ประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ที่ ธพส. ๑/๒๕๖๘

เรื่อง หลักเกณฑ์และระยะเวลาการตรวจประเมินประจำปีและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการสำหรับประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

ตามที่ประกาศหลักเกณฑ์ในการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต ในส่วนของหลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการกำหนดให้ภายหลังจากเริ่มประกอบธุรกิจ ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการและรายงานต่อสำนักงานตามหลักเกณฑ์และระยะเวลาที่สำนักงานกำหนด ดังนั้น เพื่อประโยชน์ของผู้รับใบอนุญาตในการปฏิบัติตามข้อกำหนดเกี่ยวกับหลักเกณฑ์ภายหลังจากเริ่มประกอบธุรกิจ จึงเป็นการสมควรกำหนดหลักเกณฑ์และระยะเวลาการตรวจประเมินประจำปีและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการสำหรับประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๒๓ และมาตรา ๒๔ แห่งพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕ ประกอบกับข้อ ๒๑ ของข้อกำหนดท้ายประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่ ธพส. ๑/๒๕๖๖ ฉบับที่ ๕ หลักเกณฑ์เกี่ยวกับมาตรฐานการให้บริการตามประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่ ธพส. ๑/๒๕๖๖ ลงวันที่ ๒๖ พฤษภาคม พ.ศ. ๒๕๖๖ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศกำหนดหลักเกณฑ์และระยะเวลาการตรวจประเมินประจำปีและจัดทำรายงานผลการตรวจประเมินระบบการให้บริการสำหรับประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลไว้ ดังนี้

ข้อ ๑ ในประกาศนี้

“ผู้รับใบอนุญาต” หมายความว่า บุคคลที่ได้รับใบอนุญาตให้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลตามกฎหมายว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

“ระบบการให้บริการ” หมายความว่า ระบบและเทคโนโลยีที่ใช้สำหรับการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่มีลักษณะเป็นบริการที่ต้องได้รับใบอนุญาต และหมายรวมถึงระบบงานที่เกี่ยวข้องกับการประกอบธุรกิจบริการดังกล่าวด้วย

“สำนักงาน” หมายความว่า สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ข้อ ๒ ภายหลังจากเริ่มประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ผู้รับใบอนุญาตต้องจัดให้มีการตรวจประเมินระบบการให้บริการตามหลักเกณฑ์ในการควบคุมดูแล

การประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต อย่างน้อยปีละ ๑ ครั้ง ประกอบด้วย หลักเกณฑ์ในเรื่อง ต่อไปนี้

(๑) หลักเกณฑ์การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของระบบการให้บริการ

(๒) หลักเกณฑ์การควบคุมดูแลและป้องกันการทุจริตหรือการฉ้อโกงจากการใช้งานระบบ

(๓) หลักเกณฑ์ตามลักษณะของการให้บริการ

การกำหนดขอบเขตในการตรวจประเมินระบบให้บริการตามวรรคหนึ่ง ต้องครอบคลุมการปฏิบัติงาน กระบวนการทำงาน และระบบงานด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยง และการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเพียงพอ ทั้งนี้ ผู้รับใบอนุญาตยังคงต้องปฏิบัติให้สอดคล้องตามหลักเกณฑ์ทั้งหมดเกี่ยวกับมาตรฐานการให้บริการในส่วนที่เกี่ยวกับการตรวจประเมินระบบการให้บริการ ภายใต้หลักเกณฑ์การควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต

ข้อ ๓ การตรวจประเมินระบบการให้บริการตามข้อ ๒ ให้ผู้รับใบอนุญาตกำหนดแผนงานการตรวจประเมินให้สอดคล้องตามระดับความเสี่ยงสำหรับธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยให้ผู้รับใบอนุญาตดำเนินการประเมินความเสี่ยงตามแบบประเมินความเสี่ยงประจำปีที่สำนักงานกำหนด

ผลการประเมินระดับความเสี่ยงตามวรรคหนึ่ง ต้องผ่านการพิจารณาจากผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการประเมินก่อนนำส่งต่อสำนักงาน

ข้อ ๔ การกำหนดแผนงานการตรวจประเมินตามข้อ ๓ ให้ผู้รับใบอนุญาตพิจารณาตามระดับความเสี่ยง ดังนี้

(๑) กรณีผลการประเมินอยู่ในความเสี่ยงระดับต่ำ ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการให้ครอบคลุมข้อกำหนดทั้งหมดของหลักเกณฑ์ตามข้อ ๒ แบบปีเว้นปี โดยปีที่มีการตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมดให้ตรวจประเมินให้ครบทุกข้อกำหนดภายในปีนั้น และปีที่ไม่ได้มีการตรวจประเมินแบบครอบคลุมข้อกำหนดทั้งหมด ให้ดำเนินการตรวจประเมินเฉพาะบางข้อกำหนดแต่ต้องครบตามหลักเกณฑ์ในข้อ ๒

(๒) กรณีผลการประเมินอยู่ในความเสี่ยงระดับปานกลางหรือสูง ให้กำหนดแผนงานและดำเนินการตรวจประเมินระบบการให้บริการให้ครอบคลุมข้อกำหนดทั้งหมดของหลักเกณฑ์ตามข้อ ๒ ทุกปี

การรายงานผลการตรวจประเมินระบบการให้บริการตามวรรคหนึ่ง ให้ใช้แบบรายงานผลการตรวจประเมินประจำปีที่สำนักงานกำหนด และต้องผ่านการพิจารณาจากผู้บริหารระดับสูง คณะกรรมการ หรือบุคลากรที่ได้รับมอบหมายรับรองผลการตรวจประเมินระบบการให้บริการก่อนนำส่งต่อสำนักงาน

ข้อ ๕ ให้ผู้รับใบอนุญาตจัดส่งผลการประเมินความเสี่ยงประจำปี และรายงานผลการตรวจประเมินระบบการให้บริการต่อสำนักงานภายในวันที่ ๓๑ มีนาคมของปีถัดไป โดยวิธีการทางอิเล็กทรอนิกส์ตามช่องทางที่สำนักงานกำหนด โดยถือว่าสำนักงานได้รับตามวันและเวลาที่ข้อมูลได้เข้าสู่ระบบอิเล็กทรอนิกส์ของสำนักงาน ทั้งนี้ หากเป็นการนำส่งนอกวันและเวลาทำการของสำนักงาน ถือว่าสำนักงานได้รับข้อมูลดังกล่าวในวันและเวลาทำการถัดไป

ข้อ ๖ ในการตรวจประเมินระบบการให้บริการตามข้อ ๒ และการประเมินระดับความเสี่ยงตามข้อ ๓ สำหรับปี พ.ศ. ๒๕๖๘ ให้ผู้รับใบอนุญาตดำเนินการ ดังต่อไปนี้

(๑) ดำเนินการประเมินและจัดส่งผลการประเมินระดับความเสี่ยงต่อสำนักงาน ภายในวันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๘

(๒) กำหนดแผนงานการตรวจประเมินและดำเนินการตรวจประเมินระบบการให้บริการและนำส่งรายงานผลการตรวจประเมินต่อสำนักงาน ภายในวันที่ ๓๑ มีนาคมของปีถัดจากปีที่ประกาศฉบับนี้ใช้บังคับ

ข้อ ๗ ประกาศนี้ให้ใช้บังคับแก่ผู้ประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาตซึ่งได้ประกอบธุรกิจบริการอยู่ในวันก่อนวันที่พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ต้องได้รับใบอนุญาต พ.ศ. ๒๕๖๕ ที่ได้ยื่นคำขอรับใบอนุญาตและอยู่ระหว่างการพิจารณาออกใบอนุญาตด้วย

ข้อ ๘ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๘ เป็นต้นไป

ประกาศ ณ วันที่ ๒๗ กุมภาพันธ์ พ.ศ. ๒๕๖๘
ชัยชนะ มิตรพันธ์
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์