# กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป
# General Data Protection Regulation (GDPR)

## ภูมิหลัง

๑. สภาสหภาพยุโรปผ่าน General Data Protection Regulation (GDPR) หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลเมื่อวันที่ ๒๗ เมษายน ๒๕๕๙ และกำลังจะมีผลใช้บังคับในวันที่ ๒๕ พฤษภาคม ศกนี้

๒. GDPR จะเข้ามาแทนที่กฎหมายเดิมหรือ EU Data Protection Directive[๑] ที่ใช้บังคับมาตั้งแต่ปี ๒๕๓๘ สำหรับใช้เป็นหลักการเบื้องต้นให้สมาชิกใช้เป็นแนวทางในการร่างกฎหมายภายในและกำหนดบทลงโทษของตนเอง **GDPR จึงไม่ใช่กฎหมายที่เข้ามาเปลี่ยนแปลงหลักการเดิม เพียงแต่ขยายความเรื่องการคุ้มครองข้อมูลและข้อมูลส่วนบุคคลของ EU ให้มีความชัดเจน/รัดกุมมากขึ้น เพิ่มความโปร่งใส และเป็นมาตรฐานเดียวกันทั่วยุโรป และสิ่งสำคัญคือการคุ้มครองข้อมูลของพลเมือง EU ที่ไม่ว่าข้อมูลจะเก็บอยู่ที่ใดในโลก ก็ต้องทำตาม GDPR**[๒]

## ความแตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของ EU ที่ผ่านมา

๓. สหภาพยุโรปได้ออกรายงานการเปลี่ยนแปลงสำคัญใน GDPR รวมทั้งความแตกต่างจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ผ่านมา[๓] ได้แก่

- **การบังคับใช้กฎหมายนอกอาณาเขต (extraterritorial applicability)** คือผู้รับข้อมูลไม่ว่าจะอยู่ที่ใดก็ต้องทำตาม GDPR
- **บทลงโทษแรงขึ้น** คือมีค่าปรับสูงถึง ๒๐ ล้านยูโร
- **การขอความยินยอม (consent) จากเจ้าของข้อมูลต้องใช้ภาษาที่ชัดเจน กระชับ ไม่ใช่ภาษากฎหมาย และเข้าใจง่าย** เช่นเดียวกันกับการถอนความยินยอมก็ต้องทำได้ง่ายเช่นกัน
- **การแจ้งเตือนเมื่อเกิดเหตุข้อมูลรั่ว (breach notification)** ต้องดำเนินการภายใน ๗๒ ชั่วโมง
- **สิทธิในการเข้าถึง (right to access)** คือต้องแจ้งให้เจ้าของข้อมูลทราบว่าข้อมูลถูกใช้ไปเพื่อวัตถุประสงค์ใด และต้องจัดทำสำเนาข้อมูลให้กับเจ้าของข้อมูลในรูปแบบอิเล็กทรอนิกส์โดยห้ามเก็บค่าใช้จ่ายเพิ่ม
- **สิทธิที่จะถูกลืม (right to be forgotten)** คือเจ้าของข้อมูลสามารถขอให้ลบข้อมูลของตัวเองออกได้ และข้อมูลที่ไม่มีความเกี่ยวข้องกับการประมวลผลก็ต้องลบออกด้วย
- **สิทธิในการโอนย้ายข้อมูลของตนจากผู้ประกอบการหนึ่งไปยังผู้ประกอบการอื่นได้ (Data Portability)**

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[2] *รู้จัก GDPR กฎใหม่คุ้มครองข้อมูลยุโรป ข้อมูลเก็บที่ไหน กฎหมายตามไปคุ้มครองที่นั่น.*
https://www.blognone.com/node/100324

3 EU. *An overview of the main changes under GPDR and how they differ from the previous directive.*
https://www.eugdpr.org/key-changes.html

- **ให้ความสำคัญกับการป้องกันข้อมูลส่วนบุคคลตั้งแต่การออกแบบ (Privacy by Design)** โดยให้ใช้มาตรการทางเทคนิคที่เหมาะสมและมีประสิทธิภาพในการป้องกันข้อมูลตั้งแต่เริ่มต้น
- **ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือ Data Protection Officers (DPO)**[๔] ทำหน้าที่ติดตามกิจกรรมประมวลผลข้อมูลขนาดใหญ่และข้อมูลอ่อนไหว และมีการกำหนดคุณสมบัติของ DPO ไว้ด้วย เช่น มีความรู้ความเชี่ยวชาญการจัดเก็บข้อมูล รายงานการทำงานตรงต่อผู้บริหาร และต้องไม่ทำงานอื่นที่อาจสร้างความขัดแย้งเรื่องผลประโยชน์ เป็นต้น

<u>หลักการสำคัญของ GDPR</u>

๔. แม้ว่า GDPR จะมีการกำหนดเงื่อนไขให้เกิดความรัดกุมและชัดเจนยิ่งขึ้น แต่ยังให้ความสำคัญกับ **การไหลเวียนของข้อมูลส่วนบุคคลข้ามพรมแดนโดยเสรี** (free/cross-border flow of personal data)[๕] เนื่องจากเห็นว่าจำเป็นต่อการขยายตัวของการค้าและความร่วมมือระหว่างประเทศ และการให้ policy space ในกรณีควบคุมหรือถ่ายโอนข้อมูลส่วนบุคคลเพื่อ**ความมั่นคงของชาติ** (Public security/ National security) ซึ่งไม่จำเป็นต้องยึดตาม GDPR แต่ให้ยึดตาม Union Legal Act และกฎหมายของประเทศสมาชิก (national law)[๖] รวมทั้งหน่วยงาน**รัฐบาลยังคงมีสิทธิ "เก็บ-ใช้-ถ่ายโอน" ข้อมูลเพื่อประโยชน์สาธารณะ (public interest)** เช่น การใช้ประโยชน์ด้านการจัดเก็บภาษี และการสืบสวนเรื่องการเงิน[๗] เป็นต้น[๘]

<u>ผลกระทบของ GDPR</u>

๕. เมื่อ GDPR มีการใช้บังคับ จะส่งผลกระทบโดยตรงกับการประกอบธุรกิจการค้าระหว่างประเทศที่มีลูกค้าเป็นพลเมือง EU ไม่ว่าจะเป็นการโอนข้อมูลภายในองค์กรเดียวกันที่ตั้งอยู่คนละประเทศ การโอนข้อมูลไปยังองค์กรอื่นที่ตั้งอยู่ในต่างประเทศ หรือการโอนข้อมูลเพื่อประโยชน์ในการประมวลผลหรือการจัดเก็บฐานข้อมูลในต่างประเทศ **ซึ่งไม่ว่าจะส่งข้อมูลไปที่ใด ที่นั้นต้องมีความคุ้มครองข้อมูลส่วนบุคคลในระดับที่เท่าเทียมหรือมากกว่า GDPR (essential equivalence)** สำนักงานรัฐบาลทางอิเล็กทรอนิกส์ (องค์การมหาชน) คาดการณ์ว่า<u>ธุรกิจที่จะได้รับผลกระทบ ได้แก่ บริษัทโทรคมนาคม ธนาคาร การค้าส่งออกและนำเข้า ธุรกิจท่องเที่ยว และธุรกิจการบิน</u> ซึ่งเกี่ยวข้องกับการเก็บบันทึก ประมวลผล หรือโอนข้อมูลส่วนบุคคลของผู้ใช้บริการข้ามพรมแดน เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ บัตรเครดิต ซึ่งถือว่าเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว (sensitive data) นอกจากนี้ อาจส่งผลกระทบต่อ<u>ธุรกิจบริการสุขภาพ</u> ที่มีการบันทึกข้อมูลด้านสุขภาพและประวัติการรักษาพยาบาลของผู้ป่วย และ<u>ธุรกิจเทคโนโลยีสารสนเทศ</u>ที่ให้บริการผ่านเครือข่ายสังคมออนไลน์ แอปพลิเคชันบนอุปกรณ์อิเล็กทรอนิกส์ต่างๆ และการให้บริการ cloud computing ที่ให้บริการ

---

[๔] เดิมองค์กรต้องแจ้งกิจกรรมการประมวลผลข้อมูลต่อหน่วยงานท้องถิ่น (Local Data Protection Authority) ซึ่งเป็นข้อบังคับตามกฎหมายเดิม (Data Protection Act 1998) ซึ่งใน GDPR ไม่มีการกำหนดให้ต้องแจ้งอีกต่อไป

[๕] Recital 5-6 และ 101

[๖] Recital 16

[๗] Recital 50

[๘] วรรษชล ศิริจันทนันท์. *ชวนรู้จัก GDPR หลักคุ้มครองข้อมูลส่วนบุคคลของยุโรปที่จะประกาศใช้จริงกลางปีนี้.* https://themomentum.co/general-data-protection-regulation-europe/

แก่บุคคลที่มีถิ่นพำนักใน EU โดยอาจส่งผลกระทบต่อองค์กรและธุรกิจเกิดใหม่อื่นๆ ที่จะต้องพึ่งพาระบบ cloud computing และการ outsourcing ไปให้บริษัทที่รับจ้างช่วงดำเนินการต่อเพื่อลดต้นทุน[๙]

๖. นอกจากนี้ ยังอาจส่งผลต่อการทำการตลาดอิเล็กทรอนิกส์ (e-marketing) และพาณิชย์อิเล็กทรอนิกส์ที่ใช้ข้อมูลประวัติการใช้งานบนเว็บไซต์ (cookies) ในการประเมินความสนใจและป้อนโฆษณาให้ตรงกับกลุ่มเป้าหมาย การใช้อินเทอร์เน็ตเป็นสื่อกลางในการโฆษณา รวมทั้งการใช้อุปกรณ์อิเล็กทรอนิกส์ในการประมวลผลและเก็บข้อมูลของผู้รับบริการ[๑๐] เนื่องจากมีความเกี่ยวข้องกับข้อมูลที่สามารถชี้กลับมายังตัวบุคคลได้ ไม่ว่าจะเป็นสิ่งที่ใช้ระบุตัวตนบนโลกออนไลน์ (เช่น IP) หรืออัตลักษณ์บนโลกโซเชียล

<u>กรณีที่ปลายทางยังไม่มีกฎหมายที่เทียบเท่า GDPR</u>

๗. หน่วยงานที่เกี่ยวข้องอาจต้องทำสัญญาร่วมกันเพื่อพิสูจน์ประสิทธิภาพของมาตรฐานป้องกันข้อมูล รวมทั้งระบุผู้รับผิดชอบกรณีเกิดการละเมิดขึ้น เช่น (๑) การจัดทำนโยบายหรือกฎเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลภายในองค์กร (Binding Corporate Rules) เพื่อโอนข้อมูลส่วนบุคคลระหว่างสาขาในแต่ละประเทศที่มีระดับการให้ความคุ้มครองแตกต่างกัน โดยพิจารณาว่าองค์กรผู้รับโอนมีกลไกการเก็บรักษาข้อมูลส่วนบุคคลที่เป็นไปตามมาตรฐาน EU (๒) การจัดทำสัญญามาตรฐานของ EU (Model Contracts) สำหรับการโอนข้อมูลส่วนบุคคลระหว่างผู้จัดเก็บข้อมูลส่วนบุคคล (Data Controller) กับผู้ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ซึ่งจะต้องได้รับการอนุมัติจากคณะกรรมาธิการยุโรป หรือ (๓) การจัดทำความตกลงทวิภาคีเพื่อรับโอนข้อมูลส่วนบุคคลของผู้ที่มีถิ่นพำนักในอียู เช่น ความตกลง Privacy Shield ระหว่างคณะกรรมาธิการยุโรปและสหรัฐฯ ที่มีการตกลงไปเมื่อวันที่ ๒ กุมภาพันธ์ ๒๕๕๙ เป็นต้น ซึ่งอาจต้องเสียเวลาและค่าใช้จ่ายสูง และอาจเกิดความยุ่งยากซ้ำซ้อนในทางปฏิบัติ ในกรณีที่มีหน่วยงานหรือองค์กรที่เกี่ยวข้องเป็นจำนวนมาก

<u>การดำเนินการของไทย</u>

๘. ปัจจุบัน ไทยมีกฎหมายคุ้มครองข้อมูลเฉพาะรายสาขา เช่น พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และ พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต เป็นต้น โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอยู่ระหว่างการผลักดัน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ... ที่จะบังคับใช้เป็นการทั่วไป โดยยึดหลักให้มีความสอดคล้องกับ GDPR และบริบทแวดล้อมที่เหมาะสมกับประเทศไทย โดยสำหรับ SMEs กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จะมีการกำหนดขนาดของธุรกิจเป็นเล็ก กลาง และใหญ่ เพื่อกำหนดระยะเวลาในการปฏิบัติตามหลักการของกฎหมาย และมีหลักสำคัญที่จะไม่ยกเว้นหลักการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากเป็นกฎหมายกลางในการดูแลข้อมูลส่วนบุคคลของประเทศ

---

สำนักเจรจาการค้าบริการและการลงทุน
กรมเจรจาการค้าระหว่างประเทศ
เมษายน ๒๕๖๑

---

[๙] ทีมงาน ThaiEurope.net. ***กฎใหม่โอนข้อมูลส่วนบุคคลระหว่างประเทศ กระทบห่วงโซ่อุปทานโลก***.
http://www.bangkokbiznews.com/blog/detail/637251

[๑๐] เรื่องเดียวกัน