การใช้ AWS ในบริบทของการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลทั่วไป

*พฤษภาคม **2561***

(สำหรับฉบับล่าสุด โปรดศึกษาได้ที่ https://aws.amazon.com/compliance/resources/)

ภาพรวม

เอกสารฉบับนี้ได้จัดทำข้อมูลเพื่อให้ความช่วยเหลือลูกค้าที่ใช้ AWS เพื่อเก็บหรือเพื่อประมวลผลซึ่งมีข้อมูลส่วนบุคคลในบริบทของการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลทั่วไป ทั้งนี้ เอกสารฉบับนี้จะช่วยให้ลูกค้าสามารถเข้าใจถึง:

- วิธีการบริการของ AWS รวมไปถึงวิธีที่ลูกค้าสามารถจัดการกับความปลอดภัยและการเข้ารหัสลับเนื้อหาได้
- ที่ตั้งทางภูมิศาสตร์ที่ลูกค้าสามารถเลือกเก็บเนื้อหาและประเด็นอื่นๆ ที่ควรพิจารณา
- บทบาทหน้าที่ความรับผิดชอบของลูกค้าและ AWS ในการจัดการและการป้องกันเนื้อหาที่ได้จัดเก็บอยู่ในบริการ AWS

ขอบเขต

สมุดปกขาวฉบับนี้จะให้ความสำคัญเกี่ยวกับประเด็นคำถามที่มักจะถูกถามบ่อยๆ โดยลูกค้าของ AWS ในด้านการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลในการใช้บริการของ AWS ซึ่งได้มีการจัดเก็บหรือประมวลเนื้อหาซึ่งมีข้อมูลส่วนบุคคลอยู่ อีกทั้ง ยังมีประเด็นอื่นๆ ที่ลูกค้าแต่ละรายต้องพิจารณา เช่น กรณีที่ลูกค้าต้องปฏิบัติตามข้อกำหนดเฉพาะของธุรกิจ กฎหมายในแต่ละเขตการปกครอง หรือภาระผูกพันตามสัญญาที่ลูกค้ามีกับบุคคลที่สาม

เอกสารฉบับนี้จัดทำขึ้นเพื่อวัตถุประสงค์ในการให้ข้อมูล มิใช่เป็นการให้คำแนะนำทางกฎหมาย ดังนั้นจึงไม่ควรถือว่าเป็นคำแนะนำทางกฎหมาย และเนื่องจากความต้องการของลูกค้าแต่ละรายนั้นแตกต่างกันออกไป ดังนั้น AWS เน้นย้ำให้ลูกค้าหาคำแนะนำที่เหมาะสมในการรักษาความปลอดภัยและการคุ้มครองข้อมูล รวมไปถึงกฎหมายที่บังคับใช้และข้อกำหนดอื่นๆ ที่เกี่ยวข้องกับธุรกิจของตนเสียก่อน

เมื่ออ้างถึงเนื้อหาในเอกสารฉบับนี้หมายถึงซอฟต์แวร์ (ซึ่งรวมไปถึงภาพที่สร้างจากคอมพิวเตอร์เสมือน) ข้อมูล ข้อความ ข้อความเสียง วีดีโอ ภาพถ่ายและเนื้อหาอื่นๆ ที่ลูกค้าหรือผู้ใช้ได้จัดเก็บหรือประมวลผลโดยใช้บริการของ AWS เช่น เนื้อหาของลูกค้า ที่ลูกค้าได้จัดเก็บด้วย Amazon Simple Storage Service, ไฟล์ข้อมูลซึ่งจัดเก็บผ่าน Amazon Elastic Block Store volume หรือเนื้อหาในตารางฐานข้อมูลที่อยู่ใน Amazon DynamoDB ทั้งนี้ เนื้อหาดังกล่าวอาจจะรวมถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับลูกค้า ผู้ใช้อื่นๆ หรือบุคคลภายนอก ข้อตกลงของสัญญาว่าด้วยลูกค้าที่ใช้บริการ AWS หรือสัญญาอื่นๆ ที่เกี่ยวข้องซึ่งทางบริษัทกำหนดขึ้นเพื่อควบคุมการใช้บริการของ AWS และบังคับใช้กับเนื้อหาของลูกค้า ทั้งนี้ เนื้อหาของลูกค้าจะไม่รวมไปถึงข้อมูลที่ลูกค้าได้ให้ไว้กับ AWS เพื่อการสร้างหรือการดำเนินการสร้างบัญชีของ AWS เช่น ชื่อของลูกค้า หมายเลขโทรศัพท์ที่อยู่อีเมล หรือข้อมูลในการเรียกเก็บเงิน ซึ่งในส่วนนี้บริษัทเรียกว่าข้อมูลทางบัญชีและจะถูกควบคุมโดยนโยบายรักษาความเป็นส่วนตัวของ AWS[1]

[1] http://aws.amazon.com/privacy/

เนื้อหาของลูกค้า: ประเด็นที่ควรพิจารณาเกี่ยวกับความเป็นส่วนตัวและการคุ้มครองข้อมูล

ในการจัดเก็บเนื้อหานั้นมีสิ่งที่ต้องพิจารณาเกี่ยวกับการจัดการประเด็นต่างๆ ในทางปฏิบัติเช่น:

- เนื้อหาจะปลอดภัยหรือไม่?
- เนื้อหาจะจัดเก็บที่ไหน?
- ใครสามารถเข้าถึงเนื้อหานี้ได้บ้าง?
- กฎหมายและกฎระเบียบอะไรที่บังคับใช้กับเนื้อหา และมีข้อกำหนดอะไรบ้างที่จะต้องปฏิบัติตามกฎหมายและกฎระเบียบดังกล่าว?

ประเด็นเหล่านี้ไม่ใช่เรื่องใหม่และไม่ใช่ประเด็นเฉพาะของระบบคลาวด์เท่านั้น แต่เป็นประเด็นที่เกี่ยวข้องกับระบบแม่ข่ายและระบบปฏิบัติการภายในองค์กร รวมไปถึงบริการแม่ข่ายโดยบุคคลภายนอก ประเด็นเหล่านี้เกี่ยวข้องกับการจัดเก็บเนื้อหาบนเครื่องมืออุปกรณ์ของบุคคลภายนอกหรือในพื้นที่ของบุคคลภายนอกโดยมีบุคลากรซึ่งเป็นบุคคลภายนอกเป็นผู้เข้าถึง จัดการ หรือใช้เนื้อหาเหล่านั้น ในการใช้บริการของ AWS ลูกค้าแต่ละรายจะยังคงมีกรรมสิทธิ์และควบคุมเนื้อหาของตนเองได้อยู่ รวมไปถึงการควบคุมในประเด็นต่อไปนี้:

- เนื้อหาที่ลูกค้าเลือกที่จะจัดเก็บหรือประมวลโดยใช้บริการ AWS
- บริการ AWS ชนิดไหนที่ลูกค้าใช้กับเนื้อหาของตน
- รีเจี้ยนซึ่งเนื้อหานั้นจะได้มีการจัดเก็บ
- รูปแบบ โครงสร้าง และความปลอดภัยของเนื้อหา รวมไปถึงเนื้อหาที่ต้องการจะปกปิด หรือการไม่เปิดเผยตัวตน หรือการเข้ารหัสลับหรือไม่
- ใครสามารถเข้าถึงบัญชีและเนื้อหาของลูกค้าใน AWS ได้บ้าง และการมอบ จัดการ หรือยกเลิกเพิกถอนสิทธิ์ในการเข้าถึงนั้น

เนื่องจากลูกค้าของ AWS ยังคงมีกรรมสิทธิ์และสามารถควบคุมเนื้อหาของตนภายในบริการของ AWS อยู่ ดังนั้นลูกค้าจึงมีหน้าที่ที่เกี่ยวข้องกับการรักษาความปลอดภัยของเนื้อหาอันเป็นส่วนหนึ่งของความรับผิดชอบร่วมซึ่งเป็นต้นแบบของ AWS โดยต้นแบบความรับผิดชอบร่วมนี้เป็นหลักการพื้นฐานเพื่อใช้ทำความเข้าใจบทบาทของลูกค้าและ AWS ในบริบทที่เกี่ยวกับการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลซึ่งบังคับใช้กับเนื้อหาที่ลูกค้าเลือกที่จะจัดเก็บหรือประมวลโดยใช้บริการของ AWS

แนวทางความรับผิดชอบร่วมของ AWS และลูกค้า เพื่อจัดการความปลอดภัยระบบคลาวด์

เนื้อหาของลูกค้าจะปลอดภัยหรือไม่?

การย้ายโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศมายัง AWS สร้างรูปแบบความรับผิดชอบร่วมระหว่างลูกค้าและ AWS ซึ่งทั้งลูกค้าและ AWS จะมีบทบาทที่สำคัญในการดำเนินงานและจัดการด้านความปลอดภัย AWS ได้ดำเนินการจัดการและควบคุมองค์ประกอบตั้งแต่ระบบปฏิบัติการ Host operating system และเซิร์ฟเวอร์เสมือนไปจนถึงความปลอดภัยทางกายภาพของอุปกรณ์ที่ใช้ในการให้บริการของ AWS ในขณะที่ลูกค้าเองก็รับผิดชอบในการจัดการระบบปฏิบัติการ Guest (รวมไปถึงการปรับปรุงให้ทันสมัยและติดตั้งซอฟต์แวร์อุดช่องโหว่ในระบบปฏิบัติการ Guest) และการใช้ซอฟต์แวร์ที่เกี่ยวข้อง รวมไปถึงการกำหนดค่าการทำงานของไฟร์วอลล์ที่ AWS ได้จัดให้มีไฟร์วอลล์กลุ่มเพื่อรักษาความปลอดภัยไว้ และคุณสมบัติด้านความปลอดภัยอื่นๆ ที่เกี่ยวข้อง ลูกค้ามักจะเชื่อมโยงกับระบบของ AWS ผ่านบริการที่ลูกค้าได้จากบุคคลภายนอก เช่น ผู้ให้บริการอินเทอร์เน็ต ทั้งนี้ AWS ไม่ได้จัดเตรียมระบบการเชื่อมต่อไว้ให้ ดังนั้น จึงเป็นความรับผิดชอบของลูกค้าที่จะต้องพิจารณาถึงความปลอดภัยของการใช้ระบบเชื่อมต่อและความรับผิดชอบในการรักษาความปลอดภัยของบุคคลภายนอกที่เกี่ยวข้องกับระบบดังกล่าว โดยบทบาทของทั้งลูกค้าและ AWS อันเกี่ยวกับต้นแบบความรับผิดชอบร่วมนี้จะได้แสดงอยู่ในภาพที่ 1:

ภาพที่ **1** – ต้นแบบความรับผิดชอบร่วมของ AWS และลูกค้า

ต้นแบบความรับผิดชอบร่วมมีความหมายอย่างไรสำหรับความปลอดภัยในเนื้อหาของลูกค้า?

ในการประเมินความปลอดภัยของบริการระบบคลาวด์ ลูกค้าจำเป็นที่จะต้องทำความเข้าใจและแยกแยะความแตกต่างระหว่าง:

- มาตรการความปลอดภัย ซึ่งผู้ให้บริการระบบคลาวด์ (AWS) ได้ดำเนินการและปฏิบัติการ ถือว่าเป็น "ความปลอดภัย*ของ*ระบบคลาวด์"
- มาตรการความปลอดภัย ซึ่งลูกค้าได้ดำเนินการและปฏิบัติการอันเกี่ยวข้องกับความปลอดภัยของเนื้อหาและแอพพลิเคชั่นของลูกค้าโดยใช้บริการของ AWS ถือว่าเป็น "ความปลอดภัย*ภายใน*ระบบคลาวด์"

ในขณะที่ AWS จัดการความปลอดภัย*ของ*ระบบคลาวด์ ความปลอดภัย*ภายใน*ระบบคลาวด์จะเป็นความรับผิดชอบของลูกค้าเอง โดยที่ลูกค้ายังคงสามารถควบคุมความปลอดภัยที่ตนเลือกที่จะดำเนินการเพื่อที่จะป้องกันเนื้อหา การใช้ ระบบและเครือข่ายของตนเอง ซึ่งไม่ต่างไปจากการใช้ในศูนย์ข้อมูลของลูกค้าเอง

ทำความเข้าใจความปลอดภัย*ของ*ระบบคลาวด์

AWS รับผิดชอบในการจัดการความปลอดภัยของระบบคลาวด์ ทั้งนี้ โครงสร้างพื้นฐานของระบบคลาวด์ของ AWS นั้นได้ถูกออกแบบให้เป็นการประมวลผลของระบบคลาวด์ที่ยืดหยุ่นและปลอดภัยที่สุดเท่าที่จะเป็นได้ อีกทั้งมีการออกแบบมาเพื่อให้มีความพร้อมใช้งานสูงสุด โดยสามารถแบ่งเครือข่ายลูกค้าได้อย่างชัดเจน ระบบคลาวด์ของ AWS ยังให้บริการที่ปรับขนาดได้และเชื่อถือได้สูง ซึ่งช่วยให้ลูกค้าสามารถจัดการทั้งการใช้และเนื้อหาได้อย่างรวดเร็วและปลอดภัยพร้อมรองรับการใช้งานในระดับใหญ่พร้อมกันทั่วโลกเมื่อจำเป็น

บริการของ AWS นั้นเป็นการให้บริการโดยไม่แบ่งแยกสาระหรือประเภทของเนื้อหา เพราะได้จัดให้มีบริการด้านความปลอดภัยในระดับสูงให้กับลูกค้าเหมือนกันทั้งหมดโดยไม่ได้คำนึงถึงประเภทของเนื้อหาที่จัดเก็บหรือภูมิภาคทางภูมิศาสตร์ที่ใช้ในการจัดเก็บเนื้อหาของลูกค้า ศูนย์ข้อมูลที่มีความปลอดภัยระดับโลกของ AWS มีการใช้การเฝ้าระวังทางอิเล็กทรอนิกส์ที่ล้ำสมัยและระบบควบคุมการเข้าถึงหลายๆ ปัจจัย ทั้งนี้ ศูนย์ข้อมูลดังกล่าวจะมีเจ้าหน้าที่คอยดูแล 24 ชั่วโมงโดยเจ้าหน้าที่รักษาความปลอดภัยที่ได้รับการฝึกอบรม และโดยการจำกัดการเข้าถึงเฉพาะผู้จำเป็น สำหรับรายการมาตรการความปลอดภัยซึ่งถูกกำหนดให้เป็นหัวใจสำคัญของโครงสร้างพื้นฐานและบริการของระบบคลาวด์ของ AWS นั้น โปรดอ่านสมุดปกขาวของ AWS ในส่วนที่เกี่ยวกับภาพรวมของขั้นตอนการรักษาความปลอดภัย Overview of Security Processes[2]

AWS ได้เฝ้าระวังเกี่ยวกับความปลอดภัยของลูกค้าและได้ดำเนินการมาตรการทางเทคนิคและทางกายภาพขั้นสูงเพื่อป้องกันไม่ให้เกิดการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งนี้ ลูกค้าสามารถที่จะตรวจสอบการควบคุมความปลอดภัยที่มีอยู่ของ AWS ผ่านหนังสือรับรองและรายงานของ AWS รวมไปถึง การควบคุมระบบและองค์กรของ AWS (AWS System & Organization Control: SOC) รายงานฉบับ 1 ฉบับที่ 2[3] และฉบับที่ 3[4] มาตรฐาน ISO 27001[5] 27017[6] 27018[7] และ 9,001[8] ตลอดจนรายงานการปฏิบัติตาม PCI DSS[9] ทั้งนี้ มาตรฐาน ISO 27018 ของ AWS บ่งชี้ว่า AWS มีระบบควบคุมซึ่งมีไว้เพื่อแก้ไขปัญหาการคุ้มครองความเป็นส่วนตัวในเนื้อหาของลูกค้าโดยเฉพาะ โดยรายงานและหนังสือรับรองดังกล่าวได้ออกโดยผู้ตรวจสอบอิสระซึ่งเป็นบุคคลภายนอกเพื่อรับรองถึงการออกแบบและประสิทธิภาพในการดำเนินงานของการควบคุมความปลอดภัยของ AWS อีกด้วย

---

2 https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

3 https://aws.amazon.com/compliance/soc-faqs/

4 http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

5 http://aws.amazon.com/compliance/iso-27001-faqs/

6 http://aws.amazon.com/compliance/iso-27017-faqs/

7 http://aws.amazon.com/compliance/iso-27018-faqs/

8 https://aws.amazon.com/compliance/iso-9001-faqs/

9 https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

หนังสือรับรองและรายงานเกี่ยวกับการปฏิบัติตามของ AWS นั้นสามารถขอได้ที่ https://aws.amazon.com/compliance/contact สำหรับข้อมูลเพิ่มเติมเกี่ยวกับหนังสือรับรองและรายงานเกี่ยวกับการปฏิบัติตามของ AWS ตลอดจนการยึดมั่นในแนวปฏิบัติและมาตรฐานที่เป็นที่ยอมรับสามารถศึกษาได้จากเว็บไซต์ที่เกี่ยวกับการปฏิบัติตามหน้าที่ของ AWS[10]

ทำความเข้าใจความปลอดภัย*ภายใน*ระบบคลาวด์

ลูกค้ายังคงไว้ซึ่งกรรมสิทธิ์และเป็นผู้ควบคุมเนื้อหาของตนเมื่อใช้บริการ AWS ลูกค้าเป็นผู้กำหนดว่าเนื้อหาที่ต้องการจะจัดเก็บหรือประมวลผลเนื้อหาใดโดยใช้บริการของ AWS บ้าง และเนื่องจากลูกค้าเป็นผู้กำหนดว่าจะจัดเก็บหรือประมวลผลเนื้อหา อะไรบ้างนั้นเอง ทำให้ลูกค้าเป็นเพียงผู้เดียวที่จะเป็นผู้กำหนดระดับความปลอดภัยที่เหมาะสมสำหรับเนื้อหาที่ต้องการจะจัดเก็บและประมวลผลได้ ทั้งนี้ลูกค้าจะยังเป็นผู้ควบคุมอย่างเต็มที่ว่าจะใช้บริการใด ใครบ้างที่มีสิทธิ์ที่จะเข้าถึงเนื้อหาและบริการของลูกค้า รวมไปถึงการกำหนดเงื่อนไขในการเข้าถึงอีกด้วย

ลูกค้าเป็นผู้ควบคุมการกำหนดคุณลักษณะและคุ้มครองเนื้อหาของตน รวมไปถึงว่าจะให้เนื้อหาของตนนั้นเข้ารหัสลับหรือไม่ (ทั้งที่เป็นข้อมูลที่จัดเก็บอยู่ในเซิร์ฟเวอร์ หรือข้อมูลที่อยู่ระหว่างการโอนย้ายระหว่างอุปกรณ์หรือระหว่างระบบ) และลักษณะความปลอดภัยอื่นๆ รวมไปถึงเครื่องมือที่ตนใช้คืออะไรและจะใช้อย่างไร โดย AWS จะไม่เปลี่ยนการตั้งค่าคุณลักษณะของลูกค้าเพราะการตั้งค่าเหล่านี้จะถูกกำหนดและควบคุมโดยลูกค้าเอง ลูกค้าของ AWS จะมีอิสระอย่างเต็มที่ในการออกแบบความปลอดภัยเพื่อให้ตรงกับความต้องการของตนเอง นี่จึงเป็นความแตกต่างที่สำคัญเมื่อเทียบกับบริการโฮสติ้งแบบเดิม ที่ผู้ให้บริการจะเป็นผู้กำหนดความปลอดภัยเอง นอกจากนี้ AWS ยังได้ให้อำนาจและส่งเสริมให้ลูกค้าตัดสินใจเองว่ามาตรการความปลอดภัยที่จะดำเนินการภายในระบบคลาวด์เมื่อไหร่และอย่างไรตามความต้องการทางธุรกิจของลูกค้าแต่ละราย เช่น หากต้องการให้เนื้อหาของลูกค้าได้รับการคุ้มครองในระดับที่สูงขึ้นลูกค้าก็อาจที่จะเพิ่มระบบการสำรอง การคำนึงถึงทำเลที่ตั้ง การส่งสัญญาณดาวเทียมด้วยเครือข่ายเป็นต้น เพื่อสร้างระบบควบคุมความปลอดภัยที่สูงและมีความยืดหยุ่นมากขึ้น หรือกรณีที่ต้องการให้เนื้อหานั้นเข้าถึงได้อย่างจำกัด AWS ก็จะอำนวยความสะดวกให้ลูกค้าสามารถที่จะกำหนดการควบคุมสิทธิ์ในการเข้าถึงทั้งในระดับของระบบและระดับของข้อมูลผ่านการเข้ารหัสลับ

เพื่อให้ความช่วยเหลือลูกค้าในการออกแบบ ดำเนินการ และใช้งานระบบความปลอดภัยของลูกค้าในสภาพแวดล้อมของ AWS นั้น ทาง AWS ได้จัดเตรียมเครื่องมือ และคุณลักษณะความปลอดภัยที่หลากหลายเพื่อให้บริการแก่ลูกค้า ลูกค้ายังสามารถใช้เครื่องมือความปลอดภัยและการควบคุมของตนเองรวมไปถึงเครื่องมือความปลอดภัยต่างๆ จากบุคคลภายนอกได้อีกด้วย ลูกค้าสามารถกำหนดคุณลักษณะบริการของ AWS เพื่อเลือกใช้ประโยชน์จากเครื่องมือและการควบคุมความปลอดภัยเพื่อคุ้มครองเนื้อหาของตนรวมไปถึงอัตลักษณ์บุคคลและเครื่องมือในการจัดการการเข้าถึง ศักยภาพความปลอดภัย การเข้ารหัสลับ และความปลอดภัยทางเครือข่าย ทั้งนี้ ลูกค้าสามารถพิจารณามาตรการตัวอย่างดังต่อไปนี้เพื่อช่วยในการรักษาความปลอดภัยเนื้อหาของตนซึ่งรวมไปถึง:

- นโยบายกำหนดรหัสผ่านที่มีความซับซ้อน มีการกำหนดการอนุญาตที่เหมาะสมให้กับผู้ใช้ และขั้นตอนที่รัดกุมในการคุ้มครองกุญแจเข้ารหัสลับของตน
- จัดให้มีไฟร์วอลล์ และ การแบ่งเครือข่ายย่อย เนื้อหามีการเข้ารหัสอย่างเหมาะสม รวมไปถึงระบบที่ได้มีการออกแบบให้เหมาะสมเพื่อลดความเสี่ยงกรณีข้อมูลสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

จากการที่ลูกค้า มิใช่ AWS เป็นผู้ควบคุมปัจจัยที่สำคัญต่างๆ เหล่านี้ ดังนั้นลูกค้าจึงมีหน้าที่รับผิดชอบในการกำหนดตัวเลือกและความปลอดภัยสำหรับเนื้อหาที่ต้องการจะจัดเก็บและประมวลผลโดยใช้บริการของ AWS หรือใช้เชื่อมต่อกับโครงสร้างพื้นฐานของ AWS เช่น ระบบปฏิบัติการแบบ Guest การใช้อินสแตนซ์เพื่อประมวลผล และเนื้อหาที่ได้มีการจัดเก็บและประมวลผลอยู่ในหน่วยความจำของ AWS ฐานข้อมูลหรือบริการอื่นๆ

10 https://aws.amazon.com/compliance/

AWS ได้จัดเตรียมชุดเครื่องมือที่ครบครันเกี่ยวกับการเข้าถึง การเข้ารหัสลับ และการบันทึกเพื่อช่วยให้ลูกค้าสามารถจัดการเนื้อหาของตนได้อย่างมีประสิทธิภาพ รวมไปถึงบริการการจัดการรหัส AWS (AWS Key Management Service) และบริการการกำกับดูแลการปฏิบัติตามข้อกำหนด การตรวจสอบการดำเนินการ ตลอดจนการตรวจสอบความเสี่ยงทางบัญชีของ AWS (AWS CloudTrail) เพื่อช่วยให้ลูกค้าสามารถที่จะผนวกเอาเครื่องมือเพื่อรักษาความปลอดภัยของ AWS เข้าไปในขอบข่ายการควบคุมของลูกค้าที่มีอยู่แล้วและเพื่อช่วยให้ลูกค้าสามารถออกแบบและประเมินความปลอดภัยในการใช้บริการของ AWS นั้น AWS ได้เผยแพร่สมุดปกขาว[11]ที่เกี่ยวข้องกับความปลอดภัย ธรรมาภิบาล ความเสี่ยงและการปฏิบัติตาม รายการการตรวจสอบและแนวปฏิบัติที่เป็นเลิศ นอกจากนี้ ลูกค้ายังมีอิสระที่จะออกแบบและประเมินความปลอดภัยตามความต้องการของตนเองและยังสามารถเรียกให้มีการตรวจรายละเอียดในโครงสร้างพื้นฐานระบบคลาวด์ของตนตราบเท่าที่การตรวจรายละเอียดเหล่านั้นจะเป็นไปเฉพาะอินสแตนซ์เพื่อประมวลผลของลูกค้าและไม่เป็นการละเมิดต่อนโยบายการใช้ที่ยอมรับได้ AWS Acceptable Use Policy[12]

11 http://aws.amazon.com/compliance/#whitepapers

12 https://aws.amazon.com/aup/

รีเจี้ยนของ AWS: เนื้อหาจะจัดเก็บที่ไหน?

ศูนย์ข้อมูล AWS นั้นตั้งเป็นรายกลุ่มอยู่ในภูมิภาคต่างๆ ทั่วโลก โดย AWS จะเรียกกลุ่มของศูนย์ข้อมูลที่ตั้งอยู่ในประเทศต่างๆ ว่า "รีเจี้ยนของ AWS" ลูกค้าสามารถที่จะเข้าถึงรีเจี้ยนของ AWS ได้ทั่วโลก[13] ซึ่งลูกค้าสามารถเลือกที่จะใช้รีเจี้ยนเดียวหรือทุกรีเจี้ยนหรือจะผสมกันระหว่างรีเจี้ยนก็ได้ ทั้งนี้ ภาพที่ 2 ได้แสดงให้เห็นถึงที่ตั้งรีเจี้ยนของ AWS ณ เดือนพฤษภาคม พ.ศ. 2561[14]

ภาพที่ 2 – รีเจี้ยนทั่วโลกของ AWS

[13] AWSGovCloud(US) เป็นรีเจี้ยนของ AWS ที่แยกออกมาต่างหากมีขึ้นเพื่อให้หน่วยงานรัฐบาลสหรัฐและลูกค้าได้เคลื่อนย้ายปริมาณงานที่อ่อนไหวไปยังระบบคลาวด์เพื่อตอบโจทย์ข้อกำหนดทางกฎหมายและการปฏิบัติตาม ส่วน AWS China (ปักกิ่ง) เป็นรีเจี้ยนของ AWS ที่แยกออกมาต่างหากอีกหนึ่งจุด ลูกค้าผู้ที่ประสงค์ที่จะใช้ AWS China (ปักกิ่ง) จะต้องลงทะเบียนสร้างบัญชีใหม่อีกชุดพร้อมด้วยการอ้างอิงตัวตนเฉพาะเพื่อเข้ารหัสใน AWS China (ปักกิ่ง)

14 สำหรับแผนที่ในรูปแบบเรียลไทม์ โปรดเข้าไปเยี่ยมชมได้ที่: https://aws.amazon.com/about-aws/global-infrastructure/

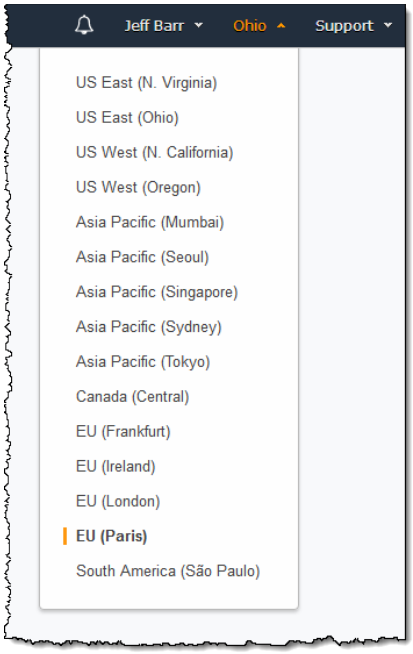
ลูกค้าของ AWS สามารถที่จะเลือกรีเจี้ยนของ AWS หรือรีเจี้ยนที่เนื้อหาและเซิร์ฟเวอร์ของตนนั้นจะตั้งอยู่ได้ การเลือกรีเจี้ยนดังกล่าวช่วยให้ลูกค้าซึ่งมีข้อกำหนดเกี่ยวกับที่ตั้งทางภูมิศาสตร์เฉพาะสามารถรักษาความปลอดภัยในที่พื้นที่หนึ่งหรือพื้นที่ต่างๆ ตามความต้องการของลูกค้าได้ เช่น ลูกค้าของ AWS ในอินเดียสามารถเลือกที่จะเลือกใช้บริการ AWS เฉพาะในรีเจี้ยนเดียวของ AWS เช่น ในรีเจี้ยนเอเชียแปซิฟิค (มุมไบ) และเก็บเนื้อหาของตนอยู่ในประเทศอินเดียได้หากว่าเป็นพื้นที่ที่ตนต้องการ และถ้าหากลูกค้าเลือกตัวเลือกนี้แล้ว AWS ก็จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าออกไปจากอินเดียโดยไม่ได้รับความยินยอมจากลูกค้าเสียก่อน ยกเว้นในกรณีที่มีข้อกำหนดทางกฎหมาย

ลูกค้าจะยังคงควบคุมว่าจะใช้รีเจี้ยนไหนของ AWS เพื่อการเก็บรักษาและประมวลเนื้อหา โดย AWS จะทำเพียงแค่จัดเก็บและประมวลเนื้อหาของลูกค้าแต่ละรายในรีเจี้ยนของ AWS ตามที่ลูกค้าเลือกเท่านั้น โดยจะไม่มีการเคลื่อนย้ายเนื้อหาของลูกค้าหากไม่ได้รับความยินยอมจากลูกค้าเสียก่อน ยกเว้นในกรณีที่เป็นข้อกำหนดทางกฎหมาย

ลูกค้าสามารถเลือกรีเจี้ยน(ต่างๆ) ของตนได้อย่างไร?

เมื่อเข้าใช้แผงควบคุมการจัดการของ AWS หรือเมื่อได้มีการร้องขอผ่านช่องทางการเชื่อมต่อของ AWS (AWS Application Programming Interface: API) ลูกค้าจะสามารถกำหนดรีเจี้ยนของ AWS (ต่างๆ) ที่ต้องการจะใช้บริการของ AWS ได้

ภาพที่ 3: การเลือกรีเจี้ยนของ AWS แสดงให้เห็นตัวอย่างเมนูการเลือกรีเจี้ยนของ AWS ที่แสดงแก่ลูกค้าเมื่อมีการอัพโหลดเนื้อหาลงไปในบริการการจัดเก็บของ AWS หรือจัดเตรียมอุปกรณ์เสมือนต่างๆ เพื่อสร้างเทคโนโลยีคอมพิวเตอร์จำลองขึ้นโดยใช้ AWS Management Console



ภาพที่ **3** – การเลือกรีเจี้ยนของ **AWS** ในแผงควบคุมจัดการ **AWS**

ลูกค้ายังสามารถกำหนดรีเจี้ยนของ AWS ที่ต้องการใช้อุปกรณ์เสมือนต่างๆ เพื่อสร้างเทคโนโลยีคอมพิวเตอร์จำลองของตนด้วยการเข้าถึงบริการ Amazon Virtual Private Cloud: VPC ได้ ทั้งนี้ บริการสร้างคลาวด์ส่วนตัว Amazon VPC นั้นจะเปิดโอกาสให้ลูกค้าจัดเตรียมการสร้างคลาวด์ AWS ที่เป็นส่วนตัวและแยกเฉพาะ โดยลูกค้าสามารถที่จะเปิดใช้ทรัพยากร AWS ในเครือข่ายเสมือนซึ่งลูกค้าได้กำหนดเอง ในการใช้ Amazon VPC นั้นลูกค้าสามารถที่จะกำหนดแบบโครงสร้างเครือข่ายเสมือนที่มีความคล้ายคลึงกับเครือข่ายแบบดั้งเดิมซึ่งอาจจะใช้ปฏิบัติการอยู่ในศูนย์ข้อมูลของตนได้

อุปกรณ์เสมือนต่างๆ เพื่อใช้สร้างเทคโนโลยีคอมพิวเตอร์จำลองหรือทรัพยากรอื่นๆ ที่ลูกค้าเลือกใช้ใน VPC จะจัดเก็บตั้งอยู่ในรีเจี้ยนของ AWS ซึ่งลูกค้ากำหนดเอง เช่น ในการสร้างVPC ในรีเจี้ยนเอเชียแปซิฟิก (มุมไบ) และมีการจัดทำการเชื่อมต่อ (ไม่ว่าจะเป็น VPN [15] หรือ Direct Connect[16]) กับศูนย์

ข้อมูลของลูกค้า อุปกรณ์เสมือนต่างๆ เพื่อสร้างเทคโนโลยีคอมพิวเตอร์จำลองทั้งหมดก็จะนำมาใช้อยู่ในการสร้างคลาวด์ส่วนตัว (VPC) ซึ่งจะอยู่ในรีเจี้ยนเอเชียแปซิฟิก (มุมไบ) เท่านั้น โดยลูกค้าสามารถที่จะเลือกตัวเลือกนี้ในรีเจี้ยนอื่นๆ ของ AWS ได้ด้วย

การถ่ายข้อมูลส่วนบุคคลข้ามพรมแดน

ในปี พ.ศ. 2559 คณะกรรมาธิการสหภาพยุโรปได้อนุมัติและเริ่มใช้กฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปฉบับใหม่ (General Data Protection Regulation: GDPR) โดยกฎระเบียบดังกล่าวได้มาแทนที่ระเบียบคุ้มครองข้อมูลแห่งสหภาพยุโรป และกฎหมายท้องถิ่นทั้งหมดที่เกี่ยวข้อง โดยบริการของ AWS ทั้งหมดจะปฏิบัติตามกฎหมายฉบับใหม่ซึ่งลูกค้าสามารถนำไปปรับใช้กับการปฏิบัติของตนเพื่อให้สอดคล้องกับกฎหมายได้ ทั้งนี้รวมไปถึงการปฏิบัติตามของ AWS ในประมวลจริยธรรม CISPE การควบคุมการเข้าถึงข้อมูล เครื่องมือการตรวจสอบและการบันทึก การเข้ารหัสลับ การจัดการรหัส การตรวจสอบ การปฏิบัติตามมาตรฐานความปลอดภัยของเทคโนโลยีสารสนเทศ และการปฏิบัติตาม C5 ของ AWS สำหรับข้อมูลเพิ่มเติมสามารถเยี่ยมชมได้ที่ศูนย์กฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไปของ AWS [17] (AWS General Data Protection Regulation (GDPR) Center) และในสมุดปกขาวของ AWS เรื่องการกำหนดทิศทางการปฏิบัติตามกฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป [18] (Navigating GDPR Compliance on AWS Whitepaper)

ในการใช้บริการของ AWS ลูกค้าอาจจะเลือกที่จะโอนถ่ายเนื้อหาซึ่งรวมข้อมูลส่วนบุคคลข้ามพรมแดนและต้องพิจารณาถึงข้อกำหนดทางกฎหมายซึ่งบังคับใช้กับการถ่ายโอนดังกล่าว AWS ได้จัดทำภาคผนวกเกี่ยวกับการประมวลผลข้อมูล (Data Processing Addendum) ที่รวมถึงข้อกฎหมายที่เป็นมาตรฐาน Standard Contractual Clauses 2010/87/EU (ซึ่งมักจะเรียกว่าต้นแบบข้อสัญญา (Model Clauses)) ให้กับลูกค้าของ AWS ที่ถ่ายโอนเนื้อหาซึ่งมีข้อมูลส่วนบุคคล (ตามที่ได้นิยามเอาไว้ในกฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป GDPR) จากสหภาพยุโรปไปยังประเทศนอกเหนือเขตเศรษฐกิจยุโรป ภาคผนวกเกี่ยวกับการประมวลผลข้อมูลและต้นแบบข้อสัญญาทำให้ลูกค้าของ AWS ไม่ว่าจะอยู่ในยุโรปหรือในบริษัทระดับโลกซึ่งดำเนินธุรกิจอยู่ในเขตเศรษฐกิจยุโรปจะยังสามารถดำเนินงานทั่วโลกต่อไปได้โดยใช้ AWS อย่างสอดคล้องกับกฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป หรือ GDPR อย่างเต็มที่ ภาคผนวกเกี่ยวกับการประมวลผลข้อมูล AWS Data Processing Addendum นั้นจะรวมอยู่ในเงื่อนไขการใช้บริการของ AWS Service Terms และปรับใช้บังคับโดยอัตโนมัติในกรณีที่กฎระเบียบว่าด้วยการคุ้มครองข้อมูลทั่วไป (GDPR) นั้นมีผลกับการประมวลผลข้อมูลส่วนบุคคลของลูกค้าในระบบของ AWS

---

15 https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html

16 https://aws.amazon.com/directconnect/

17 https://aws.amazon.com/compliance/gdpr-center/

18 https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf

ใครสามารถเข้าถึงเนื้อหาของลูกค้าได้บ้าง?

ลูกค้าเป็นผู้ควบคุมเนื้อหา

ลูกค้าที่ใช้ AWS จะยังคงเป็นเจ้าของและไม่ได้สูญเสียการควบคุมเนื้อหาของตนภายในระบบ AWS แต่อย่างใด โดยลูกค้าสามารถที่จะ:

- กำหนดว่าเนื้อหาจะตั้งอยู่ที่ใด เช่น ประเภทของการจัดเก็บที่ลูกค้าจะใช้ในระบบ AWS และที่ตั้งทางภูมิศาสตร์ (ตามรีเจี้ยนของ AWS) เพื่อการจัดเก็บนั้น
- ควบคุมรูปแบบ โครงสร้าง และความปลอดภัยของเนื้อหา รวมไปถึงเนื้อหาที่ต้องการจะปกปิด การไม่เปิดเผยตัวตน หรือการเข้ารหัสลับ AWS ยังเสนอให้ลูกค้ามีตัวเลือกที่จะกำหนดการเข้ารหัสที่ยากขึ้นสำหรับเนื้อหาที่มีการโอนย้ายข้อมูลระหว่างอุปกรณ์ หรือระหว่างระบบ หรือข้อมูลที่จัดเก็บอยู่ในเซิร์ฟเวอร์ และยังจัดให้มีตัวเลือกเพื่อให้ลูกค้าจัดการการเข้ารหัสของตนเอง หรือจะใช้เครื่องมือการเข้ารหัสของบุคคลภายนอกตามแต่ลูกค้าจะเลือก
- จัดการการควบคุมการเข้าถึงอื่นๆ เช่น การใช้อัตลักษณ์บุคคล การอนุมัติสิทธิ และการกำหนดเงื่อนไขข้อมูลรับรองความปลอดภัยในการเข้าถึง

ตัวเลือกเหล่านี้จะช่วยให้ลูกค้าของ AWS สามารถควบคุมเนื้อหาของตนในระบบ AWS ไปจนตลอดวงจรชีวิตของเนื้อหาและสามารถจัดการเนื้อหาของตนตามความประสงค์ของตนเองได้ รวมไปถึงการแยกประเภทเนื้อหา การควบคุมการเข้าถึง การเก็บรักษาและการลบทิ้ง

การเข้าถึงเนื้อหาของลูกค้าโดย AWS

AWS มีบริการการประมวลผล การจัดเก็บฐานข้อมูล เครือข่ายและอื่นๆ ตามที่ได้นำเสนอ ไว้ในเว็บไซต์ของ AWS แก่ลูกค้าแต่ละราย โดยลูกค้ามีทางเลือกต่างๆ ในการที่จะเข้ารหัสสลับเนื้อหาของตนเมื่อเข้าใช้บริการ รวมไปถึงการใช้คุณสมบัติการเข้ารหัสของ AWS เช่น บริการ AWS Key Management Service การจัดการระบบเพื่อการเข้ารหัสของตนเอง หรือการใช้เครื่องมือการเข้ารหัสของบุคคลภายนอกตามแต่ลูกค้าจะเลือก AWS จะไม่เข้าถึงหรือใช้เนื้อหาของลูกค้าโดยปราศจากความยินยอมของลูกค้า เว้นแต่จะเป็นไปตามข้อบังคับของกฎหมาย ทั้งนี้ AWS จะไม่ใช้เนื้อหาของลูกค้าหรือที่มีที่มาจากข้อมูลลูกค้าเพื่อวัตถุประสงค์อื่นๆ เช่น เพื่อการตลาดหรือเพื่อการโฆษณาแต่อย่างใด

สิทธิในการเข้าถึงของรัฐบาล

ข้อสงสัยที่ถูกหยิบยกบ่อยๆ คือเรื่องสิทธิของหน่วยงานของรัฐบาลในประเทศและต่างประเทศเพื่อเข้าถึงเนื้อหาซึ่งอยู่ในบริการคลาวด์ ลูกค้ามักจะสับสนในประเด็นที่เกี่ยวกับอธิปไตยทางข้อมูล รวมไปถึงกรณีที่รัฐบาลจะเข้าถึงเนื้อหาของลูกค้าได้หรือไม่และในกรณีไหนบ้าง ทั้งนี้ กฎหมายท้องถิ่นซึ่งบังคับใช้ในเขตอำนาจซึ่งเนื้อหานั้นได้ตั้งอยู่ก็เป็นประเด็นสำคัญประการหนึ่งสำหรับลูกค้าบางราย นอกเหนือไปจากนั้นลูกค้าจำเป็นที่จะต้องพิจารณาให้รอบคอบเสียก่อนว่ากฎหมายในเขตอำนาจอื่นๆ จะมีผลบังคับใช้กับลูกค้าหรือไม่ ในการนี้ลูกค้าพึงที่จะขอคำแนะนำเพื่อทำความเข้าใจกับการบังคับใช้กฎหมายที่เกี่ยวข้องกับธุรกิจและการปฏิบัติการของตน

เมื่อมีข้อกังวลหรือคำถามเกี่ยวกับสิทธิของรัฐบาลในประเทศหรือต่างประเทศที่จะเข้าถึงเนื้อหาซึ่งจัดเก็บอยู่ในระบบคลาวด์เกิดขึ้น จึงจำเป็นที่จะทำความเข้าใจว่าหน่วยงานของรัฐบาลที่เกี่ยวข้องอาจจะมีสิทธิ์ที่จะออกคำร้องขอเข้าถึงเนื้อหาดังกล่าวภายใต้กฎหมายที่บังคับใช้กับลูกค้า เช่น บริษัทที่ทำธุรกิจอยู่ในประเทศ X อาจจะตกอยู่ภายใต้ข้อกำหนดทางกฎหมายในการเข้าถึงข้อมูลแม้ว่าเนื้อหานั้นจะถูกจัดเก็บอยู่ในประเทศ Y ก็ตาม ซึ่งโดยปกติแล้วหน่วยงานของรัฐบาลที่ประสงค์จะเข้าถึงข้อมูลขององค์กรก็จะทำคำร้องขอข้อมูลไปยังองค์กรนั้นโดยตรงมากกว่าจะส่งคำร้องไปยังผู้ให้บริการในระบบคลาวด์

ประเทศส่วนใหญ่จะมีการบัญญัติกฎหมายให้อำนาจหน่วยงานที่บังคับใช้กฎหมายและหน่วยงานรักษาความปลอดภัยสามารถเข้าถึงข้อมูลได้ ในความเป็นจริงแล้ว ประเทศต่างๆ เหล่านี้มีขั้นตอน (รวมไปถึงสนธิสัญญาความร่วมมือทางกฎหมายร่วมกัน - Mutual Legal Assistance Treaties) เพื่ออำนวยการถ่ายโอนข้อมูลไปยังประเทศอื่นๆ เมื่อได้มีการดำเนินการทางกฎหมายเพื่อร้องขอข้อมูลอย่างเหมาะสม (เช่น การกระทำที่เกี่ยวกับอาชญากรรม) อย่างไรก็ตาม พึงทราบว่ากฎหมายต่างๆ ที่เกี่ยวข้องนั้นกำหนดให้หน่วยงานบังคับใช้กฎหมายที่จะทำคำร้องขอนั้นจะต้องดำเนินการตามเกณฑ์ที่กฎหมายกำหนดเอาไว้ให้เป็นที่พอใจเสียก่อน เช่น หน่วยงานของรัฐที่ต้องการจะเข้าถึงข้อมูลอาจจะต้องแสดงถึงเหตุผลที่เหมาะสมในการที่จะขอเข้าถึงเนื้อหาและอาจจะต้องมีคำสั่งศาลหรือหมายค้นเพื่อการนี้

หลายประเทศมีกฎหมายเข้าถึงข้อมูลซึ่งมีขึ้นเพื่อบังคับใช้นอกอาณาเขตของประเทศ ตัวอย่างเช่น กฎหมายสหรัฐอเมริกาที่ขยายเขตอำนาจรัฐซึ่งมักจะอ้างถึงบ่อยๆ ในบริบทเกี่ยวกับบริการของคลาวด์ก็คือ รัฐบัญญัติว่าด้วยความรักชาติ (the U.S. Patriot Act) โดยรัฐบัญญัติดังกล่าวจะคล้ายคลึงกับกฎหมายในประเทศที่พัฒนาแล้วอื่นๆ ซึ่งยินยอมให้รัฐบาลนั้นสามารถเข้าถึงข้อมูลที่เกี่ยวกับการสอบสวนในส่วนที่เกี่ยวกับการก่อการร้ายระหว่างประเทศและประเด็นข่าวกรองต่างประเทศอื่นๆ คำร้องขอเพื่อเข้าถึงเอกสารภายใต้รัฐบัญญัติว่าด้วยความรักชาตินี้กำหนดให้ต้องมีคำสั่งศาลซึ่งบ่งชี้ว่าคำร้องขอนั้นเป็นไปตามกฎหมาย รวมไปถึงว่าคำขอนั้นเกี่ยวข้องกับการสอบสวนที่ถูกกฎหมาย รัฐบัญญัติว่าด้วยความรักชาติดังกล่าวมักจะบังคับใช้กับทุกๆ บริษัทซึ่งประกอบธุรกิจอยู่ในสหรัฐอเมริกาโดยไม่คำนึงถึงว่าจะได้จัดตั้งที่ใด และ/หรือ มีการดำเนินธุรกิจทั่วโลกหรือไม่ รวมไปถึงไม่คำนึงว่าข้อมูลจัดเก็บอยู่ในระบบคลาวด์ ในศูนย์ข้อมูลพิเศษแบบ on-site data center หรือในประวัติบันทึกที่เป็นกายภาพหรือไม่ก็ตาม นั่นหมายความว่าบริษัทที่มีสำนักงานใหญ่หรือปฏิบัติการนอกสหรัฐอเมริกาแต่ได้ทำธุรกิจอยู่ในสหรัฐอเมริกาด้วย อาจจะตกอยู่ภายใต้รัฐบัญญัติว่าด้วยความรักชาตินี้ด้วยเหตุผลจากการประกอบธุรกิจของตน

นโยบาย AWS ว่าด้วยการอนุญาตให้รัฐบาลเข้าถึงเนื้อหา

AWS ระมัดระวังในการรักษาความปลอดภัยของลูกค้าและจะไม่เปิดเผยหรือเคลื่อนย้ายข้อมูลเมื่อได้มีคำขอจากรัฐบาลสหรัฐอเมริกาหรือรัฐบาลอื่นๆ เว้นแต่ในกรณีที่เป็นไปตามข้อกำหนดของกฎหมายให้ต้องเปิดเผย จึงต้องปฏิบัติตามและผูกพันตามคำสั่ง เช่น ตามหมายศาลหรือคำสั่งศาล หรือข้อกำหนดโดยกฎหมายที่บังคับใช้ โดยทั่วไปแล้วองค์กรที่ไม่ใช่ภาครัฐหรือหน่วยงานกำกับดูแลจะต้องใช้กระบวนการระหว่างประเทศที่เป็นที่ยอมรับ เช่น สนธิสัญญาความร่วมมือทางกฎหมายร่วมกัน - Mutual Legal Assistance Treaties กับรัฐบาลสหรัฐอเมริกาเพื่อขอความร่วมมือและผูกพันตามคำสั่ง นอกจากนี้ แนวปฏิบัติของ AWS คือ ทางบริษัทจะทำการแจ้งเตือนลูกค้าก่อนที่จะได้มีการเปิดเผยเนื้อหาของลูกค้าในกรณีที่เป็นไปได้ในทางปฏิบัติ เพื่อที่ว่าลูกค้าจะสามารถแสวงหาความคุ้มกันจากการเปิดเผยได้ทันเวลา เว้นแต่ว่าจะต้องห้ามตามกฎหมายให้กระทำได้ หรือมีการบ่งชี้ที่ชัดเจนถึงการกระทำผิดทางกฎหมายซึ่งเกี่ยวเนื่องกับการใช้บริการของ AWS สำหรับข้อมูลเพิ่มเติมโปรดเข้าไปเยี่ยมชมได้ที่ช่องทางออนไลน์ร้องขอเข้าถึงข้อมูล Amazon Information Requests Portal[19]

[19] https://aws.amazon.com/compliance/amazon-information-requests/

ประเด็นการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูล

หลายๆ ประเทศมีกฎหมายที่บัญญัติขึ้นเพื่อคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคล ซึ่งบางประเทศก็มีกฎหมายคุ้มครองข้อมูลหนึ่งฉบับที่ครอบคลุม ในขณะที่ประเทศอื่นๆ มีการจัดการการคุ้มครองข้อมูลส่วนบุคคล ในลักษณะที่แตกต่างกันออกไปด้วยกฎหมายและระเบียบต่างๆ หลายฉบับ แม้ว่าจะมีข้อกำหนดทางกฎหมายและกฎระเบียบที่แตกต่างกันออกไป ซึ่งรวมไปถึงข้อกำหนดที่เกี่ยวกับเขตอำนาจ ข้อกำหนดที่เกี่ยวกับประเภทธุรกิจและข้อกำหนดที่เกี่ยวกับเนื้อหาอันเป็นการเฉพาะ ในกฎหมายที่หลากหลายเหล่านี้ก็จะมีประเด็นร่วมภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ลูกค้าควรพิจารณา ซึ่งยึดตามและสอดคล้องกับวงจรชีวิตของข้อมูลส่วนบุคคล

เพื่อช่วยให้ลูกค้าสามารถวิเคราะห์และจัดการกับข้อกำหนดด้านความเป็นส่วนตัวและการคุ้มครองข้อมูลเมื่อใช้ AWS ในการจัดเก็บและประมวลเนื้อหาซึ่งมีข้อมูลส่วนบุคคลอยู่ AWS ได้นำเสนอขั้นตอนต่างๆ ของวงจรชีวิตของข้อมูล ระบุข้อควรพิจารณาที่สำคัญที่เกี่ยวข้องกับแต่ละขั้นตอนและให้ข้อมูลที่เกี่ยวข้องว่าบริการ AWS นั้นได้มีการปฏิบัติการอย่างไร

กฎหมายคุ้มครองข้อมูลหลายฉบับได้มีการกำหนดความรับผิดชอบโดยยึดจากปฏิสัมพันธ์กับข้อมูลส่วนบุคคล ระดับการเข้าถึงและควบคุมข้อมูลส่วนบุคคลที่บุคคล หน่วยงานหรือองค์กรมีกับข้อมูลส่วนบุคคลนั้นๆ วิธีการหนึ่งที่ใช้ปฏิบัติ ก็คือ การจำแนกระหว่างผู้ควบคุมข้อมูล ผู้ประมวลผลข้อมูลและตัวเนื้อหาหรือเจ้าของข้อมูล ซึ่งคำจำกัดความของเนื้อหาที่ใช้นั้นอาจจะมีความแตกต่างกันในแต่ละเขตอำนาจ และการจำแนกในกฎหมายบางฉบับก็อาจจะไม่ชัดเจนเสมอกันโดย AWS นั้นตระหนักดีว่าบริการของตนได้ถูกใช้ในหลายๆ บริบทที่แตกต่างกันเพื่อการประกอบธุรกิจที่หลากหลาย และอาจมีคู่สัญญาที่หลากหลายเข้ามาเกี่ยวข้องในวงจรชีวิตของข้อมูลส่วนบุคคลในเนื้อหาของลูกค้าที่ได้มีการจัดเก็บและการประมวลผลโดยใช้บริการของ AWS นี้ และเพื่อความเข้าใจง่าย ทาง AWS ได้จัดทำตารางแนะนำด้านล่างนี้ขึ้น โดยยึดสมมติฐานที่เกี่ยวกับเนื้อหาของลูกค้าที่ถูกจัดเก็บและประมวลผลโดยใช้บริการของ AWS ว่าลูกค้าจะ:

- จัดเก็บข้อมูลส่วนบุคคลจากผู้ใช้หรือบุคคลอื่นๆ (เจ้าของข้อมูลส่วนบุคคล) และกำหนดวัตถุประสงค์ที่ลูกค้าต้องการและจะใช้ข้อมูลส่วนบุคคล
- มีความสามารถในการควบคุมการเข้าถึง ปรับเปลี่ยน และใช้ข้อมูลส่วนบุคคล
- จัดการความสัมพันธ์กับบุคคลว่าข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับใคร (ซึ่งในหัวข้อนี้อ้างถึงเว่าปื่นเจ้าของข้อมูลส่วนบุคคล) รวมไปถึงการสื่อสารกับเจ้าของข้อมูลส่วนบุคคลให้เป็นไปตามข้อกำหนดการเปิดเผยและความยินยอมที่เกี่ยวข้อง

ซึ่งนั่นหมายถึงว่าลูกค้าเป็นผู้ปฏิบัติหน้าที่เป็นผู้ควบคุมข้อมูลเนื่องด้วยลูกค้าเป็นผู้ควบคุมเนื้อหาและตัดสินใจเกี่ยวกับการรักษาเนื้อหานั้น รวมไปถึงการกำหนดผู้ได้รับอนุญาตให้ประมวลเนื้อหาในนามของตนได้ ในขณะเดียวกัน AWS นั้นก็จะปฏิบัติหน้าที่ในลักษณะของผู้ประมวลผลข้อมูล เนื่องจาก AWS ใช้เนื้อหาของลูกค้าเพื่อใช้ในการให้บริการเฉพาะในส่วนที่ลูกค้าเลือกเท่านั้นโดยที่ AWS มิได้ใช้เนื้อหาของของลูกค้าเพื่อวัตถุประสงค์อื่นๆ อนึ่ง พึงรับทราบด้วยว่าคำว่า “ผู้ประมวลข้อมูล” และ “ผู้ควบคุมข้อมูล” นั้นจะมีความหมายที่แตกต่างกันอย่างมากภายใต้กฎหมายของสหภาพยุโรปและในสมุดปกขาวฉบับนี้มิได้มีจุดมุ่งหมายที่จะอธิบายข้อกำหนดของสหภาพยุโรปเป็นการเฉพาะตัวแต่อย่างใด ลูกค้าที่ต้องการคำแนะนำว่าด้วยข้อกำหนดการคุ้มครองข้อมูลแห่งสหภาพยุโรปซึ่งเกี่ยวข้องกับผู้ควบคุมข้อมูลและผู้ประมวลข้อมวลนั้นควรอ้างอิงจาก<u>สมุดปกขาวการคุ้มครองข้อมูลแห่งสหภาพยุโรป (EU Data Protection Whitepaper)</u>[20]

ในกรณีที่ลูกค้าใช้บริการของ AWS เพื่อประมวลข้อมูลส่วนบุคคลในนามของและเป็นไปตามคำสั่งของบุคคลที่สาม (ผู้ซึ่งอาจเป็นผู้ควบคุมข้อมูลส่วนบุคคลหรือเป็นบุคคลภายนอกอื่นๆ ซึ่งลูกค้าได้มีความสัมพันธ์ทางธุรกิจด้วย) ความรับผิดชอบของลูกค้าที่ได้แสดงอยู่ในตารางก็จะถือเป็นความรับผิดชอบและบริหารร่วมระหว่างลูกค้าและบุคคที่สามนั้น

[20] https://d1.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf

ขั้นตอนของวงจรของข้อมูล	คำอธิบายโดยย่อและตัวอย่าง	ประเด็นที่ต้องพิจารณา
การเก็บข้อมูลส่วนบุคคล	อาจจะมีความเหมาะสมหรือมีความจำเป็นที่จะต้องแจ้งให้บุคคล (เจ้าของข้อมูลส่วนบุคคล) ให้ได้รับทราบ หรือขอความยินยอมก่อนที่จะได้มีการจัดเก็บข้อมูลส่วนบุคคลซึ่งจะรวมไปถึงการแจ้งวัตถุประสงค์ของการจัดเก็บ ใช้ และเปิดเผยข้อมูล อาจจะมีข้อกำหนดว่าจะจัดเก็บข้อมูลส่วนบุคคลจากใครได้บ้าง เช่น ข้อกำหนดอาจมีความแตกต่างกันหากข้อมูลส่วนบุคคลนั้นจัดเก็บจากบุคคลที่สามแทนที่จะมาจากบุคคลโดยตรง การเก็บข้อมูลส่วนบุคคลนั้นอาจจะได้รับอนุญาตได้เฉพาะกรณีที่เป็นไปตามเหตุผลที่ชอบด้วยกฎหมายหรือมีจุดประสงค์ที่เหมาะสม	**ลูกค้า**: ลูกค้าเป็นผู้กำหนดและควบคุมว่าจะเก็บข้อมูลส่วนบุคคลจากบุคคลภายนอก เมื่อไหร่ อย่างไรและทำไม และตัดสินใจว่าจะให้รวมข้อมูลส่วนบุคคลนั้นในเนื้อหาของลูกค้าที่ได้มีการจัดเก็บและประมวลโดยใช้บริการของ AWS หรือไม่ ลูกค้ายังจำเป็นที่จะต้องรับรองว่าจะได้มีการเปิดเผยวัตถุประสงค์ของการจัดเก็บเนื้อหาดังกล่าวให้กับเจ้าของข้อมูลส่วนบุคคลทราบ รวมถึงรับรองว่าได้รับเนื้อหาที่มาจากแหล่งที่ได้รับอนุญาตและใช้ข้อมูลนั้นเพื่อวัตถุประสงค์ที่ได้รับอนุญาตเท่านั้น ในระหว่างลูกค้าและ AWS นั้น ลูกค้าคือผู้ที่มีความสัมพันธ์กับบุคคลต่างๆ ซึ่งลูกค้าได้นำข้อมูลส่วนบุคคลนั้นมาจัดเก็บเอาไว้อยู่ใน AWS เช่นนี้ ลูกค้าจะต้องสื่อสารโดยตรงกับบุคคลดังกล่าวเพื่อการจัดเก็บและการรักษาข้อมูลส่วนบุคคลนั้น ลูกค้า และมิใช่ AWS จะเป็นผู้ที่รู้ขอบเขตของการบอกกล่าวหรือการขอความยินยอมซึ่งลูกค้าได้รับมาจากบุคคลดังกล่าวเพื่อการจัดเก็บข้อมูลส่วนบุคคลนั้นด้วยเช่นกัน **AWS**: AWS จะไม่เก็บข้อมูลส่วนบุคคล จากบุคคลซึ่งมีข้อมูลส่วนบุคคลอยู่ในเนื้อหาที่ลูกค้าได้จัดเก็บหรือประมวลผลโดยใช้บริการของ AWS และ AWS ไม่มีการติดต่อกับบุคคลดังกล่าว ดังนั้น AWS จึงไม่จำเป็นและในกรณีนี้ไม่สามารถที่จะสื่อสารกับบุคคลดังกล่าวได้ AWS ใช้เนื้อหาของลูกค้าเพื่อจัดให้มีบริการ AWS ตามที่ลูกค้าแต่ละรายเลือกเท่านั้น และ AWS จะไม่ใช้เนื้อหาของลูกค้าเพื่อวัตถุประสงค์อื่นๆ
การใช้และการเปิดเผยข้อมูลส่วนบุคคล	มีแนวโน้มว่าจะมีความเหมาะสมหรือความจำเป็นที่จะต้องใช้หรือเปิดเผยข้อมูลส่วนบุคคลเฉพาะเพื่อวัตถุประสงค์ที่ได้มีการจัดเก็บข้อมูลเท่านั้น นี่อาจหมายความว่าบุคคล (เจ้าของข้อมูลส่วนบุคคล) จะต้องได้รับแจ้งว่าลูกค้านั้นจะใช้ AWS เป็นผู้ให้บริการ	**ลูกค้า**: ลูกค้าเป็นผู้กำหนดและควบคุมว่าจะจัดเก็บข้อมูลส่วนบุคคลทำไมและจะใช้เพื่อวัตถุประสงค์อะไร ใครสามารถใช้และเปิดเผยโดยใครได้บ้าง ลูกค้าจะต้องรับรองว่าจะใช้และเปิดเผยข้อมูลต่อเมื่อได้รับอนุญาตเท่านั้น

ขั้นตอนของวงจรชีวิตข้อมูล	คำอธิบายโดยย่อและตัวอย่าง	ประเด็นที่ต้องพิจารณา
		หากลูกค้าเลือกที่จะให้ข้อมูลส่วนบุคคลรวมอยู่ในเนื้อหาของลูกค้าซึ่งจัดเก็บอยู่ใน AWS ลูกค้าจะเป็นผู้ควบคุมรูปแบบและโครงสร้างของเนื้อหาและกำหนดว่าเนื้อหาจะได้รับการคุ้มครองจากการเปิดเผยสู่บุคคลที่ไม่ได้รับอนุญาตได้อย่างไร รวมไปถึงจะให้ข้อมูลนั้นไม่ระบุตัวตนหรือเข้ารหัสลับหรือไม่ ลูกค้าจะเป็นผู้รู้ว่าได้ใช้บริการของ AWS เพื่อจัดเก็บหรือประมวลเนื้อหาของลูกค้าที่มีอยู่ในข้อมูลส่วนบุคคลรวมอยู่ด้วยหรือไม่ และด้วยเหตุนี้ ในกรณีที่จำเป็น ลูกค้าจึงเป็นผู้ที่อยู่ในตำแหน่งที่ดีที่สุดที่จะบอกกล่าวบุคคลเหล่านั้นว่าจะใช้ AWS เป็นผู้ให้บริการ **AWS**: AWS จะใช้เนื้อหาของลูกค้าเพื่อจัดให้มีบริการ AWS ตามที่ลูกค้าแต่ละรายเลือกเท่านั้น และ AWS จะไม่ใช้เนื้อหาของลูกค้าเพื่อวัตถุประสงค์อื่น
การโอนย้ายข้อมูลส่วนบุคคลออกนอกประเทศ (Offshoring)	หากได้มีการโอนข้อมูลส่วนบุคคลออกนอกประเทศ ก็อาจจะมีความจำเป็นหรือเหมาะสมที่จะต้องบอกกล่าวให้กับบุคคลนั้น (เจ้าของข้อมูลส่วนบุคคล) ทราบถึงประเทศที่ลูกค้าจะทำการจัดเก็บข้อมูลส่วนบุคคลและหรือขอความยินยอมเพื่อจัดเก็บข้อมูลส่วนบุคคลในพื้นที่ที่จะจัดเก็บนั้น สิ่งสำคัญที่อาจจะต้องพิจารณาคือการคุ้มครองรักษาความเป็นส่วนตัวในประเทศซึ่งมีข้อมูลส่วนบุคคลนั้นจัดเก็บอยู่ เมื่อเปรียบเทียบกับประเทศอื่นๆ	**ลูกค้า:** ลูกค้าสามารถเลือกรีเจี้ยนเดียวหรือหลายแห่งของ AWS ที่จะใช้จัดเก็บเนื้อหาของลูกค้าและสามารถที่จะใช้บริการของ AWS ในรีเจี้ยนเพียงแห่งเดียวก็ได้ ทั้งนี้ บริการของ AWS นั้นจัดทำขึ้นเพื่อที่ลูกค้าจะยังคงสามารถควบคุมเนื้อหาของลูกค้าได้อย่างมีประสิทธิภาพโดยไม่ต้องคำนึงว่าลูกค้าจะใช้รีเจี้ยนใดในการจัดเก็บเนื้อหา ลูกค้าควรพิจารณาว่าจะเปิดเผยให้บุคคลที่เป็นเจ้าของข้อมูลได้รับทราบถึงที่ตั้งที่ใช้ในการจัดเก็บหรือประมวลข้อมูลส่วนบุคคลหรือไม่ และในกรณีที่จำเป็น ลูกค้าจะต้องได้รับความยินยอมให้ใช้พื้นที่ดังกล่าวในการจัดเก็บประมวลข้อมูลจากบุคคลที่เกี่ยวข้อง ในระหว่างลูกค้าและ AWS นั้น ลูกค้าคือผู้ที่มีความสัมพันธ์กับบุคคลที่ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลซึ่งลูกค้าได้มีการจัดเก็บเอาไว้ใน AWS ดังนั้นลูกค้าจึงควรเป็นผู้ที่จะต้องสื่อสารโดยตรงกับบุคคลดังกล่าวในประเด็นนี้ **AWS:** AWS จะจัดเก็บและประมวลเนื้อหาของลูกค้าแต่ละรายในรีเจี้ยนหนึ่งหรือรีเจี้ยนต่างๆ ของ AWS โดยใช้บริการซึ่งลูกค้าเลือกเท่านั้น และ AWS จะไม่เคลื่อนย้ายเนื้อหาของลูกค้าโดยมิได้รับความยินยอมจากลูกค้าเสียก่อน ยกเว้นในกรณีที่กฎหมายกำหนด

ขั้นตอนของวงจรชีวิตข้อมูล	คำอธิบายโดยย่อและตัวอย่าง	ประเด็นที่ต้องพิจารณา
		หากลูกค้าเลือกที่จะจัดเก็บเนื้อหาในมากกว่าหนึ่งรีเจี้ยนหรือให้มีการทำสำเนา หรือให้มีการเคลื่อนย้ายเนื้อหาระหว่างรีเจี้ยนนั้นก็คือสิ่งที่ลูกค้าสามารถเลือกได้ โดยที่ลูกค้าจะยังคงควบคุมเนื้อหาได้อย่างมีประสิทธิภาพต่อไปไม่ว่าเนื้อหานั้นจะได้มีการจัดเก็บและประมวลผลที่ใดก็ตาม **ทั่วไป:** AWS ได้รับการรับรองโดย ISO 27001[21] และได้จัดให้มีการคุ้มครองความปลอดภัยที่รัดกุมให้กับลูกค้าทุกรายไม่ว่าจะได้มีการจัดเก็บเนื้อหาของลูกค้าอยู่ในภูมิภาคทางภูมิศาสตร์ที่ใดก็ตาม
การรักษาความปลอดภัยของข้อมูลส่วนบุคคล	การดำเนินการคุ้มครองการรักษาความปลอดภัยของข้อมูลส่วนบุคคลเป็นสิ่งสำคัญ	**ลูกค้า:** ลูกค้าเป็นผู้รับผิดชอบในการรักษาความปลอดภัย*ภายใน*ระบบคลาวด์ รวมไปถึงการรักษาความปลอดภัยเนื้อหาของตน (และข้อมูลส่วนบุคคลที่รวมอยู่ในเนื้อหาของตน) **AWS:** AWS เป็นผู้รับผิดชอบในการจัดการความปลอดภัย*ของ*ระบบคลาวด์ สำหรับรายการมาตรการความปลอดภัยซึ่งถูกกำหนดและสร้างขึ้นให้เป็นหัวใจสำคัญของโครงสร้างพื้นฐานและบริการระบบคลาวด์ของ AWS นั้น โปรดอ่านสมุดปกขาวของบริษัทเรื่องภาพรวมของขั้นตอนการรักษาความปลอดภัย (Overview of Security Processes)[22] ทั้งนี้ ลูกค้าสามารถที่จะตรวจสอบการควบคุมความปลอดภัยที่มีอยู่ของ AWS ผ่านหนังสือรับรองและรายงานของ AWS รวมไปถึงรายงานการควบคุมระบบและองค์กร (AWS System & Organization Control: SOC) ของ AWS รายงานฉบับที่ 1 ฉบับที่ 2[23] และฉบับที่ 3[24] มาตรฐาน ISO 27001[25] 27017[26] 27018[27] ตลอดจนรายงานการปฏิบัติตาม PCI DSS[28]
การเข้าถึงและการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง	บุคคล (เจ้าของข้อมูลส่วนบุคคล) อาจมีความจำเป็นที่จะเข้าถึงข้อมูลส่วนบุคคล รวมไปถึงเพื่อการแก้ไขข้อมูลให้ถูกต้องก็ได้	**ลูกค้า**: ลูกค้าจะยังคงเป็นผู้ควบคุมเนื้อหาที่ได้จัดเก็บและประมวลโดยใช้บริการของ AWS รวมไปถึงการควบคุมการรักษาความปลอดภัย และการเข้าถึงและเปลี่ยนแปลงเนื้อหาดังกล่าวนั้น นอกจากนี้ ในระหว่างลูกค้าและ AWS นั้น ลูกค้าเป็นผู้ที่มีความสัมพันธ์กับบุคคลผู้ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ได้รวมอยู่ในเนื้อหาของลูกค้าที่จะจัดเก็บและประมวลผลโดยใช้บริการของ AWS ดังนั้น ลูกค้าจึงเป็นผู้ที่เหมาะสมที่จะประสานกับ

21 http://aws.amazon.com/compliance/iso-27001-faqs/

22 https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

23 http://aws.amazon.com/compliance/soc-faqs/

24 http://d0.awsstatic.com/whitepapers/compliance/soc3_amazon_web_services.pdf

25 http://aws.amazon.com/compliance/iso-27001-faqs/

26 http://aws.amazon.com/compliance/iso-27017-faqs/

27 http://aws.amazon.com/compliance/iso-27018-faqs/

28 https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

ขั้นตอนของวงจรชีวิตข้อมูล	คำอธิบายโดยย่อและตัวอย่าง	ประเด็นที่ต้องพิจารณา
		บุคคลดังกล่าวเพื่ออนุญาตให้มีการเข้าถึง หรือแก้ไขข้อมูลส่วนบุคคลซึ่งรวมอยู่ในเนื้อหาของลูกค้าได้ **AWS**: AWS จะใช้เนื้อหาของลูกค้าเพื่อให้บริการ AWS ซึ่งเลือกโดยลูกค้าแต่ละรายให้กับตนเองเท่านั้น และ AWS จะไม่ติดต่อกับบุคคลผู้ซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลซึ่งรวมอยู่ในเนื้อหาของลูกค้าที่ได้มีการจัดเก็บและประมวลผลโดยใช้บริการของ AWS ด้วยเหตุนี้และจากระดับความควบคุมที่ลูกค้ามีต่อเนื้อหาของลูกค้า ทำให้ AWS ไม่จำเป็นและในกรณีนี้ไม่สามารถที่จะอนุญาตให้บุคคลภายนอกสามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงในข้อมูลส่วนบุคคลได้
การรักษาคุณภาพของข้อมูลส่วนบุคคล	การสร้างความมั่นใจว่าข้อมูลส่วนบุคคลนั้นมีความแม่นยำเป็นสิ่งสำคัญ และจะต้องรักษาความถูกต้องสมบูรณ์ของข้อมูลเอาไว้	**ลูกค้า:** เมื่อลูกค้าเลือกที่จะจัดเก็บหรือประมวลผลเนื้อหาซึ่งรวมข้อมูลส่วนบุคคลโดยใช้บริการของ AWS ลูกค้าสามารถควบคุมคุณภาพของเนื้อหาและยังเป็นผู้ควบคุมการเข้าถึงและการแก้ไขเนื้อหาให้ถูกต้องได้อยู่ นั่นหมายความว่าลูกค้าจะต้องทำตามขั้นตอนที่จำเป็นเพื่อที่จะสร้างความมั่นใจว่าข้อมูลส่วนบุคคลที่รวมอยู่ในเนื้อหาของลูกค้านั้นจะมีความแม่นยำสมบูรณ์และไม่สร้างความสับสน รวมไปถึงการทำข้อมูลให้เป็นปัจจุบันด้วย **AWS**: รายงาน AWS SOC 1 ประเภทที่ 2 มีการควบคุมซึ่งได้มีการรับประกันว่าจะรักษาความถูกต้องสมบูรณ์ของข้อมูลเอาไว้ในทุกๆ ขั้นตอนรวมไปถึงการถ่ายโอน การเก็บรักษา และการประมวลผลข้อมูลในระดับที่สมเหตุสมผล
การลบทิ้งหรือการแยกการระบุอัตลักษณ์ออกจากข้อมูลส่วนบุคคล	โดยปกติข้อมูลส่วนบุคคลจะต้องไม่ถูกเก็บนานกว่าที่กำหนดเอาไว้ตามวัตถุประสงค์ของการจัดเก็บข้อมูล และให้เป็นไปตามกฎหมายกำกับการเก็บข้อมูล	**ลูกค้า:** มีเพียงลูกค้าเท่านั้นที่ทราบเหตุผลในการจัดเก็บข้อมูลส่วนบุคคลที่รวมอยู่ในเนื้อหาของลูกค้าที่เก็บอยู่ใน AWS และมีเพียงลูกค้าที่ทราบว่าเมื่อไหร่ที่ไม่จำเป็นที่จะต้องเก็บข้อมูลส่วนบุคคลนั้นตามกำหนดกฎหมายอีกต่อไป โดยลูกค้าควรที่จะลบทิ้งหรือไม่ระบุอัตลักษณ์ข้อมูลส่วนบุคคลเมื่อไม่จำเป็นต้องใช้แล้ว **AWS:** บริการของ AWS ให้ลูกค้าสามารถควบคุมการที่จะลบเนื้อหาทิ้ง ตามที่ได้อธิบายไว้ใน<u>เอกสาร AWS Documentation</u>[29]

[29] https://aws.amazon.com/documentation/

การละเมิดความเป็นส่วนตัว

จากการที่ลูกค้าจะยังคงเป็นผู้ควบคุมเนื้อหาเมื่อใช้บริการของ AWS ดังนั้นแล้ว ลูกค้าจึงมีหน้าที่ที่จะต้องตรวจสอบการละเมิดความเป็นส่วนตัวในพื้นที่ของตนเองและจะต้องแจ้งหน่วยงานกำกับดูแลและบุคคลที่ได้รับผลกระทบตามที่กำหนดเอาไว้ภายใต้กฎหมายที่บังคับใช้ โดยลูกค้าเป็นผู้เดียวเท่านั้นที่จะสามารถรับผิดชอบหน้าที่นี้

การเข้ารหัส AWS ของลูกค้านั้นเป็นตัวอย่างที่ชัดเจนในการอธิบายว่าทำไมลูกค้าจึงเป็นผู้ที่อยู่ในตำแหน่งที่ดีกว่า AWS ในการที่จะรับผิดชอบหน้าที่ดังกล่าว

ลูกค้าเป็นผู้ควบคุมการเข้ารหัสและกำหนดว่าใครที่จะได้รับอนุญาตให้เข้าถึงบัญชี AWS ของตนได้ ทั้งนี้ AWS ไม่สามารถทราบรหัสลับ หรือทราบว่าใครได้รับอนุญาต หรือใครไม่ได้รับอนุญาตให้เข้าถึงบัญชีได้ ดังนั้น จึงเป็นหน้าที่ความรับผิดชอบของลูกค้าในการที่จะตรวจสอบการใช้ การใช้ในทางที่ไม่ชอบ การเผยแพร่รหัสลับ หรือการทำรหัสลับหาย

ในบางเขตอำนาจของประเทศต่างๆ มีการกำหนดบังคับให้แจ้งบุคคลหรือหน่วยงานกำกับดูแลในกรณีที่มีการเข้าถึงโดยไม่ได้รับอนุญาต หรือการเปิดเผยข้อมูลส่วนบุคคล และมีบางสถานการณ์ที่การแจ้งเตือนให้บุคคลรับทราบเป็นวิธีที่จะลดความเสี่ยงที่ดีที่สุดถึงแม้จะมิได้เป็นข้อบังคับตามกฎหมายก็ตาม ทั้งนี้ ลูกค้าจะต้องเป็นผู้ประเมินว่าเมื่อใดที่เหมาะสมหรือจำเป็นที่จะแจ้งต่อบุคคลดังกล่าวและกระบวนการที่จะต้องดำเนินการในการแจ้งเตือน

ประเด็นอื่นๆ

สมุดปกขาวนี้ไม่ได้ระบุถึงกฎหมายว่าด้วยการรักษาความเป็นส่วนตัวหรือการคุ้มครองข้อมูลฉบับใดฉบับหนึ่งโดยเฉพาะ ลูกค้าจึงควรพิจารณาข้อกำหนดที่เป็นการเฉพาะซึ่งต้องปรับใช้กับตน รวมไปถึงข้อกำหนดเฉพาะทางธุรกิจต่างๆ กฎหมายและระเบียบที่เกี่ยวกับการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลที่บังคับใช้กับลูกค้านั้นจะขึ้นอยู่กับปัจจัยต่างๆ รวมไปถึงสถานประกอบธุรกิจของลูกค้า ประเภทธุรกิจที่ดำเนินการ ประเภทของเนื้อหาที่ลูกค้าประสงค์ที่จะจัดเก็บ เนื้อหานั้นมาจากที่ใดและจากใคร และเนื้อหานั้นจะได้ทำการจัดเก็บที่ไหน

ลูกค้าที่มีความกังวลเกี่ยวกับหน้าที่การรักษาความเป็นส่วนตัวตามกฎหมายควรที่จะศึกษาและทำความเข้าใจข้อกำหนดต่างๆ ซึ่งมีผลบังคับใช้กับตนและหาคำแนะนำที่เหมาะสม

ส่วนท้ายของเนื้อหานี้

สำหรับ AWS แล้ว การรักษาความปลอดภัยเป็นสิ่งที่ AWS ให้ความสำคัญที่สุด AWS ให้บริการกับลูกค้านับล้านราย รวมไปถึงบริษัทต่างๆ สถาบันการศึกษาและหน่วยงานของรัฐในมากกว่า 190 ประเทศ นอกจากนี้ ลูกค้าของ AWS ยังรวมไปถึงผู้ให้บริการทางการเงินและผู้ให้บริการสาธารณสุขซึ่งให้ความไว้วางใจAWS ให้ดูแลข้อมูลที่มีความละเอียดอ่อนที่สุด

บริการ AWS ออกแบบขึ้นเพื่อให้ลูกค้ามีความยืดหยุ่นในการที่จะกำหนดและใช้ตามความประสงค์ของตน การควบคุมเนื้อหาของตน รวมไปถึงการเลือกว่าจะจัดเก็บที่ไหนและจัดเก็บอย่างไร และใครสามารถเข้าถึงได้บ้าง ลูกค้าของ AWS สามารถที่จะสร้างการใช้และการจัดเก็บเนื้อหาที่มีความปลอดภัยอยู่ใน AWS ได้ด้วยตนเอง

ข้อมูลเพิ่มเติม

เพื่อช่วยให้ลูกค้าสามารถเข้าใจเพิ่มเติมว่าจะรับมือกับข้อกำหนดเกี่ยวกับการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลได้อย่างไรนั้น ลูกค้าสามารถที่จะอ่านสมุดปกขาวว่าด้วยความเสี่ยง การปฏิบัติตาม และการรักษาความปลอดภัย แนวปฏิบัติที่เป็นเลิศ รายการตรวจสอบและแนวทางซึ่งบริษัทรวบรวมและเผยแพร่ไว้ในเว็บไซต์ของ AWS เอกสารเหล่านี้สามารถพบได้ที่ http://aws.amazon.com/compliance และ http://aws.amazon.com/security.

ณ วันที่ได้เผยแพร่เอกสารฉบับนี้ AWS ยังมีสมุดปกขาวเกี่ยวกับการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลของประเทศและภูมิภาคดังต่อไปนี้:

- สหภาพยุโรป [30]
- เยอรมัน[31]
- ออสเตรเลีย[32]
- ฮ่องกง[33]
- ญี่ปุ่น[34]
- มาเลเซีย[35]
- นิวซีแลนด์[36]
- ฟิลิปปินส์[37]
- สิงคโปร์[38]

อ่านเพิ่มเติม

AWS ยังได้จัดให้มีการฝึกอบรมเพื่อช่วยให้ลูกค้าสามารถที่จะเรียนรู้การออกแบบพัฒนาและการใช้งาน AWS ในระบบคลาวด์ให้มีประสิทธิภาพ ปลอดภัยและพร้อมใช้งาน และเพิ่มพูนความเชี่ยวชาญในการใช้บริการของ AWS ทางบริษัทยังได้จัดให้มีวีดีโอคู่มือการสอน[39] แล็บแบบเรียนรู้ด้วยตนเอง[40] และห้องเรียนที่มีผู้สอน[41] ทั้งนี้สามารถศึกษาข้อมูลเพิ่มเติมเกี่ยวกับการฝึกอบรมของ AWS ได้ที่: http://aws.amazon.com/training/

ใบรับรองของ AWS เป็นการรับรองถึงทักษะและความรู้ทางเทคนิคที่เป็นเลิศในการใช้เทคโนโลยีของ AWS เพื่อสร้างแอพพลิเคชั่นบนคลาวด์ที่ปลอดภัยและเชื่อถือได้ ทั้งนี้ ข้อมูลเพิ่มเติมเกี่ยวกับการรับรองของ AWS นั้นจะมีอยู่ที่: http://aws.amazon.com/certification/ หากท่านประสงค์จะขอรับข้อมูลเพิ่มเติมโปรดติดต่อ AWS ที่: https://aws.amazon.com/contact-us/ หรือติดต่อผู้แทน AWS ซึ่งรับผิดชอบบัญชีของท่าน

---

30 https://d1.awsstatic.com/whitepapers/compliance/AWS_EU_Data_Protection_Whitepaper.pdf

31 https://d1.awsstatic.com/whitepapers/compliance/German_Data_Protection_Whitepaper.pdf

32 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf

33 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Hong_Kong_Privacy_Considerations.pdf

34 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Japanese_Privacy_Considerations.pdf

35 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Malaysian_Privacy_Considerations.pdf

36 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf

37 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Philippines_Privacy_Considerations.pdf

38 https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Singapore_Privacy_Considerations.pdf

39 https://www.aws.training/

40 https://aws.amazon.com/training/self-paced-labs/

41 https://aws.amazon.com/training/course-descriptions/

รายการแก้ไขปรับปรุงของเอกสาร

วันที่	รายละเอียด
กันยายน พ.ศ. **2559**	การตีพิมพ์ครั้งที่ 1
ธันวาคม พ.ศ. **2559**	การตีพิมพ์ครั้งที่ 2
กุมภาพันธ์ พ.ศ. **2561**	การตีพิมพ์ครั้งที่ 3
พฤษภาคม พ.ศ. **2561**	การตีพิมพ์ครั้งที่ 4