ปฏิกิริยาในยุโรปหลังการบังคับใช้กฎระเบียบ GDPR และแนวปฏิบัติในการโอนข้อมูลมายังประเทศที่สามนอกเขต EU

By **thaieurope** - August 31, 2018

กฎระเบียบ GDPR (General Data Protection Regulation) ได้ส่งผลกระทบต่อธุรกิจทั้งในและนอก EU เป็นวงกว้าง โดยเฉพาะธุรกิจที่ให้บริการออนไลน์ เพราะจะต้องปรับเปลี่ยนนโยบายการปกป้องข้อมูลส่วนบุคคลอย่างเร่งด่วน เพื่อให้บริการกับลูกค้าภายใน EU โดยสำนักข่าว Irishtimes รายงานว่า หลังจากที่กฎระเบียบ GDPR มีผลบังคับใช้ไปเมื่อวันที่ 25 พฤษภาคม 2561 มีการรายงานกรณีละเมิดข้อมูลส่วนบุคคลมากถึง 1,184 กรณี ภายในระยะเวลา 2 เดือน จากเดิมที่มีการรายงานประมาณ 230 กรณีต่อเดือน

สาเหตุหลักที่มีปริมาณการร้องเรียนสูง เนื่องจากกฎระเบียบ GDPR บังคับให้องค์กรธุรกิจต้องแจ้งหน่วยหน่วยงานคุ้มครองข้อมูล (Data Protection Authority) ภายใน 72 ชั่วโมง หลังจากได้รับแจ้งเกี่ยวกับกรณีข้อมูลส่วนบุคคลสูญหาย ถูกทำลาย หรือมีการละเมิดการใช้ข้อมูลโดยไม่ได้รับอนุญาต

ปฏิกิริยาในโลกออนไลน์หลังการบังคับใช้กฎระเบียบ GDPR

เว็บไซต์สิ่งพิมพ์ออนไลน์ของสหรัฐฯ หลายรายระงับการให้บริการลูกค้าใน EU อาทิ เว็บไซต์ Chicago Tribune, Los Angeles Times, New York Daily News, Orlando Sentinel และ Baltimore Sun ได้ระงับการให้บริการหนังสือพิมพ์ออนไลน์ใน EU เพื่อปรับปรุงระบบการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการ ขณะที่เว็บไซต์ USA Today ระงับการใช้ระบบติดตามข้อมูลเพื่อการโฆษณา (ad-tracking) ผ่านเว็บไซต์ eu.usatoday.com ที่ให้บริการเฉพาะลูกค้าใน EU โดยเฉพาะ

เว็บไซต์ Chicago Tribune **เว็บไซต์ USA Today**

สื่อ Social Media ถูกฟ้องดำเนินคดีกรณีละเมิดการใช้ข้อมูลส่วนบุคคล หลังจากที่กฎระเบียบ GDPR มีผลบังคับได้เพียง 1 วัน นาย Max Schrems ทนายประจำองค์กร NOYB และนักรณรงค์ต่อต้านการละเมิดข้อมูลส่วนบุคคลที่เคยยื่นฟ้อง Facebook ต่อศาลยุติธรรมยุโรปเมื่อปี 2558 จนทำให้ข้อตกลง Safe Harbour เกี่ยวกับการส่งผ่านข้อมูลระหว่าง EU และสหรัฐฯ ต้องกลายเป็นโมฆะ ได้ยื่นฟ้อง 4 บริษัทยักษ์ใหญ่ ได้แก่ Google ในฝรั่งเศส, Instagram ในเบลเยียม, WhatsApp ในเยอรมนี และ Facebook ในออสเตรีย โดยระบุว่า ทั้ง 4 บริษัทบังคับให้ผู้ใช้บริการยินยอมให้ใช้ข้อมูลส่วนบุคคล (Forced Consent) เป็นเงื่อนไขเบื้องต้นในการใช้บริการ ซึ่งตามกฎระเบียบ GDPR ผู้ให้บริการไม่สามารถบังคับผู้ใช้บริการได้ ต้องให้ผู้ใช้บริการสามารถเลือกที่จะให้การยินยอมหรือไม่ยินยอมให้ใช้ข้อมูลส่วนบุคคล (มาตรา 7(4)) ทั้งนี้ เจ้าหน้าที่คุ้มครองข้อมูล

(Data Protection Officers – DPO) ของประเทศไอร์แลนด์ จะทำหน้าที่ตรวจสอบข้อร้องเรียนดังกล่าว เพราะทั้ง 4 บริษัทมีสำนักงานใหญ่อยู่ในประเทศไอร์แลนด์

การเก็บและเปิดเผยข้อมูลเจ้าของเว็บไซต์ในระบบตรวจสอบข้อมูลเว็บไซต์ หรือ WHOIS มีข้อจำกัดมากขึ้น หลังจากกรณีฟ้องร้องระหว่างองค์กร ICANN ที่ทำหน้าที่ดูแลระบบตรวจสอบข้อมูลผู้ถือครองโดเมนเว็บไซต์ หรือระบบ WHOIS และบริษัท EPAG ในเยอรมนี เกี่ยวกับการเก็บข้อมูลติดต่อเจ้าหน้าที่บริหารและเจ้าหน้าที่เทคนิค (Administrative and Technical Contact Information) ของผู้ขอจดทะเบียนโดเมนเว็บไซต์ และการเปิดเผยข้อมูลเจ้าของเว็บไซต์ ซึ่งส่งผลให้องค์กร ICANN ต้องปรับเปลี่ยนนโยบายการเก็บข้อมูลและเปิดเผยข้อมูลเจ้าของเว็บไซต์ ได้แก่

- ไม่สามารถเก็บข้อมูลติดต่อเจ้าหน้าที่บริหารและหน้าที่เทคนิค (Administrative and Technical Contact Information) ของผู้ขอจดทะเบียนโดเมนเว็บไซต์ในระบบ WHOIS
- ไม่สามารถเปิดเผยข้อมูลส่วนบุคคลของผู้ขอจดทะเบียนในรูปแบบสาธารณะได้ เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ เป็นต้น การเข้าถึงข้อมูลส่วนบุคคลของผู้จดทะเบียนจะต้องมีเหตุผลอันสมควรเท่านั้น (legitimate purpose) เท่านั้น

จากเหตุการณ์ดังกล่าวส่งผลให้มีข้อกังวลเกี่ยวกับการตรวจสอบและดำเนินคดีกับเว็บไซต์ที่ขายของปลอมและของผิดกฎหมาย โดยเฉพาะเว็บไซต์ขายสินค้าเลียนแบบสินค้าแบรนด์แนม เนื่องจากการฟ้องร้องดำเนินคดีจะต้องระบุชื่อผู้ถูกฟ้องก่อน ซึ่งตามกฎระเบียบ GDPR รายละเอียดดังกล่าวไม่สามารถเปิดเผยได้ในรูปแบบสาธารณะ โดยสำนักข่าว Financial Times รายงานบทสัมภาษณ์ของ Louis Vuitton และ Gucci ว่าบริษัทนิยมใช้ระบบ WHOIS ในการตรวจสอบชื่อ และข้อมูลติดต่อของเจ้าของเว็บไซต์ ดังนั้น การตรวจสอบและฟ้องร้องดำเนินคดีกับเว็บไซต์ในลักษณะดังกล่าวจึงทำได้ยากขึ้น เนื่องจากจะต้องขออนุญาตทุกครั้งเพื่อทำการตรวจสอบ

หากต้องโอนข้อมูลลูกค้ามายังประเทศที่อยู่นอกเขต EU ต้องทำอย่างไร?

กฎระเบียบ GDPR มีขอบเขตครอบคลุมธุรกิจนอกเขต EU ที่ให้บริการการค้าสินค้าหรือบริการแก่บุคคลที่มีถิ่นพำนักในเขต EU รวมถึงการประมวลผลข้อมูลของบุคคลที่มีถิ่นพำนักในเขต EU ซึ่งจะส่งผลกระทบโดยตรงต่อผู้ประกอบธุรกิจการค้าระหว่างประเทศ ที่จะต้องโอนข้อมูลส่วนบุคคลของลูกค้าเพื่อจัดเก็บหรือประมวลผลในประเทศที่สามซึ่งอยู่นอกเขต EU

ดังนั้น คำถามต่อมา คือ หากผู้ประกอบการไทยที่ประกอบธุรกิจออนไลน์ ซึ่งมีความจำเป็นต้องมีการรับ-ส่งข้อมูลลูกค้าที่มีสัญชาติของประเทศสมาชิก EU และมีถิ่นพำนักใน EU จะต้องทำอย่างไร เพื่อป้องกันไม่ให้เกิดการละเมิดการใช้ข้อมูลส่วนบุคคล

กฎระเบียบ GDPR ไม่อนุญาตให้มีการโอนข้อมูลลูกค้าที่มีสัญชาติของประเทศสมาชิก EU และมีถิ่นพำนักใน EU ไปยังประเทศนอกเขต EU หากประเทศนั้นไม่มีการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอ (Adequate level of protection) แต่ผู้ประกอบการแต่ละรายสามารถจัดทำข้อตกลง เพื่อให้สามารถโอนข้อมูลมายังประเทศนอกเขต EU เช่น การจัดทำนโยบายหรือกฎเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules) และการจัดทำสัญญามาตรฐานของอียู (Model Contracts) สำหรับการโอนข้อมูลส่วนบุคคลระหว่างผู้จัดเก็บข้อมูลส่วนบุคคล (Data Controller) กับผู้ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งจะต้องได้รับการอนุมัติจากคณะกรรมาธิการยุโรป

อย่างไรก็ดี EU ได้กำหนดข้อยกเว้นสำหรับการโอนข้อมูลส่วนบุคคลไปยังประเทศที่สาม ตามมาตรา 49 ดังต่อไปนี้

1. เจ้าของข้อมูลยินยอมให้มีการโอนข้อมูลอย่างชัดเจน (explicit consent) โดยเจ้าของข้อมูลต้องได้รับแจ้งเกี่ยวกับลักษณะของข้อมูล ผู้เก็บข้อมูล จุดประสงค์การโอนข้อมูล ขั้นตอนการยกเลิกการให้ความยินยอม และปลายทางที่เก็บข้อมูล ก่อนการยินยอมให้มีการโอนข้อมูล เป็นต้น
2. การโอนข้อมูลเป็นสิ่งจำเป็นต่อการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลหรือเป็นการดำเนินการก่อนการจัดทำสัญญา (pre-contractual measures) ตามที่เจ้าของข้อมูลร้องขอ
3. การโอนข้อมูลเป็นสิ่งจำเป็นต่อการบรรลุข้อตกลงของสัญญาหรือการปฏิบัติตามสัญญาเพื่อผลประโยชน์ของเจ้าของข้อมูล ซึ่งได้จัดทำขึ้นระหว่างผู้ควบคุมข้อมูลและบุคคลภายนอก
4. การโอนข้อมูลเป็นสิ่งจำเป็นต่อการคุ้มครองผลประโยชน์สำคัญของเจ้าของข้อมูล
5. การโอนข้อมูลเป็นสิ่งจำเป็นในทางกฎหมาย
6. การโอนข้อมูลเป็นสิ่งจำเป็นเพื่อปกป้องผลประโยชน์ของเจ้าของข้อมูล ในกรณีที่เจ้าของข้อมูลไม่สามารถให้การยินยอมได้ เนื่องจากเป็นบุคคลไร้ความสามารถ (physically incapable) หรือบุคคลที่ไม่สามารถทำนิติกรรมได้ (legally incapable)
7. การโอนข้อมูลเป็นไปตามกฎหมายของ EU หรือประเทศสมาชิก เพื่อให้ข้อมูลแก่สาธารณะชน

โดยผู้ประกอบการไทยสามารถอ่านเพิ่มเติมเกี่ยวกับแนวปฏิบัติ (guidelines) ในการโอนข้อมูลตามกรณียกเว้นข้างต้นได้ที่ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

ทั้งนี้ ผู้ประกอบการไทยจะต้องให้ความสำคัญกับกฎระเบียบ GDPR เป็นอย่างมาก เพราะ EU ได้วางโทษปรับมากสูงสุดถึง 20 ล้านยูโร หรือ 4% ของรายได้รวม หากมีการฝ่าฝืน ซึ่งการลงโทษจะทำผ่านบริษัทตัวแทนหรือบริษัทคู่ค้าที่อยู่ใน EU นอกจากนี้ ถึงแม้ว่าผู้ประกอบการขนาดกลางและขนาดย่อม (SMEs) จะได้รับการยกเว้นจากกฎระเบียบนี้ แต่การที่บริษัทไม่มีนโยบายในการรักษาความปลอดภัยข้อมูลส่วนบุคคลของลูกค้าจะส่งผลให้บริษัทขาดความน่าเชื่อถือเป็นอย่างมาก โดยเฉพาะในเวลานี้ที่ทั่วโลก รวมถึงประเทศไทยเอง ต่างก็ให้ความสำคัญกับ[illegible]ส่วนบุคคลมากขึ้น