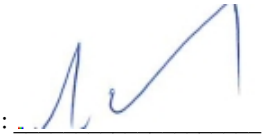
แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

(Guideline on Personal Data Protection)

สำหรับ

บริษัทชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน)

อนุมัติโดย : 

(Mr.Sung Choeng Tsoi)

ประธานเจ้าหน้าที่บริหาร

ประกาศใช้ครั้งที่ 00 ทบทวนครั้งที่ 00

วันที่ 29/04/65

แนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล

(1) คำนำ

ด้วยพัฒนาการทางด้านเทคโนโลยีสารสนเทศ และเทคโนโลยีด้านการสื่อสารเป็นไปอย่างรวดเร็ว ทำให้การเข้าถึงข้อมูลส่วนบุคคลสามารถทำได้โดยง่าย รวมถึงการใช้และการเปิดเผยข้อมูลส่วนบุคคล อันอาจนำมาซึ่งความเสียหายต่อเจ้าของข้อมูล บริษัทชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน) เคารพความเป็นส่วนตัวและตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้เป็นไปตามนโยบายคุ้มครองข้อมูลส่วนบุคคลของบริษัทชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล จึงได้จัดทำแนวปฏิบัติเกี่ยวกับฐานในการประมวลผลข้อมูลส่วนบุคคล เพื่อให้มีหลักเกณฑ์การกำกับดูแลการเก็บรวบรวม การใช้ การเปิดเผยและการบริหารจัดการการคุ้มครองข้อมูลส่วนบุคคลอย่างเหมาะสม

(2) คำนิยาม

บริษัท	หมายถึง บริษัทชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน)
ผู้ควบคุมข้อมูล	หมายถึง บริษัทชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน)
พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล	หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

(3) แนวปฏิบัติ

ตามมาตรา 24 ของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บัญญัติให้ความยินยอมเป็นฐานหลักในการประมวลผลข้อมูล ซึ่งความยินยอม (consent) เป็นฐานที่มีความสำคัญมากเนื่องจากเป็นสิ่งที่ทำให้เจ้าของข้อมูลสามารถ “เลือก” จัดการของข้อมูลของตนเองได้อย่างเต็มที่ที่สุด แต่ยังมีการประมวลผลอีกหลายประเภทที่ไม่สามารถอิงอยู่กับฐานความยินยอมได้ มาตรา 24 จึงกำหนดฐานอื่นๆไว้อีก 6 ฐาน คือ

(1) ฐานเอกสารประวัติศาสตร์ จดหมายเหตุและการศึกษาวิจัยหรือสถิติ (research)

(2) ฐานประโยชน์สำคัญต่อชีวิต (vital interest)

(3) ฐานสัญญา (contract)

(4) ภารกิจของรัฐ (public task)

(5) ฐานประโยชน์อันชอบธรรม (legitimate interest)

(6) ฐานการปฏิบัติตามกฎหมาย (legal obligation)

ซึ่งบริษัทอาจมีความจำเป็นในการอ้างอิงฐานต่างๆ เหล่านี้แตกต่างกันไปตามลักษณะของธุรกรรมที่เกี่ยวข้องกับข้อมูลส่วนบุคคล โดยจะต้องระบุฐานในการประมวลผลก่อนการเก็บรวบรวมข้อมูลส่วนบุคคล และอาจใช้มากกว่าหนึ่งฐานในการประมวลผลข้อมูลชุดเดียวกัน โดยการประมวลผลในฐานที่แตกต่างกันนั้นเจ้าของข้อมูลจะมีสิทธิแตกต่างกันไป

1. ฐานสัญญา (Contract)

1.1 กรณีที่การประมวลผลข้อมูลจำเป็นต่อการให้บริการตามสัญญาที่ตกลงกันไว้ระหว่างบริษัทและเจ้าของข้อมูลหรือเมื่อจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติตามคำขอของเจ้าของข้อมูลก่อนที่จะเข้าสู่การทำสัญญาใดๆหากใช้สัญญาดังกล่าวเป็นฐานในการประมวลผลแล้วก็ไม่ต้องขอความยินยอมเพิ่มเติม เช่น การทำสัญญาจ้างงานหลังจากทางบริษัทรับพนักงานเข้าทำงานแล้ว ฐานนี้ใช้ได้กับข้อมูลส่วนบุคคลทั่วไปเท่านั้น ข้อมูลอ่อนไหว (sensitive data) ใช้การทำตามสัญญาเป็นฐานในการประมวลผลไม่ได้

1.2 การประมวลผลข้อมูลบนฐานสัญญานี้จำกัดอยู่เฉพาะข้อมูลของเจ้าของข้อมูลส่วนบุคคลที่เป็นคู่สัญญาเท่านั้น การประมวลผลข้อมูลของบุคคลที่สามจะกระทำได้โดยใช้ฐานความยินยอม หรือฐานผลประโยชน์อันชอบธรรม (ซึ่งจะต้องมีการประเมินแล้วว่าผลประโยชน์ที่เกิดแก่คู่สัญญาหรือบริษัทนั้นไม่ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูลโดยไม่เกินขอบเขตที่ตัวเจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผลด้วย) ไม่ใช่ฐานสัญญา

1.3 ในกรณีที่ผู้ประมวลผลข้อมูลทำงานให้กับผู้ควบคุมข้อมูลโดยประมวลผลข้อมูลที่จำเป็นต่อการปฏิบัติตามสัญญานั้นๆ ถือเป็นการประมวลผลตามฐานสัญญา ดังนั้นผู้ประมวลผลข้อมูลไม่จำเป็นต้องขอความยินยอมเพิ่มเติมแต่อย่างใด

1.4 ผู้ควบคุมข้อมูลไม่ควรขอความยินยอมพร่ำเพรื่อเพราะจะทำให้คู่สัญญาเข้าใจผิดว่าสามารถถอนความยินยอมได้ทั้งที่ยังมีนิติสัมพันธ์ทางสัญญากันอยู่ และอาจนำไปสู่กรณีร้องเรียนและสูญเสียความเชื่อใจต่อกันโดยใช่เหตุได้

1.5 การประมวลผลข้อมูลนั้นอาจเกิดขึ้นโดยใช้ฐานสัญญาที่มีมากกว่าหนึ่งฉบับ

1.6 ในกรณีที่สามารถปฏิบัติหน้าที่ตามสัญญาหรือตามคำขอได้โดยไม่ต้องประมวลผลข้อมูลส่วนบุคคลถือว่า “ไม่จำเป็น” ดังนั้นผู้ควบคุมข้อมูลควรประเมินขอบเขตของสัญญาให้แน่ชัด เพื่อจะได้ทราบถึงขอบเขตของข้อมูลที่จำเป็นในการปฏิบัติตามสัญญา อีกทั้ง การประมวลผลข้อมูลเพื่อการปฏิบัติตามสัญญาจะต้องเป็นไปอย่างเฉพาะเจาะจงตามที่ระบุในสัญญานั้นๆ ซึ่งไม่รวมถึงการประมวลผลข้อมูลนั้นเป็นไปเพื่อให้เกิดผลดีกับธุรกิจโดยรวม

1.7 “ความจำเป็น” ในที่นี้จำกัดอยู่แค่เพียง “การปฏิบัติตามสัญญา” ตามปกติของการดำเนินงานให้เป็นไปตามสัญญาเท่านั้น ไม่รวมถึงกรณีที่เกิดปัญหาหรือข้อพิพาทที่เกี่ยวข้องกับสัญญานั้น ผู้ควบคุมข้อมูลต้องอ้างฐานอื่น เช่นฐานผลประโยชน์อันชอบธรรม หรือฐานความยินยอม

2. ฐานความยินยอม (Consent)

2.1 ความยินยอมเป็นฐานในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลได้สมัครใจ “เลือก” ที่จะยินยอมให้ผู้ควบคุมข้อมูลประมวลผลได้ โดยหากต้องการใช้ความยินยอมเป็นฐานในการประมวลผล ผู้ควบคุมข้อมูลจะต้องเชิญชวนให้เจ้าของข้อมูลยอมรับหรืออนุญาตให้มีการประมวลผลข้อมูลส่วนบุคคลนั้นๆได้ โดยมั่นใจว่าเป็นสถานการณ์ที่เจ้าของข้อมูลเลือกที่จะปฏิเสธได้จริง และหากเจ้าของข้อมูลเลือกที่จะปฏิเสธผู้ควบคุมข้อมูลก็ไม่สามารถประมวลผลได้

2.2 ความยินยอมจะต้องไม่เป็นเงื่อนไขในการรับบริการ หรือผูกติดอยู่กับความจำเป็นในการปฏิบัติตามสัญญา การใช้ฐานความยินยอมจึงต้องกระทำโดยความระมัดระวัง อีกทั้ง ควรตระหนักว่าผู้ควบคุมข้อมูลจะมีภาระพิสูจน์ว่าเจ้าของข้อมูลนั้นได้เลือกที่จะยินยอมโดยสมัครใจจริงๆ และความยินยอมของเจ้าของข้อมูลไม่ใช่ใบอนุญาตให้ทำอะไรกับข้อมูลนั้นก็ได้ การประมวลผลข้อมูลบนฐานของความยินยอมยังต้องยึดตามหลักความจำเป็น และต้องทำให้เนื้อหาของข้อมูลถูกต้องด้วย

2.3 ด้วยลักษณะที่ยึดโยงอยู่กับความสมัครใจของเจ้าของข้อมูลส่วนบุคคล ซึ่งจะต้องสอดคล้องกับเงื่อนไขที่กำหนดไว้ในมาตรา 19 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ความยินยอมจึงเป็นฐานการประมวลผลที่มีความเสี่ยงมาก เพราะอาจต้องหยุดประมวลผลเมื่อใดก็ตามที่เจ้าของข้อมูลถอนความยินยอมไป ดังนั้น หากการประมวลผลข้อมูลส่วนบุคคลเป็นไปเพื่อความจำเป็นในการปฏิบัติตามสัญญาโดยแท้จริง ไม่มีความจำเป็นใดๆ ที่จะต้องขอความยินยอมอีก

2.4 ความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น ผู้ควบคุมข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนจึงจะเก็บรวบรวม ใช้ เปิดเผยข้อมูลนั้นๆ ได้

2.5 ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ ผู้ควบคุมข้อมูลจะไม่นำฐานความยินยอม(consent) กับฐานการปฏิบัติตามสัญญา (contract) มาปะปนกัน ดังนั้นจะต้องแยกแยะให้ได้ว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาและข้อมูลใดไม่จำเป็น

2.6 ผู้ควบคุมข้อมูลต้องระบุชี้แจงประโยชน์ที่จะเกิดขึ้นแก่ตนและแก่เจ้าของข้อมูลหากได้รับความยินยอม เช่นลดขั้นตอนและระยะเวลาในการตรวจสอบตัวตน เป็นต้น อีกทั้งการอธิบายเกี่ยวกับมาตรการที่จะช่วยสร้างความปลอดภัยให้กับข้อมูลที่ได้รับความยินยอมให้ประมวลผลนั้นก็อาจช่วยทำให้เจ้าของข้อมูลมีความไว้วางใจและยินยอมให้ประมวลข้อมูลได้ง่ายขึ้น

2.7 ความยินยอมต้องอยู่แยกส่วนกับกับเงื่อนไขในการให้บริการ การขอความยินยอมจะต้องไม่แสร้งว่าเป็นส่วนหนึ่งของสัญญาหรือเงื่อนไขในการให้บริการ หรือทำให้เข้าใจผิดว่าหากไม่ให้ความยินยอมแล้วจะไม่ได้รับบริการโดยเฉพาะในกรณีที่การประมวลผลข้อมูลนั้นไม่จำเป็นสำหรับการให้บริการตามสัญญานั้นๆ ซึ่งหากการประมวลผลข้อมูลนั้นจำเป็นสำหรับการให้บริการให้ไปใช้ฐานสัญญา

2.8 วัตถุประสงค์ของการประมวลผลข้อมูลต้องเฉพาะเจาะจง วัตถุประสงค์ในการประมวลข้อมูลแต่ละอย่างต้องชัดเจนและเฉพาะเจาะจง ผู้ควบคุมข้อมูลไม่สามารถเติมวัตถุประสงค์ใหม่เองได้โดยไม่ขอความยินยอมใหม่ การประมวลผลหลายอย่างเพื่อวัตถุประสงค์เดียวกันสามารถรวมอยู่ในความยินยอมครั้งเดียว แต่หากใช้ข้อมูลชุดเดียวกันเพื่อประมวลผลหลายวัตถุประสงค์ ต้องให้เจ้าของข้อมูลมีทางเลือกได้ว่ายินยอมสำหรับวัตถุประสงค์ใดบ้าง

2.9 ความยินยอมต้องชัดเจนไม่คลุมเครือ การให้ความยินยอมต้องเกิดขึ้นโดยสมัครใจและเป็นการเลือกของเจ้าของข้อมูลเสมอ ดังนั้นเพื่อให้เจ้าของข้อมูลสามารถ “เลือก” ได้อย่างแท้จริงจึงต้องออกแบบให้เจ้าของข้อมูลต้องมีการกระทำที่ให้ความยินยอมอย่างชัดเจน (clearaffirmative action) จะต้องไม่ขอความยินยอมในลักษณะที่กำหนดไว้แล้วล่วงหน้า การเงียบเฉยหรือการเช็คถูกในช่องไว้ก่อน (pre-ticked box) ไม่ถือเป็นความยินยอมที่ชัดเจน

2.10 การเคลื่อนไหวทางกายภาพ (physical motion) อาจถือเป็นการกระทำที่ให้ความยินยอมอย่างชัดเจน (clear affirmative action) ได้ แต่ต้องออกแบบให้ลำดับขั้นตอนการขอความยินยอม (consent flow) นั้นให้ข้อมูลชัดว่าพฤติกรรมแต่ละอย่างนั้นหมายถึงอะไร เป็นการให้ความยินยอมสำหรับวัตถุประสงค์ใด และผู้ควบคุมข้อมูลต้องเก็บข้อมูลได้ด้วยว่าใช้วิธีใดในการขอความยินยอม อีกทั้งควรระมัดระวังไม่ให้เกิดความเหนื่อยล้าจากการคลิกให้ความยินยอมมากจนเกินไป (click fatigue) ทำให้การให้ความยินยอมแต่ละครั้งไม่มีความหมายที่แท้จริง

2.11 ออกแบบทางเลือกให้สามารถปฏิเสธที่จะให้ความยินยอมได้ หรือมีโอกาสถอนความยินยอมได้โดยไม่ได้รับผลกระทบมากเกินเหตุ ผู้ควบคุมข้อมูลต้องประเมินและแยกแยะให้ชัดเจนว่าข้อมูลใดจำเป็นสำหรับการปฏิบัติตามสัญญาอีกทั้งการถอนความยินยอมจะต้องจะกระทำได้ง่ายในระดับเดียวกันกับการให้ความยินยอม

2.12 เนื้อหาความยินยอมเข้าใจง่ายและเข้าถึงง่าย การขอความยินยอมจะต้องมีรายละเอียดข้อมูลต่างๆอย่างครบถ้วน แต่เนื้อหาจะต้องไม่ยาวจนเกินไป โดยอาจใช้เทคนิคเสริม เช่นFAQs, pop-up screen, chatbot ที่ทำให้การให้ข้อมูลนั้นชัดเจนมากขึ้น การให้ข้อมูลอาจกระทำได้หลายรูปแบบ ทั้งข้อเขียน ปากเปล่า วิดีโอ ข้อความเสียง หรือข้อความอิเล็กทรอนิกส์ก็ได้ ตราบใดที่ข้อมูลเหล่านั้นสามารถเข้าถึงได้ง่ายและมีความชัดเจนแยกออกจากเนื้อหาเรื่องอื่นๆ ผู้ควบคุมข้อมูลควรทดสอบด้วยว่าเนื้อหาสามารถอ่านเข้าใจได้ง่ายและไม่แตกต่างไปจากความคาดหมายปกติสำหรับคนทั่วไป อีกทั้งต้องคำนึงถึงอายุของผู้ให้ความยินยอมว่าภาษาที่ใช้นั้นเหมาะสมกับระดับความสามารถในการเข้าใจในบริบทนั้นๆด้วยหรือไม่ การอธิบายด้วยภาพเคลื่อนไหวหรือรูปภาพหรือ infographic เป็นที่นิยมเพราะสามารถช่วยอำนวยความเข้าใจได้โดยเฉพาะในกรณีของการขอความยินยอมจากผู้เยาว์

2.13 การขอความยินยอมแบบชัดแจ้ง (Explicit Consent) สำหรับข้อมูลที่อ่อนไหว การประมวลผลข้อมูลที่อ่อนไหวใช้การทำตามสัญญาเป็นฐานไม่ได้ จึงต้องใช้ฐานความยินยอมหรือฐานภารกิจของหน่วยงานรัฐ หรือฐานประโยชน์อันชอบธรรมเป็นหลัก ผู้ควบคุมข้อมูลควรขอความยินยอมเป็นข้อเขียน และอาจให้ลงลายมือชื่อกำกับไว้ด้วยเพื่อลดความเสี่ยง หากเป็นการขอความยินยอมด้วยช่องทางอิเล็กทรอนิกส์ อาจใช้วิธีอื่นๆเช่น ส่งอีเมล์ อัพโหลดเอกสารสแกนที่มีลายมือชื่อ หรือใช้ลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น

2.14 การให้ความยินยอมปากเปล่าก็เป็นความยินยอมแบบชัดแจ้งได้ แต่อาจยากต่อการพิสูจน์ ในกรณีของโทรศัพท์อาจทำได้หากให้ข้อมูลเพียงพอ มีทางเลือก และเนื้อหาชัดเจน

2.15 เนื้อหาของการขอความยินยอม การขอความยินยอมอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้เป็นหลัก

ใคร?	☐ ข้อมูลเกี่ยวกับตัวผู้ควบคุมข้อมูล (ชื่อ ที่อยู่ DPO ฯลฯ)
อะไร?	☐ วัตถุประสงค์การประมวลผลที่ชัดเจนและเฉพาะเจาะจง ☐ ข้อมูลใดบ้างที่จะถูกเก็บรวบรวมและใช้
อย่างไร?	☐ วิธีการประมวลผลข้อมูล ☐ การใช้ระบบตัดสินใจอัตโนมัติ หรือ โปรไฟลิ่ง (profiling) (หากมี) ☐ การโอนข้อมูลไปต่างประเทศ ☐ การเปิดเผยข้อมูลต่อบุคคลอื่น
เมื่อไร?	☐ ระยะเวลาในการจัดเก็บข้อมูล
หากมีปัญหา?	☐ วิธีการถอนความยินยอม ☐ สิทธิต่างๆ ของเจ้าของข้อมูล โดยเฉพาะสิทธิในการถอนความยินยอม

2.16 ข้อควรระวังในการจัดการความยินยอม ผู้ควบคุมข้อมูลพึงระวังในการจัดการความยินยอมโดยเฉพาะประเด็นดังต่อไปนี้

(1) ขอความยินยอมเมื่อจำเป็นต้องประมวลผลข้อมูลนั้นเท่านั้น

(2) บันทึกเนื้อหาข้อมูลที่แจ้งตอนขอความยินยอม และวิธีการให้ความยินยอม

(3) แยกประเภทและขอบเขตของความยินยอมรายบุคคลเอาไว้

(4) กำหนดการตรวจสอบความเหมาะสมและขอบเขตของความยินยอมเมื่อผ่านไประยะหนึ่ง

(5) กระบวนการถอนความยินยอมต้องชัดเจน ไม่ยุ่งยากกว่าตอนที่ให้ความยินยอม

(6) เตรียมพร้อมเพื่อตอบสนองต่อคำขอการใช้สิทธิของเจ้าของข้อมูล โดยเฉพาะการถอนความยินยอมได้อย่างรวดเร็ว

(7) ต้องไม่ลงโทษหรือทำให้เจ้าของข้อมูลเสียประโยชน์เมื่อถอนความยินยอม

2.17 มาตรา 95 ของพ.ร.บ. คุ้มครองข้อมูลสวนบุคคล อนุญาตให้ประมวลผลข้อมูลบนฐานของความยินยอมที่เกิดขึ้นก่อนพระราชบัญญัติจะมีผลบังคับใช้ได้ตามขอบเขตวัตถุประสงค์เดิมซึ่งเป็นจุดที่มีความยืดหยุ่นแตกต่างจาก GDPR แม้ว่าความยินยอมนั้นจะเก็บรวบรวมอย่างไม่ตรงตามเงื่อนไขอื่นๆ ของมาตรา 19 ทั้งหมดก็ตาม แต่ผู้ควบคุมข้อมูลจะต้องประชาสัมพันธ์ให้สามารถถอนความยินยอมได้โดยง่ายด้วย

2.18 “การกำหนดวิธีการยกเลิกความยินยอม และเผยแพร่ประชาสัมพันธ์ให้เจ้าของข้อมูลส่วนบุคคลที่ไม่ประสงค์ให้ผู้ควบคุมข้อมูลส่วนบุคคลเก็บรวมรวม และใช้ข้อมูลสาวนบุคคลดังกล่าวสามารถแจ้งยกเลิกความยินยอมได้โดยง่าย” นั้นอาจทำได้โดยเผยแพร่ช่องทางการยกเลิกความยินยอม เช่น ทางเว็บไซต์ของผู้ควบคุมข้อมูล พร้อมกันนั้นควรแจ้งแนวปฏิบัติเรื่องการคุ้มครองข้อมูลส่วนบุคคล ที่สอดคล้องกับกฎหมายปัจจุบันเพื่อลดความเสี่ยง และสร้างความ

น่าเชื่อถือให้แก่องค์กรด้วย ซึ่งอาจช่วยให้เจ้าของข้อมูลส่วนบุคคลตัดสินใจไม่ยกเลิกความยินยอม หรือ ไม่ opt-out ออกไป

2.19 ในกรณีที่ความยินยอมที่เก็บไว้ก่อนหน้ากฎหมายจะมีผลบังคับใช้นั้นมีขอบเขตวัตถุประสงค์ที่กว้างขวาง คลุมเครือจนขัดแย้งกับมาตรา 19 โดยชัดแจ้ง เช่น เป็นการขอความยินยอมแบบเหมารวมทุกกรณี หรือเป็นการขอความยินยอมแบบไม่แยกระหว่างฐานความยินยอมกับฐานสัญญา ต้องถือว่าความยินยอมนั้นมีผลเฉพาะส่วนที่ขอบเขตวัตถุประสงค์ชัดเจนเท่านั้น

2.20 การอ้างอิงความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้นั้นมีความเสี่ยงค่อนข้างมาก โดยเฉพาะหากความยินยอมนั้นมีขอบเขตวัตถุประสงค์ที่กว้างขวางคลุมเครือ จนมีลักษณะขัดแย้งกับมาตรา 19 โดยอย่างเห็นได้ชัด จึงควรปรับปรุงโดยขอความยินยอมใหม่จากเจ้าของข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติให้ได้มากที่สุด เพื่อป้องกันปัญหาความไม่ไว้วางใจหรือการร้องเรียนที่อาจตามมา

2.21 การขอความยินยอมใหม่นั้นย่อมทำได้ไม่ยากสำหรับผู้ที่มีการติดต่อสื่อสารกันเป็นประจำอยู่แล้วการอ้างความยินยอมเก่าที่เก็บรวบรวมไว้ก้อนพระราชบัญญัติจะมีผลบังคับใช้นั้นควรทำเฉพาะในกรณีของเจ้าของข้อมูลที่ติดต่อเพื่อขอความยินยอมใหม่ได้ยากและจำเป็นต้องประมวลผลข้อมูลของลูกค้ารายนั้นจริงๆ เท่านั้น

2.22 แม้กฎหมายไทยจะอนุญาตให้สามารถใช้ความยินยอมที่เก็บรวบรวมไว้ก่อนพระราชบัญญัติจะมีผลบังคับใช้ แต่ GDPR กำหนดไว้ชัดเจนว่าไม่สามารถอ้างอิงได้ ดังนั้นผู้ควบคุมข้อมูลที่ประมวลผลข้อมูลส่วนบุคคลของคนสหภาพยุโรป หรือมีการดำเนินธุรกรรมกับสหภาพยุโรปจะต้องไม่อ้างอิงความยินยอมที่เก็บรวบรวมไว้ก่อน GDPR จะมีผลบังคับใช้ แต่หากผู้ควบคุมข้อมูลได้ขอความยินยอมใหม่ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทยแล้ว ความเสี่ยงในส่วนนี้ก็จะลดน้อยลงไปเนื่องจากแนวทางเงื่อนไขความยินยอมของกฎหมายไทยนั้นสอดคล้องกับ GDPR

2.23 เนื่องจากความยินยอมจะต้องเกิดขึ้นโดยสมัครใจอย่างแท้จริง ในกรณีที่อำนาจต่อรองของผู้ควบคุมข้อมูลและเจ้าของข้อมูลแตกต่างกันมากๆ จึงมักใช้ความยินยอมเป็นฐานไม่ได้ เช่น ในกรณีของการดำเนินภารกิจหน่วยงานของรัฐ และความสัมพันธ์ระหว่างนายจ้างกับลูกจ้างยกเว้นแต่ในกรณีที่เจ้าของข้อมูลสามารถมีทางเลือกในการปฏิเสธที่จะไม่ให้ข้อมูลได้จริงๆ

2.24 การประมวลผลข้อมูลเพื่อการทำการตลาดแบบตรงต้องใช้ฐานความยินยอมเป็นหลัก ไม่สามารถใช้ฐานอื่นโดยเฉพาะฐานผลประโยชน์อันชอบธรรมได้ การติดต่อเพื่อการตลาดแบบตรงนั้นแตกต่างไปจากการส่งใบปลิวหรือการโฆษณาทั่วไปในพื้นที่ใดพื้นที่หนึ่งแบบไม่เฉพาะเจาะตัวผู้รับ เนื่องจากเป็นการติดต่ออย่างเฉพาะเจาะจงจึงรุกล้ำความเป็นส่วนตัวและไม่ใช่สิ่งที่คนทั่วไปคาดหวังจะให้เกิดขึ้นโดยมิได้ร้องขอ ดังนั้นการบริหารจัดการข้อมูลภายในองค์กรก็จะต้องจะต้องแยกแยะออกจากข้อมูลที่ใช้ในการทำโฆษณาแบบไม่เฉพาะเจาะจงด้วย

2.25 ความยินยอมเพื่อการทำการตลาดแบบตรงนั้นต้องเป็นไปอย่างเฉพาะเจาะจง ไม่แอบแฝงในรูปของวัตถุประสงค์อื่นจะต้องกระทำในลักษณะของ opt-in คือให้เจ้าของข้อมูลส่วนบุคคลเลือกได้อย่างชัดเจน ซึ่งในการขอความยินยอม

นั้นควรแจกแจงวิธีการในการส่งข้อมูลเพื่อทำการตลาดแบบตรงด้วย (ทางอีเมล์โทรศัพท์ จดหมาย ฯลฯ) ซึ่งหากให้เจ้าของข้อมูลส่วนบุคคลเลือกวิธีการรับข้อมูลด้วยก็อาจทำให้โอกาสการได้ความยินยอมเพิ่มมากขึ้น (เนื่องจากบางคนอาจไม่รู้สึกรำคาญหากได้รับอีเมล์การตลาดแบบตรง แต่ไม่ต้องการรับโทรศัพท์ เป็นต้น)

2.26 เมื่อมีการติดต่อเจ้าของข้อมูลส่วนบุคคลเพื่อทำการตลาดแบบตรง ต้องเปิดโอกาสให้เจ้าของข้อมูลถอนความยินยอม หรือ opt-out ออกได้โดยง่ายด้วย

2.27 หากมีความจำเป็นต้องส่งต่อข้อมูลไปยังบุคคลที่สามเพื่อให้ช่วยประมวลผลข้อมูลหรือเพื่อให้ทำการตลาดให้ จะต้องตรวจสอบว่าเป็นบุคคลที่สามารถไว้วางใจได้ และจะปฏิบัติกับข้อมูลส่วนบุคคลด้วยมาตรฐานการคุ้มครองข้อมูลที่เหมาะสมตามหน้าที่ของผู้ควบคุมข้อมูลที่ต้องตรวจสอบและกำกับการทำงานของผู้ประมวลผลข้อมูล อีกทั้งต้องแจ้งการเปิดเผยข้อมูลต่อบุคคลเหล่านั้นด้วย และต้องบันทึกรายละเอียดของความยินยอมไว้เสมอ

2.28 การทำการตลาดแบบตรงที่ไม่ได้มีลักษณะรุกล้ำความเป็นส่วนตัวมากและผู้บริโภคสามารถคาดหมายได้อยู่แล้วอาจใช้ฐานผลประโยชน์อันชอบธรรมได้แต่การเสนอขายสินค้าโดยตรงหรือโฆษณาแบบเจาะจง (targeted advertisement) ที่ต้องอาศัยข้อมูลที่เฉพาะเจาะจงรายบุคคล หรือข้อมูลในลักษณะโปรไฟลิ่ง ที่ทำให้ผู้โฆษณาทราบถึงข้อมูลส่วนบุคคลของเป้าหมายอย่างละเอียดนั้นย่อมไม่อาจใช้ฐานผลประโยชน์อันชอบธรรมได้ ต้องใช้ฐานความยินยอม

2.29 การใช้ข้อมูลเครือข่ายสังคม (social network) เพื่อกระตุ้นยอดขายจำเป็นต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เพราะไม่ใช่การประมวลผลที่จำเป็นสำหรับการปฏิบัติตามสัญญา การขอความยินยอมต้องทำโดยแจ้งวัตถุประสงค์ชัดเจน การนำข้อมูลไปใช้ประโยชน์ต้องเป็นไปตามที่แจ้งเท่านั้น และควรแจ้งให้ชัดเจนว่าขอข้อมูลใดบ้าง ซึ่งหากสามารถอธิบายได้ชัดเจนว่าจะนำข้อมูลนั้นไปใช้งานอะไร

2.30 เนื่องจากข้อมูลเครือข่ายสังคม (เช่น รายชื่อเพื่อน รายชื่อในสมุดโทรศัพท์) ควรต้องระมัดระวังอย่างยิ่งยวดในการไม่เปิดเผยข้อมูลต่อบุคคลที่สามโดยไม่จำเป็น ควรออกแบบค่าพื้นฐาน (default) เป็นการไม่เปิดเผยไว้ก่อน แล้วค่อยให้ผู้ใช้เลือกที่จะเปิดเผยเอง (opt-in)

2.31 การสร้างข้อมูลโปรไฟล์ (profiling) ของเป้าหมายที่ต้องการทำการโฆษณาจากข้อมูลการใช้บริการออนไลน์ เช่น ข้อมูล cookies หรือ IP Address หรือ Location นั้นมีลักษณะที่รุกล้ำความเป็นส่วนตัวและมักไม่อาจคาดหมายได้อย่างสมเหตุสมผล ไม่ว่าจะเป็นข้อมูลโปรไฟล์ที่รวบรวมจากพฤติกรรมโดยตรง หรือข้อมูลโปรไฟล์ที่เกิดจากการทำนายพฤติกรรม ดังนั้น การขอความยินยอมจึงต้องยิ่งกระทำอย่างรัดกุม อีกทั้งเจ้าของข้อมูลส่วนบุคคลยังมีสิทธิที่จะคัดค้านการประมวลผลเพื่อทำโปรไฟล์ลิ่งได้อีกด้วย

2.32 การขอความยินยอมจากผู้เยาว์นั้นจะต้องคำนึงถึงเงื่อนไขของประมวลกฎหมายแพ่งตามที่มาตรา 20 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลกำหนดไว้ อีกทั้งผู้ควบคุมข้อมูลยังต้องระวังเป็นพิเศษ เนื่องจากโดยทั่วไปแล้วผู้เยาว์มีความสามารถในการเข้าใจวัตถุประสงค์และรายละเอียดของการประมวลผลข้อมูลไม่เท่ากับบุคคลที่บรรลุนิติภาวะแล้ว หรืออาจยังไม่มีความสามารถในเลือกหรือตัดสินใจตามความต้องการของตนเองได้อย่างเต็มที่ รวมถึง

การประเมินผลกระทบจากการให้ความยินยอมต่อผู้เยาว์ในอนาคตนั้นก็ทำได้ยาก ทำให้ความยินยอมที่ได้มาจากผู้เยาว์นั้นอาจกลายเป็นความยินยอมที่ไม่สมบูรณ์ตามเงื่อนไขของมาตรา19

2.33 นอกเหนือจากการใช้ภาษาที่ผู้เยาว์สามารถเข้าใจได้ง่ายแล้ว ยังอาจพิจารณาใช้เครื่องมือในการป้องกันไม่ให้เกิดการเก็บข้อมูลส่วนบุคคลของผู้เยาว์โดยไม่สมควร เช่น สอบถามว่าผู้ใช้บริการอายุเกินเกณฑ์แล้วหรือไม่ หรือแจ้งเตือนให้มีผู้ปกครองให้ความยินยอม หรือกำหนดให้มีการตั้งค่าโดยผู้ปกครอง (parental setting หรือ parental mode) ในการใช้บริการเพื่อป้องกันมิให้ผู้เยาว์ให้ข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์

2.34 ข้อจำกัดเกี่ยวกับความสามารถในการให้ความยินยอมของผู้เยาว์นั้นเป็นเรื่องที่มีความสำคัญมาก GDPR จึงให้ความคุ้มครองผู้เยาว์เป็นพิเศษในกรณีของการใช้ความยินยอมเป็นฐานในการประมวลผลสำหรับการบริการออนไลน์ประเภท Information Society Services เช่น บริการเกมออนไลน์ การขายสินค้าออนไลน์ ที่มุ่งให้บริการแก่ผู้เยาว์โดยตรง โดยให้ผู้ควบคุมข้อมูลต้องได้รับความยินยอมจากผู้ปกครองจากผู้เยาว์ที่อายุต่ำกว่า 16 ปี หรือต่ำกว่า 13 ปีหากมีกฎหมายภายในของประเทศนั้นๆ กำหนดไว้ (แต่หากเป็นการประมวลผลบนฐานอื่นๆ เช่นฐานสัญญานั้นก็สามารถทำได้ โดยต้องคำนึงถึงข้อจำกัดเกี่ยวกับความสามารถของผู้เยาว์ตามกฎหมายแพ่ง)

3. ฐานประโยชน์สำคัญต่อชีวิต (Vital Interest)

3.1 กรณีที่การประมวลผลข้อมูลมีความจำเป็นต่อการปกป้องประโยชน์สำคัญของเจ้าของข้อมูลหรือบุคคลอื่น เช่น ป้องกันอันตรายร้ายแรงอันอาจเกิดต่อสุขภาพและชีวิตด้วยการประมวลผลข้อมูลสุขภาพหรือข้อมูลอ่อนไหว (sensitive data) ผู้ประกอบการจะสามารถใช้ฐานนี้ในการประมวลผลได้เฉพาะในกรณีที่เจ้าของข้อมูลอยู่ในสภาวะที่ไม่สามารถให้ความยินยอมได้ และไม่มีวิธีอื่นที่สามารถปกป้องชีวิตบุคคลอื่นโดยไม่ต้องประมวลผลข้อมูลนี้แล้ว

4. ฐานหน้าที่ตามกฎหมาย (Legal Obligation)

4.1 กรณีการประมวลผลข้อมูลจำเป็นต้อการปฏิบัติหน้าที่ที่ผู้ควบคุมข้อมูลนั้นมีตามที่กฎหมายกำหนด ผู้ควบคุมข้อมูลจะต้องระบุได้อย่างชัดเจนว่ากำลังปฏิบัติหน้าที่ตามบทบัญญัติใดของกฎหมาย หรือทำตามคำสั่งของหน่วยงานใดของรัฐที่มีอำนาจ

4.2 ฐานนี้จะใช้ไม่ได้หากผู้ควบคุมข้อมูลสามารถใช้ดุลยพินิจได้ว่าจะประมวลผลข้อมูลนี้เพื่อทำตามกฎหมาย หรือมีทางเลือกอื่นที่เหมาะสมในการปฏิบัติตามกฎหมายนอกเหนือจากการประมวลผลข้อมูลส่วนบุคคล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ โอนย้ายข้อมูล หรือคัดค้านการประมวลผล

5. ฐานภารกิจของรัฐ (Public Task)

5.1 กรณีที่การประมวลผลข้อมูลจำเป็นต่อการดำเนินงานตามภารกิจของรัฐเพื่อประโยชน์สาธารณะที่กำหนดไว้ตามกฎหมาย โดยอำนาจหน้าที่อันเป็นที่มาของภารกิจจะต้องมีความชัดเจนโดยสามารถอ้างอิงถึงกฎหมายที่ให้อำนาจได้อย่างเฉพาะเจาะจง

5.2 ฐานนี้ใช้ไม่ได้ในกรณีที่สามารถดำเนินงานตามภารกิจของรัฐได้โดยไม่จำเป็นต้องประมวลผลข้อมูลส่วนบุคคล

5.3 การประมวลผลบนฐานภารกิจของรัฐไม่ได้ให้อำนาจโดยไร้เงื่อนไข หลักการความได้สัดส่วนยังเป็นเงื่อนไขสำคัญและมีหน้าที่ของผู้ควบคุมข้อมูลที่ต้องปฏิบัติตามอยู่เช่นเดียวกับฐานอื่นๆ โดยเฉพาะในเรื่องที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล ในกรณีที่ประมวลผลตามฐานนี้ เจ้าของข้อมูลจะไม่มีสิทธิในการลบ และโอนย้ายข้อมูล แต่มีสิทธิในคัดค้านการประมวลผล อนึ่ง ในกรณีที่เป็นการประมวลผลโดยหน่วยงานของรัฐ จำเป็นต้องพิจารณาหลักความจำเป็นในพระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. 2540 มาตรา 23(1) ประกอบ อีกทั้งต้องสอดคล้องกับหลักการของรัฐธรรมนูญมาตรา 77 เรื่องหลักความจำเป็นในการใช้เครื่องมือทางกฎหมายและการใช้อำนาจรัฐ รวมถึงการประเมินผลกระทบของการออกกฎเกณฑ์ทางกฎหมาย (Regulatory Impact Assessment - RIA) ควรคำนึงถึงผลกระทบต่อความเป็นส่วนตัวของข้อมูลส่วนบุคคลด้วย

5.4 แม้มาตรา 4 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลจะยกเว้นการบังคับใช้กับกิจกรรมของรัฐบางประการ แต่ก็ยังกำหนดให้การมีการจัดการรักษาความมั่นคงปลอดภัยตามมาตรฐานตามวรรค 3 ของมาตราเดียวกันด้วย และไม่ได้ยกเว้นหน้าที่ของทั้งองค์กร ซึ่งในความเป็นจริงแล้ว กิจกรรมของภาครัฐส่วนใหญ่นั้นสามารถใช้ฐานภารกิจของรัฐในการประมวลผลได้อยู่แล้ว หากการประมวลผลข้อมูลเกิดขึ้นโดยปฏิบัติตามมาตรฐานของการใช้ฐานภารกิจของรัฐก็จะลดความเสี่ยงของผู้ควบคุมข้อมูลลง

6. ฐานประโยชน์อันชอบธรรม (Legitimate Interest)

6.1 ผู้ประกอบการอาจประมวลผลข้อมูลส่วนบุคคลในกรณีที่จำเป็นต้อการดำเนินการเพื่อประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลและบุคคลอื่น โดยไม่เกินขอบเขตที่เจ้าของข้อมูลสามารถคาดหมายได้อย่างสมเหตุสมผล เช่น การป้องกันอาชญากรรมและการฉ้อโกง การส่งต่อในเครือบริษัทเพื่อการบริหารจัดการภายในองค์กรที่ไม่รวมการส่งไปต่างประเทศ การรักษาความปลอดภัยของระบบและเครือข่าย การช่วยเหลือเจ้าหน้าที่รัฐในการปฏิบัติภารกิจในลักษณะที่ไม่ขัดกับหน้าที่ในการรักษาความลับ การปฏิบัติตามกฎหมายของต่างประเทศที่จำเป็น เป็นต้น

6.2 การใช้ฐานประโยชน์อันชอบธรรม (legitimate interest) ในการประมวลผลข้อมูลทำให้มีขอบเขตค่อนข้างกว้างและค่อนข้างยืดหยุ่นในการปรับใช้ ดังนั้นผู้ควบคุมข้อมูลจะต้องใช้ดุลยพินิจอย่างมาก เพื่อชั่งน้ำหนักระหว่างประโยชน์อันชอบธรรมนั้นไม่ให้ขัดกับสิทธิและประโยชน์ของเจ้าของข้อมูล โดยผู้ควบคุมข้อมูลจะต้องระบุได้ว่าอะไรคือประโยชน์อันชอบธรรมที่จะได้รับ และอะไรคือความจำเป็นของการประมวลผลข้อมูล อีกทั้งยังต้องมีหน้าที่

ในการปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลให้สมดุลกับประโยชน์อันชอบธรรมที่จะได้รับด้วย การใช้ดุลยพินิจเช่นนี้ย่อมทำให้เกิดความเสี่ยงมากในการตัดสินใจผิดพลาดซึ่งผู้ควบคุมข้อมูลอาจต้องรับผิดภายหลังได้

6.3 ผู้ควบคุมข้อมูลไม่อาจอ้างได้ว่าเจ้าของข้อมูลควรจะคาดหมายการประมวลผลข้อมูลได้ เพราะประกาศไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคลไว้แล้ว หากเนื้อหานั้นไม่ได้เฉพาะเจาะจงและสามารถมั่นใจได้ว่าเจ้าของข้อมูลส่วนบุคคลจะมีโอกาสได้อ่านจริงๆ เนื่องจากโดยทั่วไปแล้วในยุคปัจจุบัน เราไม่อาจคาดหมายให้ทุกคนอ่านนโยบายคุ้มครองข้อมูลส่วนบุคคลอย่างละเอียดได้

6.4 ในการอ้างฐานนี้เพื่อประมวลผล ผู้ควบคุมข้อมูลควรแน่ใจว่ามีความจำเป็นในการประมวลผลจริง ผลประโยชน์อันชอบธรรมนั้นมีความชัดเจน และต้องชั่งน้ำหนักระหว่างผลประโยชน์กับสิทธิและประโยชน์ของเจ้าของข้อมูล (Legitimate Interest Assessments - LIA) ในการใช้ฐานนี้ผู้ควบคุมข้อมูลควรประเมินปัจจัยต่อไปนี้
(1) ลักษณะของข้อมูลและผลประโยชน์ ซึ่งอาจขึ้นอยู่กับความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลกับเจ้าของข้อมูลเพื่อให้เข้าใจว่าเจ้าของข้อมูลมีความคาดหวังอย่างไรต่อการจัดการข้อมูล
(2) ผลกระทบและความเสี่ยงที่จะเกิดขึ้นจากการประมวลผล เช่นการเปิดเผยต่อข้อมูลต่อบุคคลอื่น
(3) มาตรการปกป้องข้อมูลและคุ้มครองสิทธิและประโยชน์ของเจ้าของข้อมูล

7. ฐานจดหมายเหตุ/วิจัย/สถิติ

7.1 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดฐานในการประมวลผลข้อมูลหนึ่งที่แตกต่างไปจากกฎหมายของประเทศอื่นรวมถึง GDPR คือการจัดทำเอกสารประวัติศาสตร์จดหมายเหตุ และการศึกษาวิจัยและสถิติ

7.2 ความหมายของการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสถิตินั้นอาจกินความได้กว้างขวาง เนื่องจากการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ การศึกษาวิจัยและสถิตินั้นโดยทั่วไปถูกมองว่าเป็นเพียง “วิธีการ” เพื่อให้บรรลุวัตถุประสงค์อย่างใดอย่างหนึ่งก็ได้ ซึ่งแตกต่างจากการประมวลผลในฐานอื่นๆ ที่เน้นไปที่ลักษณะของวัตถุประสงค์เป็นหลัก ซึ่งแต่ละฐานก็อ้างอิงความชอบธรรมในการประมวลผลในรูปแบบต่างๆทั้งจากกฎหมาย (ฐานภารกิจของรัฐ ฐานการปฏิบัติตามกฎหมาย) จากการตัดสินใจของเจ้าของข้อมูลส่วนบุคคลเอง (ฐานความยินยอม) จากผลประโยชน์ของเจ้าของข้อมูลส่วนบุคคล(ฐานประโยชน์อันสำคัญต่อชีวิต) และจากผลประโยชน์ของผู้ควบคุมข้อมูลหรือบุคคลที่สามที่เหนือกว่าของเจ้าของข้อมูลส่วนบุคคล (ฐานผลประโยชน์อันชอบธรรม) ดังนั้นใน GDPR จึงกำหนดให้การศึกษาวิจัยและสถิติจะต้องอ้างฐานใดฐานหนึ่งใน 6 ฐานประกอบด้วยเสมอ

7.3 การประมวลผลบนฐานนี้มีเงื่อนไขสำคัญคือต้องจัดให้มีมาตรการปกป้องที่เหมาะสม โดยอย่างน้อยต้องเป็นไปตามที่คณะกรรมการประกาศกำหนด ซึ่งหากผู้ควบคุมข้อมูลจัดให้มีมาตรการที่สอดคล้องกับมาตรฐานจริยธรรมของระเบียบวิธีในการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ วิจัยและสถิติของการศึกษาประเภทต่างๆ ด้วย ก็จะทำให้การส่งต่อข้อมูลหรือนำไปใช้งานต่อในบริบทอื่นๆ ก็จะเป็นไปได้ง่ายและถูกต้องตามเงื่อนไขของกฎหมายของประเทศ

อื่นๆ ด้วยอีกทั้งยังคาดหมายได้ว่าประกาศของคณะกรรมการก็น่าจะต้องอ้างอิงไปตามมาตรฐานสากลของระเบียบวิธีเหล่านี้ด้วย

7.4 มาตรการปกป้องที่เหมาะสมสามารถอ้างอิงตามตามมาตรฐานจริยธรรมของสาขาวิชาต่างๆ ที่เกี่ยวข้องกับการจัดทำเอกสารประวัติศาสตร์ จดหมายเหตุ และการศึกษาวิจัยและสถิติ ซึ่งมีถือปฏิบัติตามแนวทางที่เป็นสากลอยู่แล้ว และสอดคล้องกับหลักการพื้นฐานของการคุ้มครองข้อมูลส่วนบุคคล คือ หลักความจำเป็น หลักความได้สัดส่วน และการเคารพสิทธิขั้นพื้นฐานของเจ้าของข้อมูลส่วนบุคคล

7.5 การประมวลผลข้อมูลส่วนบุคคลที่ไม่จำเป็นต้อการบรรลุวัตถุประสงค์ของการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิตินั้นย่อมไม่สามารถอ้างฐานนี้ได้

แนวปฏิบัติเกี่ยวกับสิทธิหน้าที่โดยทั่วไปของผู้ควบคุมและผู้ประมวลผลข้อมูล

ผู้ควบคุมข้อมูล (Data Controller)

1. ผู้ควบคุมข้อมูลจะประมวลผลข้อมูลส่วนบุคคลได้ตามขอบเขตที่ได้รับความยินยอมหรืออาศัยฐานทางกฎหมายในการประมวลผลอื่นๆ
2. ผู้ควบคุมข้อมูลจะต้องแจ้งเจ้าของข้อมูลเมื่อได้รับข้อมูลส่วนบุคคลไม่ว่าจะได้รับข้อมูลโดยตรงจากเจ้าของข้อมูลหรือได้รับข้อมูลจากแหล่งอื่นและไม่ว่าจะอาศัยฐานทางกฎหมายใด (ทั้งที่ ประมวลผลข้อมูลบนฐานความยินยอมหรือฐานอื่นโดยที่ไม่ต้องได้รับความยินยอม)

   2.1 จะต้องจัดเตรียมข้อมูลและแจ้งข้อมูลเกี่ยวกับการเก็บรวบรวม และการใช้ข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลโดยจะต้องแจ้งให้แก่เจ้าของข้อมูลขณะที่มี การได้รับข้อมูลส่วนบุคคลนั้นทันทีที่ได้รับข้อมูลส่วนบุคคล โดยข้อมูล (information) ที่จะต้องจัดเตรียมให้แก่เจ้าของข้อมูลนั้นขึ้นอยู่กับแหล่งที่มาของข้อมูล ตามรายละเอียดในบันทึกการประมวลผลข้อมูล

   2.2 ระยะเวลาในการแจ้งข้อมูลให้แก่เจ้าของข้อมูลนั้น แตกต่างกันขึ้นอยู่กับสถานการณ์
   -กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ต้องแจ้งก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล (ทั้งนี้การเก็บรวบรวมหมายถึงเก็บจากการที่เจ้าของข้อมูลให้ด้วยตนเองโดยตรงและจากการสำรวจหรือสังเกตุการณ์
   -กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น ต้องแจ้งภายในระยะเวลาตามสมควร แต่ต้องไม่เกิน 30 วันนับแต่วันที่เก็บรวบรวม
   -กรณีใช้ข้อมูลเป็นไปเพื่อการติดต่อสื่อสารกับเจ้าของข้อมูล จะต้องแจ้งอย่างช้าเมื่อมีการติดต่อสื่อสารครั้งแรก

-กรณีคาดหมายได้ว่าจะมีการเปิดเผยข้อมูลส่วนบุคคลดังกล่าวต่อบุคคลที่สาม จะต้องแจ้งอย่างช้าเมื่อมีการเปิดเผยข้อมูลดังกล่าวเป็นครั้งแรก

-เมื่อมีการเปลี่ยนแปลงของข้อมูลที่มีผลกระทบอย่างมีนัยสำคัญต่อการประมวลผลข้อมูลที่เคยแจ้งให้เจ้าของข้อมูลทราบ เช่น การเพิ่มขึ้นของบุคคลที่อาจได้รับการเปิดเผยข้อมูลส่วนบุคคลอย่างมีนัยสำคัญแม้ว่าจะมีวัตถุประสงค์ในการเปิดเผยที่เคยแจ้งไว้ก็ตาม หรือเป็นการเพิ่มขั้นตอนการประมวลผลข้อมูลอย่างมาก ควรทำการแจ้งก่อนการมีผลของการเปลี่ยนแปลงข้อมูลนั้นๆ หรือโดยเร็วที่สุด

3. ข้อมูลที่จัดเตรียมต้องชัดเจน โปร่งใส สามารถเข้าใจได้ง่าย อยู่ในรูปแบบที่เข้าถึงได้ง่าย ใช้ภาษาที่เรียบง่ายไม่คลุมเครือ เนื้อความของข้อมูลไม่ควรใช้คำว่า “อาจ” “บางครั้ง” หรือ “มีความเป็นไปได้ว่า” ซึ่งแสดงให้เห็นถึงความไม่ชัดเจนและคลุมเครือของเนื้อหา

4. ในกรณีต่อไปนี้ ไม่แจ้งข้อมูลให้แก่เจ้าของข้อมูลได้
   - กรณีได้รับข้อมูลส่วนบุคคลจากเจ้าของข้อมูล เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว
   - กรณีได้รับข้อมูลส่วนบุคคลจากแหล่งอื่น เมื่อเจ้าของข้อมูลมีข้อมูลดังกล่าวอยู่แล้ว
   - เมื่อพิสูจน์ได้ว่าการแจ้งวัตถุประสงค์ใหม่หรือข้อมูลดังกล่าวไม่สามารถกระทำได้ หรือเป็นอุปสรรคต่อการใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ การวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือทางสถิติ เมื่อเป็นการเก็บรวบรวมหรือเปิดเผยข้อมูลส่วนบุคคลโดยเร่งด่วนตามที่กฎหมายกำหนด
   - เมื่อมีหน้าที่ต้องรักษาความลับตามกฎหมายที่คุ้มครองเกี่ยวกับข้อมูลส่วนบุคคลนั้น เนื่องมาจากการล่วงรู้ข้อมูลส่วนบุคคลจากหน้าที่ และจะต้องรักษาวัตถุประสงค์ใหม่หรือรายละเอียดของข้อมูลไว้เป็นความลับตามที่กฎหมายกำหนด

5. ผู้ควบคุมข้อมูลอาจจัดให้มีขั้นตอนเพิ่มเติม เพื่อให้เกิดแนวปฏิบัติที่ดี เช่น
   - จัดให้มีการสอบถามลูกค้าที่เป็นเจ้าของข้อมูลเพื่อประเมินศักยภาพและให้ความเห็นเกี่ยวกับระบบการแจ้งข้อมูลส่วนบุคคล
   - ตรวจสอบความถูกต้องของข้อมูลอย่างสม่ำเสมอ
   - นอกจากข้อมูลที่ต้องแจ้งตามข้างต้นแล้ว อาจพิจารณาระบุถึงผลกระทบที่อาจเกิดขึ้นต่อสิทธิขั้นพื้นฐานของเจ้าของข้อมูลจากการประมวลผลข้อมูลเพื่อวัตถุประสงค์บางประเภท
   - ข้อมูลควรปรากฏอยู่ในที่เดียวกันกับที่จะเก็บรวบรวมข้อมูลส่วนบุคคล และควรจัดทำเป็นเอกสารฉบับเดียวกัน หรือรวมอยู่ในตำแหน่งเดียวกัน
   - กรณีที่ดำเนินการประมวลผลข้อมูลหรือเก็บรวบรวมด้วยช่องทางออนไลน์ การแจ้งข้อมูลก็ควรจะอยู่ในรูปแบบออนไลน์เช่นเดียวกัน

6. ผู้ควบคุมข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมกับความเสี่ยง

6.1 ผู้ควบคุมข้อมูลจะต้องพิจารณาถึงความเสี่ยง ความเป็นไปได้ รวมถึง ความร้ายแรงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยอาจใช้มาตรการ รักษาความมั่นคงปลอดภัยดังต่อไปนี้

- การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption)
- ความสามารถในการรักษาความลับ ความถูกต้องและแท้จริง ความพร้อมใช้งาน และการพร้อมรับมือต่อการเปลี่ยนแปลงต่างๆ ของระบบหรือบริการประมวลผล
- ความสามารถที่จะทำให้ความพร้อมและใช้งานและเข้าถึงข้อมูลส่วนบุคคลกลับสู่สภาพที่ใช้งานได้ทันท่วงทีเมื่อมีเหตุขัดข้องทางกายภาพหรือทางเทคนิค
- กระบวนการตามปกติในการทดสอบ ประเมิน และวัดผลประสิทธิภาพของ มาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อสร้างความมั่นคงปลอดภัยในการ ประมวลผล

6.2 ผู้ควบคุมข้อมูลจะต้องมีมาตรการเพื่อควบคุมบุคคลธรรมดาซึ่ง ปฏิบัติงานภายใต้อำนาจของผู้ควบคุมข้อมูลและเข้าถึงข้อมูลได้ให้บุคคลนั้นไม่ประมวลผลข้อมูลโดยปราศจากคำสั่งหรือข้อกำหนดของผู้ควบคุมข้อมูล

6.3 ผู้ควบคุมข้อมูลควรต้องมีการเตรียมพร้อมไว้เพื่อให้เกิดการบริหารจัดการเมื่อเกิดเหตุการณ์ฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัย

7. ผู้ควบคุมข้อมูลจะต้องแจ้งเหตุแก่ผู้กำกับดูแลหรือเจ้าของข้อมูลเมื่อมีข้อมูลส่วนบุคคลรั่วไหล (data breach)

7.1 กรณีข้อมูลส่วนบุคคลรั่วไหลมีความหมายกว้างครอบคลุมการที่ข้อมูลถูก ทำลาย การสูญหาย การแก้ไขเปลี่ยนแปลง การเปิดเผย หรือการเข้าถึง ส่งต่อ เก็บรักษา หรือถูกประมวลผลอย่างอื่นไม่ว่าจะเกิดจากการกระทำอันมิชอบด้วยกฎหมายหรือโดย อุบัติเหตุ

7.2 หากบุคคล หรือองค์พบการรั่วไหลของข้อมูล สามรถแจ้งการรั่วไหลมายังผู้ควบคุมข้อมูลผ่านช่องทางต่างๆ เช่น

7.2.1 ทางโทรศัพท์ 038 540 000 , โทรสาร 038842032

7.2.2 ทางช่องทางร้องเรียนในwebsite ของบริษัท (www.shrinkflexthailand.com)

7.2.3 ทาง e-mail : pdpa_admin@shrinkflexthailand.com

7.2.4 ทางไปรษณีย์ หรือแจ้งโดยตรง บริษัทชริ้งเฟล็กซ์ (ประเทศไทย) จำกัด (มหาชน) สำนักงานใหญ่ : 68/2-5 หมู่ 5 ตำบลบางสมัคร อำเภอบางปะกง จังหวัดฉะเชิงเทรา 24130

7.3 ผู้ควบคุมข้อมูลมีหน้าที่แจ้งกรณีข้อมูลส่วนบุคคลรั่วไหล ภายใน 72 ชั่วโมงนับแต่ได้ทราบ เว้นแต่เหตุที่เกิดนั้นไม่น่าจะก่อให้เกิดความเสี่ยงใดๆ ต่อ สิทธิและเสรีภาพของเจ้าของข้อมูล กรณีที่ไม่อาจแจ้งเหตุได้ภายใน 72 ชั่วโมง ผู้ควบคุมจะต้องแจ้งเหตุแห่งการแจ้งล่าช้าด้วย ข้อมูลที่ต้องแจ้ง มีดังต่อไปนี้

7.3.1 คำอธิบายลักษณะของการละเมิดข้อมูลหรือข้อมูลรั่วไหล ประเภทของข้อมูลและจำนวนเจ้าของข้อมูลที่ได้รับผลกระทบโดยประมาณ และปริมาณข้อมูลที่เกี่ยวข้อง

7.3.2 ชื่อหรือข้อมูลติดต่อสำหรับการติดต่อสอบถามข้อมูลเพิ่มเติม

7.3.3 คำอธิบายผลที่อาจจะเกิดขึ้นได้จากเหตุการณ์ดังกล่าว

7.3.4 คำอธิบายขั้นตอนกระบวนการในการรับมือเหตุการณ์ดังกล่าวเพื่อลดหรือป้องกันผลร้ายที่อาจจะเกิดขึ้น

7.4 ผู้ควบคุมข้อมูลมีหน้าที่แจ้งเจ้าของข้อมูลโดยไม่ชักช้า ต่อเมื่อการรั่วไหลของข้อมูลนั้นก่อให้เกิดความเสี่ยงสูงต่อสิทธิเสรีภาพของเจ้าของข้อมูล ในกรณีเช่นว่านี้จะต้องแจ้งให้เจ้าของข้อมูลทราบด้วยภาษาที่เข้าใจง่ายและมีความชัดเจนและมีรายละเอียดอย่างน้อยดังต่อไปนี้

7.4.1 คำอธิบายลักษณะของการรั่วไหลของข้อมูล

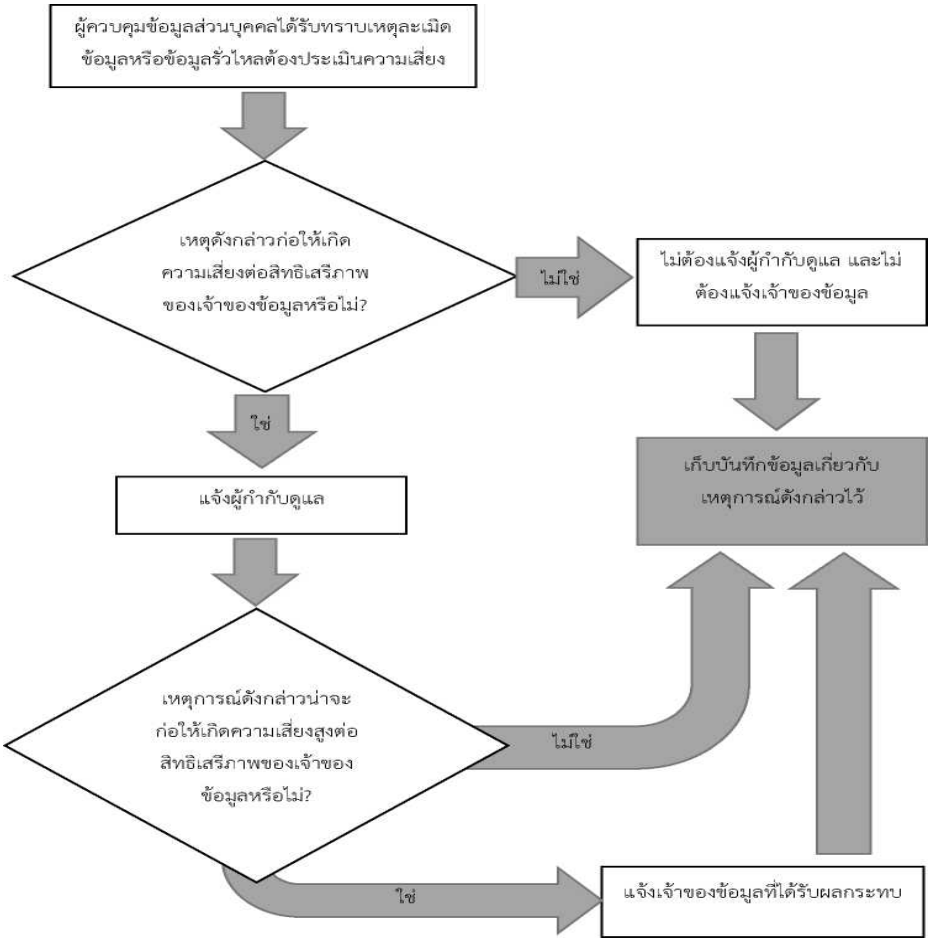
7.4.2 ชื่อหรือข้อมูลการติดต่อเจ้าหน้าที่ผู้รับผิดชอบหรือ เจ้าหน้าที่คุ้มครอง ข้อมูล (Data Protection Officer)

7.4.3 ผลที่อาจจะเกิดขึ้นจากการที่ข้อมูลรั่วไหล ซึ่งรวมถึงความเสี่ยงต่อเจ้าของข้อมูล

7.4.4 มาตรการที่เสนอแนะหรือแนวทางเยียวยาให้เจ้าของข้อมูลกระทำเพื่อรับมือกับกรณีดังกล่าวที่อาจจะลดผลร้ายที่อาจเกิดจากการที่ข้อมูลรั่วไหลได้

7.4.5 เก็บบันทึกเกี่ยวกับเหตุการณ์รั่วไหลข้อมูลในแบบฟอร์ม

แผนผังขั้นตอนการแจ้งเหตุข้อมูลรั่วไหล



8 ผู้ควบคุมข้อมูลจะต้องจัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

8.1 ระยะเวลาการเก็บรักษาข้อมูล (retention period) นั้นโดยปกติแล้วจะต้องกำหนดตามความจำเป็นของข้อมูลนั้นในการประมวลผลข้อมูล ซึ่งความจำเป็นนั้นก็ด้วยการอาศัยฐานตามกฎหมายฐานใดฐานหนึ่งนั้นเอง ในบางครั้งก็จะสามารถกำหนดระยะเวลาได้แน่นอน แต่ในบางกรณีก็ไม่อาจจะกำหนดเวลาไว้ได้แน่นอน ทั้งนี้ ควรมีหลักการพิจารณาระยะเวลาจัดเก็บตามลำดับ ดังนี้

- หากมีระยะเวลาตามกฎหมายระบุชัดเจนให้เก็บรักษาไว้เป็นระยะเวลานานเท่าใด ให้จัดเก็บตามกำหนดเวลานั้น
- ระยะเวลาในการเก็บรักษาข้อมูลในหลายกรณีจะเป็นไปตามรูปแบบความสัมพันธ์ ที่มีต่อเจ้าของข้อมูลบางกรณีสามารถระบุระยะเวลาเก็บรักษาที่แน่นอนได้ แต่บางกรณีก็ไม่สามารถระบุระยะเวลาเก็บรักษาที่แน่นอนได้ เช่น กรณีที่ขอความยินยอม และได้ระบุระยะเวลาไว้ชัดเจน เมื่อพ้นระยะเวลาดังกล่าวก็ต้องลบ

หรือทำลายไป หรือหากไม่ได้ระบุไว้อย่างชัดเจนก็ต้องพิจารณาว่าข้อมูลหมดความจำเป็นในกิจกรรมประมวลผลที่ได้รับความยินยอมเมื่อใด หรือเมื่อมีการถอนความยินยอม เป็นต้น

- แม้กระทั่งความสัมพันธ์ระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลสิ้นสุดลงแล้วก็อาจมีเหตุจำเป็นที่ยังคงจะต้องมีการเก็บข้อมูลต่อไปด้วย เช่น เพื่อยืนยันว่าเคยมี ความสัมพันธ์ต่อกัน และความสัมพันธ์ดังกล่าวได้สิ้นสุดไปแล้ว เช่น บริษัทอาจมีความจำเป็นที่จะเก็บข้อมูลส่วนบุคคลของลูกค้าที่ยุติความสัมพันธ์ไปแล้วเพื่อที่จะสามารถ จัดการข้อร้องเรียนต่างๆ ที่ลูกค้าอาจจะมีต่อบริการที่ตนได้รับบริการ
- การเก็บรักษาข้อมูลส่วนบุคคลบางประเภทอาจมีเหตุผลหรือความจำเป็นที่จะต้อง เก็บไว้ตลอดไป

8.2 เมื่อข้อมูลหมดความจำเป็นและไม่มีเหตุอื่นใดให้เก็บรักษาข้อมูลต่อไปได้ ผู้ควบคุมข้อมูลย่อมต้องมีหน้าที่ในการลบทำลายข้อมูลส่วนบุคคลหรือทำให้ข้อมูลนั้นกลายเป็นข้อมูลนิรนาม

- เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลอาจเลือกการลบทำลาย ข้อมูล หรือการทำให้ข้อมูลกลายเป็นข้อมูลนิรนามก็ได้ในการลบทำลายข้อมูลขึ้นอยู่กับลักษณะของข้อมูล ข้อมูลในรูปแบบเอกสารก็อาจพิจารณาวิธีการ ทำลายเอกสาร โดยเครื่องทำลายเอกสารหรือการเผาทำลาย ข้อมูลในรูปแบบอิเล็กทรอนิกส์หากบรรจุอยู่ในอุปกรณ์ อาจจะทำลายตัวอุปกรณ์ หรือการลบออก จากระบบออนไลน์
- กฎหมาย มิได้กำหนดระยะเวลาแน่นอนที่จะต้องลบ ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูล นิรนามไว้อย่างชัดเจน เพียงแต่กำหนดหลักการว่าเมื่อข้อมูลหมดความจำเป็นก็ให้ ดำเนินการดังกล่าว พร้อมกันนี้กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มี ระบบตรวจสอบเพื่อการลบ ทำลายหรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนามดังนั้น ผู้ควบคุมข้อมูลจึงควรจัดให้มีรอบในการพิจารณาเพื่อลบ ทำลาย หรือทำให้ข้อมูลกลายเป็นข้อมูลนิรนามให้เกิดการทำลายภายในระยะเวลาอันสมควรตามรอบที่กำหนด

9 ผู้ควบคุมข้อมูลจะต้องเก็บบันทึกรายการประมวลผลข้อมูล

9.1 บันทึกรายการประมวลผลข้อมูลจะต้องมีรายการดังต่อไปนี้

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล
- ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึง ข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูล
- การปฏิเสธคำขอหรือการคัดค้านของเจ้าของข้อมูลส่วนบุคคล
- คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

9.2 บันทึกรายการประมวลผลข้อมูลจะต้องจัดทำเป็นลายลักษณ์อักษร โดยจะอยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้

10 ผู้ควบคุมข้อมูลจะต้องมีบุคลากรที่ทำหน้าที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

10.1 สถานะและคุณสมบัติของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะเป็นพนักงานหรือลูกจ้างก็ได้ หรือจะเป็นผู้ รับจ้างตามสัญญาให้บริการก็ได้

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลควรจะมีคุณสมบัติเป็นผู้มีความรู้ด้านกฎหมาย คุ้มครองข้อมูลส่วนบุคคล เข้าใจกิจกรรมการประมวลผลข้อมูลขององค์กร เข้าใจงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัย มีความรู้เกี่ยวกับ ภาคธุรกิจและองค์กร และมีความสามารถที่จะสร้างวัฒนธรรมคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร

10.2 การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับการสนับสนุนการทำงานและได้รับ การอำนวยความสะดวกอย่างเพียงพอ เช่น การสนับสนุนจากฝ่ายบริการงานทั่วไป การให้เวลาเพียงพอ ในการทำงานของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล การจัดหาทรัพยากรในการ ทำงานให้เพียงพอแก่การทำงาน ไม่ว่าจะในลักษณะของเงิน โครงสร้างพื้นฐานและพนักงานสนับสนุน การสื่อสารองค์กร การเข้าถึงบริการอื่นๆ ของกิจการเพื่อ สนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รับความคุ้มครองและควรมีมาตรการเพื่อให้ การปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นไปโดยอิสระ การให้ออกหรือเลิกจ้างเพราะเหตุที่เจ้าหน้าที่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562 จะทำมิได้

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องสามารถรายงานไปยังผู้บริหารสูงสุดของ องค์กรได้

- เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจได้รับมอบหมายให้ปฏิบัติภารกิจอื่น แต่ต้องไม่ขัดหรือแย้งกับการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

10.3 ภารกิจของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

10.3.1 ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคล เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

10.3.2 เป็นบุคคลที่ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครอง ข้อมูลส่วนบุคคล

10.3.3 รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

10.4 ความรับผิดของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

10.4.1 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่มีความรับผิดเป็นส่วนตัวต่อการฝ่าฝืน พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพราะผู้ที่ต้องรับผิดชอบ ได้แก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลแล้วแต่กรณี

10.4.2 ถ้าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้รู้ข้อมูลส่วนบุคคลของผู้อื่น เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษอาญาตามกฎหมาย เว้นแต่จะเป็นการเปิดเผยที่ชอบด้วยกฎหมาย

10.5 ควบคุมข้อมูลจะต้องดำเนินการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA)

10.6 ในกรณีที่ผู้ควบคุมข้อมูลไม่ได้เป็นผู้ประมวลผลข้อมูลด้วยตนเอง ผู้ควบคุมข้อมูลมีหน้าที่เลือกผู้ ประมวลผลข้อมูลที่มีมาตรการเชิงเทคนิคและเชิงบริหารจัดการที่เหมาะสมในการประมวลผล และการรักษาความมั่นคงปลอดภัย

10.7 ผู้ควบคุมข้อมูลที่มอบหมายให้ผู้ประมวลผลข้อมูลเป็นผู้ดำเนินการแทนจะต้องจัดให้มีข้อตกลง กับผู้ประมวลผลข้อมูลเพื่อควบคุมให้ผู้ประมวลข้อมูลดำเนินการให้เป็นไปตามกฎหมาย

10.8 ผู้ควบคุมข้อมูลในกรณีที่จะโอนข้อมูลไปยังต่างประเทศหรือองค์การระหว่างประเทศจะต้องทำ โดยชอบด้วยกฎหมายกล่าวคือ ปลายทางที่รับโอนจะต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคล เพียงพอ หากไม่เพียงพอก็จะต้องมีการดำเนินการตามขั้นตอนของกฎหมาย

10.9 ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลจะต้องดำเนินการเพื่อป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลโดยปราศจากอำนาจ หรือโดยมิชอบ

ผู้ประมวลผลข้อมูล (Data Processor)

1. ผู้ประมวลผลข้อมูลจะต้องประมวลผลตามข้อตกลงระหว่างผู้ควบคุมและผู้ประมวลผลข้อมูลหรือตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคล การประมวลผลข้อมูลส่วนบุคคลที่ขัดคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลย่อมทำให้ผู้ประมวลผลข้อมูลต้องรับผิดต่อผู้ควบคุมข้อมูลตามข้อตกลง อีกทั้งยังเป็นการฝ่าฝืนกฎหมายคุ้มครองข้อมูลส่วนบุคคลในขณะเดียวกันด้วย
2. ผู้ประมวลผลข้อมูลจะต้องมีมาตรการเชิงเทคนิคและเชิงบริหารจัดการเพื่อรักษาความมั่นคง ปลอดภัยในการประมวลผลที่เหมาะสมกับความเสี่ยง
3. ผู้ประมวลผลข้อมูลจะต้องแจ้งเหตุแก่ผู้ควบคุมข้อมูลกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach)
4. ผู้ประมวลผลข้อมูลจะต้องตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) ในกรณีที่
   - เป็นหน่วยงานของรัฐที่คณะกรรมการประกาศกำหนด

- เป็นการประมวลผลข้อมูลซึ่งมีการติดตามเจ้าของข้อมูลจำนวนมากอย่างสม่ำเสมอและเป็นระบบ ตามที่คณะกรรมการประกาศกำหนด
- ผู้ที่มีกิจกรรมหลักเป็นการประมวลผลข้อมูลอ่อนไหว

แนวปฏิบัติเกี่ยวกับการจัดทำข้อตกลงระหว่างข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) คุ้มครองข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล โดยผู้ควบคุมข้อมูลส่วนบุคคลอาจมอบหมายให้บุคคลหรือนิติบุคคลอื่น ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูล ในกรณีนี้ บุคคลหรือนิติบุคคลที่ได้รับการมอบหมายให้ประมูลผลข้อมูลส่วนบุคคลจะมีสถานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล” (“Data processor”) ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โดยทั้งสองฝ่ายตกลงกันทำเป็นสัญญาว่าจ้าง ซึ่งโดยทั่วไปแล้วสัญญาว่าจ้างดังกล่าวจะกำหนดสิทธิหน้าที่ของคู่สัญญาในฐานะผู้ว่าจ้างและผู้รับจ้างในเรื่องของหน้าที่และวิธีการในการวิเคราะห์ข้อมูล การชำระ ค่าบริการ ความรับผิด และสิทธิในทรัพย์สินทางปัญญา และอาจไม่มีข้อกำหนดในสัญญาเกี่ยวกับการ คุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ กรณีจึงมีประเด็นว่า “ข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล” ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในทางปฏิบัติ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลสามารถทำสัญญาประมวลผล ข้อมูล (Data Processing Agreement)ในฐานะเป็นสัญญาอุปกรณ์ของสัญญาให้บริการหลัก (Principal Agreement) โดยไม่ต้องยกเลิกสัญญาเดิม และสามารถทำสัญญา ประมวลผลข้อมูลแยกต่างหากอีกฉบับหนึ่ง โดยกำหนดให้สัญญาประมวลผลข้อมูลนี้เป็นส่วนหนึ่งของสัญญาให้บริการหลักโดยสัญญาประมวลผลข้อมูลดังกล่าวควรมีการกำหนดโครงสร้างและเนื้อหาของสัญญาดังต่อไปนี้

1. บททั่วไป กล่าวถึงบทนำว่าสัญญานี้ใช้เป็นส่วนหนึ่งกับสัญญาการให้บริการหลัก คู่สัญญา ความประสงค์ และคำนิยามต่างๆ ที่ใช้ในสัญญา
2. หน้าที่ของคู่สัญญา
   2.1 หน้าที่ส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล และความเกี่ยวเนื่องกับสัญญาหลัก
   2.2 มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม

2.3 สิทธิของเจ้าของข้อมูลส่วนบุคคล

2.4 การแจ้งต่อผู้ควบคุมข้อมูลหากทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

2.5 การลบและเก็บรักษาข้อมูลส่วนบุคคล

2.6 การส่งหรือโอนข้อมูลส่วนบุคคล

แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูล

แนวปฏิบัติเกี่ยวกับการจัดการคำร้องขอของเจ้าของข้อมูลนั้นเพื่อให้ผู้ควบคุมข้อมูลหรือผู้ ประมวลผลข้อมูลสามารถดำเนินการเพื่อให้เป็นไปตามสิทธิของเจ้าของข้อมูลตามกฎหมายได้อย่างเหมาะสม

1. ขั้นตอนสำหรับการปฏิบัติหน้าที่ของผู้ควบคุมข้อมูลเมื่อเจ้าของข้อมูลร้องขอ สามารถสรุปพอสังเขปได้ดังนี้

2. โดยในแต่ละขั้นตอนสำหรับการดำเนินการตามคำขอของเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการทุกขั้นตอนให้แล้วเสร็จโดยไม่ชักช้า และจะต้องไม่เกิน 30 วันนับแต่ได้รับคำขอ ตามขั้นตอน

2.1 เมื่อมีเจ้าของข้อมูลส่วนบุคคลยื่นคำร้องในรูปแบบต่างๆ เช่น email, website, วาจา,ต่อหน้าบุคคล ทางผู้ควบคุมข้อมูลพิจารณาให้ใช้แบบฟอร์มการใช้สิทธิ์ของเจ้าของข้อมูลส่วนบุคคล

2.1.1 กรอกแบบฟอร์มแล้วยื่นผ่าน website ของบริษัทฯ ซึ่งจะเข้าสู่เจ้าหน้าที่ลงทุนสัมพันธ์ของบริษัทฯ แล้วเจ้าหน้าที่ลงทุนสัมพันธ์ ส่งต่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) หรือส่ง email มายัง pdpa_admin@shrinkflexthailand.com ซึ่ง DPO เป็นผู้ดูแลอยู่แล้ว

2.2 DPO บันทึกรายการเกี่ยวกับคำร้องขอ เช่น วันที่ได้รับ ผู้ขอ ผู้รับเรื่อง เป็นต้น แล้วดำเนินการขั้นตอนต่อไป

2.3 ทำการตรวจสอบตัวตนของผู้ยื่นคำร้องขอ กรณีที่เป็นเจ้าของข้อมูลยื่นคำร้องขอด้วยตนเอง ให้พิจารณาเอกสารที่เกี่ยวข้องเช่น บัตรประชาชน เพื่อระบุตัวตนว่าเป็นเจ้าของข้อมูลที่แท้จริง

กรณีที่ผู้ยื่นคำร้องขอเป็นบุคคลอื่น จะต้องพิจารณาต่อไปว่าบุคคลดังกล่าวเป็นบุคคลที่มีอำนาจในการดำเนินการแทนเจ้าของข้อมูลหรือไม่ เช่น หนังสือมอบอำนาจ (กรณีมอบอำนาจ) หรือผู้ปกครอง (ในกรณี เจ้าของข้อมูลเป็นผู้เยาว์ หรือผู้อนุบาล ผู้พิทักษ์ (ในกรณีเจ้าของข้อมูลเป็น คนไร้ความสามารถหรือเสมือนไร้ความสามารถ)

หากมีความจำเป็นให้ผู้ยื่นคำร้องขอหรือเจ้าของข้อมูลจัดเตรียม ข้อมูลเพิ่มเติมเพื่อพิจารณายืนยันตัวตน จะต้องแจ้งให้แก่บุคคล ดังกล่าวทราบโดยไม่ชักช้า

2.4 เมื่อดำเนินการตรวจสอบตัวตนเรียบร้อยแล้ว อาจพิจารณา เก็บข้อมูลเท่าที่จำเป็นเกี่ยวกับการพิจารณายืนยันตัวตน เช่น log ในการขอใช้สิทธิ วันเวลา รูปแบบคำขอ ผลสำเร็จในการตรวจสอบตัวตน เพื่อเป็นหลักฐานไว้พิสูจน์ความน่าเชื่อถือ และมาตรการในการตรวจสอบตัวตนของ หากเกิดกรณีมีการฟ้องร้องคดีในอนาคต

2.5 พิจารณาความถูกต้องของคำร้องขอ ว่าคำร้องขอดังกล่าวถูกต้อง สมบูรณ์ เป็นคำร้องขอที่ใช้สิทธิ์ตามที่กฎหมายรับรองหรือไม่ และมีข้อยกเว้นในการปฏิเสธ เช่น คำขอนั้นไม่สมเหตุสมผล หรือฟุ่มเฟือยเกินความจำเป็นอย่างชัดแจ้ง หรือเหตุอื่นๆ หรือไม่หากเป็นไปตามเงื่อนไขแห่งการปฏิเสธ DPO มีสิทธิที่จะปฏิเสธไม่ดำเนินการตามคำร้องขอหรือคิดค่าใช้จ่ายตามสมควรสำหรับการดำเนินการดังกล่าวได้

2.6 ในกรณีที่มีการปฏิเสธไม่ดำเนินการตามคำร้องขอนั้น DPO จะต้องแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลแห่งการปฏิเสธ สิทธิในการร้องทุกข์ต่อหน่วยงานกำกับดูแล ให้แก่เจ้าของข้อมูลทราบด้วย ในกรณีที่ประสงค์จะคิดค่าใช้จ่ายสำหรับการดำเนินการตามคำร้องขอนั้น DPO จะต้องแจ้งให้เจ้าของข้อมูลทราบโดยไม่ชักช้า และ DPO มีสิทธิ ยังไม่ดำเนินการตามคำร้องขอจนกว่าจะได้รับชำระเงินค่าใช้จ่ายดังกล่าว

2.7 เมื่อพิจารณาแล้วคำร้องขอนั้นเข้าเกณฑ์ที่จะต้องดำเนินการนั้นDPO แจ้งบุคลคลที่เกี่ยวข้องเพื่อรวบรวมข้อมูลต่างๆ เพื่อแจ้งและดำเนินการตามคำร้องขอของเจ้าของข้อมูล

3. สิทธิของเจ้าของข้อมูลที่ได้รับการรับรองตามแนวปฏิบัตินี้ได้แก่
   - 3.1 สิทธิในการเพิกถอนความยินยอม (right to withdraw consent)
   - 3.2 สิทธิการได้รับแจ้งข้อมูล (right to be informed)
   - 3.3 สิทธิในการเข้าถึงข้อมูลส่วนบุคคล (right of access)
   - 3.4 สิทธิในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง (right to rectification)
   - 3.5 สิทธิในการลบข้อมูลส่วนบุคคล (right to erasure)
   - 3.6 สิทธิในการห้ามมิให้ประมวลผลข้อมูลส่วนบุคคล (right to restriction of processing)
   - 3.7 สิทธิในการให้โอนย้ายข้อมูลส่วนบุคคล (right to data portability)

3.8 สิทธิในการคัดค้านการประมวลผลข้อมูลส่วนบุคคล (right to object)

3.9 สิทธิในการไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว (right not to be subject to automated individual decision-making, including profiling)

แนวทางในการปฏิบัติ ตามคำร้องขอตามสิทธิต่างๆ

1. หน้าที่ในการหยุดการดำเนินการประมวลผลข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลเพิกถอนความยินยอม

1.1 เมื่อเจ้าของข้อมูลเพิกถอนความยินยอมในการประมวลผลข้อมูลแล้ว ผู้ควบคุมข้อมูลจะต้องหยุดประมวลผลข้อมูลดังกล่าว เว้นแต่ กรณีมีเหตุให้การดำเนินการประมวลผลไม่จำเป็นต้องขอความยินยอมจากเจ้าของข้อมูล เช่น การประมวลผลอันเนื่องมาจากการปฏิบัติตามสัญญา ระหว่างผู้ควบคุมข้อมูลและเจ้าของข้อมูล หรือกรณีการประมวลผลเพื่อปกป้องสิทธิในชีวิตของ เจ้าของข้อมูลเป็นต้น

1.2 การเพิกถอนความยินยอมนั้นอาจทำในรูปแบบใดก็ได้ ซึ่งต้องสามารถกระทำได้ด้วยขั้นตอนที่ไม่ยากไปกว่าการให้ความยินยอม เช่น การเพิกถอนความยินยอมทางอิเล็กทรอนิกส์ เป็นต้น ทั้งนี้ความยินยอมที่มีลักษณะเป็นลายลักษณ์อักษร ผู้ควบคุมข้อมูลกำหนดให้การเพิกถอนมีลักษณะเป็นลายลักษณ์อักษรเช่นกันเพื่อให้มีหลักฐานที่ชัดเจน

1.3 ในกรณีที่เจ้าของข้อมูลเป็นผู้เยาว์ซึ่งมีอายุต่ำกว่า 20 ปี การเพิกถอนความยินยอมต้องได้รับความยินยอมจากผู้ปกครอง ผู้แทนโดยชอบธรรม หรือบุคคลที่มีอำนาจตามกฎหมาย เว้นแต่กรณีที่การถอนความยินยอมนั้นมีลักษณะที่กฎหมายกำหนดให้ผู้เยาว์อาจเพิกถอนความยินยอมได้เอง

1.4 เมื่อเจ้าของข้อมูลได้เพิกถอนความยินยอมแล้ว หากไม่มีความจำเป็นหรือไม่มีฐานโดยชอบด้วยกฎหมายอื่นๆ ที่จะประมวลผลข้อมูลส่วนบุคคลดังกล่าวอีกต่อไป ผู้ควบคุมข้อมูลจะต้องดำเนินการลบข้อมูลส่วนบุคคลนั้นออกจากระบบการจัดเก็บข้อมูลทั้งหมด ทั้งนี้ เนื่องจากการประมวลผลโดยนิยามแล้วรวมถึงการจัดเก็บข้อมูลด้วย อย่างไรก็ตาม การเพิกถอนความยินยอมไม่กระทบ ต่อการประมวลผลที่เกิดขึ้นก่อนหน้าอันเนื่องมาจากการให้ความยินยอมที่ชอบด้วยกฎหมายแล้ว

2. หน้าที่ในการให้เจ้าของข้อมูลเข้าถึงข้อมูลส่วนบุคคลที่อยู่ในครอบครองของผู้ควบคุมข้อมูลส่วนบุคคล

2.1 เมื่อได้รับคำร้องขอจากเจ้าของข้อมูลเพื่อขอเข้าถึงข้อมูลส่วนบุคคลของตนที่อยู่ในความครอบครองของผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลต้องจัดเตรียมข้อมูลที่เกี่ยวข้อง ข้อมูลส่วนบุคคลและการประมวลผลข้อมูลกล่าวคือ

- คำรับรองว่าได้ประมวลผลข้อมูลส่วนบุคคลนั้น และเปิดเผยการได้มาซึ่งข้อมูลส่วนบุคคลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอม
- สำเนาของข้อมูลส่วนบุคคลดังกล่าวให้แก่เจ้าของข้อมูล

- ข้อมูลที่เกี่ยวข้องต่างๆ ทั้งนี้ข้อมูลที่จะต้องส่งให้แก่เจ้าของข้อมูลควรเป็นข้อมูลที่มีอยู่ในขณะที่ส่งข้อมูลให้แก่เจ้าของข้อมูล แม้ว่าจะมีการแก้ไขข้อมูลในระหว่างที่ได้รับคำร้องขอกับการดำเนินการแจ้งข้อมูลตามคำร้องขอก็ตาม

2.2 หากมีการปฏิเสธ ต้องเป็นไปตามหลักการต่อไปนี้

2.2.1 เป็นการปฏิเสธตามกฎหมาย หรือ ตามคำสั่งศาล

2.2.2 เป็นการปฏิเสธ หากการดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ เช่น การเปิดเผยข้อมูลที่มีความลับทางการค้า หรือมีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูล เป็นต้น

2.2.3 กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการเข้าถึงข้อมูล ต้องทำบันทึกคำร้องขอ ของเจ้าของข้อมูลด้วย

2.2.4 สำหรับการเปิดเผยข้อมูลที่มีข้อมูลของบุคคลที่สามอยู่ด้วยนั้น ผู้ควบคุมข้อมูลมีสิทธิที่จะปฏิเสธไม่เปิดเผยข้อมูลเฉพาะในส่วนที่เกี่ยวข้องกับบุคคลที่สามนั้นให้แก่เจ้าของข้อมูลได้ แต่ไม่สามารถอ้างเหตุผลดังกล่าวเพื่อปฏิเสธการเข้าถึงข้อมูลทั้งหมด ซึ่งมีข้อมูลของเจ้าของข้อมูลรวมอยู่ด้วยตามสิทธิในข้อนี้ได้

3. หน้าที่ในการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

3.1 ผู้ควบคุมข้อมูลส่วนบุคคล มีหน้าที่ต้องดำเนินการให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด แม้จะไม่มีเจ้าของข้อมูลร้องขอ

3.2 ให้เจ้าของข้อมูลนำหลักฐานหรือเอกสารที่เกี่ยวข้องมาเพื่อพิสูจน์ประกอบการพิจารณาว่าข้อมูลส่วนบุคคลที่มีอยู่ไม่ถูกต้องหรือไม่สมบูรณ์อย่างไร

3.3 ในกรณีที่ข้อมูลนั้นไม่ถูกต้องในตัวเองอันเนื่องมาจากความผิดพลาดในการพิจารณาข้อมูล และมีการแก้ไขข้อมูลเพิ่มเติมให้ถูกต้องนั้น ต้องเก็บข้อมูลทั้งสองชุดไว้เพื่อเป็นหลักฐานแสดงความมีอยู่ของเจ้าของข้อมูลส่วนบุคคลนั้น

3.4 ในกรณีที่ข้อมูลส่วนบุคคลได้ถูกเผยแพร่ไปยังบุคคลที่สาม เมื่อมีการแก้ไขเพิ่มเติมความถูกต้องสมบูรณ์ ต้องแจ้งรายการดังกล่าวให้แก่ผู้รับข้อมูลทราบด้วย

4. หน้าที่ในการดำเนินการตามสิทธิการขอให้ลบข้อมูลส่วนบุคคล

4.1 ผู้ควบคุมข้อมูลส่วนบุคคล ต้องทำการลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ ตามเหตุดังนี้

4.1.1 ข้อมูลส่วนบุคคลดังกล่าว ไม่มีความจำเป็นสำหรับการเก็บรวบรวมหรือประมวลผลตามวัตถุประสงค์ที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลอีกต่อไป

4.1.2 เจ้าของข้อมูล เพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลไม่สามารถอ้างฐานในการประมวลผลอื่นได้

4.1.3 เจ้าของข้อมูลส่วนบุคคล ทำการคัดค้านการประมวลผล โดยผู้ควบคุมข้อมูลไม่สามารถอ้างความยินยอมในการเก็บรวบรวมข้อมูลได้

4.1.4 เจ้าของข้อมูลใช้สิทธิในการคัดค้านการประมวลผลข้อมูล และผู้ควบคุมข้อมูลไม่มีเหตุอันชอบด้วยกฎหมายหรือ เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย เพื่อใช้อ้างเพื่อประมวลผลได้

4.1.5 เจ้าของข้อมูลส่วนบุคคลคัดค้านการประมวลผลที่มีลักษณะเพื่อวัตถุประสงค์เกี่ยวกับการตลาดแบบตรง

4.1.6 การประมวลผลข้อมูลส่วนบุคคลนั้นไม่ชอบด้วยกฎหมาย

4.1.7 การลบข้อมูลเป็นไปตามหน้าที่ตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

4.2 ผู้ควบคุมข้อมูลส่วนบุคคล ต้องลบ หรือ ทำลาย หรือ ทำให้ข้อมูลส่วนบุคคลนั้นเป็นข้อมูลที่ไม่สามารถระบุถึงตัวบุคคลที่เป็นเจ้าของข้อมูลได้ ในลักษณะที่ทำให้บุคคลอื่น ไม่สามารถเข้าถึง อ่าน หรือประมวลผลข้อมูลส่วนบุคคลดังกล่าวได้ รวมถึงทำให้ไม่สามารถนำกลับมาใช้ได้อีกด้วย

4.3 ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม หรือผู้ควบคุมข้อมูลได้ทำให้ข้อมูลดังกล่าวเผยแพร่สู่สาธารณะ จะต้องจัดให้มีมาตรการทางเทคโนโลยีสำหรับการแจ้งให้บุคคลอื่นลบข้อมูลดังกล่าวด้วย ไม่ว่าข้อมูลนั้นจะอยู่ในรูปแบบใด ไม่ว่าจะเป็นต้นฉบับ หรือสำเนาหรือลิงค์ใดๆ ที่เชื่อมโยงถึงข้อมูลส่วนบุคคลนั้น ด้วยค่าใช้จ่ายของผู้ควบคุมข้อมูลเอง

4.4 หากมีกรณีดังต่อไปนี้ สามารถปฏิเสธไม่ดำเนินการลบข้อมูลตามคำร้องขอได้

4.4.1 เมื่อการประมวลผลมีความจำเป็นในการแสดงออกหรือการใช้สิทธิเสรีภาพในข้อมูล ซึ่งควรพิจาณาถึงความจำเป็นและความเหมาะสมในการนำข้อมูลส่วนบุคคลมาใช้เพื่อแสดงออก เช่น ข้อมูลเก่าเกินสมควรที่จะนำมาใช้แล้ว

4.4.2 การประมวลผลเป็นไปตามวัตถุประสงค์ในการจัดทำ เอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย สถิติ เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการเพื่อประโยชน์สาธารณะ หรือการใช้อำนาจรัฐที่ได้มอบหมายให้ หรือเป็นการเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว ที่เป็นการจำเป็นในการปฏิบัติหน้าที่ตากกฎหมายเพื่อให้บรรลุวัตถุประสงค์ในด้านเวชศาสตร์ป้องกัน อาชีวเวชศาสตร์ ประโยชน์สาธารณะด้านสาธารณสุข

4.4.3 การเก็บรักษาข้อมูลส่วนบุคคลนั้นเป็นไปเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อปฏิบัติตามกฎหมาย

4.4.4 กรณีที่มีการปฏิเสธการลบข้อมูล ต้องทำการบันทึกคำร้องขอของเจ้าของข้อมูลไว้ด้วย นอกจากนี้เจ้าของข้อมูลมีสิทธิในการร้องเรียนต่อคณะกรรมการผู้เชี่ยวชาญได้

5. หน้าที่ในการระงับการประมวลผลข้อมูล แบ่งออกเป็น 2 กรณี คือ กรณีที่เจ้าของข้อมูลห้ามมิให้ประมวลผล และกรณีที่เจ้าของข้อมูลคัดค้านการประมวลผล

5.1 หน้าที่ในการระงับการประมวลผล เมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผล

5.1.1 เมื่อเจ้าของข้อมูลห้ามมิให้ประมวลผลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ ผู้ควบคุมข้อมูลต้องระงับการประมวลผล (โดยส่วนใหญ่แล้วจะเป็นช่วงระยะเวลาใดเวลาหนึ่ง อันเนื่องมาจากความถูกต้องของข้อมูล หรือลักษณะการประมวลผลข้อมูลไม่ถูกต้อง)

- เจ้าของข้อมูลโต้แย้งความถูกต้องของข้อมูลส่วนบุคคล และอยู่ในระหว่างการตรวจสอบความถูกต้อง
- การประมวลผลข้อมูลส่วนบุคคลเป็นไปโดยมิชอบด้วยกฎหมาย และเจ้าของข้อมูลได้ร้องขอให้มีการห้ามมิให้ประมวลผลแทนการขอให้ลบข้อมูลส่วนบุคคล
- ผู้ควบคุมข้อมูลไม่มีความจำเป็นต้องประมวลผลข้อมูลส่วนบุคคลดังกล่าวต่อไป แต่เจ้าของข้อมูลได้เรียกร้องให้เก็บข้อมูลไว้เพื่อใช้ในการก่อตั้ง ใช้ หรือป้องกันสิทธิเรียกร้องทางกฎหมายของเจ้าของข้อมูล

5.1.2 เจ้าของข้อมูลอาจห้ามมิให้ประมวลผลได้ แม้จะได้ใช้สิทธิ อื่นๆ อยู่แล้วก็ตาม เช่น กรณีการขอห้ามมิให้ประมวลผลในระหว่างท่านตรวจสอบความถูกต้องของข้อมูลตามสิทธิ หรืออยู่ในระหว่างการพิจารณาการระงับการประมวลผลข้อมูลส่วนบุคคลตามสิทธิในการคัดค้านการประมวลผล

5.1.3 การระงับการประมวลผลนั้น อาจกระทำได้หลาย วิธี ขึ้นอยู่กับลักษณะการประมวลผลในรูปแบบต่างๆ โดยอาจระงับการประมวลผล ด้วยวิธีการดังต่อไปนี้

- การเคลื่อนย้ายข้อมูลส่วนบุคคลชั่วคราวไปไว้ที่ระบบการประมวลผลอื่น
- การระงับการให้ผู้ใช้ข้อมูล เข้าถึงข้อมูลชั่วคราว
- การถอนข้อมูลออกจากหน้าเว็บไซต์ หรือ ระบบชั่วคราว

5.1.4 ในกรณีที่ข้อมูลส่วนบุคคลถูกเปิดเผยให้แก่บุคคลที่สาม จะต้องแจ้งให้บุคคลอื่นระงับการประมวลผลด้วย

5.1.5 กรณีที่มีการระงับการประมวลผลข้อมูลส่วนบุคคลแล้ว หากเกิดกรณีดังต่อไปนี้ อาจพิจารณาในการยกเลิกการระงับการประมวลผลและแจ้งให้แก่เจ้าของข้อมูลทราบก่อนการยกเลิกการระงับการประมวลผล พร้อมทั้งแจ้งสิทธิในการดำเนินการต่างๆ ในลักษณะเดียวกับการแจ้งการปฏิเสธสิทธิ

- กรณีที่ตรวจสอบข้อมูลส่วนบุคคลที่ร้องขอแล้วเห็นว่าข้อมูลดังกล่าวถูกต้อง ครบถ้วนสมบูรณ์ หรือเห็นว่ามีสิทธิปฏิเสธไม่ลบข้อมูลตามคำร้องขอ
- กรณีเจ้าของข้อมูลคัดค้านการประมวลผลแล้วเห็นว่ามีสิทธิในการดำเนินการประมวลผลต่อไปตามเหตุแห่งการปฏิเสธ อาทิ การปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ หรือการอ้างผลประโยชน์โดยชอบธรรมเพื่อประมวลผล เป็นต้น
- กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผลข้อมูล จะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ด้วย

5.1.6 ผู้ควบคุมข้อมูลส่วนบุคคล ควรจะต้องระงับการประมวลผลทันทีที่มีการร้องขอจากเจ้าของข้อมูล หรือ จัดให้มีผู้รับผิดชอบในการติดตามการระงับการประมวลผล เพื่อ ตรวจสอบความถูกต้อง

ข้อมูล หรือ อยู่ในระหว่างการพิจารณาฐานตามกฎหมายในการปฏิบัติหรือไม่ปฏิบัติตามสิทธิของเจ้าของข้อมูล

5.2 หน้าที่ในการระงับการประมวลผลเมื่อเจ้าของข้อมูลคัดค้านการประมวลผลข้อมูล

5.2.1 เมื่อเจ้าของข้อมูลคัดค้านการประมวลข้อมูลส่วนบุคคลด้วยเหตุดังต่อไปนี้ จะต้องระงับการประมวลผล

- กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) ที่มีวัตถุประสงค์เพื่อการตลาด แบบตรง (direct marketing) (ไม่มีข้อยกเว้นสำหรับการประมวลผลในลักษณะนี้)
- กรณีที่มีการประมวลผล หรือโปรไฟลิ่ง (profiling) โดยทั่วไป ซึ่งรวมถึงกรณีการปฏิบัติหน้าที่เพื่อประโยชน์สาธารณะ การปฏิบัติตามคำสั่งของเจ้าหน้าที่รัฐ การประมวลผลโดยใช้ฐานผลประโยชน์โดยชอบธรรม ทั้งนี้ เว้นแต่การประมวลผลนั้นสำคัญกว่าผลประโยชน์ สิทธิ เสรีภาพของเจ้าของ ข้อมูล หรือ เป็นการประมวลผลเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติ ตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตาม กฎหมาย
- กรณีข้อมูลที่ประมวลผล หรือโปรไฟลิ่ง (profiling) นั้นเป็นข้อมูลทางการวิจัย เกี่ยวกับวิทยาศาสตร์ ประวัติศาสตร์ หรือ ข้อมูลทางสถิติ ซึ่งมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล ทั้งนี้ เว้นแต่เป็นการประมวลผลเพื่อประโยชน์สาธารณะ

5.2.2 จะต้องแจ้งสิทธิในการคัดค้านการประมวลผลให้แก่เจ้าของข้อมูลทราบ อย่างช้าที่สุด ณ เวลาแรกที่ได้ติดต่อกับเจ้าของข้อมูล โดยทั่วไปแล้ว เมื่อต้องระงับการประมวลผลข้อมูลตามสิทธิการคัดค้านการประมวลผล ผู้ควบคุมข้อมูลจะต้องดำเนินการลบข้อมูลส่วนบุคคลดังกล่าวด้วย ไม่ได้มีข้อยกเว้นให้เก็บข้อมูลได้เช่นเดียวกับกรณีการระงับการประมวลผลข้อมูลตามสิทธิในการห้ามการประมวลผล อย่างไรก็ดี อาจมีบางกรณีที่ไม่ต้องลบข้อมูลส่วน บุคคลดังกล่าว หากท่านยังคงมีความจำเป็นในการประมวลผลตามวัตถุประสงค์อื่นที่เจ้าของข้อมูลมิได้คัดค้าน หรือไม่มีสิทธิคัดค้าน

5.2.3 กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการระงับการประมวลผลข้อมูล ต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ด้วย

6. หน้าที่ในการโอนย้ายข้อมูลส่วนบุคคล

6.1 ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องจัดเตรียมข้อมูลส่วนบุคคลให้อยู่ในรูปแบบที่มีการจัดเรียงแล้ว (structured) ใช้กันทั่วไป และเครื่องคอมพิวเตอร์สามารถอ่านได้ เพื่อเตรียมพร้อมกรณีที่มีการร้องข้อให้มีการโอนย้ายข้อมูลส่วนบุคคลให้แก่ผู้ควบคุมข้อมูลรายอื่น โดยการโอนย้ายข้อมูลนั้นจะต้องไม่มีลักษณะที่เป็นอุปสรรคต่อการประมวลผลของผู้รับโอนย้ายข้อมูล

6.2 ข้อมูลส่วนบุคคลที่ต้องปฏิบัติตามข้อนี้ จะต้องเป็นข้อมูลส่วนบุคคลที่ได้รับมาจากเจ้าของข้อมูลเท่านั้นไม่รวมถึงข้อมูลที่มีการทำให้ไม่สามารถบ่งบอกถึงตัวตนของเจ้าของข้อมูลได้

6.3 การโอนย้ายข้อมูลส่วนบุคคลสามารถกระทำได้ เฉพาะกรณี ดังต่อไปนี้

- ได้รับความยินยอมจากเจ้าของข้อมูล และเป็นข้อมูลที่เกิดจากการประมวลผลด้วย วิธีการอัตโนมัติ
- เป็นการปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล และเป็น ข้อมูลที่เกิดจากการประมวลผลด้วยวิธีการอัตโนมัติ

6.4 ข้อยกเว้น ในการปฏิเสธไม่ดำเนินการโอนย้ายข้อมูล มีดังนี้

- การประมวลผลนั้นเป็นการดำเนินการตามหน้าที่เกี่ยวกับประโยชน์สาธารณะ ผู้ควบคุมข้อมูลเป็นหน่วยงานรัฐที่ใช้อำนาจรัฐเอง
- การดำเนินการดังกล่าวกระทบในด้านลบต่อสิทธิ เสรีภาพของบุคคลอื่นๆ เช่น การ เปิดเผยข้อมูลที่มีความลับทางการค้า (trade secret) หรือ มีทรัพย์สินทางปัญญาของบุคคลอื่นเป็นส่วนหนึ่งของข้อมูลดังกล่าว
- กรณีที่มีการปฏิเสธการปฏิบัติตามสิทธิในการโอนย้ายข้อมูล จะต้องบันทึกคำร้องขอของเจ้าของข้อมูลไว้ด้วย

7. หน้าที่ในการไม่ใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) เพียงอย่างเดียว

7.1 ในกรณีที่ใช้กระบวนการตัดสินใจอัตโนมัติและโปรไฟลิ่ง (profiling) ที่ก่อให้เกิดผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูลส่วนบุคคล ซึ่งมีผลในทางด้านลบอย่างรุนแรง เช่น การจ้างงานออนไลน์ การประมวลผลการทดสอบต่างๆ การประมวลผลข้อมูลเพื่อกำหนดรสนิยมของบุคคล หรือพฤติกรรมของเจ้าของข้อมูล ซึ่งส่วนใหญ่จะเกิดขึ้นในธุรกิจที่เกี่ยวข้องกับการตลาด การเงิน การศึกษา สุขภาพ เป็นต้น ซึ่งเจ้าของข้อมูลมีสิทธิที่จะร้องขอให้ผู้ควบคุมข้อมูลจัดให้มีบุคคลเข้าไปมีส่วนร่วงในการพิจารณาและตัดสินใจในเรื่องนั้นๆ ด้วย โดยไม่ใช้แค่กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียว

7.2 หากมีกรณีดังต่อไปนี้ สามารถที่จะดำเนินการใช้กระบวนการ ตัดสินใจอัตโนมัติเพียงอย่างเดียวได้แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือ ผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม แต่จะต้องมีมาตรการเพื่อปกป้องสิทธิของเจ้าของข้อมูลจากการประมวลผลในรูปแบบดังกล่าว ซึ่งอย่างน้อยจะต้องมีการให้สิทธิเจ้าของข้อมูลในการให้มีบุคคลเข้ามามีส่วนร่วมในการตัดสินใจด้วย หรือ มีสิทธิในการโต้แย้งการตัดสินใจดังกล่าวได้

- กรณีการเข้าทำสัญญา หรือ การปฏิบัติหน้าที่ตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูล
- ต้องได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล

7.3 หากเป็นกรณีมีกฎหมายกำหนดให้สามารถใช้การประมวลผลรูปแบบดังกล่าวได้เพียงอย่างเดียว เช่นกรณีการพิจารณาเรื่องการฉ้อโกง หรือ การเลี่ยงภาษี สามารถที่จะดำเนินการใช้กระบวนการตัดสินใจอัตโนมัติเพียงอย่างเดียวได้ แม้เป็นเรื่องที่กระทบต่อผลทางกฎหมาย หรือผลในลักษณะเดียวกันต่อเจ้าของข้อมูลก็ตาม

7.4 หากเป็นกรณีที่การประมวลผลนั้นเป็นการประมวลผลข้อมูลส่วนบุคคลชนิดพิเศษ จะไม่สามารถกระทำการประมวลผลด้วยกระบวนการตัดสินใจอัตโนมัติเพียงอย่าง เดียวได้ เว้นแต่

- ได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูล
- การประมวลผลมีความจำเป็นเพื่อประโยชน์สาธารณะ

7.5 ตารางเปรียบเทียบสิทธิของเจ้าของข้อมูลและเหตุในการปฏิเสธไม่ดำเนินการตามคำร้องขอ ของเจ้าของข้อมูล

สิทธิ	เหตุแห่งการปฏิเสธการปฏิบัติตามคำร้องของเจ้าของข้อมูล										
	คำขอไม่สมเหตุสมผล	คำขอฟุ่มเฟือย	เจ้าของข้อมูลมีข้อมูลอยู่แล้ว	เก็บเพื่อเสรีภาพในการแสดงความคิดเห็น	เกี่ยวกับการทำตามสัญญา	กฎหมายอนุญาต	เกิดผลกระทบด้านลบแก่บุคคลอื่น	จำเป็นสำหรับการประมวลผล	ประโยชน์สาธารณะหรืออำนาจรัฐ หรือหน้าที่ตามกฎหมาย	ก่อตั้ง ใช้ หรือป้องกันสิทธิทางกฎหมาย	ประโยชน์โดยชอบด้วยกฎหมาย
1.การเพิกถอนความยินยอม	×	×	×	×	×	×	×	×	×	×	×
2.การเข้าถึงข้อมูลส่วนบุคคล	✓	✓	×	×	×	✓	✓	×	×	×	×
3.การแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	✓	✓	×	×	×	×	×	×	×	×	×
4.การลบข้อมูลส่วนบุคคล	✓	✓	×	✓	×	✓	×	✓	✓	✓	×
5.การระงับการประมวลผลข้อมูล.[215]	✓	✓	×	×	×	×	✓	×	✓	✓	×
6.การให้โอนย้ายข้อมูลส่วนบุคคล	✓	✓	×	×	×	×	✓	×	✓	×	×
7.การคัดค้านการประมวลผลข้อมูล	✓	✓	×	×	×	×	×	×	✓	✓	✓
8.การไม่ตกอยู่ภายใต้การตัดสินใจอัตโนมัติเพียงอย่างเดียว	✓	✓	×	×	✓	✓	×	×	✓	×	×

แนวปฏิบัติกรณีมีคำร้องขอหรือคำสั่งขอเข้าถึงข้อมูลส่วนบุคคลจากรัฐ (Government Request)

1. กรณีนี้เป็นกรณีที่หน่วยงานรัฐ หรือองค์กรผู้ถืออำนาจรัฐมีคำร้องขอเข้าถึงข้อมูลส่วนบุคคลเท่านั้น ไม่รวมไปถึงกรณีที่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลมีหน้าที่ตามกฎหมายอยู่แล้วในการรายงานหรือส่งข้อมูลให้แก่ผู้กำกับดูแลตามปกติ เช่น การรายงานธุรกรรมที่ต้องสงสัยตามกฎหมายฟอกเงิน กรณีนี้แม่ไม่มีการร้องขอก็เป็นหน้าที่ตามกฎหมายที่จะต้องทำอยู่แล้ว เป็นต้น กรณีเช่นนี้เมื่อกฎหมายกำหนดให้ต้องทำจึงเป็นฐานในการประมวลผลที่ชอบแล้วเพราะเป็นหน้าที่ตามกฎหมาย (Legal Obligation)
2. ผู้ควบคุมข้อมูลมีหน้าที่ให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ควบคุมข้อมูลส่วนบุคคลจะมีความรับผิดตามกฎหมายจากการให้รัฐเข้าถึงหรือเปิดเผยข้อมูลให้รัฐโดยไม่มีหน้าที่ตามกฎหมาย

3. ผู้ประมวลผลข้อมูลให้หน่วยงานของรัฐ/รัฐบาลเข้าถึงข้อมูลส่วนบุคคลได้เฉพาะเมื่อรัฐมีอำนาจตามกฎหมายเท่านั้น ในขณะเดียวกันตนก็มีความผูกพันกับผู้ควบคุมข้อมูลตามสัญญาว่าจะไม่ให้เข้าถึงหรือเปิดเผยข้อมูลแก่บุคคลอื่น หากรัฐไม่มีอำนาจตามกฎหมาย ผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องไม่ให้รัฐเข้าถึงหรือเปิดเผยข้อมูลส่วนบุคคล มิเช่นนั้นผู้ประมวลผลข้อมูลอาจมีความรับผิดตามกฎหมายและความรับผิดทางสัญญาต่อผู้ควบคุมข้อมูล หากให้รัฐเข้าถึงข้อมูลหรือเปิดเผยข้อมูลดังกล่าวให้รัฐอีกด้วย
4. ขั้นตอนในการพิจารณาดำเนินการเมื่อมีคำร้องขอหรือคำสั่งจากรัฐเพื่อเข้าถึงข้อมูลส่วนบุคคล
   4.1 พิจารณาคำร้องขอ/คำสั่ง โดยระบุหน่วยงาน/องค์กรของรัฐ/เจ้าหน้าที่ ผู้ร้องขอ
   -เจ้าหน้าที่และต้นสังกัด
   -วันที่ได้รับคำร้องขอ
   -ข้อมูลส่วนบุคคลที่ต้องการเข้าถึงหรือให้เปิดเผย
   4.2 ตรวจสอบอำนาจของผู้ร้องขอว่ามีอำนาจตามกฎหมายหรือไม่และมีข้อยกเว้นอย่างไร
   -เจ้าหน้าที่ไม่มีเอกสารมาแสดง
   -เจ้าหน้าที่มีเอกสารมาแสดง (หมายศาล/คำสั่งศาล หรืออื่นๆ)
   4.3 พิจารณาความถูกต้องแท้จริงของเอกสาร (ถ้ามี)
   -กรณีหมายศาล/คำสั่งศาล ให้ดำเนินการตามคำร้องขอ
   -กรณีเอกสารอื่นๆ ให้ตรวจสอบเป็นพิเศษ โดยพิจารณาถึงสถานะของผู้ร้องขอ อำนาจหน้าที่ตามกฎหมาย วัตถุประสงค์ที่จะเข้าถึงข้อมูล และแหล่งอ้างอิงที่มาของอำนาจตามกฎหมายซึ่งต้องเป็นอำนาจเฉพาะ มิใช่อำนาจสืบสวนสอบสวนเป็นการทั่วไปหรืออำนาจที่บัญญัติไว้ กว้างๆ ทำนองว่ามีอำนาจหน้าที่อื่นใดเพื่อให้การปฏิบัติหน้าทีบรรลุวัตถุประสงค์ หากพิจารณาแล้วมีความน่าเชื่อถือและเห็นว่ามีหน้าที่ตามกฎหมายจริง ให้ดำเนินการตามคำร้องขอ
   -กรณีไม่มีเอกสารหรือมีข้อสงสัยเกี่ยวกับเอกสาร ให้ไม่ดำเนินการตาม คำร้องขอจนกว่าจะพิสูจน์ได้ว่าเจ้าหน้าที่มีอำนาจตามกฎหมายจริงหรือมีข้อยกเว้นตามกฎหมาย ประการอื่นที่จะทำให้เข้าถึงหรือเปิดเผยข้อมูลได้ (เช่น เปิดเผยเพื่อประโยชน์สำคัญของเจ้าของข้อมูล (Vital Interest) เป็นต้น)
   -เก็บบันทึกเกี่ยวกับการร้องขอและกระบวนการดำเนินการ/ไม่ดำเนินการตามคำร้อง ขอทั้งหมดตั้งแต่ต้นจนสิ้นสุดกระบวนการ
5. การที่กิจกรรมบางประเภทได้รับยกเว้นไม่ต้องปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 4 นั้น บริษัทยังคงมีหน้าที่ตามพระราชบัญญัตินี้ เนื่องจากกิจกรรมของหน่วยงานรัฐเท่านั้นที่ได้รับยกเว้น ในฐานะเอกชน ไม่ได้รับยกเว้นไปด้วยตามมาตรา 4 ดังนั้นการที่จะเปิดเผยให้หน่วยงานรัฐเข้าถึงข้อมูลนั้น จะต้องมั่นใจว่าบริษัทมีหน้าที่ตามกฎหมายหรือประโยชน์อันชอบธรรมอื่นที่จะเปิดเผยให้แก่หน่วยงานเหล่านั้น มิเช่นนั้นก็จะเป็นการเปิดเผยข้อมูลที่ไม่ชอบด้วยกฎหมาย
6. เพื่อให้มีหลักฐานในกรณีของการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานของรัฐไป ให้ใช้แบบฟอร์มคำขอให้เปิดเผยข้อมูลแก่หน่วยงานของรัฐ เพื่อให้เจ้าหน้าที่หรือหน่วยงานที่ร้องขอมีคำยืนยันถึงอำนาจ หน้าที่ของหน่วยงานและหน้าที่ตามกฎหมายที่บริษัทจะต้องเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานเหล่านั้น

ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครอง

ในส่วนนี้จะได้อธิบายความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษทางปกครองที่ ปรากฏในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 จากการปฏิบัติการฝ่าฝืนหรือขัดต่อกฎหมายดังกล่าวซึ่งแบ่งออกเป็น 3 ส่วนได้แก่ ความรับผิดทางแพ่ง ความรับผิดทางอาญา และโทษ ทางปกครอง

ความรับผิดทางแพ่ง

หากการกระทำที่ฝ่าฝืนหรือไม่เป็นไปตามกฎหมายแล้วย่อมก่อให้เกิดความรับผิดทางแพ่ง

1. การฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่ทำให้เจ้าของข้อมูลเสียหาย ผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องใช้ค่าสินไหมทดแทนไม่ว่าการดำเนินการที่ฝ่าฝืนกฎหมายนั้นจะเป็นการกระทำโดยจงใจหรือประมาทเลินเล่อหรือไม่ เว้นแต่จะพิสูจน์ได้ว่าความเสียหายเกิดจากเหตุสุดวิสัยหรือเกิดจากการกระทำหรือละเว้นการกระทำของเจ้าของข้อมูลส่วนบุคคลนั้นเอง หรือเป็นการปฏิบัติตามคำสั่งของเจ้าหน้าที่ ซึ่งปฏิบัติการตามหน้าที่และอำนาจตามกฎหมาย ทั้งนี้ค่าสินไหมทดแทนยังหมายความรวมถึงค่าใช้จ่ายที่เจ้าของข้อมูลส่วนบุคคลได้ใช้จ่ายไปตามความจำเป็นเพื่อป้องกันความเสียหายที่กำลังจะเกิดขึ้นหรือระงับความเสียหายที่เกิดขึ้นแล้วด้วย
2. นอกจากค่าสินไหมทดแทนแล้ว ศาลอาจสั่งให้มี การจ่ายค่าสินไหมทดแทนเพื่อการลงโทษเพิ่มขึ้นจากจำนวนค่าสินไหมทดแทนที่แท้จริง แต่ไม่เกิน 2 เท่าของค่าสินไหมทดแทนที่แท้จริง
3. การเรียกร้องค่าเสียหายที่เกิดจากการละเมิดข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้มีอายุความ 3 ปี นับแต่วันที่ผู้เสียหายรู้ถึงความเสียหายและรู้ตัวผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ต้องรับผิด หรือ 10 ปี นับแต่วันที่มีการละเมิดข้อมูลส่วนบุคคล

ความรับผิดทางอาญา

1. ความรับผิดทางอาญาของผู้ควบคุมข้อมูลส่วนบุคคลมีดังต่อไปนี้
   1.1 การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย ที่น่าจะทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำ ทั้งปรับ
   1.2 การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหวโดยปราศจากฐานทางกฎหมาย หรือการใช้หรือเปิดเผยข้อมูลส่วนบุคคลซึ่งเป็นข้อมูลอ่อนไหวนอกไปจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือโอนข้อมูลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมาย (โดย

ทุจริต)สำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1,000,000 บาท หรือทั้งจำทั้งปรับ

2. ความผิดฐานเปิดเผยข้อมูลส่วนบุคคล ผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ แล้วนำไปเปิดเผยแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 500,000 บาท หรือทั้งจำทั้งปรับ เว้นแต่จะเป็นการเปิดเผยตามหน้าที่ การเปิดเผยเพื่อประโยชน์แก่การสอบสวนหรือพิจารณาคดี การเปิดเผยแก่หน่วยงานของรัฐ ในประเทศหรือต่างประเทศที่มีอำนาจหน้าที่ตามกฎหมาย การเปิดเผยที่ได้รับความยินยอม เป็นหนังสือเฉพาะครั้งจากเจ้าของข้อมูลส่วนบุคคล หรือการเปิดเผยข้อมูลส่วนบุคคลที่เกี่ยวกับการฟ้องร้องคดีต่างๆ ที่เปิดเผยต่อสาธารณะ
3. กรณีบริษัท เป็นผู้กระทำความผิด ถ้าการกระทำความผิดของบริษัทเกิดจากการสั่งการ หรือการกระทำของกรรมการ หรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของบริษัท หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการ หรือไม่กระทำการจนเป็นเหตุให้บริษัทกระทำความผิด ผู้นั้นต้องรับโทษตามที่กฎหมายบัญญัติไว้สำหรับความผิดนั้นๆ ด้วย

โทษทางปกครอง

โทษทางปกครองของผู้ควบคุมข้อมูลสามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย (มาตรา 24, มาตรา 27)	**ไม่เกิน 3,000,000 บาท**
การไม่ขอความยินยอมให้ถูกต้องตามกฎหมายหรือไม่แจ้งผลกระทบจากการถอนความยินยอม (มาตรา 19)	**ไม่เกิน 1,000,000 บาท**
การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลผิดไปจากวัตถุประสงค์ที่ได้แจ้งไว้โดยไม่ได้แจ้งวัตถุประสงค์ใหม่หรือมีกฎหมายให้ทำได้ (มาตรา 21)	**ไม่เกิน 3,000,000 บาท**
การเก็บรวบรวมข้อมูลเกินไปกว่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล (มาตรา 22)	**ไม่เกิน 3,000,000 บาท**
การเก็บข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรงที่ต้องห้ามตามกฎหมาย (มาตรา 25)	**ไม่เกิน 3,000,000 บาท**
การขอความยินยอมที่เป็นการหลอกลวงหรือทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจผิดในวัตถุประสงค์	**ไม่เกิน 3,000,000 บาท**
การเก็บรวบรวม ใช้ หรือเปิดเผย การโอนข้อมูลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย (มาตรา 26, มาตรา 27, มาตรา 28, มาตรา 29)	**ไม่เกิน 5,000,000 บาท**
การไม่ปฏิบัติตามหน้าที่ความรับผิดชอบ	
การไม่แจ้งเจ้าของข้อมูลทั้งในกรณีเก็บข้อมูลจากเจ้าของข้อมูลโดยตรงหรือโดยอ้อม (มาตรา 23 หรือมาตรา 25)	**ไม่เกิน 1,000,000 บาท**
การไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ (มาตรา 30)	**ไม่เกิน 1,000,000 บาท**
การไม่ดำเนินการตามสิทธิคัดค้านของเจ้าของข้อมูล (มาตรา 32 วรรค 2)	**ไม่เกิน 3,000,000 บาท**

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41)	**ไม่เกิน 1,000,000 บาท**
การไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ หรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา 42)	**ไม่เกิน 1,000,000 บาท**
การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 28, มาตรา 29)	**ไม่เกิน 3,000,000 บาท**
การไม่จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดให้มีระบบตรวจสอบเพื่อลบทำลายข้อมูลหรือไม่ปฏิบัติสิทธิในการลบเมื่อถอนความยินยอมหรือตามสิทธิในการขอลบข้อมูลโดยไม่มีเหตุตามกฎหมาย การไม่แจ้งเหตุละเมิดข้อมูล หรือการไม่ตั้งตัวแทนในราชอาณาจักร	**ไม่เกิน 3,000,000 บาท**

D5.6 โทษทางปกครองของผู้ประมวลผลข้อมูลสามารถสรุปได้ในตารางต่อไปนี้

การกระทำที่เป็นความผิด	โทษปรับทางปกครอง
การไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (มาตรา 41) หรือการไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอย่างเพียงพอ หรือการให้ออกหรือเลิกจ้างเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเพราะเหตุที่ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (มาตรา 42)	**ไม่เกิน 1,000,000 บาท**
การไม่ปฏิบัติตามคำสั่งของผู้ควบคุมข้อมูล การไม่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม การไม่จัดทำบันทึกรายการกิจกรรมการประมวลผล (มาตรา 40)	**ไม่เกิน 3,000,000 บาท**
การโอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 29)	**ไม่เกิน 3,000,000 บาท**
การไม่ตั้งตัวแทนในราชอาณาจักรในกรณีที่กฎหมายกำหนด (มาตรา 38 วรรค 2, มาตรา 37(5))	**ไม่เกิน 3,000,000 บาท**
การโอนข้อมูลอ่อนไหวไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย (มาตรา 29, มาตรา 26)	**ไม่เกิน 5,000,000 บาท**

โทษทางปกครองอื่นๆ

- ตัวแทนของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูล ไม่จัดให้มีบันทึกรายการประมวลผลข้อมูลต้องระวางโทษปรับทางปกครองไม่เกิน 1,000,000 บาท

- ผู้ใดไม่ปฏิบัติตามคำสั่งคณะกรรมผู้เชี่ยวชาญหรือไม่มาชี้แจงข้อเท็จจริง หรือไม่ส่งข้อมูลให้คณะกรรมการผู้เชี่ยวชาญ มีระวางโทษปรับทางปกครองไม่เกิน 500,000 บาท