Privacy Policy

Element Group (the "**company**", "**we**", "**us**", or "**our**") recognizes the importance of protecting personal data. "Personal Data" refers to any information relating to an individual that enables the identification of that individual, directly or indirectly.

As a Data Controller under the Personal Data Protection Act B.E. 2562 (PDPA), we are committed to ensuring the proper management, protection, and lawful processing of your personal data. This Privacy Policy ("**Privacy Policy**") is designed to inform data subjects of our principles, purposes, and security measures related to the collection, use, disclosure, and protection of personal data.

This Privacy Policy applies to all personal data collected through our websites, mobile applications, online platforms, service points, social media pages, events, and any other channels through which we may interact with you. We may also collect personal data directly from you or indirectly through our affiliated companies, subsidiaries, or trusted business partners.

By engaging with our services, you acknowledge that you have read and understood this Privacy Policy.

1. PERSONAL DATA

1.1. Definition

"Personal Data" refers to any information that relates to an individual and enables the identification of that individual, either directly or indirectly.

"Sensitive Personal Data" refers to personal information that includes, but is not limited to, race, ethnicity, political opinions, religious or philosophical beliefs, sexual orientation, criminal records, health data, disability information, trade union membership, genetic data, biometric data (e.g., fingerprints, facial recognition), or any other data as prescribed by the Personal Data Protection Committee which may significantly impact the data subject.

1.2 Sources of Personal Data

We may receive your personal data through various channels, as follows:

1.2.1 Personal Data Provided Directly by You

We collect your personal data directly from you during your interaction with our services, including but not limited to the following situations:

a: When you register for our services or submit a request to exercise your rights

b: When you voluntarily complete surveys or communicate with us via email or other communication channels

c: When you use our website and we collect data through your browser's cookies

d: When you engage in transactions or business dealings with us through any of our service channels

e: When you choose to participate in company campaigns or activities, such as wellness programs (e.g., weight loss challenges), employee engagement events, or other promotional or social initiatives.

f: When you submit your information through third-party job platforms such as JobsDB, LinkedIn and others in relation to job applications or recruitment processes

g: When you provide explicit consent for specific purposes, such as:

- Receiving marketing or promotional materials

- Allowing the collection or processing of sensitive personal data

- Participating in optional surveys, research, or third-party referrals

- Joining specific company programs or services that require additional data handling

Note: We will always inform you of the purpose of data collection and request your clear, informed, and specific consent before collecting or using your personal data—especially in cases involving sensitive personal data or non-essential processing activities.

1.2.1 Personal Data Received from Third Parties

We may also receive your personal data from third parties, including:

a. Individuals or legal entities we engage to collect personal data on our behalf, such as our group companies, business partners, or service providers that you have previously consented to disclose your information to. The data may be obtained through the following means:

- Received via email
- Received via phone calls
- Received in physical or electronic documents
- Received through other contact methods on our platforms
- Receiving disclosures from our affiliates, group companies, business partners, or third parties

Such data collection will be carried out for the purposes specified in this Privacy Policy and in compliance with applicable laws. In all such cases, the Company will notify the data subject of the collection of their personal data without undue delay, and in any event no later than 30 (thirty) days from the date the data was obtained. Where required, the Company will also obtain the data subject's consent for such collection, unless the collection or notification is exempted under applicable data protection laws, such as Thailand's Personal Data Protection Act (PDPA).

1.3 Categories of Personal Data Collected

In the course of providing financial technology services and digital payment solutions**,** the Company may collect, use, or process the following categories of personal data:

a) Identification and Profile Data

- Full name, title, date of birth, gender, nationality
- Identification numbers (e.g., national ID, passport, tax ID)
- Signature, photographs, audio recordings (e.g., call center recordings), and video footage
- Login credentials, usernames, passwords, user account history

b) Contact Information

- Home, work, or mailing addresses
- Phone numbers (mobile and landline)
- Email addresses

c) Financial and Transactional Information

- Bank account numbers, PromptPay ID, digital wallet ID
- Credit card or debit card details, credit bureau reports

d) Transaction and Usage Data

- Transaction history, payment logs, amounts, timestamps
- Merchant details, goods/services purchased, pricing, discounts
- Service usage records, purchase preferences
- Receipts, invoices, delivery information, refund requests
- Loyalty program participation and reward points (if any)

e) KYC (Know Your Customer) and AML (Anti-Money Laundering) Information

- Customer verification documentation
- Source of funds, source of wealth
- Risk profiles, screening results against sanction lists or watchlists
- Transaction monitoring and suspicious activity reports

1.4 Purpose of Data Processing and Utilization

We process and utilize your personal data for the following purposes:

1.4.1 To fulfill contractual obligations, such as processing payments, completing financial transactions, and delivering products or services you have requested.

1.4.2 To ensure secure and reliable payment services, including fraud detection, identity verification, transaction monitoring, and dispute resolution.

1.4.3 To comply with legal and regulatory requirements, including anti-money laundering (AML), counter-terrorism financing (CTF), and Know Your Customer (KYC) obligations.

1.4.4 To provide customer support and service improvements, including responding to inquiries, resolving complaints, and enhancing the performance and quality of our platform.

1.4.5 To support business operations and system integrity, such as audits, internal analytics, risk management, and maintaining the security of our infrastructure.

1.4.6 To enhance and personalize the user experience, including remembering user preferences, improving interface design, and analyzing usage patterns to better tailor our services.

1.4.7 To engage in marketing and promotional activities, such as sending relevant offers or updates—only with your prior consent where required.

1.5 Legal Basis for the Collection of Personal Data

We collect and process personal data based on the following legal bases:

1.5.1 Contractual Necessity

1.5.1.1 To enter into and fulfill contracts with the data subject (e.g., service agreements, loan agreements, employment contracts, agency or other agreements).

1.5.1.2 To facilitate services such as entering into agreements with third-party vendors, sellers, or insurers.

1.5.2 Compliance with Legal Obligations

1.5.2.1 To comply with applicable laws and regulations, including:

1.5.2.1.1. Tax laws

1.5.2.1.2. Anti-Money Laundering (AML) laws

1.5.2.1.3. Labor protection laws

1.5.2.1.4. Court orders and regulatory directives

1.5.3. Legitimate Interests

1.5.3.1. To carry out activities necessary for the Company's legitimate interests, which do not override the data subject's fundamental rights. These include:

1.5.3.1.1 Verifying identity

1.5.3.1.2 Controlling entry and ensuring workplace security

1.5.3.1.3 Conducting internal audits and operational reviews

1.5.3.1.4 Complying with internal and external corporate governance and regulatory audits

1.5.3.1.5 Protecting the Company's legal rights and business status

1.5.3.1.6 Managing and operating the Company efficiently

1.5.3.1.7 Organizing social, corporate, or promotional events

1.5.3.1.8 Preventing crime and managing physical and digital security, including the use of CCTV within and around the premises, which may capture video, images, and audio

1.5.4. Vital Interests

1.5.4.1 To protect or prevent harm to the life, physical integrity, or health of an individual.

1.5.4.1 For example:

1.5.4.1.1. Contacting emergency references when the data subject is incapacitated

1.5.4.1.2. Monitoring and preventing infectious disease outbreaks

1.5.5. Consent from the Data Subject

1.5.5.1. When legal consent is required for the collection, use, or disclosure of personal data.

1.5.5.2. The Company will clearly inform the data subject of the purpose before or at the time of obtaining consent.

1.5.5.3. Examples include:

1.5.5.3.1. Personalized marketing and promotions by affiliated companies or partners

1.5.5.3.1. Targeted advertising

1.5.5.3.1. Collection or use of sensitive personal data where no legal exemption applies

Note: The Company may rely on additional legal bases where necessary, depending on the nature of the service or business operation, in compliance with the Personal Data Protection Act and relevant laws.

1.6 Principles for the Use and Disclosure of Personal Data

The use and disclosure of personal data by the Company are aligned with the objectives and legal bases outlined in **Section 1.4-1.5**. The Company may disclose personal data to external parties only as necessary, with the consent of the data subject, unless such disclosure is permitted or required by law.

Personal data may be disclosed to the following third parties, organizations, or government authorities:

1.6.1 Affiliated companies or companies within the same corporate group
(e.g., subsidiaries, parent companies, or related entities providing joint services or shared infrastructure).

1.6.2 Contractual partners, service providers, and business partners of the Company, including but not limited to:

1.6.2.1 Financial institutions and banks

1.6.2.2 Insurance companies and insurance brokers

1.6.2.3 E-commerce platforms

1.6.2.4 IT service providers

1.6.2.5 Cloud computing and data storage providers

1.6.2.6 Fraud detection and risk management service providers

1.6.2.7 Marketing and communications agencies

1.6.2.8 Payment processors and acquiring banks

1.6.2.9 API integrators or payment facilitators

1.6.3 Merchants or commercial partners who interact with the Company's payment solutions or platforms.

1.6.4 Banks and financial institutions involved in the processing, settlement, or verification of transactions.

1.6.5 Government authorities and regulatory bodies, as required by law, such as:

1.1.5.1 Bank of Thailand

1.1.5.2 Anti-Money Laundering Office (AMLO)

1.1.5.3 Revenue Department

1.1.5.4 Social Security Office of Thailand

1.1.5.5 Office of the Personal Data Protection Committee (PDPC)

1.1.1.1 Court of Justice

1.1.1.2 Immigration Bureau

1.1.1.3 Legal Execution Department

1.1.1.4 Any other agency with legal authority or relevance to the Company's operations

1.6.6 Other relevant organizations or third parties involved in the Company's business activities or regulatory compliance, including auditors, legal advisors, and professional consultants.

2. RETENTION PERIOD OF PERSONAL DATA

The Company retain personal data for the following durations:

In accordance with the period required by applicable laws governing data retention, such as:

- The Accounting Act B.E. 2543 (2000)
- The Anti-Money Laundering Act B.E. 2542 (1999)
- The Revenue Code and other relevant laws or regulations

Where there is no specific legal requirement for data retention, the Company will retain personal data for a duration that is reasonably necessary to fulfill the purposes for which the data was collected, based on operational needs and internal policies.

Once the applicable retention period has ended or the data is no longer necessary for the stated purposes, the Company will securely delete, destroy, or anonymize the personal data so that it can no longer be used to identify the data subject.

3. CROSS-BOARD TRANSFER OF PERSONAL DATA

The Company may transfer or transmit personal data collected from data subjects to affiliates, group companies, or third-party service providers located outside of Thailand. This includes, for example:

- Cloud computing providers with platforms or servers based overseas
- Data processors
- Platform-as-a-Service (PaaS) providers
- Any other business partners or service providers necessary to fulfill the purposes outlined in this Privacy Policy

Such transfers are carried out to support the Company's services and operations as stated in this Policy. The Company will take necessary steps to ensure that the destination country maintains **an adequate level of personal data protection** in line with applicable standards.

In cases where the destination country does not provide adequate data protection standards, the Company will implement appropriate safeguards to ensure that the personal data is protected in accordance with the Personal Data Protection Act B.E. 2562 (2019) and other relevant laws and regulations. These measures may include binding agreements, standard contractual clauses, or other lawful mechanisms.

4. PERSONAL DATA SECURITY MEASURES

The Company implements appropriate security measures to protect personal data from loss, unauthorized access, misuse, alteration, or disclosure, whether intentional or unlawful. These measures are aligned with the Company's Information Security Policies and applicable data protection laws.

In the case that the Company engages third-party service providers to collect, use, or disclose personal data on its behalf, such parties are required to maintain strict confidentiality and implement robust security controls to ensure that personal data is not used or disclosed beyond the scope of the engagement or in violation of the law.

4.1. Administrative Safeguards

Measures related to policies, procedures, and internal controls to ensure proper handling of personal data.

4.2. Technical Safeguards

Implementation of technology-based protections, including encryption, firewalls, and intrusion detection systems.

4.3. Physical Safeguards

Controls over physical access to systems and devices used for storing and processing personal data. These safeguards include, but are not limited to:

4.3.1. Access Control to Personal Data and Related Equipment Ensuring that only authorized personnel can access systems or devices based on necessity and security risk.

4.3.2 Authorization and Permission Management Assigning access rights and privileges based on roles and responsibilities.

4.3.3 User Access Management Ensuring access to personal data is granted only to those who are properly authorized.

4.3.4 User Responsibility Definition Outlining responsibilities to prevent unauthorized access, disclosure, copying, or theft of personal data or devices.

4.3.5 Audit and Logging Measures Implementing audit trails that allow tracking and verification of access, alteration, deletion, or transfer of personal data—appropriate to the methods and media used in collecting, using, or disclosing such data.

5. DATA SUBJECT RIGHTS

This Privacy Policy is intended to assure data subjects that they are entitled to exercise the following rights under the Personal Data Protection Act B.E. 2562 (2019) and other applicable laws:

5.1 Right to Withdraw Consent

Data subjects have the right to withdraw their consent to the processing of their personal data at any time while the company continues to retain such data.

5.2 Right of Access

Data subjects have the right to access their personal data held by the company and request a copy. They may also request that the company disclose the source of the data if it was not provided directly by the data subject.

5.3 Right to Rectification

Data subjects have the right to request correction of inaccurate personal data or completion of incomplete data.

5.4 Right to Erasure

Data subjects have the right to request the deletion of their personal data under certain legal conditions.

5.5 Right to Restriction of Processing

Data subjects have the right to request that the company restrict the use of their personal data under specific circumstances.

5.6 Right to Data Portability

Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transfer such data to another data controller, where technically feasible.

5.6 Right to Object

Data subjects have the right to object to the processing of their personal data under certain grounds as permitted by law.

6. CONTACT INFORMATION

If you have any questions, concerns, or wish to exercise your rights relating to your personal data, you may contact us through the following channels:

Element Payment Solutions (Thailand) Co., Ltd.

(Privacy Team)

Address: 17 Soi Rama 9 60 (Soi 8 Seri 7) Phatthanakan Sub-District, Suan Luang District, Bangkok, Thailand

Email: legal@elementpay.io

Tel: +6620737189

Business Hours: Monday to Friday, 9:00 AM – 6:00 PM

We are committed to addressing your concerns in accordance with the applicable data protection laws, including the Personal Data Protection Act B.E. 2562 (PDPA).

7. POLICY REVIEW AND UPDATES

The Company will review and update this policy at least once a year, or whenever there are amendments or changes to the relevant laws and regulations related to this policy.

Effective date: 1 September 2025