แนวทางการผยแพร่ ข้อมูล PAPD

คำนำ

เป็นสวนหนึ่งของโครงการศึกษาและวางหลักเกณฑ์และแนวทางการคมครองข้อมูลส่วนบุคคลในโรงพยาบาลบ่อทอง ฉบับนี้ เป็นส่วนหนึ่งของโครงการศึกษาและวางหลักเกณฑ์และแนวทางการควบคุมข้อมูลส่วนบุคคล ที่จัดทำโดยภาคเอกชนที่เข้าร่วมในการศึกษาและวางหลักเกณฑ์และแนวทางการบริหารจัดการข้อมูลส่วนบุคคลของราชการ สำนักงานปลัดสำนักนายกรัฐมนตรี เมื่อปี พ.ศ. 2550

สาระในเอกสารหลักเกณฑ์และแนวปฏิบัติในการบริหารจัดการข้อมูลส่วนบุคคลในโรงพยาบาลบ่อทอง ฉบับนี้ เป็นการสรุปหลักเกณฑ์และแนวทางปฏิบัติที่เป็นมาตรฐานกลางเพื่อให้ยอมรับและนำเสนอให้โรงพยาบาลได้นำไปพิจารณา และถอดประกายตามความเหมาะสมหรือสอดคล้องกับบริบทในการประกอบธุรกิจของตน โดยเฉพาะในส่วนที่เกี่ยวข้องกับการใช้ข้อมูลส่วนบุคคลของ ผู้รับบริการ หรือ ผู้ใช้บริการให้เป็นไปตามมาตรฐานสากลและเป็นไปตามกฎหมาย คำคมครองข้อมูลส่วนบุคคลในขณะนี้ การอ้างถึงบทบัญญัติในพระราชบัญญัติคมครองข้อมูลส่วนบุคคลพ.ศ. 2562 ในเอกสาร ฉบับนี้ ผู้เขียนเห็นว่าเป็นการเพิ่มเติมสาระให้ครบถ้วนและสอดรับกับสาระของพระราชบัญญัติ ดังนั้น ผู้เขียนจึงไม่ได้ทำการปรับปรุงถอยคำต่าง ๆ ในเอกสารฉบับนี้ เพื่อให้เป็นข้อมูลส่วนบุคคลพ.ศ. 2562 บัญญัติไว้ ซึ่งต่อไปหากมีเวลาผู้เขียนก็จะปรับปรุงสาระและถอยคำให้เป็นไปตามที่บัญญัติไว้ในพระราชบัญญัติคมครองข้อมูลส่วนบุคคลพ.ศ. 2562 เพื่อผู้อ่านจะได้เข้าใจถึงสาระของกฎหมายคมครองข้อมูลส่วนบุคคลตามโครงสร้างของหลักเกณฑ์และแนวปฏิบัติที่นำเสนอโดยเอกสารฉบับนี้ต่อไปครับ

หลักเกณฑ์และแนวทางปฏิบัติในการบริหารจัดการข้อมูลส่วนบุคคลในโรงพยาบาลบ่อทอง

ในปัจจุบัน, องค์กรธุรกิจใช้เทคโนโลยีสารสนเทศเป็นส่วนสำคัญในการเพิ่มประสิทธิภาพในการบริหารจัดการองค์กรและทำให้องค์กรมีภาพลักษณ์ที่ยอมรับในสายงานที่ควรจะรักษาความลับของข้อมูลที่เกี่ยวกับลูกค้าหรือผู้ใช้บริการ ข้อมูลส่วนบุคคลบางส่วนที่ถูกเก็บรักษาอยู่ในความครอบครองหรือควบคุมขององค์กรมีการนำมาใช้เพื่อวัตถุประสงค์ทางธุรกิจหรือการพาณิชย์ โดยบุคคลที่เป็นเจ้าของข้อมูลหรือผู้ที่เกี่ยวข้องกับข้อมูลนั้นอาจไม่ได้เห็นด้วย และบางครั้งอาจก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลนั้น ในกรณีขององค์กรธุรกิจขนาดใหญ่หรือองค์กรธุรกิจที่มีการติดต่อทางธุรกิจกับองค์กรธุรกิจในต่างประเทศ, อาจจำเป็นต้องส่งหรือโอนข้อมูลที่เกี่ยวกับลูกค้าหรือผู้ใช้บริการระหว่างกัน แต่การดำเนินการดังกล่าวจะต้องเผชิญกับอุปสรรคสำคัญเนื่องจากในหลายประเทศมีกฎหมายที่กำกับการคุ้มครองข้อมูลส่วนบุคคล ที่บังคับใช้แล้ว ทำให้การเจรจาทางธุรกิจมีปัญหาเนื่องจากองค์กรธุรกิจต้องส่งหรือโอนข้อมูลที่เกี่ยวข้องกับบุคคลเช่นข้อมูลลูกค้ามายังประเทศไทย ข้อมูลดังกล่าวอาจได้รับการคุ้มครองไม่เพียงให้ผู้อื่นรู้หรือนำไปใช้โดยมิชอบ หรือผิดจากข้อตกลงทางธุรกิจหรือไม่ แม้แต่ในกรณีที่องค์กรธุรกิจในประเทศไทยเองก็มีปัญหาว่าแต่ละองค์กรมีมาตรฐานต่างกันในการจัดเก็บข้อมูลส่วนบุคคลและในการนำข้อมูลไปใช้งาน บางองค์กรมีการควบคุมและควบคุมข้อมูลลูกค้าอย่างเข้มงวด แต่บางองค์กรไม่ให้ความสนใจในการรักษาความลับของข้อมูลส่วนบุคคลดังกล่าว การมีความคุ้มครองข้อมูลส่วนบุคคลในภาคเอกชนนั้นขาดความเอกภาพและขาดข้อรับประกันที่ชัดเจน จากสถานการณ์ที่เป็นปัญหาและเป็นอุปสรรคต่อการคุ้มครองข้อมูลส่วนบุคคลนี้ เราจึงมีความจำเป็นที่จะต้องกำหนดหลักเกณฑ์ที่เป็นมาตรฐานหรือแนวทางปฏิบัติที่ชัดเจนเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในองค์กรภาคเอกชน โดยใช้มาตรฐานระหว่างประเทศเพื่อให้เป็นที่ยอมรับของนานาประเทศและทำให้การเจรจาทางธุรกิจและการติดต่อสื่อสารสื่อสารด้วยเทคโนโลยีสารสนเทศเป็นไปอย่างสะดวกสรรค์ สมควรสำหรับทุกฝ่าย และได้รับความมั่นใจว่าข้อมูลส่วนบุคคลจะได้รับการคุ้มครองจากคู่ค้าหรือคู่สัญญาทุกฝ่าย

สำหรับหลักเกณฑ์และแนวทางการบริหารจัดการข้อมูลส่วนบุคคลในโรงพยาบาลบ่อทอง มี 3 แนวทางหลักคือ

1.หลักเกณฑ์และแนวทางปฏิบัติในการบริหารจัดการข้อมูลส่วนบุคคลสำหรับผู้บริหารองค์กร เนื่องจากในการดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลที่ดีและมีประสิทธิภาพจำเป็นต้องมีแนวปฏิบัติที่เป็นมาตรฐานสากลในระดับประเทศและระหว่างประเทศ

2.หลักเกณฑ์และแนวทางการดำเนินการในเชิงนโยบายที่ต้องประกาศให้สาธารณชนได้ทราบ ซึ่งจะเน้นหลักเกณฑ์ที่เป็นมาตรฐานขั้นต่ำที่องค์กรธุรกิจควรเปิดเผยสู่สาธารณชนเพื่อสร้างความมั่นใจแก่ลูกค้าหรือผู้ใช้บริการในระบบการจัดเก็บข้อมูลส่วนบุคคลขององค์กรนั้นๆ

3.หลักเกณฑ์และแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

3.1 การเก็บรวบรวม รักษาและประมวลผลข้อมูล:องค์กรธุรกิจหรือหน่วยงานเอกชนที่เก็บข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคลควรเก็บข้อมูลด้วยความเป็นไปตามความจำเป็นและตามวัตถุประสงค์ตามที่กำหนดไว้ให้ถูกต้องตามกฎหมายขององค์กรธุรกิจหรือหน่วยงานเอกชนนั้น ๆ และเท่าที่จำเป็นในการดำเนินการตามอำนาจหน้าที่หรือวัตถุประสงค์ที่ระบุให้ดำเนินการตามกฎหมายขององค์กรธุรกิจหรือหน่วยงานเอกชนนั้น ๆองค์กรธุรกิจหรือหน่วยงานเอกชนที่เก็บข้อมูลควรรักษาข้อมูลตามกฎหมายและเป็นไปตามอำนาจที่เป็นหน้าที่ และต้องรักษาข้อมูลด้วยวิธีการที่เป็นไปตามกฎหมายและเป็นธรรมต่อเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล โดยที่วิธีการดังกล่าวต้องไม่เป็นวิธีการที่เขียนลักษณะคุกคามหรือรบกวนสิทธิของเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล. ในขณะหรือก่อนที่องค์กรธุรกิจหรือหน่วยงานเอกชนจะทำการเก็บรวบรวมข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคลจากเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล องค์กรธุรกิจหรือโรงพยาบาลต้องดำเนินการเพื่อให้เกิดความมั่นใจว่าเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลได้ตระหนักและรับทราบถึง

(1) ชื่อ, สถานที่ทำการ, และสถานภาพขององค์กรธุรกิจหรือหน่วยงานที่จัดเก็บข้อมูล.
(2) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคล.
(3) ประเภทข้อมูลส่วนบุคคลที่จะเก็บรวบรวม.
(4) วิธีการเก็บรวบรวมข้อมูลส่วนบุคคล.
(5) ระยะเวลาในการรักษาข้อมูลส่วนบุคคล.
(6) เงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคล.
(7) บุคคล, องค์กรธุรกิจหรือหน่วยงานเอกชนที่ข้อมูลจะถูกเปิดเผยต่อ.
(8) กฎหมายที่อนุญาตให้เก็บข้อมูลได้เป็นการเฉพาะ (ถ้ามี).
(9) ผลกระทบที่อาจเกิดขึ้น (ถ้ามี) กับบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล หากบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลไม่ได้ให้ข้อมูลทั้งหมดหรือบางส่วน
หมายเหตุ: นอกจาก (1) - (9) ดังกล่าวข้างต้น พระราชบัญญัติคุมครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 23 (5) และ (6) ยังกำหนดรายละเอียดของข้อมูลและสิทธิของเจ้าของข้อมูลที่องค์กร ธุรกิจหรือหน่วยงานเอกชนจะต้องแจ้งให้ทราบเพิ่มเติมดังนี้:
(5) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูลสถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคลด้วย.
(6) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 73 วรรคหนึ่ง
7 โรงพยาบาลบ่อทองจัดเก็บข้อมูลต้องจัดเก็บข้อมูลจากบุคคลผู้เป็น เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลโดยตรงในกรณีโรงพยาบาลบ่อทองจัดเก็บข้อมูลจากบุคคลที่สามหรือจากแหล่ง อื่นที่ไม่ใช้จากเจ้าของข้อมูลโดยตรงจะต้องเป็นข้อมูลที่มาจากแหล่งที่เชื่อถือได้ โรงพยาบาลบ่อทอง ดังกล่าวต้องแจ้งให้เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลทราบ และต้องขอความยินยอม จากเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลก่อนจัดเก็บ
หมายเหตุ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 25 ได้บัญญัติห้าม มิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช้จากเจ้าของข้อมูลส่วนบุคคลโดยตรง เว้นแต่
(1) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้เจ้าของข้อมูลส่วนบุคคลทราบ โดยไม่ชักชา แต่ต้องไม่เกินสามสิบวันนับแต่วันที่เก็บรวบรวมและได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล
(2) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26
โรงพยาบาลจัดเก็บข้อมูลต้องไม่จัดเก็บรวบรวมข้อมูลที่ เกี่ยวข้องกับข้อมูลที่มีลักษณะอื่นไหวต่อความรู้สึกของบุคคล เช่น ข้อมูลที่แสดงให้เห็นถึง ชาติพันธุ์ ลัทธิความเชื่อ ความคิดเห็นทางการเมือง ความเชื่อทางศาสนา ความเชื่อส่วนบุคคล รายละเอียดเกี่ยวกับ สุขภาพ ทัศนะคติเกี่ยวกับเพศ ประวัติอาชญากรรม และอื่นๆ ตามที่กฎหมายกำหนด เว้นแต่
(1) บุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลได้ให้ความยินยอมเป็นหนังสือ
(2) เป็นการเก็บข้อมูลตามกฎหมายหรือได้รับการอนุญาตโดยผลของกฎหมาย หรือ
(3) เป็นการเก็บรวบรวมข้อมูลที่จำเป็นสำหรับการป้องกันภัยอันตรายที่กำลังจะเกิดขึ้นต่อชีวิต ร่างกายหรือสุขภาพของเจ้าของข้อมูล หรือการรักษาพยาบาลเจ้าของข้อมูล และเจ้าของ ข้อมูลไม่สามารถที่จะให้ความยินยอมได้ หรือ
(4) การเก็บรวบรวมนั้นเป็นการดำเนินการที่จำเป็นต่อการต่อสู้คดีเสียหายจากองครึจรญิธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล หรือ

(5) การเก็บรวบรวมข้อมูลนั้นจำเป็นสำหรับวัตถุประสงค์เชิงป้องกันในทางการ แพทย์ หรือการตรวจสอบทางการแพทย์ หรือ
(6) เป็นการเก็บรวบรวมตามบทบัญญัติแห่งกฎหมาย หรือกฎที่ออกโดยองครึกร วิชาชีพซึ่งองครึจรญิธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลมีหน้าที่ที่จะต้องรักษาความลับตามจรรยาบรรณ แห่งวิชาชีพนั้นๆ
(7) เป็นการเก็บรวบรวมเพื่อการสืบสวน สอบสวน หรือการตรวจสอบการกระทำ หรือความประพฤติ และมีเหตุที่น่าเชื่อได้ว่าการเก็บข้อมูลส่วนบุคคลโดยขอคำยินยอมจากเจ้าของข้อมูล ก่อนจะมีผลกระทบต่อความมีอยู่หรือความถูกต้องของข้อมูล
(8) เป็นการเก็บรวบรวมข้อมูลส่วนบุคคลซึ่งได้จากการดูหรือสังเกตการณ์ การแสดง กีฬา หรือกิจกรรมอื่นๆ ที่คล้ายคลึงกัน เมื่อบุคคลที่ถูกเก็บรวบรวมข้อมูลนั้นได้ปรากฏตัว หรือเข้าร่วมในกิจกรรมนั้นด้วยความสมัครใจ และกิจกรรมนั้นเป็นกิจกรรมที่เปิดเผยต่อสาธารณชน

การเก็บรวบรวมนั้นเป็นสิ่งจำเป็นเพื่อใช้ประกอบการพิจารณาความเหมาะสมของบุคคลในการได้รับรางวัลเกียรติยศหรือผลประโยชน์ในลักษณะที่คล้ายคลึงกัน

การเก็บรวบรวมข้อมูลโดยหน่วยงานด้านข้อมูลเครดิต ซึ่งมีหน้าที่เก็บรวบรวมข้อมูลของบุคคลเพื่อทำรายงานข้อมูลเครดิต และเจ้าของข้อมูลส่วนบุคคลได้ให้ความยินยอมในครั้งแรกที่มีการจัดเก็บข้อมูลว่าให้สามารถเก็บรวบรวมและเปิดเผยเพื่อการจัดทำข้อมูลเครดิตดังกล่าวได้

หมายเหตุ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 ห้ามไม่ให้เก็บรวบรวมข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผาพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูล สหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด โดยไม่ได้รับความยินยอมโดยชัดเจนจากเจ้าของข้อมูลส่วนบุคคล นอกจาก
(1) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าด้วยเหตุใดก็ตาม
(2) เป็นการดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพ แรงงานให้แกสมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น
(3) เป็นข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมชัดเจนของเจ้าของข้อมูลส่วนบุคคล
(4) เป็นการจำเป็นเพื่อการกฎหมายเพื่อทำสิทธิรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิรียกร้องตามกฎหมาย หรือการยกร้องต่อสิทธิรียกร้องตามกฎหมาย
(5) เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ
(ก) เวชศาสตร์ เพื่อป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพหรือระบบและการให้บริการด้านสังคมสงเคราะห์ โดยไม่ใช้การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นเป็นความลับตามกฎหมาย ต้องปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์
(ข) ประโยชน์สาธารณะในด้านการสาธารณสุข เช่น การป้องกันโรคติดต่อ อันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์หรือเครื่องมือทางการแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

(ค) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการ เกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการ คุ้มครองทางสังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล

ข้อมูลชีวภาพ ตามวรรคหนึ่งหมายถึงข้อมูลส่วนบุคคลที่เกิดขึ้นจากการใช้เทคนิคหรือเทคโนโลยีที่เกี่ยวข้องกับการนำลักษณะเดิมพลังงานทางกายภาพหรือพฤติกรรมของบุคคลมาใช้ให้สามารถยืนยันตัวตนของบุคคลนั้นได้ว่าไม่เหมือนกับบุคคลอื่น ๆ เช่นข้อมูลภาพจำลองใบหน้า ข้อมูลจำลองมานตา หรือข้อมูลจำลองลายนิ้วมือ

การเก็บรักษาข้อมูลส่วนบุคคล ต้องมีมาตรการที่เหมาะสมเพื่อคุ้มครองความมั่นคงและความปลอดภัยของข้อมูลส่วนบุคคล โดยเป็นไปตามวัตถุประสงค์ของการเก็บรักษาและต้องป้องกันการสูญหาย การเข้าถึง การใช้งาน การเปลี่ยนแปลง การแก้ไข หรือการเปิดเผยข้อมูลส่วนบุคคลโดยไม่มีอำนาจหรือไม่มีความยินยอม นอกจากนี้, เจ้าของข้อมูลส่วนบุคคลต้องได้รับความยินยอมก่อนจากเจ้าของข้อมูลก่อนที่จะทำการเก็บรักษาข้อมูลนอกเหนือจากวัตถุประสงค์เดิมของการเก็บรักษา ยกเว้นในกรณีที่มีหลักความยินยอมหรือด้วยอำนาจตามกฎหมาย.

การใช้และเปิดเผยข้อมูล จากส่วนที่ได้รับความยินยอมของเจ้าของข้อมูลต้องใช้หรือเปิดเผยข้อมูลเพียงเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บข้อมูล โดยในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนต้องใช้หรือเปิดเผยข้อมูลนอกเหนือจากวัตถุประสงค์เดิมการแจ้งเจ้าของข้อมูลความเหตุผลที่ดำเนินการและรับความยินยอมเป็นลายลัดจากเจ้าของข้อมูลก่อน ยกเว้นในกรณีที่วัตถุประสงค์ในการใช้หรือเปิดเผยข้อมูลเป็นวัตถุประสงค์ที่เกี่ยวเนื่องหรือเกี่ยวข้องกับวัตถุประสงค์เดิมของการเก็บข้อมูล และสามารถคาดการณ์ได้อย่างมีเหตุมีผลว่าองค์กรธุรกิจหรือหน่วยงานเอกชนจะใช้หรือเปิดเผยข้อมูลนอกเหนือจากวัตถุประสงค์เดิมที่เกี่ยวเนื่องกับวัตถุประสงค์ที่จัดเก็บข้อมูลเดิม.

การเก็บรวบรวมข้อมูล ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์เท่าที่จำเป็นและต้องมีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนด.ทั้งนี้ควรจะคำนึงถึงความควบคุมและความปลอดภัยของข้อมูลส่วนบุคคลอย่างสมบูรณ์เพื่อป้องกันไม่ให้ข้อมูลนั้นสูญหาย, ถูกเข้าถึง, ใช้งาน, แก้ไข, หรือเปิดเผยโดยไม่มีอำนาจหรือความยินยอม ตลอดจนมีการควบคุมข้อมูลส่วนบุคคลตามหลักการปกป้องสิทธิและความเป็นส่วนตัวของบุคคลตามกฎหมาย.

1.2 การใช้และเปิดเผยข้อมูล:องค์กรธุรกิจหรือหน่วยงานเอกชนที่เก็บข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคลต้องใช้หรือเปิดเผยข้อมูลเพียงเท่าที่จำเป็นตามวัตถุประสงค์ของการเก็บข้อมูล. ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนต้องใช้หรือเปิดเผยข้อมูลนอกเหนือจากวัตถุประสงค์ของการจัดเก็บเดิม, องค์กรธุรกิจหรือหน่วยงานเอกชนต้องแจ้งเจ้าของข้อมูลให้ทราบโดยแสดงเหตุผลในการดำเนินการดังกล่าว และต้องได้รับความยินยอมเป็นลายลัดจากเจ้าของข้อมูลก่อน เว้นแต่

(1) วัตถุประสงค์ในการใช้หรือเปิดเผยเป็นวัตถุประสงค์ที่เกี่ยวเนื่องหรือมีความสัมพันธ์กับวัตถุประสงค์ของการจัดเก็บเดิม และบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลสามารถที่จะคาดการณ์ได้อย่างมีเหตุมีผลว่าองค์กรธุรกิจหรือหน่วยงานเอกชนจะใช้หรือเปิดเผยข้อมูลตามวัตถุประสงค์อื่นที่เกี่ยวเนื่องกับวัตถุประสงค์ที่จัดเก็บข้อมูลเดิม.

(2) ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนได้ใช้ข้อมูลเพื่อประโยชน์เกี่ยวกับการตลาดแบบตรง, ในทางปฏิบัติมีการยากที่องค์กรธุรกิจหรือหน่วยงานเอกชนจะขอคำยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลก่อนการใช้หรือเปิดเผยข้อมูลนั้น. อย่างไรก็ตาม, ในทันทีที่ผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลร้องขอปฏิเสธที่จะรับการติดต่อสำหรับการตลาดแบบตรงอีกต่อไป, องค์กรธุรกิจหรือหน่วยงานเอกชนจะต้องยุติการใช้หรือเปิดเผยข้อมูลดังกล่าว.

(3) องค์กรธุรกิจหรือหน่วยงานเอกชนนั้นมีเหตุผลที่สมควรเชื่อได้ว่าการใช้หรือเปิดเผยข้อมูลเป็นกรณีที่จำเป็นต่อการประโยชน์ของบุคคลที่เกี่ยวข้อง หรืออันเป็นภยันตรายต่อชีวิต, ร่างกาย, หรืออนามัยของบุคคลและภยันตรายนั้นเป็นภยันตรายที่ใกล้จะถึง หรือเพื่อการรักษาพยาบาลของเจ้าของข้อมูล ซึ่งในขณะนั้น เจ้าของข้อมูลไม่อยู่ในสภาวะตามกฎหมายที่จะให้คำยินยอมได้.
(4) องค์กรธุรกิจหรือหน่วยงานเอกชนนั้นมีเหตุผลที่สมควรเชื่อได้ว่ามีการกระทำที่ไม่ชอบด้วยกฎหมายหรือมีการกระทำซึ่งกำลังเกิดขึ้นและเป็นการกระทำที่เกี่ยวข้องกับการกระทำที่ไม่ชอบด้วยกฎหมาย, การใช้หรือเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลเกี่ยวกับบุคคลดังกล่าวเป็นกรณีจำเป็นสำหรับการสืบสวนหรือการฟ้องคดี, หรือการใช้หรือเปิดเผยดังกล่าวเป็นส่วนหนึ่งของการจัดทำรายงานที่จำเป็นต้องจัดทำขึ้นเพื่อประโยชน์ของบุคคลที่เกี่ยวข้องหรือเจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้องกับเรื่องดังกล่าว.
(5) เป็นการใช้หรือเปิดเผยตามที่กฎหมายกำหนด, หรือเป็นการใช้หรือเปิดเผยต่อศาลหรือเจ้าหน้าที่ของรัฐหรือหน่วยงานของรัฐที่มีอำนาจตามกฎหมายที่ขอข้อมูลส่วนบุคคลดังกล่าว.
(6) เป็นการใช้หรือเปิดเผยอย่างสมเหตุสมผลและจำเป็นต่อการบังคับใช้กฎหมาย, ที่มีโทษทางอาญา หรือกฎหมายที่เกี่ยวข้องกับการจัดเก็บภาษีอากรของรัฐ.
(7) เป็นการใช้หรือเปิดเผยเพื่อประโยชน์ในการศึกษาวิจัยโดยต้องไม่ระบุชื่อหรือมีส่วนใดที่ทำให้รู้ว่าเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับบุคคลใด.
(8) เป็นการใช้หรือเปิดเผยเพื่อประโยชน์ในการศึกษาวิจัยโดยต้องไม่ระบุชื่อหรือมีส่วนใดที่ทำให้รู้ว่าเป็นข้อมูลส่วนบุคคลที่เกี่ยวกับบุคคลใด.
หากองค์กรธุรกิจหรือหน่วยงานเอกชนต้องใช้หรือเปิดเผยข้อมูลก่อนได้รับความยินยอม:หากองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะต้องใช้หรือเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับความยินยอมจากเจ้าของข้อมูลด้วยเหตุผลดังกล่าวในข้อ 1), องค์กรธุรกิจหรือหน่วยงานเอกชนต้องใช้หรือเปิดเผยข้อมูลเฉพาะที่เกี่ยวข้องกับเจ้าของข้อมูลนั้นโดยตรง, ที่เท่าที่จำเป็น, และต้องทำเท่าที่จำเป็น และเมื่อเปิดเผยข้อมูลใดแล้วต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า. ส่วนผู้ซึ่งได้รับข้อมูลส่วนบุคคลดังกล่าวต้องไม่ใช้หรือเปิดเผยข้อมูลนั้นเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งความประสงค์ไว้แล้ว. องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องจัดทำบันทึกการใช้หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวเพื่อประโยชน์ในการตรวจสอบของเจ้าของข้อมูลและพนักงานเจ้าหน้าที่ที่เกี่ยวข้อง.
การปกปิดข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้อง:ในกรณีที่เอกสารฉบับหนึ่งฉบับมีข้อมูลเกี่ยวกับบุคคลของบุคคลตั้งแต่สองคนขึ้นไป, องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอนุญาตให้เข้าถึงข้อมูลดังกล่าวได้ แต่จะปกปิดข้อมูลของบุคคลอื่นที่ไม่เกี่ยวข้องกับบุคคลผู้ขอข้อมูล, โดยการปกปิดชื่อ, นามสกุล, เลขประจำตัวประชาชน, หรือ สัญลักษณ์อื่นที่สามารถระบุตัวบุคคลอื่นได้

คุณภาพของข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลหรือข้อมูลเกี่ยวกับบุคคลที่จัดเก็บนั้นมีคุณภาพที่ถูกต้อง ครบถ้วน สมบูรณ์ และเป็นปัจจุบัน ตรงกับวัตถุประสงค์ของการจัดเก็บข้อมูล และไม่นอกเหนือจากวัตถุประสงค์ที่กำหนดไว้ด้วยเช่นกันควรระบุช่วงเวลาในการเก็บรักษาข้อมูล

1.4 การรักษาความปลอดภัยของข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจจัดเก็บและรักษาข้อมูลตามระยะเวลาที่กำหนดหรือเพียงเท่าที่จำเป็นตามวัตถุประสงค์ที่ได้แจ้งต่อเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล โดยยกเว้นกรณีที่บุคคลที่เกี่ยวข้องกับข้อมูลหรือเจ้าของข้อมูลให้ความยินยอมอย่างชัดเจนว่าเก็บรักษาข้อมูลนานเกินกว่าระยะเวลาที่กำหนดไว้ใน

นโยบาย หรือเว้นแต่จะมีเหตุจำเป็นในการเก็บรักษาข้อมูลเกินระยะเวลาที่กำหนด และองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะลบหรือทำลายข้อมูลดังกล่าวเมื่อระยะเวลาที่กำหนดหมดลงหรือเมื่อไม่มีความจำเป็นในการเก็บรักษาข้อมูลอีกต่อไป ทั้งนี้ องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการด้วยความระมัดระวังและรอบคอบเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคลไม่สามารถระบุตัวตนได้อย่างถาวร องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยไม่มีอำนาจหรือไม่ได้รับอนุญาต หรือป้องกันไม่ให้มีการแก้ไขหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงต้องดำเนินการป้องกันไม่ให้ข้อมูลสูญหาย ถูกใช้หรือเปิดเผยโดยไม่ได้รับอนุญาต หรือสำหรับการรักษาความปลอดภัยของข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องคุ้มครองรักษาข้อมูลส่วนบุคคลตลอดเวลาด้วยเทคนิคและระบบรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลไม่สูญหาย ไม่ถูกใช้หรือเปิดเผยโดยไม่ได้รับอนุญาต หรือป้องกันไม่ให้มีผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือเปิดเผยข้อมูล ทั้งยังควรดำเนินการป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยมิชอบ การแก้ไขข้อมูลหรือการเปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต และการป้องกันข้อมูลไม่สูญหาย ไม่ถูกใช้หรือเปิดเผยโดยไม่ได้รับอนุญาต

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลให้บุคคลอื่นดำเนินการตามระบบการบริหารงานบุคคลขององค์กร ถ้าเจ้าของข้อมูลให้ความยินยอมเป็นหนังสือ หรือตามที่กฎหมายกำหนด ยกเว้นกรณีที่จำเป็นเร่งด่วนเกี่ยวกับประโยชน์ของส่วนรวม หรือกรณีที่อาจกระทำให้เกิดความเสียหายแก่ชีวิต ร่างกาย หรืออนามัยของบุคคล องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะแจ้งให้เจ้าของข้อมูลทราบโดยเร็วภายใน 15 วัน นับแต่วันส่งหรือโอนข้อมูลดังกล่าว

ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลได้จ่ายหรือมอบหมายให้บุคคลที่สามดำเนินการเกี่ยวกับระบบการบริหารงานบุคคลขององค์กรไม่ว่าทั้งหมดหรือบางส่วน องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้เกิดความมั่นใจว่าบุคคลที่สามซึ่งได้รับมอบหมายให้ดำเนินการดังกล่าวได้ตระหนักถึงความจำเป็นที่ต้องปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูล

1.5 ความโปร่งใส

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องกำหนดแนวนโยบายที่เกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคล และเปิดเผยแนวนโยบายดังกล่าวให้เป็นที่ปรากฏชัดเจนต่อบุคคลที่เกี่ยวข้องกับข้อมูล

หากมีการร้องขอ, องค์กรหรือหน่วยงานที่จัดเก็บข้อมูลต้องดำเนินการตามขั้นตอนที่เหมาะสมและอย่างสมเหตุสมผล เพื่อให้บุคคลผู้เป็นเจ้าของข้อมูลหรือผู้เกี่ยวข้องกับข้อมูลที่ตนจัดเก็บได้ทราบถึงประเภทของข้อมูลที่จัดเก็บ, วัตถุประสงค์ของการจัดเก็บ, วิธีการจัดเก็บ, การเก็บรักษา, การใช้, หรือเปิดเผยข้อมูลนั้น

1.6 การเข้าถึงข้อมูลและการแก้ไขข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องเปิดโอกาสให้บุคคลผู้เป็นเจ้าของข้อมูลหรือผู้เกี่ยวข้องกับข้อมูลเข้าตรวจดูข้อมูลส่วนบุคคลที่เกี่ยวกับตนเอง, ขอสำเนาหรือขอสำเนารับรองความถูกต้องของข้อมูลดังกล่าว, ขอแก้ไขหรือเปลี่ยนแปลง, หรือให้ระงับการใช้หรือระงับการเปิดเผยข้อมูล, หรือให้ลบหรือทำลายข้อมูลส่วนที่พ้นระยะเวลาการเก็บรวบรวมหรือที่ไม่เกี่ยวข้องหรือเกินกว่าความจำเป็นตามวัตถุประสงค์ของการเก็บรวบรวมนั้นได้เมื่อมีการร้องขอ, เว้นแต่:

(1) การอนุญาตให้เข้าถึงนั้นจะก่อให้เกิดภัยที่เป็นการคุกคามอย่างรุนแรงต่อชีวิต, ร่างกาย, หรือสุขภาพของบุคคล
(2) การอนุญาตให้เข้าถึงนั้นจะก่อให้เกิดผลกระทบต่อสิทธิส่วนบุคคลของบุคคลอื่นโดยไม่สมควร
(3) การอนุญาตให้เข้าถึงนั้นจะก่อให้เกิดภาระอันเกินสมควรแก่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล

(4) การร้องขอเพื่อเข้าถึงเป็นการร้องขอที่ไม่จริงจังหรือไม่มีจตรังตามที่ต้องการ, เข้าถึงข้อมูลซึ่งเป็นที่เห็นได้อย่างชัดเจน
(5) การอนุญาตให้เข้าถึงจะก่อให้เกิดความเสียหายต่อการสืบสวนหรือสอบสวน, ที่เกี่ยวกับการกระทำที่มิชอบด้วยกฎหมาย
(6) การอนุญาตให้เข้าถึงเป็นการอันตรายโดยกฎหมาย
(7) มีกฎหมายห้ามไม่ให้มีการเข้าถึงข้อมูลดังกล่าว เนื่องจากเหตุผลที่เกี่ยวข้องกับความมั่นคงของประเทศ

ถ้าการอนุญาตให้เข้าถึงข้อมูลจะเป็นการเปิดเผยถึงข้อมูลที่เกี่ยวข้องกับกระบวนการตัดสินใจทางธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล, องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวอาจใช้วิธีการอธิบายเกี่ยวกับกระบวนการตัดสินใจแทนการอนุญาตให้เข้าถึงข้อมูลนั้นได้ถ้าการเข้าถึงข้อมูลเป็นสิ่งที่ไม่สามารถปฏิบัติได้อย่างเหมาะสมและอย่างสมเหตุสม, องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลและบุคคลผู้ร้องขออาจตกลงที่จะพิจารณาว่าการดำเนินการแทนโดยคนกลางจะเป็นการเข้าถึงที่เพียงพอต่อความต้องการของทั้งสองฝ่ายหรือไม่ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกำหนดข้อกำหนดในการอนุญาตให้เข้าถึงข้อมูล, ข้อกำหนดนั้น

(1) ต้องไม่สูงจนเกินไปและ

(2) ต้องไม่ใช้กับคำขอเข้าถึงข้อมูล

ถ้าองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลหรือบุคคลผู้ร้องขอข้อมูลสามารถแสดงให้เห็นได้ว่าข้อมูลที่จัดเก็บนั้นไม่ถูกต้อง, สมบูรณ์, หรือไม่เป็นปัจจุบัน, องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องดำเนินการตามขั้นตอนที่เหมาะสมเพื่อทำให้ข้อมูลที่จัดเก็บถูกต้อง, สมบูรณ์, และปัจจุบันถ้าองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลและบุคคลที่ร้องขอข้อมูลมีความเห็นที่ไม่ตรงกันเกี่ยวกับความถูกต้อง, สมบูรณ์, หรือปัจจุบันของข้อมูล, หากบุคคลผู้ร้องขอข้อมูลได้ขอให้องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวจัดทำหมายเหตุหรือบันทึกเพื่อให้มีการระบุถึงความไม่ถูกต้อง, สมบูรณ์, หรือไม่ปัจจุบันของข้อมูลนั้น, องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวต้องดำเนินการตามที่ร้องขอตามขั้นตอนที่เหมาะสม

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลมีหน้าที่ที่จะต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลตามที่ร้องขอ หรือในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลปฏิเสธที่จะดำเนินการแก้ไขข้อมูลตามที่ร้องขอด้วยเหตุผลตามที่มีกฎหมายให้อำนาจลงคราวล่ะ องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องมีหน้าที่ที่จะต้องแจ้งให้บุคคลที่ร้องขอทราบถึงการปฏิเสธดังกล่าวพร้อมทั้งเหตุผล

1.7 การปกปิดตัวตน

ในกรณีที่ไม่เป็นการขัดต่อบทบัญญัติแหล่งกฎหมายหรือแนวปฏิบัติที่ชอบด้วยกฎหมาย บุคคลยอมมีสิทธิ์หรือทางเลือกที่จะไม่เปิดเผยตัวตนหรือเปิดเผยตัวตนเมื่อติดต่อหรือทำธุรกรรมกับองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล

1.8 การส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศอื่นองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคลไปยังประเทศอื่นได้ หาก:องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลเชื่อโดยปราศจากข้อสงสัยว่าผู้รับข้อมูลอยู่ภายใต้บังคับของกฎหมาย, ข้อตกลงหรือข้อสัญญาซึ่งยึดถือหลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางที่กฎหมายกำหนดและมีมาตรฐานในการให้ความคุ้มครองข้อมูลส่วน

บุคคลในสาระสำคัญไม่ต่ำกว่าบทบัญญัติแห่งกฎหมายภายในประเทศ บุคคลผู้เป็นเจ้าของข้อมูลหรือที่เกี่ยวข้องกับข้อมูลได้ให้ความยินยอมเป็นหนังสือในการส่งข้อมูลนั้นการส่งข้อมูลไปยังประเทศอื่นดังกล่าวเป็นกรณีที่จำเป็นต่อการปฏิบัติตามสัญญาระหว่างบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลกับองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล หรือเป็นเรื่องที่จำเป็นต่อการดำเนินการก่อนทำสัญญาตามคำร้องขอของบุคคลดังกล่าวนั้นการส่งข้อมูลไปยังประเทศอื่นเป็นความจำเป็นต่อการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของสัญญาระหว่างองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกับบุคคลที่สาม เพื่อประโยชน์ของบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลการส่งข้อมูลไปยังประเทศอื่นเป็นไปเพื่อประโยชน์ของบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล

(1) เป็นการยากในทางปฏิบัติที่จะได้รับความยินยอมของบุคคลผู้เป็นเจ้าของข้อมูล หรือบุคคลที่เกี่ยวข้องกับข้อมูล และ

(2) เป็นที่เชื่อได้ว่าในทางปฏิบัติ บุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลจะให้ความยินยอมในการส่งข้อมูลนั้น

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการเพื่อให้เกิดความแน่ใจว่าข้อมูลที่จัดส่งจะไม่ถูกเก็บรวบรวม, เก็บรักษา, ใช้หรือเปิดเผยโดยผู้รับข้อมูลในลักษณะที่ไม่สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวกับบุคคลที่ใช้บังคับอยู่ในประเทศ ในขณะที่มีการส่งข้อมูล

การส่งข้อมูลไปยังประเทศอื่นดังกล่าวเป็นการกระทำตามบทบัญญัติแห่งกฎหมาย หรือเพื่อการดำเนินคดีนอกราชอาณาจักร

หมายเหตุ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 28 ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ ประเทศปลายทางหรือองค์การ ระหว่างประเทศที่รับข้อมูลส่วนบุคคลต้องมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ทั้งนี้ ต้องเป็นไปตามหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลตามที่คณะกรรมการประกาศกำหนดตามมาตรา 16 (5) เว้นแต่ว่า

(1) เป็นการปฏิบัติตามกฎหมาย

(2) ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลโดยได้แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบ ถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลแล้ว

(3) เป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนที่จะทำสัญญานั้น

(4) เป็นการกระทำตามสัญญาระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับบุคคลหรือนิติบุคคลอื่นเพื่อประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(5) เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่น เมื่อเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมในขณะนั้นได้

(6) เป็นการจำเป็นเพื่อการดำเนินภารกิจเพื่อประโยชน์สาธารณะที่สำคัญในกรณีที่มีปัญหาเกี่ยวกับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพอของประเทศปลายทางหรือองค์การระหว่างประเทศ ที่รับข้อมูลส่วนบุคคล ให้เสนอต่อคณะกรรมการเป็นผู้พิจารณา ทั้งนี้ คำพิจารณาของคณะกรรมการอาจขอให้ตรวจสอบได้เมื่อมีหลักฐานใหม่ที่ทำให้เชื่อได้ว่าประเทศปลายทางหรือองค์การระหว่างประเทศ ที่รับข้อมูลส่วนบุคคลมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ

1.9 ความรับผิดชอบขององค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องแต่งตั้งบุคคลหนึ่งหรือหลายคน ให้มีหน้าที่รับผิดชอบในการพัฒนานโยบายเกี่ยวกับความเป็นส่วนตัวและการรักษาความปลอดภัยของข้อมูล ฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้อมูล

และดูแลให้มีการปฏิบัติตามนโยบายอย่างจริงจัง องค์กรควรกำหนด ศูนย์ประสานงานเพื่อคอยตอบคำถามและรับเรื่องร้องเรียน และคอยดูแลให้มีการเยียวยาความเสียหาย จากการที่ข้อมูลเกี่ยวข้อมูลตัวของผู้นั้นถูกนำไปใช้โดยมิชอบ

ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกระทำการใดๆ เกี่ยวกับ ข้อมูลส่วนบุคคลแล้วก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือแก่บุคคลที่เกี่ยวข้อมูล องค์กรธุรกิจหรือ หน่วยงานเอกชนที่จัดเก็บข้อมูลต้องรับผิดชดใช้ค่าเสียหายทดแทนเพื่อการนั้นไม่ว่าจะกระทำโดยจงใจหรือ ประมาทเลินเลอก็ตาม รวมทั้งต้องรับผิดในทางแพร่สำหรับการกระทำหรือการดำเนินการของพนักงาน ผู้มีหน้าที่รับผิดชอบในการเก็บรักษาหรือควบคุมดูแลข้อมูลเกี่ยวข้อมูลบุคคลในกรณีที่พนักงานนั้นกระทำ การหรือดำเนินการตามบทบัญญัติของกฎหมาย แม้แม่ว่าการกระทำหรือการดำเนินการดังกล่าวจะ เป็นการกระทำหรือการดำเนินการที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลไม่ทราบหรือไม่ได้ให้การ อนุญาตตาม เว้นแต่จะพิสูจน์ได้ว่าการกระทำนั้นเกิดจากเหตุสุดวิสัย หรือเป็นการกระทำตามกฎหมาย หรือตามคำสั่งของเจ้าหน้าที่ตามกฎหมาย หรือเกิดเพราะการกระทำของเจ้าของข้อมูลเอง หรือของบุคคลที่เกี่ยวข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องรับผิดในทางแพร่สำหรับการกระทำหรือการดำเนินการของบุคคลที่สาม ซึ่งดำเนินการในนามขององค์กรธุรกิจหรือหน่วยงานเอกชนที่ จัดเก็บข้อมูล หรือในฐานะตัวแทนขององค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลไม่ว่าด้วยชัดแจ้ง หรือด้วยปริยายด้วย

หมายเหตุ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 ได้กำหนดให้ ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่รับอนุญาตหรือโดยมิชอบ และต้อง ทบทวนมาตรการดังกล่าว เมื่อมีความจำเปรียนหรือเมื่อเทคโนโลยีเปลี่ยนแปลงเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการ ประกาศกำหนด

(2) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันไม่ให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่รับอนุญาตหรือ โดยมิชอบ

(3) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้อมูลหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บ รวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือเท่าที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพ

ในการแสดงความคิดเห็น การเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือมาตรา 26 (5) (ก) หรือ (ข) การใช้เพื่อการก๊อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความในมาตรา 33 วรรคที่ห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม

(4) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก้สำนักงานโดยไม่ชักชำาภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักชำด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

(5) ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง ต้องแต่งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือ ซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูล

ส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตา วัตถุประสงค์ของผู้ควบคุมข้อมูล ส่วนบุคคล
(6) การใช้หรือเปิดเผยตามมาตรา 27 วรรคสาม
(7) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา 30 วรรคสาม มาตรา 31 วรรคสาม มาตรา 32 วรรคสาม และ มาตรา 36 วรรคหนึ่ง
(8) คำอธิบายเกี่ยวกับมาตการรักษาความมั่นคงปลอดภัยตามมาตรา 37 (1) ความในวรรคหนึ่งให้นำมาใช้บังคับกับ ตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา 5 วรรคสอง โดยอนุโลม ความใน (1) (2) (3) (4) (5) (6) และ (8) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการ ประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิ และเสรีภาพของ เจ้าของข้อมูลส่วนบุคคล หรือมิใช้กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็น ครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26
หมายเหตุ: พระราชบัญญัติคุมครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 77 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ดำเนินการใด ๆ เกี่ยวกับข้อมูลส่วนบุคคลอันเป็นการละาญหรือไม่ปฏิบัติตาม บทบัญญัติข้างพระราชบัญญัตินี้ทำให้เกิดความสียหายต่อเจ้าของข้อมูลส่วนบุคคลต้องชดใช้ค่าสินไหมทดแทนเพื่อ การนั้นและเจ้าของข้อมูลส่วนบุคคลไม่ต้องพิสูจน์ว่าการดำเนินการนั้นจะเกิดจากการกระทำโดยจงใจหรือประมาท เหลินเหลือหรือไม่ ยกเว้นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลนั้นจะพิสูจน์ว่า
(1) ความเสียหายนั้นเกิดจากเหตุสุดวิสัย หรือเกิดจากการกระทำหรือละเวนการกระทำของ เจาของขอมูลสวน บุคคลนั้นเอง
(2) ให้เป็นการปฏิบัติตามคำสั่งของเจ้าของข้อมูลที่ซึ่งปฏิบัติการตามคำของเจ้าข้อมูลและอำนาจตามกฎหมาย ค่า สินไหมทดแทนตามวรรคหนึ่ง หมายความรวมถึงค่าใช้จ่ายทั้งหมดที่เจ้าของข้อมูลได้ใช้จ่ายไปตามความจำเป็นใน การป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วยหลักเกณฑ์และแนวทางการ ดำเนินการในเชิงนโยบายที่ต้องประกาศให้สาธารณชนทราบองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลส่วน บุคคลควรกำหนดแนวนโยบายที่เกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคล และ เปิดเผยแนวนโยบายดังกล่าวให้เป็นที่รู้จักชัดเจนต่อบุคคลที่เกี่ยวข้องกับข้อมูล โดยต้องไม่ถือว่ากระบวนการเกี่ยวกับ การจัดเก็บข้อมูลส่วนบุคคลดังกล่าวเป็นความลับขององค์กร ทั้งนี้เพื่อสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้ใช้บริการ และเพื่อให้องค์กรธุรกิจนั้น ยอมรับทั้งในระดับประเทศและในระดับระหว่างประเทศ การดำเนินการในเชิงนโยบายที่ ควรประกาศให้สาธารณชนทราบควรมีหัวข้อที่เป็นมาตรฐานขั้นต่ำดังต่อไปนี้:
2.1 แนวนโยบายเกี่ยวกับการเก็บรวบรวม การเก็บรักษา และการประมวลผลข้อมูลส่วนบุคคล
ควรมีหลักการที่สอดคล้องกับมาตรฐานสากล ดังนี้: องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลส่วนบุคคลหรือ ข้อมูลที่เกี่ยวข้องกับบุคคลควรจัดเก็บรวบรวมข้อมูลดังกล่าวเพียงเท่าที่เกี่ยวข้องและจำเป็นต่อการดำเนินการตาม อำนาจ หน้าที่ หรือลักษณะขององค์กรหรือหน่วยงานเอกชนนั้นองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล ควรจัดเก็บข้อมูลตามที่กฎหมายอนุญาต อำนาจไว้ และจะจัดเก็บด้วยวิธีการที่ถูกต้องและเป็นธรรมต่อเจ้าของข้อมูล หรือบุคคลที่เกี่ยวข้องกับข้อมูล โดยจะเคารพสิทธิส่วนบุคคลของเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลตาม รัฐธรรมนูญองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือใน ขณะที่จะดำเนินการเก็บรวบรวมข้อมูลถึงการให้ข้อมูลต้องเป็นไปตามความสมัครใจโดยมีรายละเอียดดังต่อไปนี้ ข้อมูลที่จัดเก็บได้วัตถุประสงค์ของการเก็บรวบรวมประเภทของข้อมูลส่วนบุคคลที่จะเก็บรวบรวมวิธีการเก็บรวบรวม ข้อมูลส่วนบุคคลระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคลเงื่อนไขหรือหลักเกณฑ์ที่เจ้าของข้อมูลหรือบุคคลที่ เกี่ยวข้องกับข้อมูลสามารถขอบุคคล หรือองค์กรที่ข้อมูลจะต้องเปิดเผยต่อกฎหมายที่อนุญาตให้จัดเก็บข้อมูลได้

เฉพาะ (ถ้ามี)สิทธิของบุคคลที่เกี่ยวข้องกับข้อมูลในการขอเข้าถึงข้อมูล รวมถึงสิทธิในการขอให้มีการแก้ไขข้อมูลที่เกี่ยวข้องกับตนให้ถูกต้องผลที่อาจจะเกิดขึ้น (ถ้ามี) กับบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลหากบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลไม่ให้ข้อมูลทั้งหมดหรือบางส่วน
องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะจัดเก็บข้อมูลจากบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลโดยตรง
ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนจัดเก็บข้อมูลจากบุคคลที่สามหรือจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรง จะต้องเป็นข้อมูลที่จัดเก็บจากแหล่งข้อมูลที่เชื่อถือได้ และองค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวจะต้องแจ้งให้เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลทราบ และจะต้องขอความยินยอมจากเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลก่อนจัดเก็บองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะต้องไม่จัดเก็บรวบรวมข้อมูลที่เกี่ยวข้องกับข้อมูลที่มีลักษณะอ่อนไหวต่อความรู้สึกของบุคคล เช่น ข้อมูลที่แสดงให้เห็นถึงชาติพันธุ์, ลัทธิ ความเชื่อ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนา, ความเชื่อส่วนบุคคล, รายละเอียดเกี่ยวกับสุขภาพ, ทัศนะคติเกี่ยวกับเพศ, และอื่น ๆ ตามที่กฎหมายกำหนด เว้นแต่:
(1) บุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลได้ให้ความยินยอม
(2) เป็นการเก็บข้อมูลตามกฎหมายหรือได้รับการอนุญาตตามผลของกฎหมาย
(3) เป็นการเก็บรวบรวมข้อมูลที่จำเป็นต่อการป้องกันภัยร้ายที่กำลังจะเกิดขึ้น หรือเกิดต่อชีวิต, ร่างกาย, หรือสุขภาพของบุคคล และบุคคลนั้นไม่สามารถที่จะให้ความยินยอมได้
(4) การเก็บรวบรวมนั้นเป็นการดำเนินการที่จำเป็นต่อการสู้คดีในกรณีที่มีการฟ้องเรียกร้องค่าเสียหายจากองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล
(5) การเก็บรวบรวมข้อมูลนั้นจำเป็นสำหรับวัตถุประสงค์เชิงป้องกันในทางการแพทย์ หรือการตรวจสอบทางการแพทย์
(6) เป็นการเก็บรวบรวมตามบทบัญญัติหรือกฎที่ออกโดยองค์กรวิชาชีพซึ่งองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลมีหน้าที่ที่จะต้องรักษาความลับตามจรรยาบรรณแห่งวิชาชีพนั้น ๆ
2.2 แนวนโยบายเกี่ยวกับการใช้และการเปิดเผยข้อมูลส่วนบุคคลควรมีหลักการที่สอดคล้องกับมาตรฐานสากลดังนี้:
องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคลควรใช้หรือเปิดเผยข้อมูลส่วนบุคคลเพียงเท่าที่เป็นไปตามวัตถุประสงค์ของการจัดเก็บ
ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนต้องการใช้หรือเปิดเผยข้อมูลนอกเหนือไปจากวัตถุประสงค์ของการจัดเก็บเดิม องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวควรแจ้งให้เจ้าของข้อมูลทราบและขอความยินยอมจากเจ้าของข้อมูลก่อน ยกเว้นว่า:
(1) วัตถุประสงค์ในการใช้หรือเปิดเผยเป็นวัตถุประสงค์ที่เกี่ยวเนื่องหรือมีความสัมพันธ์กับวัตถุประสงค์ของการจัดเก็บเดิม และบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลสามารถที่จะคาดการณ์ได้อย่างมีเหตุมีผลว่าองค์กรธุรกิจหรือหน่วยงานเอกชนนั้นจะใช้หรือเปิดเผยข้อมูลตามวัตถุประสงค์อื่นที่เกี่ยวเนื่องกับวัตถุประสงค์ที่จัดเก็บข้อมูลเดิม
(2) ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนได้ใช้ข้อมูลเพื่อประโยชน์เกี่ยวกับการตลาดแบบตรง ซึ่งในทางปฏิบัติเป็นการยากที่องค์กรธุรกิจหรือหน่วยงานเอกชนจะขอความยินยอมจากบุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลก่อนการใช้หรือเปิดเผยข้อมูลนั้น อย่างไรก็ตาม ในกรณีที่บุคคลผู้เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลปฏิเสธที่จะรับการติดต่อเพื่อการตลาดแบบตรงอีกต่อไป องค์กรธุรกิจหรือหน่วยงานเอกชนนั้นจะต้องยุติการใช้หรือเปิดเผยข้อมูลดังกล่าว

(3) องค์กรธุรกิจหรือหน่วยงานเอกชนนั้นมีเหตุผลอันสมควรเชื่อได้ว่าการใช้หรือเปิดเผยข้อมูลเป็นกรณีที่จำเป็นต่อการป้องกันภัยันตรายต่อชีวิต ร่างกายหรือสุขภาพของบุคคลและภัยันตรายนั้นเป็นภัยันตรายที่ใกล้จะเกิดขึ้น
(4) องค์กรธุรกิจหรือหน่วยงานเอกชนนั้นมีเหตุผลอันควรเชื่อได้ว่ามีการกระทำที่ไม่ชอบด้วยกฎหมายหรือมีการกระทำซึ่งกำลังเกิดขึ้นและเป็นการกระทำที่เกี่ยวข้องกับการกระทำที่ไม่ชอบด้วยกฎหมาย ซึ่งการใช้หรือเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลเกี่ยวกับบุคคลดังกล่าวเป็นกรณีจำเป็นสำหรับการสืบสวนหรือการใช้หรือเปิดเผยดังกล่าวเป็นส่วนหนึ่งของการจัดทำรายงานที่ต้องจัดทำขึ้นเพื่อประโยชน์ของบุคคลที่เกี่ยวข้องหรือเจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้องกับเรื่องดังกล่าว
(5) เป็นการใช้หรือเปิดเผยตามที่กฎหมายกำหนด หรือเป็นการใช้หรือเปิดเผยต่อผู้มีอำนาจตามกฎหมาย
(6) เป็นการใช้หรือเปิดเผยอย่างสมเหตุสมผลและจำเป็นต่อการบังคับใช้กฎหมาย ที่มีโทษทางอาญา หรือกฎหมายที่เกี่ยวข้องกับการจัดเก็บภาษีอากรของรัฐ
(7) เป็นการใช้หรือเปิดเผยตามที่องค์กรหรือหน่วยงานด้านความมั่นคงร้องขอ ด้วยเหตุผลที่เกี่ยวข้องกับความมั่นคงของประเทศ

หากองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะต้องเปิดเผยข้อมูลส่วนบุคคลก่อนได้รับความยินยอมจากเจ้าของข้อมูลด้วยเหตุผลดังกล่าวใน 2) ข้างต้น องค์กรธุรกิจหรือหน่วยงานเอกชนจะเปิดเผยข้อมูลเฉพาะที่เกี่ยวข้องกับเจ้าของข้อมูลนั้นโดยตรงเท่านั้น และจะทำเท่าที่จำเป็น และเมื่อเปิดเผยข้อมูลใดแล้วจะแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้อย ส่วนผู้รับข้อมูลส่วนบุคคลดังกล่าว ต้องไม่ใช้หรือเปิดเผยข้อมูลเพื่อวัตถุประสงค์อื่นนอกเหนือจากที่ได้แจ้งความประสงค์ไว้แล้ว
ในกรณีที่เอกสารฉบับหนึ่งฉบับใดมีข้อมูลเกี่ยวกับบุคคลของบุคคลตั้งแต่สองคนขึ้นไป ห้ามมิให้องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลป้องกันการเข้าถึงข้อมูลดังกล่าว หากองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลสามารถที่จะปกป้องข้อมูลของบุคคลอื่นที่ไม่เกี่ยวข้องกับบุคคลผู้ขอข้อมูลได้ โดยการปิดบังชื่อ, นามสกุล, เลขประจำตัวประชาชน หรือ สัญลักษณ์อื่นใดที่สามารถระบุตัวบุคคลอื่นนั้นได้

แนวนโยบายเกี่ยวกับการเก็บรักษา การแก้ไขและการโอนข้อมูลส่วนบุคคลควรมีหลักการที่สอดคล้องกับมาตรฐานสากลดังนี้:

1) องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะจัดเก็บรักษาข้อมูลเพียงเท่าที่จำเป็นตามที่ได้แจ้งต่อเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลแล้ว เว้นแต่บุคคลที่เกี่ยวข้องกับข้อมูลหรือบุคคลผู้เป็นเจ้าของข้อมูลจะให้ความยินยอมอย่างชัดเจนว่าให้เก็บรักษาข้อมูลเกินระยะเวลาตามที่กำหนดหรือเว้นแต่มีเหตุจำเป็นที่ต้องกำหนด นอกจากนี้ หน้าที่ให้องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องเก็บรักษาข้อมูลเกินระยะเวลาที่กำหนดหรือมีเหตุจำเป็นอื่นใดที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องเก็บรักษาข้อมูลเกินระยะเวลาที่กำหนด และองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะต้องลบหรือทำลายข้อมูลดังกล่าวเมื่อพ้นระยะเวลาที่กำหนดหรือหมดความจำเป็นในการเก็บรวบรวมหรือเจ้าของข้อมูลเพิกถอนความยินยอม ในกรณีนี้ องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะต้องดำเนินการด้วยความระมัดระวังและรอบคอบเพื่อให้เกิดความมั่นใจว่ามีการลบหรือทำลายข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้องกับบุคคล หรือทำให้ข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลได้แบบชัดเจน
2) โอรเวลิส เป็นยาที่ใช้เพื่อรักษาหรือควบคุมอาการเกี่ยวกับสภาพจิตใจ เช่น ซึมเศร้า (depression), วิตก (anxiety), อารมณ์ผิดปกติ (mood disorders), โรคจิตเวช (psychiatric disorders), อาการออกพฤติ (behavioral problems), หรืออาการระบบทางประสาทอื่น ๆ ซึ่งอาจมีอาการทางร่างกายร่วมด้วย เช่น

อาการสั่น (tremors) หรืออาการหดตัว (twitching) ซึ่งส่วนใหญ่จะถูกแพทย์หรือจิตแพทย์สั่งจากใบสั่งยาของแพทย์ เนื่องจากอยู่ในกลุ่มยาที่ควรใช้ใต้ควบคุมและมีผลข้างเคียงที่สามารถเกิดขึ้นได้

3) ในการใช้ยาโอรเวลิส ควรปฏิบัติตามคำสั่งของแพทย์อย่างเคร่งครัด และปฏิบัติตามคำแนะนำในบ้านที่ได้รับจากแพทย์หรือผู้ให้บริการดูแล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้เกิดความมั่นใจว่าข้อมูลส่วนบุคคลหรือข้อมูลเกี่ยวกับบุคคลที่จัดเก็บใช้หรือเปิดเผยเป็นข้อมูลที่ถูกต้องครบถ้วนสมบูรณ์และเป็นปัจจุบัน สอดคล้องกับวัตถุประสงค์ของการจัดเก็บ และไม่นอกเหนือวัตถุประสงค์ที่กำหนด

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการตามขั้นตอนที่เหมาะสมเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยไม่มีอำนาจหรือไม่ได้รับอนุญาต หรือป้องกันไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลโดยไม่ชอบ รวมทั้งจะดำเนินการป้องกันไม่ให้ข้อมูลเกิดการสูญหาย ใช้หรือเปิดเผยข้อมูลโดยมิชอบ

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะคุมครองรักษาข้อมูลส่วนบุคคลตลอดเวลาด้วยเทคนิคและการวางระบบรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลสูญหาย หรือไม่ให้ผู้ใดนำไปใช้ในทางที่ผิดหรือไม่สมควร หรือทำลายหรือเปลี่ยนแปลงข้อมูล หรือเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือเปิดเผยข้อมูล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลที่อยู่ในความครอบครองหรือควบคุมดูแลให้กับบุคคลอื่นได้ หากเจ้าของข้อมูลให้ความยินยอม เว้นแต่กรณีจำเป็นเร่งด่วนเกี่ยวกับประโยชน์ของส่วนรวม หรือกรณีที่อาจส่งให้เกิดความเสียหายแก่ชีวิตร่างกายหรืออนามัยของบุคคล องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลดังกล่าวไปก่อนได้ แต่จะแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้อ

ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลได้ว่าจากหรือมอบหมายให้บุคคลที่สามดำเนินการเกี่ยวกับระบบการบริหารงานบุคคลขององค์กรไม่ให้ทั้งหมดหรือบางส่วน องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการตามขั้นตอนที่เหมาะสมเพื่อให้เกิดความมั่นใจว่าบุคคลที่สามซึ่งได้รับมอบหมายให้ดำเนินการดังกล่าวได้ตระหนักถึงความจำเป็นที่ต้องปฏิบัติตามมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจส่งหรือโอนข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวข้อมูลไปยังประเทศอื่นได้ หาก

(1) องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลเชื่อโดยมั่นใจว่าผู้รับข้อมูลอยู่ภายใต้บังคับของกฎหมาย ข้อตกลง หรือข้อสัญญาซึ่งยึดถือหลักการคุ้มครองข้อมูลส่วนบุคคลตามแนวทางที่กฎหมายกำหนด และมีมาตรฐานในการให้ความคุ้มครองข้อมูลส่วนบุคคลใน สาระสำคัญไม่ต่ำกว่าที่บัญญัติแห่งกฎหมายภายในประเทศ

(2) บุคคลที่เป็นเจ้าของข้อมูลหรือเกี่ยวข้องกับข้อมูลต้องให้ความยินยอมในการส่งข้อมูลนั้น

(3) การส่งข้อมูลไปยังประเทศอื่นดังกล่าวเป็นกรณีที่จำเป็นต่อการปฏิบัติตาม สัญญาระหว่างบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูลกับองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล หรือเป็นเรื่องที่จำเป็นต่อการดำเนินการก่อนทำสัญญาตามคำร้องขอของบุคคล ดังกล่าวนั้น

(4) การส่งข้อมูลไปยังประเทศอื่นเป็นความจำเป็นต่อการดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของสัญญาระหว่างองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกับบุคคลที่สาม เพื่อ ประโยชน์ของบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้องกับข้อมูล

(5) การส่งข้อมูลไปยังประเทศอื่นเป็นไปเพื่อประโยชน์ของบุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อมูล และ
(ก) เป็นการยากในทางปฏิบัติที่จะได้รับความยินยอมของบุคคลที่เป็น เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อมูล และ
(ข) เป็นที่เชื่อได้ว่าในทางปฏิบัติ บุคคลที่เป็นเจ้าของข้อมูลหรือบุคคลที่ เกี่ยวข้อมูลจะให้ความยินยอมในการส่งข้อมูลนั้น

(6) องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการเพื่อให้มั่นใจว่าข้อมูลที่จัดส่ง จะไม่ถูกเก็บรวบรวม เก็บรักษา ใช้หรือเปิดเผยโดยผู้รับข้อมูลในลักษณะที่ ไม่สอดคล้องกับหลักการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลที่เกี่ยวกับบุคคลที่ใช้บังคับอยู่ในประเทศ ในขณะที่มีการส่งข้อมูล
2.4 แนวนโยบายเกี่ยวกับการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลควรมีหลักการที่สอดคล้องกับมาตรฐานสากล ดังนี้:

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรเปิดโอกาสให้บุคคลผู้เป็นเจ้าของ ข้อมูลหรือเกี่ยวข้องกับข้อมูลเข้าตรวจดูข้อมูลส่วนบุคคลที่เกี่ยวกับตนเอง ขอสำเนาหรือขอสำเนารับรองความถูกต้องของข้อมูลดังกล่าว ขอแก้ไขหรือเปลี่ยนแปลงหรือให้ระงับการใช้หรือระงับการเปิดเผยข้อมูล หรือให้ลบหรือทำลายข้อมูลส่วนที่พึงระยะเวลาการเก็บรวบรวมหรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็น ตามวัตถุประสงค์ของการเก็บรวบรวมนั้นได้ เมื่อมีการร้องขอ เว้นแต่:
(1) การอนุญาตให้เข้าถึงนั้นจะก่อให้เกิดภัยที่เป็นการคุกคามอย่างรุนแรงต่อชีวิต ร่างกายหรือสุขภาพของบุคคล
(2) การอนุญาตให้เข้าถึงนั้นจะก่อให้เกิดผลกระทบต่อสิทธิส่วนบุคคลของบุคคลอื่นโดยไม่สมควร
(3) การอนุญาตให้เข้าถึงนั้นจะก่อให้เกิดภาระอันเกินควรแก่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล
(4) การร้องขอเพื่อเข้าถึงข้อมูลเป็นการร้องขอที่ไม่จริงจังหรือไม่มีเจตนาที่จำเป็น เข้าถึงข้อมูลซึ่งเป็นที่เห็นได้ชัดเจน
(5) การอนุญาตให้มีการเข้าถึงจะก่อให้เกิดความเสียหายต่อการสืบสวนหรือสอบสวน ที่เกี่ยวกับการกระทำที่มิชอบด้วยกฎหมาย
(6) การอนุญาตให้เข้าถึงเป็นการอันตรายโดยกฎหมาย
(7) มีกฎหมายห้ามไม่ให้มีการเข้าถึงข้อมูลดังกล่าวไว้เป็นการเฉพาะ

(8) ข้อมูลที่ขอเข้าถึงเป็นข้อมูลที่เกี่ยวข้องกับข้อโต้แย้งทางกฎหมายที่เกี่ยวข้องกับกระบวนการไกลเกลี่ยข้อมูลระหว่างองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกับบุคคลที่ร้องขอ และข้อมูลดังกล่าวเป็นข้อมูลซึ่งไม่สามารถเข้าถึงหรือเปิดเผยได้โดยกระบวนการไกลเกลี่ยข้อมูลนั้น

(9) การอนุญาตให้เข้าถึงจะเป็นการเปิดเผยถึงแนวทางการเจรจาต่อรองของ องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกับบุคคลผู้ร้องขอ ซึ่งหากมีการเปิดเผยจะทำให้เกิดความเสียหายต่อการเจรจาต่อรองนั้น

(10) หน่วยงานทางด้านความมั่นคง หน่วยงานที่เกี่ยวข้องกับราชการลับหรือ หน่วยงานที่เกี่ยวข้องกับการบังคับใช้กฎหมายสั่งห้ามไม่ให้องค์กรธุรกิจหรือหน่วยงานเอกชนอนุญาตให้ มีการเข้าถึงข้อมูลดังกล่าว เนื่องจากเหตุผลที่เกี่ยวข้องกับความมั่นคงของประเทศ
ถ้าการอนุญาตให้เข้าถึงข้อมูลจะเป็นการเปิดเผยข้อมูลที่เกี่ยวข้องกับกระบวนการตัดสินใจทางการคำขอขององค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวอาจใช้วิธีการอธิบายถึงกระบวนการตัดสินใจแทนการอนุญาตให้เข้าถึงข้อมูลนั้นได้

ถ้าการเข้าถึงข้อมูลเป็นสิ่งที่ไม่สามารถปฏิบัติได้อย่างสมเหตุสมผล องค์กรธุรกิจหรือ หน่วยงานเอกชนที่จัดเก็บข้อมูลและบุคคลผู้ร้องขออาจตกลงที่จะพิจารณาว่าการดำเนินการแทนโดยคนกลาง จะเป็นการเข้าถึงที่เพียงพอต่อความต้องการของทั้งสองฝ่ายหรือไม่

ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกำหนดเงื่อนไขในการ อนุญาตให้เข้าถึงข้อมูล ค่าใช้จ่ายนั้น
(1) ต้องไม่สูงเกินไป และ
(2) ต้องไม่ใช้กับคำขอเข้าถึงข้อมูล

ถ้าองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล หรือบุคคลผู้ร้องขอข้อมูล สามารถแสดงให้เห็นได้ว่าข้อมูลที่จัดเก็บนั้นไม่ถูกต้อง สมบูรณ์ หรือไม่เป็นปัจจุบัน องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะดำเนินการตามขั้นตอนที่เหมาะสมเพื่อทำให้ข้อมูลที่จัดเก็บถูกต้อง สมบูรณ์ และปัจจุบันถ้าองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล และบุคคลที่ร้องขอข้อมูลมีความเห็นไม่ตรงกันเกี่ยวกับความถูกต้อง สมบูรณ์ หรือปัจจุบันของข้อมูล หากบุคคลผู้ร้องขอข้อมูลได้ขอให้ องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวจัดทำหมายเหตุหรือบันทึกเพื่อให้มีการระบุถึงความไม่ถูกต้อง สมบูรณ์ หรือไม่เป็นปัจจุบันของข้อมูลนั้น องค์กรธุรกิจหรือหน่วยงานเอกชนดังกล่าวจะดำเนินการตามขั้นตอนที่เหมาะสมตามคำขอของรายละเอียดข้อมูลและบันทึกอื่น ๆ ในกรณีที่เหมาะสมของคำขอข้อมูล ในทางปฏิบัติ องค์กรธุรกิจหรือหน่วยงานเอกชนอาจระบุความไม่ถูกต้อง สมบูรณ์ หรือไม่เป็นปัจจุบันของข้อมูลทางอิเล็กทรอนิกส์หรือใช้หมายเหตุทางเสียงหรือการเขียนเพื่อประทานคำขอข้อมูลเช่นกัน และติดตามในการทำคำขอในอนาคตหากเห็นจำเป็นขึ้นอย่างค่อยตามขั้นตอนที่เหมาะสม.
องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลมีหน้าที่ที่จะต้องให้เหตุผลในการปฏิเสธการเข้าถึงข้อมูลตามที่ร้องขอ หรือในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลปฏิเสธที่จะดำเนินการแก้ไขข้อมูลตามที่ร้องขอด้วยเหตุผลตามที่มีกฎหมายให้อำนาจไว้ องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลมีหน้าที่ที่จะต้องแจ้งให้บุคคลที่ร้องขอทราบถึงการปฏิเสธดังกล่าวพร้อมทั้งเหตุผล

ในกรณีที่ไม่เป็นการละเมิดบทบัญญัติหรือกฎหมายหรือแนวปฏิบัติที่กฎหมายกำหนด บุคคลมีสิทธิ์หรือความเลือกที่จะไม่เปิดเผยตัวตนหรือแสดงตนเมื่อติดต่อหรือทำธุรกรรมกับองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล

หมายเหตุ: ในส่วนของการคุ้มครองสิทธิของเจ้าของข้อมูล, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 32 ได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลมีสิทธิ์คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับตนเมื่อใดก็ได้ ดังต่อไปนี้:
กรณีที่เป็นข้อมูลส่วนบุคคลที่เก็บรวบรวมได้โดยไม่ต้องขอความยินยอมตาม มาตรา 24 (4) หรือ (5) ยกเว้นผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ว่า
(ก) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้น ผู้ควบคุมข้อมูลส่วนบุคคลได้แสดงให้เห็นถึงเหตุอันชอบธรรมตามกฎหมายที่สำคัญยิ่งกว่าหรือ
(ข) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อต่อสิทธิเรียกร้องตามกฎหมาย ปฏิบัติตามหรือใช้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อยกขึ้นต่อสู่สิทธิเรียกร้องตามกฎหมาย
(2) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงคราวกับการตลาด แบบตรง
(3) กรณีที่เป็นการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อวัตถุประสงคราวกับการ ศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ เว้นแต่เป็นการจำเป็นเพื่อการดำเนินภารกิจ เพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล
ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิ์คัดค้านตามวรรคหนึ่ง ผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลต่อไปได้ ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแยกเอกสารข้อมูลนี้ออกจากข้อมูลอื่นอย่างชัดเจนทันทีเมื่อเจ้าของข้อมูลส่วนบุคคลได้แจ้งการคัดค้าน
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลปฏิเสธคำขอดังใน (1) (ก) หรือ (ข) หรือ (3) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องระบุการปฏิเสธพร้อมกับเหตุผลในบันทึกตามมาตรา 39
หมายเหตุ: นอกจากนี้ตามที่ระบุในมาตรา 32 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 33 ระบุว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิ์ขอให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ในกรณีดังต่อไปนี้:
(1) เมื่อข้อมูลส่วนบุคคลไม่จำเป็นต่อการเก็บรักษาตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
(2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไป
(3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม มาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2)
(4) เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบตามกฎหมายตามที่ กำหนดในหมวดนี้ ความในวรรคหนึ่งมิให้นำมาใช้บังคับกับการเก็บรักษาเพื่อวัตถุประสงค์ในการใช้เสรีภาพในการ แสดงความคิดเห็น การเก็บรักษาเพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือ มาตรา 26
(5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้ สิทธิเรียกร้องตามกฎหมาย หรือเพื่อยกขึ้นต่อสู่สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติ ตามกฎหมาย
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึ่งหรือวรรคสาม เจ้าของข้อมูลส่วนบุคคลมีสิทธิ์ร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอนี้ โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการตามคำขอ
คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึ่งได้

(1) เมื่อข้อมูลส่วนบุคคลไม่จำเป็นต่อการเก็บรักษาตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
(2) เมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลไม่มีอำนาจตามกฎหมายที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลนั้นต่อไป
(3) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตาม มาตรา 32 (1) และผู้ควบคุมข้อมูลส่วนบุคคลไม่สามารถปฏิเสธคำขอตามมาตรา 32 (1) (ก) หรือ (ข) ได้ หรือเป็นการคัดค้านตามมาตรา 32 (2)
(4) เมื่อข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้ หรือเปิดเผยโดยไม่ชอบตามกฎหมายตามที่ กำหนดไว้ในหมวดนี้ ความบรรยายในวรรคหนึ่งไม่ใช้กับการเก็บรักษาเพื่อวัตถุประสงค์ในการแสดงความคิดเห็น การเก็บรักษาเพื่อวัตถุประสงค์ตามมาตรา 24 (1) หรือ (4) หรือ มาตรา 26
(5) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้ สิทธิเรียกร้องตามกฎหมาย หรือเพื่อยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่ดำเนินการตามวรรคหนึงหรือวรรคสาม เจ้าของข้อมูลส่วนบุคคลมีสิทธิ์ร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญเพื่อสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตามคำขอนี้ โดยแจ้งผู้ควบคุมข้อมูลส่วนบุคคลอื่น ๆ เพื่อให้ได้รับคำตอบในการดำเนินการตามคำขอ
คณะกรรมการอาจประกาศกำหนดหลักเกณฑ์ในการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลตามวรรคหนึงได้

แนวนโยบายที่สะท้อนให้เห็นถึงความรับผิดชอบขององค์กรธุรกิจหรือหน่วยงานเอกชน ที่จัดเก็บข้อมูลควรมีหลักการที่สอดคล้องกับมาตรฐานสากล ดังนี้

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจะต้องแต่งตั้งบุคคลหนึ่งหรือหลายคน ให้มีหน้าที่รับผิดชอบในการพัฒนานโยบายเกี่ยวกับความเป็นส่วนตัวและการรักษาความปลอดภัยของข้อมูล ฝึกอบรมเจ้าหน้าที่ที่เกี่ยวข้อง และดูแลให้มีการปฏิบัติตามนโยบายอย่างจริงจัง องค์กรควรกำหนด ศูนย์ประสานงานเพื่อคอยตอบคำถามและรับเรื่องร้องเรียน และคอยดูแลให้มีการเยียวยาความเสียหาย จากการที่ข้อมูลเกี่ยวกับตัวของผู้นั้นถูกนำไปใช้โดยไม่ชอบหมายเหตุ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 41 ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ของตน ในกรณีดังต่อไปนี้
(1) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานของรัฐตามที่ คณะกรรมการประกาศกำหนด
(2) การดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการ เก็บรวบรวม ใช้ หรือเปิดเผย จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลหรือระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากตามที่คณะกรรมการประกาศกำหนด
(3) กิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา 26
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจรวมกันตามที่คณะกรรมการประกาศกำหนดตามมาตรา 29 วรรคสอง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ดังกล่าวอาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรวมกันได้ ทั้งนี้

สถานที่ทำการแต่ละแห่ง ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในเครือกิจการหรือเครือ ธุรกิจเดียวกันดังกล่าวต้องสามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้โดยง่าย
ความในวรรคสองให้นำมาใช้บังคับแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งเป็นหน่วยงานของรัฐตาม (1) ซึ่งมีขนาดใหญ่หรือมีสถานที่ทำการหลายแห่งโดยอนุโลม
ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลตามวรรคหนึ่งต้องแต่งตั้ง ตัวแทนตามมาตรา 37 (5) ให้นำความในวรรคหนึ่งมาใช้บังคับแก่ตัวแทนโดยอนุโลม
ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้เจ้าของข้อมูลส่วนบุคคลและ สำนักงานทราบ ทั้งนี้ เจ้าของข้อมูลส่วนบุคคลสามารถติดต่อเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคล เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลและการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้ได้
คณะกรรมการอาจประกาศกำหนดคุณสมบัติของเจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคลได้ โดย คำนึงถึงความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
เจ้าหน้าที่ที่คุ้มครองข้อมูลส่วนบุคคลอาจเป็นพนักงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้รับจ้างให้บริการตามสัญญากับผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลก็ได้
ให้คำแนะนำแก่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้าง หรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัตินี้

ประสานงานและให้ความร่วมมือกับสำนักงานในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลในการปฏิบัติตามพระราชบัญญัตินี้

รักษาความลับของข้อมูลส่วนบุคคลที่ตนรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ที่คุมครองข้อมูลส่วนบุคคลโดยจัดหาเครื่องมือหรืออุปกรณ์อย่างเพียงพอ รวมทั้งอำนวยความสะดวกในการเข้าถึงข้อมูลส่วนบุคคลเพื่อการปฏิบัติหน้าที่

ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจะให้เจ้าหน้าที่ที่คุมครองข้อมูลส่วนบุคคลออกจากงานหรือเลิกสัญญาการจ้างด้วยเหตุที่เจ้าหน้าที่ที่คุมครองข้อมูลส่วนบุคคลปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ไม่ได้ ทั้งนี้ ในกรณีที่มีปัญหาในการปฏิบัติหน้าที่ เจ้าหน้าที่ที่คุมครองข้อมูลส่วนบุคคลต้องรายงานไปยังผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยตรง

เจ้าหน้าที่ที่คุมครองข้อมูลส่วนบุคคลอาจปฏิบัติหน้าที่หรือภารกิจอื่นได้ แต่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องรับรองการปฏิบัติหน้าที่ดังกล่าว ตามพระราชบัญญัตินี้ และไม่ขัดหรือแย้งต่อการ

ปฏิบัติหน้าที่ตามกฎหมาย หรือตามคำสั่งของเจ้าหน้าที่ที่ปฏิบัติหน้าที่ตามกฎหมาย หรือเกิดเพราะการกระทำของเจ้าของข้อมูลเองหรือของบุคคลที่เกี่ยวข้อง

ในกรณีที่องค์การธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลกระทำการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลแล้วส่งผลให้เกิดความเสียหายแก่เจ้าของข้อมูลหรือบุคคลที่เกี่ยวข้อง องค์การนั้นจะต้องรับผิดชดเชยค่าเสียหายทดแทนเพื่อการนั้น ไม่ว่าจะกระทำโดยจงใจหรือประมาทเจ้าของข้อมูลเอง รวมทั้งต้องรับผิดในทางแพร่สำหรับการกระทำหรือการดำเนินการของพนักงานผู้มีหน้าที่ในการเก็บรักษาหรือควบคุมดูแลข้อมูลเกี่ยวกับบุคคลในกรณีที่พนักงานนั้นกระทำการหรือดำเนินการตามบทบัญญัติของกฎหมาย แม้ว่าการกระทำหรือการดำเนินการดังกล่าวจะเป็นการกระทำหรือการดำเนินการที่องค์การธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลไม่ทราบหรือไม่ได้ให้การอนุญาต ยกเว้นในกรณีที่พิสูจน์ได้ว่าการกระทำนั้นเกิดจากเหตุสุดวิสัย หรือเป็นการกระทำตามกฎหมาย หรือตามคำสั่งของเจ้าของข้อมูลเองหรือของบุคคลที่เกี่ยวข้อง

องค์การธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องรับผิดในทางแพร่สำหรับการกระทำหรือการดำเนินการของบุคคลที่สาม ซึ่งดำเนินการในนามขององค์การธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูล หรือในฐานะตัวแทนขององค์การธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลไม่ว่าจะโดยชัดแจ้งหรือโดยปริยายด้วย

3. หลักเกณฑ์และแนวทางการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรภาคเอกชน
องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลส่วนบุคคลควรจัดทำหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลขึ้นใช้ภายในองค์กรเพื่อเป็นแนวทางปฏิบัติสำหรับพนักงานหรือเจ้าหน้าที่ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลสามารถนำไปปฏิบัติได้อย่างถูกต้อง ดังมีรายละเอียดต่อไปนี้:

3.1 แนวทางในการกำหนดนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ

องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรจำแนกความสำคัญของข้อมูลตามลักษณะของข้อมูล เช่น ข้อมูลที่มีลักษณะอ่อนไหวต่อความรู้สึกของบุคคล ซึ่งการเปิดเผยอาจเสี่ยงต่อการทำให้เจ้าของข้อมูลหรือผู้ที่เกี่ยวข้องกับข้อมูลได้รับความเสียหาย
กำหนดมาตรการการรักษาความปลอดภัยตามระดับความสำคัญของข้อมูลที่จำแนก
จัดให้มี Data Privacy Policy ที่ชัดเจน ทั้งในเรื่องของ Moral obligation และความรับผิดชอบตามกฎหมาย
กำหนดระดับของการเข้าถึงข้อมูลไว้ใน Access Control Policy เนื่องจากพนักงานแต่ละฝ่ายอาจมีความจำเป็นในการเข้าถึงข้อมูลที่แตกต่างกัน ทั้งนี้เพื่อลดโอกาสในการใช้ข้อมูลในทางที่ไม่ชอบและเข้าถึงข้อมูลโดยไม่จำเป็น Access Control Policy ควรเป็นไปตามหลักการ Need-to-know
กำหนดการลบหรือทำลายข้อมูลดังกล่าวเมื่อเลยระยะเวลาที่กำหนดหรือหมดความจำเป็นในการเก็บรวบรวมหรือเจ้าของข้อมูลเพิกถอนความยินยอม
3.2 แนวทางในการกำหนดมาตรการทางเทคนิคที่จำเป็นสำหรับการให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ

กำหนดให้มี Access Authorization System ซึ่งจะมีรายละเอียดเกี่ยวกับ:
(1) application procedures สำหรับการขออนุญาตให้เข้าถึงข้อมูลส่วนบุคคล

(2) กำหนดตัวผู้มีอำนาจในการอนุญาตหรืออนุมัติในแต่ละระดับอย่างเหมาะสม
(3) กำหนด User name และ Password สำหรับพนักงานที่มีสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
(4) มีการแจ้งเตือนถึงความจำเป็นในการรักษาความลับของ User name และPassword รวมทั้งการ log off ออกจากระบบภายหลังการใช้งาน ทั้งนี้เพื่อไม่ให้ลวงรู้ถึงบุคคลอื่นที่ไม่มีสิทธิในการเข้าถึงข้อมูลได้
(5) ควรมีแนวทางการจัดการ Password อย่างเหมาะสม (Password Management) เช่น การไม่ให้ใช้ Password ที่สามารถคาดเดาได้อย่างง่าย หรือบังคับให้มีการเปลี่ยน Password ทันทีเมื่อเข้าสู่ระบบครั้งแรก หรือในระยะเวลาหนึ่ง
ในกรณีที่ลูกค้าต้องการทราบข้อมูลเกี่ยวกับตัวเอง รวมทั้งข้อมูลการใช้บริการของตัวเอง องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรกำหนดแนวปฏิบัติให้ลูกค้าแต่ละรายต้องแจ้งข้อมูล หรือรายละเอียดที่สามารถระบุและยืนยันตัวตนของลูกค้าก่อนที่จะให้บริการข้อมูลแก่ลูกค้า
ควรจัดให้มีการตรวจสอบการเข้าถึงข้อมูลของลูกค้าของพนักงานเป็นระยะๆ อย่างสม่ำเสมอเพื่อเป็นการตรวจสอบการทำงานของพนักงานที่สามารถเข้าถึงข้อมูลของลูกค้า ทั้งนี้ข้อมูลการตรวจสอบดังกล่าวต้องเก็บรักษาไว้ชั่วระยะเวลาหนึ่งเพื่อประโยชน์ในการสืบสวนหรือสอบสวนหรือเพื่อกำหนดมาตรฐานในการเฝ้าระวัง
4) ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลมีหน่วยงานสาขาซึ่งอาจมีความจำเป็นที่จะต้องเข้าถึงข้อมูลในระบบคอมพิวเตอร์ขององค์กรธุรกิจหรือหน่วยงานเอกชนผ่านทางเครือข่ายคอมพิวเตอร์ องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องตรวจสอบว่าการเข้าถึงระบบข้อมูลดังกล่าวเป็นการเข้าถึงข้อมูลจากระบบคอมพิวเตอร์ที่ได้รับอนุญาตให้เชื่อมต่อและเข้าถึงข้อมูลหรือไม่ และในกรณีจำเป็นอาจต้องจัดให้มีการเข้ารหัสข้อมูลที่มีการรับ-ส่งระหว่างกัน ทั้งนี้เพื่อป้องกันการดักข้อมูลหรือการโจมตีข้อมูลโดยไม่ชอบ

5) ในกรณีการให้ความคุ้มครองข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับการใช้ Internet ควรดำเนินการดังนี้
(1) องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรดำเนินการตามขั้นตอนที่เหมาะสมสำหรับการจัดให้มีมาตรการหรือวิธีการที่สามารถรักษาความปลอดภัยของการส่งผ่านข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการบนเครือข่ายคอมพิวเตอร์สาธารณะ เช่น Internet
(2) ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลจัดให้มีระบบที่สามารถเข้าถึงหรือใช้ Internet ซึ่งรวมถึงการใช้ E-mail เพื่ออำนวยความสะดวกแก่ลูกค้า องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรแจ้งให้ลูกค้าทราบถึงนโยบายขององค์กรที่เกี่ยวกับการอนุญาตให้ใช้ระบบดังกล่าว รวมทั้งข้อสงวนสิทธิ์ขององค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลที่จะเข้าถึงหรืออ่าน E-mail ของลูกค้าที่ใช้ระบบ E-mail ขององค์กร

**6) ควรจัดให้มีวิธีการที่เหมาะสมเพื่อป้องกันไม่ให้มีการเข้าถึงหรือเปิดเผยข้อมูลต่าง ๆ ของลูกค้าที่จัดเก็บอยู่ในรูปของเอกสาร เช่น รายละเอียดที่ระบุไว้ในใบสมัครใช้บริการหรือในรายงานที่จัดพิมพ์จากระบบคอมพิวเตอร์ หรือเอกสารอื่น ๆ
7) สำเนาเอกสารแสดงตัวหรือยืนยันตัวบุคคลควรที่จะต้องมีการจัดเก็บเพียงเท่าที่จำเป็น และควรที่จะต้องถือปฏิบัติในลักษณะเดียวกันกับเอกสารที่ต้องเก็บรักษาเป็นความลับ และต้องจัดเก็บไว้ในสถานที่ที่มีความปลอดภัยและมีการจำกัดการเข้าถึง และไม่ควรเก็บรักษาไว้เป็นระยะเวลานานเกินความจำเป็น

3.3 แนวทางในการรักษาความปลอดภัยของสถานที่และอุปกรณ์

สถานที่ตั้งของระบบคอมพิวเตอร์แม้ว่าจะขายและเครื่องลูกขาย รวมทั้งสถานที่เก็บเอกสาร และอื่น ๆ ซึ่งเป็นสถานที่ที่สามารถเข้าถึงข้อมูลของลูกค้าได้โดยวิธีการใด ต้องจัดให้มีการควบคุม ดูแลการเข้าถึงอย่างปลอดภัยและเหมาะสม และโดยผู้มีอำนาจในการเข้าถึงเท่านั้น
องค์กรธุรกิจหรือหน่วยงานเอกชนผู้ให้บริการที่อนุญาตให้มีการจัดสรรเอกสารการสมัครใช้บริการผ่านทางเครื่องแฟกซ์ จะต้องระมัดระวังไม่ให้เครื่องแฟกซ์ที่ใช้ในการรับเอกสารติดตั้งอยู่ในสถานที่ที่ไม่มีการจำกัดการเข้าถึง
3.4 แนวทางปฏิบัติเกี่ยวกับพนักงานที่มีหน้าที่รับผิดชอบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

องค์กรธุรกิจหรือหน่วยงานเอกชนที่เก็บข้อมูลควรจัดให้มีการฝึกอบรมอย่างสม่ำเสมอเพื่อให้ความรู้เกี่ยวกับระบบการรักษาความปลอดภัยของข้อมูล รวมถึงการฝึกอบรมทางเทคนิคที่เกี่ยวข้องกับพนักงานของตน โดยเฉพาะพนักงานที่มีหน้าที่เกี่ยวข้องกับข้อมูลของลูกค้า รวมทั้งการจัดทำหนังสือประชาสัมพันธ์เพื่อแจ้งพนักงานทราบเพื่อเป็นการเตือนเตือนเป็นระยะ ๆ และอย่างสม่ำเสมอ
การรับพนักงาน ซึ่งโดยตำแหน่งหน้าที่ตอบรับ ความรับผิดชอบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ทางองค์กรธุรกิจหรือหน่วยงานเอกชนที่เก็บข้อมูลควรให้ความสำคัญกับเกณฑ์การคัดเลือกที่สามารถแสดงถึงความซื่อสัตย์และ/หรือ ความน่าเชื่อถือเฉพาะตัวของบุคคลที่สมัครงาน
องค์กรธุรกิจหรือหน่วยงานเอกชนที่เก็บข้อมูลต้องจัดให้มีการสังเกต ตรวจสอบ หรือ เฝ้าระวัง การปฏิบัติงานของพนักงานที่ถูกมอบหมายให้ปฏิบัติหน้าที่ที่มีความเสี่ยงต่อการกระทำที่มิชอบ ได้อย่างง่าย เช่น พนักงานที่มีหน้าที่จัดพิมพ์ข้อมูลของลูกค้ามากมายหรือสามารถดาวน์โหลดข้อมูลต่าง ๆ ของลูกค้าได้
3.5 การโอนข้อมูลส่วนบุคคลของลูกค้าหรือผู้ใช้บริการ
ในกรณีที่องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องมอบหมายหรือจ้างบุคคลที่สามให้ทำหน้าที่ในการให้บริการ ซ่อมแซมหรือบำรุงรักษา ซึ่งองค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลอาจต้องให้ข้อมูลที่จำเป็นของลูกค้าหรือผู้ใช้บริการต่อบุคคลดังกล่าวเพื่อประโยชน์ในการให้บริการ ซ่อมแซมหรือบำรุงรักษา องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลต้องเป็นผู้รับผิดชอบในกรณีที่เกิดความเสียหายต่อลูกค้าหรือผู้ใช้บริการเนื่องจากการกระทำของบุคคลดังกล่าว ในกรณีเช่นนี้
3.6 การทบทวนและประเมินระบบและมาตรการการรักษาความปลอดภัยที่มีอยู่

ในกรณีที่มีการเปลี่ยนแปลงสภาพแวดล้อมในการทำธุรกิจ หรือปรับเปลี่ยนเทคโนโลยี, บางครั้ง อาจทำให้มาตรการรักษาความปลอดภัยที่ใช้อยู่เดิมไม่มีความเหมาะสมกับความเปลี่ยนแปลงที่เกิดขึ้น องค์กรธุรกิจหรือหน่วยงานเอกชนที่จัดเก็บข้อมูลควรจัดให้มีการทบทวน และประเมินระบบและมาตรการการรักษาความปลอดภัยที่มีอยู่เพื่อให้สอดคล้องกับสภาพแวดล้อมของการทำธุรกิจหรือเทคโนโลยีที่เปลี่ยนแปลงไปด้วย

หมายเหตุ: พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (1) ได้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ดังต่อไปนี้:

(1) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย, เข้าถึง, ใช้, เปลี่ยนแปลง, แก้ไข , หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด

กล่าวโดยสรุป, สำหรับองค์กรธุรกิจ, การกำหนดหลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลและแนวปฏิบัติภายในองค์กรภาคเอกชนไม่เพียงแต่จะเป็นการตอบสนองต่อหน้าที่ของพนักงานที่เกี่ยวข้องเท่านั้น แต่ยังสะท้อนถึงภาพลักษณ์ที่ดีขององค์กรในสายตาของประชาชน, ลูกค้า หรือผู้ใช้บริการด้วย เนื่องจากเขาจะมั่นใจว่าข้อมูลส่วนบุคคลของเขาจะได้รับการดูแลและป้องกันอย่างเหมาะสม และไม่โดนละเมิด การกำหนดมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลทำให้ความเชื่อมั่นของประชาชนในทุกองค์กรยังคงได้รับการรักษาไว้ ถึงแม้ข้อมูลจะถูกส่งต่อหรือโอนข้ามองค์กร ลูกค้าหรือผู้ใช้บริการก็ยังคงมีความสบายใจ การกำหนดหลักเกณฑ์และแนวทางปฏิบัติข้างต้นเป็นเครื่องมือในการสร้างความน่าเชื่อถือในการประกอบธุรกิจ ทำให้ธุรกิจภาคเอกชนได้พัฒนาและก้าวหน้าในเชิงมาตรฐานสากล และเติบโตอย่างยั่งยืนในอนาคต.

อ้างอิง

PDPA Thailand
เราคือผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคลภายใต้ พระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) มีบริการหลากหลายที่ตอบโจทย์องค์กรทุกกลุ่ม
Our PDPA Services
PDPA Thailand Starter kit (New Arrival)
ชุดพื้นฐานรวม 8 สินค้า/บริการ “ถูกต้อง-ครบถ้วน-ปลอดภัย-คุ้มค่า” สำหรับองค์กรเริ่มต้นดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
PDPA Consultant
บริการที่ปรึกษาโดยผู้เชี่ยวชาญ PDPA พร้อมเป็นผู้ช่วยเปลี่ยนแปลง ขององค์กรคุณทุกย่างก้าว ให้มีการดำเนินงานที่สอดคล้องตามกฎหมายฯ
PDPA Compliance Audit สอบทานการดำเนินงานขององค์กรเกี่ยวกับเอกสารและการบริหารจัดการ ข้อมูลส่วนบุคคล เสริมความมั่นใจจาก 0 เป็น 100 ว่าถูกต้องตามกฎหมาย ลดความเสี่ยงละเมิดและโทษ
PDPA In-House Training บริการอบรมภายในด้วยหลักสูตรบรรยาย และ workshop ที่ออกแบบ เฉพาะองค์กรของคุณ โดยผู้เชี่ยวชาญจาก สถาบันพัฒนาและทดสอบ ทักษะดิจิทัล (DDTI)
PDPA Public Training
จัดอบรมและ Workshop กฎหมาย PDPA อย่างเจาะลึก ผู้เรียนสามารถ นำความรู้ไปปรับใช้ในดำเนินงานภายใต้กฎหมายได้อย่างถูกต้อง ครบทุกมิติ

Certification ทดสอบเพื่อรับวุฒิบัตรด้านการคุ้มครองข้อมูลส่วนบุคคลมาตรฐานสากล ICDL, DCT, DDTI

แบบฟอร์มการขอเผยแพร่ข้อมูลผ่านเว็บไซต์ของหน่วยงานในราชการบริหารส่วนกลาง สำนักงานปลัดกระทรวงสาธารณสุข
ตามประกาศสำนักงานปลัดกระทรวงสาธารณสุข

แบบฟอร์มการขอเผยแพร่ข้อมูลผ่านเว็บไซต์ของหน่วยงานในสังกัดโรงพยาบาลบ่อทอง

ชื่อหน่วยงาน : โรงพยาบาลบ่อทอง
วัน/เดือน/ปี : ๑๗ มกราคม ๒๕๖๕
หัวข้อ : .....

รายละเอียดข้อมูล ตามเอกสารแนบท้าย

Link **ภายนอก :** ไม่มี
หมายเหตุ : .....
.....
.....

ผู้รับผิดชอบการให้ข้อมูล	**ผู้อนุมัติรับรอง**
.....	.....
(.....)	(นางแววดาว พิมลธเรศ)
ตำแหน่ง	ผู้อำนวยการโรงพยาบาลบ้านบึง รักษาการในตำแหน่ง
วันที่ ๑๗ มกราคม ๒๕๖๖	ผู้อำนวยการโรงพยาบาลบ่อทอง
	วันที่...../...../.....

ผู้รับผิดชอบการนำข้อมูลขึ้นเผยแพร่

.....
(นายสิทธิชัย แสงจู)
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
วันที่...../...../.....