

PDPA

PDPA คือ กฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยระบุให้องค์กรหรือหน่วยงานที่เกี่ยวข้องที่เก็บข้อมูลส่วนบุคคลของประชาชนไม่ว่าจะเป็นบริษัทเอกชน หรือหน่วยงานภาครัฐ ต้องไม่นำเอาข้อมูลส่วนตัวของเราไปใช้ในกิจกรรมอื่น ๆ ที่เราไม่ยินยอม

ข้อมูลส่วนบุคคลนั้นครอบคลุม ตั้งแต่ ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ไปจนถึงอีเมล หมายเลขบัตรประจำตัวประชาชน และอื่นๆ นอกจากนี้ กฎหมายยังคุ้มครองไปถึงข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) เช่น เชื้อชาติ เผ่าพันธุ์ ความเห็นทางการเมือง ความเชื่อ ลัทธิ ศาสนา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลทางด้านสุขภาพ ข้อมูลทางพันธุกรรม และ ข้อมูลชีวภาพ

บทลงโทษของ PDPA คือ

- โทษทางอาญา จำคุกไม่เกิน 1 ปี และ/หรือ ปรับสูงสุด 1 ล้านบาท
- โทษทางแพ่ง จ่ายสินไหมไม่เกิน 2 เท่าของสินไหมที่แท้จริง
- โทษทางปกครองปรับไม่เกิน 5 ล้านบาท

การยินยอม (CONSENT)

คือ การยอมรับการจัดเก็บ การใช้และ/หรือการประมวลผลเพื่อวัตถุประสงค์ตามเงื่อนไขที่ระบุไว้ในเอกสาร

สิ่งที่ต้องตรวจสอบ

1. ตรวจสอบข้อมูลที่ได้รับจากลูกค้า ในปัจจุบันไม่ว่าจะช่องทางใดที่เรานำมาเก็บไว้ ว่าบริษัทเรามี consent หรือยัง

กรณีที่ 1 มี consent หากอยู่ในเงื่อนไขที่ตกลงกันไว้ในครั้งแรกไม่ผิดสามารถใช้ได้เลย แต่หากใช้นอกเหนือจากที่ตกลงไว้ ต้องส่งคำร้องขอใช้ใหม่ เช่น ต้องการเพิ่ม active เช่น Co-promotion หากเพิ่มจากเดิมต้องขอใหม่

กรณีที่ 2 ไม่มี consent ก่อนหน้า ต้องขอใหม่เท่านั้น

(หากมีหลาย version ต้องเก็บ version control ของ consent ด้วย)

2. ในส่วนของระบบดูแลและแบ่งเป็น 2 ส่วน (กรณีที่ลูกค้าต้องการแก้ไขข้อมูล)

กรณีที่ 1 admin

ถ้าไม่มีระบบให้ลูกค้าแก้ไขด้วยตัวเองได้ ต้องมีทำผ่าน call center หรือสร้างทีมที่มีอำนาจลบข้อมูลได้ทันเวลา ภายใน 30 วัน

กรณีที่ 2 ทำโปรแกรม

1. ต้องมี data protection เช่น firewall หรือ password 2 ชั้น

2. identify การทำ ux การทำขั้นตอน การเข้าถึงข้อมูลหลายชั้น หากเป็นให้แก้ไขด้วยตนเอง

3. ในส่วนของการขอ consent

การดำเนินการเขียน Consent

- ขอ consent data ใช้ทำอะไร

- เก็บถึงเมื่อไหร่

- เราเก็บชื่อบริษัทอะไร

- ถ้าลูกค้าต้องการถอน consent ถอนได้ที่ช่องทางไหน (ลูกค้ามีสิทธิขอลบ, ขอแก้ไข, ขอระงับ, โอนย้าย, ขอดู)

อสังหาริมทรัพย์ สิ่งที่ต้องทำเพิ่มเติม

- 1.ตรวจสอบข้อมูลที่ได้ทำการเก็บไว้ว่า ได้มี consent จากลูกค้าหรือยัง หากยังไม่มีให้ทำเรื่องขอ consent
- 2.จัดทำ cookie consent แยกประเภทให้ละเอียด เช่น necessary cookies, functional cookies, marketing cookies ในต่างประเทศนิยมแยก consent ตามข้อมูล แต่ไม่จำเป็นต้องแยกเสมอไป
- 3.จัดทำระบบเก็บข้อมูล โดยระบบควรมีการเก็บข้อมูลเป็น record เพื่อให้ทราบถึงวันเวลาในการเก็บข้อมูล และ version ของไฟล์ข้อมูลนั้นๆ (ในกรณีที่ข้อมูลมีการเปลี่ยนต้องส่งให้ลูกค้า consent ใหม่ทุกครั้ง)

หมายเหตุ

- ต้องทำตามคำขอภายใน 30 วันตามกฎหมาย
- กฎหมายเริ่มใช้ 27 พฤษภาคม แต่มีผลเมื่อ consumer ขอตรวจสอบ