台達集團
DELTA GROUP

Document Name:	Personal Data Protection System and Organization Bylaws
Document No.:	PIMS-ENG-02-04-003
Version:	001 (Approved by the Chairman of Personal Data Protection Team on June 23, 2021) 002 (Approved by the Chairman of Personal Data Protection Team on Jan. 01, 2022) 003 (Approved by the Project Leader of Personal Data Protection Team on Jul. 21, 2022) 004 (Approved by the Project Leader of Personal Data Protection Team on Dec. 29, 2022)

Table of Contents

1. **Purpose**

Delta Group is dedicated to ensure the effectiveness of personal information management system and with the accordance of “Delta Group Personal Data Protection Management Policy” in order to define the personal information management roles and responsibilities.

2. **Scope**

2.1 The procedure applies to the Delta Group

2.2 Delta Group personal information management system is based on the framework of ISO27701 international standard, and it covers the critical business of Delta Group.

3. **Roles and Responsibilities**

3.1 Management level shall conduct the following points in order to show the support of implementing personal information management system.

3.1.1 Communicate with stakeholders and comply with the regulation requirements in order to enhance the personal information management objectives.

3.1.2 Authorize Personal Data Protection Team to manage personal information management process.

3.1.3 Approve “Delta Group Personal Data Protection Management Policy” in order to establish personal information management objectives and strategies.

3.1.4 Approve personal information audit plan and result.

3.1.5 Approve the acceptable risk level within the group.

3.1.6 Provide necessary resource that support the personal information management system.

3.2 Delta Group shall establish a Personal Data Protection Team in order to manage personal information management related process.

3.2.1 Organization Structure

The team is consisted of 1-2 representatives from each business group, business unit or corporate unit, a chairman, or a proxy chairman designated by the chairman. The chairman is in charge of managing personal information related work. Please refer to “Personal Data Protection Team Organization List”.

3.2.2 Roles and responsibilities

The responsibilities of the organization include but not limited to planning, formulating and revising the Personal Data Protection Management Policy, implementation method and related procedures; defining the roles and responsibilities; developing personal information management measures; supervising and ensuring the operation result; and providing Delta Group overall personal data guidance and consultation.

3.2.3 Member

3.2.3.1 Chairman:

Responsible for promoting, coordinating and supervising Delta Group's personal data protection management business, and providing the necessary resources for personal data collection, processing and utilization.

3.2.3.2 Personal data protection convener ：

A. Assist in confirming the adaptability of the purpose of collecting, processing, and using personal data, the legal basis and the minimum requirements for data processing.
B. Provide suggestions for adjustments to this bylaw at any time in accordance with the requirements of relevant laws and regulations on personal information.

3.2.3.3 Personal Data Management Team：

A. Responsible for conducting Delta Group personal information protection measures：
   a. Initiate risk assessment
   b. Compile personal information related key performance evaluation results
   c. Plan personal information related education training.
   d. Assess the risk of personal information outsourcing process
   e. Prepare management review meeting materials
B. Regarding the division of labor and required resources of the organization, it may include the following information, legal affairs, etc., and the details of the personal data management related matters that should be implemented, please refer to the relevant policies and regulations of Delta Group's personal data protection.
   a. Information technology team：
      i. Manage and maintain the information systems and equipment related to the Delta Group's personal data to ensure that the Delta Group has the technical specifications required for the processing and utilization of systems and databases involved in the processing and utilization of personal data.
      ii. When collecting, retrieving, sealing and transporting personal data in digital form, coordinate relevant information systems and equipment to cooperate.
   b. Legal compliance and risk management team：
      i. Provide analysis and legal advice on the personal data protection laws and regulations that are applicable to each business unit, and provide legal advice on the collection, processing and utilization of personal data.

ii. Review the relevant provisions of the applicable personal data protection laws and complete the “Personal Data Protection Legal Compliance List”. If there is any changes in the laws and regulations, the team should adjust this bylaw and the “Personal Data Protection Legal Compliance List” with the Personal Data Protection Team.

3.2.3.4 Personal Data Internal Audit Team：

Responsible for conducting Delta Group personal information internal audit and the following up the findings and improvement plans. Please refer to chapter 4.9 of this bylaw.

3.2.3.5 Incident Response Team：

As major personal data incident occurs, incident response team shall be gathered to manage the incident response, process, internal communication related matters. Please refer to “Personal Data Incident Response Management Procedure”.

3.2.3.6 Data Protection Representatives of Each Unit：

All units shall cooperate and implement Delta Group’s related policies and procedures regarding to personal information management. Related matters include：

A. For the collection, processing, or use of personal data, the necessity, specific purpose, use method, and retention period of personal data should be confirmed in advance
B. When processing or using personal data, units shall notice that it does not exceed the scope necessary for the purpose at the time of collection, and that the purpose is legitimate and reasonable.
C. For any legal compliance issue related to the collection, processing and utilization of personal data, units shall actively consult the local legal affairs unit, relevant authority and units for their opinions.
D. If the collection, processing, and utilization of personal data involves information technology systems, databases, etc., for external use or cross-border transmission through network connections, it is necessary to first consult the local legal affairs unit, the IT office, and relevant units for opinions to ensure that it complies with relevant laws, regulations and technical requirements.

3.3 All business groups, divisions, and corporate headquarters of the Delta Group should follow the following matters to ensure the security of personal data：

3.3.1 Collect, process and use personal data within the scope of legal, specified, and reasonable purpose in reasonable way.

3.3.2 Protect the personal data collected, processed and used by using appropriate and safe technology and manners.

3.3.3 Establish a contact window to provide channels for data subjects to exercise their rights regarding personal data or submit related complaints and consultations, or arrange appropriate responses or measures according to local laws and regulations.

3.3.4 Plan emergency response procedures to deal with accidents such as theft, alteration, damage, loss or leakage of personal data.

3.3.5 When outsourcing the collection, processing and use of personal data, properly supervise the entrusted agency.

3.3.6 In order to ensure the security of personal data, units shall continue to follow the Delta Group Personal Data Protection Management Policy, the personal data operation manuals formulated by each unit in response to business and operational needs, and the local laws and regulations of each region.

3.3.7 Continuously respond to the security maintenance requirements of personal data protection, and propose improvement plans after audits. If the department holds or handles personal data, it shall follow the Delta Group Personal Data Protection Management Policy, personal information related operating procedures, laws and regulations, and international standards, and etc. Each unit should establish an appropriate personal information management plan; adopt appropriate security management measures, according to the business scope, characteristics, functions, and needs; inform employees to follow by sending out written notice, email, or other means.

3.4 The roles and responsibilities could be modified by each local organizational structures, but corresponding procedural documents should be established for confirmation. Documents should be revised regularly in accordance with the applicable personal information laws, regulations, and related policies.

4. Contents

4.1 Personal information management system mechanism

4.1.1 Management system structure establishment

Delta Group establishes personal information management system based on the framework of ISO27701 international standard.

4.1.1.1 Delta Group establishes a Personal Data Protection Promotion Team.

4.1.1.2 Issue Personal Data Management Policy in order to explain the direction, objectives, and implementation measures.

4.1.1.3 Conduct risk assessments. Collect personal information and the organization's security vulnerabilities, threats and impacts to evaluate their risk levels. After a risk assessment report is produced, follow-ups are regularly checked and tracked.

4.1.1.4 Determine the scope of implementation of risk management based on Personal Data Management Policy and the results of risk assessment.

4.1.1.5 Choose the personal data control objectives and measures that are suitable for the Delta Group to implement, and regularly review and confirm their feasibility and effectiveness.

4.1.1.6 After the personal information management system documents are issued, conduct internal audits of personal information management to confirm the effectiveness of implementation.

4.1.1.7 In order to implement personal information management and continue improving, the Delta Group shall review the above steps regularly based on findings, and make necessary adjustments and amendments. The Group shall also form preventive procedures if necessary, submit risk assessment reports and appropriate solutions, and notify the Personal Data Protection Promotion Team for review.

4.2 Personal information management system- PDCA cycle

4.2.1 Plan

Based on the strategy and objectives of the Delta Group, a personal information management system us established by forming a personal information management organization, controlling potential threats and vulnerabilities, conducting risk assessment and security control measures.

4.2.2 Do

Based on evaluation results, establish or modify the existing control measures and implement the new ones.

4.2.3 Check

Conduct regular personal information management internal audit to ensure the implementation and effectiveness of personal data management.

4.2.4 Act

Based on the results of the internal audit, implement corrective and preventive measures to improve the management system. Review relevant personnel's performances by conducting personal information management review meetings.

4.3 Risk Assessment

4.3.1 The procedures for risk assessment are as follows:

4.3.1.1 Each unit shall carry out a risk assessment at least once a year.

4.3.1.2 The risk assessment shall include the assessment of known risks and potential risks:

A. The risk assessment of known risks should include the re-evaluation of the value of personal information groups, the weight of weaknesses and the weight of threats. When considering the weight of weakness and the weight of threat, the existing management system and the current status of control should be fully considered.

B. The risk assessment of potential risks should include factors such as

potential impacts, potential weaknesses, and potential threats. Consider and quantify the level of potential risks faced by personal information as the basis for selecting control measures.

4.3.1.3 Internal and external issues and requirements of stakeholders shall be identified, and risk assessment shall be carried out. For details, please refer to the “Personal Information Management System Stakeholder List".

4.3.1.4 All weights should be entered into the risk assessment, and the results of each execution should be archived for future reference.

4.4 Acceptable Level of Risk

4.4.1 After the calculation of all of risk weights of personal information management system is completed, the results will be filled in the risk assessment report, and the Personal Data Management Team will follow the report and formulate the acceptable level of risk, and report to the Personal Data Protection Team for review.

4.5 File system requirements

4.5.1 File system architecture

The relevant documents of Delta Group's personal data management system are divided into the following items:

4.5.1.1 First-level document: policy and organization-the highest guidance for personal information management system.

4.5.1.2 Second-level documents: specification-describe the direction and process of operations in various fields of personal information management.

4.5.1.3 Third-level documents: operating methods, operation manuals-standardize the details of personal information management and standard work routines.

4.5.1.4 Fourth-level documents: forms, records, etc.-used when performing various control operations of personal information management.

4.5.1.5 Others: Personal data related documents which are not made by the Personal Data Protection Promotion Team, such as laws and regulations, international standards, etc.

4.6 Document and record management

4.6.1 Regarding to Delta Group's personal information management system document drafting, revision, approval and announcement process, and its responsible personnel, please refer to “Personal Data Document and Record Management Regulation”.

4.6.2 When there is a need to access records, please follow “Personal Data Document and Record Management Regulation”.

4.7 Resource Management

4.7.1 Provide Resources

Delta Group shall determine and provide sufficient and appropriate resources to achieve the following objectives:

4.7.1.1 Establish and maintain a personal information management system.

4.7.1.2 Establish and deploy personal information management and control mechanisms.

4.7.1.3 Confirm that the personal information management procedures can support the needs of operations.

4.7.1.4 Identify and discover regulations and related contract requirements.

4.7.1.5 Maintain an appropriate and effective control mechanism, and use relevant technical solutions for control when necessary.

4.7.1.6 Conduct regular personal information management reviews and implement an appropriate action plan.

4.7.1.7 Improve the operational process measures of personal information management as needed.

4.7.2 Organize education trainings to enhance personal data protection awareness

In the personal data management system of Delta Group, the relevant colleagues are assigned relevant responsibilities to complete the required personal data management tasks, and their capabilities can be achieved through the following methods:

4.7.2.1 Provide adequate personal information management education and training to meet the requirements.

4.7.2.2 Evaluate the effectiveness of the personal information management education trainings provided.

4.7.2.3 Confirm that the Delta Group employees have fully realized the importance of their work and personal data management related tasks, and how to achieve the requirements of personal data management goals.

4.8 Implementation of education training

4.8.1 Delta Group shall hold personal data management related education training periodically to ensure its employees' personal data management awareness.

4.8.2 Education and training can be implemented in the form of internal or external training. Internal training can be implemented by internal and external experts; external training should be implemented if needed with approval by the department head. The human resources unit of Delta Group should properly keep the training records of its employees.

4.8.3 The content and frequency of education training can be adjusted according to local regulations. Please refer to "Personnel Management, Education, and Training Regulations".

4.9 Personal Information Management System Internal Audit

4.9.1 Requirements for Internal audit

Delta Group should continue to improve the effectiveness of the personal information management system by formulating personal information management policies, establishing personal information management goals, conducting self-checking results based on personal information management, implementing corrective and preventive measures, and reviewing management. Management should ensure the implementation of regular audits, at least once a year.

4.9.2 Personal Data Internal Audit Team

4.9.2.1 Team Leader

A. Elected by the Personal Data Protection Team.
B. Convene a team meeting for Personal Data Internal Audit Team.
C. Coordinate and assign the internal audit work for the personal data management system.

4.9.2.2 Team members

A. Assigned by the senior managers of Data Protection Representatives of Each Unit
B. Draw up an internal audit plan for the personal information management system. Please refer to “Personal Information Management System Internal Audit Plan”.
C. Perfrom the internal audit
D. Track the improvement and implementation of non-conformities.

4.9.3 Procedure for Audit

4.9.3.1 By conducting internal audit operations, Delta Group expects to find problems in a timely manner, make improvements, and maintain the effectiveness of personal information management operations.

4.9.3.2 Internal audit shall be carried out at least once a year as scheduled by each unit. The execution method can be carried out by the company's internal personnel or external experts.

4.9.3.3 Preparatory Work for Personal Information Management Internal Audit

A. The leader of the Personal Data Internal Audit Team shall notify the inspected unit before the audit.
B. During the audit process, if the audit tools need to be used, the implementation method and possible risks should be discussed with the supervisor of the audit unit in advance. The consideration should include:

a. Avoid peak hours or omit unnecessary audit items.

b. During the audit process, relevant personnel should be assigned to monitor from the side to ensure that problems can be dealt with in time.

C. The designated internal auditor should fully understand the

purpose, scope, implementation method and possible risks of audit before performing the internal audit, and should fully understand the "Personal Information Management System Internal Audit Work Item List".

4.9.3.4 Implementation of the internal audit operation:

The following matters should be noted in the implementation of the internal audit operation of personal information management:

A. The internal auditor shall conduct the audit in an objective and fair manner, and shall record every inspected item and findings in the “Personal Information Management System Internal Audit Work Item List”. This form will be sent to the supervisor of the inspected unit for confirmation, and then sent to the leader of the Personal Data Internal Audit Team for review.

B. The relevant information obtained by the internal auditor during the audit shall be confidential.

C. After the Personal Data Internal Audit Team leader has completed the review, he should consolidate and complete the "Personal Information Management System Internal Audit Report” is submitted to the inspected unit for confirmation, and submitted to the chairman of the personal information protection promotion group for review.

D. The leader of the Personal Data Internal Audit Team may use the audit result as a reference for revising the personal information management internal audit items.

4.9.3.5 Please refer to the” Personal Information Management System Internal Audit Plan” for internal audit details, such as the scope of audit, qualifications of internal auditor, tracking of non-conformities and review.

4.10 Personal Information Management Review Meeting

In order to ensure the implementation of personal information management, the Personal Data Protection Team should regularly hold personal information management meetings. In addition, in order to ensure the flexibility of personal information management meetings, it can be conducted in paper form.

4.10.1 Conducting Meeting

4.10.1.1 The information management meeting shall be held once a year.

4.10.1.2 The management review meetings shall be held by the Personal Data Management Team unless otherwise specified.

4.10.1.3 When necessary, the chairman may convene an impromptu meeting.

4.10.2 Proxy system

When the chairman is unable to attend the meeting, the personal data protection convener shall act as the deputy; when the representatives of each unit are unable to attend the meeting, they should designate a proxy to attend.

4.10.3 Attendees

According to needs, internal colleagues and external experts on related topics of the meeting may be invited to attend to report or express opinions

4.10.4 Meeting minutes

4.10.4.1 The meeting minutes should be recorded, and should be reviewed after the meeting.

4.10.4.2 Meeting records should follow the confidentiality level of personal information and be properly protected.

4.10.5 Contents of personal information management meetings:

The contents of the personal information management meeting are as follows:

4.10.5.1 Evaluation of the personal information management system.

4.10.5.2 Carry out the development and review of personal information management policies, provide the resources required for personal information management system, and integrate the objectives of personal information management into related processes to ensure the implementation of the personal information management system.

4.10.5.3 Assess the requirements and integrity of the personal information management system.

4.10.5.4 In accordance with various internal and external requirements, laws and regulations, evaluate the applicable scope, legality and integrity of the implementation of the personal information management system, and determine whether adjustments and amendments are needed. Review the risk assessment methods and risk assessment results reported by the personal information management execution group, and review the control measures selected and the acceptable risk level based on the risk assessment results.

4.10.6 Personal data incident report

Report personal data incidents and its status, and review necessary improvement or punishment measures.

4.10.7 Assignment of responsibilities

Regarding to various personal information management needs, assign authorized personnel to work, and evaluate the suitability of the authorized personnel by viewing the results of the assignment.

4.10.7.1 According to ISO 27701, the following issues will be reviewed at management review meetings:

A. The status of previous meeting proposals.
B. Changes in internal and external issues related to the personal information management system
C. Feedback on personal information management performance.
D. Non-conformities and corrective measures.
E. Supervisory and measurement results.
F. Audit results.

G. Achievement of personal information management objectives.
H. Feedback from interested parties.
I. The results of the risk assessment and the status of the risk mitigation plan.
J. Opportunities for continuous improvement.

4.10.8 According to ISO 27701, the following decisions or actions should be made:

4.10.8.1 Decisions related to opportunities for continuous improvement of the personal information management system.

4.10.8.2 The needed changes of the personal information management system.

4.10.9 Special subject report

Invite internal colleagues, external experts, or stakeholder groups (such as criminal investigation and prevention units, supervision agencies, and etc.) to report or make suggestions on personal information management issues for the reference of the Personal Data Protection Promotion Team.

4.11 Purpose of the management review of the personal information management system:

Ensure the applicability, completeness and effectiveness of the continuous operation of the personal data management system.

4.11.1 Review input

The review content of the management review meeting should include the following items:

4.11.1.1 Follow-up measures for previous management reviews.

4.11.1.2 Changes to internal and external issues related to the personal data management system.

4.11.1.3 The expectations and feedback of stakeholders in the personal information management system.

4.11.2 The performance feedback of the personal information management system includes the following trends:

4.11.2.1 Non-conformities and corrective measures.

4.11.2.2 Supervision and measurement results.

4.11.2.3 Audit results.

4.11.2.4 Opportunities for continuous improvement.

4.11.2.5 Risk of personnel identification and upgrade.

4.11.2.6 Records of procedural review.

4.11.2.7 Technologies, products or procedures that can be used to improve the performance and effectiveness of the organization's personal information management system.

4.11.2.8 Requirements after formal assessment by the competent authority.

4.11.2.9 Handling of complaints.

4.11.2.10 Personal data incidents that have occurred.

4.11.3 Review output

The following items should be recorded and proposed after the management review meeting.

4.11.3.1 Resolution to improve the effectiveness of the personal information management system.

4.11.3.2 Updated risk assessment and improvement plan content.

4.11.4 In response to internal or external events that may affect the personal data management system, the operation methods that affect the system should be revised when necessary, which may include the following changes:

4.11.4.1 Operational requirements.

4.11.4.2 Security requirements.

4.11.4.3 Processes that will affect existing operational requirements.

4.11.4.4 Management or regulatory environment.

4.11.4.5 Contract obligations.

4.11.4.6 Risk level or acceptable risk level.

4.11.4.7 Determine the method and scope of resource requirements.

4.11.4.8 Confirm that relevant controls have been effectively implemented.

4.12 Continuous improvement of personal data management system

4.12.1 Continuous improvement

The Delta Group continuously improves the effectiveness of the personal data management system by reviewing personal information management policies and objectives, internal and external personal information management audit results, incident tracking correction and preventive measures, and management review and other operations; monitoring risks or non-conformities by responsible personnel and tracking the improvements. Relevant corrective and preventive measures should be combined with risk assessment and brought into control, please refer to "Corrective and Preventive Measure Form".

4.12.2 Corrective measures

The Delta Group should take appropriate control measures to reduce non-conformities arising from the establishment, operation and use of the personal data management system, and to prevent accidents from recurring. The corrective action procedures are:

4.12.2.1 The internal auditor for the personal data management system assists each relevant business unit to identify the non-conformities in personal data management system, whether it is a develop, design, or operational factor, and confirm the reasons for the non-conformities.

4.12.2.2 Each relevant business unit evaluates the necessary corrective measures to prevent the non-conformity from happening.

4.12.2.3 The internal auditor for the personal data management system assists each relevant business unit to determine and establish necessary corrective measures.

4.12.2.4 Each business unit should record the implementation results of the corrective measures.

4.12.2.5 The internal auditor for the personal data management system should review the results of the implementation of the corrective measures.

4.12.3 Preventive measures

The Delta Group shall take appropriate control measures to prevent and reduce the chances of potential non-conformities. Preventive measures shall be able to prevent the possible impact of potential problems. The procedures for preventive measures are:

4.12.3.1 Relevant business units should be able to identify potential non-conformities and the reasons of them.

4.12.3.2 Relevant business units decide and confirm the necessary preventive measures.

4.12.3.3 Relevant business units should record the results of the implementation of preventive measures.

4.12.3.4 The internal auditor for the personal data management system should review the results of the implementation of preventive measures.

4.12.3.5 The internal auditor for the personal data management system should identify the risk of changes and beware of the risk due to major changes.

5. **Announcement and Implementation**

5.1 If necessary to make or amend this bylaws, the Personal Data Protection Team should draw up the draft, and it will take effect after the chairman's approval.

5.2 If any local applicable laws for Delta Group's regional offices and this bylaws are inconsistent, relevant documents shall be drawn up separately to ensure compliance with local laws and regulations.

6. **Reference Documents:**

6.1 Personal Data Incident Response Management Procedure

6.2 Personal Data Document and Record Management Regulation

6.3 Personnel Management, Education, and Training Regulations

7. **Attachments:**

7.1 Personal Data Protection Promotion Team Organization List (PIMS-ENG-04-04-001)

7.2 Personal Information Management System Stakeholder List (PIMS-ENG-04-04-002)

7.3 Corrective and Preventive Measure Form (PIMS-ENG-04-04-003)

7.4 Personal Information Management System Internal Audit Plan (PIMS-ENG-04-04-004)

7.5 Personal Information Management System Internal Audit Work Item List (PIMS-ENG-04-04-005)

7.6 Personal Information Management System Internal Audit Report (PIMS-ENG-04-04-006)

7.7 Personal Data Protection Legal Compliance List (PIMS-ENG-04-04-007)