台達集團
DELTA GROUP

Document Name:	Personal Data Incident Response Management Procedure
Document No.:	PIMS-ENG-02-03-002
Version:	01 (Approved by the Chairman of Personal Data Protection Team on June 23, 2021) 02 (Approved by the Chairman of Personal Data Protection Team on Jan. 1, 2022)

Table of Contents

1. Purpose 3
2. Scope 3
3. Rights and Responsibilities 3
4. Definition 5
5. Operating Procedures and Instruction 5
6. Announcement and Implementation 11
7. Reference Documents: 11
8. Attachments: 11

1. Purpose

In order to establish response procedures and measures for personal data incidents, and to control the risks and possible damages caused by the incident to the parties, Delta Group has specially formulated the "Personal data Incident Response Management Procedure" (hereinafter referred to as "this procedure"), to follow.

2. Scope

The scope of application of this procedure includes preparation for personal data incidents (hereinafter referred to as "the incident"), emergency management and follow-up improvement operations during and after the incident.

3. Rights and Responsibilities

3.1. The Personal Data Protection Team should set up a Personal Data Management Team responsible for the following affairs:

3.1.1. When a personal data incident occurs, receive the information of the incident and make decisions, and supervise the implementation of this procedure.

3.1.2. According to the severity of the incident, decide alongside with Personal Data Protection Team whether to activate the Incident Response Team.

3.1.3. Coordinate and designate the person responsible for contacting data subjects (customers, employees, suppliers, etc.).

3.1.4. Coordinate and designate the person responsible for contacting the media.

3.1.5. Coordinate with Delta Group's Personal Data Protection Team members to jointly formulate a strategy and responses for personal data incidents, and revise the plan as appropriate.

3.1.6. Be the main contact for relevant government authority of Delta Group, and provide necessary information according to the instructions of the authority.

3.1.7. If a personal data incident is also applicable to personal information protection laws of other countries, it is necessary to assist in reporting to the local government authority or/and relevant parties in accordance with relevant local regulations.

3.2. The personal data protection promotion team shall set up an information technology group to be responsible for the following affairs:

3.2.1. Ensure and maintain the information equipment related to the personal information of

Delta Group to avoid the occurrence of personal information protection loopholes.

3.2.2. Coordinate related information equipment to cooperate with each other in the identification, collection, retrieval, sealing and transportation of digital evidence.

3.2.3. Coordinate with the members of the emergency response team and the unit where the incident occurred to assist personnel with digital evidence preservation.

3.2.4. Handle or assist in preventive or response measures for personal data incidents undertaken by Delta Group.

3.3. The Personal Data Protection Team shall set up a legal compliance risk management group, responsible for the following matters:

3.3.1. Provide applicable analysis and legal advice of the laws and regulations related to the protection of personal data to which Delta Group should apply, and adjust this procedure in accordance with the requirements of the laws and regulations.

3.3.2. Continue to pay attention to external information or news related to violations and penalties of personal information.

3.3.3. Review the applicable personal information protection laws and regulations every six months, and confirm the requirements of the relevant government authority for contact, consultation, registration or violation notification channels.

3.3.4. Provide legal opinions on handling personal data incidents.

3.3.5. Assist in handling compensation matters for personal data incidents.

3.3.6. Discuss what needs to be notified to the government authority and parties involved.

3.3.7. Consult or confirm with relevant external units whether the associated procedures should be initiated.

3.4. Data Protection Representative / Contact Persons of Each Unit:

3.4.1. Each unit shall appoint a personal data representative /contact person to be the contact between the unit and the Personal Data Protection Team.

3.4.2. Supervise each unit, implement personal information management and respond to personal data incidents.

3.4.3. Participate the meeting held by Personal Data Protection Team to track and report on the personal data protection related tracking items of each unit. For the flexibility of meetings, tracking items and contents for meetings can be proposed or presented in written forms.

3.4.4. When a personal data incident occurs, the data protection representative/contact person of the responsible unit for the incident should decide the communication means along with the designated contact window for clients.

3.4.5. The responsibilities above may vary differently for branches abroad due to different organizational structures. However, appropriate procedures should be established for confirmation and revised in accordance with the requirements of this procedure.

4. Definition

4.1. Personal data incident: refers to any permanent or temporary incident, tampering, damage or loss of personal information, or unauthorized access or disclosure caused by Delta Group or outsourced third-parties while transmitting, storing or processing personal data.

4.2. Stakeholders: refer to people or groups involved in activities such as the collection, processing or utilization of personal data, including but not limited to parties, employees, manufacturers, competent authorities of Delta Group, mass media, etc.

4.3. All personnel: all Delta Group employees, contracted personnel, manpower dispatch or partners (customers, third parties, consultants, etc.) working with the Delta Group.

4.4. Contact Person for customers: refers to the external contact person designated by the Personal Data Protection Team when a personal data incident occurs or may affect the rights and interests of customers.

5. Operating Procedures and Instruction

5.1. General

5.1.1. Delta Group shall conduct personal data incident drills at least once a year.

5.1.2. All personnel of the Delta Group shall protect the security of personal data, and overseas locations shall take necessary measures in accordance with overseas local laws and regulations.

5.1.3. When the Delta Group’s suppliers or third-party organizations are involved in the collection, processing, or use of personal data, the personal data management and control measures shall be in accordance with Delta Group’s "Personal Data Outsourced Processing Procedures" (PIMS-ENG-02-07-001) in addition to handling, and shall follow the provisions of the personal data protection laws and regulations.

5.2. Operational Matters When a Personal Data Incident Occurs

The handling process when a personal data incident occurs includes: incident discovery phase, incident notification and response handling phase, and review operations.

5.2.1. Incident discovery stage: When the following situations occur, the personal data incident response procedure should be initiated immediately.

5.2.1.1. According to the internal report of Delta Group, it is possible that the personal data of customers, employees, etc. have been infringed;

5.2.1.2. Received a notification from an outsourcing vendor of a personal data incident;

5.2.1.3. Received notification from the party that the personal data has been infringed, and there is a clear sign of the infringement;

5.2.1.4. Received a media report or an incident is reported by the media;

5.2.1.5. Received a notification from a consumer protection agency that there is an incident;

5.2.1.6. Received a notification from the government agency, law enforcement agencies, or other government agencies that there is an incident;

5.2.1.7. The paper, digital data or computer equipment of Delta Group's personal data is stolen or lost;

5.2.1.8. Any party or client claim to reveal an information incident or has filed a lawsuit;

5.2.1.9. There are other specific evidence, and the unit supervisor judges that there is a possibility of a personal data incident.

5.2.2. Incident Notification and Response and Handling Stages

5.2.2.1. The handling of all personal data incidents shall follow the following matters:

A. When personnel of each unit discover that a personal data incident has occurred, they should notify the manager and data protection representative of the incident unit according to the “Personal Data Incident Handling Process” (PIMS-ENG-03-03-001), and fill in the "Personal Data Incident Record and Notification Form" (PIMS-ENG-04-03-001) for notification. After receiving the notification, the Personal Data Management Team should decide whether to activate the Incident Response Team, make public statements, and decide which level of manager should be notified, based on the severity of the incident. Personal Data Protection Team should complete the preliminary investigation of the incident, assess the impact, and be responsible for follow-ups.

B. If the personal data incident involves information technology technical related

matters, the information technology team should coordinate and review the abnormal state of the internal technological environment (such as network equipment, server status, terminal status, etc.), and seek external support (such as digital forensics).

C. When the unit contact person or outsourced manufacturer handles the personal data incident, the process and results should be reported to the manager or data protection representative of the relevant business unit continuously. The manager or representative shall be responsible for reporting the incident status to the Personal Data Protection team or/and the Incident Response team.

D. The unit that causes the incident should find out the cause of the incident, confirm the scope of influence with related units, and complete the preliminary incident analysis as soon as possible.

E. If the personal data incident applies to the personal information protection laws of other countries, the relevant unit shall notify the local government authority or/and the relevant parties in accordance with the relevant local regulations.

5.2.3. Review work

5.2.3.1. After handling the severe personal data incident, the Personal Data Protection Team shall convene an incident review meeting. Related personnel and units should cooperate and participate in the meeting. The content of the meeting shall include the following:

A. Explain the whole incident

B. Review of the responsiveness of relevant personnel involved in the process of personal data incidents

C. Make suggestions and plans on how to prevent the incident from recurring

D. If additional tools or resources are needed, please propose at the meeting

E. According to the conclusions of the meeting, if there is a need to modify this procedure, a revision of this procedure should be proposed.

5.3. Incident Response Team

When a personal data incident occurs and the circumstances are serious, the Incident Response Team should be activated. Its organization and responsibilities are as follows:

5.3.1. Organization: The Incident Response Team is composed of members of the Personal Data Protection Team and related personnel for the handling of personal data incidents.

The convener of the Incident Response team is selected by the convener after a resolution, and will work and lead the incident response operations and other matters jointly with the contact person of the unit where the incident occurs.

5.3.2. Responsibilities:

5.3.2.1. After the responsible unit provides a complete record of the incident occurrence, organize, summarize the incident and report to the Personal Data Management Team, and report to the highest level according to the personal information incident notification level standard, referring to "Personal Data Incident Level and Notification Level" (PIMS-ENG-03-03-002) .

5.3.2.2. Investigate the cause and authenticity of the incident, and take necessary measures to prevent the incident from expanding, controlling or reducing damage.

5.3.2.3. The unit responsible for the incident shall put forward suggestions and improvement measures to internal and external stakeholders, and provide contact methods such as telephone number and email that can handle personal data incident inquiries.

5.3.2.4. Investigate the quantity and scope of data related to personal data incidents, and evaluate the degree of damage.

5.3.2.5. The incident response team confirms that the incident has been properly handled, and the case can be closed after reporting to the highest level manager.

5.4. Classification and notification of personal data incidents

The Personal Data Management Team should determine the level of the incident based on the scope and impact of the personal data incident, referring to the "Personal Data Incident Level and Notification Level" (PIMS-ENG-03-03-002) . Assess whether it should be notified to senior supervisors, competent authorities, or data subjects.

5.5. Key Points of Handling Personal Incidents

5.5.1. Direct, decide and designate the handling of incidents (Chairman of the Personal Data Protection team)

5.5.1.1. Approve necessary responses to control the impact of the incident.

5.5.1.2. Publish the external written statement and the internal staff description.

5.5.1.3. Designate the speaker as the only external spokesperson.

5.5.2. Incident handling, review and improvement (Responsible Unit/ the Personal Data

Protection Team /Incident Response Team)

5.5.2.1. It is necessary to fully record the process of an information incident, such as the cause, time, location, related personnel, quantity and scope of the incident or impact, and the estimated degree of damage, and report to the chairman.

5.5.2.2. Participate in the incident review meeting, provide a complete record of the incident process, and make suggestions and improvement measures in response to internal and external stakeholders.

5.5.2.3. Relevant personnel should be assigned to confirm whether there is a risk of another incident.

5.5.2.4. If it is found that the incident involves a third-party violation of laws, regulations and requirements, it can be reported to the police for assistance if necessary.

5.5.3. Coordination and Communication between the Parties (request and appeal handling team)

5.5.3.1. Continuously monitor the flow of incident-related information and report internal information received.

5.5.3.2. The parties shall be notified in accordance with the law to explain the progress of the incident and the impact on the rights and interests of the parties, and to ensure that the parties understand the handling status of the Delta Group and the protection of their rights and interests.

5.5.3.3. Questions and answers (Q&A) and consultation channels should be established for handling personal data incidents, so as to adopt a unified and convenient channel to help the parties understand the handling of personal data incidents.

5.5.3.4. After the incident occurs, the parties should be notified individually, including the fact that their personal data has been infringed, the corresponding measures taken by Delta Group, the contact information of Delta Group's contact person, the possible impact of the incident, and the expected actions taken by Delta Group.

5.5.3.5. The method of notification related to personal data incidents refers to the immediate implementation of words, writing, telephone, text message, email, fax, electronic document or other methods sufficient to make the parties aware of the incident.

5.5.3.6. If an individual notification is too expensive, the scope of the notification is too large, or individual parties cannot be notified, the announcement can be made

through the internet, news media or other methods that are sufficient for the public to get notified. A summary of the occurrence of a personal data incident, and a toll-free number shall be set up when necessary, so that the parties involved can quickly know about the incident and its handling status.

5.5.3.7. When notifying data subjects about the incident, relevant records, including the notification method, time, object, execution unit, and notification content, should be recorded.

5.5.4. Notify the relevant government authority (personal data protection promotion team/emergency response team are responsible for it)

5.5.4.1. After receiving a notification that a personal data incident has occurred, notify the relevant government authority about the scope and details of the incident within the statutory time limit to avoid expansion of the damage.

5.5.4.2. After the incident, there should be procedures drawn up to prevent similar incidents from recurring. A proper follow-up plan should be done.

5.5.4.3. The notification to the relevant government authority shall include the facts and possible outcome of the incident, types and quantity of data involved, appropriate contingency plans that reduce negative effects, and preventive measures to avoid recurrence of similar accidents.

5.5.4.4. When notifying the government authority about the incident, relevant records, including the notification method, time, object, execution unit, and notification content, should be recorded.

5.5.5. Media responses (According to the [Personal Data Incident Level and Notification Level] the highest level manager or other designated person who should be notified)

5.5.5.1. Continuously monitor whether the incident escalates and cause media attention, and report any external information immediately.

5.5.5.2. If the media reports on the incident, various control measures for personal information management should be reported, including how the incident happened and current processing status, and make a unified announcement externally or internally through the spokesperson.

5.5.5.3. The emergency response team or/and the personal data protection promotion

team shall prepare press release once the incident happened, and be ready to release it to the public anytime.

6. Announcement and Implementation

6.1. If necessary to make or amend this bylaw, the personal information protection team should draw up the draft, and it will take effect after the chairman's approval.

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

7. Reference Documents

7.1. “Personal Data Outsourced Processing Procedures”(PIMS-ENG-02-07-001)

8. Attachments

8.1 “Personal Data Incident Handling Process” (PIMS-ENG-03-03-001)

8.2 “Personal Data Incident Record and Notification Form” (PIMS-ENG-04-03-001)

8.3 “Personal Data Incident Level and Notification Level” (PIMS-ENG-03-03-002)