รวม Case เจ็บหนักจากกฎหมาย GDPR ด้านสถาบันการศึกษา ไทยรู้ไว้เป็นแบบอย่าง ก่อนถูกปรับ

หลังจากที่มีการร่างกฎหมายมาเป็นระยะเวลายาวนาน ในที่สุด พรบ.คุ้มครองข้อมูลส่วนบุคคลหรือ PDPA ก็มีผลบังคับใช้ไปแล้ว ซึ่งพรบ.ฉบับนี้มีแนวคิดที่คล้ายคลึงกับกฎหมาย General Data Protection Regulation หรือ GDPR ค่อนข้างมาก ไม่ว่าจะเป็นเรื่องกระบวนการทางกฎหมายและการแจ้งเตือน ไปจนถึงนิยามของข้อมูลและบทบาทของ Data Protection Officer ไปจนถึงประเด็นอื่นๆ อีกมากมาย

หากจะพูดง่ายๆ ก็คือ กฎหมายนี้ถูกออกแบบมาเพื่อควบคุม และดูแลข้อมูลส่วนบุคคลที่ถูกประมวล โดยมีคณะกรรมการข้อมูลส่วนบุคคลเป็นผู้กำกับ โดยเฉพาะภายหลัง PDPA หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคลถูกบังคับใช้กับสถาบันการศึกษา

PDPAThailand พบว่ามีองค์กรต่าง ๆ ทั่วโลกถูกปรับจากความผิดด้านการคุ้มครองข้อมูลส่วนบุคคลมากมาย (ทั้งจาก GDPR และ กฎหมายคุ้มครองข้อมูลส่วนบุคคล ที่บังคับใช้แต่ละประเทศ) จึงรวบรวม case study ที่เป็นประโยชน์ต่อทุกคนครับ

กรณี 1 การเปิดเผยข้อมูลสุขภาพของครูในโรงเรียนมัธยม 'Isabella Gonzaga' ประเทศอิตาลี

ประเภทของกรณีศึกษา : ประมวลผลเกินความจำเป็น

หน่วยงานกำกับด้านการดูแลข้อมูลส่วนบุคคลอิตาลี (Italian Data Protection Authority) ได้สั่งปรับผู้บริหารโรงเรียน ‘Isabella Gonzaga’ เป็นจำนวนเงิน 2,500 ยูโร (หรือประมาณ 91,005 บาท) เนื่องจากโรงเรียนได้มีการเผยแพร่เอกสารซึ่งมีข้อมูลสุขภาพส่วนบุคคลของครูบางคนบนแพลตฟอร์มออนไลน์ ซึ่งเป็นแพลตฟอร์มออนไลน์สำหรับอาจารย์ผู้สอน ในระหว่างการสอบสวนหน่วยงานกำกับดูแล พบว่าโรงเรียนได้เผยแพร่ข้อมูลสุภาพซึ่งถือเป็นข้อมูลส่วนบุคคลประเภทอ่อนไหวโดยไม่มีฐานทางกฎหมายที่ถูกต้อง ซึ่งเกี่ยวกับผลประโยชน์ที่เชื่อมโยงกับสถานะสุขภาพดังกล่าว

กรณี 2 เหตุการณ์การรั่วไหลของข้อมูลนักศึกษาและอาจารย์ของมหาวิทยาลัยเทคโนโลยีวอร์ซอ ประเทศโปแลนด์

ประเภทของกรณีศึกษา : มาตรการทางเทคนิคและองค์กรไม่เพียงพอต่อการรักษาความมั่นคงปลอดภัยของข้อมูล

หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลของโปแลนด์ (UODO) ได้มีการสั่งปรับมหาวิทยาลัยเทคโนโลยีวอร์ซอ 10,000 ยูโร (หรือประมาณ 364,000 บาท) มหาวิทยาลัยได้รายงานการละเมิดข้อมูลต่อ

หน่วยงานตามมาตรา 33 ของกฎหมาย GDPR เนื่องจากหน่วยงานหนึ่งของมหาวิทยาลัยได้ใช้แอปพลิเคชันที่สร้างโดยเจ้าหน้าที่มหาวิทยาลัย เพื่อใช้ในการลงทะเบียนหลักสูตรและสามารถเข้าถึงประวัติการสอน การประเมินผลการสอบ และการเรียกเก็บค่าธรรมเนียม

ส่งผลให้ในต้นเดือนมกราคม พ.ศ.2563 มีบุคคลที่ไม่ได้รับอนุญาตได้ทำการดาวน์โหลดฐานข้อมูลจากแอปพลิเคชันที่มีข้อมูลส่วนบุคคลของนักศึกษา และอาจารย์ มากกว่า 5,000 คน

ในการสืบสวนหน่วยงานกำกับดูแลพบว่า มหาวิทยาลัยไม่มีมาตรการทางเทคนิคและองค์กรที่เหมาะสม ในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและยังพบว่ามหาวิทยาลัยไม่ได้ทำการประเมินความเสี่ยง

กรณี 3 เหตุการณ์การใช้ ใช้เทคโนโลยีการจดจำใบหน้า (facial recognition technology) โรงเรียนแห่งหนึ่งในเมืองสเกลเลฟติออ ประเทศสวีเดน

ประเภทของกรณีศึกษา : ประมวลผลเกินความจำเป็น

หน่วยงานกำกับดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลของโปแลนด์ ได้ปรับโรงเรียนแห่งหนึ่งในเมืองสเกลเลฟติออ ประเทศสวีเดน เป็นจำนวนเงิน 18,630 ยูโร (หรือประมาณ 680,441.82 บาท) โดยโรงเรียนดังกล่าว ได้ใช้เทคโนโลยีการจดจำใบหน้า (facial recognition technology) ซึ่งเป็นข้อมูลชีวภาพตามมาตรา 9 GDPR เพื่อติดตามการเข้าชั้นเรียนของนักเรียน ซึ่งการประมวลผลข้อมูลเพื่อวัตถุประสงค์ในการติดตามการเข้าร่วมนั้นไม่เพียงพอต่อการใช้เทคโนโลยีการจดจำใบหน้า

และหน่วยคุ้มครองข้อมูลของสวีเดนสรุปว่า โครงการนี้ขัดต่อข้อบังคับของมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล (General Data Protection Regulation หรือ GDPR) จึงต้องปรับเจ้าหน้าที่เทศบาลผู้รับผิดชอบต่อข้อมูลที่เก็บได้ เจ้าหน้าที่หน่วยคุ้มครองข้อมูลยังกล่าวอีกว่า โรงเรียนล้มเหลวในการเตือนผู้ร่วมโครงการถึงผลกระทบ และโรงเรียนควรปรึกษากับหน่วยงานก่อน

กรณี 4 เหตุการณ์การใช้เครื่องแสกนลายนิ้วมือของโรงเรียนแห่งหนึ่งในกดัญสก์ ประเทศโปแลนด์

ประเภทของกรณีศึกษา : ประมวลผลเกินความจำเป็น

โรงเรียนในประเทศโปแลนด์ถูกทางการสั่งปรับเป็นเงิน 20,000 zloty (หรือราว 166,000 บาท) ตามกฎหมาย GDPR หลังจากทางโรงเรียนจัดตั้งโครงการที่นำข้อมูลลายนิ้วมือของนักเรียนมาใช้เพื่อการรับสิทธิทานอาหารกลางวัน โดยไม่มีมาตรฐานตามกฎหมาย โดยถ้านักเรียนคนใดปฏิเสธที่จะใช้ไบโอเมตริก หรือปฏิเสธการให้ข้อมูล

ลายนิ้วมือ จะต้องไปต่อท้ายแถวและต้องรอให้เด็กที่ให้ความร่วมมือในการใช้ไบโอเมตริกเข้าโรงอาหารหรือ ซื้ออาหารจนเสร็จก่อน เด็กที่ไม่เข้าร่วมจึงจะเข้ารับอาหารได้ ซึ่งเห็นได้ชัดว่ากฎเหล่านี้สร้างการปฏิบัติอย่างไม่เท่าเทียม ถึงแม้โครงการนี้มีการขอความยินยอมจากผู้ปกครองแล้ว แต่ UODO ซึ่งเป็นหน่วยงานกำกับดูแลด้านการปกป้องข้อมูลส่วนบุคคลในโปแลนด์ตัดสินว่า การใช้ข้อมูลอ่อนไหวประเภท Biometric อย่างลายนิ้วมือ เพื่อวัตถุประสงค์ในการให้สิทธินักเรียนได้รับประทานอาหารกลางวันก่อนนั้นเป็นเหตุผลที่ไม่เหมาะสม เพราะข้อมูลอ่อนไหวเหล่านี้เราต้องระมัดระวังในการเก็บ ใช้ และเปิดเผยเป็นพิเศษ และไม่ควรถูกนำไปประมวลผลหากไม่มีความจำเป็น

สถาบันการศึกษา ลองพิจารณาดูกันนะครับ ว่าคุณมีความเสี่ยงมากน้อยเพียงใด เพราะแม้เคสข้างต้นจะเป็นของต่างประเทศ แต่อย่างที่รู้กัน GDPR คือต้นแบบของ PDPA ที่ใช้ในไทย และก็ปฏิเสธไม่ได้ว่าสถาบันการศึกษามีการรวบรวม/ประมวลผลข้อมูลส่วนบุคคลจำนวนมาก ซึ่งควรมีความระมัดระวังเป็นพิเศษเพราะอาจตกเป็นเป้าการโจมตีหรือเกิดอุบัติเหตุ และเสี่ยงได้รับโทษคล้ายเคสข้างต้นเช่นกัน