SUAN SUNANDHA RAJABHAT UNIVERSITY

ETHICS, LAW, AND DATA PROTECTION IN CRM

KARDPAKORN NINAROON

INTRO

- Customer Relationship Management (CRM) in the present era covers the tracking of digital behavior and personal preferences through Artificial Intelligence, which enables businesses to deliver experiences that "understand" customers accurately and can predict future behaviors. At the same time, however, this brings about important questions regarding the appropriateness and security of customers' personal data.
- When data is likened to the most valuable asset, the responsibility toward that asset becomes a matter of "Trust," which is the foundation of the CRM system. Without trust, customers will not provide truthful data to the brand, consequently causing the CRM system to lose its efficiency. Understanding ethics and laws is therefore not just to avoid penalties, but to create a sustainable business operation standard.

CUSTOMER DATA GOVERNANCE

- To enter professional customer management, the first thing to recognize is "Data Governance," which means structuring the authority and regulations for data management within the organization to ensure that the data is accurate, secure, and utilized with maximum efficiency according to international standards.
- However, data governance in CRM does not stop at the accuracy of numbers in the system but must go hand-in-hand with "Ethics," which serves as a guiding compass where the law may not yet reach. Ethics here involves asking the question: "Even if we have the technical right to access this data, should we use it in a way that might disturb the customer's privacy?" Having good data governance will help the organization answer these questions in a principled manner, focusing on transparency and prioritizing the customer's benefit over just the organization's short-term profits. This consists of 3 important topics as follows:

CUSTOMER DATA GOVERNANCE

Brand Trust

In Customer Relationship Management, Trust is like the most important "currency" of the relationship. A customer's decision to provide personal data is based on the assumption that the organization will manage that data ethically and use it to enhance their experience. Without this, a relationship cannot occur.

Loyalty

Adhering to ethics as a practical principle directly impacts the building of Brand Trust, which is as important as product quality. Refraining from secretly reselling data or providing notifications when errors occur helps transform "one-time customers" into "regular customers." Ethics is, therefore, a vital foundation that makes customers ready to protect and grow alongside the organization in the long term.

CUSTOMER DATA GOVERNANCE

Impacts of Unethical Conduct on Brand Value

A lack of ethics in data management brings about immeasurable damage and causes customers to feel "betrayed," leading to a surge in service cancellations and destroying a reputation that could take years to recover. Especially in the world of social media, a single instance of negative criticism can collapse trust built over decades.

Therefore, integrating ethics as part of the organizational culture in CRM creates a sustainable competitive advantage. On the day when competitors can replicate technology or match price cuts, the only thing that will retain customers is the "Trust" the brand has provided regarding the customer's privacy and rights.

CUSTOMER DATA GOVERNANCE

Personalization vs. Privacy Invasion

Personalized marketing to deliver experiences that resonate with customers faces the challenge of distinguishing between "attentiveness" and "creepiness." If this line is crossed, marketing intended to create an impression can immediately become a privacy violation in the eyes of the customer. Marketers must therefore be cautious of the thin line between personalized offerings and rights infringement. Key points to consider include:

- The Power of Anticipation vs. The Feeling of Being Spied On: Having a CRM system analyze interests and send coupons is considered skillful. However, using deep insights that the customer did not directly consent to disclose creates a feeling of being spied on and raises the question: "How does the brand know this?" This is a sign of invading personal space. This sense of being threatened does more harm than good to the relationship and destroys the power of anticipation the brand intended to build.

CUSTOMER DATA GOVERNANCE

Personalization vs. Privacy Invasion

- Transparency Theory (The Key to Drawing the Line): What separates personalized marketing from the feeling of being threatened is "transparency" and "giving control." Customers will accept the use of personal data only when:
    - Receiving Clear Value: Customers are willing to provide data if exchanged for worthwhile benefits.
    - Transparency: The brand is straightforward about the sources of data collection.
    - Having Options: Customers can adjust the level of "personalization" or disable certain functions as desired.
- The "Creepy Factor" Phenomenon in CRM: Each individual has a different privacy boundary based on age and attitude. Forcing the use of data to invade personal space just because the system can, without considering the customer's readiness, is a long-term failure. A good CRM system must therefore have various settings management so that each customer can define their own "line."

CUSTOMER DATA GOVERNANCE

Ethics of Using AI and Algorithms in Customer Behavior Analysis

The use of AI and Algorithms in CRM systems has transformed databases into "artificial brains" that function to predict customer needs in advance. However, empowering technology to make decisions on behalf of humans in customer relationship management brings about new forms of ethical responsibility that must be recognized for accuracy and fairness, including:

1. Algorithm Bias Issues: AI may lead to discrimination if the data used to train the system contains underlying biases (such as rejecting offers based on gender or domicile). Regular audits are therefore necessary to ensure that algorithms do not evaluate based on inappropriate factors, which could reinforce inequality. Ensuring the system does not become a tool for creating social disparity is a vital duty when using behavioral analysis technology.

CUSTOMER DATA GOVERNANCE

Ethics of Using AI and Algorithms in Customer Behavior Analysis

2. Transparency and Explainability: A challenge for AI in CRM is the "black box" problem, where the system provides results but cannot explain the reasoning behind them. Ethics dictate that brands must be able to explain to customers the origin of offers or customer segmentation based on transparency principles.
3. Preserving Customer Autonomy: Using algorithms to "guide" customers must be done carefully to avoid becoming behavioral control or manipulating data by exploiting psychological weaknesses. AI should be used to support decision-making and provide greater convenience. Preserving the customer's freedom of choice is what makes the relationship between the brand and the customer sustainable.
4. Responsibility for Outcomes: When AI makes a mistake (such as sending messages that cause embarrassment or misunderstanding to customers), the brand cannot deflect responsibility by claiming it was a system error. Organizations must have "humans" in control, ready to intervene and rectify the situation when automated systems operate outside the established ethical boundaries

PERSONAL DATA PROTECTION LAW

- Governance and ethics are responsibilities that organizations "voluntarily" undertake to build trust and maintain good relationships with customers. However, when personal data breaches have a broad impact beyond what any single organization's ethics can control alone, the government steps in to set minimum standards through legal regulations that every business must comply with equally.

- In Thailand, customer relationship data management has entered a new era since the enactment of the Personal Data Protection Act B.E. 2562 (2019) (PDPA), which has become the primary framework that completely changes the mindset of CRM practitioners. It shifts from previously viewing customer data as "company property" to recognizing that such data is the "right of the data subject," which the company merely requests permission to use temporarily. This consists of 3 important topics as follows:

PERSONAL DATA PROTECTION LAW

Summary of the Personal Data Protection Act (PDPA) Key Essentials for Business

The enactment of the Personal Data Protection Act B.E. 2562 (2019), or commonly known as PDPA, is not merely an addition of paperwork steps, but the establishment of a new standard in customer data management for Thai businesses. The essential aspects that customer relationship managers must understand for correct application are as follows:

1. Definition of Personal Data: In CRM work, we must legally categorize data into two main types:
    - General Personal Data: Information that enables the identification of a customer, whether directly or indirectly (such as first-last name, phone number, email, address, including IP Address), or Cookie data that brands use to track behavior on websites.
    - Sensitive Personal Data: Information that is delicate and carries a risk of discrimination (such as religion, health data, genetic data, or political opinions). Collecting this type of data always requires explicit consent.

PERSONAL DATA PROTECTION LAW

Summary of the Personal Data Protection Act (PDPA) Key Essentials for Business

2. Legal Roles and Responsibilities: In working with CRM systems, customer data is constantly moved between departments and partners. The law, therefore, defines clear roles to identify responsibilities as follows:
   - Data Controller: This refers to the organization or business that decides what data to collect and for what purpose it will be used. They are considered the primary party responsible to the customer.
   - Data Processor: This refers to external entities hired by the brand to manage data, such as Cloud CRM service providers or marketing agencies. They must act according to the instructions of the Data Controller.

PERSONAL DATA PROTECTION LAW

Summary of the Personal Data Protection Act (PDPA) Key Essentials for Business

3. Three Principles of Data Management: To create a CRM system that is "elegant" and "secure," customer relationship managers must adhere to three principles:
    - Principle of Transparency: The purpose of data collection must be informed through a "Privacy Policy" in a straightforward and easy-to-understand manner.
    - Principle of Purpose Limitation: Data collected for providing discounts must be used only for that purpose. It is prohibited to share or use it for other activities to which the customer has not previously consented.
    - Principle of Data Minimization: Adhere to the concept of collecting only the data necessary to achieve business goals. If marketers can analyze behavior without using a national ID number, they should not compel customers to provide that information.

PERSONAL DATA PROTECTION LAW

Summary of the Personal Data Protection Act (PDPA) Key Essentials for Business

4. Impacts and Credibility: Damages from PDPA violations are not limited to monetary terms but often come with severe impacts in 3 dimensions:
    - Legal Penalties: Administrative fines up to 5 million THB and criminal penalties that may include imprisonment.
    - Business Damages: Costs of remediation and compensation to the affected parties.
    - Crisis of faith: What is immeasurable is the "Brand Reputation." If customers feel the company neglects data security, the loyalty built over a long time may collapse instantly.

PERSONAL DATA PROTECTION LAW

Lawful Basis for Data Processing Related to CRM

In customer data management, the law does not always mandate obtaining "consent" for every matter. Instead, it requires a "Lawful Basis" for using that data. Choosing the correct legal basis helps CRM operations remain agile while simultaneously building customer trust. The three primary bases related to CRM work are as follows:

1. **Contractual Basis: This is the most important and frequently used processing basis in CRM. When a customer decides to purchase a product or sign up for a service, it means a "contract" has been formed between the brand and the customer. This includes activities "necessary" to fulfill the agreement made with the customer, such as:**
   - Using names and addresses to deliver products ordered by customers.
   - Processing accumulated points in a membership card system according to agreed conditions.
   - Sending SMS payment reminders or OTP (One-Time Password) confirmations for system access.

Caution: This basis applies only to what is "strictly necessary" to achieve the goals of the contract.

PERSONAL DATA PROTECTION LAW

Lawful Basis for Data Processing Related to CRM

2. Consent Basis: Used in cases where activities are "beyond the customer's expectations" or not supported by other laws (such as sending promotional newsletters, sharing customer data with business partners, or using sensitive data). Obtaining consent must be done freely; customers must have the right to choose whether to consent without affecting their primary service usage, and they must be able to "withdraw consent" as easily as it was given.
3. Legitimate Interest Basis: Used for internal activities to increase business efficiency (such as conducting data analytics to improve CRM systems, database security, or direct marketing to "existing customers" within a scope the customer can reasonably expect). Before using this basis, a business must conduct a Legitimate Interest Assessment (LIA) to prove that the benefits received by the company are "worthwhile" and "do not intrude" upon the customer's privacy excessively.

PERSONAL DATA PROTECTION LAW

Lawful Basis for ata rocessing Relate to CRM

Co parison a le ic Basis S oul Be Selecte for CRM or

CRM Activity	Appropriate Lawful Basis	Supporting Reason
Product delivery according to orders	Contractual Basis	Necessary to use name and address to fulfill the sales contract.
Creating customer profiles for internal market research	Legitimate Interest Basis	To develop services, provided that data is kept confidential.
Sending promotional SMS to new customers	Consent Basis	This constitutes a privacy intrusion; prior permission must be obtained.
Fraud prevention in the membership system	ฐานผลประโยชน์อันชอบธรรม	To protect company assets and the rights of other customers.

ote C oosing t e wrong processing asis ay lea to custo er co plaints an penalties fro t e ffice of t e ersonal ata rotection Co ittee C erefore t e custo er s e pectations ust always e use as a pri ary consi eration

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

- Once the ethical principles and PDPA legal regulations are understood, the important following question is: "How do we transform those rules into a functional system?" It is therefore necessary to make attentiveness to personal rights the primary essence of CRM system design.
- Designing a legally compliant CRM system means making privacy the "default setting" for every workflow—from designing membership registration pages and database storage to transferring data for marketing analysis. If a CRM system is designed correctly from day one, the organization will not only avoid legal violations but also reduce the costs of subsequent system modifications. Furthermore, it can create a smooth experience for customers, ensuring they do not have to worry about their data being misused. Designing a legally compliant CRM system will delve into 3 important topics as follows:

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Consent Management: Designing Accurate Data Collection Forms

In the CRM process, the first touchpoint where a brand interacts with customers is data collection through forms, whether for membership applications, special privilege registrations, or using website cookies. Designing a good "Consent Management System" is not just about having an "Agree" button; it must be clear communication that grants true rights to the customer. Key issues to understand are as follows:

- **Elements of a Data Collection Form: A good form in a CRM system must consist of 4 essential parts:**
  - Clarity: Clearly separate the purposes for requesting data without bundling them together; customers must have the right to opt-in to only certain items.
  - Active Opt-in: "Pre-ticked boxes" are prohibited; the customer must perform the action themselves only.
  - Clear Identification of the Requester: The name of the Data Controller must be clearly specified.
  - Notification of Withdrawal Rights: It must state that "customers can withdraw consent at any time," and the withdrawal process must not be complicated.

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Consent Management: Designing Accurate Data Collection Forms

- Language Used in Forms: Avoid using overly complex legal jargon; instead, use language that is easy to understand, friendly, and communicates the benefits the customer will receive.
- Backend System (Recording Evidence of Consent): The CRM system must be able to record "evidence" of:
  - Who provided the consent?
  - When was it provided?
  - Through which channel was it provided?
  - Under which version of the terms was it consented to?
- The "Less is More" Concept in Data Requests: The key principle is to request only necessary data. Information should be requested gradually as the relationship grows. In addition to legal compliance, this helps reduce the feeling of intrusion and increases the likelihood that customers will complete the form.

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Management Processes for Customer Access or Data Deletion Requests

In a CRM system, customer data is not the company’s "absolute asset" but something the customer has merely allowed us to "borrow." Therefore, the PDPA law defines fundamental rights that data subjects can exercise at any time. The mission of CRM managers is to design system processes capable of responding to these rights quickly and accurately, with details as follows:

- Common Fundamental Rights in CRM: These are the primary rights that customers often choose to exercise through customer service systems or various website interfaces:
  - Right of Access: Customers have the right to view their data and request a copy of that information.
  - Right to Rectification: When data in the system is incorrect or outdated, customers must be able to request corrections to ensure the data is accurate and reflects reality.
  - Right to Erasure (Right to be Forgotten): When customers cancel their membership or no longer want the brand to store their data, they have the right to request its deletion from the database (unless other laws require its retention, such as tax laws).
  - Right to Restriction of Processing: For example, a customer may still want to remain a member but requests that their data not be used for analysis to send advertisements.

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Management Processes for Customer Access or Data Deletion Requests

- Setting up Management Procedures: When customers submit various requests, the organization must have clear supporting procedures as follows:
    - Identity Verification: Before providing or deleting data, it must be verified that the requester is the "actual data subject" to prevent impersonation.
    - Action within the Timeframe: The law requires that requests must be acted upon within 30 days from the date the request is received.
    - Recording Reasons: If the company cannot fulfill a request (e.g., being legally required to retain data under Anti-Money Laundering laws), it must inform the customer of the reasons in writing.
- Technical Preparedness in the CRM System: In designing a CRM system, a "Self-Service Privacy Portal" feature should be promoted to allow customers to manage their rights independently, such as:
    - A "Download My Data" button for the right of access.
    - A "Delete Account" button that links to data deletion across all company databases.
    - A "Preference Center" menu to allow customers to opt-in or opt-out of specific marketing activities.

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Preparing a Record of Processing Activities (RoPA) for Marketing Activities

As a CRM manager, keeping customer data organized in the system is not enough for legal compliance. The PDPA requires organizations to prepare a "Record of Processing Activities," or RoPA, which acts like a "map and ledger" showing the flow of customer data from the beginning to the end of marketing activities. It consists of the following key points:

- What is RoPA and why should CRM practitioners care? RoPA is a document that records "who, what, where, when, and how" regarding customer data. If there is a complaint or a data breach, this document serves as essential evidence to prove to the Office of the Personal Data Protection Committee (PDPC) that the organization has planned and managed data systematically, rather than collecting data arbitrarily.

Note: The Office of the Personal Data Protection Committee (PDPC) refers to the government agency under the Personal Data Protection Act B.E. 2562 (2019). Its objective is to regulate personal data protection and promote the development of personal data protection in the country.

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Preparing a Record of Processing Activities (RoPA) for Marketing Activities

- Key Elements of RoPA in Marketing: In preparing records for CRM activities (such as loyalty programs or sending promotional emails), the record must contain at least the following information:
    - Purpose: For example, for point accumulation to redeem discounts or for analyzing customer behavior.
    - Data Types: Clearly specify what is collected, such as first-last names and purchase history.
    - Retention Period: Must specify how long the data will be stored (e.g., 2 years after the customer terminates membership) and how it will be destroyed upon expiration.
    - Data Transfer: Whether data is transferred to other companies, such as delivery companies or advertising platforms like Facebook or Google.
    - Security Measures: Specify how this data is protected, such as using passwords or restricting access rights for employees who can access the system.

DESIGNING A LEGALLY COMPLIANT CRM SYSTEM

Preparing a Record of Processing Activities (RoPA) for Marketing Activities

- Data Mapping Process for CRM Activities: Before a RoPA can be written, a "Data Mapping" must be performed to trace the data journey, with the following details:
  - Data Inflow: From which channel? (Website, event booth, or application)
  - Data Storage: Where is it stored? (Excel on a computer, company CRM system, or international Cloud)
  - Data Outflow: Who uses it? (Sales department, analytics department, or external agencies)
- Keeping RoPA Up-to-Date: RoPA is not a "one-time" document; it must be updated every time there are new marketing activities (such as switching from sending SMS to using a Chatbot on LINE OA). The RoPA records must be revised to reflect the current reality of data processing.

CRISIS MANAGEMENT AND DATA SECURITY

- In Customer Relationship Management, the most fearsome thing is not a decline in sales, but the "trust" that customers have given to the brand being destroyed overnight. No matter how excellently a CRM system is designed, in an era where cyber threats are becoming increasingly complex and human error can always occur, we must accept the reality that "no system in the world is one hundred percent secure."
- Data security management in CRM, therefore, does not stop at just installing protective software; it is about establishing a robust "defense foundation" alongside a swift "incident response plan" (for example, in the event of a "data breach"). What will decide whether a brand survives a crisis or loses all credibility is not just the technical prowess of the IT department, but the spirit and professionalism of the brand in communicating and demonstrating responsibility toward customers transparently and professionally. The core essentials of customer data protection consist of 3 important topics as follows:

CRISIS MANAGEMENT AND DATA SECURITY

Database Security Measures

As a CRM manager, understanding basic security measures is a vital duty to ensure that the vast amount of data we collect does not become a "time bomb" that returns to destroy the organization. The international standard security measures in line with ISO/IEC 27001 and PDPA requirements are as follows:

- Restricting Data Access Rights: This is the most important first line of defense, adhering to the principle of "Least Privilege"—granting employees access to data only as "necessary for their operations." This consists of two characteristics:
  - Role-Based Access Control (RBAC): Frontline staff may see only the name and membership level of a customer, while only accounting staff can see credit card information, or only senior executives can see overall analytical reports.
  - Multi-Factor Authentication (MFA): Enforcing a two-layer authentication system (such as a password coupled with an OTP code on a mobile phone) for logging into the CRM system to prevent password theft.

CRISIS MANAGEMENT AND DATA SECURITY

Database Security Measures

- Making Data Unreadable in Case of a Breach: When data must be transmitted over the internet or stored on a server, we must have technology to protect the data itself, consisting of two parts:
    - Data at Rest: Encrypting data stored in the database so that if a hard drive is stolen, someone without the "decryption key" will be unable to view the information.
    - Data in Transit: Encrypting data during transmission (such as using HTTPS protocols) to prevent data "eavesdropping" while employees are entering customer data into the Cloud Server.
- De-identification: In the "Data Analysis" stage, if we only need to know overall behavioral patterns without needing to know who that specific customer is, the processes are as follows:
    - Anonymization: Making personal data incapable of identifying an individual for personal data protection purposes.
    - Pseudonymization: Replacing identifying information with "aliases" or codes to reduce the risk of direct individual identification if this part of the data is leaked.

CRISIS MANAGEMENT AND DATA SECURITY

Database Security Measures

- Audit Trails and Usage Monitoring: A good CRM system must always have "event logs" showing "who" accessed whose data, "when," and "whether any modifications were made." Having a good audit log helps the organization perform traceability when anomalies are detected and serves as a crucial tool to demonstrate transparency to regulatory bodies.
- Data Backup and Recovery: Security does not only mean preventing system breaches but also includes availability. Organizations must have regular data backup plans to ensure that if the system crashes or is hit by ransomware, customer data accumulated over many years will not be permanently lost.

CRISIS MANAGEMENT AND DATA SECURITY

Incident Response and Notification Procedures for Customer Data Breaches

In Customer Relationship Management, what is more fearsome than a technical error is an organization "concealing" or "ignoring" a data breach. The Personal Data Protection Act (PDPA) therefore mandates that Data Controllers fulfill their duties according to the procedures set by the Office of the Personal Data Protection Committee (PDPC) as follows:

- Reporting the Incident to the Office: When an organization "becomes aware" of a personal data breach (whether caused by hacking, employee data leaks, or system errors), the organization is obligated to notify the PDPC as soon as possible, within 72 hours.
- Notifying the Data Subject (Customer): If the incident poses a "high risk" to the customer's rights and freedoms (such as financial data or password leaks), the brand must notify the customer without delay, along with providing "remedial measures" and contact channels for further information.

CRISIS MANAGEMENT AND DATA SECURITY

Incident Response and Notification Procedures for Customer Data Breaches

- 5 Practical Steps for Incident Response: When data issues occur, which can severely impact customer trust, a good CRM management approach dictates that the organization must have appropriate response measures. The recommended response steps are as follows:
  - Containment and Control: Immediately disconnect the compromised systems to stop the breach.
  - Risk Assessment: Analyze the type and volume of the leaked data.
  - Legal Notification: Proceed with notifying the Office (PDPC) and/or the customers.
  - Remediation and Correction: Provide assistance to affected customers, such as recommending password changes or providing compensation for damages.
  - Review and Prevention: Record the incident details, causes, and corrective measures to improve future security.
- Penalties for Negligence: Failure to report a data breach within the legally required timeframe carries an administrative fine of up to 3 million THB. Furthermore, intentional concealment that results in serious damage may lead to criminal penalties.

Q & A

Thank you