

ประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง วิธีการและเงื่อนไขในการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

พ.ศ. ๒๕๖๙

เพื่อพัฒนาและส่งเสริมมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้ทัดเทียมกับมาตรฐานสากล และเพื่อสร้างความเชื่อมั่นและความยั่งยืนทางข้อมูลส่วนบุคคล ในภาครัฐและภาคเอกชน สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลจึงจัดให้มีการตรวจสอบและรับรองกระบวนการคุ้มครองข้อมูลส่วนบุคคลภายในองค์กรต่าง ๆ เพื่อขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล ซึ่งกระบวนการดังกล่าวต้องสอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ จึงเห็นสมควรกำหนดวิธีการและเงื่อนไขในการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์เพื่อรับรองหน่วยงานภาครัฐและภาคเอกชนตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายอื่นที่เกี่ยวข้อง

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

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

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“เลขที่การ” หมายความว่า เลขที่การคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

“คณะทำงาน” หมายความว่า คณะทำงานกลั่นกรองการตรวจประเมินมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

“พนักงานตรวจประเมิน” หมายความว่า พนักงานหรือลูกจ้างของสำนักงานที่ได้รับการแต่งตั้งหรือมอบหมายให้ทำการตรวจประเมินตามเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานกำหนด

“ผู้ยื่นคำขอ” หมายความว่า หน่วยงานของรัฐ หน่วยงานภาครัฐอื่น ๆ หรือนิติบุคคล ภาคเอกชน

“การตรวจ” หมายความว่า การตรวจประเมินตามเกณฑ์การตรวจมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานกำหนด

“เครื่องหมาย” หมายความว่า เครื่องหมายรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

“ใบรับรองมาตรฐาน” หมายความว่า เอกสารหรือหลักฐานแสดงการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลซึ่งออกโดยสำนักงาน เพื่อแสดงว่าผู้ยื่นคำข้อมีมาตรการการคุ้มครองข้อมูลส่วนบุคคลที่เป็นไปตามมาตรฐานที่สำนักงานประกาศกำหนด

“ค่าบริการ” หมายความว่า เงินที่สำนักงาน เรียกเก็บในการตรวจ หรือค่าบริการอื่น ๆ ที่สำนักงานประกาศกำหนด

ข้อ ๔ ให้มีคณะกรรมการหนึ่ง เรียกว่า “คณะกรรมการกึ่งการตรวจประเมินมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล” ซึ่งแต่งตั้งโดยเลขาธิการ ประกอบด้วย

(๑) รองเลขาธิการ ด้านส่งเสริมและกำกับดูแล เป็นประธานคณะกรรมการ

(๒) คณะทำงานผู้ทรงคุณวุฒิ จำนวน ๕ คน แต่งตั้งจากผู้มีความรู้ความสามารถและความเชี่ยวชาญ ประกอบด้วย ผู้แทนจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จำนวน ๑ คน ผู้แทนจากสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม จำนวน ๑ คน ผู้แทนจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จำนวน ๑ คน ผู้แทนจากสภาอุตสาหกรรมแห่งประเทศไทย จำนวน ๑ คน และผู้แทนจากสภาหอการค้าแห่งประเทศไทย จำนวน ๑ คน

(๓) ผู้อำนวยการสำนักส่งเสริมการคุ้มครองข้อมูลส่วนบุคคล เป็นคณะกรรมการ

ให้ผู้อำนวยการฝ่ายตรวจสอบและรับรอง เป็นเลขานุการ และให้พนักงานฝ่ายตรวจสอบและรับรองจำนวน ๒ คน เป็นผู้ช่วยเลขานุการ

ข้อ ๕ คณะทำงานมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ตรวจสอบและรับรองผลการตรวจตามที่พนักงานตรวจประเมินเสนอ

(๒) ปฏิบัติหน้าที่อื่น ๆ ที่เกี่ยวข้องกับการตรวจตามที่ได้รับมอบหมายจากเลขาธิการ

ข้อ ๖ เกณฑ์การพิจารณาให้เป็นไปตามที่สำนักงานกำหนด

ข้อ ๗ ผู้ยื่นคำขอต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ หรือหน่วยงานภาครัฐอื่น ๆ ต้องเป็นหน่วยงานที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนดให้ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามที่ประกาศกำหนด หน่วยงานของรัฐระดับกรม หรือเทียบเท่า

กรณีเป็นนิติบุคคลภาคเอกชน ต้องเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายไทยและมีสำนักงานตั้งอยู่ในราชอาณาจักร หรือหากเป็นนิติบุคคลที่จัดตั้งขึ้นตามกฎหมายต่างประเทศ ต้องมีสำนักงานสาขาตั้งอยู่ในราชอาณาจักร หรือต้องแต่งตั้งตัวแทนผู้มีอำนาจในการดำเนินการ

(๒) ผ่านการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Maturity Model) โดยมีคะแนนในระดับ ๕

(๓) ไม่เคยถูกปฏิเสธคำขอรับรองมาตรฐาน ภายในระยะเวลา ๔๕ วัน ก่อนวันยื่นคำขอ

(๔) ไม่เคยถูกเพิกถอนใบรับรองมาตรฐาน ภายในระยะเวลา ๑ ปี ก่อนวันยื่นคำขอ

(๕) ในกรณีที่ผู้ยื่นคำขอเคยต้องคำพิพากษาตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ต้องเป็นกรณีที่ได้ปฏิบัติตามคำพิพากษาดังกล่าวโดยครบถ้วน และพ้นระยะเวลาไม่น้อยกว่า ๒ ปี นับแต่วันที่ได้ปฏิบัติตามนั้นแล้ว

ข้อ ๘ ให้ผู้ยื่นคำขอจัดทำแบบการขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล พร้อมทั้งแนบเอกสารหลักฐานตามที่กำหนด เพื่อตรวจสอบคุณสมบัติเบื้องต้นตามช่องทางที่สำนักงานกำหนด หรือผ่านระบบอิเล็กทรอนิกส์ ประกอบด้วย

(๑) เอกสารจัดตั้งหน่วยงาน

กรณีผู้ยื่นคำขอเป็นหน่วยงานรัฐให้แนบพระราชบัญญัติ พระราชกฤษฎีกา หรือ เอกสารอื่นใดซึ่งแสดงการจัดตั้งหน่วยงาน

กรณีผู้ยื่นคำขอเป็นนิติบุคคลภาคเอกชนให้แนบสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล ซึ่งออกไว้ไม่เกิน ๓ เดือน นับแต่วันที่ยื่นคำขอ

(๒) กรณีการมอบอำนาจให้ผู้อื่นดำเนินการแทน ให้แนบหนังสือมอบอำนาจ พร้อมปิดอากรแสตมป์ ตามที่กฎหมายกำหนด พร้อมสำเนาบัตรประชาชนหรือเอกสารอื่นใด ของทั้งผู้มอบอำนาจและผู้รับมอบอำนาจ โดยลงนามรับรองสำเนาถูกต้องด้วย

(๓) กรณีผู้ยื่นคำขอเคยมีลักษณะต้องห้ามให้แนบเอกสารที่แสดงว่า ผู้ยื่นคำขอพ้นจากระยะเวลาต้องห้ามแล้ว

ข้อ ๙ เมื่อสำนักงานได้รับเอกสารตามข้อ ๘ เรียบร้อยแล้ว ให้ดำเนินการ ดังต่อไปนี้

(๑) พนักงานตรวจประเมินดำเนินการตรวจสอบเอกสาร

(ก) กรณีเอกสารถูกต้องครบถ้วนให้แจ้งผู้ยื่นคำขอชำระค่าบริการ ภายในระยะเวลา ๗ วัน นับแต่ที่ได้รับแจ้ง

(ข) กรณีเอกสารไม่ถูกต้องครบถ้วนให้แจ้งผู้ยื่นคำขอจัดส่งเอกสารเพิ่มเติม ภายในระยะเวลา ๗ วัน นับแต่ที่ได้รับแจ้ง และเมื่อผู้ยื่นคำขอจัดส่งเอกสารเพิ่มเติมแล้วให้ดำเนินการตามข้อ ๙

(๑) (ก) แต่หากไม่จัดส่งเอกสารเพิ่มเติม หรือจัดส่งแล้วแต่เอกสารไม่ถูกต้อง คำขอจะถูกยกเลิก โดยไม่ต้องแจ้งล่วงหน้า

(๒) ผู้ยื่นคำขอจัดทำแบบประเมินตามเกณฑ์ที่สำนักงานกำหนด พร้อมแนบเอกสารประกอบผ่านระบบอิเล็กทรอนิกส์ และชำระค่าบริการการตรวจ

(๓) เมื่อผู้ยื่นคำขอชำระค่าบริการแล้ว ให้พนักงานตรวจประเมินดำเนินการตรวจ

(ก) กรณีผู้ยื่นคำขอผ่านเกณฑ์ที่สำนักงานกำหนด ให้เสนอผลการตรวจต่อคณะกรรมการ เพื่อพิจารณาตรวจทานและรับรองผลการตรวจก่อนเสนอเลขานุการเพื่อพิจารณารับรองมาตรฐาน

(ข) กรณีผู้ยื่นคำขอไม่ผ่านเกณฑ์ที่สำนักงานกำหนด ให้แจ้งผู้ยื่นคำขอปรับปรุงแก้ไข ให้ถูกต้องและครบถ้วนทุกเรื่องในคราวเดียวกัน ภายในระยะเวลา ๑๕ วัน นับแต่วันที่ได้รับแจ้ง เมื่อปรับปรุงแก้ไขแล้วให้พนักงานตรวจอีกครั้งหนึ่ง กรณีที่ผู้ยื่นคำขอผ่านเกณฑ์ที่สำนักงานกำหนดแล้ว ให้ดำเนินการตามข้อ ๙ (๓) (ก) แต่หากไม่ปรับปรุงแก้ไขหรือปรับปรุงแก้ไขแล้วแต่ยังไม่ผ่านเกณฑ์ที่สำนักงานกำหนด ให้แจ้งผลการพิจารณาไปยังผู้ยื่นคำขอทราบ

ในการตรวจตามข้อ ๙ (๓) สำนักงานอาจมอบหมายพนักงานตรวจประเมินดำเนินการตรวจจากเอกสาร หรืออาจตรวจ ณ สถานที่ทำการของผู้ยื่นคำขอ แล้วแต่กรณี และต้องดำเนินการตรวจให้แล้วเสร็จภายในระยะเวลา ๖๐ วัน นับแต่วันที่เริ่มดำเนินการตรวจ

ข้อ ๑๐ เมื่อเลขอาชีวการพิจารณารับรองมาตรฐานแล้ว ให้พนักงานตรวจประเมินแจ้งผู้ยื่นคำขอทราบและให้ชำระค่าบริการการออกใบรับรองมาตรฐานหรือเครื่องหมาย และต้องชำระค่าบริการภายในระยะเวลา ๑๕ วัน นับแต่วันที่ได้รับแจ้ง หากผู้ยื่นคำขอไม่ชำระค่าบริการภายในกำหนดระยะเวลาดังกล่าว สำนักงานจะยกเลิกการออกใบรับรองมาตรฐานหรือเครื่องหมาย โดยไม่ต้องแจ้งล่วงหน้า

ข้อ ๑๑ การชำระค่าบริการตามประกาศฉบับนี้ ให้ชำระผ่านระบบธนาคารอิเล็กทรอนิกส์ (e-Banking) ของธนาคารกรุงไทย หรือช่องทางที่สำนักงานกำหนด

อัตราค่าบริการให้เป็นไปตามที่สำนักงานประกาศกำหนด

ข้อ ๑๒ สำนักงานจะดำเนินการออกใบรับรองมาตรฐานหรือเครื่องหมาย ภายหลังจากที่ได้รับหลักฐานการชำระค่าบริการการออกใบรับรองมาตรฐานจากผู้ยื่นคำขอ และจะจัดส่งผ่านช่องทางที่ผู้ยื่นคำขอระบุไว้ หรือผ่านช่องทางที่สำนักงานกำหนด

หลักเกณฑ์การตรวจและการให้เครื่องหมาย ให้เป็นไปตามที่สำนักงานประกาศกำหนด

ข้อ ๑๓ กระบวนการตรวจและออกใบรับรองมาตรฐานหรือเครื่องหมาย สำนักงานจะดำเนินการให้แล้วเสร็จภายในระยะเวลา ๑๘๐ วัน นับแต่วันที่ผู้ยื่นคำขอได้ยื่นคำขอต่อสำนักงาน

ในกรณีมีความจำเป็น สำนักงานอาจขยายกรอบระยะเวลาการดำเนินการได้อีกหนึ่งครั้ง ไม่เกิน ๓๐ วัน นับแต่ระยะเวลา ๑๘๐ วัน สิ้นสุดลง

ข้อ ๑๔ ใบรับรองมาตรฐานและเครื่องหมายมีอายุ ๓ ปี นับแต่วันที่ออกใบรับรอง เว้นแต่จะมีการแก้ไขเปลี่ยนแปลง หรือเพิกถอนโดยสำนักงาน

ภายหลังจากที่ผู้ยื่นคำขอได้รับใบรับรองมาตรฐานหรือเครื่องหมายแล้ว เมื่อครบกำหนด ๑ ปี สำนักงานอาจดำเนินการติดตามตรวจสอบผลการรับรองมาตรฐาน

ข้อ ๑๕ ผู้ยื่นคำขออาจต่ออายุใบรับรองมาตรฐานหรือเครื่องหมายก่อนครบกำหนดระยะเวลา ๓ ปี โดยยื่นความประสงค์ขอต่ออายุล่วงหน้าแต่ไม่เกิน ๖ เดือน ก่อนที่จะสิ้นสุดอายุการรับรอง หรือเมื่ออายุการรับรองสิ้นสุดลงแล้วแต่ไม่เกิน ๖ เดือน

ข้อ ๑๖ สำนักงานจะจัดให้มีการประกาศรายชื่อผู้ยื่นคำขอที่ได้รับใบรับรองมาตรฐานหรือเครื่องหมายไว้บนเว็บไซต์ของสำนักงาน

ข้อ ๑๗ แบบการขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามที่สำนักงาน ประกาศกำหนด

ประกาศ ณ วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๙

พันตำรวจเอก สุรพงศ์ เปล่งขำ

เลขาธิการคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

แบบการขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
แบบท้ายประกาศสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
เรื่อง วิธีการและเงื่อนไขในการรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๙

เลขที่คำขอ.....



แบบการขอรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

๑. ข้อมูลผู้ยื่นคำขอ

ชื่อหน่วยงาน

ประเภทหน่วยงาน หน่วยงานภาครัฐ หน่วยงานภาคเอกชน (แนบเอกสารจัดตั้งหน่วยงาน)

ผ่านการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล (Privacy Maturity Model) โดยมีคะแนนในระดับ ๕

ไม่เคยถูกปฏิเสธการรับรองมาตรฐาน ภายใน ๔๕ วัน ก่อนวันยื่นคำขอ

ไม่เคยถูกเพิกถอนการรับรองมาตรฐาน ภายใน ๑ ปี ก่อนการยื่นคำขอครั้งล่าสุด

การต้องโทษตามคำพิพากษา (เลือกเพียง ๑ ข้อ)

ไม่เคยต้องคำพิพากษามาตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

เคยต้องคำพิพากษามาตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล แต่ได้ปฏิบัติตามคำพิพากษาดังกล่าว โดยครบถ้วน และพ้นระยะเวลาไม่น้อยกว่า ๒ ปี นับแต่วันที่ได้ปฏิบัติตามนั้นแล้ว (แนบเอกสารหลักฐาน)

๒. ข้อมูลผู้ประสาน

ชื่อ-นามสกุล ตำแหน่ง

เลขประจำตัวประชาชน -

อีเมล
.....

๓. การยื่นรับรองมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล

หน่วยงานดำเนินการเอง

หน่วยงานมอบอำนาจให้ผู้อื่นดำเนินการแทน (แนบเอกสารประกอบการมอบอำนาจ)

ข้าพเจ้าขอรับรองว่าข้อมูลและเอกสารหลักฐานประกอบการพิจารณาข้างต้น ถูกต้อง ครบถ้วน และเป็นความจริง
ทุกประการ ทั้งนี้ พร้อมอำนวยความสะดวกแก่เจ้าหน้าที่ในการดำเนินการตรวจสอบเอกสาร

ลงชื่อ.....

(.....)

ผู้ยื่นคำขอ

ลงวันที่.....