SUAN SUNANDHA RAJABHAT UNIVERSITY

ETHICS, LAW, AND DATA PROTECTION IN CRM

จริยธรรม กฎหมาย และการคุ้มครองข้อมูลในงาน CRM

KARDPAKORN NINAROON

INTRO

- **การบริหารจัดการลูกค้าสัมพันธ์ (CRM)** ในยุคปัจจุบัน **ครอบคลุมถึงการติดตามพฤติกรรม**ดิจิทัลและ**ความชอบส่วนบุคคล**ผ่านปัญญาประดิษฐ์ ซึ่ง**ช่วยให้ธุรกิจ**สามารถส่ง**มอบประสบการณ์ที่ "รู้ใจ"** ลูกค้าได้อย่างแม่นยำและสามารถคาดการณ์พฤติกรรมในอนาคตได้ **แต่ในขณะเดียวกันก็นำมาซึ่งคำถามสำคัญเกี่ยวกับความเหมาะสม**และ**ความปลอดภัยของข้อมูลส่วนบุคคล**ของ**ลูกค้า**

- **เมื่อข้อมูลเปรียบเสมือนสินทรัพย์ที่มีค่า**ที่สุด **ความรับผิดชอบต่อสินทรัพย์นั้น**จึงเป็นเรื่องของ **"ความไว้วางใจ"** (Trust) ซึ่งเป็นรากฐานของระบบ CRM **หากปราศจากความเชื่อใจ ลูกค้าจะไม่มอบข้อมูลที่แท้จริง**ให้แก่แบรนด์ และ**ส่งผลให้ระบบ CRM สูญเสียประสิทธิภาพ**ไปโดยปริยาย **การทำความเข้าใจจริยธรรม**และ**กฎหมาย**จึง**ไม่ใช่เพียง**เพื่อ**หลีกเลี่ยงโทษ**ปรับ **แต่คือการสร้างมาตรฐานการดำเนินธุรกิจที่ยั่งยืน**ในระยะยาว

ธรรมาภิบาลข้อมูลลูกค้า

- การก้าวเข้าสู่**การบริหารจัดการลูกค้าอย่างมืออาชีพ** สิ่งแรกที่**ต้องตระหนัก**คือ **"ธรรมาภิบาลข้อมูล"** ซึ่ง**หมายถึง การวางโครงสร้างอำนาจหน้าที่**และ**กฎระเบียบในการบริหารจัดการข้อมูล**ภายในองค์กร **เพื่อให้มั่นใจ**ว่าข้อมูลเหล่านั้นมี**ความถูกต้อง ปลอดภัย** และถูก**นำไปใช้**ได้อย่างมีประสิทธิภาพสูงสุดตามมาตรฐานสากล

- อย่างไรก็ตาม **ธรรมาภิบาลข้อมูลในงาน CRM ไม่ได้หยุด**อยู่**แค่ความถูกต้องของตัวเลข**ในระบบ **แต่**ต้อง**ควบคู่ไปกับ "จริยธรรม"** ซึ่งเป็นเข็มทิศนำทางในจุดที่กฎหมายอาจยังไปไม่ถึง จริยธรรมในที่นี้**คือการตั้งคำถามว่า "แม้เราจะมีสิทธิ์เข้าถึงข้อมูลนี้ตามเทคนิค แต่เราควรนำมันมาใช้ในทางที่อาจรบกวนความเป็นส่วนตัวของลูกค้าหรือไม่?"** การมีธรรมาภิบาลข้อมูลที่ดีจะ**ช่วยให้องค์กรสามารถตอบคำถาม**เหล่านี้**ได้อย่างมีหลักการ** โดย**มุ่งเน้น**ที่**ความโปร่งใส** และ **การคำนึงถึงประโยชน์ของลูกค้า** เป็นที่ตั้ง **มากกว่าเพียงแค่ผลกำไร**ระยะสั้นขององค์กรเท่านั้น ซึ่งประกอบด้วย 3 หัวข้อสำคัญ ดังนี้:

ธรรมาภิบาลข้อมูลลูกค้า

ความสำคัญของจริยธรรมต่อความเชื่อมั่นในตราสินค้า (Brand Trust)

ในระบบการบริหารจัดการลูกค้าสัมพันธ์ **ความเชื่อมั่น** (Trust) **เปรียบเสมือนเป็น "สกุลเงิน"** ที่สำคัญที่สุดของความสัมพันธ์ การที่**ลูกค้าตัดสินใจให้ข้อมูล**ส่วนบุคคล **ตั้งอยู่บนสมมติฐาน**ที่ว่า**องค์กรจะดูแลข้อมูลเหล่านั้นอย่างมีจริยธรรม** และ**นำไปใช้**เพื่อ**ยกระดับประสบการณ์**ของพวกเขาให้ดียิ่งขึ้น หากปราศจากสิ่งนี้ความสัมพันธ์ก็ไม่อาจเกิดขึ้นได้

จริยธรรมในฐานะรากฐานของความจงรักภักดี (Loyalty)

การยึดถือจริยธรรมเป็นหลักปฏิบัติ **ส่งผลโดยตรงต่อการสร้างความเชื่อมั่น**ในตราสินค้า (Brand Trust) ซึ่งมีความ**สำคัญเทียบเท่ากับคุณภาพสินค้า** การไม่แอบนำข้อมูลไปขายต่อหรือการแจ้งเตือนเมื่อเกิดข้อผิดพลาด จะช่วย**เปลี่ยนจาก "ลูกค้าขาจร" ให้กลายเป็น "ลูกค้าประจำ"** จริยธรรม จึงเป็นรากฐานสำคัญที่ทำให้ลูกค้าพร้อมจะปกป้องและเติบโตไปพร้อมกับองค์กรในระยะยาว

ธรรมาภิบาลข้อมูลลูกค้า

ผลกระทบจากการขาดจริยธรรมต่อมูลค่าแบรนด์

การขาดจริยธรรมในการจัดการข้อมูล **นำมาซึ่งความเสียหาย**ที่ไม่อาจประเมินค่าได้ และทำให้**ลูกค้าเกิดความรู้สึก "ถูกทรยศ"** ซึ่ง**นำไปสู่การยกเลิกใช้บริการ**ที่พุ่งสูงขึ้น และ**ทำลายภาพลักษณ์ชื่อเสียง**ที่ต้องใช้เวลานานหลายปีกว่าจะกอบกู้กลับคืนมาได้ **โดยเฉพาะในโลกโซเชียลมีเดีย**ที่เสียงวิพากษ์วิจารณ์ด้านลบเพียงครั้งเดียว อาจทำลายความเชื่อมั่นที่สร้างมาเป็นสิบปีให้พังทลายลงได้

ดังนั้น **การผนวกจริยธรรม**เข้าเป็นส่วนหนึ่งของวัฒนธรรมองค์กรในการทำ CRM จึง**เป็นการสร้างความได้เปรียบทางการแข่งขัน**ที่ยั่งยืน **เพราะ**ในวันที่**คู่แข่งสามารถเลียนแบบเทคโนโลยีหรือตัดราคาได้เท่ากัน สิ่งเดียวที่จะรั้งลูกค้าไว้ได้คือ "ความไว้วางใจ"** ที่แบรนด์มีให้ต่อความเป็นส่วนตัวและสิทธิของลูกค้านั่นเอง

ธรรมาภิบาลข้อมูลลูกค้า

การตลาดแบบรู้ใจ (Personalization) กับ การละเมิดสิทธิ (Privacy Invasion)

การทำการตลาดแบบรู้ใจเพื่อมอบประสบการณ์ที่ตรงใจลูกค้า มีความท้าทายในการ**แยกแยะระหว่าง "ความใส่ใจ"** กับ **"ความน่าสะพรึงกลัว"** เพราะ**หากก้าวข้ามเส้นแบ่งนี้ไป** การตลาดที่ตั้งใจจะสร้างความประทับใจ **อาจกลายเป็นการละเมิดความเป็นส่วนตัวในสายตาลูกค้าทันที** นักการตลาด**จึงต้องระวังเส้นบางๆ** ระหว่างการนำเสนอสินค้าแบบรู้ใจกับการละเมิดสิทธิประเด็นสำคัญที่ต้องพิจารณา ประกอบด้วย:

- **พลังของการเดาใจ vs. ความรู้สึกถูกสอดแนม:** การที่ระบบ CRM วิเคราะห์ความสนใจแล้วส่งคูปองให้ถือเป็นความเก่งกาจ แต่**หากใช้ข้อมูลเชิงลึกที่ลูกค้าไม่ยินยอม**เปิดเผยโดยตรง จะ**สร้างความรู้สึกเหมือนถูกสอดแนม**และ**เกิดคำถามว่า "แบรนด์รู้เรื่องนี้ได้อย่างไร?"** ซึ่ง**เป็นสัญญาณของการละเมิดพื้นที่ส่วนตัว** ความรู้สึกถูกคุกคามนี้**ส่งผลเสียต่อความสัมพันธ์**มากกว่าผลดี และ**ทำลายพลังของการเดาใจที่แบรนด์ตั้งใจสร้างขึ้น**

ธรรมาภิบาลข้อมูลลูกค้า

การตลาดแบบรู้ใจ (Personalization) กับ การละเมิดสิทธิ (Privacy Invasion)

- **ทฤษฎีความโปร่งใส (กุญแจสำคัญในการขีดเส้นแบ่ง): สิ่งที่แยกการทำตลาดแบบรู้ใจออกจากความรู้สึกถูกคุกคามคือ "ความโปร่งใส" และ "การให้สิทธิ์ควบคุม" ลูกค้าจะยอมรับการใช้ข้อมูลส่วนบุคคลได้ก็ต่อเมื่อ:**
  - **ได้รับคุณค่าที่ชัดเจน:** ลูกค้ายินดีให้ข้อมูลถ้า**แลกกับสิทธิประโยชน์**ที่คุ้มค่า
  - **มีความโปร่งใส:** แบรนด์บอกอย่าง**ตรงไปตรงมา**ว่าเก็บข้อมูลจากแหล่งใด
  - **มีทางเลือก: ลูกค้าสามารถปรับระดับ**ความ "รู้ใจ" หรือปิดการทำงานบางส่วนได้ตามต้องการ
- **ปรากฏการณ์ "ปัจจัยที่น่าขนลุก" ในงาน CRM: แต่ละบุคคล**มีเส้นแบ่ง**ความเป็นส่วนตัวไม่เท่ากัน**ตามวัยและทัศนคติ **การฝืนใช้ข้อมูลรุกรานพื้นที่ส่วนตัว**เพียงเพราะระบบทำได้โดยไม่คำนึงถึงความพร้อมของลูกค้า **คือความล้มเหลว**ในระยะยาว **ระบบ CRM ที่ดี**จึง**ต้องมีรูปแบบการจัดการการตั้งค่าต่างๆ** เพื่อให้**ลูกค้า**แต่ละราย**เป็นผู้กำหนด "เส้นแบ่ง"** ของตนเอง

ธรรมาภิบาลข้อมูลลูกค้า

จริยธรรมการใช้ AI และ Algorithm ในการวิเคราะห์พฤติกรรมลูกค้า

การใช้ **AI และ Algorithm** ในระบบ CRM ได้**เปลี่ยนฐานข้อมูล**ให้**เป็น "สมองกล"** ที่ทำหน้าที่**คาดการณ์ความต้องการของลูกค้าล่วงหน้า** อย่างไรก็ตาม การมอบอำนาจให้เทคโนโลยีทำหน้าที่ตัดสินใจแทนมนุษย์ในงานบริหารความสัมพันธ์ลูกค้านั้น **นำมาซึ่งความรับผิดชอบทางจริยธรรมรูปแบบใหม่**ที่จำเป็นต้องตระหนักถึงเพื่อความถูกต้องแม่นยำ ได้แก่:

1. **ปัญหาความลำเอียงของอัลกอริทึม: AI อาจ**นำไปสู่การ**เลือกปฏิบัติ หากข้อมูลที่ใช้สอนระบบมีความลำเอียงแฝงอยู่** (เช่น การปฏิเสธข้อเสนอจากเพศหรือภูมิลำเนา) จึง**ต้องหมั่นตรวจสอบ** เพื่อให้แน่ใจว่าอัลกอริทึมไม่ได้ประเมินจากปัจจัยที่ไม่เหมาะสมจนกลายเป็นการตอกย้ำความเหลื่อมล้ำ การ**ดูแลไม่ให้ระบบกลายเป็นเครื่องมือที่สร้างความไม่เท่าเทียม**ในสังคม จึงเป็นหน้าที่สำคัญในการใช้เทคโนโลยีวิเคราะห์พฤติกรรม

ธรรมาภิบาลข้อมูลลูกค้า

จริยธรรมการใช้ AI และ Algorithm ในการวิเคราะห์พฤติกรรมลูกค้า

2. **ความโปร่งใสและการอธิบายได้:** ความท้าทายของ AI ใน CRM คือปัญหาที่**ระบบให้ผลลัพธ์ แต่ไม่สามารถอธิบายเหตุผลเบื้องหลังได้** จริยธรรมกำหนดว่าแบรนด์ต้องอธิบายให้ลูกค้าทราบได้ถึงที่มาของข้อเสนอหรือการจัดกลุ่มลูกค้าตามหลักความโปร่งใส
3. **การรักษาเจตจำนงอิสระของลูกค้า: การใช้อัลกอริทึมเพื่อ "ชี้นำ" ต้องระวังไม่ให้กลายเป็นการควบคุมพฤติกรรม**หรือ**บิดเบือนข้อมูล**เพื่อใช้จุดอ่อนทางจิตวิทยา จึงควรใช้ AI เพื่อสนับสนุนการตัดสินใจ ให้ลูกค้าได้รับความสะดวกสบายมากขึ้น การ**รักษาความเป็นอิสระในการเลือกของลูกค้า** ที่ทำให้ความสัมพันธ์ระหว่างแบรนด์กับลูกค้ายั่งยืน
4. **ความรับผิดชอบต่อผลลัพธ์: เมื่อ AI ทำงานผิดพลาด** (เช่น ส่งข้อความที่สร้างความอับอายหรือความเข้าใจผิดไปให้ลูกค้า) แบรนด์**ไม่สามารถปัดความรับผิดชอบ**โดยอ้างว่าเป็นความผิดของระบบได้ องค์กรจึง**ต้องมี "มนุษย์" คอยควบคุม** และ**พร้อมที่จะเข้าแก้ไขสถานการณ์เมื่อระบบอัตโนมัติทำงานนอกเหนือขอบเขต**จริยธรรมที่วางไว้

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

- **ธรรมาภิบาลและจริยธรรม** คือ**ความรับผิดชอบที่องค์กร "สมัครใจ"** กระทำเพื่อ**สร้างความเชื่อมั่น**และ**รักษาความสัมพันธ์อันดีกับลูกค้า** **แต่เมื่อการละเมิด**ข้อมูลส่วนบุคคล**ส่งผลกระทบในวงกว้าง**เกินกว่าที่จริยธรรมขององค์กรใดองค์กรหนึ่ง จะควบคุมได้เพียงลำพัง **ภาครัฐจึงเข้ามามีบทบาทกำหนดบรรทัดฐานขั้นต่ำ ผ่านข้อบังคับทางกฎหมาย**ที่ทุกธุรกิจต้องปฏิบัติตามอย่างเท่าเทียมกัน

- **ในประเทศไทย** **การจัดการข้อมูล**ลูกค้าสัมพันธ์**ได้ก้าวเข้าสู่ยุคใหม่**นับ**ตั้งแต่**การประกาศใช้ **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA)** ซึ่ง**กลายมาเป็นแม่บทหลักที่เปลี่ยนวิธีคิด**ของคนทำ CRM ไปอย่างสิ้นเชิง **จากเดิม**ที่เคยมองว่าข้อมูล**ลูกค้าเป็น "สมบัติของบริษัท" มาสู่**การยอมรับว่า**ข้อมูลเหล่านั้นเป็น "สิทธิของเจ้าของข้อมูล"** ที่**บริษัทเพียงแต่ขออนุญาตนำมาใช้ชั่วคราว**เท่านั้น ซึ่งประกอบด้วย 3 หัวข้อสำคัญ ดังนี้:

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

สรุปสาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่เกี่ยวข้องกับธุรกิจ

การประกาศใช้ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือที่เรียกติดปากว่า PDPA ไม่ใช่เพียงการเพิ่มขั้นตอนทางเอกสาร แต่**คือการวางมาตรฐานใหม่ในการบริหารจัดการข้อมูลลูกค้า**สำหรับธุรกิจไทย โดยสาระสำคัญที่นักบริหารความสัมพันธ์ลูกค้า จำเป็นต้องทำความเข้าใจเพื่อให้นำไปประยุกต์ใช้ได้อย่างถูกต้อง มีดังนี้:

1. **นิยามของข้อมูลส่วนบุคคล:** ในงาน CRM เราต้องแยก**ข้อมูลออกเป็น 2 ประเภทหลักตามกฎหมาย** ได้แก่:
    - **ข้อมูลส่วนบุคคลทั่วไป: ข้อมูลที่ทำให้ระบุตัวตนของลูกค้าได้** ไม่ว่า**ทางตรง**หรือ**ทางอ้อม** (เช่น ชื่อ-นามสกุล, เบอร์โทรศัพท์, อีเมล, ที่อยู่, ไปจนถึงหมายเลข IP Address) หรือข้อมูล Cookies ที่แบรนด์ใช้ติดตามพฤติกรรมบนเว็บไซต์
    - **ข้อมูลส่วนบุคคลอ่อนไหว: ข้อมูลที่มีความละเอียดอ่อน**และ**เสี่ยงต่อการถูกเลือกปฏิบัติ** (เช่น ศาสนา, ข้อมูลสุขภาพ, ข้อมูลพันธุกรรม, หรือความเห็นทางการเมือง) ซึ่งก**ารเก็บข้อมูล**ส่วนนี้**ต้องได้รับความยินยอม**โดยชัดแจ้งเสมอ

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

สรุปสาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่เกี่ยวข้องกับธุรกิจ

2. **บทบาทหน้าที่ภายใต้กฎหมาย:** ในการทำงานกับระบบ CRM ข้อมูลลูกค้าจะมีการเคลื่อนย้ายระหว่างหน่วยงานและคู่ค้าเสมอ กฎหมายจึงกำหนดบทบาทให้ชัดเจนเพื่อระบุความรับผิดชอบ ดังนี้:
    - **ผู้ควบคุมข้อมูลส่วนบุคคล:** คือ**ตัวองค์กรหรือธุรกิจ** ที่เป็นผู้ตัดสินใจว่าจะ**เก็บข้อมูลอะไร** และเอาไป**ใช้ทำอะไร** ถือเป็นผู้**รับผิดชอบหลักต่อตัวลูกค้า**
    - **ผู้ประมวลผลข้อมูลส่วนบุคคล:** คือ**หน่วยงานภายนอก** ที่แบรนด์จ้างมาจัดการข้อมูล เช่น ผู้ให้บริการระบบ Cloud CRM หรือบริษัท Agency ที่ทำการตลาดให้ ซึ่ง**ต้องทำตามคำสั่งของผู้ควบคุมข้อมูล**เท่านั้น

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

สรุปสาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่เกี่ยวข้องกับธุรกิจ

3. **หลักปฏิบัติ 3 ประการของการบริหารจัดการข้อมูล:** เพื่อสร้างระบบ CRM ที่ "**สง่างาม**" และ "**ปลอดภัย**" นักบริหารความสัมพันธ์ลูกค้า**ต้องยึดถือหลักปฏิบัติ 3 ข้อ**:
   - **หลักความโปร่งใส: ต้องแจ้งวัตถุประสงค์การจัดเก็บข้อมูล**ผ่าน **"นโยบายความเป็นส่วนตัว"** อย่าง**ตรงไปตรงมา**และ**เข้าใจง่าย**
   - **หลักการใช้ข้อมูลตามวัตถุประสงค์:** ข้อมูลที่เก็บมาเพื่อมอบส่วนลด ต้องใช้เพื่อการนั้นเท่านั้น **ห้ามนำไปแชร์ต่อ**หรือ**ใช้ในกิจกรรมอื่น**ที่ลูกค้าไม่ได้ยินยอมล่วงหน้า
   - **หลักการเก็บข้อมูลเท่าที่จำเป็น:** ยึดถือแนวคิดการ**เก็บเฉพาะข้อมูลที่จำเป็น**ต่อการบรรลุเป้าหมายทางธุรกิจ หากนักการตลาดสามารถวิเคราะห์พฤติกรรมได้โดยไม่ใช้เลขบัตรประชาชน ก็ไม่ควรบังคับให้ลูกค้าต้องระบุข้อมูลนั้น

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

สรุปสาระสำคัญของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ที่เกี่ยวข้องกับธุรกิจ

4. **ผลกระทบและความเชื่อมั่น:** ค่าเสียหายจาก**การละเมิด PDPA** นั้นไม่ได้จำกัดอยู่เพียงตัวเงิน แต่มัก**มาพร้อมกับผลกระทบรุนแรงใน 3 มิติ**:
    - **โทษทางกฎหมาย:** ค่า**ปรับ**ทางปกครอง**สูงสุดถึง 5 ล้านบาท** และโทษทางอาญาที่**อาจถึงขั้นจำคุก**
    - **ความเสียหายทางธุรกิจ:** ต้นทุน**การเยียวยา**และ**ค่าสินไหมทดแทน**ให้แก่ผู้เสียหาย
    - **วิกฤตความศรัทธา:** สิ่งที่ประเมินค่าไม่ได้คือ **"ชื่อเสียงของแบรนด์"** หากลูกค้าเกิดความรู้สึกว่าบริษัทละเลยความปลอดภัยของข้อมูล **ความจงรักภักดี ที่สร้างมานานอาจพังทลายลงในทันที**

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูล (Lawful Basis) ที่เกี่ยวข้องกับงาน CRM

ในการบริหารจัดการข้อมูลลูกค้า **กฎหมายไม่ได้บังคับให้ต้องขอ "ความยินยอม"** ในทุกเรื่องเสมอไป **แต่กฎหมายกำหนด**ให้ต้องมี "**เหตุอันชอบด้วยกฎหมาย**" **ในการนำข้อมูลนั้นมาใช้** หากเลือกใช้ฐานทางกฎหมายที่ถูกต้อง จะช่วยให้การทำ CRM มีความคล่องตัวและสร้างความเชื่อมั่นให้กับลูกค้าไปพร้อมกัน โดย**ฐานหลักที่เกี่ยวข้องกับงาน CRM มี 3 ฐาน** ดังนี้:

1. **ฐานสัญญา:** ฐานการประมวลผลที่สำคัญที่สุดและถูกใช้บ่อยที่สุดในงาน CRM เพราะ**เมื่อลูกค้าตัดสินใจซื้อ**สินค้าหรือ**สมัครใช้**บริการ นั่น**หมายความว่าเกิด "สัญญา"** ขึ้นระหว่างแบรนด์กับลูกค้าแล้ว ซึ่งกิจกรรมที่ "จำเป็น" ต่อการทำตามสัญญาที่ให้ไว้กับลูกค้า เช่น:
    - การ**นำชื่อ**และ**ที่อยู่ไปใช้ในการจัดส่งสินค้าที่ลูกค้าสั่งซื้อ**
    - การ**ประมวลผลคะแนนสะสมในระบบบัตรสมาชิก**ตามเงื่อนไขที่ตกลงกันไว้
    - การ**ส่ง SMS** แจ้ง**เตือนยอดชำระ**เงิน หรือการ**ยืนยันรหัส OTP** เพื่อเข้าใช้งานระบบ

ข้อควรระวัง: ฐานนี้**ใช้ได้เฉพาะกับสิ่งที่ "จำเป็นจริงๆ"** เพื่อบรรลุ**เป้าหมายตามสัญญา**เท่านั้น

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ฐานการประมวลผลข้อมูล (Lawful Basis) ที่เกี่ยวข้องกับงาน CRM

2. **ฐานความยินยอม: ใช้ในกรณีที่กิจกรรมนั้น "เกินความคาดหมาย"** ของ**ลูกค้า** หรือ**ไม่มีกฎหมายอื่นรองรับ** (**เช่น** การส่งจดหมายข่าวประชาสัมพันธ์, การแชร์ข้อมูลลูกค้าให้พันธมิตรทางธุรกิจ หรือ การใช้ข้อมูลอ่อนไหว) ซึ่ง**การขอความยินยอม**ต้องทำโดยอิสระ **ลูกค้าต้องมีสิทธิ์เลือก**ว่าจะยินยอมหรือไม่ก็ได้โดยไม่กระทบต่อการใช้บริการหลัก **และต้องสามารถ "ถอนความยินยอม"** ได้ง่ายพอๆ กับตอนที่ให้
3. **ฐานผลประโยชน์อันชอบธรรม: ใช้กับกิจกรรมภายใน**เพื่อเพิ่มประสิทธิภาพธุรกิจ (**เช่น** การทำ Data Analytics เพื่อปรับปรุงระบบ CRM, การรักษาความปลอดภัยของฐานข้อมูล, หรือ การทำการตลาดแบบตรงกับ "ลูกค้าเก่า" ในขอบเขตที่ลูกค้าคาดเดาได้) ก่อนใช้ฐานนี้ ธุรกิจต้องทำแบบประเมิน **การใช้ฐานประโยชน์โดยชอบด้วยกฎหมาย (Legitimate Interest Assessment: LIA) เพื่อพิสูจน์ว่าประโยชน์**ที่บริษัทได้รับนั้น **"คุ้มค่า"** และ **"ไม่รุกราน" ความเป็นส่วนตัว**ของลูกค้าจนเกินไป

กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ฐานการประมวลผล อมล ที่เกี่ ว อ กบ าน CRM

ตารา เปรี บเที บ เลอก ฐาน หน ี น าน CRM

กิจกรรม CRM	ฐานการประมวลผลที่เหมาะสม	เหตุผลประกอบ
การจัดส่งสินค้าตามคำสั่งซื้อ	ฐานสัญญา	จำเป็นต้องใช้ชื่อ-ที่อยู่เพื่อทำตามสัญญาซื้อขาย
การทำประวัติลูกค้าเพื่อวิจัยตลาดภายใน	ฐานผลประโยชน์อันชอบธรรม	เพื่อพัฒนาบริการ โดยข้อมูลต้องถูกเก็บเป็นความลับ
การส่ง SMS โปรโมชั่นให้ลูกค้าใหม่	ฐานความยินยอม	เป็นการรบกวนความเป็นส่วนตัว ต้องขออนุญาตก่อน
การป้องกันการทุจริตในระบบสมาชิก	ฐานผลประโยชน์อันชอบธรรม	เพื่อปกป้องทรัพย์สินของบริษัทและสิทธิของลูกค้าคนอื่น

หมา เหตุ การเลือกใช้ฐานการประมวลผลผิดที่ผิดพลาด อาจนำ ปสู่การร้องเรียนจากลูกค้าและการลงโทษจาก สำนักงานค ะกรรมการคุ้มครองข้อมูลส่วนบุคคล ดังนั้น จงต้องพิจาร า ความคาดหมายของลูกค้า เป็นตัวตั้งเสมอ

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

- เมื่อทำความเข้าใจถึงหลักจริยธรรมและข้อบังคับทางกฎหมาย PDPA มาแล้ว คำถามสำคัญที่ตามมาคือ "เราจะนำกฎเกณฑ์เหล่านั้นมาเปลี่ยนให้เป็นระบบที่ใช้งานจริงได้อย่างไร?" จึงต้องนำเอาความใส่ใจในสิทธิส่วนบุคคล มาเป็นสาระสำคัญส่วนแรกของการออกแบบระบบ CRM
- โดย**การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย คือการทำให้ความเป็นส่วนตัวเป็น "ค่าเริ่มต้น" ของทุกกระบวนการทำงาน** ตั้งแต่การออกแบบหน้าเว็บสมัครสมาชิก การจัดเก็บฐานข้อมูล หรือการส่งต่อข้อมูลไปวิเคราะห์ทางการตลาด หากระบบ CRM ถูกออกแบบมาอย่างถูกต้องตั้งแต่วันแรก องค์กรจะไม่เพียงแค่**รอดพ้นจากการทำผิดกฎหมาย** แต่ยังช่วย**ลดต้นทุนในการแก้ไขระบบภายหลัง** และยังสามารถ**สร้างประสบการณ์ที่ราบรื่นให้กับลูกค้า** โดยที่**ลูกค้าไม่ต้องกังวลว่าข้อมูลของตนจะถูกนำไปใช้ในทางที่ผิด**อีกด้วย ซึ่งการออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย จะเจาะลึกผ่าน 3 หัวข้อสำคัญ ดังนี้:

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

การจัดการความยินยอม: การออกแบบแบบฟอร์มเก็บข้อมูลลูกค้าที่ถูกต้อง

ในกระบวนการ CRM ด่านแรกที่แบรนด์ได้ปฏิสัมพันธ์กับลูกค้า คือการเก็บข้อมูลผ่านแบบฟอร์ม ไม่ว่าจะเป็นการสมัครสมาชิก การลงทะเบียนรับสิทธิพิเศษ หรือการใช้คุกกี้บนเว็บไซต์ **การออกแบบ "ระบบจัดการความยินยอม"** ที่ดี จึง**ไม่ใช่แค่**การมี**ปุ่มให้กด "ตกลง" แต่ต้องเป็นการสื่อสารที่ชัดเจน**และ**ให้สิทธิแก่ลูกค้า**อย่างแท้จริง โดยมีประเด็นสำคัญที่ต้องทำความเข้าใจ ดังนี้:

- **องค์ประกอบของแบบฟอร์มเก็บข้อมูล:** แบบฟอร์มที่ดีในระบบ CRM ต้องประกอบด้วยส่วนสำคัญ 4 ส่วน ดังนี้:
  - **ความชัดเจน:** แยกจุดประสงค์การขอข้อมูลให้ชัดเจน ไม่มัดรวมกัน และลูกค้าต้องมีสิทธิ์เลือกยอมรับเพียงบางอย่างได้
  - **เป็นปัจจุบัน:** ห้ามใช้การ "ยอมรับไว้ล่วงหน้า" ลูกค้าต้องเป็นผู้ลงมือทำด้วยตนเองเท่านั้น
  - **ระบุตัวตนผู้ขอได้ชัดเจน:** ต้องระบุชื่อผู้ควบคุมข้อมูลให้ชัดเจน
  - **แจ้งสิทธิการถอนความยินยอม:** ต้องระบุไว้ว่า "ลูกค้าสามารถถอนความยินยอมได้ทุกเมื่อ" และกระบวนการถอนต้องไม่ยุ่งยาก

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

การจัดการความยินยอม: การออกแบบแบบฟอร์มเก็บข้อมูลลูกค้าที่ถูกต้อง

- **การใช้ภาษาในแบบฟอร์ม:** ควรหลีกเลี่ยงการใช้ภาษากฎหมายที่ซับซ้อนเกินไป แต่ควรใช้ภาษาที่เข้าใจง่าย เป็นมิตร และสื่อสารผลประโยชน์ที่ลูกค้าจะได้รับ
- **ระบบหลังบ้าน (การบันทึกหลักฐานความยินยอม):** ระบบ CRM ต้องสามารถบันทึก "หลักฐาน" ได้ว่า:
  - ใครเป็นคนให้ความยินยอม?
  - ให้ไว้เมื่อไหร่?
  - ให้ผ่านช่องทางไหน?
  - ยินยอมภายใต้ข้อกำหนดฉบับไหน?
- **แนวคิด "Less is More" ในการขอข้อมูล:** หลักการสำคัญคือการขอข้อมูลเท่าที่จำเป็น ควรขอข้อมูลทีละนิดตามความสัมพันธ์ที่เพิ่มขึ้น นอกจากจะสอดคล้องกับกฎหมายแล้ว ยังช่วยลดความรู้สึกถูกรุกรานและเพิ่มโอกาสที่ลูกค้าจะกรอกแบบฟอร์มจนจบ

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

กระบวนการจัดการเมื่อลูกค้าขอเข้าถึงหรือลบข้อมูลในฐานข้อมูล

ในระบบ CRM **ข้อมูลลูกค้าไม่ใช่ "ทรัพย์สินเบ็ดเสร็จ" ของบริษัท แต่เป็นสิ่งที่**ลูกค้าอนุญาตให้เรา **"ยืมมาใช้" เท่านั้น** ดังนั้น กฎหมาย PDPA จึง**กำหนดสิทธิพื้นฐานที่เจ้าของข้อมูล**สามารถ**เรียกใช้ได้ทุกเมื่อ** ภารกิจของ**นักบริหาร CRM** คือการ**ออกแบบกระบวนการ**ในระบบ**ให้สามารถตอบสนองต่อสิทธิเหล่านี้ได้อย่างรวดเร็ว**และ**ถูกต้อง** ตามรายละเอียดดังนี้:

- **สิทธิพื้นฐานที่พบบ่อยในงาน CRM:** เป็นสิทธิหลักที่ลูกค้ามักจะเลือกใช้ผ่านระบบบริการลูกค้าหรือหน้าเว็บไซต์ต่างๆ ดังนี้:
  - **สิทธิในการเข้าถึงข้อมูล:** ลูกค้ามีสิทธิขอดูข้อมูลของเขาและขอรับสำเนาข้อมูลนั้นๆ
  - **สิทธิในการแก้ไขข้อมูล:** เมื่อข้อมูลในระบบผิดพลาดหรือไม่อัปเดต ลูกค้าต้องสามารถสั่งแก้ไขได้เพื่อให้ข้อมูลถูกต้องตรงกับความเป็นจริง
  - **สิทธิในการลบข้อมูล:** เมื่อลูกค้ายกเลิกการเป็นสมาชิก หรือไม่ต้องการให้แบรนด์เก็บข้อมูลอีกต่อไป พวกเขามีสิทธิขอให้ลบข้อมูลออกจากฐานข้อมูล (เว้นแต่จะมีกฎหมายอื่นบังคับให้ต้องเก็บไว้ เช่น กฎหมายภาษี)
  - **สิทธิในการระงับการประมวลผล:** เช่น ลูกค้ายังอยากเป็นสมาชิกอยู่ แต่ขอไม่ให้นำข้อมูลไปวิเคราะห์เพื่อส่งโฆษณา

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

กระบวนการจัดการเมื่อลูกค้าขอเข้าถึงหรือลบข้อมูลในฐานข้อมูล

- **การวางขั้นตอนการจัดการ:** เมื่อลูกค้าแจ้งความประสงค์เรื่องต่างๆ เข้ามา องค์กรต้องมีขั้นตอนรองรับที่ชัดเจน ดังนี้:
  - **การยืนยันตัวตน:** ก่อนจะให้ข้อมูลหรือลบข้อมูล **ต้องตรวจสอบ**ให้แน่ใจว่าผู้ที่ขอคือ **"เจ้าของข้อมูลตัวจริง"** เพื่อป้องกันการสวมรอย
  - **การดำเนินการภายในกรอบเวลา: กฎหมายกำหนด**ให้ต้อง**ดำเนินการตามคำขอภายใน 30 วัน** นับแต่วันที่ได้รับคำขอ
  - **การบันทึกเหตุผล: หาก**บริษัท**ไม่สามารถทำตามคำขอได้** (เช่น จำเป็นต้องเก็บข้อมูลไว้ตามกฎหมายฟอกเงิน) **ต้องแจ้งเหตุผลเป็นลายลักษณ์อักษร**ให้ลูกค้าทราบ
- **การเตรียมความพร้อมทางเทคนิคในระบบ CRM:** ในการออกแบบระบบ CRM ควรผลักดันให้มีฟีเจอร์ "Self-Service Privacy Portal" ที่ช่วยให้ลูกค้าจัดการสิทธิได้ด้วยตนเอง เช่น:
  - ปุ่ม "Download My Data" สำหรับสิทธิการเข้าถึงข้อมูล
  - ปุ่ม "Delete Account" ที่เชื่อมโยงกับการลบข้อมูลในทุกฐานข้อมูลของบริษัท
  - เมนู "Preference Center" เพื่อให้ลูกค้าเลือกเปิด-ปิดเฉพาะบางกิจกรรมทางการตลาด

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

การจัดทำบันทึกรายการประมวลผล (RoPA) สำหรับกิจกรรมทางการตลาด

ในฐานะนักบริหาร CRM การเก็บข้อมูลลูกค้าให้เป็นระเบียบในระบบนั้น ยังไม่เพียงพอต่อการปฏิบัติตามกฎหมาย เพราะ **PDPA กำหนดให้องค์กร**ต้อง**จัดทำ "บันทึกรายการประมวลผลข้อมูลส่วนบุคคล"** หรือที่เรียกสั้นๆ ว่า RoPA (Record of Processing Activities) **ซึ่งเปรียบเสมือน "แผนที่และสมุดบัญชี" ที่แสดงเส้นทางการไหลของข้อมูลลูกค้าตั้งแต่ต้นจนจบ** กิจกรรมทางการตลาด โดยประกอบด้วยประเด็นสำคัญ ดังนี้:

- **RoPA คืออะไร และทำไมคนทำ CRM ต้องใส่ใจ: RoPA คือเอกสารที่บันทึกว่า "ใคร ทำอะไร ที่ไหน เมื่อไหร่ และอย่างไร" กับข้อมูลลูกค้า** หากมีการร้องเรียนหรือข้อมูลรั่วไหล **เอกสารฉบับนี้จะเป็นหลักฐานสำคัญที่ใช้ยืนยัน**กับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ว่าองค์กรได้วางแผนและจัดการข้อมูลอย่างมีระบบ มิใช่การเก็บข้อมูลตามอำเภอใจ

หมายเหตุ: สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) หมายถึง หน่วยงานของรัฐตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีวัตถุประสงค์เพื่อกำกับดูแลเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล และส่งเสริมให้เกิดการพัฒนาด้านการคุ้มครองข้อมูลส่วนบุคคลของประเทศ

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

การจัดทำบันทึกรายการประมวลผล (RoPA) สำหรับกิจกรรมทางการตลาด

- **องค์ประกอบสำคัญของ RoPA ในงานการตลาด:** ในการจัดทำบันทึกสำหรับกิจกรรม CRM (เช่น การทำ Loyalty Program หรือการส่งอีเมลส่งเสริมการขาย) บันทึกนั้นต้องมีข้อมูลอย่างน้อยดังนี้:
  - **วัตถุประสงค์:** เช่น เพื่อการสะสมคะแนนแลกส่วนลด หรือเพื่อวิเคราะห์พฤติกรรมลูกค้า
  - **ประเภทข้อมูล:** ระบุให้ชัดว่าเก็บอะไรบ้าง เช่น ชื่อ-นามสกุล, ประวัติการซื้อ
  - **ระยะเวลาการจัดเก็บ:** ต้องระบุว่าจะเก็บข้อมูลไว้นานเท่าใด (เช่น 2 ปีหลังจากลูกค้าเลิกเป็นสมาชิก) และจะทำลายอย่างไรเมื่อครบกำหนด
  - **การส่งต่อข้อมูล:** มีการส่งข้อมูลให้บริษัทอื่นหรือไม่ เช่น ส่งให้บริษัทขนส่ง หรือส่งให้แพลตฟอร์มโฆษณาอย่าง Facebook หรือ Google
  - **มาตรการรักษาความปลอดภัย:** ระบุว่าข้อมูลนี้ถูกปกป้องอย่างไร เช่น การใช้รหัสผ่านหรือการจำกัดสิทธิ์พนักงานที่เข้าถึงระบบ CRM

การออกแบบระบบ CRM ที่สอดคล้องกับกฎหมาย

การจัดทำบันทึกรายการประมวลผล (RoPA) สำหรับกิจกรรมทางการตลาด

- **ขั้นตอนการทำ Data Mapping สำหรับกิจกรรม CRM:** ก่อนจะเขียน RoPA ได้ จะต้องทำสิ่งที่เรียกว่า **"Data Mapping"** คือ**การลากเส้นทางของข้อมูล** โดยมีรายละเอียดว่า:
  - **ข้อมูลเข้า:** มาจากช่องทางไหน? (หน้าเว็บ, บูธกิจกรรม, หรือแอปพลิเคชัน)
  - **ข้อมูลอยู่:** จัดเก็บไว้ที่ใด? (Excel ในคอมพิวเตอร์, ระบบ CRM ของบริษัท, หรือ Cloud ของต่างประเทศ)
  - **ข้อมูลออก:** ใครเอาไปใช้บ้าง? (ฝ่ายขาย, ฝ่ายวิเคราะห์, หรือเอเจนซี่ภายนอก)
- **การปรับปรุง RoPA ให้เป็นปัจจุบัน: RoPA ไม่ใช่เอกสาร**ที่ทำ**ครั้งเดียวแล้วจบ** แต่**ต้องปรับปรุงทุกครั้งที่มีกิจกรรมทางการตลาดใหม่ๆ** (เช่น การเปลี่ยนจากการส่ง SMS มาเป็นการทำ Chatbot ใน LINE OA) ซึ่งการบันทึก RoPA ก็ต้องถูกแก้ไข เพื่อสะท้อนความจริงของการประมวลผลข้อมูลที่เปลี่ยนไป

การจัดการวิกฤตและความปลอดภัยข้อมูล

- ในการบริหารจัดการลูกค้าสัมพันธ์ สิ่งที่น่ากลัวที่สุดไม่ใช่การที่ยอดขายลดลง แต่คือการที่ **"ความไว้วางใจ"** ของลูกค้าที่มอบให้แบรนด์ถูกทำลายลงในชั่วข้ามคืน แม้ว่าจะออกแบบระบบ CRM มาอย่างดีเยี่ยมเพียงใดก็ตาม แต่ในยุคที่ภัยคุกคามทางไซเบอร์ทวีความซับซ้อนและการทำงานของมนุษย์อาจเกิดข้อผิดพลาดได้เสมอ จึงต้องยอมรับความจริงว่า **"ไม่มีระบบใดในโลกที่ปลอดภัยแบบร้อยเปอร์เซ็นต์"**
- **การจัดการความปลอดภัยข้อมูล**ในงาน CRM **จึงไม่ได้หยุดอยู่แค่การติดตั้ง**ซอฟต์แวร์**ป้องกัน แต่คือการวางรากฐาน "ระบบป้องกัน"** ที่แข็งแกร่ง**ควบคู่ไปกับ "แผนเผชิญเหตุ"** ที่รวดเร็ว (ตัวอย่างเช่น หากเกิดเหตุการณ์ "ข้อมูลรั่วไหล") **สิ่งที่จะตัดสินว่าแบรนด์**จะ**รอดพ้นจากวิกฤต**หรือ**สูญสิ้นความน่าเชื่อถือ ไม่ใช่**เพียง**แค่ความเก่งกาจทางเทคนิค**ของฝ่าย IT **แต่คือสปิริต**และ**ความเป็นมืออาชีพ**ของแบรนด์ **ในการสื่อสาร**และ**แสดงความรับผิดชอบ**ต่อลูกค้าอย่างโปร่งใสและเป็นมืออาชีพ โดยหัวใจสำคัญในการคุ้มครองข้อมูลลูกค้าประกอบด้วย 3 หัวข้อสำคัญ ดังนี้:

การจัดการวิกฤตและความปลอดภัยข้อมูล

มาตรการรักษาความปลอดภัยของฐานข้อมูลลูกค้า

ในฐานะนักบริหาร CRM การเข้าใจมาตรการรักษาความปลอดภัยขั้นพื้นฐานถือเป็นหน้าที่สำคัญ เพื่อให้มั่นใจว่าข้อมูลมหาศาลที่เราจัดเก็บนั้นจะไม่กลายเป็น "ระเบิดเวลา" ที่ย้อนกลับมาทำลายองค์กร โดยมาตรการรักษาความปลอดภัย ที่เป็นมาตรฐานสากลตามแนวทาง ISO/IEC 27001 และข้อกำหนดของ PDPA มีดังนี้:

- **การจำกัดสิทธิ์การเข้าถึงข้อมูล:** คือปราการด่านแรกที่สำคัญที่สุด โดยยึดหลักการ "Least Privilege" หรือการให้สิทธิ์พนักงานเข้าถึงข้อมูลเท่าที่ "จำเป็นต่อการปฏิบัติงาน" เท่านั้น ประกอบด้วย 2 ลักษณะ:
    - **การควบคุมการเข้าถึงตามบทบาท:** พนักงานหน้าร้านอาจเห็นเพียงชื่อและระดับสมาชิกของลูกค้า แต่พนักงานฝ่ายบัญชีเท่านั้นที่เห็นข้อมูลเลขบัตรเครดิต หรือผู้บริหารระดับสูงเท่านั้นที่เห็นรายงานการวิเคราะห์ภาพรวม
    - **การยืนยันตัวตนโดยใช้หลายปัจจัย:** การบังคับใช้ระบบการยืนยันตัวตน 2 ชั้น (เช่น รหัสผ่านควบคู่กับรหัส OTP ในมือถือ) สำหรับการล็อกอินเข้าสู่ระบบ CRM เพื่อป้องกันการถูกขโมยรหัสผ่าน

การจัดการวิกฤตและความปลอดภัยข้อมูล

มาตรการรักษาความปลอดภัยของฐานข้อมูลลูกค้า

- **การทำให้อ่านไม่ออกเมื่อข้อมูลหลุดลอย:** เมื่อข้อมูลต้องถูกส่งผ่านอินเทอร์เน็ตหรือจัดเก็บใน Server เราต้องมีเทคโนโลยีปกป้องตัวข้อมูลเอง ประกอบด้วย 2 ส่วน ได้แก่:
  - **ข้อมูลที่จัดเก็บอยู่:** การ**เข้ารหัสข้อมูลที่เก็บ**อยู่ในฐานข้อมูล เพื่อที่ว่าหาก Hard Drive ถูกขโมยไป ผู้ที่ไม่มี **"กุญแจถอดรหัส"** ก็จะไม่สามารถเปิดดูข้อมูลได้
  - **ข้อมูลระหว่างการส่งผ่าน:** การ**เข้ารหัสขณะส่งข้อมูล** (เช่น โปรโตคอล HTTPS) เพื่อ**ป้องกันการถูก "ดักฟัง"** ข้อมูลระหว่างที่พนักงานกำลังคีย์ข้อมูลลูกค้าส่งไปยัง Cloud Server
- **การลดระดับการระบุตัวตน:** ในขั้นตอน "การวิเคราะห์ข้อมูล" หากเราต้องการเพียงแค่ทราบพฤติกรรมภาพรวม ไม่จำเป็นต้องรู้ว่าลูกค้ารายนั้นคือใคร มีกระบวนการดังนี้:
  - **การทำข้อมูลให้เป็นนิรนาม:** ทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนของบุคคลได้ เพื่อวัตถุประสงค์ด้านการคุ้มครองข้อมูลส่วนบุคคล
  - **การแฝงข้อมูล:** การแทนที่ข้อมูลระบุตัวตนด้วย "นามแฝง" หรือรหัส เพื่อลดความเสี่ยงในการระบุตัวบุคคลโดยตรงหากข้อมูลส่วนนี้หลุดออกไป

การจัดการวิกฤตและความปลอดภัยข้อมูล

มาตรการรักษาความปลอดภัยของฐานข้อมูลลูกค้า

- **การตรวจสอบร่องรอยการใช้งาน:** ระบบ CRM ที่ดีต้องมีการ **"บันทึกเหตุการณ์"** เสมอว่า "ใคร" เข้ามาดูข้อมูลของใคร "เมื่อไหร่" และ "มีการแก้ไขอะไรหรือไม่" การมีทะเบียนบันทึกเหตุการณ์ที่ดี จะช่วยให้**องค์กรสามารถตรวจสอบย้อนกลับได้** เมื่อพบสิ่งผิดปกติ และเป็นเครื่องมือชิ้นสำคัญในการ**ยืนยันความโปร่งใส**ต่อหน่วยงานกำกับดูแล
- **การสำรองข้อมูลและการกู้คืน:** **ความมั่น**คงปลอดภัยไม่ได้หมายถึง**การป้องกัน**การเจาะระบบเท่านั้น แต่รวมถึง**ความพร้อม**ใช้งาน องค์กรต้องมี**แผนสำรอง**ข้อมูลสม่ำเสมอ เพื่อให้แน่ใจว่าหากระบบล่มหรือถูกโจมตีด้วยเรียกค่าไถ่ ข้อมูลลูกค้าที่สะสมมาหลายปีจะไม่สูญหายไปถาวร

การจัดการวิกฤตและความปลอดภัยข้อมูล

ขั้นตอนการรับมือและแจ้งเหตุเมื่อข้อมูลลูกค้าถูกละเมิด

ในการบริหารความสัมพันธ์ลูกค้า สิ่งที่น่ากลัวกว่าความผิดพลาดทางเทคนิค คือการที่องค์กร "ปกปิด" หรือ "เพิกเฉย" เมื่อข้อมูลรั่วไหล **พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)** จึง**กำหนดให้ผู้ควบคุมข้อมูล** มีหน้าที่ต้อง**ดำเนินการตามขั้นตอนที่ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) กำหนดไว้**ดังนี้:

- **การแจ้งเหตุต่อสำนักงาน: เมื่อองค์กร "ทราบเหตุ"** การละเมิดข้อมูลส่วนบุคคล (ไม่ว่าจะเกิดจากการถูกแฮก, พนักงานทำข้อมูลหลุด, หรือความผิดพลาดของระบบ) องค์กรมีหน้าที่**ต้องแจ้งเหตุให้ สคส. (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล)** ทราบโดยเร็วที่สุด **ภายใน 72 ชั่วโมง**
- **การแจ้งเหตุต่อเจ้าของข้อมูล (ลูกค้า): หากเหตุการณ์**ที่เกิดขึ้นมีความ **"เสี่ยงสูง"** ที่จะกระทบต่อสิทธิและเสรีภาพของลูกค้า (เช่น ข้อมูลการเงินหรือรหัสผ่านรั่วไหล) แบรนด์**ต้องแจ้งให้ลูกค้าทราบโดยไม่ชักช้า พร้อม**กับ**แจ้ง "แนวทางการเยียวยา"** และ**ช่องทางการติดต่อขอรับข้อมูลเพิ่มเติม**

การจัดการวิกฤตและความปลอดภัยข้อมูล

ขั้นตอนการรับมือและแจ้งเหตุเมื่อข้อมูลลูกค้าถูกละเมิด

- **ขั้นตอนปฏิบัติ 5 ประการ ในการรับมือ:** เมื่อเกิดปัญหาทางด้านข้อมูล ซึ่งอาจส่งผลกระทบอย่างร้ายแรงต่อความเชื่อมั่นของลูกค้า ในการบริหาร CRM ที่ดี องค์กรควรมีมาตรการการรับมือที่เหมาะสม โดยมีขั้นตอนการรับมือที่แนะนำ ดังนี้:
  - **หยุดยั้งและควบคุม:** ตัดการเชื่อมต่อระบบที่ถูกโจมตีทันทีเพื่อหยุดการรั่วไหล
  - **ประเมินความเสี่ยง:** วิเคราะห์ประเภทและปริมาณข้อมูลที่รั่วไหล
  - **แจ้งเหตุตามกฎหมาย:** ดำเนินการแจ้งสำนักงาน และ/หรือ ลูกค้า
  - **เยียวยาและแก้ไข:** ให้ความช่วยเหลือลูกค้าที่ได้รับผลกระทบ เช่น การแนะนำให้เปลี่ยนรหัสผ่าน หรือการชดเชยความเสียหาย
  - **ทบทวนและป้องกันซ้ำ:** บันทึกรายละเอียดเหตุการณ์ สาเหตุ และมาตรการแก้ไข เพื่อปรับปรุงความมั่นคงปลอดภัยในอนาคต
- **บทลงโทษหากเพิกเฉย:** **การไม่แจ้งเหตุ**ละเมิดข้อมูล**ตามระยะเวลาที่กฎหมายกำหนด** มีโทษ**ปรับทางปกครองสูงสุดถึง 3 ล้านบาท** และ**หากจงใจปกปิด**จนก่อให้เกิดความเสียหายร้ายแรง **อาจมีโทษทางอาญาร่วมด้วย**

Q & A

Thank you