ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวทางการใช้บริการคลาวด์

พ.ศ. ๒๕๖๒

โดยที่ในปัจจุบันการให้บริการธุรกรรมทางอิเล็กทรอนิกส์มีการใช้บริการคลาวด์ (Cloud Computing) อย่างแพร่หลาย อาศัยจากการให้บริการคลาวด์จากผู้ประกอบการรายอื่น เพื่อให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการคลาวด์ มีความมั่นคงปลอดภัย ความน่าเชื่อถือ และมาตรฐานในการให้บริการซึ่งเป็นที่ยอมรับในระดับสากล

อาศัยอำนาจตามความในมาตรา ๓๗ (๗) แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดแนวทางการใช้บริการคลาวด์ ดังต่อไปนี้

ข้อ ๑ กรณีที่ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์มีการใช้บริการคลาวด์ ไม่ว่าจะเป็นการดำเนินการโดยผู้ให้บริการคลาวด์อื่นหรือไม่ก็ตาม เพื่อวางมาตรฐานในการให้บริการและเป็นข้อมูลอ้างอิง การประมวลผลดังกล่าวอาจดำเนินการตามแนวทางการใช้บริการที่กำหนดตามเอกสารแนบท้ายประกาศนี้ได้

ข้อ ๒ การนำแนวทางการใช้บริการคลาวด์ตามที่กำหนดในข้อ ๑ มาใช้ในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์นั้น ให้คำนึงถึงหลักเกณฑ์ขั้นพื้นฐานซึ่งเป็นมาตรการขั้นต่ำในการลดความเสี่ยงจากภัยคุกคามของบริการ โดยจะต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ รวมทั้งปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยอย่างเหมาะสมและสอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงไป

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๒

พิเชฐ ดุรงคเวโรจน์

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

แนบท้าย ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. ๒๕๖๒

---

๑. บทนำ

เนื่องจากปัจจุบันผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ทั้งภาครัฐและภาคเอกชน มีการให้บริการผ่านช่องทางออนไลน์อย่างแพร่หลาย โดยใช้บริการคลาวด์ (Cloud Computing) เป็นเทคโนโลยีพื้นฐานในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อส่งเสริมและพัฒนาการให้บริการแบบคลาวด์ที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย ความน่าเชื่อถือตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวทางการใช้บริการคลาวด์

แนวทางการใช้บริการคลาวด์ฉบับนี้มีวัตถุประสงค์เพื่อให้ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ใช้อ้างอิงประกอบการพิจารณาบริการของผู้ให้บริการคลาวด์ โดยคำนึงถึงหลักเกณฑ์ขั้นพื้นฐาน ซึ่งเป็นมาตรการขั้นต่ำในการลดความเสี่ยงจากภัยคุกคาม โดยจะต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ รวมทั้งปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

๒. คำนิยาม

“บริการคลาวด์ (Cloud Computing)” หมายถึง บริการประมวลผลด้วยการใช้ทรัพยากรคอมพิวเตอร์ร่วมกันผ่านเครือข่ายตามความต้องการได้อย่างสะดวก โดยมีรูปแบบ ดังนี้

๑. การให้บริการโครงสร้างพื้นฐานหลัก (Infrastructure as a Service: IaaS) ประกอบด้วย ระบบประมวลผลข้อมูล ระบบการจัดเก็บข้อมูล ระบบเครือข่าย และทรัพยากรพื้นฐานอื่นๆ ที่เกี่ยวข้องกับระบบประมวลผล ผู้ใช้บริการสามารถใช้งานซอฟต์แวร์บนโครงสร้างพื้นฐานและทรัพยากรที่ผู้ให้บริการจัดหาให้ได้อย่างมีประสิทธิภาพ โดยไม่ต้องบริหารจัดการโครงสร้างพื้นฐานที่จำเป็นด้วยตนเอง หรือ

๒. การให้บริการแพลตฟอร์ม (Platform as a Service: PaaS) ประกอบด้วย ระบบโปรแกรมงานคอมพิวเตอร์ ระบบฐานข้อมูล และระบบจัดการหรืองานบริการจากคอมพิวเตอร์ ผู้ใช้บริการสามารถพัฒนา ติดตั้ง และปรับแต่งซอฟต์แวร์ได้ โดยไม่ต้องบริหารจัดการในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐาน เครือข่าย ระบบปฏิบัติการ และระบบจัดการฐานข้อมูล หรือ

๓. การให้บริการซอฟต์แวร์ (Software as a Service: SaaS) ผู้ให้บริการจัดเตรียมซอฟต์แวร์สำเร็จรูปแล้ว โดยผู้ใช้บริการสามารถกำหนดค่าความต้องการ พารามิเตอร์ ปริมาณหน่วยประมวลผลข้อมูล หน่วยเก็บข้อมูล และบริหารจัดการเพื่อให้ได้บริการตามวัตถุประสงค์ หรือ

๔. การให้บริการใดที่เป็นการรวมกันของสองบริการขึ้นไป จาก ข้อ ๑ ถึง ๓ หรือ

๕. การให้บริการอื่นที่ประกาศกำหนด

“ผู้ให้บริการ” หมายถึง ผู้ให้บริการคลาวด์

“ผู้ใช้บริการ” หมายถึง ผู้ให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่มีการใช้บริการคลาวด์

๓. หลักเกณฑ์การให้บริการ

เพื่อให้บริการธุรกรรมทางอิเล็กทรอนิกส์ที่ใช้บริการคลาวด์ มีความมั่นคงปลอดภัย เชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล ผู้ใช้บริการควรพิจารณาข้อมูลที่เกี่ยวข้องกับบริการตามแนวทางที่กำหนด ดังนี้

๓.๑ นโยบายและแนวทางปฏิบัติขององค์กร

ผู้ใช้บริการควรพิจารณานโยบายและแนวปฏิบัติในองค์กรของผู้ให้บริการที่เกี่ยวข้องกับกระบวนการทำงาน มาตรการป้องกันทางกายภาพ และมาตรการป้องกันทางเทคนิค ซึ่งมีสาระสำคัญดังต่อไปนี้

๓.๑.๑ กระบวนการทำงาน

นโยบายและแนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยสารสนเทศ นโยบายการพัฒนาทรัพยากรบุคลากรให้มีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล นโยบายการจัดการสินทรัพย์ นโยบายการจัดการเปลี่ยนแปลง นโยบายการบริหารความเสี่ยง กระบวนการตอบสนองต่อเหตุการณ์ฉุกเฉิน การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน การติดตามดูแลการให้บริการ กระบวนการจ้างช่วงต่อสัญญา และการปฏิบัติอื่นใดตามที่กฎหมายกำหนด

๓.๑.๒ มาตรการป้องกันทางกายภาพ

มาตรการป้องกันเพื่อรักษาความมั่นคงปลอดภัยแก่สินทรัพย์ทางกายภาพ เช่น การกำหนดควบคุมพื้นที่ ความปลอดภัยในพื้นที่หวงห้าม การควบคุมการเข้าออกพื้นที่

๓.๑.๓ มาตรการป้องกันทางเทคนิค

มาตรการป้องกันสำหรับความมั่นคงปลอดภัยและความน่าเชื่อถือทางเทคนิค เช่น โครงสร้างระบบเสมือน (Virtual Infrastructure) และสภาพแวดล้อมของระบบ การควบคุมการเข้าถึง การยืนยันตัวตน การตรวจสอบสิทธิของผู้ใช้งาน ระบบความมั่นคงปลอดภัยเครือข่าย การคุ้มครองข้อมูล การเข้ารหัส การวิเคราะห์ ออกแบบและพัฒนาระบบตามวัฏจักรการพัฒนาระบบงาน (System Development Life Cycle : SDLC) แนวทางการรักษาความปลอดภัยในการพัฒนาซอฟต์แวร์และ Application Programming Interface (API) และแนวทางในการรักษาความปลอดภัยในการจ้างบุคคลภายนอก (Outsourcing)

๓.๒ ประสิทธิภาพการให้บริการ

ผู้ใช้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับสภาพพร้อมใช้งาน ระยะเวลาการตอบสนอง ความสามารถรองรับปริมาณงาน บริการสนับสนุน และกระบวนการยุติสัญญา ซึ่งมีสาระสำคัญดังต่อไปนี้

๓.๒.๑ สภาพพร้อมใช้งาน (Availability)

ความพร้อมใช้งานของบริการครอบคลุมร้อยละของเวลาที่พร้อมให้บริการต่อปี (Uptime) เช่น ไม่ต่ำกว่าร้อยละ ๙๙.๙ เป็นต้น

๓.๒.๒ ระยะเวลาการตอบสนอง (Response Time)

ระยะเวลาการตอบสนองต่อเหตุการณ์ ซึ่งเป็นระยะเวลานับแต่ผู้ใช้บริการแจ้งความประสงค์และผู้ให้บริการได้ดำเนินการต่อความประสงค์นั้น โดยระยะเวลาการตอบสนองเป็นหลักการพิจารณาที่สำคัญของผู้ใช้บริการ การตอบสนองล่าช้ากว่ากำหนดอาจส่งผลให้เกิดความเสียหาย

๓.๒.๓ ความสามารถรองรับปริมาณงาน (Capacity)

จำนวนปริมาณการเชื่อมต่อสูงสุดพร้อมกัน (Maximum Simultaneous Connections) ปริมาณการใช้งานของผู้ใช้บริการพร้อมกัน (Maximum Simultaneous Users) ปริมาณความจุของระบบที่รองรับการใช้งาน (Resource Capacity) และปริมาณงาน (Throughput)

๓.๒.๔ การบริการสนับสนุน

ช่องทางและช่วงเวลาที่ผู้ใช้บริการสามารถแจ้งปัญหา หรือติดต่อสอบถามจากผู้ให้บริการ เช่น การกำหนดให้ผู้ใช้บริการสามารถติดต่อผู้ให้บริการได้ตลอด ๒๔ ชั่วโมง และระยะเวลาในการแก้ไขปัญหาการใช้งานตั้งแต่เริ่มต้นจนปัญหานั้นสิ้นสุด

๓.๒.๕ กระบวนการยุติสัญญา

แนวทางกระบวนการยุติสัญญาล่วงหน้า กรณีผู้ใช้บริการ หรือผู้ให้บริการต้องการยุติสัญญา โดยควรกำหนดแนวทางการดำเนินการ เช่น ระยะเวลาสำหรับการเข้าถึงข้อมูลของผู้ใช้บริการ และระยะเวลาการเก็บรักษาข้อมูลของผู้ให้บริการ และการกำหนดแผนการเลิกใช้บริการ (Exit Plan)

๓.๓ การรักษาความมั่นคงปลอดภัย

ผู้ใช้บริการควรพิจารณามาตรการ การรักษาความมั่นคงปลอดภัยในระบบสารสนเทศในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับความน่าเชื่อถือของบริการ การพิสูจน์ตัวตนและการอนุญาต การเข้ารหัส การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัย การจัดการช่องโหว่ และธรรมาภิบาล ซึ่งมีสาระสำคัญดังต่อไปนี้

๓.๓.๑ ความน่าเชื่อถือของบริการ

การควบคุมความมั่นคงปลอดภัย การบริหารจัดการความต่อเนื่องทางธุรกิจ และการจัดให้มีระบบฉุกเฉินสำรอง โดยอ้างอิงตามมาตรฐานสากล เช่น

- **ISO**
  - ☐ ISO/IEC 20000-1 (Information Technology Service Management System: ITSMS)
  - ☐ ISO/IEC 27001 (Information Security Management System)
  - ☐ ISO/IEC 27017 (Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for Cloud Service)
  - ☐ ISO/IEC 27018 (Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)
- **CSA STAR**
  - ☐ CSA STAR Self-Assessment
  - ☐ CSA STAR Certification
  - ☐ CSA STAR Attestation
- **NIST**
  - ☐ SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

๓.๓.๒ การพิสูจน์ตัวตนและการอนุญาต

กระบวนการพิสูจน์ตัวตนเพื่อเป็นการตรวจสอบความมีตัวตนของผู้มีสิทธิ์ในการเข้าใช้งาน ระยะเวลาเวลาในการดำเนินการเพิ่มหรือถอนสิทธิ์ผู้ใช้บริการที่เหมาะสม การป้องกันการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์ การกำหนดระดับการยืนยันตัวตน (Authentication Level) และการควบคุมการเข้าถึงการใช้งานจากบุคคลภายนอกที่สนับสนุนการให้บริการ (Outsourcing)

๓.๓.๓ การเข้ารหัส

การเข้ารหัสในการแปลงข้อมูลเพื่อปกปิดข้อมูลป้องกันการเข้าถึง การแก้ไข และการใช้งานโดยไม่ได้รับอนุญาต การกำหนดการเข้ารหัสให้สอดคล้องกับประเภทข้อมูล (Data Classification) และจัดให้มีนโยบายการควบคุมกุญแจสำหรับการเข้ารหัส (Key Access Control Policy) ตามความเหมาะสม

๓.๓.๔ การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย

การจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล เริ่มตั้งแต่กระบวนการตรวจพบเหตุการณ์ การรายงานเหตุการณ์ การประเมิน การตอบสนอง การแก้ปัญหา และการเรียนรู้จากเหตุการณ์ความปลอดภัยที่เกิดขึ้น

๓.๓.๕ การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ

การบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการและการใช้บริการเพื่อให้สามารถตรวจสอบข้อมูลย้อนหลังได้

๓.๓.๖ การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัย

การตรวจสอบกระบวนการทำงานและความปลอดภัยอย่างเป็นระบบอ้างอิงมาตรฐานสากล มีความเป็นอิสระ มีขั้นตอนการทำงานที่มีเอกสารหลักฐาน และกำหนดสิทธิของผู้ตรวจสอบภายในผู้ตรวจสอบภายนอก เป็นประจำอย่างสม่ำเสมอ รวมถึงการกำหนดให้หน่วยงานของรัฐที่มีอำนาจตามกฎหมายสามารถเข้าตรวจสอบได้

๓.๓.๗ การจัดการช่องโหว่

การตรวจสอบ ประเมิน และบริหารจัดการช่องโหว่ หรือจุดเสี่ยงในระบบ กระบวนการรักษาความปลอดภัยของระบบ มาตรการรักษาความมั่งคงปลอดภัยไซเบอร์ การควบคุมภายใน หรือการใช้งานที่อาจถูกนำไปใช้หรือถูกเรียกใช้โดยภัยคุกคาม กรณีบริการที่มีความสำคัญและมีความจำเป็นอาจมีการทดสอบระบบความปลอดภัย Vulnerability Assessments และ Penetration Testing โดยจะต้องดำเนินการตามมาตรการ และวิธีการที่เหมาะสมเพื่อลดความเสี่ยงในการเกิดความเสียหาย

๓.๓.๘ ธรรมาภิบาล

การแจ้งให้ผู้ใช้บริการทราบล่วงหน้าในระยะเวลาที่เหมาะสม กรณีการเปลี่ยนแปลงการให้บริการอันเนื่องมาจากการปรับปรุง อัพเดตซอฟต์แวร์ ที่อาจส่งผลกระทบต่อกระบวนการทำงาน ช่องทางการให้บริการหรือรายละเอียดในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

๓.๔ การจัดการข้อมูล

ผู้ใช้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับการจัดประเภทข้อมูล การสำรองข้อมูลและการเรียกคืนข้อมูล วงจรชีวิตของข้อมูล และการโอนย้ายข้อมูล ซึ่งมีสาระสำคัญดังต่อไปนี้

๓.๔.๑ การจัดประเภทข้อมูล

ประเภทความเป็นเจ้าของข้อมูล ได้แก่ ข้อมูลของผู้ใช้บริการ ข้อมูลของผู้ให้บริการ และข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการ (Derived Data) ผู้ให้บริการควรจัดให้มีนโยบายที่เกี่ยวข้องกับการใช้ข้อมูลของผู้ใช้บริการ การกำหนดขอบเขตและแนวปฏิบัติ รวมถึงกำหนดสิทธิ์ในการตรวจสอบข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการ

๓.๔.๒ การสำรองข้อมูล และการเรียกคืนข้อมูล

การสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน โดยกำหนดระยะเวลา ความถี่ในการดำเนินการ วิธีการ และการเก็บรักษาที่เหมาะสม ในกรณีที่ข้อมูลปัจจุบันถูกทำลายหรือได้รับความเสียหายส่งผลทำให้ไม่สามารถใช้งานได้ ผู้ให้บริการควรดำเนินการเรียกคืนข้อมูลเพื่อให้เกิดความพร้อมในการใช้งานตามที่ระบุไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

๓.๔.๓ วงจรชีวิตของข้อมูล

นโยบายและแนวปฏิบัติที่เหมาะสมในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ ครอบคลุม กระบวนการสร้าง การเก็บรักษา การใช้ การเปิดเผย และการทำลายข้อมูล

๓.๔.๔ การโอนย้ายข้อมูล

นโยบายและแนวปฏิบัติในการส่งออกข้อมูล โดยกำหนดรูปแบบ หรือกระบวนการส่งออก ตามความเหมาะสมในกรณียุติข้อตกลงการให้บริการ

๓.๕ การคุ้มครองข้อมูลส่วนบุคคล

ผู้ใช้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับแนวปฏิบัติตามมาตรฐานสากลในการคุ้มครองข้อมูลส่วนบุคคล การระบุวัตถุประสงค์การเก็บข้อมูล การเก็บรักษาข้อมูลเท่าที่จำเป็น การใช้ เก็บรักษาและการเปิดเผย ความโปร่งใสและการแจ้งเตือน ความรับผิดชอบต่อข้อมูล สถานที่จัดเก็บข้อมูล และการอำนวยความสะดวกในการเข้าถึงข้อมูล ซึ่งมีสาระสำคัญดังต่อไปนี้

๓.๕.๑ แนวปฏิบัติตามมาตรฐานสากล

นโยบาย แนวทางปฏิบัติ มาตรการ หรือมาตรฐานที่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๓.๕.๒ การระบุวัตถุประสงค์

ระบุวัตถุประสงค์และความยินยอมในการรวบรวม เก็บรักษา การใช้ และการเปิดเผยข้อมูลให้ชัดเจน ทั้งนี้ ผู้ให้บริการควรระมัดระวังในการดำเนินการกับข้อมูลส่วนบุคคล

๓.๕.๓ การเก็บรักษาข้อมูลเท่าที่จำเป็น

ระยะเวลาในการเก็บรักษาข้อมูลที่เหมาะสม และการกำหนดระยะเวลาในการเก็บรักษาข้อมูลหลังจากมีการแจ้งให้ทำลายข้อมูล

๓.๕.๔ การใช้ เก็บรักษา และการเปิดเผย

การแจ้งผู้ใช้บริการทราบว่า ผู้ให้บริการจะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ หรือเป็นกรณีที่กฎหมายกำหนด หรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตามคำสั่งศาล

๓.๕.๕ ความโปร่งใส และการแจ้งเตือน

การแจ้งให้ผู้ใช้บริการทราบและให้ข้อมูลที่เพียงพอเกี่ยวกับความโปรงใส่ ในการดำเนินการกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

๓.๕.๖ ความรับผิดชอบต่อข้อมูล

นโยบายและแนวปฏิบัติในกรณีการละเมิดข้อมูล และควรมีกระบวนการ เอกสารหลักฐานที่ได้ดำเนินการที่สอดคล้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากความรับผิดชอบด้านสารสนเทศจะเป็นส่วนสำคัญในการตรวจสอบการละเมิดข้อมูลส่วนบุคคล

๓.๕.๗ สถานที่จัดเก็บข้อมูล

การแสดงให้ผู้ใช้บริการทราบสถานที่ในการจัดเก็บข้อมูล หรือกำหนดให้ผู้ใช้บริการสามารถเลือกสถานที่จัดเก็บข้อมูลได้ เพื่อเป็นการลดความเสี่ยงในการถูกละเมิดเนื่องจากการประมวลผลข้อมูลส่วนบุคคลอาจจะถูกโอนย้ายข้อมูลไปยังต่างประเทศ ซึ่งอาจจะมีกฎหมาย กฎระเบียบหรือระดับการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน

๓.๕.๘ การอำนวยความสะดวกในการเข้าถึงข้อมูล

การอำนวยความสะดวกแก่ผู้ใช้บริการในระยะเวลาที่เหมาะสมและมีประสิทธิภาพ ทั้งนี้ห้ามมิให้ผู้ให้บริการใช้ข้อกำหนดทางเทคนิคหรือข้อกำหนดขององค์กรเป็นอุปสรรคในการ ปฏิเสธสิทธิ์ของเจ้าของข้อมูล
