ประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง หลักเกณฑ์การให้ใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙

เพื่อเป็นการกำหนดหลักเกณฑ์เกี่ยวกับกระบวนการตรวจสอบและรับรองกระบวนการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรต่าง ๆ ที่จะขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล อันเป็นการพัฒนาและส่งเสริมมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้ทัดเทียมกับมาตรฐานสากล และเพื่อสร้างความเชื่อมั่นและความยั่งยืนทางข้อมูลส่วนบุคคล ในภาครัฐและภาคเอกชน จึงเห็นสมควรกำหนดหลักเกณฑ์การให้ใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อออกใบรับรองและเครื่องหมายรับรองให้กับหน่วยงานภาครัฐและภาคเอกชนที่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลตามที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

อาศัยอำนาจตามความในมาตรา ๔๔ (๓) มาตรา ๔๕ (๔) และมาตรา ๖๓ (๑) (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ประกอบมติคณะกรรมการกำกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ในการประชุมครั้งที่ ๒/๒๕๖๙ เมื่อวันที่ ๑๘ กุมภาพันธ์ ๒๕๖๙ เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์การให้ใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจะจัดให้มีการให้ใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อ

(๑) เพื่อสนับสนุนและส่งเสริมให้องค์กรต่าง ๆ พัฒนาและปรับปรุงระบบการดำเนินงานภายในองค์กรให้สอดคล้องกับหลักการตรวจเกณฑ์มาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และผลักดันให้มีการขอรับการตรวจประเมินตามเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

(๒) เพื่อสนับสนุนและส่งเสริมให้องค์กรต่าง ๆ ดำเนินการตามหลักความรับผิดชอบ (Accountability) และการบริหารจัดการข้อมูลส่วนบุคคลให้มีประสิทธิภาพ

(๓) เพื่อสนับสนุนและส่งเสริมให้องค์กรต่าง ๆ สร้างระบบรับรองที่เชื่อมโยงกับกลไกการรับรองระหว่างประเทศ (Cross-Border Recognition) ในอนาคต

ข้อ ๔ การตรวจประเมินตามเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อขอรับใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล อยู่ภายในขอบเขตดังต่อไปนี้

(๑) ผู้ยื่นคำขอต้องเป็นหน่วยงานของรัฐ หน่วยงานภาครัฐอื่น ๆ และนิติบุคคลภาคเอกชน

(๒) พิจารณาตรวจระบบการคุ้มครองข้อมูลส่วนบุคคลซึ่งครอบคลุมทั้งองค์กร

ข้อ ๕ ในการให้เครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล สำนักงานจะพิจารณาว่าผู้ยื่นคำขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ผ่านเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ครอบคลุมทั้ง ๔ กลุ่ม ๑๐ ด้าน จำนวน ๑๒๘ ข้อ ตามที่สำนักงานกำหนดไว้ตามเอกสารแนบท้ายประกาศฉบับนี้ ซึ่งประกอบด้วย

(๑) กลุ่มที่ ๑ นโยบายและการบริหารจัดการ (Policy and Governance) ประกอบด้วย

ด้านที่ ๑ องค์กรและการกำกับดูแล (Organization and Oversight)

ด้านที่ ๒ นโยบายและแนวปฏิบัติ (Policies and Procedures)

(๒) กลุ่มที่ ๒ การพัฒนาทรัพยากรบุคคลขององค์กร (Human Resource Development : HRD) ประกอบด้วย

ด้านที่ ๓ การอบรมและการสร้างความตระหนักรู้ (Training and awareness)

(๓) กลุ่มที่ ๓ กระบวนการและขั้นตอนการดำเนินงาน (Process and Procedure) ประกอบด้วย

ด้านที่ ๔ สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual Rights)

ด้านที่ ๕ การแจ้งวัตถุประสงค์และความโปร่งใส (Transparency)

ด้านที่ ๖ การจัดทำบันทึกรายการและฐานทางกฎหมาย (ROPA and Lawful Basis)

ด้านที่ ๗ ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Processing Agreement and Data Sharing Agreement)

ด้านที่ ๘ ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Risks and Data Protection Impact Assessment)

(๔) กลุ่มที่ ๔ ระบบเทคโนโลยีและความมั่นคงปลอดภัย และการแจ้งเหตุละเมิด (Technology Security and Breach Response) ประกอบด้วย

ด้านที่ ๙ มาตรการรักษาความมั่นคงปลอดภัย (Data Security)

ด้านที่ ๑๐ การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล (Breach Response)

ข้อ ๖ การดำเนินการตรวจประเมินการตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลเพื่อขอรับใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล จะดำเนินการตรวจประเมิน ดังต่อไปนี้

(๑) การตรวจประเมินโดยยึดจากเอกสารหลักฐาน และหลักฐานเชิงประจักษ์

(๒) การตรวจประเมินโดยพิจารณาตามข้อที่กฎหมายกำหนดให้ต้องปฏิบัติและข้อที่เป็นแนวปฏิบัติที่ดี

ข้อ ๗ สำนักงานจะพิจารณาให้เครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลกับผู้ยื่นคำขอ หากปรากฏว่าผ่านเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล โดยได้ปฏิบัติตามข้อที่กฎหมายกำหนดให้ต้องปฏิบัติและข้อที่เป็นแนวปฏิบัติที่ดี ซึ่งได้รับคะแนนตามเกณฑ์ดังต่อไปนี้

(๑) เมื่อผู้ยื่นคำขอได้ปฏิบัติตามข้อที่กฎหมายกำหนดให้ต้องปฏิบัติทุกข้อที่ถูกประเมิน หากได้รับคะแนนการประเมินไม่ต่ำกว่าร้อยละ ๘๐ แต่ไม่เกินร้อยละ ๘๙.๙ ของคะแนนตามหัวข้อที่ถูกประเมิน จะได้ใบรับรองระดับผ่านการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance Certificate)

(๒) เมื่อผู้ยื่นคำขอได้ปฏิบัติตามข้อที่กฎหมายกำหนดให้ต้องปฏิบัติทุกข้อที่ถูกประเมินและข้อที่เป็นแนวปฏิบัติที่ดี หากได้รับคะแนนการประเมินไม่ต่ำกว่าร้อยละ ๙๐ ของคะแนนตามหัวข้อที่ถูกประเมิน จะได้รับใบรับรองระดับได้รับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (PDPA Certificate) และเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (Certification mark)

ข้อ ๘ ลักษณะของใบรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล จะมีลักษณะเป็นโฮโลแกรมลายน้ำ เพื่อป้องกันการปลอมแปลงเอกสาร

ทั้งนี้ ใบรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล และเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามที่สำนักงานประกาศกำหนด

ข้อ ๙ การดำเนินการตามประกาศนี้ ไม่มีการเรียกเก็บค่าธรรมเนียมหรือค่าบริการ

ประกาศ ณ วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๙
พันตำรวจเอก สุรพงศ์ เปล่งขำ
เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
แนบท้ายประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง หลักเกณฑ์การให้ใบรับรองและเครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๙

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
กลุ่มที่ ๑ นโยบายและการบริหารจัดการ (Policy and Governance)			
ด้านที่ ๑ องค์การและการกำกับดูแล (Organization and Oversight)			
๑	องค์กรต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ตามมาตรา ๔๑ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตามที่กฎหมายกำหนด	๑.๒.๑	มาตรา ๔๑
๒	องค์กรต้องกำหนดอำนาจ หน้าที่ และจัดสรรทรัพยากรที่เพียงพอให้แก่ DPO เพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพและเป็นอิสระ	๑.๒.๒	มาตรา ๔๒
๓	กรณีที่องค์กรไม่เข้าข่ายที่ต้องแต่งตั้ง DPO ตามกฎหมาย องค์กรต้องมอบหมายบุคลากรที่มีความเหมาะสมรับผิดชอบงานด้านการคุ้มครองข้อมูลส่วนบุคคลแทน พร้อมจัดสรรทรัพยากรให้เพียงพอที่จะดำเนินการต่าง ๆ ให้สอดคล้องกับหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคล	๑.๒.๕	แนวปฏิบัติที่ดี
๔	องค์กรต้องกำหนดให้ DPO มีความเป็นอิสระและรายงานตรงต่อผู้บริหารระดับสูงโดยต้องไม่มีผลประโยชน์ทับซ้อนในการตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล	๑.๓.๓	มาตรา ๔๒ วรรคสาม
๕	องค์กรควรเปิดโอกาสให้ DPO ให้คำแนะนำแก่ผู้บริหารระดับสูงได้โดยตรง รวมถึงสามารถรายงานปัญหาในการปฏิบัติหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลได้อย่างอิสระ	๑.๓.๔	มาตรา ๔๒ วรรคสาม
๖	องค์กรต้องจัดบุคลากรและกระบวนการสนับสนุน DPO เพื่อช่วยในการจัดการและกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง	๑.๔.๑	มาตรา ๓๗, ๔๐
๗	องค์กรต้องจัดตั้งคณะทำงานหรือคณะกรรมการกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลที่ครอบคลุมถึงการดำเนินงาน การจัดทำตัวชี้วัด (KPI) รวมถึงการระบุปัญหาและความเสี่ยง สำหรับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร	๑.๕.๕	แนวปฏิบัติที่ดี
๘	ผู้บริหารระดับสูงขององค์กรต้องพิจารณาประเด็นด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูล และความเสี่ยงที่จัดทำโดยคณะทำงานของ DPO อย่างสม่ำเสมอ	๑.๕.๗	มาตรา ๔๑
๙	องค์กรต้องมีการรายงานปัญหาด้านการคุ้มครองข้อมูลส่วนบุคคลและการกำกับดูแลข้อมูลและความเสี่ยงใด ๆ ที่เกิดขึ้นไปยังคณะทำงานของ DPO	๑.๖.๔	มาตรา ๔๒
๑๐	องค์กรมีการพัฒนากระบวนการและเครื่องมือเพิ่มเติมเพื่อสนับสนุนการทำงานของ DPO และ DPO มีการตรวจสอบการดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายและประกาศที่เกี่ยวข้อง	-	มาตรา ๔๒

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๑๑	องค์กรต้องประกาศแต่งตั้ง DPO หรือ มอบหมายบุคลากรที่มีความเหมาะสมรับผิดชอบงานด้านการคุ้มครองข้อมูลส่วนบุคคล เป็นลายลักษณ์อักษร	-	มาตรา ๔๒
๑๒	องค์กรต้องเผยแพร่ข้อมูลช่องทางการติดต่อ DPO อย่างชัดเจน ผ่านช่องทางต่าง ๆ ขององค์กร เพื่อให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกรับทราบ	-	มาตรา ๔๑
๑๓	องค์กรต้องมีการตรวจสอบการปฏิบัติ ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ว่าสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล	-	แนวปฏิบัติที่ดี
ด้านที่ ๒ นโยบายและแนวปฏิบัติ (Policies and Procedures)			
๑๔	องค์กรต้องจัดทำนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล ที่ครอบคลุมการบริหารจัดการและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล	๒.๑.๒	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๕	องค์กรต้องจัดทำนโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล พร้อมระบุบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องอย่างชัดเจน	๒.๑.๔	มาตรา ๓๗, ๔๐
๑๖	องค์กรโดยผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายต้องกำหนดกระบวนการทบทวนและอนุมัตินโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล	๒.๒.๒	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๗	องค์กรต้องมีการทบทวนนโยบายและขั้นตอนปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างทันท่วงที เมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น มีการเปลี่ยนแปลงต่อองค์กร ที่สำคัญ ๆ การตัดสินใจของหน่วยงานกำกับดูแล หรือการเปลี่ยนแปลงในแนวทางปฏิบัติงานของหน่วยงานผู้กำกับดูแล	๒.๒.๓	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๘	องค์กรต้องแจ้งให้พนักงานทุกคนทราบถึงนโยบายและขั้นตอนปฏิบัติที่ปรับปรุงใหม่ เพื่อให้เข้าใจและปฏิบัติได้อย่างถูกต้อง	๒.๓.๒	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๙	องค์กรต้องจัดทำนโยบายและขั้นตอนเพื่อให้แน่ใจว่าประเด็นการคุ้มครองข้อมูลได้รับการพิจารณาเมื่อมีการออกแบบและดำเนินการระบบ บริการ ผลิตภัณฑ์ และแนวทางธุรกิจที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และข้อมูลส่วนบุคคลได้รับการคุ้มครองโดยค่าเริ่มต้น	๒.๔.๒	มาตรา ๓๗, ๔๐ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๒๐	องค์กรต้องกำหนดวิธีการปฏิบัติตามหลักการคุ้มครองข้อมูลส่วนบุคคล การป้องกันสิทธิ์ส่วนบุคคล ที่รวมถึงการจำกัดข้อมูลให้น้อยที่สุด (Data Minimization) การจำกัดวัตถุประสงค์การใช้งาน (Purpose Limitation) และการทำเป็นข้อมูลแฝง (Pseudonymization)	๒.๔.๓	มาตรา ๑๙, ๒๑, ๒๒, ๒๓, ๒๔, ๒๗ มาตรา ๓๐, ๓๑, ๓๓, ๓๔, ๓๕, ๓๖
๒๑	องค์กรมีการจัดทำแนวทางปฏิบัติและคู่มือในแต่ละกระบวนการย่อย เพื่อรองรับนโยบายด้านการคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้พนักงานและผู้ที่เกี่ยวข้องสามารถปฏิบัติได้อย่างถูกต้อง	-	มาตรา ๓๗ มาตรา ๔๐

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๒๒	องค์กรมีการทบทวนนโยบายและกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างน้อย ปีละ ๑ ครั้ง เพื่อให้มั่นใจว่ายังคงมีความถูกต้องและทันสมัย	-	มาตรา ๓๗, ๔๐
๒๓	องค์กรมีการวัดผลดำเนินการหลังจากประกาศนโยบายและแนวทางปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล โดยสะท้อนให้เห็นว่านโยบายดังกล่าวได้เข้ามาช่วยในการปกป้องข้อมูลส่วนบุคคลหรือลดความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้น (เช่น ลดช่องว่างที่เกิดขึ้นจากการดำเนินการไม่ครบถ้วนตามกฎหมาย เป็นต้น)	-	มาตรา ๓๗, ๔๐
กลุ่มที่ ๒ การพัฒนาทรัพยากรบุคคลขององค์กร (Human Resource Development: HRD) ด้านที่ ๓ การอบรมและการสร้างความตระหนักรู้ (Training and Awareness)			
๒๔	องค์กรต้องจัดทำแผนการสร้างความตระหนักรู้แก่พนักงานทุกคนที่อยู่ในกระบวนการปกป้องข้อมูลส่วนบุคคล เช่น การจัดการคำขอต่าง ๆ การแชร์ข้อมูล การรักษาความมั่นคงปลอดภัยของข้อมูล การละเมิดข้อมูล การบริหารจัดการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล	๓.๑.๒	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๒๕	องค์กรต้องจัดสรรทรัพยากรที่เพียงพอสำหรับการดำเนินการฝึกอบรมและกิจกรรมสร้างความตระหนักรู้ให้แก่บุคลากรทุกระดับ	๓.๑.๖	ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๒๖	องค์กรต้องมีการทบทวนหลักสูตรการอบรมเพื่อสร้างความตระหนักรู้ในการปฏิบัติงานให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และแนวทางการฝึกอบรมเพื่อให้มีความเหมาะสม ถูกต้อง และเป็นปัจจุบัน	๓.๑.๓	แนวปฏิบัติที่ดี
๒๗	องค์กรต้องจัดให้พนักงานเข้ารับการฝึกอบรมเพื่อเป็นการเตรียมความพร้อมก่อนการเข้าถึงข้อมูลส่วนบุคคล ภายในระยะเวลาที่เหมาะสม หรือได้รับการฝึกอบรมภายใน ๑ เดือน นับตั้งแต่วันที่เริ่มต้นปฏิบัติงาน	๓.๒.๒	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๒๘	องค์กรต้องจัดให้พนักงานเข้ารับการฝึกอบรมเพิ่มเติมในช่วงเวลาที่เหมาะสม	๓.๒.๔	มาตรา ๓๗ (๑) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๒๙	องค์กรต้องมีการประเมินผลหลังการอบรม เพื่อทดสอบความรู้ ความเข้าใจ และความพร้อมของพนักงาน โดยกำหนดเกณฑ์ขั้นต่ำในการผ่านการประเมิน	๓.๔.๑	แนวปฏิบัติที่ดี
๓๐	องค์กรได้จัดให้มีการทบทวนการอบรมและสร้างความตระหนักรู้ให้กับพนักงานในเรื่องการปกป้องข้อมูลส่วนบุคคลอยู่เป็นประจำ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของนโยบายและกระบวนการด้านการคุ้มครองข้อมูลส่วนบุคคล	-	ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
กลุ่มที่ ๓ กระบวนการและขั้นตอนการทำงาน (Process and Procedure) ด้านที่ ๔ สิทธิของเจ้าของข้อมูลส่วนบุคคล (Individual Right)			
๓๑	องค์กรต้องแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคลอย่างชัดเจน รวมถึงวิธีการใช้สิทธิตามที่กฎหมายกำหนด เช่น การเข้าถึง ขอสำเนา แก้ไข หรือลบข้อมูล	๔.๑.๑	มาตรา ๒๓

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๓๒	องค์กรต้องจัดทำนโยบายและขั้นตอนปฏิบัติในการจัดการคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมาย (โดยมีเอกสาร SOP Charter หรือขั้นตอนกำกับอย่างชัดเจน)	๔.๑.๓	มาตรา ๓๐, ๓๑, ๓๓, ๓๔, ๓๕, ๓๖
๓๓	ในกรณีที่องค์กรจะปฏิเสธการดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องจัดทำบันทึกการปฏิเสธคำขอดังกล่าวพร้อมด้วยเหตุผลไว้ในบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) และแจ้งเหตุผลของการปฏิเสธหรือข้อยกเว้นใด ๆ ไปยังเจ้าของข้อมูลส่วนบุคคลที่ขอใช้สิทธิ	๔.๔.๒	มาตรา ๓๐ วรรคสอง, วรรคสาม มาตรา ๓๑ วรรคสาม, ๓๒ วรรคสาม มาตรา ๓๖, ๓๙ (๗)
๓๔	องค์กรต้องจัดให้มีขั้นตอนและกระบวนการ ตามความเหมาะสม ได้สัดส่วนและสมเหตุสมผลในการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคลที่เก็บไว้ และหากจำเป็นก็สามารถทำการแก้ไขข้อมูลนั้นได้	๔.๖.๑	มาตรา ๓๕, ๓๖
๓๕	องค์กรต้องดำเนินการลบข้อมูลส่วนบุคคลจากระบบสำรองข้อมูล รวมถึงระบบที่ใช้งานจริงเมื่อจำเป็น และทำการชี้แจงพร้อมแจ้งวิธีการจัดการข้อมูลอย่างชัดเจนให้แก่เจ้าของข้อมูลส่วนบุคคล	๔.๗.๑	มาตรา ๒๒, ๒๗, ๓๓ ประกาศ กคส. เรื่อง หลักเกณฑ์ในการลบหรือทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ พ.ศ. ๒๕๖๗
๓๖	องค์กรสามารถส่งข้อมูลไปยังองค์กรอื่นด้วยวิธีการทางอิเล็กทรอนิกส์ได้โดยตรง ในกรณีที่เป็นไปได้และมีบุคคลร้องขอ	๔.๙.๒	มาตรา ๓๑
๓๗	องค์กรต้องแจ้งให้เจ้าของข้อมูลทราบถึงสิทธิในการร้องเรียนต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) หรือกรรมการผู้เชี่ยวชาญในประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice/Privacy Policy)	๔.๑๑.๒	มาตรา ๒๓ (๖)
๓๘	องค์กรมีการปรับปรุงนโยบายและกระบวนการการจัดการคำขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลโดยวิเคราะห์จากแนวโน้มคำขอต่าง ๆ	-	แนวปฏิบัติที่ดี
๓๙	องค์กรมีการแจ้งให้เจ้าของข้อมูลทราบถึงช่องทางในการขอเข้าถึงและขอสำเนาข้อมูลส่วนบุคคลตนเอง (Right to Access)	-	มาตรา ๒๓, ๓๐
๔๐	องค์กรสามารถระงับหรือจำกัดการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่เหมาะสมกับประเภทของการประมวลผลและระบบที่เกี่ยวข้อง เช่น การย้ายข้อมูลไปยังระบบอื่นชั่วคราวหรือลบออกจากเว็บไซต์	-	มาตรา ๓๒, ๓๔
๔๑	องค์กรมีการวัดผลการจัดการคำขอใช้สิทธิจากเจ้าของข้อมูลส่วนบุคคลได้ว่าสามารถจัดการได้ครบถ้วน	-	แนวปฏิบัติที่ดี
ด้านที่ ๕ การแจ้งวัตถุประสงค์และความโปร่งใส (Transparency)			
๔๒	องค์กรต้องมีการแจ้งรายละเอียดเกี่ยวกับข้อมูลการติดต่อที่เกี่ยวข้อง ได้แก่ (๑) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	๕.๑.๑	มาตรา ๒๓ (๕)

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
	(๒) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี) (๓) ข้อมูลชื่อและรายละเอียด รวมถึงสถานที่ติดต่อและวิธีการติดต่อของ DPO ของผู้ควบคุมข้อมูลส่วนบุคคล (ถ้ามี)		
๔๓	องค์กรต้องมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ฐานทางกฎหมายที่ใช้และอาจรวมถึงประโยชน์โดยชอบด้วยกฎหมายของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลนั้น	๕.๑.๒	มาตรา ๒๓ (๑) แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔๔	ในกรณีที่องค์กรได้ข้อมูลส่วนบุคคลมาจากแหล่งที่มาอื่น องค์กรต้องมีการแจ้งประเภทและแหล่งที่มาของข้อมูลส่วนบุคคลที่เก็บรวบรวม	๕.๑.๓	มาตรา ๒๕ แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔๕	องค์กรต้องมีการแจ้งประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย รวมถึงรายละเอียดการส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ	๕.๑.๔	มาตรา ๒๓ (๔) แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔๖	องค์กรต้องมีการแจ้งระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลไว้ ทั้งนี้หากไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน องค์กรต้องแจ้งระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวมข้อมูลส่วนบุคคล	๕.๑.๕	มาตรา ๒๓ (๓) แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔๗	องค์กรต้องมีการแจ้งสิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงสิทธิในการถอนความยินยอมของเจ้าของข้อมูลส่วนบุคคล (กรณีมีการขอความยินยอม) และสิทธิในการร้องเรียนในกรณีที่มีการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล	๕.๑.๖	มาตรา ๒๓ (๖) แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๔๘	องค์กรต้องมีการแจ้งให้เจ้าของข้อมูลส่วนบุคคลได้รับทราบถึงวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคล อาทิ ในขณะที่กรอกแบบฟอร์ม หรือจากกรณีที่อาจสังเกตเห็นได้เอง (or by observation) เช่น การถูกบันทึกภาพโดยระบบกล้องวงจรปิด หรือการถูกติดตามพฤติกรรมออนไลน์ เป็นต้น	๕.๒.๑	มาตรา ๒๓ แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๔๙	องค์กรต้องมีการทบทวนประกาศคุ้มครองข้อมูลส่วนบุคคลโดยพิจารณาเปรียบเทียบกับบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: ROPA) เพื่อให้แน่ใจว่าข้อมูลเป็นปัจจุบันและอธิบายสิ่งที่เกิดขึ้นกับข้อมูลส่วนบุคคลของบุคคลได้จริง	๕.๖.๒	แนวปฏิบัติที่ดี
๕๐	องค์กรต้องมีการดำเนินการทดสอบโดยผู้ใช้บริการเพื่อประเมินประสิทธิภาพของการแจ้งข้อมูลเกี่ยวกับวัตถุประสงค์และรายละเอียดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล	๕.๖.๔	แนวปฏิบัติที่ดี
๕๑	องค์กรต้องจัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคลที่มีความชัดเจนและง่ายสำหรับการเข้าถึงของบุคคลทั่วไป	๕.๗.๑	แนวปฏิบัติที่ดี
๕๒	องค์กรมีการปรับปรุงและพัฒนาประสิทธิภาพของแนวทางการแจ้ง Privacy Notice		แนวปฏิบัติที่ดี
ด้านที่ ๖ การจัดทำบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลและการกำหนดฐานทางกฎหมาย (ROPA and Lawful Basis)			
๕๓	องค์กรต้องจัดทำหรือทบทวนแผนผังข้อมูล (Data Mapping) เพื่อทำความเข้าใจการไหลเวียนและจุดที่มีการประมวลผลข้อมูลส่วนบุคคลภายในองค์กร	๖.๑.๑	แนวปฏิบัติที่ดี
๕๔	องค์กรต้องจัดทำ ROPA โดยมีรายการอย่างน้อยตามที่กำหนดไว้ในมาตรา ๓๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังต่อไปนี้ (๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม (๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท (๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล (๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล (๕) สิทธิและวิธีการเข้าถึงข้อมมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น (๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม (๗) การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด (หากมี) (๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)	๖.๓.๑	มาตรา ๓๙
๕๕	กรณีที่องค์กรมีผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) องค์กรต้องกำกับให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดทำ ROPA ในส่วนที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งให้แก่องค์กร ทั้งนี้ ROPA ต้องมีรายการที่บันทึกอย่างน้อยตามที่กฎหมายกำหนด	๖.๓.๒	มาตรา ๔๐ (๓) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการ

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
			ประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๕๖	องค์กรต้องกำหนดฐานทางกฎหมาย (Lawful Basis) ที่เหมาะสมและสอดคล้องกับวัตถุประสงค์ในการประมวลผลตาม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	๖.๕.๑	มาตรา ๒๔, ๒๖
๕๗	องค์กรต้องจัดทำประกาศการคุ้มครองข้อมูลส่วนบุคคลขององค์กร (Privacy Notice) อยู่ในรูปแบบที่เข้าถึงได้โดยง่ายและอ่านเข้าใจง่าย	๖.๖.๓	แนวทางการดำเนินการในการแจ้งวัตถุประสงค์และรายละเอียดในการเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๕๘	องค์กรต้องมีมาตรการที่เหมาะสมในการตรวจสอบว่าบุคคลดังกล่าวสามารถให้ความยินยอมด้วยตนเองได้ (ตรวจสอบอายุและความสามารถของบุคคล) ในกรณีที่ไม่สามารถให้ความยินยอมด้วยตนเองได้ ต้องมีมาตรการที่เหมาะสมในการได้รับความยินยอมจากผู้ใช้อำนาจปกครอง แล้วแต่กรณี	๖.๙.๒	แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๕๙	ในกรณีขอความยินยอมจากผู้เยาว์หรือบุคคลไร้ความสามารถหรือเสมือนไร้ความสามารถ องค์กรต้องมีมาตรการตรวจสอบที่เหมาะสมว่าบุคคลที่ให้ความยินยอมแทนเป็นผู้มีอำนาจกระทำการแทนเจ้าของข้อมูลส่วนบุคคลอย่างแท้จริง	๖.๙.๔	แนวทางการดำเนินการในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๖๐	องค์กรต้องมีการจัดทำ ROPA และมีการทบทวนกระบวนการและแก้ไข ROPA		มาตรา ๓๙
๖๑	องค์กรต้องทบทวนฐานทางกฎหมายที่ใช้ในการประมวลผลข้อมูลส่วนบุคคล	-	แนวปฏิบัติที่ดี
๖๒	ROPA ขององค์กรมีการระบุ “ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล”	-	มาตรา ๓๙
๖๓	ROPA ขององค์กรมีการระบุ “สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขในการเข้าถึงข้อมูล” เช่น ต้องผ่านการยืนยันตัวตนก่อนได้รับสิทธิ	-	มาตรา ๓๙
๖๔	ROPA ขององค์กรมีการระบุ “การใช้หรือเปิดเผยข้อมูลให้หน่วยงานอื่น” และมีเอกสารหรือ Dashboard แสดงจำนวนกิจกรรม จำนวนข้อมูลและจำนวนเจ้าของข้อมูลส่วนบุคคลขององค์กร เพื่อนำไปใช้เป็นตัวชี้วัดประสิทธิภาพของกระบวนการ	-	มาตรา ๓๙
๖๕	ROPA ขององค์กรมีการระบุ “การปฏิเสธคำขอหรือการคัดค้านการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด”	-	มาตรา ๓๙
๖๖	ROPA ขององค์กรมีการระบุ “คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย”	-	มาตรา ๓๙
๖๗	ในการขอความยินยอม องค์กรมีขั้นตอนการยืนยันตัวตนเจ้าของข้อมูลด้วย	-	มาตรา ๒๐
๖๘	องค์กรต้องแยกเอกสารขอความยินยอมออกจากสัญญาอย่างชัดเจน	-	มาตรา ๑๙
๖๙	องค์กรต้องแจ้งเจ้าของข้อมูลส่วนบุคคลเรื่องช่องทางการถอนความยินยอม	-	มาตรา ๑๙

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
ด้านที่ ๗	ข้อตกลงการประมวลผลข้อมูลส่วนบุคคลและข้อตกลงการแบ่งปันข้อมูลส่วนบุคคล (Data Sharing Agreement and Data Processing Agreement)		
๗๐	องค์กรต้องมีขั้นตอนตรวจสอบมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอของประเทศปลายทางหรือองค์กรระหว่างประเทศ ก่อนการโอนข้อมูลส่วนบุคคลไปต่างประเทศ โดยอ้างอิงหลักเกณฑ์ของคณะกรรมการ (Adequacy Decision) หรือเอกสารสนับสนุน (ถ้ามี)	๗.๓.๑	มาตรา ๒๘ ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาใช้บังคับ พ.ศ. ๒๕๖๖
๗๑	เมื่อมีการโอนข้อมูลส่วนบุคคลไปต่างประเทศ การส่งหรือโอนดังกล่าวมีความสอดคล้องกับข้อกำหนดของกฎหมายในกรณีอื่น ๆ ตามที่กำหนดในมาตรา ๒๘ หรือมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และต้องมีฐานทางกฎหมายที่เหมาะสมรองรับการโอน	๗.๓.๒	มาตรา ๒๘, ๒๙ ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศ ตามมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาใช้บังคับ พ.ศ.๕๖๖ ประกาศ กคส. เรื่อง หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปต่างประเทศ ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาใช้บังคับ ๒๕๖๖
๗๒	องค์กรต้องทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) กับผู้ประมวลผลข้อมูลส่วนบุคคลทุกรายที่เกี่ยวข้องกับองค์กร	๗.๔.๑	มาตรา ๔๐ วรรคสาม ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๗๓	องค์กรต้องจัดทำ DPA โดยมีเงื่อนไขอย่างน้อยตามที่มาตรา ๔๐ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนด ได้แก่ (๑) ดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งเท่านั้น (๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (๓) แจ้งให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น (๔) จัดทำและเก็บรักษา ROPA	๗.๔.๒	มาตรา ๔๐ วรรคหนึ่ง
๗๔	ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยทั้งด้านองค์กรและเทคนิค เช่น การเข้ารหัสข้อมูล การทำข้อมูลแฝง และการกู้คืนระบบ	๗.๕.๒	มาตรา ๔๐ วรรคสาม ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
			ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๗๕	DPA ต้องมีข้อกำหนดที่อนุญาตให้องค์กรดำเนินการตรวจสอบ (Right to Audit) เพื่อยืนยันว่าผู้ประมวลผลข้อมูลส่วนบุคคลปฏิบัติตามข้อกำหนดและเงื่อนไขตามสัญญาทั้งหมด	๗.๗.๑	แนวปฏิบัติที่ดี
๗๖	หากมีบุคคลที่สามจัดหาผลิตภัณฑ์หรือบริการเพื่อประมวลผลข้อมูลส่วนบุคคล องค์กรต้องเลือกบุคคลที่สามผู้ค้า (Supplier) ที่มีมาตรฐานในการปกป้องข้อมูลส่วนบุคคล โดยออกแบบผลิตภัณฑ์หรือบริการของตนโดยคำนึงถึงการปกป้องข้อมูล (Privacy by Design)	๗.๘.๑	แนวปฏิบัติที่ดี
๗๗	องค์กรต้องสามารถระบุผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ทั้งหมดภายในประเทศ ที่ส่งข้อมูลส่วนบุคคลมาให้องค์กร	-	แนวปฏิบัติที่ดี
๗๘	องค์กรต้องสามารถระบุผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ทั้งหมดภายในประเทศที่ดำเนินการประมวลผลข้อมูลส่วนบุคคล	-	มาตรา ๔๐
๗๙	องค์กรต้องจัดทำ DPA ให้ครอบคลุมผู้ประมวลผลข้อมูลส่วนบุคคล และมีเอกสารหรือ Dashboard ที่แสดงจำนวนข้อตกลง สัญญา สถานะ และระยะเวลาผูกพัน ของทุกคู่สัญญาเพื่อนำไปใช้เป็นตัวชี้วัดประสิทธิภาพของกระบวนการดำเนินงาน	-	แนวปฏิบัติที่ดี
๘๐	องค์กรได้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (การส่งข้อมูลในลักษณะ Binding Cooperate Rule)	-	มาตรา ๒๙
๘๑	องค์กรได้มีการส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (การส่งข้อมูลในลักษณะ Standard Contractual Clauses)	-	มาตรา ๒๙
๘๒	ในกรณีที่การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศและอยู่ในเครือกิจการหรือเครือธุรกิจเดียวกัน องค์กรมีนโยบายคุ้มครองข้อมูลส่วนบุคคลที่สามารถบังคับใช้ครอบคลุมไปถึงเครือกิจการหรือเครือธุรกิจเดียวกันได้ (ตามมาตรา ๒๙ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (BCR))	-	มาตรา ๒๙
๘๓	ในกรณีที่การส่งหรือโอนข้อมูลส่วนบุคคลไปต่างประเทศ องค์กรมีการกำหนดมาตราการที่เหมาะสมภายในสัญญากับผู้ประมวลผลข้อมูลส่วนบุคคล (ตามมาตรา ๒๙ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (SSC))	-	มาตรา ๒๙
๘๔	องค์กรต้องบันทึกการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูล ส่วนบุคคลรายอื่น ทั้งที่ได้รับความยินยอมและกรณียกเว้นตามกฎหมาย (ตามมาตรา ๒๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒)	-	มาตรา ๒๗
๘๕	องค์กรต้องจัดทำแบบฟอร์ม (Template) สำหรับบันทึกการโอนข้อมูลส่วนบุคคลไปต่างประเทศ ตามมาตรา ๒๘ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	-	มาตรา ๒๘
๘๖	องค์กรต้องจัดทำ Template ของนโยบายคุ้มครองข้อมูลส่วนบุคคลที่สามารถบังคับใช้ครอบคลุมไปถึงเครือกิจการหรือเครือธุรกิจเดียวกัน	-	มาตรา ๒๘

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๘๗	องค์กรต้องจัดทำ Template ของสัญญาที่ระบุมาตรการคุ้มครองข้อมูลส่วนบุคคล	-	มาตรา ๒๙
๘๘	องค์กรต้องจัดทำแบบฟอร์ม DPA	-	มาตรา ๔๐
ด้านที่ ๘ ความเสี่ยงและการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Risk and Data Protection Impact Assessment)			
๘๙	องค์กรต้องระบุและจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล โดยบันทึกไว้ในทะเบียนการจัดการความเสี่ยง (Risk Register) ที่ชัดเจน เชื่อมโยงกับแผนกหรือส่วนงานที่เกี่ยวข้อง และประเมินความเสี่ยงของทรัพย์สินสารสนเทศ	๘.๑.๒	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๙๐	องค์กรต้องมีขั้นตอนอย่างเป็นระบบ ในการระบุ บันทึก และจัดการความเสี่ยง เพื่อให้มั่นใจว่าเกี่ยวข้องกับทรัพย์สินสารสนเทศในทะเบียนควบคุมทรัพย์สินสารสนเทศ	๘.๑.๕	ประกาศ กคส. มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๙๑	องค์กรต้องจัดทำและทดสอบมาตรการลดความเสี่ยง ตามที่ได้ระบุไว้ใน Risk Categories เพื่อให้มั่นใจว่ามาตรการเหล่านั้นมีประสิทธิภาพ	๘.๑.๖	ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๙๒	องค์กรต้องมีการติดตามและทบทวนความเสี่ยงที่ระบุไว้ เพื่อประเมินว่าความเสี่ยงอยู่ในระดับที่องค์กรสามารถยอมรับได้ (Residual Risk)	-	มาตรา ๓๗
๙๓	องค์กรต้องกำหนดรอบการประเมินความเสี่ยงด้านข้อมูลส่วนบุคคลอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลง	-	มาตรา ๓๗
๙๔	องค์กรต้องวัดผลความมีประสิทธิภาพของกระบวนการจัดการความเสี่ยงด้านข้อมูลส่วนบุคคล โดยเปรียบเทียบผลลัพธ์กับระดับความเสี่ยงที่เหลือ (Residual Risk)	-	แนวปฏิบัติที่ดี
๙๕	องค์กรต้องปรับปรุงขั้นตอนและนำเทคโนโลยีใหม่มาใช้ เพื่อเพิ่มประสิทธิภาพในการระบุ จัดการ และลดความเสี่ยงด้านข้อมูลส่วนบุคคลให้สอดคล้องกับผลการประเมิน	-	แนวปฏิบัติที่ดี
กลุ่มที่ ๔ ระบบเทคโนโลยีและความมั่นคงปลอดภัย และการแจ้งเหตุละเมิด (Technology Security and Breach Response) ด้านที่ ๙ มาตรการรักษาความมั่นคงปลอดภัย (Data Security)			
๙๖	องค์กรต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลระหว่างการส่งหรือโอนข้อมูล เช่น การเข้ารหัส การใช้โปรโตคอลที่ปลอดภัย หรือ VPN	๙.๒.๓	มาตรา ๓๗ (๑) (๓) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๙๗	องค์กรต้องจัดให้มีการทบทวนคุณภาพของข้อมูลส่วนบุคคลอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องเหมาะสม และไม่ถูกเก็บเกินความจำเป็น	๙.๓.๑	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๙๘	องค์กรต้องกำหนดระยะเวลาการจัดเก็บข้อมูลส่วนบุคคลตามความต้องการทางธุรกิจ ซึ่งรวมถึงให้สอดคล้องกับกฎหมายระเบียบ ข้อบังคับ และหลักการที่เกี่ยวข้อง	๙.๔.๑	มาตรา ๒๒,๓๗ (๑) (๓),๒๒ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๙๙	องค์กรต้องทบทวนข้อมูลที่จัดเก็บไว้เพื่อระบุโอกาสในการลดการจัดเก็บข้อมูล และแปลงข้อมูลให้เป็นข้อมูลแฝง (Pseudonymization) หรือทำให้ข้อมูลเป็นนิรนาม (Anonymization)	๙.๔.๔	มาตรา ๒๒, ๓๗ (๓) ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๐	องค์กรต้องจัดทำบัญชีทรัพย์สินสารสนเทศ โดยบัญชีดังกล่าวได้รวมถึงเจ้าของทรัพย์สิน สถานที่จัดเก็บทรัพย์สิน ระยะเวลาการจัดเก็บ และมาตรการความมั่นคงปลอดภัย (เพื่อป้องกันทรัพย์สิน)	๙.๖.๑	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๑	องค์กรต้องประเมินความเสี่ยงของทรัพย์สินที่บันทึกไว้ในรายการบัญชีทรัพย์สินสารสนเทศ และดำเนินการตรวจสอบทางกายภาพเพื่อให้มั่นใจว่าทรัพย์สินมีความถูกต้องและครบถ้วน	๙.๖.๓	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๒	องค์กรต้องจัดให้มีการเก็บบันทึกการเข้าถึงระบบ (Access Logs) ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล	๙.๘.๔	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๓	องค์กรต้องจำกัดสิทธิการเข้าถึงข้อมูลส่วนบุคคล โดยใช้หลักการให้สิทธิการเข้าถึงให้น้อยที่สุดตามความจำเป็น (Principle of Least Privilege)	๙.๙.๑	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๔	องค์กรต้องกำหนดนโยบายการตั้งรหัสผ่านที่มีความซับซ้อนและปลอดภัย รวมถึงการจำกัดจำนวนครั้งที่ล็อกอินผิดพลาด	๙.๙.๒	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๕	องค์กรต้องมีมาตรการจัดการรหัสผ่านอย่างปลอดภัย เช่น การเปลี่ยนรหัสผ่านเริ่มต้น การห้ามแชร์รหัสผ่าน และการจัดเก็บอย่างมั่นคงปลอดภัย	๙.๙.๓	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๖	องค์กรต้องจัดให้มีมาตรการรักษาความปลอดภัยของพื้นที่ที่จำเป็น เช่น การควบคุมการเข้าออก การติดตั้งกล้องวงจรปิด หรือสัญญาณกันขโมย	๙.๑๑.๑	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๗	องค์กรต้องมีขั้นตอนการควบคุมการเข้าถึงของบุคคลภายนอก เช่น การแลกบัตร ลงนามเข้าออก ก่อนเข้าสู่พื้นที่ภายในที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	๙.๑๑.๒	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๐๘	องค์กรต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity) และแผนกู้คืนจากภัยพิบัติ (Disaster Recovery) ที่ครอบคลุมระบบ ข้อมูล และบริการที่สำคัญ	๙.๑๒.๑	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๑๐๙	องค์กรต้องมีการสำรองข้อมูลส่วนบุคคลอย่างสม่ำเสมอ และจัดเก็บสำเนาข้อมูลสำรองในสถานที่ที่ปลอดภัยนอกสถานที่ปฏิบัติงานหลัก	๙.๑๒.๒	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๐	องค์กรต้องทดสอบการเข้าถึงและการกู้คืนข้อมูลจากระบบสำรอง เพื่อให้มั่นใจในการเตรียมพร้อมสำหรับการกู้คืนระบบ	๙.๑๒.๔	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๑	องค์กรต้องมีนโยบายและกระบวนการตรวจสอบช่องโหว่ (Vulnerability Assessment) และปรับปรุงระบบ/เทคโนโลยีเพื่ออุดช่องโหว่อย่างต่อเนื่อง	-	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๑๒	องค์กรต้องจัดทำตัวชี้วัด (KPI) เพื่อติดตามและประเมินประสิทธิภาพของมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ และปรับปรุงมาตรการเมื่อยังไม่เป็นไปตามเป้าหมาย	-	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
ด้านที่ ๑๐ การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Breach Response)			
๑๑๓	องค์กรต้องกำหนดขั้นตอนการแจ้งเหตุด้านความมั่นคงปลอดภัยและการละเมิดข้อมูลส่วนบุคคลภายในองค์กร ให้พนักงานสามารถ รายงานต่อผู้ที่เกี่ยวข้องได้ทันที	๑๐.๑.๓	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๔	องค์กรต้องมีแผนรับมือเหตุด้านความมั่นคงปลอดภัยและเหตุละเมิดข้อมูลส่วนบุคคล โดยกำหนดบทบาทและความรับผิดชอบอย่างชัดเจน	๑๐.๑.๔	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๕	องค์กรต้องมีแบบฟอร์มบันทึกเหตุละเมิดข้อมูลส่วนบุคคล ที่ระบุประเภทของเหตุการณ์ ผลกระทบ และมาตรการแก้ไข/ป้องกัน	๑๐.๑.๕	มาตรา ๓๗ ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๖	องค์กรต้องมีขั้นตอนการประเมินผลกระทบจากเหตุละเมิดข้อมูลส่วนบุคคล โดยพิจารณาความรุนแรงและโอกาสที่อาจกระทบสิทธิและเสรีภาพของบุคคล	๑๐.๒.๑	มาตรา ๓๗ (๑) (๔)

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
			ประกาศ กคส. เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๗	องค์กรต้องแจ้งเหตุละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ ตามที่กฎหมายกำหนดโดยอาจแจ้งบางส่วนก่อนได้ หากยังไม่มีข้อมูลทั้งหมด	๑๐.๒.๒	มาตรา ๓๗ (๔) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๘	องค์กรต้องจัดทำรายละเอียดที่เพียงพอในการแจ้งเหตุละเมิดต่อ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เช่น ลักษณะของเหตุการณ์ ผลกระทบ และมาตรการแก้ไข	๑๐.๒.๓	มาตรา ๓๗ (๔) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๑๙	กรณีที่องค์กรพิจารณาว่าเหตุละเมิดไม่ก่อให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูล องค์กรต้องบันทึกเหตุผลในการไม่แจ้งเหตุไว้เป็นหลักฐาน	๑๐.๒.๔	มาตรา ๓๗ ประกาศ กคส. เรื่อง หลักการและวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๒๐	หากเหตุละเมิดมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล องค์กรต้องแจ้งเจ้าของข้อมูลให้ทราบโดยไม่ชักช้า	๑๐.๓.๑	มาตรา ๓๗ (๔) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕
๑๒๑	การแจ้งเจ้าของข้อมูลต้องทำอย่างชัดเจน กระชับ และใช้ภาษาที่เข้าใจง่าย พร้อมให้ข้อมูลที่จำเป็น เช่น ลักษณะของเหตุการณ์ ผลกระทบ และช่องทางติดต่อ	๑๐.๓.๒	มาตรา ๓๗ (๔) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๒๒	การแจ้งเจ้าของข้อมูลต้องรวมแนวทางการเยียวยา และมาตรการป้องกันที่องค์กรได้ดำเนินการหรือจะดำเนินการต่อไป	๑๐.๓.๓	มาตรา ๓๗ (๔) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๒๓	องค์กรต้องให้คำแนะนำแก่เจ้าของข้อมูลส่วนบุคคล เกี่ยวกับวิธีการป้องกันความเสียหายจากผลกระทบที่อาจเกิดจากเหตุละเมิด	๑๐.๓.๔	มาตรา ๓๗ (๔) ประกาศ กคส. เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๒๔	องค์กรต้องตรวจสอบข้อเท็จจริงของเหตุละเมิด และจัดทำรายงานสรุปผลการดำเนินงาน พร้อมจัดทำ Dashboard ติดตามจำนวนเหตุการณ์	-	ประกาศ กคส. เรื่อง หลักการและวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๒๕	แบบบันทึกเหตุละเมิดข้อมูลส่วนบุคคลต้องมีรายละเอียดครบถ้วน ได้แก่ ลักษณะของเหตุการณ์ ผลกระทบ มาตรการแก้ไข และการเยียวยา	-	มาตรา ๓๗ ประกาศ กคส. เรื่อง หลักการและวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

ข้อ	เกณฑ์การตรวจมาตรฐาน	ICO	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
๑๒๖	องค์กรต้องจัดทำตัวชี้วัด (KPI) เพื่อติดตามประสิทธิภาพของกระบวนการจัดการเหตุละเมิด และใช้ผลการประเมินเพื่อปรับปรุงอย่างต่อเนื่อง	-	มาตรา ๓๗
๑๒๗	องค์กรต้องมีการปรับปรุงและพัฒนาแผนรับมือเหตุด้านความมั่นคงปลอดภัยและเหตุละเมิดข้อมูลส่วนบุคคลเป็นประจำ เพื่อให้สอดคล้องกับสถานการณ์จริง	-	มาตรา ๓๗ ประกาศ กคส. เรื่อง หลักการและวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
๑๒๘	องค์กรต้องวิเคราะห์แนวโน้มของเหตุละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น และนำผลการวิเคราะห์มาใช้ในการออกมาตรการเชิงป้องกันไม่ให้เกิดเหตุซ้ำ	-	มาตรา ๓๗ ประกาศ กคส. เรื่อง หลักการและวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕