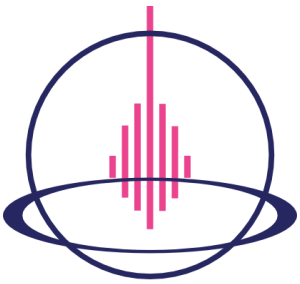
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่

สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เอกสารผลการรับฟังความเห็นเกี่ยวกับร่างกฎหมายลำดับรองกลุ่มที่ 3

โครงการศึกษาและเตรียมการเพื่อจัดทำร่างกฎหมายลำดับรองภายใต้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



ศูนย์บริการวิชาการแห่งจุฬาลงกรณ์มหาวิทยาลัย

1. ร่างกฎหมายลำดับรองกลุ่มที่ 3

1.1 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

สรุปสาระสำคัญของร่างประกาศฯ

(2.1) กำหนดนิยามคำว่า

"หน่วยงานเจ้าของข้อปฏิบัติ (Code Owners)" หมายความว่า สมาคมหรือหน่วยงานต่าง ๆ ที่มีลักษณะตามประกาศนี้ ซึ่งเป็นผู้จัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

"หน่วยงานตรวจสอบ (Monitoring Body)" หมายความว่า หน่วยงานที่ทำหน้าที่ติดตามและตรวจสอบการปฏิบัติตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่ระบุในประกาศนี้

<u>หมวด 1 : หน่วยงานที่สามารถเสนอข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการพิจารณา</u>

(2.2) หน่วยงานกำกับดูแล สมาคม และหน่วยงานที่เกี่ยวข้องอาจสนับสนุนให้กลุ่มองค์กรของตนเอง หรือกลุ่มองค์กรภายใต้การกำกับดูแลของตนเองจัดให้มีข้อปฏิบัติ (Codes of conduct) เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลซึ่งมีเนื้อหารายละเอียดในหัวข้อใดหัวข้อหนึ่งตามประกาศนี้ ที่มีเนื้อหาสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง โดยพิจารณาความเหมาะสมตามลักษณะเฉพาะของ การประมวลผลและขนาดของกิจการในภาคธุรกิจ ต่าง ๆ เพื่อให้สมาชิกภายในกลุ่มสามารถยึดข้อปฏิบัตินั้นเป็นแนวทางปฏิบัติและเป็นสิ่งพิสูจน์ให้เห็นถึงการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้

(2.3) หน่วยงานเจ้าของข้อปฏิบัติ (Code Owners) ซึ่งเป็นตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ซึ่งมีลักษณะอย่างน้อยดังต่อไปนี้ มีสิทธิในการเสนอข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้สำนักงานพิจารณา

- สมาคม กลุ่มสมาคมหรือหน่วยงานอื่น ๆ ซึ่งเป็นตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลแต่ละประเภท กลุ่มธุรกิจในภาคธุรกิจต่าง ๆ
- สมาคมหรือองค์กรการค้า
- องค์กรวิชาการ

- องค์กรวิชาชีพ
- กลุ่มผู้มีส่วนได้เสีย ตามที่คณะกรรมการอาจประกาศกำหนดเพิ่มเติม

ทั้งนี้ หน่วยงานเจ้าของข้อปฏิบัติต้องแสดงให้สำนักงานเห็นว่าหน่วยงานตนสามารถแสดงเจตจำนงในนามกลุ่มองค์กรของตนได้ มีความสามารถและประสบการณ์ที่เกี่ยวข้องในภาคธุรกิจนั้น รวมถึงมีความเข้าใจในลักษณะและความต้องการของกลุ่มองค์กร

<u>หมวด 2 : รายละเอียดของข้อปฏิบัติ</u>

(2.4) หน่วยงานเจ้าของข้อปฏิบัติอาจจัดทำข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลในเรื่องใดเรื่องหนึ่งหรือหลายเรื่องเพื่อให้แสดงให้เห็นถึงการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 รวมถึงแต่ไม่จำกัดเฉพาะเรื่อง ดังต่อไปนี้

- หลักความเป็นธรรมและความโปร่งใสในการประมวลผล
- บริบทในด้านต่าง ๆ ของประโยชน์โดยชอบด้วยกฎหมาย (legitimate interest) ของผู้ควบคุมข้อมูลส่วนบุคคล
- การเก็บรวบรวมข้อมูลส่วนบุคคล
- การปกปิดอัตลักษณ์หรือการแฝงข้อมูล (pseudonymisation)
- แนวทางในการกำหนดลักษณะของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลของกลุ่มสมาชิกไม่ว่าจะเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล
- ลักษณะของข้อมูลส่วนบุคคลที่เปิดเผยแก่สาธารณะและข้อมูลที่ให้เจ้าของข้อมูลส่วนบุคคล
- การใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- การคุ้มครองข้อมูลส่วนบุคคลของผู้เยาว์ตามมาตรา 20 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- มาตรฐานความมั่นคงปลอดภัยขั้นต่ำของการประมวลผลข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามกฎหมาย
- การแจ้งเหตุละเมิดข้อมูลส่วนบุคคลไปยังสำนักงานและเจ้าของข้อมูลส่วนบุคคล
- การส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ
- กลไกการระงับข้อพิพาทโดยไม่กระทบต่อสิทธิของเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- หลักเกณฑ์การพิจารณากำหนดฐานการประมวลผลข้อมูลส่วนบุคคล

- การการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล และการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

(2.5) หน่วยงานเจ้าของข้อปฏิบัติอาจยื่นร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้สำนักงานเพื่อดำเนินการตรวจสอบและรับรองความถูกต้องได้

<u>หมวด 3 : การรับและการพิจารณาข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล</u>

(2.6) หน่วยงานเจ้าของข้อปฏิบัติที่จัดทำข้อปฏิบัติไม่ว่าทั้งหมด หรือแก้ไขเพิ่มเติม อาจส่งร่างข้อปฏิบัติทั้งหมด หรือการแก้ไขเพิ่มเติมให้กับสำนักงานเป็นลายลักษณ์อักษรไม่ว่าจะอยู่ในรูปแบบหนังสือหรืออิเล็กทรอนิกส์ตามที่เห็นสมควร

(2.7) สำนักงานจะตรวจสอบและให้ความเห็นต่อข้อปฏิบัติดังกล่าวได้ก็ต่อเมื่อหน่วยงานเจ้าของข้อปฏิบัติเข้าเกณฑ์การพิจารณาและแสดงให้เห็นถึงรายละเอียดดังต่อไปนี้

- มีวัตถุประสงค์ ขอบเขต และผลสัมฤทธิ์จากข้อปฏิบัติที่เสนอในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งเอกสารประกอบที่เกี่ยวข้อง
- หน่วยงานเจ้าของข้อปฏิบัติเป็นตัวแทนซึ่งเข้าใจความต้องการตามลักษณะของกิจการและลักษณะการประมวลผลของสมาคมหรือหน่วยงานนั้นอย่างชัดเจน
- มีขอบเขตเนื้อหาที่เกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลชัดเจน (Processing Scope)
- มีกลไกการตรวจสอบการปฏิบัติตาม
- มีหน่วยงานตรวจสอบและกลไกที่ช่วยให้หน่วยงานตรวจสอบสามารถปฏิบัติหน้าที่ได้
- มีการปรึกษาหารือกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
- มีความสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง

(2.8) เมื่อได้รับร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลแล้ว ให้สำนักงานพิจารณาว่าจะรับหรือไม่รับพิจารณาร่างข้อปฏิบัติของหน่วยงานเจ้าของข้อปฏิบัติภายในสามสิบวันนับแต่ได้รับรายละเอียดครบถ้วน

- หากพิจารณาแล้วสั่งรับให้สำนักงานส่งให้คณะทำงานที่ได้รับมอบหมายจากคณะกรรมการให้ทำการตรวจสอบและให้ความเห็นต่อร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวตามหลักเกณฑ์ต่อไป

- หากพิจารณาแล้วสั่งไม่รับให้ส่งคืนร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนั้นพร้อมทั้งเหตุผลในการปฏิเสธ หน่วยงานเจ้าของข้อปฏิบัติจะสามารถยื่นร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้พิจารณาได้อีกครั้งหนึ่ง เมื่อพ้นระยะเวลาเก้าสิบวันนับแต่ได้รับการปฏิเสธ

(2.9) ให้คณะทำงานที่ได้รับมอบหมายจากคณะกรรมการดำเนินการตรวจสอบและให้ความเห็นร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนั้นภายในหกสิบวันนับแต่ได้รับร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลจากสำนักงาน โดยมีหลักเกณฑ์ขั้นต่ำที่ต้องพิจารณาดังต่อไปนี้

- ร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตอบสนองความต้องการเฉพาะของภาคธุรกิจหรือลักษณะการประมวลผลนั้นอย่างมีประสิทธิภาพหรือไม่ ทั้งนี้ ร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลจะต้องกำหนดรายชื่อของสมาชิกของหน่วยงานเจ้าของข้อปฏิบัติด้วย
- ร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลส่งผลสัมฤทธิ์ต่อการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้องแก่ภาคธุรกิจหรือลักษณะการประมวลผลนั้นอย่างมีประสิทธิภาพหรือไม่
- ร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสามารถบ่งชี้ได้ว่าสามารถแสดงให้เห็นถึงการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้องในส่วนใด และสามารถปฏิบัติได้จริงและเป็นมาตรฐาน
- ร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสามารถบ่งชี้ได้ว่ามีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ
- ร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสามารถบ่งชี้ได้ว่ามีรายละเอียดเกี่ยวกับกลไกการติดตามและตรวจสอบการปฏิบัติตามอย่างมีประสิทธิภาพ

(2.10) หากคณะทำงานที่ได้รับมอบหมายจากคณะกรรมการเห็นว่าร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนั้นครบถ้วนสมบูรณ์แล้ว ให้ส่งผลการพิจารณาไปยังสำนักงานและแจ้งให้หน่วยงานเจ้าของข้อปฏิบัติทราบภายในเจ็ดวันนับแต่ได้รับผลการพิจารณา เมื่อได้รับความเห็นชอบแล้ว ให้หน่วยงานเจ้าของข้อปฏิบัติจัดทำและเผยแพร่ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว และให้สามารถเข้าถึงได้โดยสาธารณะด้วยวิธีการตามสมควร

(2.11) กรณีคณะทำงานที่ได้รับมอบหมายจากคณะกรรมการตรวจสอบและมีความเห็นให้ปรับปรุง แก้ไข หรือทำใหม่ทั้งหมดหรือบางส่วน ให้ส่งผลการพิจารณาไปยังสำนักงานและให้สำนักงานส่งกลับให้

หน่วยงานเจ้าของข้อปฏิบัติปรับปรุง แก้ไข หรือทำใหม่ทั้งหมดหรือบางส่วน ภายในเจ็ดวันนับแต่ได้รับผลการพิจารณา โดยหน่วยงานเจ้าของข้อปฏิบัติจะต้องแก้ไขเพิ่มเติมให้แล้วเสร็จภายในหกสิบวันและนำส่งให้สำนักงานเพื่อให้คณะทำงานที่ได้รับมอบหมายจากคณะกรรมการพิจารณาอีกครั้งหนึ่ง

(2.12) คณะทำงานที่ได้รับมอบหมายจากคณะกรรมการต้องตรวจสอบและให้ความเห็นต่อร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่มีการแก้ไขภายในสามสิบวันนับแต่ได้รับร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลจากสำนักงาน

- หากคณะทำงานที่ได้รับมอบหมายจากคณะกรรมการเห็นว่าร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลนั้นครบถ้วนสมบูรณ์แล้ว ให้ส่งผลการพิจารณาไปยังสำนักงานและแจ้งให้หน่วยงานเจ้าของข้อปฏิบัติทราบภายในเจ็ดวันนับแต่ได้รับผลการพิจารณา
- หากยังมีความเห็นให้ปรับปรุง แก้ไขในสาระสำคัญ ให้คณะทำงานที่ได้รับมอบหมายจากคณะกรรมการปฏิเสธและให้สำนักงานแจ้งผลภายในเจ็ดวันนับแต่ได้รับผลการพิจารณา โดยหน่วยงานเจ้าของข้อปฏิบัติจะสามารถยื่นร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้พิจารณาได้อีกครั้งหนึ่ง เมื่อพ้นระยะเวลาเก้าสิบวันนับแต่ได้รับการปฏิเสธ

(2.13) หากระยะเวลาสามสิบวันสิ้นสุดลงโดยที่คณะทำงานที่ได้รับมอบหมายจากคณะกรรมการไม่มีความเห็นเพิ่มเติม ให้ถือว่าร่างข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าวได้รับความเห็นชอบจากคณะทำงานที่ได้รับมอบหมายจากคณะกรรมการแล้ว ให้สำนักงานแจ้งให้หน่วยงานเจ้าของข้อปฏิบัติทราบภายในเจ็ดวันนับแต่สิ้นสุดระยะเวลาดังกล่าว

เมื่อได้รับความเห็นชอบแล้ว ให้หน่วยงานเจ้าของข้อปฏิบัติจัดทำและเผยแพร่ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว และให้สามารถเข้าถึงได้โดยสาธารณะด้วยวิธีการตามสมควร

(2.14) เมื่อมีการเปลี่ยนแปลงแก้ไขสมาชิกที่อยู่ภายใต้การปฏิบัติตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลใด หน่วยงานเจ้าของข้อปฏิบัตินั้นมีหน้าที่แจ้งการเปลี่ยนแปลงแก้ไขต่อสำนักงานภายในสิบห้าวันนับแต่มีการเปลี่ยนแปลงแก้ไขครั้งล่าสุด

(2.15) เพื่อประโยชน์ในการค้นหาและการอ้างอิงข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับความเห็นชอบแล้ว ให้สำนักงานประกาศรายชื่อข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่ได้รับความเห็นชอบผ่านช่องทางสาธารณะตามที่เห็นสมควร ซึ่งรวมถึงรายชื่อสมาชิกที่อยู่ภายใต้การปฏิบัติตามข้อปฏิบัตินั้นด้วย

(2.16) เมื่อคณะกรรมการผู้เชี่ยวชาญตรวจพบเองหรือได้รับเรื่องร้องเรียนแล้วพบว่าข้อปฏิบัตินั้นมีเนื้อหาไม่สอดคล้องกับกฎหมาย ให้บุคคลดังกล่าวเสนอเรื่องให้คณะทำงานที่ได้รับมอบหมายจาก

คณะกรรมการทำการพิจารณา และคณะทำงานที่ได้รับมอบหมายจากคณะกรรมการอาจมีคำสั่งให้เจ้าของข้อปฏิบัติดำเนินการแก้ไข ปรับปรุงข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลภายในหกสิบวันนับแต่ได้รับแจ้ง กระบวนการดังกล่าวให้ใช้บังคับรวมถึงกรณีที่คณะกรรมการหรือคณะทำงานที่ได้รับมอบหมายจากคณะกรรมการพบเรื่องดังกล่าวเองไม่ว่าด้วยวิธีการใดก็ตาม

<u>หมวด 4 : การติดตามและตรวจสอบข้อปฏิบัติ (Monitoring)</u>

(2.17) ในการกำหนดกลไกการติดตามและตรวจสอบการปฏิบัติตามอย่างมีประสิทธิภาพ ให้จัดให้มีหน่วยงานตรวจสอบ (Monitoring Body) เป็นผู้รับผิดชอบในการติดตามและตรวจสอบการปฏิบัติตามดังกล่าว หน่วยงานตรวจสอบ (Monitoring Body) อาจเป็นหน่วยงาน หรือคณะกรรมการภายในหรือภายนอกหน่วยงานเจ้าของข้อปฏิบัติซึ่งได้เสนอไว้ในข้อปฏิบัติก็ได้โดยจะต้องเป็นบุคคลที่ได้รับการรับรองจากสำนักงานแล้วตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยมาตรฐานและการรับรองการคุ้มครองข้อมูลส่วนบุคคล

(2.18) หน่วยงานตรวจสอบ มีหน้าที่ติดตามและตรวจสอบเรื่องดังต่อไปนี้

- ติดตามและตรวจสอบการปฏิบัติตามข้อปฏิบัติที่ได้รับการรับรอง หากพบการละเมิดข้อกำหนดของข้อปฏิบัติ หน่วยงานตรวจสอบต้องดำเนินการให้สมาชิกจัดมาตรการที่เหมาะสมเพื่อหยุดการละเมิดและหลีกเลี่ยงการเกิดซ้ำในอนาคต
- แจ้งผลการตรวจสอบการปฏิบัติตามข้อปฏิบัติที่ได้รับการรับรองให้สำนักงานทราบ รวมถึงแต่ไม่จำกัดเฉพาะ เรื่องที่ตรวจสอบ ข้อปฏิบัติที่เกี่ยวข้อง ระยะเวลาที่ตรวจสอบล่าสุด รายชื่อของสมาชิกที่ปฏิบัติตามข้อปฏิบัติอย่างครบถ้วนและบกพร่องในการปฏิบัติตาม โดยให้เป็นไปตามรูปแบบข้อมูลที่สำนักงานกำหนด

  เมื่อได้รับแจ้งผลการตรวจสอบแล้ว สำนักงานอาจเผยแพร่ผลการตรวจสอบการปฏิบัติตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลดังกล่าว และให้สามารถเข้าถึงได้โดยสาธารณะด้วยวิธีการตามสมควร
- ตรวจสอบว่าข้อปฏิบัติยังคงเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล หากพบว่าข้อปฏิบัติต้องได้รับการทบทวน อาจให้หน่วยงานเจ้าของข้อปฏิบัติปรับปรุงหรือแก้ไขเพิ่มเติมในส่วนที่ต้องทบทวนแล้วเสนอให้สำนักงานพิจารณาต่อไป

(2.19) หน่วยงานเจ้าของข้อปฏิบัติต้องยอมให้หน่วยงานตรวจสอบสามารถตรวจสอบการปฏิบัติตามข้อกำหนดในข้อปฏิบัติได้ หากพบการละเมิดการปฏิบัติตามข้อปฏิบัติ หรือพบว่าไม่มีการติดตามหรือ

ตรวจสอบการปฏิบัติตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล สำนักงานอาจสั่งเพิกถอนการรับรองหน่วยงานตรวจสอบหรือเพิกถอนข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล หรือสั่งให้ทบทวนได้ ทั้งนี้ ตามความร้ายแรงของพฤติการณ์

1.2 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ที่จะให้เจ้าของข้อมูลส่วนบุคคลปฏิเสธการถูกตัดสินใจโดยใช้กระบวนการอัตโนมัติเพียงอย่างเดียว

สรุปสาระสำคัญของร่างประกาศฯ

(2.1) กำหนดคำนิยาม

“ผู้เปราะบาง” หมายถึง บุคคลที่ภายใต้วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้น มีความจำกัดของความสามารถในการให้ความยินยอมโดยอิสระ หรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้โดยอิสระ หรือเข้าใจผลกระทบที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคลนั้น

“โปรไฟลิ่ง” หมายถึง รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินแง่มุมเกี่ยวกับบุคคล โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลธรรมดาในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล ประโยชน์ของบุคคล พฤติกรรมของบุคคล ความน่าเชื่อถือของบุคคล ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล

“การตัดสินใจโดยใช้กระบวนการอัตโนมัติเพียงอย่างเดียว” หมายถึง กระบวนการการตัดสินใจโดยใช้วิธีอัตโนมัติ และปราศจากการมีส่วนร่วมของมนุษย์ ซึ่งเป็นการตัดสินใจโดยอาศัยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลทั้งที่เป็นข้อมูลที่ได้รับมา และเป็นข้อมูลที่ถูกสร้างขึ้นโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเอง

(2.2) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

- การประมวลผลอันจะส่งผลให้สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลต้องเสื่อมเสียไป หรือทำให้ไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ ถือเป็นการประมวลผลข้อมูลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- คณะกรรมการอาจกำหนดให้กิจกรรมการประมวลผลบางประเภทเป็นการประมวลผลข้อมูลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลตามรายชื่อแนบท้ายประกาศ หรือตามที่กำหนดไว้ในข้อปฏิบัติที่ได้รับการรับรองจากคณะกรรมการ
- ในกรณีที่การประมวลผลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และให้สันนิษฐานว่าผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลและจัดให้มีมาตรการที่เหมาะสมแล้วตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

- ในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องประเมินความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคลก่อนหรือในขณะที่มีการประมวลผลข้อมูลส่วนบุคคล รวมถึงการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่แล้ว
- นอกเหนือจากกรณีที่กำหนดในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือที่กำหนดในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยรูปแบบ วิธีการ และมาตรฐานขั้นต่ำที่กำหนดร่วมกัน การประมวลผลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลให้รวมถึงกิจกรรมการประมวลผลที่มีลักษณะดังต่อไปนี้
    - กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ รวมถึงการโปรไฟลิ่ง ซึ่งการประมวลผลดังกล่าวส่งผลเป็นการตัดสินใจที่ส่งผลทางกฎหมายหรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
    - กรณีที่มีการประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลส่วนบุคคลตาม มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยพิจารณาจากจำนวนบุคคลที่เกี่ยวข้อง ปริมาณข้อมูลที่เกี่ยวข้อง ความหลากหลายของข้อมูลที่เกี่ยวข้อง ระยะเวลาการประมวลผลข้อมูลที่เกี่ยวข้อง และขนาดพื้นที่ทางภูมิศาสตร์ของการประมวลผลข้อมูลที่เกี่ยวข้อง
    - กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ
- ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลตามหน้าที่ที่กฎหมายกำหนดทั้งโดยฐานภายใต้มาตรา 24 (4) หรือ (6) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาจหารือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อกำหนดกิจกรรมที่มีความเสี่ยงสูงซึ่งอาจไม่จำต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลก็ได้ ทั้งนี้ขั้นตอนและรายละเอียดให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลอาจมีขึ้นเพื่อรองรับการประมวลผลข้อมูลหลายกรณีที่มีลักษณะเดียวกันทั้งโดยสภาพ วัตถุประสงค์ หรือความเสี่ยง กรณีเช่นนี้พึงเปิดเผยข้อมูลอ้างอิงของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลสู่สาธารณะ รวมถึงมาตรการที่กำหนดและเหตุผลที่จัดทำการประเมินร่วมกัน
- กรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล พึงระบุหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลแต่ละรายและมาตรการที่แต่ละฝ่ายรับผิดชอบไว้เป็นลายลักษณ์อักษร โดยระบุถึงเหตุผลความจำเป็นและข้อมูลของแต่ละฝ่าย แต่ทั้งนี้เท่าที่ไม่กระทบเทือนถึงความลับหรือจุดอ่อนทางธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล

(2.3) การจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

- ในกรณีที่จำเป็นผู้ควบคุมข้อมูลส่วนบุคคลอาจมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมที่อยู่ภายใต้ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลแทนก็ได้
- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล อาจแสดงให้เห็นขั้นตอนอย่างน้อยดังต่อไปนี้
    - ระบุความจำเป็นในการทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
    - อธิบายรายละเอียดการประมวลผลข้อมูลส่วนบุคคล
    - การรับฟังความคิดเห็นผู้มีส่วนได้เสีย
    - แสดงให้เห็นความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูลส่วนบุคคล
    - การประเมินความเสี่ยง ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน
    - ระบุมาตรการลดความเสี่ยง
    - บันทึกรายละเอียดของแต่ละขั้นตอน
    - การติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการที่ได้จากการทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- หากได้ดำเนินการตามข้อปฏิบัติที่ได้รับการรับรองจากคณะกรรมการแล้ว ให้ถือว่าได้ดำเนินการจัดทำ DPIA แล้ว
- ผู้ควบคุมข้อมูลส่วนบุคคลต้องเผยแพร่เอกสารการบันทึกผลการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลให้สามารถเข้าถึงได้โดยสาธารณะด้วยวิธีการตามสมควรและแจ้งช่องทางเผยแพร่นั้นแก่สำนักงาน โดยอาจปกปิดหรือตัดเฉพาะส่วนที่เป็นข้อมูลลับทางการค้าหรือที่กระทบความมั่นคงปลอดภัยหรือความเสี่ยงต่าง ๆ ออกจากการเผยแพร่ได้

(2.4) หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลที่ใช้กระบวนการอัตโนมัติเพียงอย่างเดียว

- ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการประมวลผลด้วยมนุษย์หรือโดยมนุษย์มีส่วนร่วม ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่ยอมรับการถูกตัดสินใจโดยใช้กระบวนการอัตโนมัติเพียงอย่างเดียว รวมถึงการโปรไฟลิ่ง ซึ่งทำให้เกิดผลทางกฎหมายหรือผลกระทบอื่น ๆ ที่ร้ายแรงในทำนองเดียวกันต่อเจ้าของข้อมูลส่วนบุคคล
- ข้อยกเว้นการจัดทำ คือในกรณีที่การตัดสินใจนั้นจำเป็นต่อการเข้าทำสัญญาหรือปฏิบัติตามสัญญา ได้รับอนุญาตตามกฎหมาย หรือได้รับความยินยอมโดยชัดแจ้งจากเจ้าของข้อมูลส่วนบุคคล โดยในกรณีจำเป็นต่อการเข้าทำสัญญาหรือปฏิบัติตามสัญญา และได้รับอนุญาตตามกฎหมาย ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์โดยชอบด้วยกฎหมายของเจ้าของข้อมูลส่วนบุคคลอย่างน้อยที่สุดต้องรับรองให้เจ้าของข้อมูลส่วนบุคคลสามารถจะเลือกให้มีการแทรกแซงของมนุษย์เป็นส่วนหนึ่งของการควบคุมข้อมูลเพื่อแสดงความเห็นและโต้แย้งการตัดสินใจ

- ต้องไม่ใช่การตัดสินใจโดยใช้ข้อมูลส่วนบุคคลตามมาตรา 26 เว้นเสียแต่ว่าเข้ากรณีตามมาตรา 26 วรรคแรก หรือมาตรา 26 (5) (จ) และได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์โดยชอบด้วยกฎหมายของเจ้าของข้อมูลส่วนบุคคลแล้ว
- ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ในการอธิบายและตอบคำถาม รวมถึงการรับฟังความเห็นเกี่ยวกับการตัดสินใจโดยกระบวนการอัตโนมัติเพียงอย่างเดียวจากเจ้าของข้อมูล ทั้งขณะก่อนหน้าหรือในขณะที่มีการเก็บรวบรวมข้อมูลส่วนบุคคล ทั้งนี้ให้เป็นไปตามบทบัญญัติในมาตรา 21 มาตรา 23 และมาตรา 25 ของพระพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศที่เกี่ยวข้อง
- ผู้ควบคุมข้อมูลส่วนบุคคลที่ใช้กระบวนการอัตโนมัติเพียงอย่างเดียวต้องแจ้งรายละเอียดกิจกรรมการประมวลผลอย่างชัดเจนก่อนการประมวลผลข้อมูลส่วนบุคคล พร้อมรายงานการประเมินผลกระทบหากมีการจัดทำไว้แล้วในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่ยอมรับการถูกตัดสินใจโดยใช้กระบวนการอัตโนมัติเพียงอย่างเดียว และขอให้ประมวลผลโดยมนุษย์ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องแจ้งผลการประมวลผลดังกล่าวให้แก่เจ้าของข้อมูลส่วนบุคคลทราบ ทั้งนี้ให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หน้าที่ในการให้ใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

(2.5) รูปแบบ วิธีการ และมาตรฐานขั้นต่ำที่กำหนดร่วมกันเพื่อประโยชน์ในการพิสูจน์

- หน่วยงานกำกับดูแล สภาวิชาชีพ สมาคม หรือ กลุ่มอุตสาหกรรม อาจร่วมกันกำหนดรูปแบบ วิธีการ และมาตรฐานขั้นต่ำของกรณีนั้น ๆ ที่เหมาะสมกับกิจกรรมการประมวลผลกรณีที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคลไว้ในข้อปฏิบัติของตนเพื่อรับการรับรองจากคณะกรรมการ โดยต้องดำเนินการและมีรายละเอียดตามประกาศ และให้มีการเผยแพร่ไว้เป็นการทั่วไปเพื่อให้ผู้ควบคุมข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงข้อปฏิบัติดังกล่าวได้โดยง่าย
- คณะกรรมการอาจกำหนดรูปแบบ วิธีการ และมาตรฐานขั้นต่ำ ของกรณีที่สำคัญไว้ เพื่อให้หน่วยงานกำกับดูแล สภาวิชาชีพ สมาคม หรือ กลุ่มอุตสาหกรรม สามารถใช้เป็นต้นแบบในการพิจารณากำหนดรูปแบบ วิธีการ และมาตรฐานขั้นต่ำของกรณีที่เหมาะสมกับกิจกรรมต่าง ๆ ของผู้ควบคุมข้อมูลส่วนบุคคลที่อยู่ภายใต้การกำกับดูแลหรือภายในกลุ่มดังกล่าวต่อไปก็ได้

รายชื่อกิจกรรมการประมวลผลข้อมูลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่คณะกรรมการกำหนด

กิจกรรมใดที่มีลักษณะดังต่อไปนี้รวมกันตั้งแต่ 2 ประการขึ้นไป ให้ถือเป็นกิจกรรมที่มีความเสี่ยงสูง

1. การประมวลผลข้อมูลส่วนบุคคลที่มีการใช้เทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (artificial intelligence)
2. การใช้โปรไฟลิ่งหรือข้อมูลที่อ่อนไหวในการปฏิเสธไม่ให้เข้าถึงบริการ
3. การทำโปรไฟลิ่งของบุคคลในปริมาณมาก
4. การประมวลผลข้อมูลชีวภาพ
5. การประมวลผลข้อมูลพันธุกรรม
6. การจับคู่หรือเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง
7. การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว
8. การติดตามตำแหน่งที่อยู่หรือพฤติกรรมของบุคคล
9. การทำโปรไฟลิ่งหรือทำการตลาดแบบระบุเป้าหมาย (target marketing) หรือบริการออนไลน์ที่มุ่งโดยตรงแก่ผู้เยาว์หรือผู้เปราะบาง
10. การประมวลผลข้อมูลที่อาจเป็นอันตรายต่อสุขอนามัยหรือความปลอดภัยของบุคคลในกรณีที่มีการรั่วไหล

1.3 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง มาตรฐานและการรับรองด้านการคุ้มครองข้อมูลส่วนบุคคล

สรุปสาระสำคัญของร่างพระราชกฤษฎีกาฯ

(2.1) กำหนดนิยามคำว่า

"องค์กรรับรองมาตรฐาน" หมายความว่า องค์กรที่ได้รับอนุญาตจากคณะกรรมการให้สามารถรับรองด้านการคุ้มครองข้อมูลส่วนบุคคลได้ตามหมวด 2 ของประกาศนี้

"หน่วยงานตรวจสอบ" หมายความว่า หน่วยงานที่ทำหน้าที่ติดตามและตรวจสอบการปฏิบัติตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่ระบุในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

<u>หมวด 1 : บททั่วไป</u>

(2.2) ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอาจยื่นคำขอต่อองค์กรรับรองมาตรฐานเพื่อให้ได้รับการรับรองมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคล

(2.3) การรับรองมาตรฐานต่าง ๆ ที่อยู่ภายใต้การอนุญาตของคณะกรรมการนั้นไม่เป็นการห้ามมิให้มีการรับรองมาตรฐานด้านการคุ้มครองอื่น ๆ

<u>หมวด 2 : การรับรองมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคลและองค์กรรับรองมาตรฐาน</u>

<u>การยื่นขอเป็นองค์กรรับรองมาตรฐานและการพิจารณาอนุญาต</u>

(2.4) สมาคมวิชาชีพ องค์กร หรือบุคคลใด สามารถยื่นคำขอต่อสำนักงานเพื่อให้คณะกรรมการอนุญาตในการรับรองมาตรฐานด้านการคุ้มครองข้อมูลส่วนบุคคลได้ ทั้งนี้ สำนักงานอาจกำหนดให้คำขอเป็นไปตามที่รูปแบบที่สำนักงานกำหนดได้

(2.5) ในการพิจารณาอนุญาตให้เป็นองค์กรรับรองมาตรฐานนั้น ผู้ยื่นคำขอจะต้องแสดงให้เห็นว่า

- ผู้ยื่นคำขอมีความเป็นอิสระและความเชี่ยวชาญในเรื่องที่จะรับรองมาตรฐาน
- ผู้ยื่นคำขอแสดงให้เห็นว่ามาตรฐานประการต่าง ๆ ที่จะต้องพิจารณาในการรับรองไม่ต่ำกว่ามาตรฐานตามที่กำหนดไว้ในข้อ 2.6

- ผู้ยื่นคำขอมีการกำหนดกระบวนการในการรับรอง การทบทวน และการเพิกถอนการรับรอง รวมถึงตราสัญลักษณ์ที่แสดงว่าได้รับการรับรองแล้ว ทั้งนี้จะต้องมีรายการอย่างน้อยตามที่กำหนดไว้ในข้อ 2.7
- ผู้ยื่นคำขอมีกระบวนการในการรับเรื่องร้องเรียนเกี่ยวกับการละเมิดมาตรฐานที่ได้รับการรับรอง โดยกระบวนการดังกล่าวจะต้องมีความโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคลและต่อสาธารณะ
- ผู้ยื่นคำขอจะต้องแสดงให้ปรากฏแก่คณะกรรมการว่าการปฏิบัติหน้าที่จะไม่ก่อให้เกิดการขัดกันซึ่งผลประโยชน์

(2.6) มาตรฐานในการตรวจสอบเพื่อรับรองด้านการคุ้มครองข้อมูลส่วนบุคคลต้องได้รับความเห็นชอบจากคณะกรรมการ โดยจะต้องมีรายการอย่างน้อยดังต่อไปนี้

- การประมวลผลข้อมูลนั้นมีความชอบด้วยกฎหมายเป็นไปตามมาตรา 24 และมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง
- มีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลประกาศให้เจ้าของข้อมูลส่วนบุคคลทราบ และมีการแจ้งข้อมูลที่ครบถ้วนตามมาตรา 23 หรือมาตรา 25 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง
- มีการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคลตามมาตรา 30 ถึงมาตรา 36 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง
- มีการกำหนดระยะเวลาในการจัดเก็บข้อมูลและมาตรการในการลบหรือทำลายข้อมูลตามมาตรา 37 (3) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง
- มีกระบวนการรองรับเพื่อแจ้งเหตุละเมิดข้อมูลตามมาตรา 37 (4) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง
- มีการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (data protection impact assessment) ในกรณีที่เป็นการประมวลผลที่ใช้เทคโนโลยีใหม่หรือมีแนวโน้มที่จะก่อให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล และประกาศคณะกรรมการที่เกี่ยวข้อง

- มีการแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา 41 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง
- มีการโอนข้อมูลไปยังต่างประเทศที่ชอบด้วยกฎหมายตามมาตรา 28 ถึงมาตรา 29 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง และ
- กรณีที่มีการประมวลผลโดยผู้ประมวลผลข้อมูลส่วนบุคคล จะต้องมีการทำข้อตกลงประมวลผลข้อมูลส่วนบุคคลตามมาตรา 40 วรรคสามแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการที่เกี่ยวข้อง

(2.7) กระบวนการในการรับรองจะต้องมีรายละเอียดอย่างน้อยดังต่อไปนี้

- ผู้ที่สามารถยื่นคำขอได้และขั้นตอนในการยื่นคำขอรับรอง
- ขั้นตอนวิธีการหรือรายละเอียดในการประเมินตามหลักเกณฑ์ที่ใช้ในการประเมินแต่ละประการ
- ระยะเวลาการดำเนินการในแต่ละกระบวนการ
- รูปแบบใบรับรองและตราสัญลักษณ์ที่แสดงให้เห็นถึงการรับรองมาตรฐาน
- การตรวจสอบ ทบทวน และเพิกถอนใบรับรองและตราสัญลักษณ์

(2.8) เมื่อได้รับคำขอให้เป็นองค์กรรับรองมาตรฐานแล้ว ให้สำนักงานตรวจสอบคำขอเสียก่อน หากพิจารณาแล้วเห็นว่ารายละเอียดยังไม่ครบถ้วนตามที่กำหนด ให้สำนักงานแจ้งผู้ยื่นคำขอดำเนินการแก้ไขแล้วยื่นคำขอมาอีกครั้ง ในกรณีที่คำขอมีความครบถ้วนแล้ว ให้สำนักงานแจ้งรับคำขอไปยังผู้ยื่นคำขอทราบและส่งเรื่องดังกล่าวเพื่อให้คณะกรรมการพิจารณาต่อไป

(2.9) คณะกรรมการจะต้องดำเนินการพิจารณาอนุญาตหรือไม่อนุญาต ทั้งนี้อาจมอบหมายให้คณะอนุกรรมการหรือบุคคลอื่นเป็นผู้พิจารณาเพื่อเสนอให้คณะกรรมการพิจารณาก็ได้ อย่างไรก็ดี คณะกรรมการจะมีคำสั่งอนุญาตหรือไม่อนุญาตให้แล้วเสร็จภายใน 60 วัน นับแต่วันที่สำนักงานแจ้งรับคำขอ หากจะไม่แล้วเสร็จภายในกำหนดเวลาให้แจ้งเหตุแห่งความล่าช้าแก่ผู้ยื่นคำขอพร้อมทั้งกำหนดเวลาเพิ่มเติมซึ่งต้องไม่เกิน 60 วันนับแต่วันที่ครบกำหนดแรก

(2.10) ระหว่างการพิจารณารับรอง คณะกรรมการหรือสำนักงานอาจมีการร้องขอเพื่อเข้าไปตรวจสอบยังที่ทำการของผู้ยื่นคำขอหรือร้องขอเอกสารเพิ่มเติมหรือเรียกให้มีผู้เข้ามาชี้แจงรายละเอียดเพิ่มเติมได้ รวมถึงให้ผู้ยื่นคำขอแก้ไขรายละเอียดเกี่ยวกับมาตรฐาน หรือกระบวนการให้เหมาะสมยิ่งขึ้น

(2.11) กรณีที่คณะกรรมการมีคำสั่งอนุญาตให้ผู้ยื่นคำขอเป็นองค์กรรับรองมาตรฐาน ให้สำนักงานมีหน้าที่ดำเนินการจัดทำรายชื่อขององค์กรรับรองมาตรฐานอีกทั้งรายละเอียด เพื่อประกาศให้ประชาชนทราบโดยทั่วไป

(2.12) กรณีที่คณะกรรมการเห็นว่าผู้ยื่นคำขอไม่อาจแสดงให้เห็นว่าสามารถดำเนินการหลักเกณฑ์พิจารณาการเป็นองค์กรรับรองมาตรฐาน หรือไม่สามารถดำเนินการตามมาตรฐานในการตรวจสอบเพื่อรับรองด้านการคุ้มครองข้อมูลส่วนบุคคลได้ กระบวนการในการรับรองหรือปฏิเสธการตรวจสอบ การเรียกข้อมูลเพิ่มเติม หรือการแก้ไขตามที่สำนักงานร้องขอ ให้คณะกรรมการมีดุลพินิจในการสั่งไม่อนุญาตให้ผู้ยื่นคำขอเป็นองค์กรรับรองมาตรฐาน พร้อมทั้งชี้แจงเหตุแห่งการไม่อนุญาตนั้นแจ้งให้ผู้ยื่นคำขอทราบต่อไป กรณีที่สำนักงานปฏิเสธคำขอ ผู้ยื่นนั้นอาจยื่นคำขอมาใหม่ได้ แต่เมื่อเวลาได้ล่วงผ่านไปไม่น้อยกว่า 180 วัน นับแต่วันที่คณะกรรมการมีคำสั่งไม่อนุญาต

(2.13) สถานะในการเป็นองค์กรรับรองมาตรฐานนั้นมีกำหนดอายุ 5 ปี นับแต่วันที่คณะกรรมการมีคำสั่งอนุญาต

(2.14) การขอต่อสถานะการรับรองให้ดำเนินการได้เมื่อสถานะการเป็นองค์กรรับรองมาตรฐานเหลือไม่เกิน 6 เดือน การยื่นต่ออายุให้นำเอากระบวนการยื่นคำขอและพิจารณาสำหรับการยื่นคำขอครั้งแรกมาใช้โดยอนุโลม โดยสถานะเป็นองค์กรรับรองเมื่อคณะกรรมการมีคำสั่งอนุญาตให้มีสถานะต่อไปได้อีก 5 ปี นับแต่วันที่สิ้นสุดสถานะครั้งก่อนหน้า

(2.15) กรณีที่ข้อเท็จจริงปรากฏแก่คณะกรรมการว่าองค์กรรับรองมาตรฐานไม่ได้ดำเนินการรับรองมาตรฐานต่าง ๆ ที่อยู่ภายใต้การอนุญาตของคณะกรรมการอีกต่อไป หรือไม่ดำเนินการให้เป็นไปตามมาตรฐานหรือกระบวนการที่ได้รับการรับรอง คณะกรรมการมีอำนาจสั่งระงับสถานะการเป็นองค์กรรับรองมาตรฐานได้เพื่อมีคำสั่งให้ดำเนินการแก้ไขให้ถูกต้อง หากไม่สามารถดำเนินการแก้ไขได้ให้คณะกรรมการสามารถสั่งเพิกถอนการเป็นองค์กรรับรองมาตรฐานได้

(2.16) กรณีที่มีการเพิกถอนองค์กรรับรองมาตรฐาน ให้สำนักงานดำเนินการลบชื่อดังกล่าวออกจากรายชื่อโดยไม่ชักช้า

<u>การรับรองหน่วยงานตรวจสอบ</u>

(2.17) หน่วยงานตรวจสอบ (Monitoring body) ที่จะได้รับการรับรองอาจเป็นหน่วยงานหรือคณะกรรมการภายในหรือภายนอกซึ่งมีลักษณะดังต่อไปนี้

- มีความเป็นอิสระจากหน่วยงานเจ้าของข้อปฏิบัติ

- ไม่มีผลประโยชน์ขัดหรือแย้งกับการปฏิบัติหน้าที่ (Conflict of interest)
- มีความเชี่ยวชาญในงานด้านการติดตามและตรวจสอบ กฎหมายคุ้มครองข้อมูลส่วนบุคคล และลักษณะการประมวลผลซึ่งข้อมูลส่วนบุคคลตามข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
- มีโครงสร้างและวิธีการในการติดตามและตรวจสอบอย่างมีประสิทธิภาพ
- มีกระบวนการจัดการข้อร้องเรียนที่เป็นกลางและโปร่งใส
- มีกระบวนการประสานงานและให้ความร่วมมือกับสำนักงาน
- มีกลไกการทบทวนตามการเปลี่ยนแปลงของกฎหมายคุ้มครองข้อมูลส่วนบุคคลและเทคโนโลยี

(2.18) ให้นำเอาบทบัญญัติในส่วนการยื่นขอเป็นองค์กรรับรองมาตรฐานและการพิจารณาอนุญาต มาใช้กับการยื่นคำขอ การพิจารณาอนุญาต การตรวจสอบคำขอ อายุของการอนุญาต การต่ออายุ ระงับใช้และเพิกถอนสถานะหน่วยงานตรวจสอบโดยอนุโลม ทั้งนี้ เท่าที่ไม่ขัดกับบทบัญญัติในส่วนนี้และไม่ขัดต่อประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง ข้อปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

<u>การรับรองมาตรฐานโดยองค์กรรับรองมาตรฐาน</u>

(2.19) องค์กรรับรองมาตรฐานมีหน้าที่ในการดำเนินการรับรองมาตรฐานให้เป็นไปตามหลักเกณฑ์และกระบวนการตามที่ได้รับความเห็นชอบจากคณะกรรมการและได้รับอนุญาตให้เป็นองค์กรรับรองมาตรฐาน

(2.20) องค์กรรับรองมาตรฐานมีหน้าที่ในการประกาศมาตรฐานและกระบวนการนั้นต่อสาธารณะเพื่อให้บุคคลทั่วไปได้ทราบ รวมทั้งกระบวนการในการประเมินนั้นจะต้องมีความโปร่งใสตรวจสอบได้ ทั้งนี้ หากคณะกรรมการหรือสำนักงานร้องขอ องค์กรรับรองมาตรฐานจะต้องสามารถชี้แจงได้ถึงเหตุในการออกใบรับรองหรือให้ต่ออายุใบรับรองได้

(2.21) ในกระบวนการประเมินเพื่อรับรองมาตรฐาน ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลข้อมูลส่วนบุคคลมีหน้าที่ที่ยื่นขอรับรองมาตรฐานจะต้องให้ข้อมูลทั้งหมดเกี่ยวกับกิจกรรมประมวลผลข้อมูลแก่องค์กรรับรองมาตรฐาน อีกทั้งให้องค์กรรับรองมาตรฐานเข้าถึงข้อมูลดังกล่าวได้ตามที่มีความจำเป็นที่จะต้องตรวจสอบในกระบวนการประเมินเพื่อรับรองมาตรฐาน

(2.22) องค์กรรับรองมาตรฐานมีหน้าที่จัดทำรายชื่อของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่ผ่านการรับรอง รวมถึงรายละเอียดและขอบเขตของการดำเนินการที่ได้รับการรับรอง เพื่อประกาศให้ทราบโดยทั่วกัน

(2.23) ใบรับรองและสิทธิในการใช้ตราสัญลักษณ์ที่กำหนดโดยองค์กรรับรองตามมาตรฐานนั้นให้มีกำหนดไม่เกิน 3 ปี แต่สามารถต่ออายุไปอีกกี่คราวก็ได้ แต่คราวละไม่เกิน 3 ปี

<u>หมวด 3 : การรับรองหลักสูตรฝึกอบรม</u>

(2.24) การยื่นขอรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคลนั้นให้ยื่นต่อสำนักงาน

(2.25) ผู้มีสิทธิในการขอยื่นรับรองหลักสูตรฝึกอบรมด้านการคุ้มครองข้อมูลส่วนบุคคล ได้แก่

- สถาบันการศึกษา
- สถาบันวิจัย
- สถาบันหรือหน่วยงานของรัฐที่มีวัตถุประสงค์เพื่อจัดฝึกอบรม
- บริษัทหรือห้างหุ้นส่วนนิติบุคคลที่มีหน่วยฝึกอบรมภายใน
- บริษัทหรือห้างหุ้นส่วนนิติบุคคลที่มีวัตถุประสงค์เพื่อจัดฝึกอบรมหรือพัฒนาบุคลากร

(2.26) หลักสูตรที่จะได้รับการรับรองนั้น จะต้องผ่านเกณฑ์การพิจารณา ได้แก่

- หลักสูตรครอบคลุมความรู้พื้นฐานด้านการคุ้มครองข้อมูลส่วนบุคคล กฎหมายคุ้มครองข้อมูลส่วนบุคคล และมาตรฐานทางอุตสาหกรรมที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเป้าหมายของหลักสูตร
- หลักสูตรมีการวิธีการประเมินผลหลังจากฝึกอบรมอย่างมีระบบ
- วิทยากรมีความรู้ความเชี่ยวชาญด้านการคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการหรือสำนักงานตามที่ได้รับมอบหมายจากคณะกรรมการเป็นผู้พิจารณารับรองหลักสูตร สำนักงานมีหน้าที่จัดทำรายชื่อหลักสูตรและสถาบันที่ได้รับการรับรอง

1.4 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง ความร่วมมือกับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
ในต่างประเทศและองค์การระหว่างประเทศ

สรุปสาระสำคัญของร่างประกาศฯ

(2.1) กำหนดนิยามคำว่า

"หน่วยงานผู้กำกับดูแล" หมายความว่า หน่วยงานราชการที่ทำหน้าที่ในการกำกับดูแลให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศ อาจมีลักษณะคล้ายคลึงหรือเทียบเท่ากับคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(2.2) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประสานงานกับหน่วยงานผู้กำกับดูแลในต่างประเทศเพื่อบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างมีประสิทธิภาพทั้งในลักษณะทวิภาคีและพหุภาคี โดยอาจกำหนดกรอบความร่วมมือในระยะยาวกับประเทศที่มีผู้ควบคุมข้อมูลส่วนบุคคลที่ให้ประมวลผลข้อมูลของเจ้าของข้อมูลส่วนบุคคลในประเทศไทยเป็นจำนวนมาก เพื่อให้สามารถแลกเปลี่ยนข้อมูลและขอความร่วมมือในการบังคับใช้กฎหมายได้อย่างรวดเร็ว

(2.3) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลดำเนินการเตรียมความพร้อมเพื่อให้รับการยอมรับว่ามีมาตรฐานในการคุ้มครองข้อมูลส่วนบุคคลอยู่ในระดับที่เพียงพอตามเงื่อนไขของการส่งข้อมูลข้ามพรมแดนในประเทศหรือกลุ่มประเทศที่มีมาตรฐานสูงและได้รับการยอมรับ โดยเฉพาะการพิจารณาความเพียงพอของระดับการคุ้มครองในสหภาพยุโรป (adequacy decision)

(2.4) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเข้าร่วมประชุมต่าง ๆ ระดับสากลของหน่วยงานผู้กำกับดูแลเพื่อร่วมกำหนดแนวปฏิบัติที่สอดคล้องกันในการบังคับใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อรับทราบถึงพัฒนาการของเทคโนโลยีที่เปลี่ยนแปลงไป และจัดทำรายงานเสนอแนะแนวทางการปรับปรุงกฎหมายต่อคณะรัฐมนตรีได้

(2.5) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเข้าร่วมในการสร้างมาตรฐานระหว่างประเทศที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้ได้ข้อมูลที่จำเป็นสำหรับการพัฒนาแนวปฏิบัติและพัฒนากฎหมายภายในประเทศ

(2.6) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเป็นตัวแทนของรัฐบาลหรือทำงานร่วมกับตัวแทนของรัฐบาลในอาเซียน ในกรอบความร่วมมือในระดับภูมิภาคและระดับสากล และในองค์การระหว่างประเทศที่เกี่ยวข้อง

(2.7) คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสนับสนุนหน่วยงานเอกชนในการเข้ารับการรับรองตามกรอบแนวปฏิบัติในการส่งข้อมูลส่วนบุคคลข้ามพรมแดนต่าง ๆ ทั้งในระดับภูมิภาคและระดับสากล