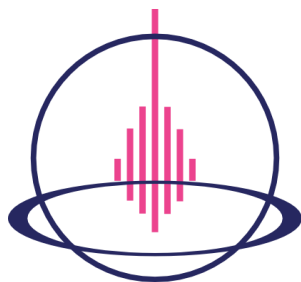




สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่  
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เอกสารผลการรับฟังความเห็นเกี่ยวกับร่างกฎหมายลำดับรองกลุ่มที่ 1

โครงการศึกษาและเตรียมการเพื่อจัดทำร่างกฎหมายลำดับรองภายใต้  
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย



## สารบัญ

สารบัญ .....	3
1. ร่างกฎหมายลำดับรองกลุ่มที่ 1 .....	4
1.1 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการขอความยินยอม จากเจ้าของข้อมูลส่วนบุคคล .....	4
1.2 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการประมวลผล ข้อมูลส่วนบุคคล .....	6
1.3 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการคุ้มครองที่เหมาะสมสำหรับการประมวลผล ข้อมูลส่วนบุคคลตามมาตรา 26 .....	13
1.4 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครอง ข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ .....	17
1.5 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีบันทึกการกิจกรรมประมวลผล การจัด มาตรการเกี่ยวกับการขอใช้สิทธิในการเข้าถึงของเจ้าของข้อมูลส่วนบุคคล และการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล .....	28
1.6 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานความมั่นคงปลอดภัยของการประมวลผล ข้อมูลส่วนบุคคล .....	35
1.7 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล .....	39
1.8 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กระบวนการรับเรื่องร้องเรียน และการบังคับทางปกครอง .....	46

## 1. ร่างกฎหมายลำดับรองกลุ่มที่ 1

### 1.1 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

#### เรื่อง หลักเกณฑ์และวิธีการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

##### สรุปสาระสำคัญของร่างประกาศ

(2.1) กำหนดนิยามคำว่า

“หน่วยงานกำกับดูแล” หมายความว่า หน่วยงานที่มีหน้าที่ควบคุมหรือกำกับดูแลหน่วยงานเฉพาะด้านตามที่กฎหมายอื่นกำหนดผู้ประกอบการธุรกิจเฉพาะ เช่น ธนาคารแห่งประเทศไทย สำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

“สภาวิชาชีพ” หมายความว่า นิติบุคคลที่จัดตั้งขึ้นตามพระราชบัญญัติวิชาชีพเฉพาะ ทำหน้าที่ควบคุมการประกอบวิชาชีพให้ถูกต้องตามจรรยาบรรณแห่งวิชาชีพ การขึ้นทะเบียนและออกใบอนุญาต สั่งพักใช้ใบอนุญาต หรือเพิกถอนใบอนุญาต และรับรองวิทยฐานะของสถาบันที่ทำการสอน รับรองปริญญา ประกาศนียบัตรในวิชาชีพนั้น ๆ

“สมาคมและกลุ่มอุตสาหกรรม” หมายความว่า การรวมกลุ่มของหน่วยงานหรือกิจการเพื่อวัตถุประสงค์ในการส่งเสริมกิจการและประสานงานกับหน่วยงานภาครัฐที่เกี่ยวข้อง

(2.2) แบบหรือข้อความในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่หน่วยงานกำกับดูแลเฉพาะด้านของผู้ควบคุมข้อมูลส่วนบุคคลกำหนด ซึ่งรวมถึงสภาวิชาชีพที่มีอำนาจกำกับดูแลตามกฎหมายเฉพาะด้วย ทั้งนี้ แบบหรือข้อความในการขอความยินยอมต้องไม่ขัดหรือแย้งกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยเฉพาะในกรณีที่กฎหมายเฉพาะกำหนดให้หน่วยงานมีอำนาจออกแบบหรือข้อความในการขอความยินยอมที่มีสภาพบังคับ (compulsory standard form) หน่วยงานกำกับดูแลอาจเสนอแบบหรือข้อความให้คณะกรรมการพิจารณาและให้คำปรึกษาเกี่ยวกับความสอดคล้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

(2.3) สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสนับสนุนให้สมาคมและกลุ่มอุตสาหกรรมร่วมกันจัดทำแบบหรือข้อความในการขอความยินยอมที่เป็นมาตรฐานไว้ โดยอาจเสนอแบบหรือข้อความให้สำนักงานพิจารณาและให้คำปรึกษาเกี่ยวกับความสอดคล้องพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. 2562 ได้ แบบหรือข้อความในการขอความยินยอมที่เป็นมาตรฐานแต่ไม่มีสภาพบังคับ (voluntary standard form) นี้มีวัตถุประสงค์เพื่อจะช่วยให้ปฏิบัติตามกฎหมายได้ง่ายขึ้นในส่วนที่เป็นประเด็นหลัก แม้ไม่ได้มีสภาพบังคับตามกฎหมาย แต่กรณีที่หน่วยงานกำหนดแตกต่างหรือเพิ่มเติมไปจากแบบมาตรฐาน ก็ควรอธิบายให้เจ้าของข้อมูลส่วนบุคคลเข้าใจได้ว่ามีเหตุจำเป็น

- (2.4) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องจัดให้มีแนวปฏิบัติหรือส่งเสริมและสนับสนุนให้หน่วยงานของรัฐ สมาคม กลุ่มอุตสาหกรรม และผู้ควบคุมข้อมูลส่วนบุคคลโดยทั่วไปจัดทำแบบหรือข้อความในการขอความยินยอมที่เป็นมาตรฐานแต่ไม่มีสภาพบังคับ (voluntary standard form) ไม่ขัดหรือแย้งกับหลักเกณฑ์ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (2.5) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลต้องรวบรวมแบบหรือข้อความในการให้ความยินยอมที่หน่วยงานกำกับดูแล สภาวิชาชีพ สมาคม หรือกลุ่มอุตสาหกรรมกำหนดหรือจัดทำเป็นสารบบ (directory) เพื่อสะดวกต่อการเข้าถึงของผู้ควบคุมข้อมูลส่วนบุคคลและการตรวจสอบของเจ้าของข้อมูลส่วนบุคคล

## 1.2 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การแจ้งวัตถุประสงค์และรายละเอียดในการประมวลผลข้อมูลส่วนบุคคล

### สรุปสาระสำคัญของร่างประกาศฯ

#### (2.1) กำหนดนิยามคำว่า

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“หน่วยงานกำกับดูแล” หมายความว่า หน่วยงานที่มีหน้าที่ควบคุมหรือกำกับดูแลหน่วยงานเฉพาะด้านตามที่กฎหมายอื่นกำหนดผู้ประกอบการธุรกิจเฉพาะ เช่น ธนาคารแห่งประเทศไทย สำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

“สภาวิชาชีพ” หมายความว่า นิติบุคคลที่จัดตั้งขึ้นตามพระราชบัญญัติวิชาชีพเฉพาะ ทำหน้าที่ควบคุมการประกอบวิชาชีพให้ถูกต้องตามจรรยาบรรณแห่งวิชาชีพ การขึ้นทะเบียนและออกใบอนุญาต สั่งพักใช้ใบอนุญาต หรือเพิกถอนใบอนุญาต และรับรองวิทยฐานะของสถาบันที่ทำการสอน รับรองปริญญา ประกาศนียบัตรในวิชาชีพนั้น ๆ

“สมาคมและกลุ่มอุตสาหกรรม” หมายความว่า การรวมกลุ่มของหน่วยงานหรือกิจการเพื่อวัตถุประสงค์ในการส่งเสริมกิจการและประสานงานกับหน่วยงานภาครัฐที่เกี่ยวข้อง

“ปัญญาประดิษฐ์” หมายความว่า ระบบปฏิบัติการที่แสดงผลในมิติทางกายภาพหรือทางดิจิทัลโดยมีความสามารถในการรับรู้สภาพแวดล้อมผ่านการรับข้อมูล การตีความข้อมูลที่มีโครงสร้างหรือไม่มีโครงสร้างซึ่งถูกรวบรวมไว้ การให้เหตุผล หรือการประมวลผลจากข้อมูลที่ได้รับและตัดสินใจดำเนินการด้วยวิธีการที่ดีที่สุดเพื่อให้บรรลุเป้าหมายที่กำหนด ทั้งนี้ โดยเรียนรู้จากแบบจำลองตัวเลข การใช้สัญลักษณ์ หรือปรับเปลี่ยนพฤติกรรมโดยวิเคราะห์จากสภาพแวดล้อมที่ได้รับผลกระทบจากการกระทำก่อนหน้า

“เทคโนโลยีสมัยใหม่” หมายความว่า เทคโนโลยีอื่น ๆ นอกจากปัญญาประดิษฐ์ที่ยังไม่เป็นที่รู้จักอย่างแพร่หลาย และอาจมีผลกระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลในลักษณะเดียวกับปัญญาประดิษฐ์ ทั้งนี้คณะกรรมการอาจประกาศกำหนดชนิดของเทคโนโลยีเพิ่มเติมก็ได้

“ข้อมูลเชิงคุณภาพ” หมายความว่า ข้อมูลที่แสดงถึงสถานภาพ คุณลักษณะ หรือคุณสมบัติ เช่น เพศ เชื้อชาติ สถานภาพสมรส ศาสนา กลุ่มเลือด เป็นต้น

“ข้อมูลเชิงปริมาณ” หมายความว่า ข้อมูลที่อยู่ในรูปตัวเลข (numerical data) ที่แสดงถึงปริมาณ อาจเป็นค่าที่ไม่ต่อเนื่อง (discrete) คือค่าที่เป็นจำนวนเต็มหรือจำนวนนับ เช่น จำนวนรถยนต์ในกรุงเทพมหานคร จำนวนบุตรในครอบครัว เป็นต้น หรือเป็นค่าที่ต่อเนื่อง (continuous) คือค่าที่มีจุดทศนิยมได้ เช่น ความสูง น้ำหนัก อายุ อัตราเงินเฟ้อ สถิติน้ำฝนในปีต่าง ๆ เป็นต้น

“ความถี่ของข้อมูลในเชิงเวลา” หมายความว่า จำนวนครั้ง หรือจำนวนรอบของการเก็บรวบรวมข้อมูลที่เกิดขึ้นในช่วงเวลาหนึ่ง เช่น สองครั้งต่อชั่วโมง ทุกครั้งที่มีการเข้าใช้งาน เป็นต้น

(2.2) การแจ้งวัตถุประสงค์ที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ก่อนหน้าตามมาตรา 21 จะถือว่าเจ้าของข้อมูลส่วนบุคคลได้รับแจ้งวัตถุประสงค์ที่แตกต่างไปนั้นแล้ว ถ้าผู้ควบคุมข้อมูลส่วนบุคคลพิสูจน์ได้ว่าได้แจ้งข้อมูลนั้นอย่างชัดเจน โปร่งใส สามารถเข้าใจ และเข้าถึงได้ตามวิสัยและพฤติการณ์ของบุคคลทั่วไป หรือบุคคลซึ่งตามปกติการแจ้งวัตถุประสงค์นั้นต้องกระทำโดยอาศัยมาตรฐานที่สูงกว่าระดับของบุคคลทั่วไป เพื่อประโยชน์แห่งการพิสูจน์ นอกเหนือไปจากความในมาตรา 23 ในระหว่างที่แจ้งวัตถุประสงค์ใหม่ ผู้ควบคุมข้อมูลส่วนบุคคลต้องแสดงให้เห็นถึงรายละเอียดอย่างน้อยดังต่อไปนี้

- ความแตกต่างระหว่างวัตถุประสงค์เดิมและวัตถุประสงค์ที่แตกต่างไป และจัดให้มีการเข้าถึงโดยเจ้าของข้อมูลส่วนบุคคลซึ่งเนื้อหาของการแจ้งวัตถุประสงค์ที่ได้แจ้งไว้แล้วในครั้งที่ผ่านมา
- ฐานในการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 24 หรือมาตรา 26 วรรคหนึ่ง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ผลกระทบที่อาจเกิดขึ้นต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่เกิดจากวัตถุประสงค์ใหม่
- ประโยชน์ที่อาจเกิดขึ้นต่อผู้มีส่วนได้เสียของวัตถุประสงค์ที่แตกต่างไปอันหมายรวมถึงถึงเจ้าของข้อมูลส่วนบุคคล และผู้ควบคุมข้อมูลส่วนบุคคล
- วัน เวลา เครื่องหมายแสดงเวลา หรือข้อมูลอื่นใดอันจะทำให้ทราบได้ว่าการแจ้งวัตถุประสงค์ใหม่นั้นเกิดขึ้นเมื่อใด

ผู้ควบคุมข้อมูลส่วนบุคคลอาจให้เจ้าของข้อมูลส่วนบุคคลตอบรับการแจ้งวัตถุประสงค์นั้น ๆ เพื่อเป็นหลักฐานในการพิสูจน์ถึงการเข้าถึงได้ของการแจ้งวัตถุประสงค์ก็ได้ โดยกระทำด้วยวิธีการที่เหมาะสมกับวิธีการซึ่งผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้เพื่อแจ้งวัตถุประสงค์นั้น ๆ และไม่เป็นภาระต่อเจ้าของข้อมูลส่วนบุคคลมากเกินไป

- (2.3) กรณีที่เป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ให้ถือว่าวัตถุประสงค์ดังกล่าวเป็นวัตถุประสงค์ที่เคยแจ้งไว้โดยชอบ หากผู้ควบคุมข้อมูลส่วนบุคคลสามารถแสดงให้เห็นถึงการพิจารณาปัจจัยดังต่อไปนี้
- วัตถุประสงค์ใหม่มีความเกี่ยวข้องกับวัตถุประสงค์เดิมที่แจ้งไว้โดยชอบแล้ว
  - บริบทในขั้นตอนการเก็บรวบรวมข้อมูล โดยพิจารณาถึงความสัมพันธ์ระหว่างผู้ควบคุมข้อมูลส่วนบุคคลกับเจ้าของข้อมูลส่วนบุคคล และความคาดหมายได้ตามสมควรถึงวัตถุประสงค์ใหม่ของเจ้าของข้อมูลส่วนบุคคล
  - ลักษณะของข้อมูลส่วนบุคคลที่เกี่ยวข้องโดยเฉพาะข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  - ผลกระทบต่าง ๆ ที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากการประมวลผลตามวัตถุประสงค์ใหม่นั้นน้อยกว่าประโยชน์ที่เกิดขึ้นจากการประมวลผลดังกล่าว โดยเฉพาะหากผลประโยชน์ดังกล่าวนั้นเกิดแก่สังคมโดยรวม
  - มีการใช้มาตรการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลโดยเหมาะสมกับลักษณะของข้อมูลและสภาพแวดล้อมของข้อมูล เช่น การเข้ารหัสหรือการทำข้อมูลแฝง
- การประมวลผลข้อมูลส่วนบุคคลนี้ ต้องมีการจดบันทึกไว้ในบันทึกการปฏิบัติตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (2.4) ในกรณีที่วัตถุประสงค์ที่แจ้งนั้นเป็นการประมวลผลด้วยปัญญาประดิษฐ์ หรือเทคโนโลยีสมัยใหม่ เพื่อให้เกิดความชัดเจนและคาดหมายได้โดยบุคคลทั่วไป หรือบุคคลซึ่งตามปกติการแจ้งวัตถุประสงค์นั้นต้องกระทำโดยอาศัยมาตรฐานที่สูงกว่าระดับของบุคคลทั่วไป และเพื่อประโยชน์แห่งการพิสูจน์คณะกรรมการออกประกาศเพื่อกำหนดรายละเอียดอันเกี่ยวข้องกับเรื่องดังกล่าวก็ได้
- (2.5) ในกรณีที่บทบัญญัติแห่งพระราชบัญญัตินี้ หรือกฎหมายอื่นบัญญัติให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้แจ้งไว้ได้ตามมาตรา 21 วรรคสอง (2) ให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องทำบันทึกรายละเอียดของบทบัญญัติหรือกฎหมายที่ใช้อ้างอิงนั้นไว้ก่อนหรือในขณะที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่แตกต่างไปจากวัตถุประสงค์ที่ได้เคยแจ้งไว้
- (2.6) การแจ้งวัตถุประสงค์จะต้องเป็นไปเพื่อให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับแจ้งวัตถุประสงค์เข้าใจถึงวัตถุประสงค์ดังกล่าวโดยชัดเจนตามแต่วิสัยและพฤติการณ์ ซึ่งต้องพิจารณาถึงความสามารถในความ



เข้าใจถึงวัตถุประสงค์ต่าง ๆ ของเจ้าของข้อมูลส่วนบุคคลจนถึงขนาดที่ประเมินได้ถึงผลกระทบและผลประโยชน์ที่อาจเกิดกับตนที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ได้แจ้งไว้

(2.7) ภายใต้ข้อยกเว้นไม่จำเป็นต้องแจ้งวัตถุประสงค์ใหม่หรือรายละเอียดต่อเจ้าของข้อมูลส่วนบุคคล การเก็บรวบรวมข้อมูลส่วนบุคคลที่กระทำต่อเจ้าของข้อมูลส่วนบุคคลโดยตรง หรือแหล่งอื่นอันไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งรายละเอียดของข้อมูลส่วนบุคคลที่เก็บรวบรวมต่อเจ้าของข้อมูลส่วนบุคคล ไม่ว่าจะการประมวลผลนั้นจะกระทำเพื่อวัตถุประสงค์ใดในมาตรา 24 หรือมาตรา 26 ก็ตาม เว้นแต่สามารถพิสูจน์ข้อยกเว้นตามมาตรา 23 หรือมาตรา 25 ได้แล้วแต่กรณี

(2.8) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งวัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลอย่างชัดเจนเพียงพอให้เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายและเข้าใจถึงผลกระทบที่อาจเกิดขึ้นจากการให้ข้อมูลส่วนบุคคลนั้นตามวิสัยและพฤติการณ์ของบุคคลทั่วไปหรือบุคคลซึ่งตามปกติการแจ้งวัตถุประสงค์นั้นต้องกระทำโดยอาศัยมาตรฐานที่สูงกว่าระดับของบุคคลทั่วไป โดยแสดงให้เห็นได้ว่าการพิจารณาถึงปัจจัยดังต่อไปนี้

- ความครบถ้วนสมบูรณ์ของวัตถุประสงค์ในการประมวลผล
- ความง่ายในการเข้าใจของวัตถุประสงค์ในการประมวลผล
- ความชัดเจนและโดดเด่นที่สามารถดึงดูดความสนใจของเจ้าของข้อมูลส่วนบุคคลได้
- ความเป็นมาตรฐานเดียวกันระหว่างสินค้าและบริการของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งอาจรวมถึงตำแหน่งของการแจ้ง ขนาดและสีของตัวอักษรหรือรูปภาพ การเลือกระหว่างตัวอักษรและรูปภาพ และลักษณะของภาษาที่ใช้ในการสื่อสาร
- ความสอดคล้องกับบริบทในการแจ้งวัตถุประสงค์นั้น ๆ อันจะทำให้เจ้าของข้อมูลส่วนบุคคลสามารถทำความเข้าใจข้อมูลได้ง่ายขึ้น และมีการตัดสินใจที่มีประสิทธิภาพมากขึ้น ซึ่งอาจรวมถึง ตำแหน่งของการแจ้ง ขนาดและสีของตัวอักษรหรือรูปภาพ การเลือกระหว่างตัวอักษรและรูปภาพ และลักษณะของภาษาที่ใช้ในการสื่อสาร

เพื่อประโยชน์แห่งการพิสูจน์ผู้ควบคุมข้อมูลส่วนบุคคลอาจจัดทำรายงานที่มีการระบุรายละเอียดของการพิจารณาถึงปัจจัยดังกล่าวไว้เป็นหลักฐานก็ได้

(2.9) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคลที่จะเก็บรวบรวมให้เจ้าของข้อมูลส่วนบุคคลทราบโดยง่าย ซึ่งการแจ้งนั้นต้องแสดงให้เห็นให้เจ้าของข้อมูลส่วนบุคคลสามารถคาดหมายได้ถึงลักษณะของข้อมูล ทั้งนี้ โดยแจ้งภายใต้ประเภทของข้อมูลส่วนบุคคล ดังต่อไปนี้

- ข้อมูลส่วนบุคคลทั่วไปอันมิใช่ข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

นอกจากประเภทของข้อมูลส่วนบุคคลตามความในวรรคก่อนแล้ว ในกรณีที่สามารถแจ้งได้ และไม่ส่งผลกระทบต่อผลประโยชน์ของผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลจนเกินควร ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดเกี่ยวกับข้อมูลส่วนบุคคล ดังต่อไปนี้

- กลุ่มของเจ้าของข้อมูลส่วนบุคคล อาทิ พนักงาน ผู้ใช้บริการ คู่ค้า เป็นต้น
- วัตถุประสงค์ที่ข้อมูลถูกนำไปใช้เพื่อบรรลุวัตถุประสงค์นั้น ๆ
- ความถี่ของข้อมูลในเชิงเวลา
- รายละเอียดของข้อมูลในเชิงปริมาณ และคุณภาพ
- รายละเอียดอื่น ๆ อันอาจส่งผลกระทบต่อความคาดหมายต่อผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

(2.10) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งให้ทราบถึงกรณีที่เจ้าของข้อมูลส่วนบุคคลต้องให้ข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย หรือสัญญา หรือความจำเป็นอื่นที่เจ้าของข้อมูลส่วนบุคคลต้องกระทำเพื่อเข้าทำสัญญา รวมทั้งต้องแจ้งถึงผลกระทบที่เป็นไปได้จากการไม่ให้ข้อมูลส่วนบุคคลนั้นเพื่อให้เกิดความชัดเจนและคาดหมายได้โดยบุคคลทั่วไป หรือบุคคลซึ่งตามปกติการแจ้งวัตถุประสงค์นั้นต้องกระทำโดยอาศัยมาตรฐานที่สูงกว่าระดับของบุคคลทั่วไป

(2.11) ในการกำหนดระยะเวลาในการเก็บรวบรวมที่ไม่อาจกำหนดได้ชัดเจนตามมาตรา 23 (3) ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิสูจน์ว่าการกำหนดระยะเวลาดังกล่าวเป็นระยะเวลาที่จำเป็นเท่าที่ต้องใช้ในวัตถุประสงค์นั้น ๆ พร้อมทั้งแสดงให้เห็นว่าเป็นระยะเวลาที่อาจคาดหมายได้โดยเจ้าของข้อมูลส่วนบุคคล หรือผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการเท่าที่จำเป็นเพื่อให้เกิดความคาดหมายดังกล่าว

(2.12) การแจ้งประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผยตามมาตรา 23 (4) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งให้ชัดเจนเป็นรายบุคคลหรือหน่วยงาน หรือหากไม่สามารถทำได้ ให้ระบุ เหตุอันเป็นอุปสรรคต่อการแจ้งรายละเอียดดังกล่าว พร้อมทั้งแจ้ง

รายละเอียดเท่าที่เพียงพอที่จะทำให้เจ้าของข้อมูลส่วนบุคคลเข้าใจถึงลักษณะของบุคคล หน่วยงาน หรือ กลุ่มของบุคคลหรือหน่วยงานนั้น ๆ ซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจถูกเปิดเผยเพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถระบุตัวตนได้โดยง่าย และสามารถคาดหมายได้ถึงประเภทข้อมูลที่อาจถูกเปิดเผยต่อบุคคลหรือหน่วยงานของตน หากเป็นกรณีที่มีบุคคลหรือหน่วยงานจำนวนมาก และเปลี่ยนแปลงอย่างสม่ำเสมอ ผู้ควบคุมข้อมูลส่วนบุคคลอาจยกตัวอย่างเท่าที่จำเป็นต่อความเข้าใจของเจ้าของข้อมูลส่วนบุคคล และจัดทำรายชื่อที่มีรายละเอียดไว้แยกต่างหากก็ได้ แต่ต้องแสดงให้เห็นเจ้าของข้อมูลส่วนบุคคลรับทราบถึงการมีอยู่ และสามารถเข้าถึง หรือทำคำขอในการเข้าถึงรายชื่อดังกล่าวได้โดยสะดวก โดยต้องมีการทำให้รายละเอียดดังกล่าวเป็นปัจจุบันและถูกต้องตามสมควร หากเป็นกรณีอื่นไม่สามารถแจ้งให้ชัดแจ้งเป็นรายบุคคลหรือหน่วยงานได้ รายละเอียดการแจ้งนั้นให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่หน่วยงานกำกับดูแลเฉพาะด้านของผู้ควบคุมข้อมูลส่วนบุคคลกำหนด ซึ่งรวมถึงสภาวิชาชีพที่มีอำนาจกำกับดูแลตามกฎหมายเฉพาะด้วย ทั้งนี้ รายละเอียดการแจ้งต้องไม่ขัดหรือแย้งกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยหน่วยงานกำกับดูแลอาจเสนอรายละเอียดการแจ้งให้คณะกรรมการพิจารณาและให้คำปรึกษาเกี่ยวกับความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้

- (2.13) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อ ทั้งนี้ ในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลนั้นด้วย
- (2.14) ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 19 วรรคห้า มาตรา 30 วรรคหนึ่ง มาตรา 31 วรรคหนึ่ง มาตรา 32 วรรคหนึ่ง มาตรา 33 วรรคหนึ่ง มาตรา 34 วรรคหนึ่ง มาตรา 36 วรรคหนึ่ง และมาตรา 73 วรรคหนึ่ง แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (2.15) หน่วยงานกำกับดูแล สภาวิชาชีพ สมาคม หรือกลุ่มอุตสาหกรรม อาจร่วมกันกำหนดรูปแบบ วิธีการ และมาตรฐานขั้นต่ำของการแจ้งวัตถุประสงค์ที่เหมาะสมกับผู้ควบคุมข้อมูลส่วนบุคคลภายใต้การกำกับดูแล หรือภายในกลุ่มดังกล่าว โดยเสนอต่อคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อพิจารณาและให้คำปรึกษาเกี่ยวกับความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทั้งนี้หากคณะกรรมการพิจารณาแล้วเห็นว่าสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้มีการประกาศไว้เป็นการทั่วไปเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถเข้าถึงข้อมูลได้โดยง่าย

- (2.16) ให้ถือว่าการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลที่ต้องกระทำตามที่กฎหมายกำหนดไว้อย่างชัดเจน เป็นกรณีที่เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ใหม่อยู่แล้วตาม มาตรา 25 วรรคสอง (1) ทั้งนี้ ต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคล
- (2.17) ผู้ควบคุมข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรง ไม่จำเป็นต้องแจ้งวัตถุประสงค์หรือรายละเอียดต่อเจ้าของข้อมูลส่วนบุคคล เมื่อพิสูจน์ได้ว่าการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลดังกล่าวไม่สามารถกระทำได้ด้วยเหตุที่มีพฤติการณ์บางอย่างเกิดขึ้นชัดเจนไม่ให้ผู้ควบคุมข้อมูลส่วนบุคคลกระทำการเช่นนั้น หรือเป็นการแจ้งที่ทำให้วัตถุประสงค์ของการประมวลผลต่อค่าลงอย่างมีนัยสำคัญ โดยต้องจัดบันทึกเหตุดังกล่าวไว้อย่างชัดเจน หากพฤติการณ์ที่ชัดเจนนั้นสิ้นสุดลง ผู้ควบคุมข้อมูลส่วนบุคคลต้องรีบแจ้งข้อมูลดังกล่าวแก่เจ้าของข้อมูลส่วนบุคคลโดยพลัน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลอาจจัดทำแนวปฏิบัติ หรือคู่มือเพื่อสร้างความชัดเจนถึงข้อยกเว้นไว้ก็ได้
- (2.18) ถ้าการใช้หรือเปิดเผยข้อมูลส่วนบุคคลใดก่อให้เกิดอุปสรรคเป็นอย่างมากต่อผู้ควบคุมข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมข้อมูลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลส่วนบุคคลโดยตรงและเมื่อประเมินผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคลที่ไม่ได้รับการแจ้งข้อมูลแล้วปรากฏว่ามีน้อยกว่าหากเปรียบเทียบกับอุปสรรคและผลประโยชน์ที่อาจเกิดขึ้น ผู้ควบคุมข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งวัตถุประสงค์หรือรายละเอียดดังกล่าว หากการใช้หรือเปิดเผยข้อมูลส่วนบุคคลเป็นไปเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับการศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ ให้พิจารณาเป็นกรณีที่มีผลประโยชน์ที่อาจเกิดขึ้นอย่างมากกว่าผลกระทบที่อาจเกิดขึ้นต่อเจ้าของข้อมูลส่วนบุคคล หากมีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล เว้นแต่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลพบว่าข้อเท็จจริงปรากฏเป็นอย่างอื่นหรือมีเหตุควรสงสัยเป็นอย่างอื่น ทั้งนี้ให้เป็นไปตามประกาศกำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- (2.19) มาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ เสรีภาพ และประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ต้องเป็นมาตรการที่เหมาะสมกับผลกระทบที่อาจเกิดขึ้นจากการไม่แจ้งวัตถุประสงค์ใหม่หรือรายละเอียดต่อเจ้าของข้อมูลส่วนบุคคล ทั้งนี้ มาตรการดังกล่าวควรมีความชัดเจนและคาดหมายได้โดยบุคคลทั่วไปหรือบุคคลซึ่งตามปกติการแจ้งวัตถุประสงค์นั้นต้องกระทำโดยอาศัยมาตรฐานที่สูงกว่าระดับของบุคคลทั่วไป เพื่อประโยชน์แห่งการพิสูจน์ในวรรคแรก นอกจากประกาศกำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้มีหน้าที่แจ้งวัตถุประสงค์ใหม่หรือรายละเอียดอาจอ้างถึงมาตรฐานการคุ้มครองอันเป็นที่ยอมรับโดยทั่วไป หรือเป็นสากลก็ได้

### 1.3 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

#### เรื่อง มาตรการคุ้มครองที่เหมาะสมสำหรับการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26

##### สรุปสาระสำคัญของร่างประกาศฯ

(2.1) กำหนดนิยามคำว่า

“ข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม” หมายความว่า ข้อมูลส่วนบุคคลเกี่ยวกับการสืบสวนสอบสวนความผิด การดำเนินคดี หรือการลงโทษทางอาญา ที่เป็นข้อมูลที่เป็นทางการและรับรองโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่เกี่ยวกับข้อมูลประวัติอาชญากรรมนั้น ทั้งนี้ไม่ว่าคดีจะถึงที่สุดแล้วหรือไม่ก็ตาม

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

(2.2) ให้ใช้บังคับแก่การประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อวัตถุประสงค์ที่กำหนดไว้ตามมาตรา 26 วรรคหนึ่ง (2), (5)(ข), (5)(ค) และ (5)(จ) และการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมตามมาตรา 26 วรรคสาม ที่มีได้อยู่ในความควบคุมของหน่วยงานที่มีอำนาจหน้าที่ตามกฎหมาย

(2.3) ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แสดงให้เห็นว่าตนได้ประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ใดตามที่มาตรา 24 และมาตรา 26 วรรคหนึ่งแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ประมวลผลได้

(2.4) ถ้าผู้ควบคุมข้อมูลส่วนบุคคลมีการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในการแจ้งเจ้าของข้อมูลส่วนบุคคลเมื่อเก็บรวบรวมข้อมูลตามมาตรา 23 หรือมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วแต่กรณี และบันทึกรายการที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดทำขึ้นตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จะต้องปรากฏรายละเอียดวัตถุประสงค์ที่ให้ประมวลผลข้อมูลส่วนบุคคลได้ตามที่มาตรา 24 และมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด

(2.5) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้เหมาะสมกับ

ความเสี่ยงที่มีต่อสิทธิเสรีภาพของบุคคลและจะต้องไม่น้อยไปกว่ามาตรฐานขั้นต่ำที่ประกาศกำหนด โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2.6) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีนโยบายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงได้ โดยอาจเป็นส่วนหนึ่งของนโยบายคุ้มครองข้อมูลส่วนบุคคลโดยทั่วไปก็ได้ ทั้งนี้ต้องมีรายละเอียดต่อไปนี้เป็นอย่างน้อย

- คำอธิบายเกี่ยวกับกิจกรรมประมวลผลข้อมูล ซึ่งอาจอ้างอิงถึงกิจกรรม รายการใดรายการหนึ่งหรือหลายรายการในบันทึกรายการตามมาตรา 39 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ก็ได้
- วัตถุประสงค์ตามที่มาตรา 24 และมาตรา 26 วรรคหนึ่งแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ประมวลผลได้โดยปราศจากความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และคำอธิบายความจำเป็นที่ต้องประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ดังกล่าว
- รายละเอียดอื่น ๆ ตามมาตรา 23 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เท่าที่ไม่ซ้ำกับความใน (1) และ (2)
- นโยบายเกี่ยวกับการเก็บรักษาข้อมูลและทำลายข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งอาจอ้างอิงถึงนโยบายเกี่ยวกับการเก็บรักษาข้อมูลและทำลายข้อมูลส่วนบุคคลทั่วไปก็ได้

(2.7) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีกำหนดระยะเวลาเก็บรักษาและทำลายข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่เหมาะสม ระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลจะต้องกำหนดไว้เท่าที่จำเป็นตามวัตถุประสงค์ของการประมวลผล โดยผู้ควบคุมข้อมูลส่วนบุคคลจะต้องสามารถแสดงให้เห็นถึงความจำเป็นในการกำหนดระยะเวลาเช่นนั้น ความจำเป็นดังกล่าวอาจเป็นไปตามข้อกำหนดโดยกฎหมาย มาตรฐานหรือแนวปฏิบัติในทางธุรกิจ หรือวิชาชีพ หรือความจำเป็นที่กำหนดโดยผู้ควบคุมข้อมูลส่วนบุคคลเอง ในกรณีที่ไม่มีข้อกำหนดตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่พิสูจน์ให้เห็นถึงความจำเป็นสำหรับระยะเวลาในการเก็บรักษาข้อมูลดังกล่าว ทั้งนี้หากผู้ควบคุมข้อมูลส่วนบุคคลสามารถพิสูจน์ได้ว่าตนได้ปฏิบัติตามข้อปฏิบัติที่ประกาศกำหนดโดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลแล้วให้สันนิษฐานไว้ก่อนว่าระยะเวลาในการเก็บรักษาข้อมูลดังกล่าวมีความจำเป็นตามวัตถุประสงค์ของการประมวลผล

- (2.8) หากผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมโดยอาศัยความยินยอม จะต้องได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลส่วนบุคคลหรือวิธีการอื่นที่เทียบเท่า ทั้งนี้ความยินยอมที่ได้รับนั้นจะต้องเป็นไปตามเงื่อนไขที่กำหนดโดยมาตรา 19 และมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วย ผู้ควบคุมข้อมูลส่วนบุคคลจะประมวลผลข้อมูลเกี่ยวกับประวัติอาชญากรรมในกระบวนการรับบุคคลเข้าทำงานหรือการตรวจสอบบุคคลที่จะมาดำรงตำแหน่งในองค์กรจะกระทำต่อเมื่อมีกฎหมายบัญญัติให้ต้องตรวจสอบคุณสมบัติว่าไม่มีการกระทำความผิดเท่านั้น กรณีนอกจากนั้นให้ขอความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล การไม่ให้ความยินยอมในการตรวจสอบข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมจะนำมาเป็นเหตุแห่งการปฏิเสธการรับเข้าทำงานหรือการดำรงตำแหน่งของบุคคลมิได้ เว้นแต่ตำแหน่งงานหรือตำแหน่งของบุคคลนั้นจะมีความสำคัญอย่างยิ่งถึงขนาดที่มีความจำเป็นในการตรวจสอบข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมของบุคคลเสียก่อน ในกรณีเช่นนี้ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งความจำเป็นดังกล่าวตั้งแต่เริ่มต้นขั้นตอนการประกาศรับสมัครคณะกรรมการอาจประกาศข้อปฏิบัติเกี่ยวกับตำแหน่งงานหรือตำแหน่งของบุคคลที่มีความสำคัญอย่างยิ่งถึงขนาดที่มีความจำเป็นในการตรวจสอบข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมของบุคคลตามวรรคก่อนได้
- (2.9) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลอาศัยความยินยอมในการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม จะต้องแจ้งถึงผลกระทบของการไม่ให้ความยินยอมแก่เจ้าของข้อมูลส่วนบุคคลด้วย
- (2.10) ในกรณีที่ไม่มีกฎหมายอื่นบัญญัติไว้โดยเฉพาะหรือเหตุจำเป็นอื่นใดภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 26 การประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมของบุคคลเพื่อวัตถุประสงค์ในการสอบประวัติบุคคลเพื่อรับเข้าทำงาน เมื่อมีการรับเข้าหรือปฏิเสธการรับเข้าแล้วให้เก็บรักษาข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรมได้ไม่เกิน 6 เดือนนับแต่วันที่มีการตัดสินใจรับเข้าหรือปฏิเสธการรับเข้าสำหรับเจ้าของข้อมูลส่วนบุคคลรายนั้น เมื่อสิ้นสุดระยะเวลาเก็บรักษาหรือสิ้นสุดความจำเป็นในการประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม ให้ผู้ควบคุมข้อมูลส่วนบุคคลทำลายข้อมูลดังกล่าวหรือทำให้ข้อมูลดังกล่าวกลายเป็นข้อมูลนิรนามด้วยวิธีการที่เหมาะสม ทั้งนี้ผู้ควบคุมข้อมูลส่วนบุคคลอาจบันทึกข้อมูลไว้ได้เท่าที่จำเป็นเพื่อการตรวจสอบในภายหลัง แต่ต้องไม่เกินไปกว่าข้อมูลวันเวลาและผู้รับผิดชอบในการทำลาย วันที่

ตรวจสอบข้อมูลเกี่ยวกับประวัติอาชญากรรม หน่วยงานที่รับรองข้อมูล เลขที่อ้างอิงของเอกสาร และ  
ชื่อของเจ้าของข้อมูลส่วนบุคคลที่มีการตรวจสอบประวัติอาชญากรรม

- (2.11) ผู้ควบคุมข้อมูลส่วนบุคคลอาจมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลดำเนินการแทนได้ ทั้งนี้  
เท่าที่จำเป็นหรือการดำเนินการประมวลผลข้อมูลด้วยตนเองจะเป็นภาระเกินสมควรแก่ผู้ควบคุม  
ข้อมูลส่วนบุคคล

เอกสารผลการรับฟังความเห็นเกี่ยวกับร่างกฎหมายลำดับรองกลุ่มที่ 1



## 1.4 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง กำหนดหลักเกณฑ์และนโยบายการให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ

### สรุปสาระสำคัญของร่างประกาศฯ

#### (2.1) กำหนดนิยามคำว่า

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เครื่องกิจการหรือเครื่องธุรกิจเดียวกัน” หมายถึง ผู้ประกอบกิจการที่มีอำนาจควบคุม หรือกิจการที่ถูกควบคุมโดยผู้ประกอบกิจการที่มีอำนาจเหนือ หรือบุคคลธรรมดาหรือนิติบุคคลที่มีความเกี่ยวข้องกันในการประกอบกิจกรรมทางเศรษฐกิจ

“ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล” หมายถึง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ตกลงจะประมวลผลข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนโดยผู้ส่งหรือโอนข้อมูลส่วนบุคคล

“ผู้ส่งหรือโอนข้อมูลส่วนบุคคล” หมายถึง ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ส่งหรือโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล

“ระบบคลาวด์” หมายถึง ระบบที่ให้บริการการเข้าถึงทรัพยากรคอมพิวเตอร์ เช่น ระบบการเก็บข้อมูล (storage) การประมวลผลข้อมูล และซอฟต์แวร์ ตามความต้องการของผู้ใช้บริการผ่านระบบการส่งผ่านข้อมูล

“ผู้ให้บริการระบบคลาวด์” หมายถึง บุคคลที่เป็นเจ้าของและบริหารจัดการระบบคลาวด์โดยมีรูปแบบของการให้บริการเช่น ให้บริการระบบโครงข่ายพื้นฐานด้านเทคโนโลยีสารสนเทศ (IaaS) การให้บริการด้านซอฟต์แวร์ (SaaS) หรือการให้บริการแพลตฟอร์ม (PaaS)

“ส่งหรือโอนข้อมูลส่วนบุคคล” หมายถึง การส่งหรือโอนข้อมูลส่วนบุคคลโดยผู้ส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลระหว่างบุคคลที่ไม่ได้สังกัดอยู่ในองค์กรซึ่งเป็นนิติบุคคลเดียวกัน โดยหมายความรวมถึง การที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอนุญาตให้บุคคลที่อยู่นอกประเทศไทยเข้าถึงข้อมูลระยะไกล และการที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลใช้บริการระบบคลาวด์ ซึ่งตั้งอยู่หรือมีการให้บริการโดยอาศัยระบบที่ตั้งอยู่ในต่างประเทศ แต่มิให้หมายความรวมถึงการส่งผ่าน (Transit) หรือการจัดเก็บ

(Storage) ข้อมูลส่วนบุคคลโดยที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลไม่ได้ประสงค์ให้มีการเข้าถึงหรือ  
แทรกแซงข้อมูลส่วนบุคคลที่ถูกส่งหรือโอน

(2.2) ในการพิจารณาถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือ  
องค์การระหว่างประเทศที่รับการส่งหรือโอนข้อมูลส่วนบุคคล คณะกรรมการจะต้องพิจารณาถึงปัจจัย  
และข้อเท็จจริง ดังต่อไปนี้

- หลักนิติธรรม การคุ้มครองสิทธิมนุษยชนและสิทธิขั้นพื้นฐาน บัญญัติของกฎหมายเกี่ยวกับ  
ความมั่นคงสาธารณะ กลาโหม กฎหมายเกี่ยวกับความมั่นคงของชาติและกฎหมายอาญา  
การเข้าถึงข้อมูลส่วนบุคคลโดยหน่วยงานรัฐและกฎหมายที่ให้อำนาจในการดำเนินการ  
ดังกล่าว กฎเกณฑ์เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล มาตรการคุ้มครองความมั่นคง  
ปลอดภัย ซึ่งหมายรวมถึงกฎเกณฑ์เกี่ยวกับการโอนข้อมูลส่วนบุคคลไปยังประเทศปลายทาง  
หรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลซึ่งบังคับการส่งหรือโอนข้อมูลส่วนบุคคล  
แนวบรรทัดฐานการปรับใช้กฎหมาย ตลอดจนประสิทธิภาพในการคุ้มครองสิทธิของเจ้าของ  
ข้อมูลส่วนบุคคลและประสิทธิภาพในการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล  
ที่ถูกส่งหรือโอนข้อมูลส่วนบุคคลไม่ว่าโดยหน่วยงานทางปกครองหรือองค์กรตุลาการ
- การมีอยู่ของและประสิทธิภาพการทำงานขององค์กรอิสระในประเทศปลายทางหรือองค์การ  
ระหว่างประเทศที่รับข้อมูลส่วนบุคคล ซึ่งมีอำนาจหน้าที่หรือภารกิจในการบังคับใช้กฎเกณฑ์  
เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ซึ่งหมายรวมถึง การมีอำนาจอย่างเพียงพอในการ  
ช่วยเหลือและให้คำปรึกษากับเจ้าของข้อมูลส่วนบุคคลในการใช้สิทธิของตน และการร่วมมือ  
กับคณะกรรมการ และ
- พันธกรณีระหว่างประเทศของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วน  
บุคคลได้เข้าร่วมหรือมีหน้าที่ต้องปฏิบัติตามซึ่งมีผลบังคับทางกฎหมายตามอนุสัญญาหรือ  
ตราสารอื่น ตลอดจนการเข้าร่วมในความร่วมมือระดับภูมิภาคหรือพหุภาคีเกี่ยวกับการ  
คุ้มครองข้อมูลส่วนบุคคล

(2.3) ในกรณีที่คณะกรรมการพิจารณาแล้วเห็นว่าประเทศปลายทางหรือองค์การระหว่างประเทศที่รับ  
ข้อมูลส่วนบุคคลนั้นมีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ให้คณะกรรมการออก  
ประกาศกำหนดให้ประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลดังกล่าวมี  
มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ ในการออกประกาศให้คณะกรรมการกำหนดวิธีการ  
ในการทบทวนมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลในประเทศปลายทางหรือองค์การระหว่าง  
ประเทศที่รับข้อมูลส่วนบุคคลอย่างน้อยทุกสี่ปี

(2.4) ในการตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันตามมาตรา 29 วรรคหนึ่งของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำนักงานจะต้องพิจารณาถึง

- การบังคับใช้ได้ ในทางกฎหมายของนโยบายกับบุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนไปยังประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลซึ่งหมายรวมถึงการมีผลบังคับผูกพันลูกจ้างของบุคคลที่เกี่ยวข้องดังกล่าวอีกด้วย
- การกำหนดรับรองสิทธิของเจ้าของข้อมูลส่วนบุคคลต่อข้อมูลส่วนบุคคลที่ถูกส่งหรือโอน
- การมีรายละเอียดครบถ้วนตามที่กำหนดในประกาศฉบับนี้

(2.5) นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกันจะต้องมีเนื้อหาอย่างน้อยดังต่อไปนี้

- โครงสร้างและข้อมูลเพื่อการติดต่อของบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน
- ข้อมูลส่วนบุคคลที่ถูกส่งหรือโอน ซึ่งหมายรวมถึงประเภทของข้อมูลส่วนบุคคล วัตถุประสงค์ในการประมวลผล ผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล และรายละเอียดของประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล
- ลักษณะของการมีผลบังคับผูกพันทางกฎหมาย ทั้งผลระหว่างในเครือกิจการหรือเครือธุรกิจเดียวกันเพื่อการประกอบกิจการหรือธุรกิจร่วมกัน และผลต่อบุคคลภายนอก
- หลักการในการประมวลผลข้อมูลส่วนบุคคลโดยทั่วไป เช่น การมีวัตถุประสงค์ที่จำกัด การประมวลผลข้อมูลส่วนบุคคลเท่าที่จำเป็น การเก็บรักษาข้อมูลส่วนบุคคลโดยมีระยะเวลาเท่าที่จำเป็น การประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรการคุ้มครองความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และข้อกำหนดในการโอนข้อมูลส่วนบุคคลไปยังบุคคลที่ไม่ตกอยู่ในบังคับของนโยบาย
- สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ความรับผิดชอบของผู้ส่งหรือโอนข้อมูลส่วนบุคคลต่อการที่บุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันฝ่าฝืนนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน โดยมีข้อยกเว้นความรับผิดชอบเฉพาะกรณีที่สามารถพิสูจน์ได้ว่าบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันไม่มีส่วนต้องรับผิดชอบกับความเสียหายที่เกิดขึ้น
- วิธีการในการส่งข้อมูลตาม (4) (5) และ (6) ให้กับเจ้าของข้อมูลส่วนบุคคล
- หน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในการตรวจสอบการปฏิบัติตามนโยบาย การคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน
- ขั้นตอนในการร้องเรียน

- กลไกการตรวจสอบการปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกัน โดยมีรายละเอียดเกี่ยวกับผู้ตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล วิธีการในการแก้ไขการกระทำเพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล โดยผลของการตรวจสอบจะต้องถูกส่งไปยังเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามข้อ 9 และคณะกรรมการที่มีอำนาจควบคุมเครือกิจการหรือเครือธุรกิจ และจะต้องสามารถแสดงต่อคณะกรรมการได้เมื่อมีการร้องขอ
  - กลไกในการรายงานและบันทึกการเปลี่ยนแปลงและการรายงานการเปลี่ยนแปลงให้คณะกรรมการรับทราบ
  - กลไกในการร่วมมือกับคณะกรรมการในการตรวจสอบการปฏิบัติตามนโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันและการรายงานผลการตรวจสอบให้คณะกรรมการได้ทราบ
  - กลไกในการรายงานให้หน่วยงานที่มีอำนาจหน้าที่ได้รับทราบถึงข้อกำหนดทางกฎหมายที่อาจส่งผลต่อการคุ้มครองที่นโยบายในการคุ้มครองข้อมูลส่วนบุคคลในเครือกิจการหรือเครือธุรกิจเดียวกันกำหนด และ
  - การจัดการอบรมให้กับบุคลากรซึ่งสามารถเข้าถึงข้อมูลส่วนบุคคลได้ตลอดเวลาหรืออย่างสม่ำเสมอ
- (2.6) มาตรการคุ้มครองที่เหมาะสมซึ่งผู้ส่งหรือโอนข้อมูลส่วนบุคคลจัดทำขึ้นตามมาตรา 29 วรรคสามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 นั้นจะต้องมีเงื่อนไขว่าสิทธิของเจ้าของข้อมูลส่วนบุคคลนั้นสามารถใช้บังคับได้และบุคคลนั้นมีสิทธิที่จะได้รับการเยียวยาในทางกฎหมายโดยจะต้องมีเนื้อหาสอดคล้องกับหลักเกณฑ์และรายละเอียดที่กำหนด
- (2.7) ตราสารที่มีผลบังคับผูกพันทางกฎหมายและสามารถใช้บังคับได้ระหว่างหน่วยงานรัฐ
- (2.8) ข้อกำหนดสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยไปยังผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ซึ่งมีรายละเอียดอย่างน้อยตามเอกสารแนบท้ายประกาศ ก
- (2.9) ข้อกำหนดสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยไปยังผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล ซึ่งประกอบด้วยรายละเอียดอย่างน้อยตามเอกสารแนบท้ายประกาศ ข

## เอกสารแนบท้ายประกาศ ก

### ข้อกำหนดสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยไปยังผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล

ข้อกำหนดสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไทยไปยังผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้นจะต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

(1) หน้าที่ของผู้ส่งหรือโอนข้อมูลส่วนบุคคล

- รับรองว่าการประมวลผลข้อมูลส่วนบุคคลซึ่งหมายรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นไปโดยสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- มีการใช้ความพยายามตามสมควรในการพิจารณาว่าผู้รับโอนข้อมูลส่วนบุคคลนั้นสามารถปฏิบัติตามข้อกำหนดได้
- ให้ข้อมูลเกี่ยวกับกฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลซึ่งใช้บังคับอยู่ในประเทศปลายทางหรือบังคับแก่องค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล
- ตอบคำถามของเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลโดยผู้รับการส่งหรือโอนข้อมูลส่วนบุคคล
- ให้ข้อมูลเกี่ยวกับสิทธิของเจ้าของข้อมูลส่วนบุคคลซึ่งเป็นสิทธิตาม (3) แก่เจ้าของข้อมูลส่วนบุคคล

(2) หน้าที่ของผู้รับโอนข้อมูลส่วนบุคคล

- กำหนดว่าจะมีการจัดมาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ดำเนินการให้บุคคลภายนอกที่สามารถเข้าถึงข้อมูลส่วนบุคคลนั้นจะรักษาความลับของข้อมูลส่วนบุคคล
- รับรองว่าตนได้พิจารณาแล้วเชื่อได้ว่าไม่มีกฎหมายใดที่ขัดขวางไม่ให้อาจปฏิบัติตามหน้าที่เพื่อคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามข้อกำหนดนี้ได้
- ประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่กำหนดเท่านั้น

- แจ้งให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลได้ทราบถึงส่วนงานภายในองค์กรซึ่งมีหน้าที่ในการตอบสนองต่อคำร้องเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลและจะให้ความร่วมมือกับผู้ส่งหรือโอนข้อมูลส่วนบุคคลโดยสุจริต
  - แจ้งให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลได้ทราบถึงศักยภาพทางการเงินของตนในการปฏิบัติตามข้อกำหนดนี้
  - ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบ ในกรณีที่ได้รับการร้องขอจากผู้ส่งหรือโอนข้อมูลส่วนบุคคล
  - ประมวลผลข้อมูลส่วนบุคคลโดยสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (3) ความรับผิดชอบและสิทธิของบุคคลที่สาม
- ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากการฝ่าฝืนข้อกำหนด
  - ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลตกลงว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิ (ในฐานะบุคคลภายนอกสัญญา) ที่จะบังคับการตามสิทธิของตนกับผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลในกรณีที่มีการฝ่าฝืนหน้าที่ตามข้อกำหนดนี้
- (4) กฎหมายที่มีผลใช้บังคับกับข้อกำหนด
- (5) ข้อกำหนดนี้ให้ตกอยู่ในบังคับของกฎหมายไทย
- (6) การระงับข้อพิพาทกับเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐ
- ในกรณีที่มีข้อพิพาทเกิดขึ้นโดยเจ้าของข้อมูลส่วนบุคคลหรือหน่วยงานรัฐเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล ไม่ว่าจะต่อทั้งผู้ส่งหรือโอนข้อมูลส่วนบุคคลหรือผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลหรือบุคคลหนึ่งบุคคลใด ให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลหรือผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลแจ้งให้อีกฝ่ายหนึ่งทราบและจะร่วมกันระงับข้อพิพาทดังกล่าว
  - ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลตกลงที่จะใช้วิธีการระงับข้อพิพาทโดยการไกล่เกลี่ย
- (7) การยกเลิกข้อตกลง
- ในกรณีที่ผู้รับการส่งหรือการโอนข้อมูลส่วนบุคคลฝ่าฝืนหน้าที่กำหนดในข้อกำหนดนี้ ผู้ส่งหรือโอนข้อมูลส่วนบุคคลมีสิทธิที่จะพักการส่งหรือโอนข้อมูลส่วนบุคคลไปยังผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจนกว่าการฝ่าฝืนจะได้รับการแก้ไขหรือข้อกำหนดนี้ถูกยกเลิก

- ผู้ส่งหรือโอนข้อมูลส่วนบุคคลมีสิทธิที่จะเลิกข้อกำหนดนี้หากปรากฏว่า การส่งหรือโอนข้อมูลส่วนบุคคลมาให้กับผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลถูกพักเป็นเวลานานกว่าหนึ่งเดือน หรือการปฏิบัติตามข้อกำหนดนี้จะทำให้ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลฝ่าฝืนหน้าที่ตามกฎหมายของประเทศของตน หรือผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลฝ่าฝืนคำรับรองหรือหน้าที่ที่กำหนด หรือมีคำวินิจฉัยที่เป็นที่สิ้นสุดแล้วว่าการฝ่าฝืนหน้าที่โดยผู้รับการส่งหรือการโอนข้อมูลส่วนบุคคล หรือผู้รับการส่งหรือการโอนข้อมูลส่วนบุคคลถูกคำสั่งให้เลิกกิจการหรือเข้าสู่กระบวนการล้มละลาย

## เอกสารแนบท้ายประกาศ ข

### ข้อกำหนดสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไปยังผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคล

ข้อกำหนดสำหรับการส่งหรือโอนข้อมูลส่วนบุคคลจากผู้ควบคุมข้อมูลส่วนบุคคลในประเทศไปยังผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในประเทศปลายทางหรือที่เป็นองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลนั้นจะต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

(1) ข้อสัญญาที่กำหนดให้เจ้าของข้อมูลส่วนบุคคลสามารถบังคับสิทธิของตนต่อผู้ส่งหรือโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลซึ่งเป็นผู้ประมวลผลข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

(2) หน้าที่ของผู้ส่งหรือโอนข้อมูลส่วนบุคคล

- รับรองว่าการประมวลผลข้อมูลส่วนบุคคลซึ่งหมายรวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลนั้นเป็นไปโดยสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- รับรองว่าได้สั่งให้ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนตามคำสั่งของผู้ส่งหรือโอนในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลตามกฎหมายที่ใช้บังคับแก่กรณีและข้อกำหนดนี้

- รับรองว่าผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะจัดมาตรการการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- รับรองว่าจะมีการจัดมาตรการด้านความปลอดภัยเพื่อป้องกันคุ้มครองมิให้ข้อมูลส่วนบุคคลที่ถูกส่งหรือโอนสูญหายโดยอุบัติเหตุหรือโดยการกระทำโดยมิชอบ หรือการถูกทำลายโดยอุบัติเหตุหรือโดยการกระทำโดยมิชอบ การเปลี่ยนแปลงแก้ไข การถูกเปิดเผย หรือการถูกเข้าถึงโดยมิชอบ โดยเฉพาะอย่างยิ่งในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลผ่านระบบโครงข่าย (Transmission of Data over a Network) และการประมวลผลข้อมูลส่วนบุคคลโดยมิชอบด้วยกฎหมายใด ๆ

- รับรองว่าจะมีการปฏิบัติตามมาตรการการคุ้มครองความปลอดภัยของข้อมูล



- รับรองว่าเจ้าของข้อมูลส่วนบุคคลจะได้รับการแจ้งว่ามีการส่งหรือโอนข้อมูลส่วนบุคคลไปประเทศปลายทางหรือองค์การระหว่างประเทศที่รับข้อมูลส่วนบุคคลในกรณีที่เป็นการส่งหรือโอนข้อมูลส่วนบุคคลตามมาตรา 26 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  - ดำเนินการส่งการแจ้งเตือนที่ได้รับจากผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลไปยังคณะกรรมการ ในกรณีที่ผู้ส่งหรือโอนข้อมูลส่วนบุคคลตัดสินใจว่าจะส่งหรือโอนข้อมูลส่วนบุคคลต่อไป หรือยกเลิกการพักการส่งหรือโอนข้อมูลส่วนบุคคล
  - ส่งบทสรุปรายละเอียดเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลตลอดจนสำเนาสัญญาให้บริการประมวลผลข้อมูลส่วนบุคคลช่วงให้กับเจ้าของข้อมูลส่วนบุคคลที่ร้องขอ
  - ส่งรายละเอียดของการประมวลผลข้อมูลส่วนบุคคลช่วง
- (3) หน้าที่ของผู้รับการส่งหรือโอนข้อมูลส่วนบุคคล
- รับรองว่าจะประมวลผลข้อมูลส่วนบุคคลเฉพาะในฐานะผู้ประมวลผลข้อมูลส่วนบุคคลและตามคำสั่งของผู้ส่งหรือโอนข้อมูลส่วนบุคคลเท่านั้น ในกรณีที่ไม่สามารถปฏิบัติตามหน้าที่ดังกล่าวได้ จะแจ้งให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลทราบโดยไม่ชักช้า ในกรณีนี้ ผู้ส่งหรือโอนข้อมูลส่วนบุคคลสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้
  - รับรองว่าตนได้พิจารณาแล้ว เชื่อได้ว่าไม่มีกฎหมายใดที่ขัดขวางไม่让自己สามารถประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของผู้ส่งหรือโอนข้อมูลส่วนบุคคล และในกรณีที่มีการเปลี่ยนแปลงทางกฎหมายซึ่งจะส่งผลต่อการปฏิบัติหน้าที่ตามข้อกำหนดนี้ ผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลจะแจ้งให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลทราบถึงการเปลี่ยนแปลงดังกล่าวโดยไม่ชักช้า ในกรณีนี้ ผู้ส่งหรือโอนข้อมูลส่วนบุคคลสามารถพักการส่งหรือโอนข้อมูลส่วนบุคคลหรืออาจยกเลิกข้อกำหนดนี้ได้
  - รับรองว่าตนได้จัดทำมาตรการคุ้มครองความมั่นคงปลอดภัยที่เหมาะสมตามมาตรฐานขั้นต่ำที่กำหนดตามมาตรา 37 (1) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้ว
  - แจ้งให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลทราบโดยไม่ชักช้าเกี่ยวกับคำร้องให้เปิดเผยข้อมูลส่วนบุคคลโดยหน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมาย เว้นแต่ กรณีไม่สามารถแจ้งได้เนื่องจากมีกฎหมายห้าม เช่น เป็นข้อห้ามตามกฎหมายอาญาเพื่อรักษาความลับของการดำเนินกระบวนการสืบสวนสอบสวน การเข้าถึงข้อมูลโดยอุบัติเหตุหรือโดยการกระทำที่มิชอบ และคำร้องที่ได้รับจากเจ้าของข้อมูลส่วนบุคคลโดยตรง โดยไม่มีการตอบสนองต่อคำร้องดังกล่าว
  - ตอบข้อซักถามของผู้ส่งหรือโอนข้อมูลส่วนบุคคลถึงการประมวลผลข้อมูลส่วนบุคคลซึ่งถูกส่งหรือโอน

- ส่งอุปกรณ์ในการประมวลผลข้อมูลส่วนบุคคลให้ตรวจสอบ ในกรณีที่ได้รับคำร้องจากผู้ส่งหรือโอนข้อมูลส่วนบุคคล
- ส่งบทสรุปรายละเอียดเกี่ยวกับมาตรการคุ้มครองข้อมูลส่วนบุคคลตลอดจนสำเนาสัญญาให้บริการประมวลผลข้อมูลส่วนบุคคลช่วงโดยลบส่วนที่เป็นข้อมูลเชิงพาณิชย์ออก แต่มีการเติมรายละเอียดเกี่ยวกับมาตรการรักษาความปลอดภัยเข้าไปแทนในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถดำเนินการให้ได้รับรายละเอียดดังกล่าวจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลได้
- ได้มีการแจ้งผู้ส่งหรือโอนข้อมูลส่วนบุคคลให้ทราบถึงการประมวลผลข้อมูลส่วนบุคคลช่วง และได้รับความยินยอมแล้ว
- การประมวลผลข้อมูลส่วนบุคคลช่วงจะเป็นไปตามข้อกำหนดนี้
- ส่งสำเนาสัญญาประมวลผลข้อมูลส่วนบุคคลช่วงให้กับผู้ส่งหรือโอนข้อมูลส่วนบุคคล

#### (4) ความรับผิด

- ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลตกลงกันว่าเจ้าของข้อมูลส่วนบุคคลที่ได้รับความเสียหายจากการไม่ปฏิบัติตามหน้าที่ที่กำหนดในข้อกำหนดนี้ซึ่งไม่ว่าจะเป็นกระทำของผู้ส่งหรือโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลช่วง สามารถเรียกร้องค่าเสียหายได้จากผู้ส่งหรือโอนข้อมูลส่วนบุคคล
- ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถเรียกร้องค่าเสียหายจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลตาม (ก) ได้เนื่องจากผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลไม่ปฏิบัติตามหน้าที่ที่ปรากฏในข้อกำหนดนี้ เนื่องจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลไม่สามารถถูกติดตามตัวได้หรือล้มละลาย เจ้าของข้อมูลส่วนบุคคลสามารถเรียกค่าเสียหายได้จากผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล
- ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลจะไม่ยกเอาการไม่ปฏิบัติหน้าที่ของผู้ประมวลผลข้อมูลส่วนบุคคลช่วงเพื่อยกเว้นหรือจำกัดความรับผิดของตน
- ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถเรียกร้องค่าเสียหายจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลตาม (ก) และผู้รับการส่งหรือโอนข้อมูลส่วนบุคคลตาม (ข) ได้เนื่องจากผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลไม่สามารถถูกติดตามตัวได้หรือล้มละลาย และเป็นความเสียหายที่เกิดจากความผิดของผู้ประมวลผลข้อมูลส่วนบุคคลช่วง เจ้าของข้อมูลส่วนบุคคลสามารถเรียกค่าเสียหายได้จากผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

#### (5) การระงับข้อพิพาท

- ในกรณีที่เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนเพื่อเรียกร้องค่าสินไหมทดแทนหรือค่าเสียหายจากผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลตกลงว่าจะระงับข้อพิพาทดังกล่าวโดยการไกล่เกลี่ยซึ่งมีความเป็นอิสระ หรือโดยองค์การคุ้มครองข้อมูลส่วนบุคคล (ถ้ามี)

- การระงับข้อพิพาท จะไม่ส่งผลกระทบต่อการใช้สิทธิเรียกร้องค่าเสียหายของเจ้าของข้อมูลส่วนบุคคลที่มีสิทธิตามกฎหมายไทยหรือกฎหมายระหว่างประเทศ

(6) การร่วมมือกับคณะกรรมการ

- ผู้ส่งหรือโอนข้อมูลส่วนบุคคลตกลงจะส่งสำเนาของข้อกำหนดให้คณะกรรมการเก็บรักษาเอาไว้ หากได้รับการร้องขอ

- ผู้ส่งหรือโอนข้อมูลส่วนบุคคลและผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลตกลงให้คณะกรรมการมีสิทธิในการตรวจสอบผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

- ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลมีหน้าที่แจ้งให้ผู้ส่งหรือโอนข้อมูลส่วนบุคคลทราบถึงกฎหมายที่จะส่งผลในการขัดขวางมิให้มีการตรวจสอบผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลช่วง

(7) การประมวลผลข้อมูลส่วนบุคคลช่วง

- ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลจะไม่ดำเนินการให้มีการประมวลผลข้อมูลส่วนบุคคลในลักษณะของการประมวลผลข้อมูลส่วนบุคคลช่วงเว้นแต่จะได้รับความยินยอมจากผู้ส่งหรือโอนข้อมูลส่วนบุคคล

- ในกรณีที่ได้รับความยินยอมจากผู้ส่งหรือโอนข้อมูลส่วนบุคคล ผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคลจะทำสัญญาประมวลผลข้อมูลส่วนบุคคลช่วงเป็นลายลักษณ์อักษรซึ่งมีข้อกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลช่วงมีหน้าที่เช่นเดียวกับผู้รับการส่งหรือรับโอนข้อมูลส่วนบุคคล

## 1.5 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง การจัดให้มีบันทึกการกิจกรรมประมวลผล การจัดมาตรการเกี่ยวกับการขอใช้สิทธิในการเข้าถึงของเจ้าของข้อมูลส่วนบุคคล และการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

### สรุปสาระสำคัญของร่างประกาศฯ

#### (2.1) กำหนดนิยามคำว่า

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“เหตุละเมิดข้อมูลส่วนบุคคล” หมายความว่า การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลซึ่งทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง ไม่ว่าจะโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย รวมถึงการเปิดเผย หรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน เก็บรวบรวม หรือประมวลผลข้อมูลส่วนบุคคลใด ๆ โดยไม่ได้รับอนุญาต

#### (2.2) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกการกิจกรรมประมวลผลข้อมูลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยให้มีคำอธิบายประเภทเจ้าของข้อมูลส่วนบุคคลและประเภทของข้อมูลส่วนบุคคลด้วย
- วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลแต่ละประเภท
- ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) รวมถึงช่องทางการติดต่อ
- ระยะเวลาในการเก็บรักษาและการลบข้อมูลส่วนบุคคลประเภทต่าง ๆ
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประเภทของผู้ที่อาจได้รับการเปิดเผยข้อมูลและข้อมูลเกี่ยวกับการโอนข้อมูลส่วนบุคคลออกไปยังประเทศที่สามหรือองค์การระหว่างประเทศ (ถ้ามี)
- คำอธิบายทั่วไปเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล

บันทึกการรายการดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรอาจจัดให้อยู่ในรูปแบบหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงให้เห็นสำนักงานตรวจสอบได้อย่างรวดเร็ว

(2.3) ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กอาจได้รับยกเว้นให้ไม่บันทึกการตามมาตรา 39 (1) (2) (3) (4) (5) (6) และ (8) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือการประมวลผลข้อมูลส่วนบุคคลนั้นมิได้กระทำเป็นครั้งคราว หรือมีการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กิจการขนาดเล็ก หมายความว่าถึง กิจการที่มีลักษณะเป็นวิสาหกิจขนาดย่อมตามหลักเกณฑ์ที่กำหนดไว้ในกฎกระทรวงที่ออกตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2543 และที่แก้ไขเพิ่มเติม และกิจการขนาดเล็กนั้นต้องมีการประมวลผลข้อมูลส่วนบุคคลน้อยกว่า 1,000 ราย

(2.4) การทำบันทึกการปฏิเสธการใช้สิทธิตามมาตรา 39 (7) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลแยกต่างหากจากบันทึกการกิจกรรมประมวลผลข้อมูล โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- คำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- คำอธิบายพร้อมทั้งเหตุผลในการปฏิเสธการขอใช้สิทธินั้น
- กิจกรรมประมวลผลข้อมูลที่เกี่ยวข้องกับการขอใช้สิทธิ

บันทึกการปฏิเสธการใช้สิทธิดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรซึ่งอาจจัดให้อยู่ในรูปแบบหนังสือหรืออิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้บันทึกสามารถเข้าถึงได้ง่าย และสามารถแสดงให้เห็นสำนักงานตรวจสอบได้อย่างรวดเร็ว

(2.5) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อมูลดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลได้

- วัตถุประสงค์ในการประมวลผล
- ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ผู้รับหรือประเภทของผู้รับที่ข้อมูลนั้นจะถูกส่งต่อหรือถูกเปิดเผย โดยเฉพาะอย่างยิ่งผู้รับในประเทศที่สามหรือองค์การระหว่างประเทศ

- ระยะเวลาที่คาดไว้สำหรับการเก็บรักษาข้อมูลส่วนบุคคล
  - การมีอยู่ของสิทธิในการเรียกร้องการแก้ไขหรือลบข้อมูลส่วนบุคคลหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูลส่วนบุคคลหรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลดังกล่าวจากผู้ควบคุมข้อมูลส่วนบุคคล
  - สิทธิในการร้องเรียนต่อหน่วยงานกำกับดูแล
  - ข้อมูลใด ๆ ก็ตามที่มีอยู่และที่มาของข้อมูลนั้น เมื่อข้อมูลส่วนบุคคลไม่ได้ถูกเก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคล
  - การโอนข้อมูลไปยังต่างประเทศ (ถ้ามี)
- (2.6) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องจัดให้มีช่องทางการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล โดยมีช่องทางใดก็ได้ที่สามารถตรวจสอบได้ในภายหลังและต้องจัดให้มีระบบบันทึกการเกี่ยวกับคำร้องขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเพื่อประโยชน์แห่งการพิสูจน์ ทั้งนี้ ข้อกำหนดนี้ไม่กระทบต่อหน้าที่ในการจัดให้มีช่องทางการติดต่อต่าง ๆ ตามที่กฎหมายอื่นที่กำหนดไว้โดยเฉพาะ
- (2.7) ผู้ควบคุมข้อมูลส่วนบุคคลต้องมีมาตรการที่เหมาะสมเพื่อตรวจสอบตัวตนของผู้ยื่นคำร้องขอซึ่งเป็นเจ้าของข้อมูลส่วนบุคคล หรือตัวแทนของเจ้าของข้อมูลส่วนบุคคลในการเข้าถึงข้อมูลส่วนบุคคล โดยเฉพาะอย่างยิ่งการร้องขอใช้สิทธิผ่านทางระบบอิเล็กทรอนิกส์
- (2.8) เมื่อเจ้าของข้อมูลส่วนบุคคลได้ยื่นคำขอใช้สิทธิต่อผู้ควบคุมข้อมูลส่วนบุคคลแล้ว ผู้ควบคุมข้อมูลส่วนบุคคลต้องพิจารณาคำขอแต่ละคำขอว่าเป็นไปตามที่กฎหมายรับรองหรือมีเหตุในการปฏิเสธตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลส่วนบุคคลดังกล่าวด้วยวิธีการดังต่อไปนี้
- ส่งมอบสำเนาข้อมูลส่วนบุคคลและข้อมูลเกี่ยวกับการใช้และเปิดเผยข้อมูลส่วนบุคคลเป็นลายลักษณ์อักษร หรือ
  - กรณีที่ไม่สามารถส่งมอบสำเนาข้อมูลส่วนบุคคลและข้อมูลเกี่ยวกับการใช้และเปิดเผยข้อมูลส่วนบุคคลได้ ต้องจัดให้เจ้าของข้อมูลส่วนบุคคลผู้ยื่นคำขอมิมีโอกาสเข้าตรวจสอบข้อมูลส่วนบุคคลและการใช้หรือเปิดเผยข้อมูลส่วนบุคคลตามคำขอ หรือ
  - อาจจัดให้เข้าถึงข้อมูลในรูปแบบอื่นตามที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอ และการร้องขอนั้นผู้ควบคุมข้อมูลส่วนบุคคลสามารถรับดำเนินการให้ได้
- (2.9) การดำเนินการเพื่อให้เข้าถึงข้อมูลตามคำร้องขอจะต้องดำเนินการโดยไม่มีค่าใช้จ่าย เว้นแต่คำขอของเจ้าของข้อมูลส่วนบุคคลไม่มีมูลหรือไม่สมเหตุผล หรือมีลักษณะเป็นคำร้องขอฟุ่มเฟือย หรือ

ไม่สามารถยืนยันตัวตนของผู้ยื่นคำร้องขอได้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจเลือกใช้วิธีการ  
ข้อใดข้อหนึ่ง ดังต่อไปนี้

- เรียกเก็บค่าใช้จ่ายในการดำเนินการตามสมควร โดยพิจารณาถึงค่าใช้จ่ายในการให้  
ข้อมูลหรือการสื่อสารหรือการปฏิบัติการตามที่ร้องขอร่วมด้วยโดยละเอียด
- ปฏิเสธที่จะปฏิบัติตามคำร้องขอ

ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องรับภาระในการแสดงให้เห็นโดยกระจ่างถึงลักษณะที่แสดงว่าคำขอ  
ดังกล่าวไม่มีมูลหรือไม่สมเหตุสมผล

(2.10) ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการเพื่อให้เจ้าของข้อมูลส่วนบุคคลเข้าถึงข้อมูลหรือได้รับ  
สำเนาตามคำร้องขอโดยไม่ล่าช้า ทั้งนี้ ไม่เกินสามสิบวันนับตั้งแต่ได้รับคำร้องขอที่มีข้อมูลถูกต้อง  
ครบถ้วน นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจขยายระยะเวลาในการพิจารณาหรือดำเนินการ  
ตามคำร้องขอได้อีกหกสิบวันหากมีเหตุจำเป็นโดยพิจารณาตามความซับซ้อนและจำนวนของคำร้อง  
ขอร่วมด้วยโดยละเอียด ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องให้ข้อมูลแก่เจ้าของข้อมูลส่วนบุคคลเกี่ยวกับ  
การขยายระยะเวลาใด ๆ ภายในกรอบเวลาตามวรรคแรกพร้อมทั้งเหตุผลของความล่าช้า ในกรณีที่  
เจ้าของข้อมูลส่วนบุคคลทำคำขอผ่านทางระบบอิเล็กทรอนิกส์การให้ข้อมูลตามคำร้องขอจะต้อง  
กระทำการผ่านระบบอิเล็กทรอนิกส์เช่นกัน เว้นแต่เจ้าของข้อมูลส่วนบุคคลจะร้องขอเป็นอย่างอื่น

(2.11) เมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งรายละเอียดดังต่อไปนี้  
แก่สำนักงานตามเงื่อนไขและระยะเวลาที่กำหนดไว้ใน มาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครอง  
ข้อมูลส่วนบุคคล พ.ศ. 2562

- คำอธิบายลักษณะของเหตุละเมิดข้อมูลส่วนบุคคล หากสามารถระบุได้ ให้ระบุ  
ประเภทของข้อมูลส่วนบุคคลและจำนวนข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วน  
บุคคลที่เกี่ยวข้อง รวมถึงบันทึกรายการกิจกรรมประมวลผลที่เกี่ยวข้อง
- ชื่อและข้อมูลติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลติดต่ออื่น ๆ  
ของผู้ควบคุมข้อมูลส่วนบุคคล
- คำอธิบายถึงผลที่อาจจะเกิดขึ้นจากเหตุละเมิดข้อมูลส่วนบุคคล
- คำอธิบายเกี่ยวกับมาตรการในการรับมือกับเหตุละเมิดข้อมูลส่วนบุคคลเพื่อลด  
ผลกระทบและมาตรการในการเยียวยา

เมื่อได้รับแจ้งเหตุละเมิดข้อมูลจากผู้ควบคุมข้อมูลส่วนบุคคล ให้สำนักงานส่งรายละเอียดที่ได้รับแจ้ง  
แก่คณะกรรมการเพื่อพิจารณาและตรวจสอบเหตุดังกล่าวภายในสามสิบวันนับแต่ได้รับการแจ้งเหตุ

ละเมิด หากไม่สามารถแจ้งรายละเอียดได้ในคราวเดียวกันโดยมีเหตุอันสมควรเพื่อความจำเป็นแก่ การตรวจสอบเหตุละเมิดข้อมูลส่วนบุคคลหรือเพื่อที่จะป้องกันการเปิดเผยข้อมูลเพิ่มเติม ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดเพิ่มเติมในภายหลังพร้อมเหตุผลที่ไม่สามารถแจ้ง รายละเอียดทั้งหมดได้ ทั้งนี้ คณะกรรมการอาจสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียด เพิ่มเติมภายในระยะเวลาที่กำหนดได้ ผู้ควบคุมข้อมูลส่วนบุคคลต้องทำบันทึกเหตุการณ์ละเมิดข้อมูล ส่วนบุคคลประกอบด้วยข้อเท็จจริง ผลของเหตุละเมิดและการเยียวยาที่ได้ดำเนินการแล้ว รวมถึง เหตุผลที่จะไม่แจ้งเจ้าของข้อมูลส่วนบุคคลกรณีได้รับยกเว้นให้ไม่ต้องแจ้งเพื่อให้สำนักงานสามารถ ตรวจสอบและเพื่อประโยชน์แห่งการพิสูจน์เหตุแห่งการละเมิดข้อมูลส่วนบุคคล ทั้งนี้ การแจ้งเหตุ ละเมิดแก่สำนักงานไม่เป็นการยกเว้นหน้าที่อื่นของผู้ควบคุมข้อมูลส่วนบุคคลที่ต้องกระทำตาม กฎหมายเฉพาะที่เกี่ยวข้องกับกิจการนั้น

(2.12) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลประมวลผล ข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่ แจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่ชักช้านับแต่ผู้ประมวลผลข้อมูล ส่วนบุคคลได้ทราบถึงเหตุนั้น โดยผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดอย่างน้อย ดังต่อไปนี้ เพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งรายละเอียดดังกล่าวแก่สำนักงานและเจ้าของข้อมูล ส่วนบุคคลต่อไป

- ข้อมูลส่วนบุคคลที่มีการประมวลผล โดยระบุถึงประเภทของข้อมูลที่ถูกละเมิด
- จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้องและปริมาณของข้อมูลที่ถูกละเมิด
- ระยะเวลาที่เกิดการละเมิดนับแต่ทราบเหตุละเมิด

(2.13) เมื่อคณะกรรมการได้รับแจ้งเหตุละเมิดข้อมูลจากสำนักงาน คณะกรรมการจะแต่งตั้งคณะกรรมการ ผู้เชี่ยวชาญขึ้นคณะหนึ่งหรือหลายคณะก็ได้ตามความเชี่ยวชาญในแต่ละเรื่อง ทำหน้าที่ติดตามและ ตรวจสอบเหตุดังกล่าวเพื่อยืนยันการเกิดเหตุ รวมถึงตรวจสอบการกระทำใด ๆ ของผู้ควบคุมข้อมูล ส่วนบุคคลหรือผู้ที่เกี่ยวข้องกับเหตุละเมิดนั้น คณะกรรมการผู้เชี่ยวชาญอาจพิจารณาแต่งตั้งเจ้าหน้าที่ จำนวนอย่างน้อย 1 รายเพื่อรับผิดชอบในการติดตามเหตุละเมิดดังกล่าว คณะกรรมการผู้เชี่ยวชาญ อาจพิจารณาออกคำสั่งบางประการให้แก่ผู้ควบคุมข้อมูลส่วนบุคคลเพื่อปฏิบัติตามเพื่อแก้ไขเยียวยา เหตุละเมิดดังกล่าวแต่ไม่จำกัดเฉพาะการพิจารณาเห็นชอบแผนตามมาตรการในการรับมือกับเหตุ ละเมิดข้อมูลส่วนบุคคลเพื่อลดผลกระทบและมาตรการในการเยียวยาที่ผู้ควบคุมข้อมูลส่วนบุคคล เสนอมาตอนแจ้งเหตุละเมิด การให้รายงานเหตุการณ์ต่าง ๆ ตามรอบระยะเวลาที่เหมาะสม



การเข้าตรวจสอบผู้ควบคุมข้อมูลส่วนบุคคล การสั่งให้ดำเนินการใด ๆ ภายใต้กรอบของกฎหมายเพื่อการแก้ไขเยียวยาเหตุละเมิดภายในระยะเวลาที่เหมาะสม อนึ่ง ในกรณีที่คณะกรรมการผู้เชี่ยวชาญเห็นสมควร คณะกรรมการผู้เชี่ยวชาญอาจสั่งให้สำนักงานดำเนินงานจัดทำรายงานเหตุละเมิดโดยอาจจัดทำร่วมกันกับผู้ควบคุมข้อมูลส่วนบุคคลได้ ให้คณะกรรมการผู้เชี่ยวชาญและเจ้าหน้าที่ที่ได้รับการแต่งตั้งมอบหมายนั้นมีอำนาจหน้าที่เช่นเดียวกับกรณีการรับข้อร้องเรียนที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยอนุโลมตราบท่าที่ไม่ขัดแย้งกัน ให้คณะกรรมการผู้เชี่ยวชาญจัดทำสำเนาบันทึกผลการตรวจสอบรายละเอียดเกี่ยวกับเหตุละเมิดแล้วรายงานข้อเท็จจริงให้คณะกรรมการทราบ แต่ในกรณีที่เหตุละเมิดนั้นอาจถูกลงโทษตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้เสนอความเห็นของคณะกรรมการผู้เชี่ยวชาญประกอบการพิจารณาลงโทษเพื่อให้คณะกรรมการพิจารณาลงโทษต่อไป

(2.14) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลพบว่าการกระทำอันเป็นการละเมิดต่อความปลอดภัยของข้อมูลส่วนบุคคลซึ่งก่อให้เกิดความเสี่ยงอันเกิดจากอุบัติเหตุ การทำลาย การสูญหาย การเปลี่ยนแปลง การเปิดเผย การโอน การเก็บข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องประเมินระดับความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล โดยคำนึงถึงประเภทข้อมูลส่วนบุคคล จำนวนข้อมูลส่วนบุคคลที่รั่วไหล จำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง และการเข้าถึงได้ยังข้อมูลที่มีการรั่วไหล ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคลอาจทำการประเมินความเสี่ยงล่วงหน้าได้ เพื่อประโยชน์ในการแจ้งเหตุละเมิดภายในระยะเวลาที่กฎหมายกำหนด ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลพบว่าการกระทำอันเป็นการละเมิดต่อความปลอดภัยซึ่งก่อให้เกิดความเสี่ยงสูงที่จะกระทบกับเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องทำการแจ้งต่อเจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า

(2.15) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อเจ้าของข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องแจ้งรายละเอียดอย่างน้อยดังต่อไปนี้ โดยต้องใช้ข้อความที่อ่านและเข้าใจได้ง่ายถึงลักษณะของเหตุละเมิดนั้น

- คำอธิบายลักษณะของเหตุละเมิดข้อมูลส่วนบุคคล หากสามารถระบุได้ ให้ระบุประเภทของข้อมูลส่วนบุคคลและจำนวนข้อมูลส่วนบุคคล รวมถึงบันทึกรายการกิจกรรมประมวลผลที่เกี่ยวข้อง
- ชื่อและข้อมูลติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลติดต่ออื่น ๆ ของผู้ควบคุมข้อมูลส่วนบุคคล

- คำอธิบายถึงผลที่อาจเกิดขึ้นจากเหตุละเมิดข้อมูลส่วนบุคคล
- คำอธิบายเกี่ยวกับมาตรการในการรับมือกับเหตุละเมิดข้อมูลส่วนบุคคลและมาตรการในการเยียวยา

(2.16) ผู้ควบคุมข้อมูลส่วนบุคคลจะได้รับยกเว้นให้ไม่จำเป็นต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคล ภายใต้เงื่อนไขข้อใดข้อหนึ่งดังต่อไปนี้

- เมื่อผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้มาตรการคุ้มครองข้อมูลส่วนบุคคลทั้งเชิงเทคนิคและการจัดการองค์กรตามสมควรแล้ว และมาตรการนั้นได้นำไปใช้กับข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเหตุละเมิด หรือ
- ผู้ควบคุมข้อมูลส่วนบุคคลได้ใช้มาตรการหลังเกิดเหตุละเมิดข้อมูลส่วนบุคคลที่ประกันได้ว่าความเสี่ยงสูงที่กระทบต่อสิทธิและเสรีภาพของบุคคลนั้นไม่อาจบรรลุผลได้อีกต่อไป หรือ
- การแจ้งแก่เจ้าของข้อมูลส่วนบุคคลเป็นการยากเกินสมควร ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการแจ้งต่อสาธารณะหรือวิธีการอื่นในทำนองเดียวกันแทน

## 1.6 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรฐานความมั่นคงปลอดภัยของการประมวลผล ข้อมูลส่วนบุคคล

### สรุปสาระสำคัญของร่างประกาศฯ

#### (2.1) กำหนดนิยามคำว่า

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล” หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ

“คณะกรรมการผู้เชี่ยวชาญ” หมายความว่า คณะกรรมการผู้เชี่ยวชาญตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

“หน่วยงานของรัฐ” หมายความว่า หน่วยงานของรัฐตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

#### (2.2) ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

#### (2.3) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ตามที่เหมาะสม ซึ่งอาจรวมถึง

- การแฝงข้อมูล (pseudonymization) หรือการเข้ารหัส (encryption) ข้อมูลส่วนบุคคล
- การทำให้แน่ใจว่าสามารถรักษาความมั่นคงปลอดภัยของระบบหรือบริการประมวลผลข้อมูลส่วนบุคคล ซึ่งประกอบไปด้วย การธำรงไว้ซึ่งความลับ

(confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability)

- ความสามารถในการกู้คืนระบบหรือบริการที่มีการประมวลผลข้อมูลส่วนบุคคลให้กลับมาพร้อมให้บริการได้ทันการณ์หากมีเหตุละเมิดข้อมูลส่วนบุคคลขึ้น
- กระบวนการทดสอบและประเมินความมีประสิทธิภาพและประสิทธิผลของมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures)

ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องแจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่ บุคลากร พนักงาน ลูกจ้างหรือบุคคลที่เกี่ยวข้องทราบและแจ้งเตือนเมื่อมีการแก้ไขปรับปรุงมาตรการดังกล่าว รวมถึง สร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

(2.4) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด ต้องจัดให้มีมาตรการควบคุมการเข้าถึงหรือการประมวลผลข้อมูลส่วนบุคคล (Access Control) ที่เหมาะสม เพื่อป้องกันการเข้าถึงหรือการประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต และป้องกันเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยอย่างน้อยต้องประกอบด้วย

- มาตรการควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ซึ่งรวมถึงการกำหนดสิทธิผู้ใช้งาน (user access management) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)
- การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

การดำเนินการตาม (2.4) ให้ถือว่าเป็นการปฏิบัติตาม (2.3) แล้ว

(2.5) คณะกรรมการและสำนักงานจะติดตามตรวจสอบผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อให้แน่ใจว่าได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมโดยคำนึงถึง

- สภาพและลักษณะของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- ความเสี่ยงของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- ขนาดและความซับซ้อนของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล
- ภาระและต้นทุนในการดำเนินการ

กรณีพบว่าผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลกลุ่มใดกลุ่มหนึ่ง หรือรายใดรายหนึ่ง ยังไม่มีมาตรการที่เหมาะสม คณะกรรมการอาจสั่งให้แก้ไขหรือกำหนด มาตรฐานขั้นต่ำในรายละเอียดของแต่ละเรื่องแนบท้ายประกาศนี้ คณะกรรมการอาจสั่งให้ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลกลุ่มใดกลุ่มหนึ่ง หรือ รายใดรายหนึ่ง ต้องส่งรายงานประเมินเพื่อทบทวนการรักษาความมั่นคงปลอดภัยของ การประมวลผลข้อมูลส่วนบุคคล ตามรายละเอียดและวิธีการที่คณะกรรมการกำหนด รวมถึงการกำหนดระยะเวลาผ่อนปรนเพื่อให้มีการเตรียมความพร้อมได้ ทั้งนี้เป็นระยะเวลา ไม่เกิน 2 ปีและคณะกรรมการอาจทบทวนออกเป็นคำสั่งใหม่ได้ตามที่เหมาะสม

(2.6) ให้สันนิษฐานว่าการดำเนินการตามข้อปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ข้อมูลส่วนบุคคลที่ได้รับการรับรองจากคณะกรรมการ ณ ขณะนั้นๆ แสดงว่าผู้ควบคุมข้อมูล ส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณีได้จัดให้มีมาตรการรักษาความมั่นคง ปลอดภัยของการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสมแล้วตามประกาศนี้ คณะกรรมการผู้เชี่ยวชาญ แล้วแต่กรณี อาจพิจารณาว่าการดำเนินการตามข้อปฏิบัติไม่เหมาะสมกับสถานการณ์ ณ ขณะที่มี เหตุการณ์ละเมิดข้อมูลส่วนบุคคล หากปรากฏข้อเท็จจริงเป็นอย่างอื่น ทั้งนี้ ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล มีหน้าที่ต้องแสดงและพิสูจน์ให้เห็นได้อย่างชัดเจนว่าตนเองได้ ดำเนินการตามข้อปฏิบัติที่เกี่ยวข้องกับกิจกรรมประมวลผลข้อมูลส่วนบุคคลของตนแล้ว และ ข้อปฏิบัติที่อ้างอิงมีความเหมาะสม

(2.7) ให้สำนักงานติดตามตรวจสอบและดำเนินการให้มีการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลของ หน่วยงานของรัฐและจัดทำเป็นรายงานประเมินพร้อมข้อเสนอแนะการปรับปรุงมาตรการเป็นประจำ ทุก 2 ปี โดยอย่างน้อยประกอบด้วย

- รายงานกิจกรรมการประมวลผลข้อมูลส่วนบุคคลจำแนกตามระดับความเสี่ยง
- ข้อเสนอแนะมาตรการเพื่อการปรับปรุงและลดความเสี่ยงที่อาจเกิดขึ้น

ในการดำเนินการ ให้สำนักงานอำนวยความสะดวกหน่วยงานของรัฐทั้งหลายด้วยการจัดทำและ ดำเนินงานด้วยสำนักงานเอง ในกรณีนี้ที่หน่วยงานของรัฐใดประสงค์จะจัดทำรายงานประเมิน

ด้วยตนเอง ให้สำนักงานอำนวยความสะดวกและให้คำแนะนำที่เหมาะสม และรวบรวมเป็นส่วนหนึ่งของรายงานประเมินภาพรวมของสำนักงาน ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด

- (2.8) คณะกรรมการอาจกำหนดมาตรฐานขั้นต่ำสำหรับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเฉพาะประเภทใดประเภทหนึ่ง เพื่อให้หน่วยงานของรัฐที่เกี่ยวข้องใช้เป็นมาตรฐานในการปฏิบัติได้ ทั้งนี้ โดยการรับฟังความเห็นจากหน่วยงานของรัฐที่เกี่ยวข้องและประชาชนทั่วไป และกำหนดเป็นมาตรฐานขั้นต่ำแนบท้ายประกาศนี้

เอกสารผลการรับฟังความเห็นเกี่ยวกับร่างกฎหมายลำดับรองกลุ่มที่ 1

## 1.7 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

### เรื่อง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

#### สรุปสาระสำคัญของร่างประกาศฯ

##### (2.1) กำหนดนิยามคำว่า

“การประมวลผลข้อมูลส่วนบุคคล” หมายความว่า การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“กิจกรรมหลัก” หมายความว่า การดำเนินการใด ๆ อันจำเป็นเพื่อบรรลุเป้าหมายของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและไม่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลอันเป็นกิจกรรมเสริม

“กิจกรรมเสริม” หมายความว่า การดำเนินการใด ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลสำหรับงานสนับสนุน ซึ่งอาจรวมถึงงานด้านทรัพยากรบุคคลหรือด้านเทคโนโลยีสารสนเทศ

“ส่วนราชการ” หมายความว่า กระทรวง ทบวง กรม หรือส่วนราชการที่เรียกชื่ออย่างอื่น และมีฐานะเป็นกรม และให้หมายความรวมถึงจังหวัดและกลุ่มจังหวัดตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดินด้วย

“รัฐวิสาหกิจ” หมายความว่า

(1) องค์กรของรัฐบาลตามกฎหมายว่าด้วยการจัดตั้งองค์กรของรัฐบาล หรือกิจการของรัฐตามกฎหมายที่จัดตั้งกิจการนั้น หรือหน่วยงานธุรกิจที่รัฐบาลเป็นเจ้าของ

(2) บริษัทหรือห้างหุ้นส่วนนิติบุคคลที่ส่วนราชการ หรือองค์กรปกครองส่วนท้องถิ่น หรือหน่วยงานอื่นของรัฐ มีทุนรวมอยู่ด้วยเกินกว่าร้อยละห้าสิบ

(3) บริษัทหรือห้างหุ้นส่วนนิติบุคคลที่ส่วนราชการ หรือองค์กรปกครองส่วนท้องถิ่น หรือหน่วยงานอื่นของรัฐ หรือรัฐวิสาหกิจตาม (1) หรือ (2) มีทุนรวมอยู่ด้วยเกินกว่าร้อยละห้าสิบ

“องค์กรปกครองส่วนท้องถิ่น” หมายความว่า องค์กรบริหารส่วนจังหวัด เทศบาล องค์กรบริหารส่วนตำบล กรุงเทพมหานคร เมืองพัทยา หรือองค์กรปกครองส่วนท้องถิ่นอื่นที่มีกฎหมายจัดตั้ง

“หน่วยงานอื่นของรัฐ” หมายความว่า หน่วยงานในกำกับของรัฐ องค์กรมหาชน หน่วยงานที่จัดตั้งขึ้นตามกฎหมายเฉพาะ หรือหน่วยงานอื่นที่มีฐานะเป็นนิติบุคคลที่มีใช้ส่วนราชการและรัฐวิสาหกิจ ทั้งนี้ เฉพาะที่อยู่ในกำกับของฝ่ายบริหาร

“หน่วยงานรัฐในสังกัด” หมายความว่า หน่วยงานรัฐซึ่งอยู่ภายใต้อำนาจบังคับบัญชาหรือกำกับดูแลของหน่วยงานรัฐอื่น

“ผู้ให้บริการโทรคมนาคม” หมายความว่า ผู้ให้บริการที่ได้รับอนุญาตให้ประกอบกิจการโทรคมนาคมตามกฎหมายการประกอบกิจการกิจการโทรคมนาคม

“บริษัทประกันภัย” หมายความว่า บริษัทมหาชนจำกัดที่ได้รับใบอนุญาตประกอบธุรกิจประกันชีวิตหรือประกันวินาศภัยตามกฎหมายการประกอบธุรกิจประกันชีวิตหรือประกันวินาศภัยด้วย

“ธนาคารพาณิชย์” หมายความว่า บริษัทมหาชนจำกัดที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ และให้หมายความรวมถึงธนาคารพาณิชย์เพื่อรายย่อย ธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศที่ได้รับอนุญาตให้ประกอบธุรกิจธนาคารพาณิชย์ตามกฎหมายการประกอบธุรกิจสถาบันการเงิน

(2.2) ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่เป็นหน่วยงานของรัฐและมีฐานะเป็นนิติบุคคลดังต่อไปนี้ ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (1)

- ส่วนราชการ
- รัฐวิสาหกิจ
- องค์การปกครองส่วนท้องถิ่น
- หน่วยงานอื่นของรัฐ

(2.3) กรณีหน่วยงานรัฐใดเป็นหน่วยงานขนาดใหญ่เห็นว่าในการปฏิบัติงานของหน่วยงานรัฐในสังกัดของตน หน่วยงานใดมิได้มีการประมวลผลข้อมูลส่วนบุคคลอย่างสม่ำเสมอหรือเป็นระบบและหน่วยงานรัฐทั้งสองมีความประสงค์ที่จะแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน ให้หน่วยงานรัฐขนาดใหญ่ดังกล่าวขอความเห็นคณะกรรมการเป็นหนังสือผ่านสำนักงานเพื่อประกอบการพิจารณาของหน่วยงานในการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้กับหน่วยงานในสังกัดก่อนการแต่งตั้ง หนังสือขอความเห็นของหน่วยงานรัฐขนาดใหญ่จะต้องอธิบายลักษณะการปฏิบัติงานของหน่วยงานรัฐในสังกัดประกอบการขอความเห็น โดยคณะกรรมการอาจติดต่อหน่วยงานรัฐขนาดใหญ่หรือหน่วยงานรัฐในสังกัดเพื่อให้ข้อมูลเพิ่มเติมประกอบการพิจารณาได้ ทั้งนี้ หนังสือขอความเห็น ฉบับหนึ่งอาจขอความเห็นการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้กับหน่วยงานรัฐในสังกัดได้หลายหน่วยงานพร้อมกัน เมื่อคณะกรรมการพิจารณาแล้วปรากฏข้อเท็จจริงเพียงพอ ให้คณะกรรมการออกความเห็นเป็นหนังสือตอบกลับหน่วยงานรัฐผู้ขอความเห็นโดยเร็ว ทั้งนี้ การพิจารณาของคณะกรรมการจะคำนึงถึงจำนวน



เจ้าของข้อมูลส่วนบุคคล จำนวนข้อมูลส่วนบุคคล ลักษณะและความถี่ของการประมวลผลข้อมูลส่วนบุคคล เพื่อพิจารณาความเสี่ยงที่อาจเกิดผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลและความจำเป็นของการมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงานรัฐในสังกัดเป็นสำคัญ

- (2.4) จังหวัดและหน่วยงานของรัฐตาม (2.2) องค์กรปกครองส่วนท้องถิ่น อาจพิจารณาแต่งตั้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของจังหวัดเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐซึ่งอยู่ภายในพื้นที่จังหวัดเดียวกันได้ ทั้งนี้ ให้นำบทบัญญัติตาม (2.3) มาบังคับใช้แก่การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันระหว่างจังหวัดและหน่วยงานรัฐซึ่งอยู่ภายในพื้นที่จังหวัดเดียวกันโดยอนุโลม
- (2.5) ให้ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งการดำเนินกิจกรรมของตนในการประมวลผลข้อมูลส่วนบุคคล จำเป็นต้องตรวจสอบข้อมูลส่วนบุคคลเป็นระบบอย่างสม่ำเสมอ โดยเหตุที่มีข้อมูลส่วนบุคคลเป็นจำนวนมากลักษณะหนึ่งลักษณะใดดังต่อไปนี้ ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนตามมาตรา 41 (2)
- มีลักษณะเป็นการประมวลผลข้อมูลส่วนบุคคลการใช้งานของผู้ถือบัตรสมาชิกบัตรโดยสารสาธารณะ หรือบัตรอื่นใดในลักษณะเดียวกันซึ่งผู้ให้บริการบัตรหรือบุคคลอื่นใดตรวจสอบรายละเอียดข้อมูลการใช้งานบัตรได้
  - มีลักษณะเป็นการประมวลผลข้อมูลส่วนบุคคลของลูกค้าตามกิจกรรมปกติโดยบริษัทประกันภัย ธนาคารพาณิชย์หรือธุรกิจอื่นที่มีการตรวจสอบสถานะ ประวัติหรือคุณสมบัติของลูกค้าก่อนทำสัญญาหรือให้บริการในลักษณะเดียวกันเพื่อประเมินความเสี่ยงด้านต่าง ๆ ที่เกี่ยวข้อง เช่น การให้คะแนนเครดิต (credit scoring) การกำหนดเบี้ยประกัน การป้องกันการโกงหรือฉ้อฉล (fraud prevention) การป้องกันการฟอกเงิน
  - มีลักษณะเป็นการประมวลผลข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์ด้านการโฆษณาตามพฤติกรรม (behavioral advertising) โดยโปรแกรมค้นหา (search engine) หรือสื่อสังคม (social media)
  - มีลักษณะเป็นการประมวลผลข้อมูลส่วนบุคคลของลูกค้าโดยผู้ให้บริการโทรคมนาคม

- มีลักษณะเป็นการให้บริการเฝ้าระวังพฤติกรรมเพื่อวัตถุประสงค์ด้านรักษาความปลอดภัยตามสถานที่ต่าง ๆ เช่น ห้างสรรพสินค้าและสถานที่สาธารณะ จำนวนตั้งแต่สองสถานที่ขึ้นไป
  - มีลักษณะเป็นกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลและมีลักษณะตามข้อใดข้อหนึ่งดังต่อไปนี้
    - มีข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลอยู่ภายใต้ความดูแลภายในรอบระยะเวลาสิบสองเดือนมากกว่า 50,000 ราย หรือมากกว่า 5,000 รายในกรณีที่ข้อมูลส่วนบุคคลดังกล่าวเป็นข้อมูลส่วนบุคคลตามมาตรา 26
    - มีลักษณะอื่นตามที่คณะกรรมการประกาศกำหนดท้ายประกาศนี้
- (2.6) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 (3) ต่อเมื่อมีกิจกรรมหลักลักษณะใดลักษณะหนึ่งตาม (2.5) มีลักษณะเป็นกิจกรรมหลักของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- (2.7) ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลมีหน้าที่แต่งตั้งตัวแทนตามมาตรา 37 (5) และมีลักษณะตามมาตรา 41 วรรคหนึ่ง ให้ตัวแทนซึ่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแต่งตั้งตามมาตรา 37 (5) แจ้งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าวถึงหน้าที่การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล รวมถึงหน้าที่การแจ้งการแต่งตั้งต่อสำนักงานด้วย
- (2.8) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ไม่มีหน้าที่ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่กำหนดในมาตรา 41 อาจจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนได้ตามความสมัครใจ และอาจแจ้งการแต่งตั้งเจ้าหน้าที่ดังกล่าวต่อสำนักงานตามขั้นตอนและวิธีการที่กำหนดตามประกาศนี้ได้
- (2.9) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องเป็นบุคคลธรรมดาที่มีความรู้หรือความเชี่ยวชาญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการอาจประกาศรับรองหลักสูตรซึ่งจัดโดยสำนักงานหรือหน่วยงานที่ได้รับการรับรองอื่นอันเป็นหลักสูตรอบรมทักษะและความเชี่ยวชาญซึ่งจำเป็นต่อการปฏิบัติหน้าที่ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลได้ และกำหนดให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องได้รับการอบรมหรือผ่านการทดสอบจากหลักสูตรดังกล่าวก็ได้

เมื่อคณะกรรมการประกาศรับรองหลักสูตรแล้ว ผู้ที่จะได้รับการแต่งตั้งเป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลจะต้องได้รับการอบรมหรือจะต้องผ่านการทดสอบจากหลักสูตรดังกล่าว ทั้งนี้ ต้องได้รับการอบรมหรือผ่านการทดสอบไม่เกิน 1 ปี ขณะแต่งตั้ง ระหว่างการดำรงตำแหน่งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องได้รับการอบรมหรือผ่านการทดสอบจากหลักสูตรซึ่งคณะกรรมการรับรองเพื่อพัฒนาทักษะและความรู้อย่างสม่ำเสมออย่างน้อยทุก 3 ปี หลักเกณฑ์และวิธีการรับรองหลักสูตร รวมถึงข้อกำหนดอื่นใดเกี่ยวกับสถาบันผู้ดำเนินหลักสูตรตามข้อนี้ ให้เป็นไปตามประกาศคณะกรรมการที่เกี่ยวข้อง ให้ถือว่าเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลซึ่งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลได้แต่งตั้งขึ้นขณะที่ยังไม่มีประกาศมีคุณสมบัติครบถ้วนตามที่กำหนดแล้ว และให้ถือว่าได้รับการอบรมหรือผ่านการทดสอบเพื่อพัฒนาทักษะและความรู้อย่างสม่ำเสมอแล้ว

- (2.10) เมื่อผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของตนแล้ว ให้แจ้งข้อมูลเกี่ยวกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อให้สำนักงานทราบผ่านช่องทางที่สำนักงานกำหนดภายในระยะเวลา 10 วัน นับแต่การแต่งตั้ง โดยแนบเอกสารและหลักฐานให้ครบถ้วนตามที่ระบุไว้ในเอกสารแนบท้ายประกาศนี้ กรณีผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกัน ให้หน่วยงานที่มีอำนาจบังคับบัญชา หน่วยงานที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสังกัด หรือหนึ่งในบริษัทในเครือกิจการหรือเครือธุรกิจเดียวกันเป็นผู้แจ้งการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแก่สำนักงาน เมื่อได้รับแจ้งการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลแล้ว ให้สำนักงานตรวจสอบเอกสารและหลักฐานตามที่ระบุ หากเอกสารและหลักฐานครบถ้วนถูกต้องตามกรณีให้สำนักงานรับแจ้ง แต่หากเอกสารหรือหลักฐานไม่ครบถ้วนถูกต้องให้สำนักงานแจ้งผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแก้ไขเพิ่มเติมภายในเวลาอันสมควร การถอนหรือเปลี่ยนแปลงเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือ ผู้ประมวลผลข้อมูลส่วนบุคคลแจ้งแก่สำนักงานและเจ้าของข้อมูลส่วนบุคคลทราบไม่เกิน 10 วันนับแต่มีการเพิกถอนหรือเปลี่ยนแปลงตามแบบเอกสารแนบท้ายประกาศนี้พร้อมแนบหลักฐานที่เกี่ยวข้อง
- (2.11) ในการปฏิบัติหน้าที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลต้องคำนึงถึงความเสี่ยงที่เกี่ยวข้องในการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลโดยพิจารณาจากลักษณะ ขอบเขตและวัตถุประสงค์ของการประมวลผลข้อมูล

ส่วนบุคคลด้วย ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินงานโดยคำนึงถึงความเห็นและคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามสมควร ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่เห็นด้วยหรือไม่ปฏิบัติตามคำแนะนำของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลบันทึกข้อเท็จจริงและระบุเหตุผลของการตัดสินใจไว้ รวมถึงระบุผู้มีส่วนร่วมในการตัดสินใจหรืออนุมัติการดำเนินการดังกล่าวและทำบันทึกรายงานเพื่อแจ้งแก่ผู้บริหารสูงสุดของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล หากมีเหตุอันควรเชื่อว่าผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจมีการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติหรือประกาศที่ออกตามพระราชบัญญัติที่ส่งผลกระทบร้ายแรงต่อเจ้าของข้อมูลส่วนบุคคล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลอาจแจ้งต่อสำนักงานเพื่อให้ดำเนินการตรวจสอบได้

- (2.12) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลต้องจัดให้มีช่องทางการติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยตรงที่เหมาะสมเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานติดต่อด้วยภาษาไทยได้โดยง่าย ในการขอคำแนะนำในการปฏิบัติตามพระราชบัญญัตินี้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการประสานงานระหว่างผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลกับสำนักงาน
- (2.13) เมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล หรือการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัตินี้แล้ว ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการโดยไม่ชักช้า ในกรณีที่ต้องประสานไปยังผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล สำนักงาน หรือบุคคลอื่นใดแล้วแต่กรณี ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการดังกล่าวและแจ้งให้กับเจ้าของข้อมูลส่วนบุคคลทราบ โดยให้บันทึกการดำเนินการรวมถึงข้อเท็จจริงที่เกี่ยวข้องไว้ด้วย กรณีที่เจ้าของข้อมูลส่วนบุคคลติดต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพบว่าเรื่องที่เจ้าของข้อมูลส่วนบุคคลติดต่อดังกล่าวอยู่ระหว่างดำเนินการหรือได้ดำเนินการเสร็จสิ้นแล้วและมีความประสงค์จะไม่รับเรื่อง ให้แจ้งเหตุผลหรือสถานะของเรื่องต่อเจ้าของข้อมูลส่วนบุคคลด้วย
- (2.14) กรณีที่สำนักงานได้รับเรื่องร้องเรียน หรือมีเหตุอันควรเชื่อได้ว่าการฝ่าฝืนพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และได้ติดต่อเพื่อร้องขอข้อมูลและเอกสารหลักฐานจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจัดเตรียมข้อมูลและเอกสารหลักฐานเพื่อส่งให้กับสำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่สำนักงานร้องขอ ทั้งนี้ เจ้าหน้าที่

คุ้มครองข้อมูลส่วนบุคคลอาจร้องขอให้สำนักงานอนุญาตขยายระยะเวลาการจัดเตรียมและส่งข้อมูลได้ โดยสำนักงานจะอนุญาตให้ขยายได้เฉพาะเมื่อพิจารณาแล้วพบว่ามีความจำเป็นอันสมควรเท่านั้น ในการตรวจสอบข้อเท็จจริงโดยสำนักงานกรณีมีการกระทบสิทธิหรือเสรีภาพของเจ้าของข้อมูลส่วนบุคคลหรือมีการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติอันอาจเกิดจากกรณีตาม (2.11) ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจัดส่งบันทึกรายงานดังกล่าวให้กับสำนักงานเพื่อเป็นส่วนหนึ่งของข้อมูลและเอกสารหลักฐานประกอบการตรวจสอบข้อเท็จจริงที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องนำเสนอด้วย

## 1.8 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง กระบวนการรับเรื่องร้องเรียน และการบังคับทางปกครอง

### สรุปสาระสำคัญของร่างประกาศฯ

- (2.1) ภายใต้บังคับของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลต้องดำเนินการตามหน้าที่ที่พึงปฏิบัติตามกฎหมาย รวมถึงการแก้ไขเรื่องร้องเรียนของเจ้าของข้อมูลส่วนบุคคลตามประกาศนี้ เจ้าของข้อมูลส่วนบุคคลอาจดำเนินการร้องเรียนกรณีและผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล รวมทั้งลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ผ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย โดยการแจ้งมายังสำนักงานเป็นหนังสือหรือตามช่องทางพร้อมรายละเอียดที่สำนักงานกำหนดแนบท้ายประกาศนี้ การยื่นเรื่องร้องเรียนตามประกาศนี้ เจ้าของข้อมูลส่วนบุคคลคนหนึ่งหรือหลายคนรวมกัน อาจแต่งตั้งให้ผู้แทนดำเนินการแทนก็ได้ ทั้งนี้ตามกระบวนการพิสูจน์และยืนยันตัวตนตามที่สำนักงานประกาศกำหนด เจ้าของข้อมูลส่วนบุคคลอาจยื่นเรื่องร้องเรียนกรณีและผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเป็นหน่วยงานภาครัฐที่มีอำนาจตามกฎหมายก็ได้ตามประกาศนี้ โดยสำนักงานจะดำเนินการตรวจสอบว่าหน่วยงานดังกล่าวได้ดำเนินการตามกฎหมายหรือไม่เท่านั้น
- (2.2) เจ้าของข้อมูลส่วนบุคคลอาจยื่นเรื่องร้องเรียนมายังสำนักงานได้ เมื่อเจ้าของข้อมูลส่วนบุคคลได้ใช้สิทธิและร้องเรียนไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณีแต่ไม่ได้รับการแก้ไขเรื่องร้องเรียนดังกล่าวภายใน 30 วัน โดยแนบหลักฐานประกอบเรื่องร้องเรียนของตน การดำเนินการแก้ไขเรื่องร้องเรียนตามประกาศนี้ สำนักงานอาจดำเนินการตามลำดับความร้ายแรงของกรณี กรณีที่เจ้าของข้อมูลส่วนบุคคลได้ให้รายละเอียดเพียงพอแก่การดำเนินการ จะได้รับการดำเนินการก่อน
- (2.3) ในขณะที่รับเรื่องร้องเรียน ให้สำนักงานชี้แจงนโยบายคุ้มครองข้อมูลส่วนบุคคล ข้อมูลที่จำเป็นต่อการดำเนินการ กระบวนการรับเรื่องร้องเรียน และอธิบายข้อกำหนดให้เจ้าของข้อมูลส่วนบุคคลทราบ เพื่ออำนวยความสะดวกและความคาดหวังในการดำเนินการ รวมถึงกรณีที่มีหน่วยงานกำกับดูแลเฉพาะในเรื่องนั้นอยู่แล้วตามกฎหมายอื่น เมื่อได้รับเรื่องร้องเรียนแล้วและสำนักงานพิจารณาว่ามีข้อมูลเพียงพอให้สำนักงานแจ้งเรื่องไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณี ให้ทำคำชี้แจงเบื้องต้น พร้อมข้อเสนอแนวทางการแก้ไขเรื่องร้องเรียน

ภายใน 15 วัน ทั้งนี้ข้อมูลที่ระบุว่าชั้นความลับให้เป็นไปตามหลักเกณฑ์เกี่ยวกับธรรมาภิบาลข้อมูลของสำนักงาน เมื่อได้รับคำชี้แจงเบื้องต้น พร้อมข้อเสนอแนวทางการแก้ไข ให้สำนักงานประสานงานระหว่างเจ้าของข้อมูลส่วนบุคคล กับผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณี เพื่อพิจารณายุติเรื่องระหว่างกันเอง หากพ้นระยะเวลา 30 วันนับแต่ที่สำนักงานแจ้งเรื่องร้องเรียนไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแล้วแต่กรณี แต่ยังไม่สามารถยุติเรื่องระหว่างกันเองได้ ให้สำนักงานพิจารณาเสนอเรื่องต่อคณะกรรมการผู้เชี่ยวชาญที่ได้รับมอบหมายต่อไป

- (2.4) การดำเนินการรับเรื่องร้องเรียนตามหมวดนี้ สำนักงานอาจมอบหมายให้หน่วยงานภายนอกดำเนินการแทนได้ตามหลักเกณฑ์และวิธีการที่สำนักงานกำหนด ทั้งนี้ตามกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ
- (2.5) ให้สำนักงานรวบรวมข้อมูลทั้งหลายที่เกี่ยวข้องพร้อมประเมินความร้ายแรงของเรื่องร้องเรียน และจัดทำเป็นรายงานสรุปเรื่องร้องเรียนเพื่อเสนอต่อคณะกรรมการผู้เชี่ยวชาญที่ได้รับมอบหมายแล้วแต่กรณี ในการรวบรวมข้อมูลสำนักงานอาจรวบรวมมาจากบุคคลหรือหน่วยงานใด ๆ ที่ประสงค์จะให้ข้อมูลหรือเอกสารหลักฐานประกอบการจัดทำรายงานสรุปเรื่องร้องเรียน หรือข้อมูลที่สำนักงานรวบรวมหรือจัดทำเองก็ได้ ทั้งนี้รวมถึงการทำความเข้าใจเสนอคณะกรรมการผู้เชี่ยวชาญว่ามีหน่วยงานกำกับดูแลตามกฎหมายอื่น และสมควรที่จะส่งเรื่องดังกล่าวไปยังหน่วยงานนั้นเพื่อพิจารณาในส่วนที่เกี่ยวข้องหรือไม่ ในการทำรายงานสรุปเรื่องร้องเรียนเพื่อเสนอต่อคณะกรรมการผู้เชี่ยวชาญ หากไม่มีข้อเท็จจริงเป็นอย่างอื่น ให้สำนักงานสันนิษฐานว่าผู้ที่แจ้งหรือให้ข้อมูลเป็นผู้ไม่มีส่วนเกี่ยวข้องกับการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายในเรื่องนั้น
- (2.6) ในกรณีที่คณะกรรมการผู้เชี่ยวชาญเห็นว่าเรื่องที่สำนักงานเสนอตามรายงานสรุปเรื่องร้องเรียนมีข้อมูลเพียงพอและมีความเหมาะสมที่จะดำเนินการ ให้คณะกรรมการผู้เชี่ยวชาญมีมติรับเรื่องไว้พิจารณาและให้สำนักงานเริ่มกระบวนการตรวจสอบ ทั้งนี้โดยคำนึงถึงความเร่งด่วนและความร้ายแรงของกรณีเป็นสำคัญ กรณีที่คณะกรรมการผู้เชี่ยวชาญเห็นว่าข้อมูลไม่เพียงพอ และไม่มีความชัดเจนที่จะดำเนินการได้ และได้พ้นระยะเวลา 30 วันที่ได้ขอข้อมูลเพิ่มเติมแล้ว ให้มีมติไม่รับเรื่องไว้พิจารณาและสั่งยุติเรื่อง ทั้งนี้ไม่เป็นการตัดสิทธิที่เจ้าของข้อมูลส่วนบุคคลจะยื่นเรื่องร้องเรียนใหม่ กรณีที่คณะกรรมการผู้เชี่ยวชาญเห็นว่าหน่วยงานกำกับดูแลตามกฎหมายอื่น และมีความพร้อมที่จะรับเรื่องเพื่อดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล ให้มีมติส่งเรื่องไปยังหน่วยงานนั้น

ให้สำนักงานแจ้งผลการพิจารณาตามวรรคก่อนให้ผู้ร้องเรียนและผู้ถูกร้องเรียนทราบพร้อมเหตุผลประกอบ

- (2.7) เมื่อคณะกรรมการผู้เชี่ยวชาญมีมติรับเรื่องไว้พิจารณา ให้สำนักงานแจ้งไปยังผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องให้ทำรายงานชี้แจงเรื่องร้องเรียนพร้อมข้อเสนอแนวทางการแก้ไขเรื่องร้องเรียนภายใน 30 วัน คณะกรรมการผู้เชี่ยวชาญอาจสั่งให้บุคคลใด ๆ ส่งเอกสารหรือข้อมูลที่เกี่ยวข้อง หรือสั่งให้มาชี้แจงข้อเท็จจริงด้วยก็ได้ ทั้งนี้ข้อมูลที่ระบุว่าคุณค่าลับให้เป็นไปตามหลักเกณฑ์เกี่ยวกับธรรมาภิบาลข้อมูลของสำนักงาน กรณีที่คณะกรรมการผู้เชี่ยวชาญพิจารณารายงานสรุปเรื่องร้องเรียนประกอบกับรายงานชี้แจงเรื่องร้องเรียนแล้วรับฟังได้ว่าเรื่องร้องเรียนนั้นไม่มีมูล ให้มีคำสั่งยุติเรื่อง
- (2.8) ในกรณีที่มีรายงานชี้แจงเรื่องร้องเรียน พร้อมข้อเสนอแนวทางการแก้ไข ที่คณะกรรมการผู้เชี่ยวชาญเห็นว่าอาจไกล่เกลี่ยได้ และคู่กรณีประสงค์จะให้ไกล่เกลี่ย ให้คณะกรรมการผู้เชี่ยวชาญจัดให้มีการไกล่เกลี่ย โดยมอบหมายให้ผู้ไกล่เกลี่ยที่ขึ้นทะเบียนกับสำนักงานเป็นผู้ดำเนินการให้แล้วเสร็จภายใน 30 วัน ทั้งนี้ตามหลักเกณฑ์และวิธีการที่สำนักงานกำหนด ในกรณีที่สามารไกล่เกลี่ยได้ให้ผู้ร้องเรียนและผู้ถูกร้องเรียนรวมถึงบุคคลอื่นที่อาจมีส่วนเกี่ยวข้องทำข้อตกลงดำเนินการแก้ไขเรื่องร้องเรียนตามที่ได้ข้อยุติระหว่างกัน และบันทึกไว้เป็นหลักฐานกับสำนักงาน ในกรณีเช่นนี้ให้คณะกรรมการผู้เชี่ยวชาญสั่งยุติเรื่อง
- (2.9) ในกรณีที่ไมอาจไกล่เกลี่ยได้หรือไกล่เกลี่ยไม่สำเร็จ และคณะกรรมการผู้เชี่ยวชาญพิจารณาตามรายงานชี้แจงเรื่องร้องเรียนแล้ว พบว่ายังไม่มีน้ำหนักรับฟังได้ หรือมีหลักฐานประกอบไม่เพียงพอ คณะกรรมการผู้เชี่ยวชาญอาจมีคำสั่งให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ถูกร้องจัดทำรายงานชี้แจงเพิ่มเติมพร้อมหลักฐานประกอบตามที่คณะกรรมการผู้เชี่ยวชาญกำหนดภายใน 15 วัน ในกรณีที่มีความจำเป็นในการตรวจสอบและรวบรวมข้อเท็จจริงเพื่อคุ้มครองประโยชน์ของเจ้าของข้อมูลส่วนบุคคลหรือเพื่อประโยชน์สาธารณะโดยความเห็นชอบของคณะกรรมการผู้เชี่ยวชาญ ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่เข้าไปในสถานที่ของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ใดเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ในระหว่างเวลาพระอาทิตย์ขึ้นถึงพระอาทิตย์ตกหรือในเวลาทำการของสถานที่นั้น เพื่อตรวจสอบและรวบรวมข้อเท็จจริง ยึดหรืออายัดเอกสารหลักฐาน หรือสิ่งอื่นใดที่เกี่ยวกับการกระทำความผิด หรือมีเหตุอันควรเชื่อได้ว่ามีไว้หรือใช้เพื่อกระทำความผิด ทั้งนี้โดยคำนึงถึงการดำเนินคดีอาญาและแพ่งที่อาจจะเกิดขึ้น



- (2.10) ในกรณีที่พ้นระยะเวลาตาม (2.9) และผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ถูกร้องไม่สามารถชี้แจงเรื่องร้องเรียนให้มีน้ำหนักรับฟังได้ พร้อมพยานหลักฐานที่เพียงพอให้คณะกรรมการผู้เชี่ยวชาญมีคำวินิจฉัยว่ามีการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 และมีคำสั่งทางปกครองให้ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ถูกร้องต้องปฏิบัติภายในระยะเวลาที่กำหนด คำสั่งทางปกครองอาจประกอบด้วย
- ตักเตือน
  - คำสั่งให้กระทำการหรือห้ามกระทำการอย่างใดอย่างหนึ่งหรือหลายอย่างเพื่อแก้ไขการกระทำหรือพฤติกรรมให้ถูกต้องตามกฎหมาย
  - กำหนดค่าปรับทางปกครองตามหมวด 7 ส่วนที่ 2 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- (2.11) ให้สำนักงานประกาศเผยแพร่คำวินิจฉัยโดยระบุการกระทำหรือพฤติกรรมที่ฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย รวมถึงคำสั่งทางปกครองที่คณะกรรมการผู้เชี่ยวชาญกำหนดต่อสาธารณะเป็นการทั่วไปภายในหนึ่งวันทำการนับตั้งแต่วันที่มิมีคำสั่ง แต่ไม่รวมถึงข้อมูลที่ระบุชั้นความลับไม่สามารถเผยแพร่ได้ ทั้งนี้ตามหลักเกณฑ์เกี่ยวกับธรรมาภิบาลข้อมูลของสำนักงาน
- (2.12) หลังจากที่ได้มีคำสั่งตาม (2.10) แล้ว ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้รับคำสั่งทางปกครอง เห็นว่าการกระทำหรือพฤติกรรมที่เป็นปัญหาได้มีการเปลี่ยนแปลงในสาระสำคัญ ทำให้คำสั่งทางปกครองไม่เหมาะสมหรือไม่มีประสิทธิภาพ ก็อาจร้องขอให้คณะกรรมการมอบหมายให้คณะกรรมการผู้เชี่ยวชาญพิจารณามีคำสั่ง ระงับ ยกเลิก เพิ่มเติม หรือปรับปรุงคำสั่งทางปกครองใหม่ก็ได้ตามความเหมาะสมและความจำเป็น ทั้งนี้ต้องแสดงเอกสารและหลักฐานให้เป็นที่ยอมรับแก่คณะกรรมการผู้เชี่ยวชาญ คำสั่งทางปกครองที่กำหนดใหม่ให้ประกาศเผยแพร่ต่อสาธารณะเป็นการทั่วไปภายในหนึ่งวันทำการนับตั้งแต่วันที่คณะกรรมการผู้เชี่ยวชาญมีคำสั่งและอ้างอิงถึงมาตรการเดิมตาม (2.10)