บทที่ 7: การปกป้องข้อมูลส่วนบุคคล

Data Privacy & Digital Footprint

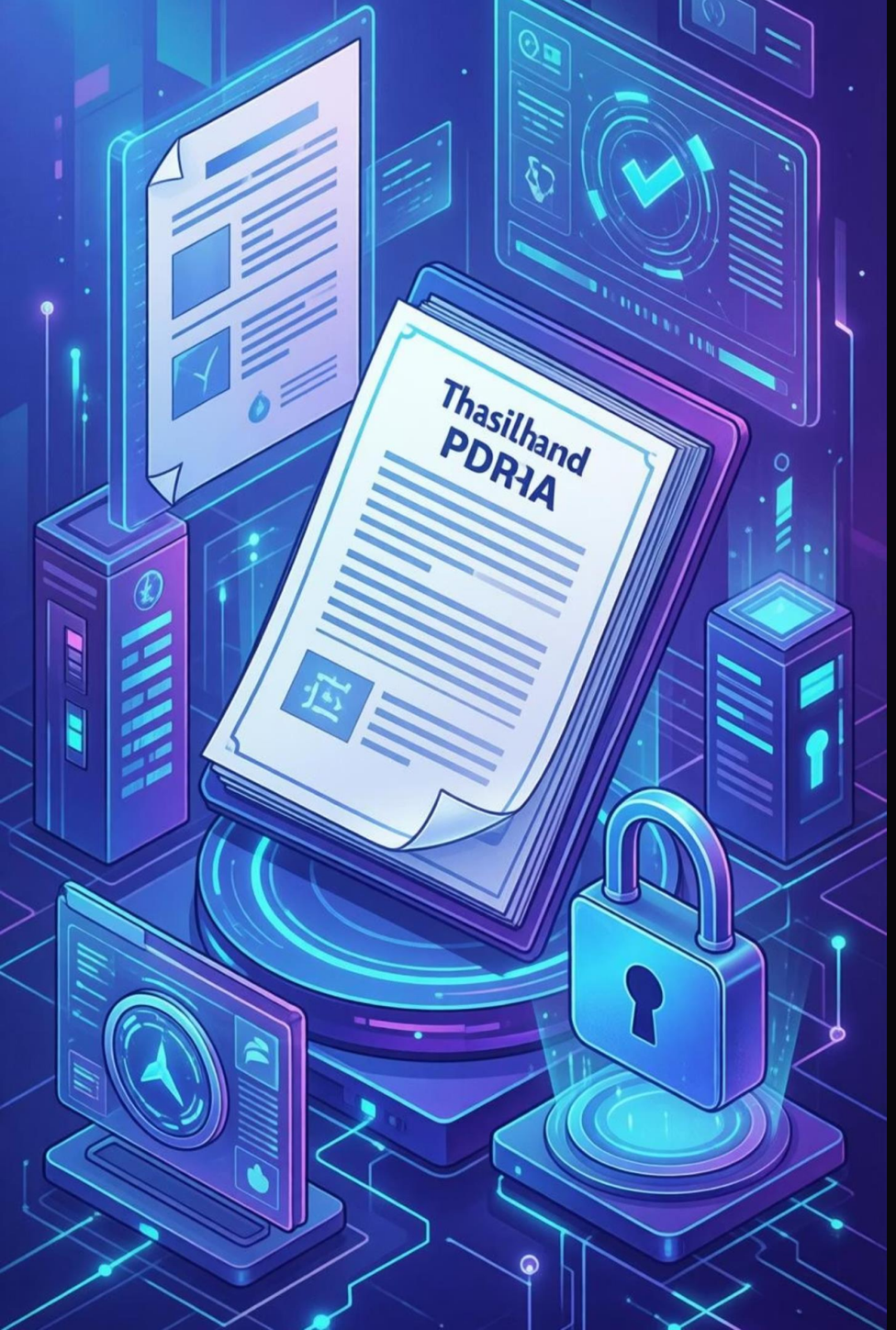
บทนำ

ข้อมูลส่วนบุคคลในยุคดิจิทัล: ทรัพย์สินที่มีค่า

ในโลกดิจิทัลที่เชื่อมโยงกันอย่างไร้พรมแดน เราทุกคนกำลังทิ้งร่องรอยดิจิทัลผ่านโซเชียลมีเดีย แอปพลิเคชัน และเว็บไซต์ต่าง ๆ ทุกวัน

ข้อมูลส่วนบุคคลของเรา ไม่ว่าจะเป็นชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ หรือแม้แต่ IP Address สามารถถูกนำไปใช้โดยไม่ได้รับอนุญาต ส่งผลกระทบต่อความเป็นส่วนตัวและความปลอดภัยของเรา

ข้อมูลสำคัญ: ปี 2025 มีรายงานว่าข้อมูลส่วนบุคคลรั่วไหลทั่วโลกเพิ่มขึ้น 35% จากปีก่อนหน้า



กฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

วันที่บังคับใช้

PDPA เริ่มบังคับใช้เต็มรูปแบบในประเทศไทย ตั้งแต่วันที่ **1 มิถุนายน 2565** เป็นต้นมา

สิทธิของเจ้าของข้อมูล

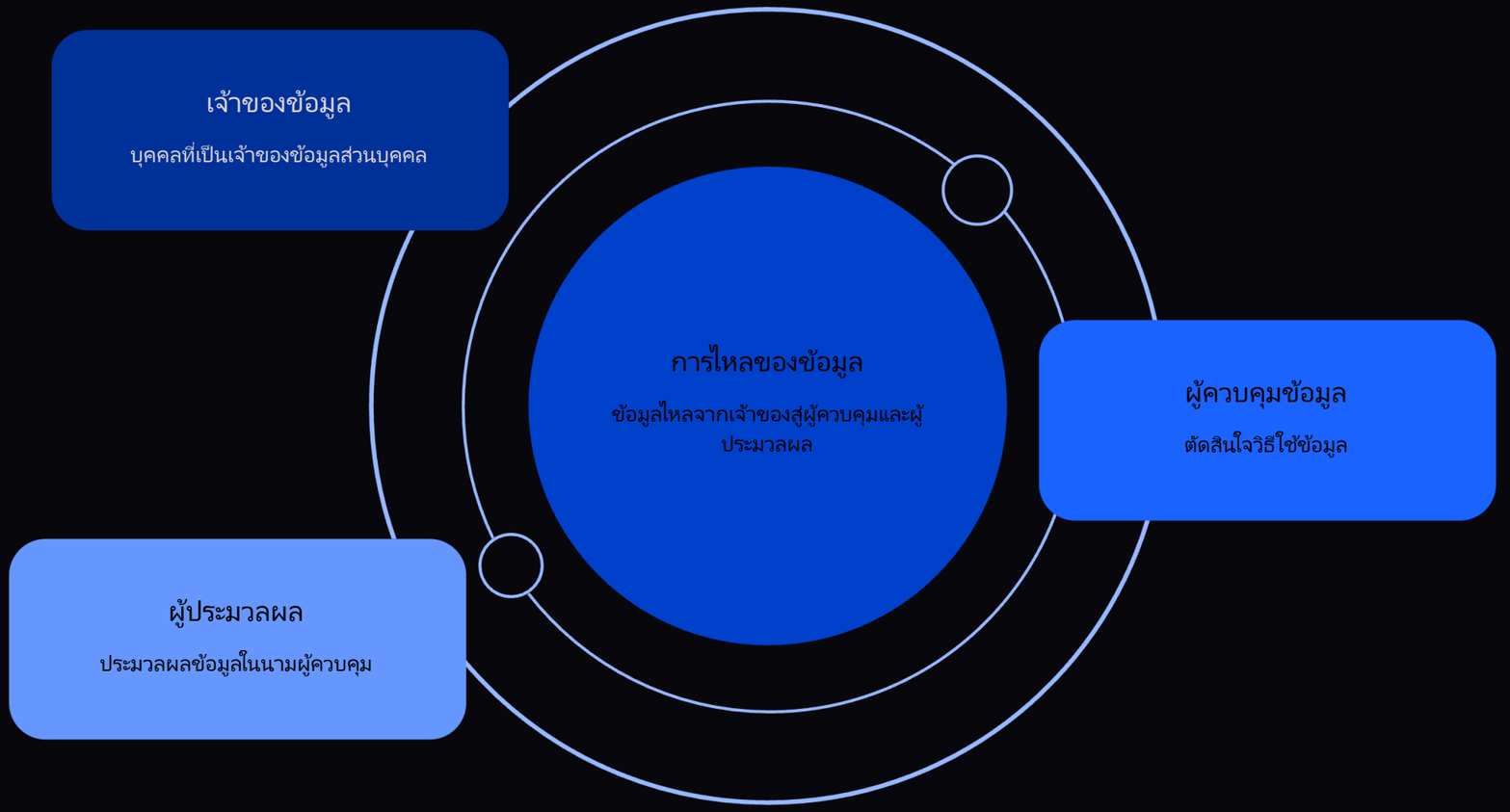
กฎหมายให้สิทธิแก่เจ้าของข้อมูล เช่น สิทธิรับทราบ ยินยอม ขอเข้าถึง แก้ไข และขอลบข้อมูลส่วนตัว

บทลงโทษ

หากองค์กรไม่ปฏิบัติตามจะมีโทษทั้งทางแพ่ง ทางอาญา และทางปกครอง รวมถึงค่าปรับสูงสุด

โครงสร้างการจัดการข้อมูลส่วนบุคคล

ความสัมพันธ์ระหว่างผู้มีส่วนเกี่ยวข้องในระบบคุ้มครองข้อมูลส่วนบุคคล



เจ้าของข้อมูล

บุคคลธรรมดาที่ข้อมูลส่วนบุคคลนั้นเกี่ยวข้องด้วย มีสิทธิควบคุมข้อมูลของตนเอง

ผู้ควบคุมข้อมูล

องค์กรหรือบุคคลที่มีอำนาจตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูล

ผู้ประมวลผลข้อมูล

องค์กรที่ดำเนินการประมวลผลข้อมูลตามคำสั่งของผู้ควบคุมข้อมูล

7 หลักการ

หลักการสำคัญของการปกป้องข้อมูลส่วนบุคคล

ตามมาตรฐาน GDPR และ PDPA ที่องค์กรทุกแห่งต้องปฏิบัติตาม

01

ความชอบด้วยกฎหมาย ความเป็นธรรม และความโปร่งใส

การเก็บข้อมูลต้องมีฐานทางกฎหมาย ดำเนินการอย่างเป็นธรรม และแจ้งให้เจ้าของข้อมูลทราบอย่างชัดเจน

02

จำกัดวัตถุประสงค์ในการใช้ข้อมูล

เก็บข้อมูลเฉพาะที่จำเป็นและใช้เพื่อวัตถุประสงค์ที่ระบุไว้เท่านั้น

03

เก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น

ไม่เก็บข้อมูลมากเกินความจำเป็นสำหรับวัตถุประสงค์ที่กำหนด

04

รักษาความถูกต้องของข้อมูล

ข้อมูลต้องเป็นปัจจุบัน ถูกต้อง และสามารถแก้ไขได้เมื่อจำเป็น

05

เก็บรักษาข้อมูลในระยะเวลาที่จำกัด

เก็บข้อมูลไว้เพียงระยะเวลาที่จำเป็น จากนั้นต้องทำลายหรือลบทิ้ง

06

รักษาความปลอดภัยของข้อมูล

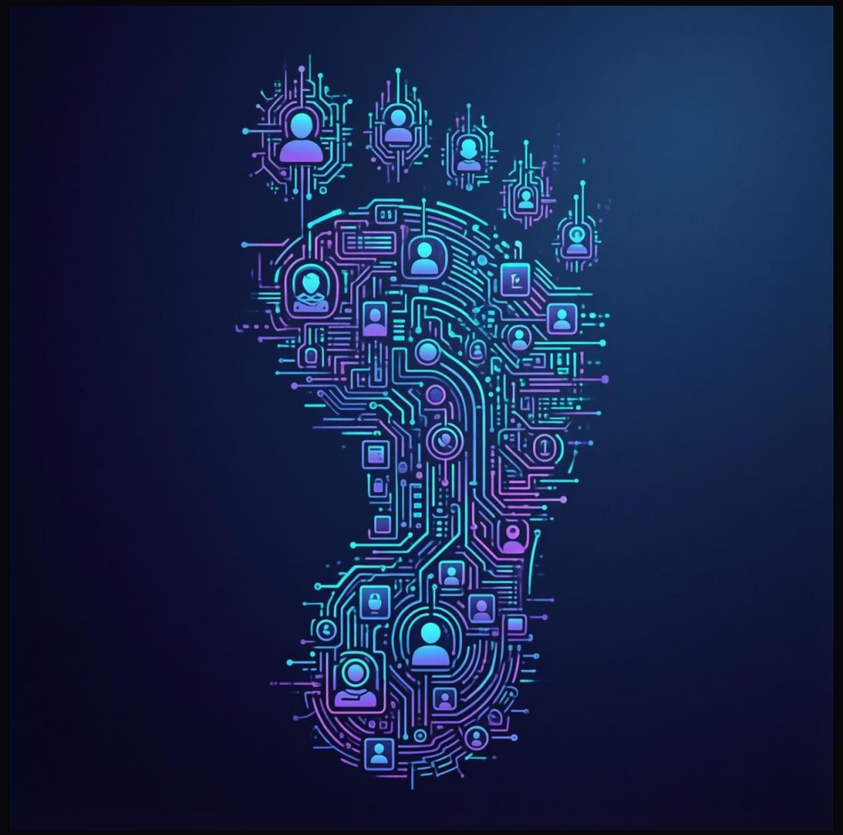
ใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการรั่วไหลหรือสูญหาย

07

ความรับผิดชอบและการตรวจสอบได้

องค์กรต้องพิสูจน์ได้ว่าปฏิบัติตามหลักการทั้งหมดอย่างครบถ้วน

ร่องรอยดิจิทัล (Digital Footprint) คืออะไร?



ร่องรอยดิจิทัลคือข้อมูลทั้งหมดที่เราทิ้งไว้เมื่อใช้งานอินเทอร์เน็ต ไม่ว่าจะเป็นประวัติการค้นหา การคลิกลิงก์ การโพสต์บนโซเชียลมีเดีย หรือการทำธุรกรรมออนไลน์

> ร่องรอยเหล่านี้สามารถถูกติดตาม วิเคราะห์ และนำไปใช้ประโยชน์โดยที่เราอาจไม่รู้ตัว

ประวัติการค้นหา

ทุกคำค้นหาบน Google หรือ Search Engine อื่น ๆ ถูกบันทึกและใช้สร้างโปรไฟล์ผู้ใช้

คุกกี้ (Cookies)

ไฟล์ขนาดเล็กที่เว็บไซต์เก็บในอุปกรณ์เพื่อติดตามพฤติกรรมและความชอบของผู้ใช้

กิจกรรมโซเชียล

โพสต์ คอมเมนต์ การกดไลค์ และการแชร์ที่สร้างภาพลักษณ์ดิจิทัลของเราในโลกออนไลน์

⚠ ความเสี่ยง

ความเสี่ยงจากการไม่ปกป้องข้อมูลส่วนบุคคล

การขโมยข้อมูลส่วนตัว

อาชญากรไซเบอร์สามารถขโมยข้อมูลส่วนตัวเพื่อใช้ในทางทุจริต เช่น **การปลอมแปลงตัวตน (Identity Theft)** เปิดบัญชีธนาคาร หรือทำธุรกรรมทางการเงินโดยไม่ได้รับอนุญาต

การถูกหลอกลวงออนไลน์

ผู้ไม่หวังดีใช้ข้อมูลส่วนตัวที่รั่วไหลเพื่อสร้างข้อความหลอกลวงผ่านโทรศัพท์หรืออีเมลที่ดูน่าเชื่อถือ ทำให้เหยื่อหลงเชื่อและถูกโกงเงิน

การสูญเสียชื่อเสียงและความน่าเชื่อถือ

ข้อมูลที่รั่วไหลอาจถูกนำไปใช้ในทางที่ผิด ทำลายชื่อเสียง ส่งผลกระทบต่อโอกาสในการทำงานและความสัมพันธ์

กรณีศึกษา: การรั่วไหลข้อมูลผู้ใช้ Facebook กว่า **87 ล้านบัญชี** ในปี 2018 ผ่านบริษัท Cambridge Analytica ส่งผลให้ข้อมูลส่วนตัวถูกนำไปใช้ในการโฆษณาทางการเมืองโดยไม่ได้รับอนุญาต

การป้องกัน

วิธีปกป้องข้อมูลส่วนบุคคลและร่องรอยดิจิทัล

แนวทางปฏิบัติที่ทุกคนสามารถทำได้เพื่อเพิ่มความปลอดภัยให้กับข้อมูลส่วนตัว

ตรวจสอบการตั้งค่าความเป็นส่วนตัว

ตรวจสอบและปรับการตั้งค่าความเป็นส่วนตัวในโซเชียลมีเดีย แอปพลิเคชัน และบริการออนไลน์ต่าง ๆ เป็นประจำ จำกัดการเข้าถึงข้อมูลเฉพาะคนที่จำเป็น

ระมัดระวังการให้ข้อมูล

คิดให้รอบคอบก่อนให้ข้อมูลส่วนบุคคลบนแพลตฟอร์มออนไลน์ อ่านนโยบายความเป็นส่วนตัวและเงื่อนไขการใช้งานก่อนยินยอม ไม่แชร์ข้อมูลที่ละเอียดอ่อนโดยไม่จำเป็น

ใช้รหัสผ่านที่แข็งแรง

สร้างรหัสผ่านที่มีความซับซ้อน ประกอบด้วยตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์พิเศษ เปลี่ยนรหัสผ่านเป็นประจำ และใช้รหัสผ่านต่างกันสำหรับแต่ละบริการ

จัดการคุกกี้และการติดตาม

ใช้เครื่องมือจัดการคุกกี้ เปิดใช้งานโหมด Do Not Track บนเบราว์เซอร์ และบล็อกการติดตามโฆษณาที่ไม่จำเป็น เพื่อลดร่องรอยดิจิทัลที่ถูกเก็บรวบรวม

กรณีศึกษา

องค์กรไทยที่ประสบความสำเร็จในการปกป้องข้อมูล

ธนาคารกรุงเทพ

นำระบบเข้ารหัสข้อมูลระดับสูง (End-to-End Encryption) และระบบยืนยันตัวตนสองชั้น (Two-Factor Authentication) มาใช้กับทุกธุรกรรมออนไลน์ เพื่อความปลอดภัยสูงสุด

92%

ความพึงพอใจของลูกค้า

ลูกค้ามั่นใจในระบบรักษาความปลอดภัยข้อมูล

AIS (แอดวานซ์ อินโฟร์ เซอร์วิส)

มีนโยบายความเป็นส่วนตัวที่โปร่งใสและชัดเจน พร้อมระบบแจ้งเตือนอัตโนมัติเมื่อมีการเข้าถึงข้อมูลส่วนบุคคล ให้ลูกค้าควบคุมข้อมูลของตนเองได้อย่างเต็มที่

45%

การลดความเสี่ยง

ลดอุบัติการณ์การรั่วไหลของข้อมูลลงได้

ผลลัพธ์ที่ได้รับ

บริษัทที่ปฏิบัติตาม PDPA อย่างเคร่งครัดได้รับความไว้วางใจจากลูกค้าและคู่ค้าเพิ่มขึ้นอย่างมีนัยสำคัญ สร้างความได้เปรียบในการแข่งขันและลดความเสี่ยงทางกฎหมาย

100%

การปฏิบัติตามกฎหมาย

สอดคล้องกับ PDPA และมาตรฐานสากลทุกประการ

สรุปและเชิญชวน

ข้อมูลคือทรัพย์สิน

ข้อมูลส่วนบุคคลของเราคือทรัพย์สินที่มีค่าและต้องได้รับการปกป้องอย่างจริงจัง ในโลกดิจิทัลที่ข้อมูลสามารถถูกนำไปใช้ในทางที่ผิดได้ง่าย

PDPA คือเครื่องมือ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) เป็นเครื่องมือสำคัญที่ช่วยให้เรามีสิทธิและความปลอดภัยในการควบคุมข้อมูลของตนเอง

ร่วมมือกันสร้างวัฒนธรรม

ทุกคน ทั้งบุคคล องค์กร และหน่วยงานภาครัฐ ต้องร่วมมือกันสร้างวัฒนธรรมการใช้ข้อมูลอย่างรับผิดชอบและมีจริยธรรม

เริ่มต้นวันนี้

ปกป้องข้อมูลของคุณ เพื่ออนาคตที่ปลอดภัยกว่า

ความปลอดภัยของข้อมูลเริ่มต้นจากการตระหนักรู้และการลงมือปฏิบัติของเราทุกคน ไม่ว่าจะเป็นการตั้งรหัสผ่านที่แข็งแรง การตรวจสอบการตั้งค่าความเป็นส่วนตัว หรือการใช้วิจารณญาณก่อนแชร์ข้อมูล

ตรวจสอบการตั้งค่าวันนี้

ปกป้องข้อมูลของคุณ

แบ่งปันความรู้