั่นคงปลอดภัย เพื่อให้ความรู้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงาน และมีการจัดฝึกอบเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำอย่างน้อยปีละ 1 ครั้ง

(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

*..(หน่วยงาน)..*มีการกำหนดสิทธิและข้อจำกัดในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากรในแต่ละลำดับชั้นไว้อย่างชัดเจน และจัดให้มีการบันทึกรวมทั้งจัดทำสำรองข้อมูลของการเข้าถึงในระยะเวลาที่กฎหมายกำหนด

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ 1 ครั้ง

*..(หน่วยงาน)..*ได้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือระบบสารสนเทศทั้งหมออย่างน้อยปีละ 1 ครั้ง.

(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

*..(หน่วยงาน)..*ได้มีการกำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น สุขภาพ ความเชื่อ เป็นต้น

(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม

*..(หน่วยงาน)..*มีการจัดเก็บข้อมูลส่วนบุคคลซึ่งมีอายุไม่เกินสิบแปดปี และใช้วิธีการโดยเฉพาะและเหมาะสม

9. การติดต่อกับเว็บไซต์

เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(ก) ชื่อและที่อยู่

(ข) หมายเลขโทรศัพท์

(ค) หมายเลขโทรสาร

(ง) ที่อยู่จดหมายอิเล็กทรอนิกส์

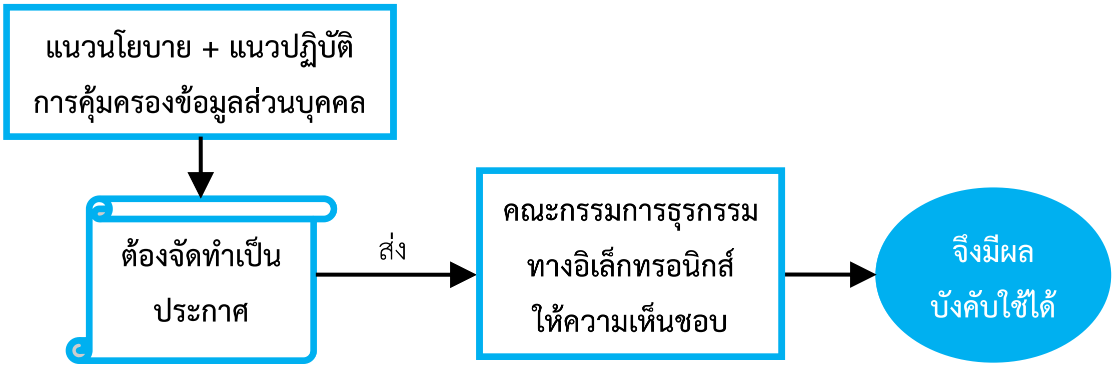
....

.......ผู้บริหารของหน่วยงานลงนาม......

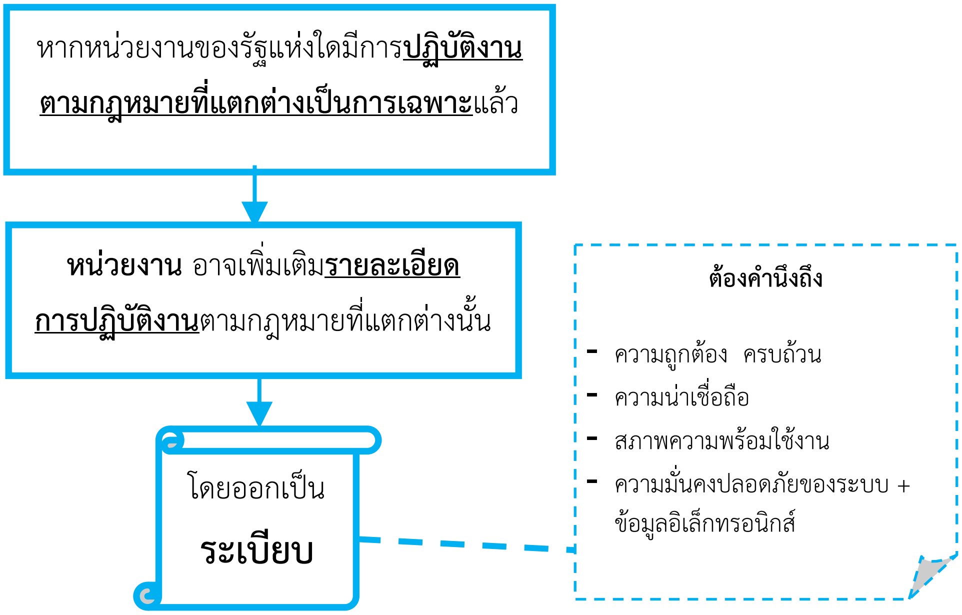
วันที่ .. เดือน .... พ.ศ. ....

ขั้นตอนการจัดส่งนโยบายและแนวปฏิบัติฯ ของหน่วยงานให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณา

1. เมื่อหน่วยงานดำเนินการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลเรียบร้อยแล้ว หน่วยงานต้องจัดทำเป็นประกาศของหน่วยงานและให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เพื่อพิจารณาให้ความเห็นชอบ จึงมีผลบังคับใช้ได้



กรณีที่หน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะ



2. ขั้นตอนการจัดส่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณาให้ความเห็นชอบ

หน่วยงานของรัฐทำการประเมินตนเองว่า
แนวนโยบายและแนวปฏิบัติสอดคล้องกับ
ประกาศคณะกรรมการฯ หรือไม่

↓

จัดส่งแนวนโยบาย+แนวปฏิบัติ
แบบประเมินและเอกสารประกอบการพิจารณา
อื่นๆ ที่เกี่ยวข้อง (ถ้ามี)

↓

โดยส่งมาที่สำนักงานคณะกรรมการธุรกรรมทาง
อิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและ
สังคม

แบบฟอร์ม

“แบบประเมินประกอบการพิจารณาการดำเนินงานตามแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐตามมาตรา 7 ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549”

3. ลำดับขั้นตอนการพิจารณานโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

1) สำนักงานฯ ในฐานะฝ่ายเลขานุการของคณะกรรมการฯ จะดำเนินการตรวจสอบแนวนโยบายและแนวปฏิบัติฯ ของหน่วยงานว่ามีความสอดคล้องกับประกาศคณะกรรมการฯ และตรงตามหลักเกณฑ์การตรวจพิจารณาหรือไม่

- หากมีข้อประเด็นซักถาม หรือ มีการปรับแก้ไขโดยไม่เป็นสาระสำคัญ เจ้าหน้าที่ของสำนักงานฯ จะประสานกับหน่วยงานเพื่อซักถาม หรือขอให้ปรับแก้ไขแนวนโยบายและแนวปฏิบัติฯ เพื่อให้มีความครบถ้วน สมบูรณ์
- เมื่อสำนักงานฯ ตรวจสอบแนวนโยบายและแนวปฏิบัติฯ ของหน่วยงานเรียบร้อยแล้วสำนักงานฯ จะนำเสนอต่อคณะกรรมการฯ เพื่อให้ความเห็นชอบต่อไป
- หากมีประเด็นทางด้านเทคนิคจะดำเนินการจัดส่งให้คณะอนุกรรมการฯ ที่เกี่ยวข้องภายใต้คณะกรรมการฯ เพื่อพิจารณาให้ความเห็นก่อนนำเสนอต่อคณะกรรมการฯ

วิธีการและช่องทางจัดส่งเอกสารให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์พิจารณา

<u>ช่องทางจัดส่งเอกสาร</u>

- จัดส่งทางไปรษณีย์ หรือยื่นเอกสารด้วยตนเอง

เรียน ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
อาคารรัฐประศาสนภักดี ชั้น 6
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210

<u>เอกสารที่ต้องจัดส่ง</u>

- ร่าง ประกาศนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน
- เอกสารอื่นๆ ที่เกี่ยวข้อง (ถ้ามี)

<u>ดาวน์โหลดเอกสารที่เกี่ยวข้อง</u> ได้ที่ www.etcommission.go.th

คู่มือการจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ ฉบับปรับปรุง

การดำเนินการอย่างไรหลังจากแนวนโยบายและแนวปฏิบัติฯ ผ่านความเห็นชอบแล้ว

เมื่อแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน ได้ผ่านความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรียบร้อยแล้ว หน่วยงานจะต้องปฏิบัติตามนโยบายและแนวปฏิบัติตามที่ได้ประกาศไว้ และต้องจัดให้มีการตรวจสอบการปฏิบัติตามนโยบายและแนวปฏิบัติที่ได้กำหนดไว้อย่างสม่ำเสมอ โดยหน่วยงานต้องดำเนินการอย่างน้อย ดังต่อไปนี้

1) ประกาศแจ้งให้ผู้ใช้บริการทราบถึงสิทธิและวิธีการในการคุ้มครองข้อมูลส่วนบุคคลด้วย เช่น ประกาศแจ้งไว้ในเว็บไซต์ของหน่วยงาน เป็นต้น

2) ประกาศแจ้งให้เจ้าหน้าที่ของหน่วยงานที่เกี่ยวข้อง ทราบและปฏิบัติตามประกาศของหน่วยงานที่ได้กำหนดไว้โดยเคร่งครัด

3) หากหน่วยงานมีการปรับปรุงแก้ไขแนวนโยบายและแนวปฏิบัติฯ หน่วยงานจะต้องแจ้งให้ผู้ใช้บริการทราบหรือขอความยินยอมจากผู้ใช้บริการก่อน

4) หน่วยงานต้องดำเนินการตรวจสอบและประเมินความเสี่ยง โดยสม่ำเสมอ

ภาคผนวก

ภาคผนวก

ก. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 และ แก้คำผิด

หน้า ๓๑
เล่ม ๑๒๗ ตอนพิเศษ ๑๒๖ ง ราชกิจจานุเบกษา ๑ พฤศจิกายน ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ

พ.ศ. ๒๕๕๓

ข้อมูลส่วนบุคคลที่มีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ในรูปของข้อมูลอิเล็กทรอนิกส์เป็นสิทธิมนุษยชนขั้นพื้นฐานที่ได้รับความคุ้มครอง ซึ่งปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย และเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมีการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐให้มีมาตรฐานเดียวกัน

อาศัยอำนาจตามความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้น ให้หน่วยงานของรัฐใช้ในการกำหนดนโยบายและข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ดังต่อไปนี้

ข้อ ๑ ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์ จัดทำนโยบายในการคุ้มครองข้อมูลส่วนบุคคลไว้เป็นลายลักษณ์อักษร โดยให้มีสาระสำคัญอย่างน้อย ดังนี้

(๑) การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด

การจัดเก็บรวบรวมข้อมูลส่วนบุคคลให้มีขอบเขตจำกัด และใช้วิธีการที่ชอบด้วยกฎหมายและเป็นธรรม และให้เจ้าของข้อมูลทราบหรือได้รับความยินยอมจากเจ้าของข้อมูลตามแต่กรณี

(๒) คุณภาพของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของหน่วยงานของรัฐตามกฎหมาย

(๓) การระบุวัตถุประสงค์ในการเก็บรวบรวม

ให้บันทึกวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลในขณะที่มีการรวบรวมและจัดเก็บ รวมถึงการนำข้อมูลนั้นไปใช้ในภายหลัง และหากมีการเปลี่ยนแปลงวัตถุประสงค์ของการเก็บรวบรวมข้อมูลให้จัดทำบันทึกแก้ไขเพิ่มเติมไว้เป็นหลักฐาน

(๔) ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้

ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดซึ่งข้อมูลส่วนบุคคลที่ไม่สอดคล้องกับวัตถุประสงค์ของการรวบรวมและจัดเก็บข้อมูล เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูล หรือเป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(๕) การรักษาความมั่นคงปลอดภัย

ให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ทำลาย ใช้ แปลง แก้ไขหรือเปิดเผยข้อมูลโดยมิชอบ

(๖) การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล

ให้มีการเปิดเผยการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคลและจัดให้มีวิธีการที่สามารถตรวจดูความมีอยู่ ลักษณะของข้อมูลส่วนบุคคลวัตถุประสงค์ของการนำข้อมูลไปใช้ ผู้ควบคุมและสถานที่ทำการของผู้ควบคุมข้อมูลส่วนบุคคล

(๗) การมีส่วนร่วมของเจ้าของข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งถึงความมีอยู่ หรือรายละเอียดของข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลเมื่อได้รับคำร้องขอภายในระยะเวลาอันสมควรตามวิธีการในรูปแบบ รวมถึงค่าใช้จ่าย (ถ้ามี) ตามสมควร

ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธที่จะให้คำชี้แจงหรือให้ข้อมูลแก่เจ้าของข้อมูล ผู้สืบสิทธิ์ ทายาท ผู้แทนโดยชอบธรรม หรือผู้พิทักษ์ ตามกฎหมาย

ให้ผู้ควบคุมข้อมูลจัดทำบันทึกคำคัดค้านการจัดเก็บ ความถูกต้อง หรือการกระทำใด ๆ เกี่ยวกับข้อมูลของเจ้าของข้อมูลไว้เป็นหลักฐาน

(๘) ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

ให้ผู้ควบคุมข้อมูลส่วนบุคคลปฏิบัติตามมาตรการที่กำหนดไว้ข้างต้นเพื่อให้การดำเนินงานตามแนวนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเป็นไปตามมาตรฐานของประกาศฉบับนี้

ข้อ ๒ ให้หน่วยงานของรัฐจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการและให้มีรายการอย่างน้อย ดังนี้

(๑) ข้อมูลเบื้องต้น ประกอบด้วย

(ก) ชื่อนโยบายการคุ้มครองข้อมูลส่วนบุคคลว่าเป็นของหน่วยงานใด

(ข) รายละเอียดขอบเขตของการบังคับใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลที่หน่วยงานของรัฐรวบรวม จัดเก็บ หรือการใช้ตามวัตถุประสงค์

(ค) ให้แจ้งการเปลี่ยนแปลงวัตถุประสงค์หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้เจ้าของข้อมูลทราบและขอความยินยอมก่อนทุกครั้งตามวิธีการและภายในกำหนดเวลาที่ประกาศ เช่น การแจ้งล่วงหน้าให้เจ้าของข้อมูลทราบก่อน ๑๕ วัน โดยการส่งทางจดหมายอิเล็กทรอนิกส์หรือประกาศไว้ในหน้าแรกของเว็บไซต์ เว้นแต่กฎหมายจะกำหนดไว้เป็นอย่างอื่น

การขอความยินยอมจากเจ้าของข้อมูลนั้น ให้มีความชัดเจนว่าหน่วยงานของรัฐขอรับความยินยอมเพื่อวัตถุประสงค์ใด

(๒) การเก็บรวบรวม จัดประเภท และการใช้ข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐที่ทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์หรือผ่านรูปแบบของการกรอกข้อความทางกระดาษแล้วนำมาแปลงข้อความเข้าระบบอิเล็กทรอนิกส์หรือจัดเก็บโดยวิธีอื่น ให้แสดงรายละเอียดของการรวบรวมข้อมูลเป็นชนิด ประเภท รวมถึงข้อมูลที่จะไม่จัดเก็บ และข้อมูลที่รวบรวมและจัดเก็บนั้นจะนำไปใช้ตามวัตถุประสงค์ใดโดยลักษณะหรือด้วยวิธีการที่ทำให้เจ้าของข้อมูลได้ทราบ ทั้งนี้ การรวบรวมและจัดเก็บข้อมูลนั้นให้ทำเป็นประกาศหรือแจ้งรายละเอียดให้เจ้าของข้อมูลทราบ

ให้หน่วยงานของรัฐที่จัดบริการผ่านทางเว็บไซต์ แสดงรายละเอียดของการรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานนั้น รวมถึงการใช้ข้อมูลซึ่งอย่างน้อยต้องระบุว่าอยู่ในส่วนใดของเว็บไซต์หรือในเว็บเพจใดที่มีการรวบรวมและจัดเก็บข้อมูล และให้มีรายละเอียดอย่างแจ้งชัดถึงวิธีการในการรวบรวมและจัดเก็บข้อมูล เช่น การจัดเก็บโดยให้มีการลงทะเบียน หรือการกรอกแบบสอบถาม เป็นต้น

ให้หน่วยงานของรัฐรวบรวม จัดเก็บและใช้ข้อมูลส่วนบุคคลจัดทำรายละเอียด ดังต่อไปนี้

(ก) การติดต่อระหว่างหน่วยงานของรัฐ

ให้หน่วยงานของรัฐซึ่งจะติดต่อไปยังผู้ใช้บริการด้วยวิธีการทางอิเล็กทรอนิกส์บอกกล่าวให้ผู้ใช้บริการทราบล่วงหน้า ทั้งนี้ ผู้ใช้บริการอาจแจ้งความประสงค์ให้ติดต่อโดยวิธีการอื่นได้

(ข) การใช้คุกกี้ (Cookies)

ให้หน่วยงานของรัฐระบุบนเว็บไซต์สำหรับการใช้คุกกี้ที่เชื่อมโยงกับข้อมูลส่วนบุคคล ว่าผู้ใช้บริการจะใช้คุกกี้เพื่อวัตถุประสงค์และประโยชน์ใด และให้สิทธิที่จะไม่รับการต่อเชื่อมคุกกี้ได้

(ค) การเก็บข้อมูลสถิติเกี่ยวกับประชากร (Demographic Information)

ให้หน่วยงานของรัฐมีเว็บไซต์สำหรับการเก็บรวบรวมข้อมูลสถิติเกี่ยวกับประชากร เช่น เพศ อายุ อาชีพ ที่สามารถเชื่อมโยงกับข้อมูลระบุตัวบุคคลได้ ระบุถึงวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วย และให้ชี้แจงวัตถุประสงค์ของการใช้ข้อมูลดังกล่าว รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(ง) บันทึกผู้เข้าชมเว็บ (Log Files)

ให้หน่วยงานของรัฐซึ่งจัดบริการเว็บไซต์ที่มีการเก็บบันทึกการเข้าออกโดยอัตโนมัติ เช่น หมายเลขไอพี (IP Address) เว็บไซต์ที่เข้าออกก่อนและหลัง และประเภทของโปรแกรมบราวเซอร์ (Browser) ที่สามารถเชื่อมโยงข้อมูลดังกล่าวกับข้อมูลซึ่งระบุตัวบุคคลได้ ระบุวิธีการรวบรวมและจัดเก็บข้อมูลดังกล่าวไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล และให้ชี้แจงวัตถุประสงค์ของการใช้ รวมถึงการให้บุคคลอื่นร่วมใช้ข้อมูลนั้นด้วย

(จ) ให้หน่วยงานของรัฐระบุข้อมูลที่มีการจัดเก็บผ่านทางเว็บไซต์ว่าเป็นข้อมูลที่ประชาชนมีสิทธิเลือกว่า "จะให้หรือไม่ให้" ก็ได้ และให้หน่วยงานของรัฐจัดเตรียมช่องทางอื่นในการติดต่อสื่อสารสำหรับผู้ใช้บริการที่ไม่ประสงค์จะให้ข้อมูลผ่านทางเว็บไซต์

(๓) การแสดงระบุความเชื่อมโยงให้ข้อมูลส่วนบุคคลกับหน่วยงานหรือองค์กรอื่น

การเก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ของหน่วยงานของรัฐและเว็บไซต์ดังกล่าวที่มีการเชื่อมโยงให้ข้อมูลแก่หน่วยงานหรือองค์กรอื่น ให้หน่วยงานของรัฐแสดงไว้อย่างชัดเจนถึงชื่อผู้เก็บรวบรวมข้อมูลผ่านทางเว็บไซต์ หรือชื่อผู้มีสิทธิในข้อมูลที่ได้มีการเก็บรวบรวม (Data Subject) และชื่อเป็นผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวทั้งหมด รวมถึงประเภทของข้อมูลที่จะใช้ร่วมกับหน่วยงานหรือองค์กรนั้น ๆ ตลอดจนชื่อผู้มีหน้าที่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ผู้ใช้บริการทราบ

ให้หน่วยงานของรัฐแจ้งให้ผู้ใช้บริการทราบและให้ความยินยอมล่วงหน้าก่อนทำการเปลี่ยนแปลงการเชื่อมโยงข้อมูลตามวรรคแรกกับหน่วยงานหรือองค์กรอื่น

(๔) การรวมข้อมูลจากที่มาหลาย ๆ แห่ง

ให้หน่วยงานของรัฐที่ซึ่งได้รับข้อมูลมาจากผู้ใช้บริการเว็บไซต์ และจะนำไปรวมเข้ากับข้อมูลของบุคคลดังกล่าวที่ได้รับจากที่มาแห่งอื่น ระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลถึงเจตนารมณ์การรวมข้อมูลดังกล่าวด้วย เช่น เว็บไซต์ได้รับข้อมูลที่เป็นชื่อและที่อยู่ของการส่งจดหมายอิเล็กทรอนิกส์จากผู้ใช้บริการโดยการกรอกข้อมูลตามแบบสอบถามผ่านทางเว็บไซต์ และจะนำข้อมูลดังกล่าวไปรวมเข้ากับข้อมูลเกี่ยวกับประวัติของผู้ใช้บริการที่ได้รับจากที่มาแห่งอื่น

(๕) การให้บุคคลอื่นใช้หรือการเปิดเผยข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลด้วยว่ามีบุคคลอื่นที่จะเข้าถึงหรือใช้ข้อมูลที่หน่วยงานนั้นได้เก็บรวบรวมมาผ่านทางเว็บไซต์ด้วย และให้ระบุไว้ด้วยว่าการให้เข้าถึง ใช้ หรือเปิดเผยข้อมูลดังกล่าวสอดคล้องกับข้อกำหนดตามกฎหมายของหน่วยงานของรัฐที่ดำเนินการดังกล่าว

(๖) การรวบรวม จัดเก็บ ใช้ และการเปิดเผยข้อมูลเกี่ยวกับผู้ใช้บริการ

ให้หน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่ประสงค์จะนำไปดำเนินการอื่นนอกเหนือไปจากวัตถุประสงค์ของการรวบรวมข้อมูลส่วนบุคคลตามที่ได้ระบุไว้ เช่น การรวบรวม จัดเก็บ ใช้ และเปิดเผยข้อมูลที่ไม่จำเป็น หรือการเปิดเผยข้อมูลส่วนบุคคลต่อบุคคลอื่น ระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลถึงสิทธิของผู้ใช้บริการที่จะเลือกว่า จะให้หน่วยงานของรัฐรวบรวม จัดเก็บหรือไม่ให้จัดเก็บ ใช้หรือไม่ให้ใช้ และเปิดเผยหรือไม่เปิดเผยข้อมูลดังกล่าว

การให้ผู้ใช้บริการใช้สิทธิเลือกตามวรรคแรกให้รวมถึงการให้สิทธิเลือกแบบที่หน่วยงานของรัฐจะต้องขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคลนั้นก่อน และการให้สิทธิเลือกแบบที่ให้สิทธิแก่ผู้ใช้บริการในการปฏิเสธไม่ให้มีการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวข้างต้นแล้วเท่านั้น ทั้งนี้ การให้สิทธิเลือกต้องกระทำให้สมบูรณ์ก่อนที่เว็บไซต์จะทำการติดต่อกับผู้ใช้บริการในครั้งแรก และหากเป็นการใช้สิทธิเลือกแบบห้ามไม่ให้มีการใช้ข้อมูลส่วนบุคคลแตกต่างไปจากวัตถุประสงค์เดิม หน่วยงานเจ้าของเว็บไซต์ต้องระบุไว้ในนโยบายการคุ้มครองข้อมูลส่วนบุคคลให้ผู้ใช้บริการได้รับทราบถึงวิธีการของการส่งการติดต่อครั้งที่สองของเว็บไซต์ด้วย

(๗) การเข้าถึง การแก้ไขให้ถูกต้อง และการปรับปรุงให้เป็นปัจจุบัน

ให้หน่วยงานของรัฐกำหนดวิธีการที่ผู้ใช้บริการเว็บไซต์สามารถเข้าถึงและแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลเกี่ยวกับตนเองที่หน่วยงานของรัฐรวบรวมและจัดเก็บไว้ในเว็บไซต์ให้ถูกต้อง

(๘) การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางจัดให้มีวิธีการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลที่รวบรวมและจัดเก็บไว้ให้เหมาะสมกับการรักษาความลับของข้อมูลส่วนบุคคล เพื่อป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวโดยมิชอบ รวมถึงการป้องกันการกระทำใดที่จะมีผลทำให้ข้อมูลไม่อยู่ในสภาพพร้อมใช้งาน ซึ่งหน่วยงานของรัฐพึงดำเนินการ ดังนี้

(ก) สร้างเสริมความสำนึกในการรับผิดชอบด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่บุคลากร พนักงาน หรือลูกจ้างของหน่วยงานด้วยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ จัดสัมมนา หรือฝึกอบรมในเรื่องดังกล่าวให้แก่บุคลากรในองค์กรเป็นประจำ

(ข) กำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของบุคลากร พนักงาน หรือลูกจ้างของตนในแต่ละลำดับชั้นให้ชัดเจน และให้มีการบันทึกรวมทั้งการทำสำรองข้อมูลของการเข้าถึงหรือการเข้าใช้งานข้อมูลส่วนบุคคลไว้ในระยะเวลาที่เหมาะสมหรือตามระยะเวลาที่กฎหมายกำหนด

(ค) ตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บไซต์หรือของระบบสารสนเทศทั้งหมดอย่างน้อยปีละ ๑ ครั้ง

(ง) กำหนดให้มีการใช้มาตรการที่เหมาะสมและเป็นการเฉพาะสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่มีความสำคัญยิ่งหรือเป็นข้อมูลที่อาจกระทบต่อความรู้สึก ความเชื่อ ความสงบเรียบร้อย และศีลธรรมอันดีของประชาชนซึ่งเป็นผู้ใช้บริการของหน่วยงานของรัฐ หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน เช่น หมายเลขบัตรเดบิต หรือบัตรเครดิต หมายเลขประจำตัวประชาชน หรือหมายเลขประจำตัวบุคคล เชื้อชาติ ศาสนา ความเชื่อ ความคิดเห็นทางการเมือง สุขภาพ พฤติกรรมทางเพศ เป็นต้น

(จ) ควรจัดให้มีมาตรการที่รอบคอบในการรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคลของบุคคลซึ่งอายุไม่เกินสิบแปดปีโดยใช้วิธีการโดยเฉพาะและเหมาะสม

(๙) การติดต่อกับเว็บไซต์

เว็บไซต์ซึ่งให้ข้อมูลแก่ผู้ใช้บริการในการติดต่อกับหน่วยงานของรัฐ ต้องจัดให้มีทั้งข้อมูลติดต่อไปยังสถานที่ทำการงานปกติและข้อมูลติดต่อผ่านทางออนไลน์ด้วย ข้อมูลติดต่อที่หน่วยงานของรัฐควรจะระบุเอาไว้ อย่างน้อยต้องประกอบด้วยข้อมูลดังต่อไปนี้

(ก) ชื่อและที่อยู่

(ข) หมายเลขโทรศัพท์

(ค) หมายเลขโทรสาร

(ง) ที่อยู่จดหมายอิเล็กทรอนิกส์

ข้อ ๓ ให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายใต้หลักการตามข้อ ๑ และข้อ ๒ สำหรับหน่วยงานของรัฐที่ได้รับทรัสต์มาร์คจากหน่วยงานหรือองค์กรอื่นที่ทำหน้าที่ออกทรัสต์มาร์ค (Trust Mark) ให้หน่วยงานของรัฐนั้นแสดงนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการรับรองจากหน่วยงานหรือองค์กรที่ออกหรือรับรองทรัสต์มาร์คดังกล่าวต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย

ทรัสต์มาร์ค (Trust Mark) ตามความในวรรคแรกหมายถึง เครื่องหมายที่รับรองว่าหน่วยงานดังกล่าวมีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลของประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งออกโดยหน่วยงานหรือองค์กรที่จัดตั้งโดยชอบด้วยกฎหมายเพื่อทำหน้าที่ในการตรวจสอบและรับรองการออกทรัสต์มาร์คให้กับผู้ขอรับการรับรอง

ข้อ ๔ ให้หน่วยงานของรัฐกำหนดชื่อเรียกนโยบายการคุ้มครองข้อมูลส่วนบุคคลไว้ให้ชัดเจน และในกรณีที่มีการปรับปรุงนโยบาย ให้ระบุวัน เวลา และปี ซึ่งจะมีการปรับปรุงหรือเปลี่ยนแปลงนโยบายดังกล่าวไว้ด้วย

ข้อ ๕ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๕๓
จุติ ไกรฤกษ์
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

แก้คำผิด

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ซึ่งประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป

เล่ม ๑๒๗ ตอนพิเศษ ๑๒๖ ง วันที่ ๑ พฤศจิกายน ๒๕๕๓

หน้า ๓๖ บรรทัดที่ ๒ คำว่า "ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางจัดให้มีวิธีการรักษาความมั่นคง" ให้แก้เป็น "ให้หน่วยงานของรัฐซึ่งรวบรวมข้อมูลส่วนบุคคลผ่านทางเว็บไซต์จัดให้มีวิธีการรักษาความมั่นคง"

ภาคผนวก

ข. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. 2549

พระราชกฤษฎีกา

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙
เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

อาศัยอำนาจตามความในมาตรา ๑๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๔๙ และมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า "พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙"

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มีระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ในลักษณะ ดังต่อไปนี้

(๑) เอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลังและยังคงความครบถ้วนของข้อความในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(๒) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณาของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ไว้ด้วยก็ได้ เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๓) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะหรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

(๔) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใดเพื่อเป็นหลักฐานว่าได้มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่งแล้ว

มาตรา ๔ นอกจากที่บัญญัติไว้ในมาตรา ๓ ในกรณีที่หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ ระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๑) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความที่ผิดหลงอันเห็นได้ชัดว่าเกิดจากความไม่รู้หรือความเลินเล่อของผู้ยื่นคำขอ หรือการขอข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณี ในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

(๒) ในกรณีมีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่าคู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

มาตรา ๙ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

มาตรา ๑๐ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
อาคารรัฐประศาสนภักดี ชั้น 6
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02-1416-991
โทรสาร 02-1438-036
www.etcommission.go.th

Electronic Transactions Commission

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
อาคารรัฐประศาสนภักดี ชั้น 6
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 02-1416-991
โทรสาร 02-1438-036
www.etcommission.go.th

Electronic Transactions Commission