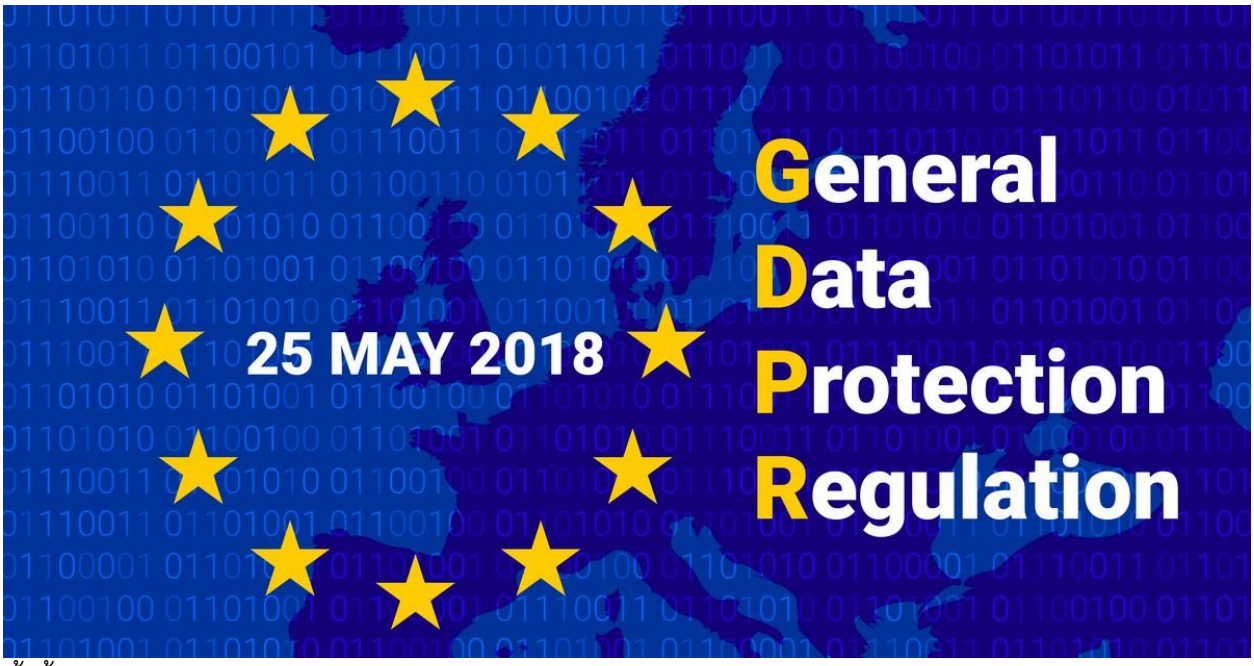
**ส่อง 6 กรณีศึกษาใน EU ที่ละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล**

**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (Personal Data Protection Act หรือใช้ตัวย่อว่า PDPA)** ที่มีในบ้านเรานั้น สาระสำคัญคือการให้ความคุ้มครองข้อมูลส่วนบุคคล (Personal Data) ที่สามารถนำไปสู่การระบุตัวตนบุคคลทั้งทางตรงและทางอ้อม ไม่ว่าจะเป็นกระดาษหรืออิเล็กทรอนิกส์ ในรูปแบบตัวหนังสือ รูปหรือเสียง เช่น เลขที่บัตรประชาชน อีเมล เบอร์โทรศัพท์ ฯลฯ เพื่อไม่ให้เจ้าของข้อมูลถูกละเมิดความเป็นส่วนตัวและให้มีมาตรการชดเชยแก่เจ้าของข้อมูลกรณีที่ถูกละเมิดข้อมูลส่วนบุคคล ดังนั้นจากที่พรบ.ฉบับนี้จะมีผลบังคับใช้ ผู้ประกอบการ องค์กรจำเป็นต้องมีมาตรการในการระมัดระวังดูแลปกป้องข้อมูลส่วนบุคคลอย่างเข้มงวด เพื่อป้องกันการถูกล่วงละเมิด ส่งผลเสียหายต่อเจ้าของข้อมูล ซึ่งเจ้าของข้อมูลเป็นได้ทั้งลูกค้า พนักงานและหุ้นส่วนธุรกิจ




ทั้งนี้ ในสหภาพยุโรปก็มีข้อกฎหมายคุ้มครองข้อมูลส่วนบุคคลเช่นกัน คือ **General Data Protection Regulation (GDPR)** บังคับใช้ในเดือนพฤษภาคม 2561 ซึ่งที่ผ่านมาก็มีองค์กรธุรกิจที่ล้มเหลวในการดูแลความปลอดภัยของข้อมูลส่วนบุคคลถูกลงโทษจากกฎหมายฉบับนี้อย่างรุนแรง มาดูรายละเอียดการละเมิด GDPR เคสสำคัญที่เกิดขึ้นในสหภาพยุโรป

**1) British Airways**

กรณีสายการบินบริติช แอร์เวย์ในเดือนมิถุนายน 2561 ที่เว็บไซต์ของสายการบินมีการเปลี่ยนเส้นทางไปสู่หน้าเพจหลอกขโมยข้อมูลของมิจฉาชีพ ทำให้ข้อมูลของลูกค้าที่ซื้อตั๋วเครื่องบินผ่านทางเว็บไซต์ราวๆ 500,000 รายตก

ไปอยู่ในมือแฮ็คเกอร์ โดยมีทั้งข้อมูลล็อคอิน ข้อมูลการเดินทาง  ชื่อ ที่อยู่ หมายเลขบัตรเครดิต ข้อมูลวันหมดอายุ เลข CVV 3 หลัก ฯลฯ บริติช แอร์เวย์โดนสำนักงานคณะกรรมาธิการด้านข้อมูล (ICO) สหราชอาณาจักรสั่งลงโทษปรับเป็นจำนวน 204.6 ล้านยูโร (ประมาณ 8,184 ล้านบาท)

**2) Marriott International Hotel**

เครือโรงแรมแมริออตต์ของสหรัฐ ถูกสำนักงาน ICO สหราชอาณาจักร สั่งปรับ 110.3 ล้านยูโร (4,412 ล้านบาท) จากเหตุการณ์ที่แฮกเกอร์เปิดเผยข้อมูลส่วนบุคคลที่เซนซิทีฟอย่างหมายเลขบัตรเครดิต หมายเลขพาสปอร์ต วันเดือนปีเกิดลูกค้ากว่า 300 ล้านรายซึ่งกว่า 30 ล้านรายเป็นประชากรสหภาพยุโรป

**3) Google**

แม้กรณีของยักษ์ใหญ่แห่งวงการดิจิทัล Google จะไม่ใช่การถูกล่วงละเมิดข้อมูล แต่ Google ก็ถูกทางการฝรั่งเศสสั่งปรับเงินจำนวน  50 ล้านยูโร (ประมาณ 200 ล้านบาท) เพราะผู้ใช้งานไม่สามารถเข้าถึงรายงานประมวลผลข้อมูลผู้บริโภค (consumer data processing statement) ได้โดยง่าย และภาษาที่ใช้อธิบายก็กำกวมไม่ชัดเจน ยิ่งไปกว่านั้น Google ยังมีความผิดที่ไม่ขอความยินยอมจากผู้บริโภคในการนำขอข้อมูลมาใช้ทำแคมเปญโฆษณาแบบ targeting ซึ่งผิดกฎหมาย GDPR

**4) Austrian Post**

เหตุการณ์นี้เกิดในช่วงต้นปี 2562 ที่ Austrian Post หน่วยงานไปรษณีย์ของออสเตรียถูกหน่วยงานป้องกันข้อมูลแห่งชาติสั่งปรับ 18.5 ล้านยูโร (ประมาณ 740 ล้านบาท) โทษฐานขายข้อมูลผู้บริโภคโดยมิชอบซึ่งเป็นการละเมิดข้อบังคับ GDPR ทั้งนี้จากการตรวจสอบพบว่า Austrian Post ได้ทำการตรวจดูข้อมูลผู้บริโภคว่าใครมีแนวโน้มลงคะแนนเสียงที่พวกเขาสนับสนุนอยู่และขายข้อมูลเหล่านั้น

**5) Deutsche Wohnen SE**

เคส Deutsche Wohnen SE ที่เกิดขึ้นในเดือนตุลาคม 2562 เป็นกรณีละเมิด GDPR ครั้งใหญ่ที่สุดของวงการอสังหาริมทรัพย์ โดย Deutsche Wohnen SE ถูกทางการปรับ 14.5 ล้านยูโร (ประมาณ 580 ล้านบาท) เพราะกระทำผิดในการเก็บข้อมูลเซนซิทีฟของผู้บริโภคนานเกินความจำเป็นโดยไม่มีเหตุผลที่ชอบธรรมตามกฎหมาย

**6) 1&1 Telecom GmbH**

เคสกรณีบริษัท 1&1 Telecom GmbH ของเยอรมนี ถูกสั่งปรับเป็นเงิน 9.5 ล้านยูโร (ประมาณ 380 ล้านบาท) ในความผิดที่ศูนย์คอลเซนเตอร์ของบริษัทไม่มีมาตการป้องกันรักษาข้อมูลลูกค้าที่ดีพอทั้งทางเทคนิคและนโยบายองค์กร โดยทางการพบว่าคนที่โทรไปติดต่อคอลเซนเตอร์ของบริษัทสามารถดึงข้อมูลลูกค้าออกมาได้เพียงแค่ใส่ชื่อกับวันดือนปีเกิด ซึ่งตรงนี้เป็นความผิดขององค์กรที่ไม่มีมาตรการพิสูจน์ตัวตนและป้องกันข้อมูลที่เข้มงวดตามกฎหมาย GDPR


กรณีเหล่านี้เป็น 6 กรณีที่โดนโทษปรับสูงสุดจากการละเมิดกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป ซึ่งนับเป็นกรณีศึกษาให้หน่วยงาน องค์กรบริษัท และประชาชนในประเทศไทยได้เรียนรู้และรับทราบเป็นแนวทางในการปฏิบัติตามได้เป็นอย่างดี

อ้างอิง :

https://secureprivacy.ai/gdpr-the-6-biggest-fines-enforced-by-regulators-so-far/

https://etda.or.th/content/personal-data-protection-act-protect-or-not.html