Central Retail Privacy Protection Management and Procedures

The Company is committed to protect personal information of all stakeholders, including shareholders, employees, customers and business partners. The framework for the Company's privacy protection is consistent with the legal compliance of Personal Data Protection Act (PDPA) in Thailand and other relevant laws and regulations.

Foremost, the Company has published Privacy Policy on the websites operated by our subsidiaries to demonstrate transparency and accountability in our operations. The Privacy Policy addresses how customers' personal data are collected, used, disclosed and transferred, and covers the use of information in stores, service through all online channels, and the customer service call center (operating under the Company).

In addition, the Company has also established internal privacy protection procedures that address how to handle personal information, designated person responsible for data privacy issues, internalization of privacy protection in Company-wide risk management, and compliance. The internal privacy protection procedures apply to all employees working for the Company.

Internal Data Handling Policy

The Company has established an internal Data Handling Policy that states the rules for proper handling of personal data when conducting business operation by employees working for the Company. This policy applies to all employees and emphasizes on the extent of utilizing personal data for marketing communication via various channels including email, SMS, phone call, and website or application notification. Strict enforcement of the internal Data Handling Policy will ensure that the Company will not face legal consequences for non-compliance of PDPA

Privacy Protection Risk Management

The Company has identified information security risks within the group-wide risk management framework. Information security is also considered as an emerging risk due to having high likelihood and high potential impact from disrupting business operation and damaging the Company's reputation. Full compliance with the Privacy Policy, the internal Information Security Policy and the internal Data Handling Privacy will help the Company limit information security risks. Information security threats will become more prominent in the future, which can lead to theft or leak of personal data collected by the Company. In order to detect, prepare, and respond to these risks at the organizational level, the Company has included the experts in risk and compliance, security architecture, security operations, and vulnerability management within the information security governance structure.

Disciplinary Actions

The Company does not tolerate non-compliance to Privacy Policy and the internal Data Handling Policy. Disciplinary actions resulting from breaches in privacy protection are clearly identified in the employment agreement, work rules, and employee code of conduct, and must be acknowledged by all employees. Disciplinary actions for privacy protection breaches can range from warnings and point deductions to termination depending on the severity of the incidents as already stated in the employment agreement, work rules, and employee codes of conduct.

Audits of Privacy Protection

The Company has performed audits of privacy protection conducted by both internal audit team and by external third party. Scope for auditing include privacy protection breach, risk assessment and protection measures, incident response management, personal data handling, and customers' agreement on personal data access and use, etc.

Customer Privacy Information Management

The Company has made Privacy Policy publicly available on the websites of our subsidiaries for customers to access. The Privacy Policy covers the nature of customer privacy information captured, use of the collected information, how long the information is stored by the Company, information security, and third-party disclosure or transfer of the information. The Company may use and disclose customer privacy information for

1. **Providing products and services,**
2. **Marketing communications,**
3. **Invitation to loyalty and reward programs, prize draws, competitions and events,**
4. **Registration and authentication of customer's identity,**
5. **Manage customer relationships,**
6. **Personalization, profiling and data analytics,**
7. **Improving business operations, products and services,**
8. **Functioning of the sites, mobile application and platform,**
9. **IT management and business management purposes,**
10. **Compliance with regulatory and compliance obligations,**
11. **Protection of the Company's interests,**
12. **Fraud detection,**
13. **Corporate transaction,**
14. **Risk management, audit performance and risk assessments,**
15. **Prevention or suppress a danger to a person's life, body, or health.**

In addition, customers have the rights to manage their consents on how information can be used, request to access the information collected by the Company, request for corrections to be made to the information, request to transfer the information to other service providers, and request to delete the information. The Company has tracked that there are none of customers whose information is used for secondary purposes.

Performance

In the past year, the Company has collected a number of incidents and complaints related to cybersecurity and privacy protection, which the results are as follows:

Cybersecurity and Privacy Protection Breaches and Incidents	Year	
	2019	2020
Total number of cybersecurity breaches or other incidents [1]	0	0
Penalties paid in relation to cybersecurity breaches or other incidents (THB)	0	0
Total number of data breaches including leaks of personal data [2]	0	0
Total number of customers and employees affected by the data breaches	0	0
Numbers of complaints received from customers or external parties concerning customer data privacy, and are substantiated	0	0
Numbers of complaints received from government agencies concerning customer data privacy	0	0

[1] Cybersecurity breaches and incidents are cases where the Company's information system and data networks are hacked with the hackers gaining unauthorized access leading to other incidents such as data breaches, ransomware, or disruption of the system.

[2] Data breaches are cases of illegal handling of data that are responsible by the Company, such theft of confidential information, leaking personal information, etc.