ประเด็นคำถามการจัดเก็บข้อมูลจราจรบนโครงข่ายโทรศัพท์เคลื่อนที่

คำตอบจากดีแทค

1. ข้อมูลของผู้ใช้บริการและข้อมูลจราจรบนโครงข่ายโทรศัพท์เคลื่อนที่ที่บริษัทฯ มีไว้ในครอบครอง หรือควบคุมดูแลมีกี่ประเภท ปริมาณข้อมูล สถานที่จัดเก็บ (เช่น รวมศูนย์หรือกระจาย) เทคโนโลยีในการจัดเก็บ จัดเก็บรักษาในรูปแบบไหน (เช่น รูปแบบที่คนอ่านได้หรือคอมพิวเตอร์อ่านได้เท่านั้น) มาตรการการรักษาความปลอดภัยเป็นอย่างไร (เช่น ความยากง่ายการเข้าถึงข้อมูล การใช้หรือแชร์ข้อมูลภายในบริษัทหรือบุคคลภายนอก หรือการเข้ารหัสหรือไม่ อย่างไร) ต้นทุน/ค่าใช้จ่ายในการเก็บรักษา และปัจจุบันมีปัญหา/อุปสรรคอย่างไรในการเก็บรักษาข้อมูลดังกล่าว

คำตอบ:

ข้อมูลจราจรจะเป็นตามประเภทที่ประกาศ กสทช กำหนด เช่น ข้อมูลดังต่อไปนี้

No.	ชนิดของข้อมูล	รวมศูนย์/หรือกระจาย	เก็บอยู่ในรูปแบบที่คนอื่นได้ หรือคอมพิวเตอร์อ่านได้เท่านั้น
1	ข้อมูลการขอจดทะเบียนผู้ใช้โทรศัพท์เคลื่นที่ (Subscriber Profile)	รวมศูนย์	ข้อมูลถูกจัดเก็บใน database ที่ต้องใช้ คอมพิวเตอร์อ่านเท่านั้น
2	ข้อมูลโทรออก/รับสาย , SMS (CDR)	รวมศูนย์	ข้อมูลถูกจัดเก็บใน database ที่ต้องใช้ คอมพิวเตอร์อ่านเท่านั้น
3	ข้อมูลระบุตำแหน่ง (Location Update)	รวมศูนย์	ข้อมูลถูกจัดเก็บใน database ที่ต้องใช้ คอมพิวเตอร์อ่านเท่านั้น
4	ข้อมูลการ mapping ระหว่าง เบอร์โทร และ IP Address	รวมศูนย์	ข้อมูลถูกจัดเก็บใน database ที่ต้องใช้ คอมพิวเตอร์อ่านเท่านั้น

การเข้าถึงข้อมูล จะสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบนั้นๆ เท่านั้น และการจะเข้าถึง Server ที่เก็บข้อมูลนั้น จะต้องเข้าผ่าน VPN เข้ามายัง Private Network ของบริษัทฯ ซึ่งต้องใช้ 2 factors authentication นอกจากนี้ หลังจาก VPN เข้ามาแล้ว ยังจะต้องมา Login เข้าเครื่อง “Jump host” ซึ่งเป็นเครื่องตัวกลางที่จะ Login ไปยังเครื่อง Server ปลายทางอีกครั้ง ไม่สามารถ login ได้โดยตรงผ่านช่องทาง Internet ปกติทั่วไป

ปัจจุบันยังไม่มีปัญหา หรืออุปสรรคในการเก็บรักษาข้อมูลดังกล่าว

2. บริษัทฯ มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบริษัทฯ อย่างไร และมีความพร้อมในการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และประกาศของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งกฎหมายอื่นๆ ที่เกี่ยวข้องหรือไม่อย่างไร

คำตอบ:

บริษัทฯ มีความพร้อมในการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และมีระบบรองรับเรียบร้อยแล้ว ทั้งนี้ บริษัทฯ จะให้ความคุ้มครองข้อมูลส่วนบุคคลของทั้งลูกค้า และพนักงานบนพื้นฐานหลักการดังต่อไปนี้

- ความโปร่งใส (Transparency): มีกระบวนการและเนื้อหาที่ชัดเจนให้ลูกค้าเข้าใจทั้งในสัญญา แบบฟอร์มขอความยินยอม และประกาศข้อมูลส่วนบุคคล
- การนำไปใช้อย่างถูกต้องตามกฎหมาย (Lawful-use of personal data): การใช้ข้อมูลส่วนบุคคลจะต้องอยู่ภายใต้กรอบที่แจ้งแก่ลูกค้า หรือที่ลูกค้ายินยอมเห็นชอบ และนำไปใช้เท่าที่จำเป็นเท่านั้น
- รับผิดชอบ (Accountability): พนักงานบริษัทฯ ได้รับการอบรมเรื่องข้อมูลส่วนบุคคล และหากกระทำผิด จะต้องรับผิดชอบ และรับโทษตามที่บริษัทฯ หรือกฎหมายกำหนด

3. ที่ผ่านมามีการเจาะระบบ หรือเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบกฎหมายด้วยหรือไม่ ไม่ว่าจะเกิดจากบุคคลภายนอก หรือพนักงานของบริษัทฯ เอง หากมี บริษัทฯ มีมาตรการดำเนินการอย่างไร และแก้ไขเยียวยาผู้เสียหายอย่างไร

คำตอบ:

- การเจาะระบบจากภายนอก: เคยมีความพยามยามหลายครั้งจากพวก Hacker แต่ไม่ประสบความสำเร็จ เหตุผลคือ บริษัทฯ มีมาตรฐานการป้องกันที่ดี มีการสอดส่องตลอด 24 ชั่วโมง ดังนั้น หากเกิดความพยายามใดๆ ในการเจาะระบบจากภายนอกขึ้น บริษัทฯ สามารถรับรู้ได้อย่างรวดเร็ว และมีเวลาเพียงพอในการป้องกันได้
- การเจาะระบบจากภายใน: เคยมีการเจาะระบบจากบุคคลภายใน แต่เป็นกรณีเล็กๆ หรือเรื่องส่วนตัว ไม่กระทบลูกค้าในภาพรวม ที่ผ่านมาบริษัทฯ สามารถพบเจอกรณีเหล่านี้ได้อย่าวรวดเร็ว และสามารถป้องกันได้ตั้งแต่เบื้องต้น

4. บริษัทฯ มีการจัดเก็บข้อมูล และสถิติเกี่ยวกับการร้องขอเข้าถึง และใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการ และข้อมูลจราจรบนโครงข่ายโทรศัพท์เคลื่อนที่โดยหน่วยงาน หรือเจ้าหน้าที่ของรัฐหรือไม่ อย่างไร

4.1 จำแนกประเภทและปริมาณของข้อมูลที่ถูกร้องขอ

4.2 จำแนกประเภทและปริมาณการร้องขอของหน่วยงานรัฐ

4.3 หลักเกณฑ์การร้องขอ และเงื่อนไขการใช้ข้อมูลเพื่อคุ้มครองสิทธิเสรีภาพของผู้ใช้บริการ

4.4 มีการเก็บค่าให้บริการข้อมูลหรือไม่

4.5 รูปแบบของข้อมูลที่ให้พนักงานเจ้าหน้าที่ เช่นกระดาษ หรือไฟล์อิเล็กทรอนิกส์ หรือข้อมูลดังกล่าวต้องมีการแปลความ หรือถอดรหัสหรือไม่

4.6 พนักงานของบริษัทฯ ต้องให้การเป็นพยานหรือไม่ เพื่อยืนยันความถูกต้องแท้จริงของข้อมูล

4.7 ปัญหาและอุปสรรคในการให้บริการข้อมูล เช่น ขอข้อมูลแบบกว้างไม่เฉพาะเจาะจง ให้ปริ๊นข้อมูลในรูปของกระดาษ

คำตอบ:

4.1 ข้อมูลส่วนบุคคลที่ถูกร้องขอจะมีประมาณเดือนละ 500-900 ครั้ง และข้อมูลอื่นๆ เดือนละ 100-300 ครั้ง

4.2 มีหลากหลายประเภทที่ถูกร้องขอ เช่น ให้ Take Down เว็บไซต์ ให้ส่งข่าวประชาสัมพันธ์ เป็นต้น

4.3 ต้องเป็นหน่วยงานของรัฐ ต้องมีพื้นฐานทางกฎหมาย ให้เท่าที่จำเป็น และในสัดส่วนที่สมเหตุสมผล

4.4 ไม่มีการเก็บค่าให้บริการข้อมูล

4.5 รูปแบบของข้อมูลที่ให้มีทั้งเป็นรูปของกระดาษ และไฟล์อิเล็กทรอนิคส์ หลักการของบริษัทฯ เวลาให้ข้อมูลคือ บริษัทฯ จะตั้งรหัสในการเข้าถึงไว้เสมอ

4.6 พนักงานของบริษัทฯ จะไปเป็นพยานบ้างเป็นครั้งคราวถ้าเป็นกรณีที่พนักงานสอบสวนนำข้อมูลที่ขอเข้าสำนวน และอัยการพิจารณาว่ามีประเด็น

4.7 ปัญหาและอุปสรรคในการให้บริการข้อมูล เช่น ไม่ระบุช่วงเวลาของข้อมูลที่ต้องการให้ชัดเจน มีการขอโดยเจ้าหน้าที่รัฐก็จริงแต่ใช้อีเมล์ส่วนตัว ข้อมูลที่ขอมีมากเกินจำเป็น ข้อมูลที่ขอไม่ชัดเจน

5. บริษัทฯ มีความเห็นเกี่ยวกับการปฏิบัติตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจ และสังคม เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พศ 2464 หรือไม่ อย่างไร มีปัญหา/อุปสรรคในการดำเนินการตามหลักเกณฑ์ดังกล่าวในข้อใด เหตุผลใด และมีข้อเสนอแนะอย่างไร

คำตอบ:

ความเห็นในเบื้องต้น เช่น

- หลักเกณฑ์ฉบับนี้จะทำให้เกิดค่าใช้จ่าย (เช่น การเพิ่มพื้นที่ในการจัดเก็บข้อมูล) และต้องใช้ทรัพยากรมาดูแลในส่วนนี้มากขึ้น (เช่น การขยายระยะเวลาในการจัดเก็บข้อมูลในมาตรา 12 ของหลักเกณฑ์ฉบับนี้ให้นานขึ้นกว่าปกติ)
- ประเด็นบางเรื่องมีความไม่ชัดเจน เช่น หลักการทางกฎหมายในการต้องขอ หรือให้ข้อมูล
- หลักเกณฑ์ฉบับนี้อาจนำมาซึ่งปัญหาอื่นๆ ตามมากับทั้งประชาชน และตัวผู้ประกอบการ เช่น ความเสี่ยงที่ประชาชนจะร้องเรียนว่าเป็นการละเมิดสิทธิข้อมูลส่วนบุคคลของผู้ใช้บริการ

6. บริษัทฯ เคยมีการปฏิเสธ หรือไม่ให้ข้อมูลแก่เจ้าหน้าที่หรือไม่ ด้วยเหตุผลอะไร

คำตอบ:

เคยมี เหตุผลที่ปฏิเสธ เช่น ไม่มีพื้นฐานหรือเหตุผลทางกฎหมาย ขอข้อมูลที่ย้อนหลังเกินเวลาที่จัดเก็บ การร้องขอข้อมูลด้วยวาจาไม่มีหลักฐานเป็นหนังสือ ขอข้อมูลที่บริษัทฯ ไม่สามารถให้ได้เช่น ข้อมูลที่อยู่บนระบบของ Social Media ต่างๆ

7. บริษัทฯ มีการแยกระดับการเข้าถึงข้อมูลในแต่ละระดับชั้นข้อมูลหรือไม่ อย่างไร และมีการตรวจสอบการเข้าถึงข้อมูลเพียงใด

คำตอบ:

บริษัทฯ มีการแยกระดับการเข้าถึงข้อมูลตั้งแต่ Confidential, Internal และ Open และแต่ละระดับจะมีข้อจำกัด และการเข้าถึงไม่เท่ากัน แตกต่างกันตามตำแหน่ง หน้าที่ และความรับผิดชอบของพนักงานที่เกี่ยวข้องกับข้อมูลนั้นๆ

นอกจากนี้ บริษัทฯ ก็มีมาตรการการตรวจสอบการเข้าถึงข้อมูลด้วยเช่นกัน เช่น มีการตรวจ Log Monitoring ว่าเข้ามาดูข้อมูลบ่อยแค่ไหน สมควรกับงาน หรือหน้าที่ความรับผิดชอบในงานที่ต้องเข้ามาดูข้อมูลนั้นๆ หรือไม่ และมีการใช้เครื่องมือ Activity Trail เพื่อดูว่าพนักงานเข้ามาดูข้อมูลเชิงลึกเพียงใด และข้อมูลเชิงลึกนั้นจำเป็นกับงาน หรือหน้าที่ความรับผิดชอบในงานนั้นหรือไม่ เป็นต้น

ที่ TRUE/REG/022/2564

วันที่ 15 ตุลาคม 2564

เรื่อง นำส่งสถิติข้อมูลจราจรทางคอมพิวเตอร์ที่นำส่งแก่หน่วยงานรัฐ และข้อคิดเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

เรียน ประธานคณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภา

อ้างถึง หนังสือคณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภา ที่ สว(กมธ 1) 0009/02546 ลงวันที่ 16 กันยายน 2564

สิ่งที่ส่งมาด้วย สถิติข้อมูลจราจรทางคอมพิวเตอร์ และข้อคิดเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

ตามที่ คณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภา (คณะกรรมาธิการ) ได้มีหนังสือเชิญบริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) (บริษัทฯ) เข้าร่วมประชุมเมื่อวันที่ 28 กันยายน 2564 เพื่อให้ข้อมูลเกี่ยวกับแนวทางการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ รวมทั้งปัญหาอุปสรรคในการดำเนินการตามประกาศรัฐมนตรี ตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และเรื่องอื่นๆ ที่เกี่ยวข้อง ความละเอียดตามหนังสือที่อ้างถึง ซึ่งในการประชุมร่วมกันดังกล่าวผู้แทนของบริษัทฯ ได้ชี้แจงข้อมูลที่เกี่ยวข้องให้ที่ประชุมรับทราบในเบื้องต้นตามประเด็นที่ปรากฏในหนังสือที่อ้างถึงแล้ว โดยคณะกรรมาธิการได้แจ้งให้บริษัทฯ นำส่งสถิติข้อมูลจราจรทางคอมพิวเตอร์ที่นำส่งแก่หน่วยงานรัฐ และข้อคิดเห็นต่อกฎหมายอื่นๆ ที่เกี่ยวข้องเพิ่มเติม นั้น

ในการนี้ บริษัทฯ ขอนำส่งสถิติข้อมูลจราจรทางคอมพิวเตอร์ที่นำส่งแก่หน่วยงานรัฐ และข้อคิดเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(วิทยา อลงกต)
บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน)

ติดต่อประสานงาน: ปุณยนุช คุณนิธิวุฒิ โทรศัพท์ : 0863641670

สถิติข้อมูลจราจรทางคอมพิวเตอร์ที่ บริษัทฯ นำส่งแก่หน่วยงานรัฐ

ปี 2562 จำนวนสถิติที่นำส่ง 1485 เคส
ปี 2563 จำนวนสถิติที่นำส่ง 1929 เคส

เอกสารแสดงข้อคิดเห็นต่อพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

โดย บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทในเครือ ("บริษัทฯ")

ส่วนที่ 1 ข้อคิดเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1.1 ความเป็นมาและเหตุผล

กฎหมายคุ้มครองข้อมูลส่วนบุคคลมีพื้นฐานจากปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights) เรื่องสิทธิและเสรีภาพของบุคคลอันเกี่ยวกับความเป็นส่วนตัว ซึ่งหลักการดังกล่าวได้มีการรับรองไว้ในบทบัญญัติมาตรา 32 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 โดยมีใจความว่า การนำข้อมูลส่วนบุคคลไปใช้ประโยชน์จะกระทำมิได้เว้นแต่จะอาศัยอำนาจบทบัญญัติของกฎหมายที่ตราขึ้นเท่าที่จำเป็นต่อประโยชน์สาธารณะ ด้วยเหตุนี้ จึงมีการจัดทำและตราพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ("พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ") ขึ้นเพื่อกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไป

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มีบทบาทสำคัญอย่างยิ่งในการปกป้องและคุ้มครองเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในความเป็นส่วนตัวและการนำข้อมูลไปใช้ประโยชน์โดยไม่ชอบ รวมทั้งลดความเสี่ยงต่อความเสียหายอันเนื่องมาจากการถูกละเมิดสิทธิดังกล่าว โดยเฉพาะอย่างยิ่งในยุคสมัยที่มีการนำเทคโนโลยีมาประยุกต์ใช้เพื่อกิจกรรมในชีวิตประจำวัน ซึ่งทำให้เกิดการนำเข้าและไหลเวียนของข้อมูลส่วนบุคคลในระบบที่มากขึ้นอย่างมีนัยสำคัญ อันอาจก่อให้เกิดผลกระทบที่ร้ายแรงต่อตัวเจ้าของข้อมูลส่วนบุคคลได้

บริษัทฯ ตระหนักถึงความสำคัญของหลักการและกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างยิ่ง อีกทั้งเห็นว่าเป็นโอกาสอันดีที่บริษัทฯจะสร้างธรรมาภิบาลด้านการประมวลผลข้อมูลส่วนบุคคลเพื่อปฏิบัติการให้สอดคล้องกับหลักการและข้อกำหนดตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ด้วยปัจจุบันพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เว้นแต่บทบัญญัติในหมวด 2 หมวด 3 หมวด 5 หมวด 6 หมวด 7 และความในมาตรา95 และมาตรา 96 ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป โดยได้มีการออกพระราชกฤษฎีกาว่าด้วยการกำหนดหน่วยงานและกิจการที่ผู้ควบคุมข้อมูลส่วนบุคคลไม่อยู่ภายใต้

บังคับแห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 จำนวน 2 ฉบับเพื่อขยายระยะเวลาการมีผลใช้บังคับของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ออกไปเป็นวันที่ 1 มิถุนายน 2564 โดยขณะนี้หน่วยงานที่เกี่ยวข้องยังคงอยู่ในระหว่างกระบวนการจัดทำกฎหมายลำดับรองอีกเป็นจำนวนหลายฉบับจึงได้จัดทำเอกสารแสดงข้อคิดเห็นต่อการดำเนินการภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ฉบับนี้ เสนอต่อคณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภาเพื่อชี้แจงผลกระทบของกฎหมายอันมีนัยสำคัญต่อบริษัทฯรวมไปถึงภาคธุรกิจอื่น รวมทั้งเสนอความคิดเห็นที่อาจเป็นประโยชน์เพื่อให้หน่วยงานที่เกี่ยวข้องพิจารณาตามลำดับ โดยมีเนื้อหาดังต่อไปนี้

1.2 **ผลกระทบและข้อเสนอแนะ**

ประเด็นที่ 1 การบังคับใช้พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ควบคู่ไปกับกฎหมายเฉพาะในแต่ละภาคอุตสาหกรรม

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯมีบทบัญญัติกำหนดเป็นหลักการให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องปฏิบัติตามบทกฎหมายเฉพาะของแต่ละภาคอุตสาหกรรมที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและยังต้องปฏิบัติตามบทบัญญัติของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เป็นการเพิ่มเติมอีกด้วย ซึ่งหน่วยงานควบคุมหรือกำกับดูแลของแต่ละภาคอุตสาหกรรมก็มีอำนาจในการออกประกาศหรือกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้เหมาะสมกับการประกอบธุรกิจและการคุ้มครองข้อมูลส่วนบุคคลในแต่ละภาคส่วน อย่างไรก็ดี ประกาศหรือกฎระเบียบเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ออกโดยหน่วยงานกำกับดูแลก็ไม่ควรมีเนื้อหาและหลักการสำคัญแตกต่างไปจากพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯโดยเฉพาะในส่วนที่เกี่ยวกับฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลหรือสิทธิของเจ้าของข้อมูลส่วนบุคคล เนื่องจากพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้รับหลักการสำคัญจาก General Data Protection Regulation (GDPR) ของสหภาพยุโรป (European Union) ซึ่งถือเป็นกฎหมายมาตรฐานสำคัญของโลกในการคุ้มครองข้อมูลส่วนบุคคลในปัจจุบัน การกำหนดหลักการเฉพาะที่แตกต่างในสาระสำคัญอาจส่งผลกระทบให้เกิดความขัดแย้งทั้งด้านการตีความและการปฏิบัติตามกฎหมาย รวมทั้งอาจทำให้เกิดมาตรฐานที่ไม่สอดคล้องกับหลักการสากลของนานาประเทศ ทั้งนี้ ข้อเท็จจริงปรากฏว่าทุกภาคส่วนต้องมีการลงทุนทั้งในแง่บุคลากร เวลาและเงินลงทุนอย่างมหาศาลเพื่อเตรียมรองรับการมีผลบังคับใช้ของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ให้เป็นมาตรฐานเดียวกัน ดังนั้น จะเป็นภาระแก่ผู้ประกอบการอย่างมากหากแต่ละภาคอุตสาหกรรมจะมีการออกประกาศหรือกฎระเบียบที่มีการกำหนดหลักการแตกต่างไปจากพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

นอกจากนี้ หากหน่วยงานกำกับดูแลประสงค์จะออกประกาศหรือกฎระเบียบที่แตกต่างเป็นการเฉพาะไปจากหลักการของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แล้ว ก็ควรมีข้อกำหนดวิธีปฏิบัติให้หน่วยงานกำกับดูแลจะต้องหารือและขอข้อเสนอแนะจากคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อให้ประกาศหรือกฎระเบียบดังกล่าวเป็นไปในแนวทางเดียวกันกับพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ในฐานะที่เป็นกฎหมายแม่บทและกฎหมายทั่วไปเพื่อการคุ้มครองข้อมูลส่วนบุคคล

ประเด็นที่ 2 การจัดทำร่างกฎหมายลำดับรอง

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ เป็นกฎหมายที่กำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งภายใต้บทบัญญัติของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ได้กำหนดให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่และอำนาจออกประกาศหรือระเบียบเพื่อกำหนดหลักเกณฑ์กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยกำหนดให้ดำเนินการออกระเบียบและประกาศตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ ใช้บังคับ ซึ่งปัจจุบันยังคงอยู่ในระหว่างการจัดทำร่างกฎหมายลำดับรองเป็นจำนวนหลายฉบับ โดยเอกสารการรับฟังความคิดเห็นในการร่างกฎหมายลำดับรองก็ได้จัดทำในรูปแบบของหลักการที่เป็นสาระสำคัญเพื่อนำไปจัดทำเป็นร่างกฎหมายต่อไป ประชาชนและผู้ที่มีส่วนเกี่ยวข้องอาจยังไม่มีความเข้าใจที่ชัดเจนทำให้ไม่สามารถแสดงความคิดเห็นได้อย่างถูกต้อง การรับฟังความคิดเห็นในการตรากฎหมายจากเพียงหลักการอาจยังไม่สามารถรับทราบถึงปัญหาและผลกระทบที่อาจเกิดขึ้นจากกฎหมายได้อย่างรอบคอบและรอบด้าน โดยจะขอยกตัวอย่างประเด็นที่ยังคงไม่มีความชัดเจนตามร่างกฎหมายลำดับรอง อาทิ ข้อยกเว้นเกี่ยวกับการปฏิบัติหน้าที่บางประการตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯหลักเกณฑ์กระบวนการจัดทำข้อมูลนิรนามให้มีผลถือเสมือนเป็นการลบข้อมูลส่วนบุคคล แนวทางการดำเนินการเพื่อพิสูจน์ว่าได้ระงับการใช้ข้อมูลส่วนบุคคลหรือ หน้าที่ในการให้ใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลเป็นต้น ซึ่งประเด็นเหล่านี้มีความสำคัญเป็นอย่างยิ่งต่อการวางแผนโครงสร้างการดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคลของผู้ประกอบการ

นอกจากนั้น กฎหมายลำดับรองที่จะออกบังคับใช้อีกเป็นจำนวนหลายฉบับไม่ควรมีข้อกำหนดในลักษณะที่กำหนดรายละเอียดอย่างเคร่งครัดในทุกกระบวนการ แต่ควรมีข้อกำหนดที่มีความยืดหยุ่นเพื่อให้ผู้ประกอบการสามารถปรับโครงสร้างการดำเนินงานให้สอดคล้องกับกฎหมายได้โดยง่ายเนื่องจากการมีข้อกำหนดที่เคร่งครัดจนเกินไปอาจเป็นการสร้างภาระและไม่เป็นธรรมต่อผู้ประกอบการที่ได้เริ่มปรับปรุงโครงสร้างการดำเนินงานให้สอดคล้องกับหลักการของกฎหมายในภาพรวมเพื่อให้ทันต่อกำหนดการมีผล

บังคับของพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ แต่กลับจำเป็นต้องทำการปรับปรุงกระบวนการใหม่อีกครั้ง เพื่อให้เป็นไปตามความในกฎหมายลำดับรองที่ประกาศออกมาในภายหลัง ดังนั้น เพื่อไม่ให้เป็นการลงทุนที่สูญเปล่า จึงขอเรียนเสนอให้กฎหมายลำดับรองที่จะออกบังคับใช้คำนึงถึงหลักการในภาพรวมและสิ่งที่ผู้ประกอบการได้เริ่มดำเนินการไปแล้ว เพื่อมิให้ก่อให้เกิดภาระที่ผู้ประกอบการจะต้องลงทุนทั้งในส่วนของค่าใช้จ่าย และทรัพยากรอื่นๆ ซ้ำซ้อนเพิ่มขึ้นอีก

ประเด็นที่ 3 การกำหนดโทษทางอาญา

โดยที่ประเทศไทยยังไม่เคยมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยเฉพาะบังคับใช้ และพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ จะเป็นจุดเริ่มต้นการบังคับใช้กฎหมาย ซึ่งถือเป็นช่วงเปลี่ยนผ่านที่ผู้เกี่ยวข้องทุกฝ่ายยังต้องอาศัยการปรับตัวและการทำความเข้าใจ ไม่ว่าจะเป็นผู้บังคับใช้กฎหมายหรือผู้ที่อยู่ภายใต้การบังคับกฎหมาย นอกจากนี้ ยังต้องมีการออกกฎระเบียบที่เป็นกฎหมายลำดับรอง หรือการวางแนวปฏิบัติร่วมกันที่ชัดเจนเพื่อการปฏิบัติตามกฎหมายอย่างถูกต้อง ดังนั้น ตามที่พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ มีการกำหนดบทลงโทษทางอาญาสำหรับการกระทำความผิดตามพระราชบัญญัตินี้ โดยไม่มีการกำหนดบทบัญญัติให้เปรียบเทียบคดีด้วยการชำระค่าปรับได้นั้น จึงอาจเป็นการกำหนดบทลงโทษที่ไม่สอดคล้องกับแนวทางสากลที่กำหนดเพียงโทษปรับเท่านั้น รวมทั้งอาจเป็นการกำหนดบทลงโทษที่ เกินสัดส่วน ด้วยเหตุดังกล่าว บริษัทฯ จึงเสนอให้มีการทบทวนถึงเหตุผล ความจำเป็น และความได้สัดส่วนสำหรับการกำหนดบทลงโทษทางอาญาตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลฯ

ส่วนที่ 2 ข้อคิดเห็นต่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

2.1 ความเป็นมาและเหตุผล

สังคมโลกกำลังก้าวสู่ยุคดิจิทัลอย่างเต็มรูปแบบและไร้พรมแดน การดำเนินชีวิตและกิจกรรมทางเศรษฐกิจและสังคมของประชาชนในประเทศส่วนใหญ่จึงเกิดขึ้นบนเครือข่ายคอมพิวเตอร์ผ่านการสื่อสารโทรคมนาคม ความเสี่ยงในการถูกโจมตีและคุกคามระบบคอมพิวเตอร์จนเกิดความเสียหายต่อความมั่นคงทางเศรษฐกิจและสังคมจึงเพิ่มมากขึ้นและเป็นประเด็นท้าทายของทุกประเทศ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562(“พ.ร.บ. มั่นคงไซเบอร์ฯ”) จึงมีบทบาทสำคัญยิ่งในการรับมือกับภัยคุกคามด้านไซเบอร์

โดย พ.ร.บ. มั่นคงไซเบอร์ฯ กำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรงตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

บริษัทฯ ตระหนักถึงความสำคัญในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามเจตนารมณ์และหลักการที่ตราไว้ในพ.ร.บ. มั่นคงไซเบอร์ฯ อย่างไรก็ดี ด้วยคณะกรรมการและหน่วยงานตาม พ.ร.บ. มั่นคงไซเบอร์ฯ เพิ่งเริ่มก่อตั้ง รวมทั้งกฎหมายลำดับรองก็เริ่มทยอยประกาศ และมีผลใช้บังคับ บริษัทฯ ซึ่งเป็นผู้ให้บริการโทรคมนาคมและเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามกฎหมายฉบับนี้ จึงขอชี้แจงผลกระทบของกฎหมายและนำเสนอความคิดเห็นที่อาจเป็นประโยชน์เพื่อให้หน่วยงานที่เกี่ยวข้องพิจารณา ดังต่อไปนี้

2.2 **ผลกระทบและข้อเสนอแนะ**

ประเด็นที่ 1 ความพิจารณาออกกฎระเบียบต้องคำนึงถึงข้อจำกัดและผลกระทบของหน่วยงานที่เกี่ยวข้อง และควรหลีกเลี่ยงการออกกฎระเบียบที่มีความซ้ำซ้อน

เนื่องจากเครือข่ายโทรคมนาคม ระบบคอมพิวเตอร์ หรือระบบอื่นใด ที่ใช้งานอยู่ในปัจจุบันมีการเชื่อมต่อสื่อสารถึงกันแทบทั้งสิ้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงไม่สามารถดำเนินการได้เพียงลำพัง การแลกเปลี่ยนข้อมูลภัยคุกคามเป็นสิ่งที่ผู้ที่เกี่ยวข้องกับการบริหารจัดการระบบและโครงข่ายดำเนินกันมาโดยตลอด ทั้งนี้ พ.ร.บ. มั่นคงไซเบอร์ฯ จัดเป็นเครื่องมือสำคัญในการสร้างความร่วมมือเตรียมความพร้อม และสร้างกลไกในการบริหารจัดการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับประเทศให้เข้มแข็งยิ่งขึ้น

ด้วยความหลากหลายของหน่วยงานที่เกี่ยวข้องกับภารกิจหรือให้บริการในแต่ละด้านที่อยู่ภายใต้ พ.ร.บ. มั่นคงไซเบอร์ฯ ทั้งหน่วยงานควบคุมหรือกำกับดูแล (Regulator) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ(Sectoral CERT) ต่างมีลักษณะของบริการ และความชำนาญที่แตกต่างกันไปในแต่ละด้าน บริษัทฯ จึงเห็นว่าในการพิจารณาออกกฎระเบียบใดๆ จึงมีความ

จำเป็นต้องคำนึงถึงข้อจำกัดและผลกระทบของหน่วยงานในทุกๆ หน่วยอย่างรอบคอบรอบด้าน เพื่อมิให้เกิดประเด็นปัญหาหรืออุปสรรคในการบังคับใช้ นอกจากนี้ บริษัทฯ ขอเรียนเพิ่มเติมว่าเนื่องจากการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ที่มีประสิทธิภาพไม่อาจดำเนินการหรือสร้างมาตรฐานพิเศษสำหรับภารกิจหรือการให้บริการในด้านในหนึ่งเป็นการเฉพาะ จึงควรหลีกเลี่ยงการออกกฎเกณฑ์หรือกฎระเบียบที่มีความซ้ำซ้อนจากหน่วยงานควบคุมหรือกำกับดูแล(Regulator) ในแต่ละด้านเพิ่มเติมด้วย

ประเด็นที่ 2 การสนับสนุนภาระค่าใช้จ่ายอันเกิดจากการปฏิบัติตามกฎหมาย

ด้วย พ.ร.บ. มั่นคงไซเบอร์ฯ กำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศโดยกำหนดให้มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีหน้าที่การป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งการดำเนินการดังกล่าวมีความจำเป็นต้องใช้งบประมาณ เครื่องมือ และบุคลากรผู้เชี่ยวชาญในการดำเนินการทั้งสิ้น อย่างไรก็ดี สำหรับกรณีหน่วยงานที่มีภารกิจหรือให้บริการในด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ในปัจจุบันมีการกำหนดให้ผู้ให้บริการบางรายเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้น ซึ่งทำให้ผู้ให้บริการดังกล่าวมีภาระหน้าที่เพิ่มเติมจากผู้ให้บริการที่ไม่ได้ถูกกำหนดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บริษัทฯ จึงขอเสนอให้หน่วยงานที่เกี่ยวข้องพิจารณามาตรการช่วยเหลือและสร้างแรงจูงใจ อาทิ มาตรการด้านภาษี มาตรการสนับสนุนงบประมาณ เป็นต้น สำหรับผู้ให้บริการที่ถูกกำหนดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วย นอกจากนี้ บริษัทฯ ขอเสนอให้การพิจารณาแนวทางการสนับสนุนค่าใช้จ่ายในการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์(Sectoral CERT) อย่างต่อเนื่องด้วย

ส่วนที่ 3 ข้อคิดเห็นต่อประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

3.1 ความเป็นมาและเหตุผล

ตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม กำหนดให้ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะ

คราวก็ได้ โดยเบื้องต้นกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ออกประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ที่เป็นการกำหนดหลักเกณฑ์ หน้าที่และรายละเอียดการเก็บข้อมูลจราจร ซึ่งต่อมาเมื่อวันที่ 13 สิงหาคม 2564 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ก็ได้ออกประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ("ประกาศฯ") มาทดแทน โดยการปรับปรุงหลักเกณฑ์ดังกล่าวเป็นไปเพื่อให้การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการให้มีความเหมาะสมกับสภาวะเศรษฐกิจ สังคม และเทคโนโลยีในปัจจุบัน

3.2 ผลกระทบและข้อเสนอแนะ

ประเด็นที่ 1ความไม่ชัดเจนของกฎหมายอันส่งผลต่อการนำไปปฏิบัติ

ด้วยเจตนารมณ์ของการปรับปรุงประกาศฯ เป็นการกำหนดหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการให้มีความเหมาะสมกับสภาวะเศรษฐกิจ สังคม และเทคโนโลยีในปัจจุบัน ส่งผลให้การบริการใหม่ๆ อาทิ สื่อสังคมออนไลน์ (Social Media) และบริการด้านดิจิทัล (Digital Services) เป็นต้น อยู่ภายใต้ประกาศฯ ฉบับนี้ด้วย โดยประกาศฯ ได้จำแนกลักษณะประเภทของผู้ให้บริการออกเป็น 2 ประเภทหลัก หรือ 9 ประเภทย่อย และกำหนดหน้าที่ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่แตกต่างกันตามประเภทของผู้ให้บริการ อย่างไรก็ดี เนื่องด้วยการให้บริการภายใต้ประกาศฯ ในปัจจุบันมีความหลากหลายทั้งรูปแบบและฟังก์ชั่นการทำงาน เกณฑ์ในการพิจารณาประเภทของผู้ให้บริการจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีความชัดเจน และสร้างความเข้าใจที่ตรงกันทั้งในอุตสาหกรรมกันเองและกับหน่วยงานของรัฐเพื่อให้การบังคับใช้กฎหมายเป็นไปตามเจตนารมณ์ของผู้ออกประกาศฯ โดยเฉพาะอย่างยิ่งกรณีผู้ให้บริการดิจิทัล (Digital ServiceProvider) ที่ใช้เครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์เป็นส่วนหนึ่งของการให้บริการ ซึ่งสามารถตีความครอบคลุมการให้บริการในลักษณะที่เป็นการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่นแทบทุกประเภทโดยบริษัทฯ เห็นว่าความไม่ชัดเจนดังกล่าวอาจส่งผลให้ผู้ประกอบการเก็บข้อมูลจราจรไม่ครบถ้วนหรือเก็บข้อมูลจราจรมากเกินกว่าที่กฎหมายกำหนดอันเกิดจากความเข้าใจผิดหรือตีความผิดพลาด

บริษัทฯ จึงขอเสนอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและหน่วยงานที่เกี่ยวข้อง ร่วมกันจัดทำคู่มือแนวทางการปฏิบัติตามประกาศฯ ทั้งภาษาไทยและภาษาอังกฤษ เพื่อให้ผู้ให้บริการประเภทต่างๆ ใช้เป็นแนวทางในการนำไปประยุกต์ใช้งาน และปฏิบัติตามกฎหมายได้อย่างถูกต้อง ครบถ้วน และการบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพต่อไป

ประเด็นที่ 2 ภาระค่าใช้จ่ายอันเกิดจากการปฏิบัติตามประกาศฯ

ด้วยในปัจจุบันกิจกรรมที่เกิดขึ้นบนเครือข่ายอินเทอร์เน็ตมีปริมาณเพิ่มขึ้นอย่างต่อเนื่อง และมีแนวโน้มเพิ่มขึ้นไปเรื่อย ๆ อันจะส่งผลโดยตรงกับขนาดพื้นที่สำหรับจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการและค่าใช้จ่ายที่เกี่ยวเนื่องอันเกิดจากการเก็บข้อมูลดังกล่าวซึ่งเป็นภาระของผู้ให้บริการอย่างหลีกเลี่ยงไม่ได้ ประกอบกับผู้ให้บริการยังจำเป็นต้องออกแบบระบบเพื่อรองรับข้อกำหนดต่างๆ ที่ระบุไว้ในประกาศฯ อาทิ ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลที่เป็นไปตามหรือไม่ต่ำกว่าที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์กำหนดหรือหลักเกณฑ์อื่นที่มีมาตรฐานสอดคล้อง ซึ่งต่างมีภาระค่าใช้จ่ายในการดำเนินงานทั้งสิ้น

อย่างไรก็ดี บริษัทฯ เข้าใจและตระหนักถึงความสำคัญในจัดเก็บและใช้ประโยชน์ของข้อมูลจราจรอันจะส่งผลให้เกิดความสงบเรียบร้อยต่อสังคมและประเทศชาติโดยรวม บริษัทฯ จึงขอเสนอหน่วยงานของรัฐพิจารณามาตรการสนับสนุนค่าใช้จ่ายในการดำเนินการตามประกาศฯ เพื่อเป็นการแบ่งเบาภาระของผู้ให้บริการและเป็นการสร้างแรงจูงใจให้ผู้ให้บริการปฏิบัติตามประกาศฯ อย่างเคร่งครัดต่อไป

ประเด็นที่ 3 การมีส่วนร่วมในการปรับปรุงกฎระเบียบ

ในปัจจุบันเทคโนโลยีบนเครือข่ายคอมพิวเตอร์มีการเปลี่ยนแปลงอย่างรวดเร็ว หน่วยงานของรัฐจึงอาจเล็งเห็นความจำเป็นในการปรับปรุงกฎหมายหรือกฎระเบียบเพื่อให้สอดรับกับการเปลี่ยนแปลงของเทคโนโลยีดังกล่าว ดังเช่นการปรับปรุงหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการตามที่ออกเป็นประกาศฯ และกำหนดให้มีผลบังคับใช้ในทันที

บริษัทฯ ขอเรียนว่ากฎระเบียบส่วนใหญ่ส่งผลกระทบต่อการให้บริการของหน่วยงานที่เกี่ยวข้องกับกฎระเบียบดังกล่าวไม่มากก็น้อย บริษัทฯ จึงขอเรียนด้วยความเคารพและขอสนับสนุนการกำหนดกระบวนการให้ผู้มีส่วนได้เสียทุกภาคส่วนมีส่วนร่วมในการแสดงความคิดเห็นอย่างทั่วถึงก่อนการออกกฎระเบียนหรือหลักเกณฑ์ต่างๆ เพื่อให้การบังคับใช้กฎหมายหรือกฎระเบียบที่ประกาศใช้บังคับให้เป็นไปอย่างมีประสิทธิภาพต่อไป

สรุป

บริษัทฯจึงได้จัดทำเอกสารฉบับนี้เพื่อชี้แจงถึงข้อจำกัดและอุปสรรคที่อาจเกิดขึ้น รวมทั้งแสดงความคิดเห็นและแนวทางที่เหมาะสมในมุมมองของผู้ประกอบการ โดยบริษัทฯ หวังเป็นอย่างยิ่งว่าข้อคิดเห็นของบริษัทฯ จะเป็นประโยชน์ต่อกระบวนการพัฒนากฎหมายในประเทศไทย ทั้งในส่วนที่เกี่ยวกับ

การคุ้มครองข้อมูลส่วนบุคคล การรับมือกับภัยคุกคามทางไซเบอร์ และการเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อให้บรรลุวัตถุประสงค์ในการคุ้มครองสิทธิของเจ้าของข้อมูลส่วนบุคคล ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และไม่เป็นอุปสรรคต่อการประกอบธุรกิจของภาคธุรกิจที่เกี่ยวข้องไปพร้อมกัน

ที่ BRD.BRD 0020/2564

วันที่ 27 ตุลาคม 2564

เรื่อง นำส่งสถิติข้อมูลจราจรทางคอมพิวเตอร์ที่นำส่งแก่หน่วยงานภาครัฐ และข้อคิดของบริษัทเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

เรียน ประธานคณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภา

อ้างถึง หนังสือคณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภา ที่ สว(กมธ 1) 0009/02547 ลงวันที่ 16 กันยายน 2564

สิ่งที่ส่งมาด้วย สถิติข้อมูลจราจรทางคอมพิวเตอร์ และข้อคิดเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่น คงปลอดภัยไซเบอร์ พ.ศ. 2562 และ ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

ตามที่ คณะกรรมาธิการเทคโนโลยีสารสนเทศ การสื่อสาร และการโทรคมนาคม วุฒิสภา (คณะกรรมาธิการ)ได้มีหนังสือเชิญบริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) เข้าร่วมประชุมเมื่อวันที่ 28 กันยายน 2564 เพื่อให้ข้อมูลเกี่ยวกับแนวทางการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ รวมทั้งปัญหาอุปสรรคในการดำเนินการตามประกาศรัฐมนตรีตามมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และเรื่องอื่นๆ ที่เกี่ยวข้อง ความละเอียดตามหนังสือที่อ้างถึง ซึ่งในการประชุมร่วมกันดังกล่าวผู้แทนของบริษัทฯ ได้ชี้แจงข้อมูลที่เกี่ยวข้องให้ที่ประชุมรับทราบในเบื้องต้นตามประเด็นที่ปรากฏในหนังสือที่อ้างถึงแล้ว โดยคณะกรรมาธิการได้แจ้งให้บริษัทฯ นำส่งสถิติข้อมูลจราจรทางคอมพิวเตอร์ที่นำส่งแก่หน่วยงานภาครัฐ และข้อคิดเห็นต่อกฎหมายอื่นๆ ที่เกี่ยวข้องเพิ่มเติมนั้น

ในการนี้ บริษัทฯ ขอนำส่งสถิติข้อมูลจราจรทางคอมพิวเตอร์ที่นำส่งแก่หน่วยงานรัฐ และข้อคิดเห็นต่อพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ของผู้ให้บริการ พ.ศ. 2564 ตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายศรัณย์ ผโลประการ)
หัวหน้าฝ่ายงานธุรกิจสัมพันธ์
บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

สำนักธุรกิจสัมพันธ์ โทร 02-029-5056

สถิติข้อมูลจราจรทางคอมพิวเตอร์ และข้อมูลโทรศัพท์เคลื่อนที่ ที่บริษัทฯ นำส่งแก่หน่วยงานภาครัฐ

ปี 2562 จำนวนสถิติที่นำส่ง 25,666 เคส

ปี 2563 จำนวนสถิติที่นำส่ง 18,183 เคส

ประเด็นการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ของผู้ให้บริการและผู้ประกอบการโทรศัพท์เคลื่อนที่

1. ข้อมูลของผู้ใช้บริการและข้อมูลจราจรบนโครงข่ายโทรศัพท์เคลื่อนที่ที่บริษัทฯ มีไว้ในครอบครองหรือควบคุมดูแลมีกี่ประเภท ปริมาณข้อมูล สถานที่จัดเก็บ (เช่น รวมศูนย์หรือกระจาย) เทคโนโลยีในการจัดเก็บ จัดเก็บรักษาในรูปแบบไหน (เช่น รูปแบบที่คนอ่านได้หรือคอมพิวเตอร์อ่านได้เท่านั้น) มาตรการการรักษาความปลอดภัยเป็นอย่างไร (เช่น ความยากง่ายการเข้าถึงข้อมูล การใช้หรือแชร์ข้อมูลภายในบริษัท หรือบุคคลภายนอก หรือการเข้ารหัสหรือไม่ อย่างไร) ต้นทุน/ค่าใช้จ่ายในการเก็บรักษา และปัจจุบันมีปัญหา/อุปสรรคอย่างไรในการเก็บรักษาข้อมูลดังกล่าว

คำตอบ เราเก็บข้อมูลของผู้ใช้บริการ และข้อมูลจราจรได้ตามความสามารถที่ระบบที่ให้บริการกับผู้ใช้บริการต่างๆ สามารถ ทำได้เท่านั้น โดยได้เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามระยะเวลาที่กฎหมายกำหนดไว้ และเป็นไปตามการจัดระดับชั้นข้อมูลขององค์กร (Data Classification) ในปัจจุบันมีการเก็บข้อมูลจราจรครบถ้วนตามที่กฎหมายกำหนด

ปัจจุบันปริมาณข้อมูลผู้ใช้บริการอยู่ที่มากกว่า 10 TB/วัน และมีแนวโน้มสูงขึ้นเรื่อยๆ โดยมีการเก็บแบบกระจายตามประเภทข้างต้น และใช้เทคโนโลยี Big Data และ Storage ในการจัดเก็บ ซึ่งมีการกำหนดสิทธิ์เข้าใช้งานผ่าน Portal เนื่องจากข้อมูลจราจรได้มาจากระบบที่สร้างขึ้นมาจากระบบที่ให้บริการ ซึ่งรูปแบบของข้อมูลที่สร้างขึ้นในระบบที่ให้บริการต่างๆ นั้นอยู่ในรูปแบบทั้งที่คนอ่านได้ และคอมพิวเตอร์อ่านได้ ตามที่ระบบนั้นๆออกแบบมา

สำหรับมาตรการการรักษาความปลอดภัย เราได้แยกการเก็บข้อมูลจราจรออกมาจากข้อมูลอื่นๆ พร้อมกับมีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลเฉพาะบุคคลทางกฎหมายที่มีหน้าที่รับเรื่องการร้องขอข้อมูลจราจรจากหน่วยงานหรือเจ้าหน้าที่ของรัฐเท่านั้น โดยมีการใส่หมายเลขอ้างอิงในการร้องขอเข้ามาทุกครั้งในการค้นหา และดึงข้อมูล เพื่อตรวจสอบถึงการที่มาของการร้องขอ

สำหรับเรื่องต้นทุน/ค่าใช้จ่ายในการเก็บรักษานั้น ขึ้นอยู่กับปริมาณข้อมูลที่เพิ่มขึ้นตามการใช้งานของลูกค้าตามระยะเวลาที่กฎหมายกำหนดในแต่ละประเภทบริการ และปริมาณข้อมูลที่ร้องขอเข้ามาในแต่ละครั้ง

2. บริษัทฯ มีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของบริษัทฯ อย่างไร และมีความพร้อมในการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลและประกาศของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้องหรือไม่ อย่างไร

<u>คำตอบ</u> บริษัทมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลตามเอกสารต่างๆ ทั้งที่เผยแพร่ทางช่องทาง AIS web site ได้แก่ประกาศการคุ้มครองข้อมูลส่วนบุคคล และนโยบายการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งเตรียมเอกสารภายในให้พนักงานปฏิบัติตามอย่างเคร่งครัด โดยเอกสารเหล่านั้นสอดคล้องกับ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ประกาศของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ และตามมาตรฐาน NIST และ ISO27001
ตัวอย่างเช่น

1. มาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของลูกค้า สำหรับพนักงานและบุคคลภายนอก
2. กรอบการดำเนินงานการจัดชั้นความลับและการควบคุมดูแลข้อมูล
3. นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์
4. กรอบการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์
5. มาตรฐานด้านการรักษาความปลอดภัยระบบคลาวด์

นอกจากนี้ยังมีมาตราการตรวจสอบภายในอย่างสม่ำเสมอ มีการควบคุมและการบริหารผ่านคณะกรรมการที่เป็นผู้บริหารระดับสูงในการบริหารความเสี่ยงของบริษัทและดูแลเรื่องข้อมูลส่วนบุคคลโดยเฉพาะ

3. ที่ผ่านมามีการเจาะระบบหรือเข้าถึงข้อมูลส่วนบุคคลโดยมิชอบกฎหมายด้วยหรือไม่ ไม่ว่าจะเกิดจบุคคลภายนอก หรือพนักงานของบริษัทฯ เอง หากมี บริษัทฯ มีมาตรการดำเนินการอย่างไร และแก้ไขเยียวยาผู้เสียหายอย่างไร

<u>คำตอบ</u> ที่ผ่านมา AIS ตรวจพบความพยายามที่จะเจาะระบบบ่อยครั้ง แต่ไม่เคยมีการเจาะข้อมูลเข้าถึงข้อมูลส่วนบุคคลได้ บริษัทฯ มีมาตรการรับมือหากเกิดเหตุการณ์ดังกล่าว

4. บริษัทมีการจัดเก็บข้อมูลและสถิติเกี่ยวกับการร้องขอเข้าถึงและใช้ข้อมูลส่วนบุคคลของผู้ใช้บริการและข้อมูลจราจรบนโครงข่ายโทรศัพท์เคลื่อนที่โดยหน่วยงานหรือเจ้าหน้าที่ของรัฐหรือไม่ อย่างไร

<u>คำตอบ</u> บริษัทฯ มีการจัดเก็บข้อมูลการร้องขอข้อมูลจราจรคอมพิวเตอร์ สามารถระบุผู้ขอและปริมาณของข้อมูลที่ถูกร้องขอได้ ยกตัวอย่างเช่น ในปี 2563 สนง. ตำรวจแห่งชาติ ขอข้อมูลจราจรคอมพิวเตอร์220 เรื่อง IP 649 หมายเลข ในปี 2564 (ถึงสิงหาคม) 280 เรื่อง IP 827 หมายเลข

4.1 จำแนกประเภทและปริมาณของข้อมูลที่ถูกร้องขอ

4.2 จำแนกประเภทและปริมาณการร้องขอของหน่วยงานรัฐ

<u>คำตอบ</u> บริษัทฯ พิจารณาว่า ผู้ร้องขอ มีอำนาจตามกฎหมายในการเข้าถึงข้อมูลหรือไม่ เป็นหัวข้อหลัก ในการพิจารณาว่าจะให้หรือไม่ให้ข้อมูล เพื่อคุ้มครองสิทธิเสรีภาพของผู้ใช้บริการ

4.3 หลักเกณฑ์การร้องขอและเงื่อนไขการใช้ข้อมูลเพื่อคุ้มครองสิทธิเสรีภาพของผู้ใช้บริการ

<u>คำตอบ</u> ในการจัดส่งข้อมูลของบริษัทฯ มี 2 รูปแบบ คือ

- นำส่งข้อมูลเป็นลายลักษณ์อักษร
- นำส่งข้อมูลเป็นไฟล์อิเล็กทรอนิกส์

4.4 มีการเก็บค่าให้บริการข้อมูลหรือไม่

<u>คำตอบ</u> บริษัทฯ ไม่ได้มีการเรียกเก็บค่าใช้จ่ายใดๆ

4.5 รูปแบบของข้อมูลที่ให้พนักงานเจ้าหน้าที่ เช่น กระดาษ หรือไฟล์อิเล็กทรอนิกส์ หรือข้อมูลดังกล่าวต้องมีการแปลความหรือถอดรหัสหรือไม่

<u>คำตอบ</u> ซึ่งข้อมูลจราจรคอมพิวเตอร์ดังกล่าว แปลงความให้เรียบร้อยแล้ว แต่จะต้องทำความเข้าใจกับข้อมูลที่ได้รับไป กรณีส่งข้อมูลเป็นไฟล์อิเล็กทรอนิกส์ จะมีการตั้งรหัสไฟล์เพื่อป้องกันข้อมูล

4.6 พนักงานของบริษัทฯ ต้องให้การเป็นพยานหรือไม่ เพื่อยืนยันความถูกต้องแท้จริงของข้อมูล

<u>คำตอบ</u> ในบางกรณีพนักงานของบริษัทฯ ต้องเดินทางไปให้การเป็นพยานด้วย เพื่อยืนยันความถูกต้องแท้จริงของข้อมูล

4.7 ปัญหาและอุปสรรคในการให้บริการข้อมูล เช่น ขอข้อมูลแบบกว้างไม่เฉพาะเจาะจงให้ปริ๊นข้อมูลในรูปของกระดาษ

<u>คำตอบ</u> ปัญหาและอุปสรรคในการให้บริการข้อมูล สาเหตุหลักมาจากผู้ขอไม่มีความเข้าใจในข้อมูลจราจรคอมพิวเตอร์ (Log File) เช่น

- ขอข้อมูลโดยไม่ระบุ วัน/เวลาแน่นอน ไม่เฉพาะเจาะจง ทำให้ข้อมูลมีปริมาณมากจนไม่สามารถเรียกดึงจากระบบได้ เช่น ขอข้อมูลย้อนหลังคราวละ 30 วัน
- ขอให้ตรวจสอบข้อมูลจราจรคอมพิวเตอร์จากที่อยู่ บ้านเลขที่ หรือพื้นที่ เป็นต้น
- ขอข้อมูลย้อนหลังเกินระยะเวลาที่จัดเก็บ (เกิน 90 วัน)

5. บริษัทมีความเห็นเกี่ยวกับการปฏิบัติตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 หรือไม่ อย่างไร มีปัญหา/อุปสรรคในการดำเนินการตามหลักเกณฑ์ดังกล่าวในข้อใด เหตุผลใด และมีข้อเสนอแนะอย่างไร

<u>คำตอบ</u> จากการเปรียบเทียบหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการฉบับเก่า กับฉบับใหม่ สิ่งที่น่าจะปัญหา/มีอุปสรรคในการดำเนินการสำหรับการจัดเก็บข้อมูลเกี่ยวกับสถานที่ในการเข้าออกระบบคอมพิวเตอร์ (Location) บนโครงข่ายโทรศัพท์เคลื่อนที่ มีดังนี้

1. โครงข่ายโทรศัพท์เคลื่อนที่ได้ถูกออกแบบให้เก็บบันทึกการโทรออก และรับสาย (ระดับภูมิภาค) เพื่อนำมาใช้ในการคิดค่าบริการเท่านั้น ดังนั้นการขอข้อมูลตำแหน่งย้อนหลังในอดีตจึงได้ในระดับภูมิภาคเท่านั้น

2. การใช้งาน App บนโทรศัพท์ เราไม่สามารถเชื่อมโยงกับหมายเลขโทรศัพท์มือถือได้ จึงไม่สามารถติดตามหาตำแหน่งได้

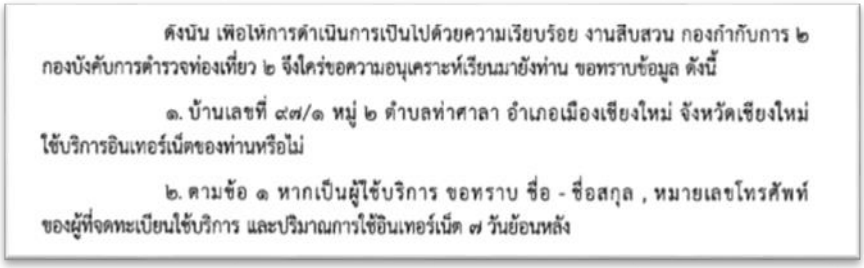
3. ในกรณีที่ App ต้องการทราบตำแหน่งของผู้ใช้บริการ App จะต้องขอเปิด GPS ซึ่งระบบ Android & IOS จะขออนุญาตผู้ใช้บริการเสมอ หากผู้ใช้บริการไม่อนุญาตก็ไม่สามารถทราบตำแหน่ง

6. บริษัทเคยมีการปฏิเสธหรือไม่ให้ข้อมูลแก่เจ้าหน้าที่หรือไม่ ด้วยเหตุผลอะไร

<u>คำตอบ</u> บริษัทฯ มีการปฏิเสธหรือไม่ให้ข้อมูลแก่เจ้าหน้าที่ ในกรณีที่เจ้าหน้าที่ไม่ได้ปฏิบัติตามหลักเกณฑ์หรือข้อกำหนดของกฎหมายที่เกี่ยวข้อง ขอข้อมูลผิดบริษัทฯ ขอข้อมูลแพลตฟอร์ม (Platform) ที่บริษัทฯ ไม่ได้เป็นผู้ให้บริการ เช่น Facebook Twitter Line เป็นต้น

<u>ตัวอย่างเหตุแห่งการปฏิเสธ</u>

- เหตุผล เป็นข้อมูลที่บริษัทไม่ได้จัดเก็บไว้

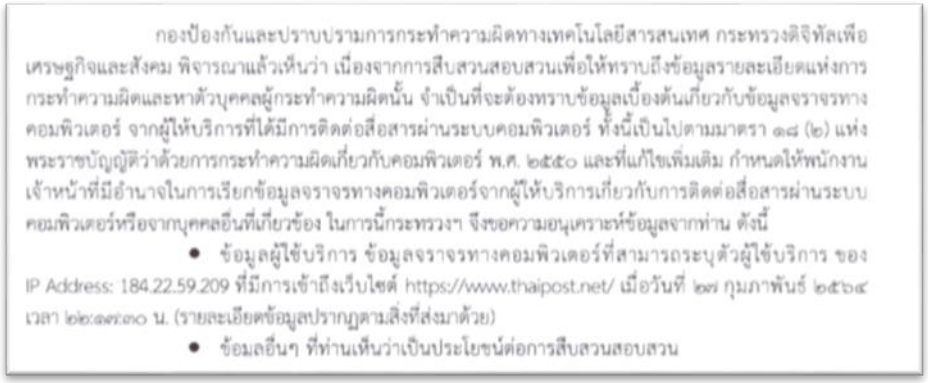


ดังนั้น เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย งานสืบสวน กองกำกับการ ๒ กองบังคับการตำรวจท่องเที่ยว ๒ จึงใคร่ขอความอนุเคราะห์เรียนมายังท่าน ขอทราบข้อมูล ดังนี้

๑. บ้านเลขที่ ๙๗/๑ หมู่ ๒ ตำบลท่าศาลา อำเภอเมืองเชียงใหม่ จังหวัดเชียงใหม่ ใช้บริการอินเทอร์เน็ตของท่านหรือไม่

๒. ตามข้อ ๑ หากเป็นผู้ใช้บริการ ขอทราบ ชื่อ - ชื่อสกุล , หมายเลขโทรศัพท์ของผู้ที่จดทะเบียนใช้บริการ และปริมาณการใช้อินเทอร์เน็ต ๗ วันย้อนหลัง

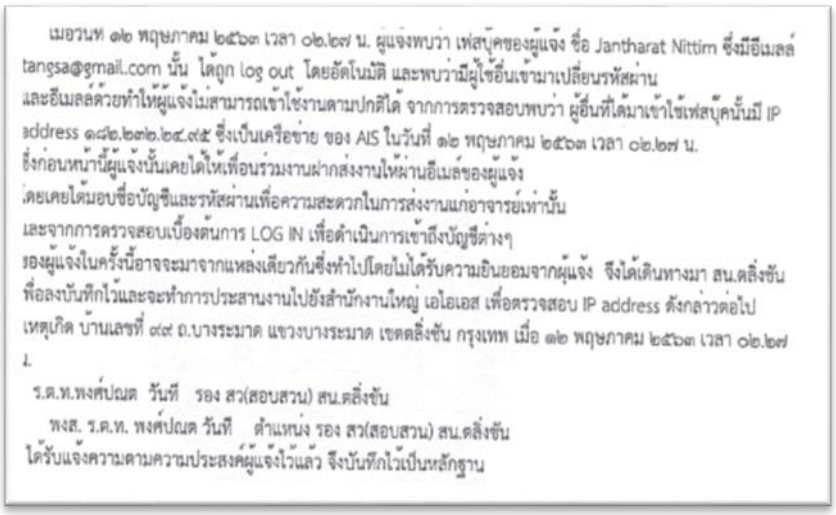
- เหตุผล ขอข้อมูลย้อนหลังเกินกว่า 90 วัน



กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม พิจารณาแล้วเห็นว่า เนื่องจากการสืบสวนสอบสวนเพื่อให้ทราบถึงข้อมูลรายละเอียดแห่งการกระทำความผิดและหาตัวบุคคลผู้กระทำความผิดนั้น จำเป็นที่จะต้องทราบข้อมูลเบื้องต้นเกี่ยวกับข้อมูลจราจรทางคอมพิวเตอร์ จากผู้ให้บริการที่ได้มีการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ ทั้งนี้เป็นไปตามมาตรา ๑๘ (๒) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง ในการนี้กระทรวงฯ จึงขอความอนุเคราะห์ข้อมูลจากท่าน ดังนี้

- ข้อมูลผู้ใช้บริการ ข้อมูลจราจรทางคอมพิวเตอร์ที่สามารถระบุตัวผู้ใช้บริการ ของ IP Address: 184.22.59.209 ที่มีการเข้าถึงเว็บไซต์ https://www.thaipost.net/ เมื่อวันที่ ๒๗ กุมภาพันธ์ ๒๕๖๔ เวลา ๒๒:๑๗:๓๐ น. (รายละเอียดข้อมูลปรากฏตามสิ่งที่ส่งมาด้วย)
- ข้อมูลอื่นๆ ที่ท่านเห็นว่าเป็นประโยชน์ต่อการสืบสวนสอบสวน

- ไม่ได้ใช้อำนาจตามกฎหมาย รับแจ้งความเป็นหลักฐานและขอข้อมูลแพลตฟอร์ม (Platform) ที่บริษัทฯ ไม่ได้เป็นผู้ให้บริการ



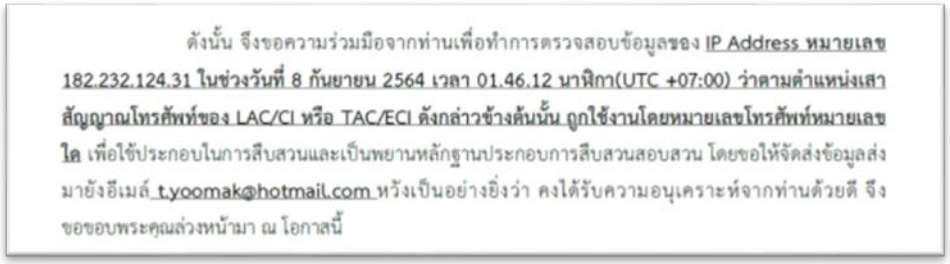
เมื่อวันที่ ๑๒ พฤษภาคม ๒๕๖๓ เวลา ๐๒.๒๗ น. ผู้แจ้งพบว่า เฟสบุ๊คของผู้แจ้ง ชื่อ Jantharat Nittim ซึ่งมีอีเมล์ tangsa@gmail.com นั้น ได้ถูก log out โดยอัตโนมัติ และพบว่ามีผู้ใช้อื่นเข้ามาเปลี่ยนรหัสผ่าน และอีเมล์ด้วยทำให้ผู้แจ้งไม่สามารถเข้าใช้งานตามปกติได้ จากการตรวจสอบพบว่า ผู้อื่นที่ได้มาเข้าใช้เฟสบุ๊คนั้นมี IP address ๑๘๒.๒๓๒.๒๔.๙๕ ซึ่งเป็นเครือข่าย ของ AIS ในวันที่ ๑๒ พฤษภาคม ๒๕๖๓ เวลา ๐๒.๒๗ น. ซึ่งก่อนหน้านี้ผู้แจ้งนั้นเคยได้ให้เพื่อนร่วมงานฝากส่งงานให้ผ่านอีเมล์ของผู้แจ้ง โดยเคยได้มอบชื่อบัญชีและรหัสผ่านเพื่อความสะดวกในการส่งงานแก่อาจารย์เท่านั้น และจากการตรวจสอบเบื้องต้นการ LOG IN เพื่อดำเนินการเข้าถึงบัญชีต่างๆ ของผู้แจ้งในครั้งนี้อาจจะมาจากแหล่งเดียวกันซึ่งทำไปโดยไม่ได้รับความยินยอมจากผู้แจ้ง จึงได้เดินทางมา สน.คลิ่งชัน เพื่อลงบันทึกไว้และจะทำการประสานงานไปยังสำนักงานใหญ่ เอไอเอส เพื่อตรวจสอบ IP address ดังกล่าวต่อไป เหตุเกิด บ้านเลขที่ ๙๙ ถ.บางระมาด แขวงบางระมาด เขตคลิ่งชัน กรุงเทพ เมื่อ ๑๒ พฤษภาคม ๒๕๖๓ เวลา ๐๒.๒๗ น.

ร.ต.ท.พงศ์ปณต วันที่ รอง สว(สอบสวน) สน.คลิ่งชัน

พงส. ร.ต.ท. พงศ์ปณต วันที่ ตำแหน่ง รอง สว(สอบสวน) สน.คลิ่งชัน

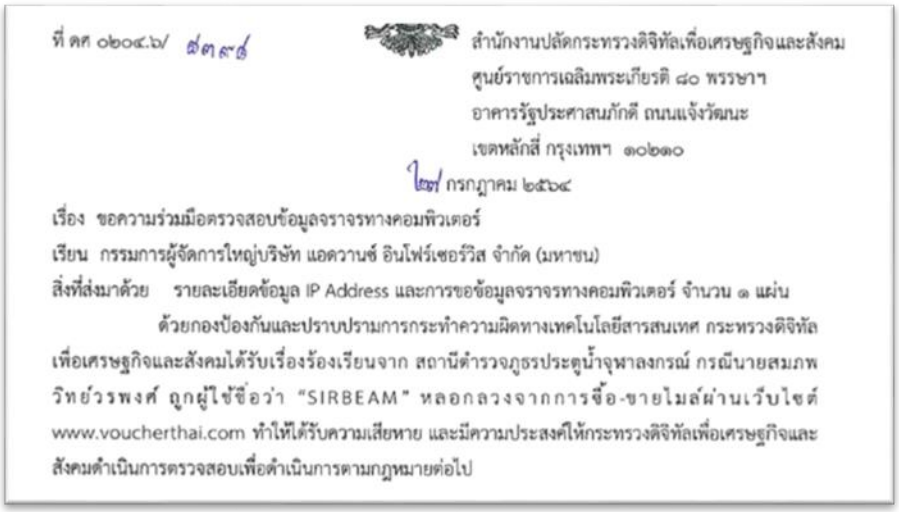
ได้รับแจ้งความตามความประสงค์ผู้แจ้งไว้แล้ว จึงบันทึกไว้เป็นหลักฐาน

- เหตุผล เป็นข้อมูลที่บริษัทไม่ได้มีการจัดเก็บไว้



ดังนั้น จึงขอความร่วมมือจากท่านเพื่อทำการตรวจสอบข้อมูลของ IP Address หมายเลข 182.232.124.31 ในช่วงวันที่ 8 กันยายน 2564 เวลา 01.46.12 นาฬิกา(UTC +07:00) ว่าตามตำแหน่งเสาสัญญาณโทรศัพท์ของ LAC/CI หรือ TAC/ECI ดังกล่าวข้างต้นนั้น ถูกใช้งานโดยหมายเลขโทรศัพท์หมายเลขใด เพื่อใช้ประกอบในการสืบสวนและเป็นพยานหลักฐานประกอบการสืบสวนสอบสวน โดยขอให้จัดส่งข้อมูลส่งมายังอีเมล์ t.yoomak@hotmail.com หวังเป็นอย่างยิ่งว่า คงได้รับความอนุเคราะห์จากท่านด้วยดี จึงขอขอบพระคุณล่วงหน้ามา ณ โอกาสนี้

- เหตุผล ขอข้อมูลผิดบริษัท



ที่ ดศ ๐๒๐๔.๖/ ๘๓๙๘

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๒๗ กรกฎาคม ๒๕๖๔

เรื่อง ขอความร่วมมือตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์

เรียน กรรมการผู้จัดการใหญ่บริษัท แอดวานซ์ อินโฟร์เซอร์วิส จำกัด (มหาชน)

สิ่งที่ส่งมาด้วย รายละเอียดข้อมูล IP Address และการขอข้อมูลจราจรทางคอมพิวเตอร์ จำนวน ๑ แผ่น

ด้วยกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้รับเรื่องร้องเรียนจาก สถานีตำรวจภูธรประตูน้ำจุฬาลงกรณ์ กรณีนายสมภพ วิทย์วรพงศ์ ถูกผู้ใช้ชื่อว่า "SIRBEAM" หลอกลวงจากการซื้อ-ขายไมล์ผ่านเว็บไซต์ www.voucherthai.com ทำให้ได้รับความเสียหาย และมีความประสงค์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินการตรวจสอบเพื่อดำเนินการตามกฎหมายต่อไป

7. บริษัทมีการแยกระดับการเข้าถึงข้อมูลในแต่ละระดับชั้นข้อมูลหรือไม่ อย่างไร และมีการตรวจสอบการเข้าถึงข้อมูลเพียงใด

คำตอบ บริษัทมีการจัดการควบคุมการเข้าถึงข้อมูลสำคัญตามความจำเป็นของการใช้งานเท่านั้น โดยแบ่งระดับชั้นข้อมูลเป็น 4 ระดับคือ

Highly confidential ซึ่งเป็นระดับชั้นข้อมูลสูงสุด เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

Restricted เป็นระดับชั้นข้อมูลที่เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้องเท่านั้น

Internal เป็นระดับชั้นข้อมูลที่ใช้ภายในบริษัทเท่านั้น

Public เป็นระดับชั้นสาธารณะ คือข้อมูลที่ส่งออกนอกบริษัทได้และมีระบบการตรวจสอบการเข้าถึงข้อมูลด้วยการเก็บ log การใช้งานให้สอดคล้องกับงานที่ได้รับมอบหมาย

.....