สรุปหลักการและสาระสำคัญของร่างพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล พ.ศ. ....

หลักการ

ด้วยบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเป็นบริการที่มีความสำคัญต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยเป็นขั้นตอนสำคัญในการทำธุรกรรมในระบบเศรษฐกิจ และช่วยสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ จึงมีความจำเป็นต้องมีการควบคุมดูแลการประกอบธุรกิจบริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยการกำหนดลักษณะหรือประเภทของการประกอบธุรกิจบริการที่ต้องได้รับใบอนุญาตและหลักเกณฑ์ในการประกอบธุรกิจบริการเพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและปลอดภัย ป้องกันความเสียหายต่อสาธารณชน ตลอดจนเสริมสร้างความน่าเชื่อถือและการยอมรับในระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล จึงมีความจำเป็นต้องตราพระราชกฤษฎีกานี้

พระราชกฤษฎีกานี้ มิได้เป็นการจำกัดให้นำเทคโนโลยีใดเทคโนโลยีหนึ่งมาใช้เป็นการเฉพาะหรือกีดกันความมีผลทางกฎหมายของการพิสูจน์และยืนยันตัวตนทางดิจิทัลด้วยเทคโนโลยีใดเทคโนโลยีหนึ่ง

วันมีผลใช้บังคับ

มีผลใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยแปดสิบวันนับแต่วันประกาศในราชกิจจานุเบกษา (มาตรา ๒)

สาระสำคัญ

๑. หลักการทั่วไป

๔.๑ กำหนดให้การพิสูจน์และยืนยันตัวตนทางดิจิทัล ประกอบด้วยอย่างน้อย ๓ กระบวนการดังต่อไปนี้ (มาตรา ๙)

(๑) มีการพิสูจน์ตัวตน

(๒) มีการออกสิ่งที่ใช้ยืนยันตัวตน

(๓) มีการยืนยันตัวตน

๔.๒ ให้ข้อสันนิษฐานทางกฎหมายของการพิสูจน์และยืนยันตัวตนทางดิจิทัล ในกรณีดังต่อไปนี้

(๑) เมื่อบุคคลได้รับการพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่อยู่ภายใต้การควบคุมดูแลตามพระราชกฤษฎีกานี้ และระบบฯ นั้นได้ดำเนินการตามเงื่อนไขเกี่ยวกับความน่าเชื่อถือสอดคล้องกับมาตรฐานที่คณะกรรมการประกาศกำหนด ให้สันนิษฐานว่าบุคคลที่ได้รับการพิสูจน์และยืนยันตัวตนเป็นบุคคลนั้นจริง

(๒) การพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ใช้เพื่อประโยชน์ภายในกิจการของบุคคลหรือนิติบุคคลนั้น ถ้าระบบฯ นั้น ได้ดำเนินการตามเงื่อนไขเกี่ยวกับความน่าเชื่อถือสอดคล้องกับมาตรฐานที่คณะกรรมการประกาศกำหนด และได้มีการตรวจรับรองโดยหน่วยตรวจรับรองที่สำนักงานประกาศกำหนดแล้ว ให้สันนิษฐานว่าบุคคลที่ได้รับการพิสูจน์และยืนยันตัวตนเป็นบุคคลนั้นจริง

๔.๓ กำหนดหลักการเพื่อป้องกันการผูกขาดทางการค้า (มาตรา ๑๐)

๒. บริการเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่อยู่ภายใต้การกำกับดูแล (มาตรา ๑๑)
ประกอบด้วยธุรกิจบริการ ๔ ประเภท ที่ต้องได้รับอนุญาต

(๑) บริการพิสูจน์ตัวตน (Identity Proofing Service)

หน้าที่: บริการที่ประกอบด้วยกระบวนการรวบรวมและตรวจสอบข้อมูลเกี่ยวกับไอเดนทิตี และการตรวจสอบความเชื่อมโยงระหว่างบุคคลกับข้อมูลเกี่ยวกับไอเดนทิตีนั้น

- เช่น รวบรวมคุณลักษณะที่เกี่ยวข้องกับตัวบุคคล/ตรวจสอบความถูกต้องของบัตรประชาชน/ตรวจสอบใบหน้า

(๒) บริการสิ่งที่ใช้ยืนยันตัวตน (Authenticator Management Service)

หน้าที่: เชื่อมโยงไอเดนทิตีของบุคคลที่ผ่านการพิสูจน์ตัวตนแล้วเข้ากับสิ่งที่ใช้ยืนยันตัวตน และการบริหารจัดการสิ่งที่ใช้ยืนยันตัวตนนั้น

- เช่น สร้าง/ออก Username และ Password หรือ Mobile Authenticator ให้กับผู้ใช้บริการที่ได้ผ่านการพิสูจน์ตัวตนมาแล้ว เพื่อให้ผู้ใช้บริการนำไปใช้ในการยืนยันตัวตน

(๓) บริการยืนยันตัวตน (Authentication Service)

หน้าที่: ตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เพื่อยืนยันไอเดนทิตีของบุคคลที่ใช้สิ่งที่ใช้ยืนยันตัวตนนั้น

- เช่น เมื่อผู้ใช้ทำการยืนยันตัวตนโดยใช้ Password หรือ Mobile Authenticator แล้ว ผู้ให้บริการดังกล่าวจะดำเนินการตรวจสอบว่าผู้ที่ใช้ Password หรือ Mobile Authenticator ดังกล่าว เป็นบุคคลนั้นจริงหรือไม่

(๔) บริการแลกเปลี่ยนข้อมูลเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital Identity Platform Service)

หน้าที่: บริการเครือข่ายหรือระบบเพื่อการเชื่อมโยงและแลกเปลี่ยนข้อมูลเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล ทั้งนี้ ไม่รวมถึงบุคคลที่เป็นสื่อกลาง

- เช่น Platform ที่เชื่อมโยงผู้ประกอบธุรกิจบริการทั้ง ๓ ประเภทและผู้ที่เกี่ยวข้องเข้าด้วยกัน

๓. บริการเกี่ยวกับการพิสูจน์และยืนยันตัวตนทางดิจิทัล ที่ได้รับการยกเว้น (มาตรา ๕)

(๑) บริการออกใบรับรองเพื่อสนับสนุนลายมือชื่ออิเล็กทรอนิกส์ (Certification Authority: CA) ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๒) บริการเกี่ยวกับระบบพิสูจน์และยืนยันตัวตนทางดิจิทัลที่บุคคลหรือนิติบุคคลใช้เพื่อประโยชน์ภายในกิจการของบุคคลหรือนิติบุคคลนั้น โดยไม่ได้ให้บริการแก่บุคคลภายนอก

(๓) บริการพิสูจน์ตัวตนที่ไม่ต้องมีการตรวจสอบหลักฐานแสดงตน และการตรวจสอบเพื่อระบุตัวบุคคล (Identity Assurance Level หรือ IAL Level 1)

(๔) บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่ดำเนินการโดยหน่วยงานของรัฐ แต่ไม่รวมถึงรัฐวิสาหกิจ

๔. กลไกการกำกับดูแล

๔.๑ ก่อนได้รับอนุญาต

กำหนดหลักเกณฑ์เกี่ยวกับการยื่นขอรับใบอนุญาต ประเภทของนิติบุคคล คุณสมบัติและลักษณะต้องห้ามของกรรมการ และเอกสารที่ต้องยื่นประกอบการขอรับใบอนุญาต รวมถึงกระบวนการในการพิจารณาอนุญาตของคณะกรรมการหรือสำนักงาน

๔.๒ ระหว่างประกอบธุรกิจ

กำหนดหลักเกณฑ์ที่ผู้ประกอบธุรกิจบริการจะต้องดำเนินการในระหว่างการประกอบธุรกิจเพื่อให้ระบบมีความมั่นคงปลอดภัยและมีประสิทธิภาพ เช่น กำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจ กำหนดมาตรการบริหารจัดการความเสี่ยงของระบบ มาตรการรักษาความมั่นคงปลอดภัยของระบบและการตรวจสอบ การเก็บรักษาและการเปิดเผยข้อมูลส่วนบุคคล กำหนดหลักเกณฑ์ เงื่อนไข และมาตรฐานการให้บริการ การเปิดเผยข้อมูลเกี่ยวกับการให้บริการ การคุ้มครองผู้ใช้บริการและมาตรการชดใช้หรือเยียวยาผู้ได้รับความเสียหายจากการประกอบธุรกิจ ฯลฯ

๔.๓ หลังเลิกประกอบธุรกิจ

กำหนดหลักเกณฑ์ในกรณีที่ประสงค์จะการเลิกประกอบธุรกิจ เช่น ต้องแจ้งให้สำนักงานทราบล่วงหน้าไม่น้อยกว่าหกสิบวัน รวมถึงกำหนดหลักเกณฑ์ที่ต้องดำเนินการเกี่ยวกับการจัดการข้อมูลและการคุ้มครองประโยชน์ของผู้ใช้บริการหลังจากเลิกประกอบธุรกิจ ตลอดจนการโอนบริการไปยังผู้ประกอบธุรกิจรายอื่นเพื่อความต่อเนื่องในการใช้งานของผู้รับบริการ

๕. กำหนดเหตุแห่งการปรับ และ การเพิกถอนใบอนุญาต

กำหนดมาตรการในกรณีที่ผู้ประกอบธุรกิจไม่ปฏิบัติตามหลักเกณฑ์ที่กำหนด รวมไปถึงการลงโทษปรับ ตลอดจนหลักเกณฑ์เกี่ยวกับการเพิกถอนใบอนุญาตในกรณีต่าง ๆ

๖. รองรับ Regulatory Sandbox

กำหนดให้มี Regulatory Sandbox เพื่อรองรับในกรณีที่มีการนำนวัตกรรมหรือเทคโนโลยีมาใช้ในการให้บริการเกี่ยวกับระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลซึ่งยังไม่มีกฎระเบียบรองรับหรือเสี่ยงจะขัดหรือแย้งกับกฎระเบียบหรือหลักเกณฑ์ของสำนักงาน รวมไปถึงกรณีที่อาจส่งผลกระทบต่อการรักษาความมั่นคงทางการเงินและการพาณิชย์ ความน่าเชื่อถือหรือการยอมรับในระบบข้อมูลอิเล็กทรอนิกส์ หรืออาจก่อให้เกิดความเสียหายต่อสาธารณชนหรือผู้บริโภค