Data protection Policy

TQR Public Company Limited

Table of Contents

Personal Data Protection Policy of TQR Public Company Limited

TQR Public Company Limited recognizes the importance of personal data protection as part of corporate social responsibility and a foundation for building trustworthy business relationships with customers. Committed to complying with data protection laws and regulations, the company ensures that the personal data of individuals is securely managed and protected.

This policy includes the following components:

1. Personal Data Classification Policy
2. Personal Data Disposal Policy
3. Data Retention Policy
4. Third-Party Data Transfer Policy
5. Cross-Border Data Transfer Policy
6. Binding Corporate Rules
7. Outsourcing Policy for Personal Data Processing

Definitions

In this Personal Data Protection Policy, the terms or expressions are defined as follows:

Term	Definition
Personal Data Protection Law	Refers to the Personal Data Protection Act B.E. 2562 (2019) and any subsequent amendments, including related rules, regulations, and directives.
Anonymization	The process of rendering personal data into anonymous data (e.g., masking, hash function), making it impossible to identify individuals.
Pseudonymization	A process that reduces or limits the ability to link personal data with original datasets without rendering the data completely

Term	Definition
	anonymous, used as a data security measure (e.g., replacing identifiers with other data or new numbers).
Data Processing	Any operation performed on personal data, whether automated or not, including collection, recording, organization, storage, modification, retrieval, usage, disclosure, restriction, erasure, or destruction.
Data Deletion/Destruction	The permanent removal or destruction of personal data so it cannot be recovered or reconstructed by any party.
Access	The right to read, view, copy, store, retrieve, download, or modify data, including managing access permissions.
Recording	Specific data or information created or obtained from individual or organizational activities, preserved as evidence for future reference.
Data	Any information, electronic or otherwise, obtained or held by the Company, its partners, or third parties.
Personal Data	Any information that can directly or indirectly identify an individual, excluding deceased persons, as defined in Section 6 of the Personal Data Protection Act B.E. 2562 (e.g., name, email, fingerprints, location data, cookies, etc.).
Sensitive Personal Data	Personal data involving race, ethnicity, political opinions, religious beliefs, sexual behavior, criminal records, health information, disability, genetic or biometric data, and other sensitive information as determined by relevant authorities.
Data Protection Officer	An officer appointed by the data controller to serve as the Data Protection Officer under the Personal Data Protection Act B.E. 2562.

Term	Definition
Data Subject	A natural person who can be identified by personal data, either directly or indirectly, excluding legal entities.
Information Owner	The individual responsible for specific information, either obtained directly from the data subject or created independently, tasked with assigning data classifications and risk levels.
Third Party	Any individual or entity, including government agencies, outside the data subject, the Company, or its data processors, authorized to process the data.
Data Controller	The Company or organization with authority over the decision-making related to the personal data collected from employees, job applicants, or other contractual obligations.
Data Processor	An individual or entity processing personal data on behalf of the data controller, as instructed.
External Service Provider	A data processor, either an individual or entity, not employed by the Company, responsible for personal data processing as instructed by or on behalf of the Company.
Data Storage Media	Various types of media used for data storage, such as paper documents, hard drives, flash drives, tapes, disks, CDs, and DVDs.

1. Personal Data Classification Policy

The company has established four levels of information confidentiality: Public Data, Internal Use Only Data, Confidential Data, and Top Secret Data. The guidelines for implementing this policy are outlined in the Personal Data Classification Procedure, which all relevant parties must strictly follow. If an information group contains data of varying confidentiality levels, the data owner must classify the group according to the highest confidentiality level within the group.

- Data owners are responsible for regularly defining and reviewing the confidentiality levels of personal data under their responsibility and ensuring appropriate controls are in place for each confidentiality level.
- Data owners must keep personal data confidential and disclose it only to authorized persons in compliance with legal and regulatory requirements.
- Relevant departments must implement appropriate access controls to ensure that only authorized individuals have access to personal data, as needed and in a timely manner.
- Requests for access to personal data beyond predefined permissions must be reviewed and approved by the data owner.
- Technical measures to grant access must comply with the company's information security protocols.
- Personal data must be retained only as necessary to fulfill the purposes of collection, use, or disclosure, and must be deleted, destroyed, or anonymized once it is no longer required for these purposes.
- When engaging external service providers to collect, use, or disclose personal data, the company must follow the **Outsourcing for Personal Data Processing** guidelines. Data owners must classify the confidentiality levels of personal data involved in such engagements.

1.1 Personal Data Classification Procedure

Data owners are responsible for defining and regularly reviewing the classification levels of personal data within their area of responsibility. This ensures alignment with the changing importance of the information over time and the implementation of appropriate controls based on the data's confidentiality level. Data owners may delegate control activities to data custodians and seek technical support from the IT department but remain ultimately accountable for classification and security controls.

Personal data must only be retained for as long as necessary to fulfill its intended purpose. Once the retention period expires, or if the data is no longer relevant, it must be deleted, destroyed, or anonymized according to the Personal Data Disposal guidelines.

Relevant departments must consider whether legal requirements or operational needs necessitate data retention for specified periods as outlined in the Data Retention guidelines. If specific information cannot be classified using predefined definitions or examples, the data owner must determine its confidentiality level. When an information group contains data with multiple confidentiality levels, the group must be classified based on the highest level of confidentiality within it.

Data Classification Levels

Classification Level	Definition	Examples
Top Secret	Information assessed to cause severe financial or non-financial harm to the company if disclosed without authorization. This information requires special care by the owner and authorized personnel. Access requires signing a **Non-Disclosure Agreement (NDA)** or equivalent confidentiality agreement approved by senior management.	Business strategy plans (pre-announcement), merger and acquisition plans, or trade secrets.
Confidential	Information that, if disclosed without authorization, violates company policies or regulations and may harm the company's reputation, financial standing, or competitive advantage. Access is limited to employees or third parties under NDA agreements.	Passwords, encryption keys, financial data, customer information, budget details, sensitive personal data (e.g., race, health, political views).

Classification Level	Definition	Examples
Internal Use Only	Information restricted to internal employees and authorized external partners. Not suitable for public disclosure.	Internal emails, company policies, employee contact directories.
Public	Information approved for public release that does not significantly impact operations. Must still be accurate and complete to maintain the company's reputation.	Marketing brochures, press releases, shareholder announcements.

1.2 Guidelines for Information Control and Protection

The control and protection of information cover the creation, storage, printing, copying, transmission, destruction, and reuse of information in both physical and electronic formats. The following outlines the necessary controls for different data classifications:

Processing Guidelines by Data Classification

Data Type	Public	Internal Use Only	Confidential	Top Secret
Data Preparation				
Marking or Labeling Documents	No special requirements.	Clearly label with "Internal Use Only" or equivalent. For external communication, specify "Internal Use Only [Company Name]". Backup tapes are exempt from labeling due to technical risks.	Clearly label with "Confidential" or equivalent on all pages where feasible. For external communication, specify "Confidential [Company Name]". Backup tapes are exempt from labeling.	Clearly label with "Top Secret" on all pages, along with department ownership, set number, and total pages. For external communication, specify "Top Secret [Company Name]".

Data Type	Public	Internal Use Only	Confidential	Top Secret
Printing Hard Copy Documents	No special requirements.	Collect printed documents immediately after printing; do not leave them unattended.	Verify the destination printer before printing. Ensure prompt retrieval and avoid printing at external locations like hotels or airports.	Verify the destination printer before printing. Ensure prompt retrieval and avoid printing at external locations like hotels or airports and ensure strict monitoring during printing.
Data storage				
Storing Hard Copy Documents	No special requirements.	Store systematically in appropriate locations for operations.	Store securely, such as in a locked cabinet or safe.	Store securely, such as in a locked cabinet or safe., ensuring maximum security.
Storing on Computers or Servers	No special requirements.	No encryption required but must be stored in controlled-access folders.	Store in encrypted files or controlled-access folders.	Store in encrypted files or controlled-access folders, ensuring encrypted storage or controlled folder access.
Cloud Storage	No special requirements.	Controlled access measures required.	Store in encrypted files or controlled-access folders.	Store in encrypted files or controlled-access folders, ensuring encrypted storage or

Data Type	Public	Internal Use Only	Confidential	Top Secret
				controlled folder access.
Storage on Mobile phone (Electronic Data)	No special requirements.	a pin-code or password are set up prior to access to prevent access to data in case the phone is lost or stolen.	a pin-code or password are set up prior to access to prevent access to data in case the phone is lost or stolen.	a pin-code or password are set up prior to access to prevent access to data in case the phone is lost or stolen.
Storage on Media (e.g., USB, SD Card)	No special requirements.	No special requirements.	Use encryption such as AES-256, Bit Locker or other approved tools.	Use encryption such as AES-256, Bit Locker or other approved tools., ensuring high-level encryption.
Media Storage	No special requirements.	Store in a place suitable for the operation and store systematically.	Keep in a tightly closed place and prevent unauthorized access, such as by keeping it in a cabinet, locking it when not in use, or storing it in a safe.	Keep in a tightly closed place and prevent unauthorized access, such as by keeping it in a cabinet, locking it when not in use, or storing it in a safe.
Data storage (when data is taken off-site)				

Data Type	Public	Internal Use Only	Confidential	Top Secret
Transporting Data During Travel	No special requirements.	Data must remain under supervision or stored in secured locations like sealed envelopes in locked hotel safes.	Data must remain under supervision or stored in secured locations like sealed envelopes in locked hotel safes, ensuring restricted access.	Data must remain under supervision or stored in secured locations like sealed envelopes in locked hotel safes, ensuring restricted access with additional verification steps.
When carrying Hard copy in the car	No special requirements	Keep it in a locked vehicle and in a location where it cannot be seen from outside.	Keep it in a locked vehicle and in a location where it cannot be seen from outside.	Keep it in a locked vehicle and in a location where it cannot be seen from outside.
Sending/receiving and transferring data				
Mailing Hard Copies or Media	No special requirements.	Use sealed opaque envelopes.	Use sealed envelopes marked "Confidential".	Mailing not recommended. If necessary, follow Confidential protocol with owner approval.
Hand delivery, hard copy documents and media	No special requirements.	No special requirements.	• Place the documents in a sealed envelope and stamp it with the word Confidential.	• The envelope must be sealed before delivery so that it cannot be seen from the outside.

Data Type	Public	Internal Use Only	Confidential	Top Secret
			• Keep a record of the sending and receiving for evidence.	• Place in 2 layers of envelopes. • The inner envelope must indicate the confidentiality level. • The outer envelope must not indicate the confidentiality level. • Keep a record of the sending and receiving as evidence. • Deliver only to the authorized person.
Fax transmission	No special requirements.	No special requirements.	• Must clearly state the sender and receiver's names. • Always check to make sure it is the actual address to be sent. • Must send fax to secure destination. • Must wait until the transmission is complete before taking the document back	Do not send via fax.

Data Type	Public	Internal Use Only	Confidential	Top Secret
			without forgetting it at the fax machine. • Have the authorized person wait to receive the document at the destination.	
Electronic Transmission (Email, FTP)	No special requirements.	No special requirements.	Encrypt data or use password-protected files with separate password transmission.	Electronic transmission discouraged unless approved by the data owner. Follow Confidential protocols if necessary.
Data Destruction				
Destroying Hard Copies	No special requirements.	Shred or use contracted destruction services.	Use a non-recyclable document shredder (cross-cut shredder) or send it to an external agency with a contract to destroy documents.	Documents must be returned to the owner for destruction or used a non-recyclable document shredder (Cross-cut Shredder) with prior approval from the Information Manager or above prior to destruction.

Data Type	Public	Internal Use Only	Confidential	Top Secret
Destroying Electronic Data	No special requirements.	Clear data from recycle bin or use tools like Eraser.	Use low-level formatting or advanced tools (e.g., Eraser 3 Passes).	Use low-level formatting or advanced tools (e.g., Eraser 3 Passes), ensuring irreversible deletion.
Destruction of configuration data and data stored on the device	No special requirements.	Reset the configuration values and data stored on the device to Factory Default values.	Reset the configuration values and data stored on the device to Factory Default values.	Reset the configuration values and data stored on the device to Factory Default values.
Media Destruction (CD/DVD, USB)	No special requirements.	Destroy using strip-cut tools or physical destruction.	Destroy using strip-cut tools or physical destruction.	Destroy using strip-cut tools or physical destruction.
Media Destruction (USB Flash Drive, Hard disk, and Tape)	No special requirements.	Destroy or in a manner that the IT group considers secure.	Destroy or in a manner that the IT group considers secure.	Destroy or in a manner that the IT group considers secure.
Data loss management				
Electronic	No special requirements.	Report responsible manager / owner immediately to minimize damage (e.g.,change	Report responsible manager / owner immediately to minimize damage (e.g.,change	Report responsible manager / owner immediately to minimize damage (e.g.,change

Data Type	Public	Internal Use Only	Confidential	Top Secret
		passwords, wipe data).	passwords, wipe data).	passwords, wipe data).
Hard Copy	No special requirements.	Report to the responsible manager immediately upon discovery.	Same as Internal Use Only, with heightened urgency.	Same as Confidential, with immediate action.
Others				
Hard copy and electronics	No special requirements.	No special requirements.	If no confidentiality level mark, but knows or should know that the information has been assigned confidentiality level, shall be treated in the same way as information marked with a confidentiality level, and shall prepare or notify the owner to prepare a confidentiality level mark as soon as possible.	If no confidentiality level mark, but knows or should know that the information has been assigned confidentiality level, shall be treated in the same way as information marked with a confidentiality level, and shall prepare or notify the owner to prepare a confidentiality level mark as soon as possible.

This framework ensures consistent, secure management and protection of data across all classification levels. All employees are responsible for adhering to these guidelines and reporting any deviations or incidents to the relevant authorities.

2. Personal Data Disposal Policy

The company acknowledges the importance of maintaining the security and confidentiality of personal data. To this end, it has established processes for the deletion, destruction, or anonymization of personal data once its retention period has expired, as stipulated in the Personal Data Retention Policy, or in response to the data subject's rights under applicable personal data protection laws. These processes aim to prevent loss, unauthorized access, destruction, misuse, alteration, or unlawful disclosure of personal data and ensure compliance with the company’s security practices.

2.1 Disposal of Physical Documents

The company requires secure methods for the destruction of paper-based personal data according to the Personal Data Classification Procedure, as follows:

- Public: Tear, shred, or send to an authorized external service provider for secure disposal.
- Internal Use Only: Tear, shred, or send to an authorized external service provider for secure disposal.
- Confidential: Use cross-cut shredders that make reconstruction impossible or send to an authorized external service provider for secure disposal.
- Top Secret: Return documents to the owner for destruction or use cross-cut shredders exclusively.

The guidelines may be updated or revised as deemed necessary by the company or to comply with applicable legal requirements.

2.2 Electronic Data Deletion/Destruction

The company requires secure methods for deleting or destroying electronic personal data according to the Personal Data Classification Procedure, as follows:

- Public: Delete files and clear the recycle bin, or use data deletion software (e.g., Eraser).
- Internal Use Only: Delete files and clear the recycle bin, or use data deletion software (e.g., Eraser).
- Confidential: Perform low-level formatting or use data deletion software that ensures irrecoverability (e.g., Eraser with 3 Passes).
- Top Secret: Perform low-level formatting or use advanced data deletion software (e.g., Eraser with 3 Passes) to ensure irrecoverability.

The guidelines may be updated or revised as necessary by the company or to comply with additional legal requirements.

2.3 Anonymization of Personal Data

In cases where direct deletion or destruction of personal data is not feasible due to potential operational impacts (e.g., database errors or system limitations), the company may anonymize the data, rendering it unidentifiable. Methods include:

1. Data Transformation: Replace identifiable elements with randomly generated characters or other irreversible transformations, such as using hash functions.
2. Blurring or Noising: Substitute data with approximate values to reduce specificity.

These methods may be updated or revised as necessary by the company or to comply with additional legal requirements.

2.4 Conditions for Data Disposal or Anonymization

The company will delete or anonymize personal data under the following circumstances:

1. The data has exceeded the retention period specified in the Personal Data Retention Policy.
2. The data is no longer relevant or exceeds the purpose for which it was collected.
3. The data was unlawfully collected, used, or disclosed.
4. The data subject exercises their right to deletion under personal data protection laws, or withdraws their consent.
5. The data subject objects to the processing of their data under Section 32(1) or (2) of the Personal Data Protection Act B.E. 2562 (PDPA), and the company cannot deny the objection.

Under Section 33 of the PDPA, the company may deny data deletion requests in the following circumstances:

1. When necessary for freedom of expression or information rights.
2. For historical, archival, public interest, or research purposes, with appropriate safeguards in place.
3. When necessary to perform public interest duties or state-authorized functions.
4. For legal compliance, including:
    - Preventive or occupational medicine, health assessments, medical diagnostics, or healthcare service provision.
    - Public health interests, such as controlling epidemics or ensuring the safety of medical devices, with safeguards to protect data confidentiality.
5. For the establishment, exercise, or defense of legal claims or compliance with laws.

3. Data Retention Policy

The company is committed to managing personal data securely, ensuring it is retained only for as long as necessary to fulfill its intended purposes, in accordance with relevant legal, business, and industry standards.

3.1 Storage Locations

3.1.1 Electronic Documents, Emails, and Multimedia Records

All electronic documents, emails, and multimedia records must be stored in appropriate locations that comply with personal data protection laws, other relevant laws, guidelines, and directives. Security measures must meet established legal standards.

3.1.2 Paper Documents

Paper documents required for daily business operations must be stored in filing cabinets or desk drawers when not in use. Employees must lock these storage units at the end of the workday to ensure security.

3.2 Document Protection

The company strives to prevent unauthorized loss, access, use, alteration, or disclosure of personal data, whether in paper or electronic formats. All documents containing personal data will be stored securely until they are destroyed. The company uses technologies and regularly reviewed processes to safeguard personal data.

3.3 Document Destruction

When the retention period expires or personal data is no longer needed, documents containing personal data will be destroyed using the following methods:

- **Paper Documents:** Shredded by assigned personnel.
- **Electronic Data:** Deleted from storage media, such as hard drives, using methods that prevent data recovery. Hard drives will be physically destroyed or securely wiped by designated personnel.

3.4 Retention Period and Procedures

The company defines retention periods based on the purpose of personal data collection and processing. These periods align with legal, business, or industry standards. Specific retention periods are detailed in the appendix.

The company will implement systems to:

1. Monitor and delete or destroy personal data upon expiration of the retention period.
2. Fulfill data subject rights under personal data protection laws.
3. Comply with other legal requirements or align with the **Personal Data Disposal Policy**.

4. Third-Party Disclosure Policy

The company may disclose personal data to external entities following these guidelines:

1. Disclosure is allowed only to partners, business affiliates, subsidiaries, or external service providers listed in the **Data Inventory**. If not listed, approval from the Data Protection Officer (DPO) is required. The DPO must verify the processing basis and compliance with the **Personal Data Protection Act B.E. 2562 (PDPA)**.
2. Contracts must include measures addressing:
    - Data processing responsibilities.
    - Security measures.
    - Activities related to data subject rights.
    - Breach notifications.
    - Data retention and disposal.
    - Cross-border data transfers.
3. The company must ensure the recipient entity implements security and personal data protection measures that meet required standards.
4. Disclosure to government entities must be based on formal legal authority (laws, regulations, or official orders). Unauthorized disclosure may result in legal liability unless it fulfills a Legal Obligation.

5. Cross-Border Data Transfer Policy

Personal data transfers are subject to data protection laws. Transfers to destination countries or international organizations must meet security standards. The company will consider the following options:

1. **Transfers to Approved Destinations:**
   Transfers are permitted to countries with certified personal data protection policies recognized by the **Office of the Personal Data Protection Committee**.
2. **Contractual Agreements:**
   Agreements can be based on:
   - **Binding Corporate Rules (BCR):** Approved by the relevant authority.
   - **Standard Data Protection Clauses (SCC):** Compliant with legal standards.
   - **Codes of Conduct:** With defined safeguards.
3. **Exceptional Transfers:**
   Transfers may occur if:
   - Required by law.
   - The data subject consents after being informed of insufficient protection standards.
   - Necessary to fulfill a contract or pre-contractual obligations.
   - Beneficial to the data subject under a controller agreement.
   - To prevent harm to the life, body, or health of the data subject or others when consent cannot be obtained.
4. **Insufficient Protection Standards:**
   For destinations lacking adequate protection, the matter must be referred to the **Office of the Personal Data Protection Committee** for approval.

6. Personal Data Protection for Corporate Group (Binding Corporate Rules)

The company may transfer personal data within its corporate group or affiliated business entities for joint operations or business purposes, provided such transfer complies with the

personal data protection policy for transferring personal data to controllers or processors located in other countries but within the same corporate group or affiliated business entities ("corporate group members"). This policy must be reviewed and certified by the Office of the Personal Data Protection Committee. The personal data protection policy, referred to as Binding Corporate Rules (BCR), must:

1. **Be legally binding** and enforceable on all corporate group members, including employees and staff of the corporate group ("corporate group members").
2. **Guarantee enforceable rights** for personal data subjects whose data is processed.
3. **BCR must include at least the following elements**:

3.1. Details of the structure and contact channels of corporate group members.

3.2. Information on disclosed personal data or sets of personal data, including types of personal data, methods, purposes of processing, categories of data subjects, and the destination countries or international organizations receiving the personal data.

3.3. Legal binding effect, both internally and externally, among the corporate group members.

3.4. Implementation of general data protection principles such as Purpose Limitation, Data Minimization, Limited Storage Periods, Data Quality, Data Protection by Design and Default, Lawful Basis for Processing, processing of sensitive data per Section 26 of the Personal Data Protection Act (PDPA) 2019, security measures, and conditions for onward transfers to non-members.

3.5. Rights of personal data subjects, mechanisms to exercise those rights, including the right to lodge complaints with the Office of the Personal Data Protection Committee and to seek judicial remedies for damages resulting from BCR violations.

3.6. Acceptance of liability by controllers or processors in Thailand for violations of the BCR by non-Thai members, with exemptions if the Thai member can prove it was not responsible for the damages caused.

3.7. Notification of BCR content (especially 3.4 to 3.6) to personal data subjects in addition to details under Sections 23 and 25 of the PDPA 2019.

3.8. Roles of the Data Protection Officer (DPO) per Section 41 of the PDPA 2019, including monitoring BCR compliance, training, and handling complaints.

3.9. Complaint-handling mechanisms.

3.10. Internal mechanisms to ensure BCR compliance, including Data Protection Audits and remedial measures for protecting data subjects' rights. The DPO and corporate group board must review and provide audit results to the Office of the Personal Data Protection Committee for inspection.

3.11. Mechanisms for reporting and documenting BCR amendments to the Office of the Personal Data Protection Committee.

3.12. Mechanisms for cooperation with the Office of the Personal Data Protection Committee to ensure BCR compliance, including audit transparency.

3.13. Reporting mechanisms for legal obligations in destination countries that might significantly impact BCR guarantees.

3.14. Appropriate personal data protection training for employees or individuals who regularly access personal data.

4. In addition to BCR, the company may adopt other appropriate safeguards enforceable on personal data subjects as determined by the Office of the Personal Data Protection Committee, such as Standard Contractual Clauses (SCC), Codes of Conduct, or Certification Mechanisms. These options include:

4.1. **Standard Contractual Clauses (SCC):**

The company adopts SCC to ensure proper and lawful personal data transfers, maintaining service standards and compliance. SCC must define contractual obligations regarding international transfers and allow data subjects to exercise their rights in such transfers.

4.2. **Codes of Conduct:**

The company transfers data only when the recipient adheres to an approved code of conduct, which includes appropriate measures to protect data subjects' rights. The code must have enforceable obligations on the recipient, aligning with corporate governance and ethical standards for transparency and accountability.

4.3. **Certification Mechanism:**

The company uses certifications recognized by the Office of the Personal Data Protection Committee, coupled with binding commitments to ensure appropriate data protection measures for international transfers, demonstrating sufficient safeguards for personal data globally.

7. Policy or Guidelines for Agreements or Contracts between Personal Data Controllers and Personal Data Processors (Outsourcing Policy for Personal Data Processing)

Guidelines for Agreements or Contracts between Personal Data Controllers and Personal Data Processors

1. Departments disclosing personal data to partners, business alliances, subsidiaries, and/or external service providers must establish a contract between the company and the respective partner, business alliance, subsidiary, and/or external service provider. The contract must comply with the format prescribed by the responsible department.
2. The content of the contract between the company and the partner, business alliance, subsidiary, and/or external service provider must include measures regarding:
    - **Responsibilities in data processing**, which must include provisions on:
        - Instructions for processing personal data, explicitly prohibiting personal data processors from processing data beyond the written instructions of the personal data controller.
        - A declaration from the personal data processor that the instructions of the personal data controller do not exceed the purpose of collecting, using, or disclosing personal data.
        - Restriction of access to personal data by the personal data processor to designated individuals necessary for the contract's purposes.
        - The obligation of the personal data processor to maintain the confidentiality of processed personal data, including measures to

ensure that authorized individuals commit to or are contractually obligated to uphold confidentiality.

- The requirement for the personal data processor to provide necessary information demonstrating compliance with contractual obligations and to cooperate with audits and inspections conducted by the personal data controller or their designated auditor.

- **Measures to ensure data security**, which must include provisions on:
  - The responsibility of the personal data processor to implement appropriate security measures to ensure the confidentiality, integrity, and availability of personal data, incorporating administrative, technical, and physical safeguards, including:
    - Controlling access to personal data and devices used for storing and processing it, considering operational and security requirements.
    - Specifying permissions or access rights to personal data.
    - User access management to ensure only authorized individuals can access personal data.
    - Defining user responsibilities to prevent unauthorized access, disclosure, exposure, copying, or theft of personal data or devices used to store or process it.
    - Establishing methods to enable traceability of access, changes, deletion, or transfer of personal data, appropriate to the methods and media used for collection, use, or disclosure.
- **Responsibilities related to personal data subject rights**, which must include provisions on:
  - The personal data processor's duty to support the personal data controller in enabling data subjects to exercise their rights.

- Notification to the personal data controller in cases where there is a request to exercise the rights of a data subject.

- **Notification of personal data breaches**, which must include provisions on:
  - Prompt notification to the personal data controller upon becoming aware of a personal data breach.
- **Retention and deletion of personal data**, which must include provisions on:
  - The duty and duration of retaining personal data only as necessary to comply with the personal data controller's instructions.
  - Methods for deleting, destroying, returning, or anonymizing personal data.
  - Retention of personal data for establishing legal claims, compliance with laws, or defense against legal claims.
- **Transfer or transmission of personal data to foreign countries**, which must include provisions on:
  - Prohibiting the personal data processor from transferring or transmitting personal data to foreign countries without the company's authorization.
  - Ensuring that such transfers or transmissions comply with conditions specified in personal data protection laws and related regulations.

Appendix A: Examples of Personal Data Confidentiality Classification

Data Category	Details	Confidential	Internal Use Only
Identity Verification Data			
	- Passwords	✓	
	- Encryption keys	✓	
	- Biometric data (e.g., facial recognition, iris scans, fingerprints)	✓	
	- Authentication logs	✓	
Electronic Card Information			
	- Cardholder name	✓	
	- Card numbers	✓	
	- PIN, PIN block	✓	
	- CVV, CVV2, CVC2, CID	✓	
	- Magnetic stripe data	✓	
Personally Identifiable Information (PII)			
	- Full name		✓
	- ID card number		✓
	- Passport number		✓
	- Social security number		✓
	- Driver's license number		✓
			✓

Data Category	Details	Confidential	Internal Use Only
	- Taxpayer identification number		✓
	- Employee code		✓
	- Bank account number		✓
	- Policy number		✓
	- Date of birth		✓
	- Age		✓
	- Gender		✓
	- Address		✓
	- Phone number		✓
	- Email address	✓	
	- Salary information		✓
	- Device data (e.g., IP address, MAC address, Cookie ID)	✓	
	- Biometric data (e.g., facial images, fingerprints, genetic data)		✓
	- Property data (e.g., vehicle registration, land deeds)		✓
	- Employment data		✓
	- Work history		✓
	- Performance evaluations		✓
	- Activity tracking data (e.g., log files)		

Data Category	Details	Confidential	Internal Use Only
Sensitive Personal Data			
	- Religious or philosophical beliefs	✓	
	- Political opinions	✓	
	- Racial or ethnic origin	✓	
	- Genetic data	✓	
	- Criminal records	✓	
	- Sexual behavior	✓	
	- Health or medical records	✓	
	- Union membership	✓	

Appendix B: Examples of Personal Data Retention

No.	Department	Function	Purpose	Retention Trigger	Retention Period	Action Required	Reason / Related Entity
1	Finance & Accounting	Receipts and payments	To record Company transactions	Completion of receipt/payment process	5 years	Review reasons for retention	Varies by activity purpose
2	Finance & Accounting	Tax submissions	To submit documents to the Revenue Department	Closing of accounts	5-7 years	Review reasons for retention	Accounting Act B.E. 2543, Section 14
3	Finance & Accounting	Financial documentation	To process payments to clients/suppliers	Completion of payment process	5 years	Review reasons for retention	Varies by activity purpose
4	Human Resources	Job applications	To retain applications for future recruitment	End of recruitment decision	2 years	Review reasons for retention	Future hiring considerations
5	Human Resources	Employment contracts	To execute employment contracts	End of employment contract	12 years	Review reasons for retention	Labor Protection Act B.E. 2541, Section 115
6	Human Resources	Social security filings	To submit to the Social Security Office	End of employment contract	12 years	Review reasons for retention	As per employment contract period
7	Information Technology	System management	To retain system logs	Achievement of data collection purpose	120 days	Delete/Destroy	Computer Crimes Act B.E. 2550