



台達集團
DELTA Group

Document Name: Personal Data Collection, Processing and Utilization Management Procedure

Document No.: PIMS-ENG-02-01-002

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 June 20, 2022)
003 (Approved by the Chairman of Personal Data Protection Team on July 21, 2022)
004 (Approved by the Chairman of Personal Data Protection Team on October 08, 2022)

Table of Contents

1. Purpose	3
2. Scope	3
3. Responsibility	3
4. Definition	3
5. Personal Data Protection Policy	4
6. Rights of Data subjects	14
7. Awareness Promotion and Education Training	14
8. Audit System	14
9. References	14
10. Announcement and Implementation	15
11. Attachments	15

Delta Electronics, Inc.
Internal Use

1. Purpose

- 1.1 In order to ensure the processing and use of personal data meets the scope of specific purposes, Delta Group has formed the “Personal Data Collection, Processing and Utilization Management Procedure” (hereinafter referred to as “this procedure”); and furthermore, regulates and guides the company to ensure the data subjects’ rights are respected.

2. Scope

- 2.1 Please refer to “Delta Group Personal Data Protection Management Policy” (hereinafter referred to as “the Policy”) for the scope of this procedure.

3. Responsibility

- 3.1 All collection, processing and utilization of personal data of Delta Group should follow this procedure; however, each department could form their own operation manual for collecting, processing, and utilizing personal data without violating this procedure.
- 3.2 The “Personal Data Protection Team” set up by Delta Group is the ultimate authority and responsibility unit for personal data-related incidents and management operations. For related organizational structure and assignment of duties, please refer to the “Personal Data Protection System and Organization Bylaws”.

4. Definition

Except as otherwise agreed in this article, please refer the definitions of terms to personal data protection laws and local regulations, which will also change when the laws are revised:

- 4.1 Personal Data (PII, Personal Identifiable Information): refers to any information that can directly or indirectly identify an individual, and can be divided into three categories as below based on the risk level

4.1.1 Normal Personal Data

4.1.2 High-risk Personal Data :

- 4.1.2.1 Information that can directly identify an individual, e.g. ID number, Passport number, Bank account or Credit card number.

- 4.1.2.2 The combination of name plus any two or more of the following items: contact information (e.g. phone number, address and email), date of birth, family, policy number or claim number, other financial situation (salary, balance, debt or limit), , account or email address compound password or answers to security questions that can login to a system data.

- 4.1.3 Special Personal Data : please refer the definitions of terms to personal data protection laws and local regulations. For instance, medical history, medical treatment, genetics, sex life, health check, and criminal history are special personal data defined in Taiwan's Personal Data Protection Act.
- 4.2 Indirect collection: The collection of personal data not directly provided by the data subjects
- 4.3 Automated decision-making: Decisions made by technical methods that do not involve human operations.
- 4.4 Specific purpose: Except for the exemplified provisions of the "Specific Purposes of the Personal Data Protection Law and Categories of Personal Data" announced by the Ministry of Legal Affairs, other purpose that may be applicable to Delta's collection, processing, and use of personal data.
- 4.5 Similar contract: The act of contact or negotiation with the data subjects before the formulation of the contract for the purpose of preparing or negotiating a contract or for the purpose of a transaction.
- 4.6 The exclusion principle of personal data inventory: Personal data collected by Delta with lower risk can apply to the exclusion principle of personal data inventory. However, the excluded personal data still needs be properly protected and controlled.
- 4.7 Temporary file: refers to temporarily needed files or automatically generated system logs that occur while processing personal data,

5. Personal Data Protection Policy

5.1 Collection

5.1.1 Personal data collection for each department of Delta Group could be done only when it has a specific purpose and meets one of the following conditions:

5.1.1.1 The law clearly regulates: personal data must be collected in accordance with the law or under the supervision of relevant government authority.

5.1.1.2 The department has a contract or similar contractual relationship with the data subjects, and has adopted appropriate security measures: The data subjects have contractual relationship with Delta Group, and processing personal data is necessary for the execution of the contract; or having similar contractual relationship before signing the contract for the purpose of negotiation and preparation; or the request of the data subjects for collecting personal data before signing the contract.

5.1.1.3 The personal data disclosed by the data subjects themselves or other legally disclosed personal data: the data subjects disclosed personal data to specific or

non-specific people; personal data been publicized, announced, or disclosed in other lawful ways in accordance with the law or a statutory order specifically authorized by the law.

- 5.1.1.4 With the consent of the data subjects: after the data subjects have been notified the statutory matters Delta Group, the data subjects express their permission based on their free will by declarations or other explicit actions, indicates they allow Delta Group to process personal data of the data subjects for one or more purposes.
- 5.1.1.5 Necessary for the promotion of public interests: Processing necessary personal data for unspecified public interests or statutory public interests; necessary processing of personal data due to receiving clear instructions or entrust by an official agency.
- 5.1.1.6 Personal data is obtained from generally available sources: e.g. through mass media, internet, news, magazines, government bulletins, and other channels through which ordinary people can learn or contact to obtain personal data. However, if the restriction of processing or utilizing personal data by the data subjects has greater interests/worth, this provision will not be applied.
- 5.1.1.7 Legal interests: Under the premise of not infringing data subject's benefits, collecting personal data for the benefit of Delta Group or a third party. However, if it is obvious that the interests or basic rights of the data subjects should take precedence over the interest of Delta Group, the legal interests shall not be used as the basis for collecting personal data. The legal interests of Delta Group may include: avoiding fraud, ensuring network security, or benefiting the rights of the data subjects, etc.

All the legal foundations mentioned above are equally effective, and no single legal basis should be considered superior to other legal foundations. Only when none of the legal foundations mentioned above can be used, the consent of the data subjects can be used as the legal basis.

5.1.2 When collecting personal data with accordance to legal interests, Delta Group should take consideration of the overall situation for processing personal data into evaluation, include but not limited by:

- 5.1.2.1 Who will benefit from personal data processing
- 5.1.2.2 The data subjects' predictability of processing
- 5.1.2.3 Relationship between the data subjects and Delta Group
- 5.1.2.4 The relative negotiation status between the data subjects and Delta Group
- 5.1.2.5 Impact of personal data processing to the data subjects
- 5.1.2.6 Whether the data subjects are in a disadvantaged position
- 5.1.2.7 Possibilities of the data subjects deny personal data processing
- 5.1.2.8 The ability of Delta to cease processing data at any time when the data subjects requested

5.1.3 Each department should keep related records of personal data collecting by permission with accordance to law. If data subjects accepted personal data collection in written form, permission needs to obtain from the data subjects. Examples are as follows:

5.1.3.1 The data subject provides a written statement or fills in Delta Group personal data collection, processing or use consent form (please refer to Annex 1 for a general consent form template. If each unit needs to modify or add to the content of the consent form, it can contact the legal department to modify it).

5.1.3.2 The data subjects send an email confirmation.

5.1.3.3 The data subjects themselves provides consent documents; or

5.1.3.4 If the personal data of the data subjects is collected by means of an information system, and the design of the information system can meet the identity verification, consent, record and other statutory requirements necessary for the various operations of this operating procedure, the personal data of the data subjects can be collected by an information system.

5.1.4 Requirements for the data subjects' consent:

5.1.4.1 After notifying necessary items for collecting, processing or using personal data, Delta Group should obtain acceptance from the data subjects. It should contain characteristics below. Include but not limited by:

- A. Explain the consent items to data subjects in clear and simple language, and should not confuse the explanation with other matters; and should not use "Agree to Provide Personal Data" as the user clause or mention before the contract becomes effective.
- B. Items requires the data subjects' consent should list out concrete possible methods and purposes for personal data processing, and obtain acceptance from the data subjects.
- C. The data subjects have complete control over whether to accept the processing of their personal data, and have rights to deny without causing damage.
- D. The data subjects must be provided with sufficient information to process the relevant personal data. Simple silence, inaction, or no objection does not constitute valid consent.

5.1.4.2 Delta Group should provide that the data subjects can withdraw their consent in a simple, effective and executable way at any time.

5.1.4.3 Previous legality of personal data processing and the service obtained from Delta Group will not be affected after the data subjects withdraw the consent of collection, processing, and utilization of personal data.

5.1.4.4 If the data subject is a minor, the consent of the minor will be legal only after Delta Group obtains the written consent of the legal representative of the minor. Delta Group should make reasonable efforts to confirm that the legal representative has agreed to provide the minor's personal data; if the data subject is an auxiliary

declared person, Delta Group should also obtain the written consent of the person's guardian or auxiliary person to declare legality of using data subject's data. Delta Group should make reasonable efforts to confirm that the guardian or auxiliary person has agreed to the guardian or auxiliary declared person to provide personal data.

- 5.1.4.5 If a third party is entrusted to collect personal data, when Delta Group continues to process or use it, it may require the third party to perform the obligation of notification, and set the request in the cooperation contract or other legally binding document.
- 5.1.5 If the specific purpose of each department for collecting personal data is not specified in the relevant personal data protection laws or the categories of personal data, other specific purposes should be specified in details in written form.
- 5.1.6 If each department collects personal data due to business needs, it should be determined in accordance with the authority of the department. If the approval authority is not agreed, it should be approved by the top executive of the department in writing or other means, and the evidence approved according to the approval authority should be preserved to provide relevant authority and responsibility unit for checking.
- 5.1.7 When each department needs to collect special personal data due to business needs, the following items should be checked, and related authorities and responsible units will ensure the collection procedure is legal. The method and content of personal data collection must be in accordance with the applicable laws and regulations of Delta Group for respecting the rights and interest of the data subjects. Honest and credible manner will be honored; data collection must not exceed the scope of the legal and specific purpose; legitimate and reasonable connection with the purpose of the collection will be kept; the principle of minimizing access to data will be performed.
 - 5.1.7.1 Category of personal data and the specific purpose of collection.
 - 5.1.7.2 Personal data processing and utilization means.
 - 5.1.7.3 Direct or indirect collect personal data, notification method and content to the data subjects.
 - 5.1.7.4 Cross-border transfer of personal data
- 5.1.8 The personal data contact window of each department should input all collected personal data items and contents in the personal data inventory, and keep them after approval of the department's authorities. Only those that meet the definition in the personal data inventory exclusion list are exempt from inputting. The aforementioned personal data inventory should be regularly maintained, compiled and updated, and provided to the relevant authority and responsibility unit for checking. (For sample of the personal data inventory, please refer to Annex 2; for the personal data inventory exclusion list, please refer to Annex 3).
- 5.1.9 Notification procedure of personal data collection

5.1.9.1 When collecting personal data provided directly by data subjects, each department of Delta Group should clearly notify the items below to the data subjects and save relevant notification records:

- A. Delta Group's name;
- B. Purpose of collections;
- C. Category of personal data;
- D. Duration, region, object and method for utilization of personal data;
- E. The data subjects may exercise their rights of inquiries, request viewing or copies, supplements or modifications, request for stop of collection, processing or use, and request for deletion of their personal data;
- F. The data subjects' rights and interests that will be affected if they elect not to provide personal data;
- G. Personal data retention period;
- H. However, the obligation to inform may be waived under any of the following circumstances:
 - a. where notification may be waived in accordance with the law;
 - b. Where the collection of personal data is necessary for Delta Group to fulfill its legal obligations
 - c. where giving notice will prevent the government agency from performing its statutory duties;
 - d. where giving notice will harm public interests;
 - e. where the data subject has already known the content of the notification; or
 - f. where the collection of personal data is for non-profit purposes and clearly has no adverse effect on the data subject.

5.1.9.2 When collecting personal data provided indirectly by data subjects, each department of Delta Group should clearly notify the items below to the data subjects, and save relevant records before processing or utilization (or during the first use of data subjects' data):

- A. Company name;
- B. Purpose of collection;
- C. Category of personal data;
- D. Duration, region, object and method for utilization of personal data;

E. The data subjects may exercise their rights and methods of inquiries, request reading or copies, supplements or modifications, request for cessation of collection, processing or use, and request for deletion of their personal data;

F. Personal data retention period;

G. However, circumstances that fit in item H of Clause 5.1.9.1, should be exempted from the notification.

5.1.9.3 If each department has doubts about whether the collection of personal data is an exemption from notification, it should actively consult the relevant authority and responsibility unit to confirm whether it is an exception to the notification. Only for the purpose to avoid disputes with the data subjects, the departments should still inform the data subjects as much as possible.

5.1.9.4 The method of notification may be one of the following methods, but if the laws and regulations state otherwise, it should be implemented in the prescribed method:

A. In writing: before or at least during the time of personal data collection, inform data subjects in written form individually;

B. Phone: After the call is connected, the notification recording will be played, or it will be notified to the data subject by the Delta employee during the phone call, and it will be recorded;

C. Email or fax: After first receiving the personal data of the data subject, reply to the email or fax provided by the data subject, or place the text or link of the notification in the appropriate place under the text of the email or fax.

D. Other electronic methods: according to personal data collection channels, provide notification statement text or link.

E. APP: In the app store and the app itself, notify the data subjects by putting notification at obvious and visible function areas.

F. Webpage: Display the notifications in a way that cannot be skipped. Before collecting personal data of the data subjects, place "Delta Group Private Policy" on the webpage where it is obvious.

G. Other appropriate and record-keeping notification methods.

5.2 Processing

5.2.1 Delta could only process and use personal data files within the scope of specific purposes. The head of each department or the authorized person should review whether the personal data processed meets the purpose, specific circumstances and necessary limits.

5.2.2 In order to create or use personal data files, Delta Group should establish relevant mechanisms for the recording, input, access, editing, updating, coping, retrieval, sharing, transmission, linking, and internal transmission of personal data:

5.2.2.1 Regulations for the scope and authorization of the people who may contact for or process personal data.

5.2.2.2 Control mechanism of personal data risk level and classification.

5.2.2.3 Control and record mechanism of personal data processing behavior.

5.2.3 Each departments processing or using personal data should make written records of their processing methods and safety measures, and keep the records safely and appropriately. In order to maintain the correctness of personal data, each department should check and confirm when recording, inputting, editing, correcting, and transmitting personal data, and keep the record of the acceptance window and changes.

5.2.4 If due to changes in circumstances, the selected legal basis for the processing of specific personal data is no longer appropriate, Delta Group should communicate with the data subjects and obtain a new legal basis for further personal data processing.

5.2.5 If the original specific purpose changes over time, or Delta Group has a new purpose that was not originally anticipated, as long as the new purpose of Delta Group is compatible with the original purpose, Delta Group does not need a new legal basis. If there is a new legal purpose, Delta Group should state the new purpose in the consent form, and the data subjects should agree separately. To assess whether the purposes are compatible, the following general rules must be considered: whether the new purpose is significantly different from the original purpose, whether it is beyond the expectations of the data subjects or unreasonably affects the interests of the data subjects.

5.2.6 If Delta Group uses automated machine learning, artificial intelligence, big data analysis, and related means to process personal data, priority should be given to reducing the identification of personal data, and it must have a mechanism for manual intervention.

5.2.7 Delta Group can only process the personal data of Delta Group employees under the following circumstances, and appropriate protection will be carried out according to the degree of data risk:

5.2.7.1 Exercising rights and performing duties within the necessary scope, and complying with relevant personal data regulation;

5.2.7.2 Within the necessary scope, perform contract or other contracts signed between Delta Group employees, shareholders or directors; or when Delta employees, shareholders or directors request, execute the measures implemented before the signing of the contract.

5.2.7.3 Based on legitimate interests of Delta.

- 5.2.7.4 Obtain written agreement from the data subjects beforehand.
- 5.2.8 Delta Group can only process personal data for job applicants under the following circumstances, and appropriately protect it according to the degree of data risk:
- 5.2.8.1 Before the employment relationship or similar employment relationship occurs, the personal data of job applicants should only be collected and processed by Delta Group employees who need to know, and should only be used to confirm whether the job applicant is suitable for the relevant position.
- 5.2.8.2 Personal data provided by job applicants, who is not employed, should be returned or destroyed immediately if without other legal basis of retention.
- 5.2.8.3 Subject to the prior written consent of the job applicant, in order to facilitate contact with the job applicant for a suitable new job vacancy, the personal data may be retained until the specific purpose of personal data collection disappears or the retention period expires.
- 5.2.9 The monitoring measures of Delta workplace are as follows:
- 5.2.9.1 The camera surveillance system used by Delta Group in the workplace should not be installed in places that may cause excessive interference to the privacy of the data subjects.
- 5.2.9.2 The purpose of the camera surveillance system is to protect employees and Delta Group property from illegal acts, so the legal basis for personal data processing lies in the legitimate interests of employees and Delta.
- 5.2.9.3 The retention period of the camera recordings of Delta Group should depend on the investigation of crimes or violations and the transfer of relevant records to law enforcement agencies. After the retention period expires, Delta Group should delete the recordings.
- 5.2.9.4 The CCTV recordings should have access and management measures, and should only be transferred to the data subjects, agencies or internal units conducting investigations according to law or internal needs. The rights of the data subjects should not be impaired when processing the CCTV recordings.
- 5.2.10 Destruction and deletion of personal data.
- 5.2.10.1 Each department should regularly review the validity and availability of personal data, and delete or destroy unnecessary personal data. The temporary archive of personal data due to business needs should also apply. The temporary archive personal data should, in principle, be deleted or destroyed immediately after the processing is completed, or retained at most half a year due to business needs. Personal data for which there is no specific retention period for deletion or destruction should, in principle, be deleted or destroyed within half a year after the termination of the specific purpose.
- 5.2.10.2 When the specific purpose of collecting personal data disappears, retention period expires, or the collection is illegal, each department should delete or

destroy the personal data on its own initiative or at the request of the data subject. However, due to business activities and other provisions of the law; for example, if Delta Group is to exercise the rights of civil, criminal or administrative litigation, or obtain the written consent of the data subjects, these circumstances will be exempted.

5.2.10.3 If the data subject is an employee, even after the termination of the employment relationship, Delta Group may still preserve data within the necessary period specified based on the purpose of maintaining public welfare, scientific or historical research purposes, statistical purposes, or for the compliance of personal data laws and regulations. Any labor laws or other documents required for potential disputes can also continue to be kept until the statute of limitations is eliminated or the retention period expires. After the expiration of the above-mentioned statutory period or the termination of related disputes, unless the data subjects have other agreements, the documents containing personal data should be returned to the data subjects or destroyed.

5.2.10.4 The deletion of personal data should be recorded in an appropriate manner and the results of its execution shall be confirmed. Any paper files containing personal data should be destroyed using appropriate methods, and should not be discarded or recycled at will. When deleting or erasing electronic files containing personal data, personal data must be deleted and erased until it could no longer be read or reached.

5.3 Utilization

5.3.1 Personal data utilization for each department of Delta Group should follow Personal Data Protection Management Policy, this procedure, relevant laws and regulations, international standard, etc.

5.3.1.1 Utilization of personal data should meet the scope of specific purpose.

5.3.1.2 No illegal use or misuse of personal data outside the scope of the specific purpose is allowed, and data in each database should not be arbitrarily linked.

5.3.2 When each department collects personal data with the written consent of the data subjects, the use of the personal data should comply with the content contained in the consent, including the period, region, object, method and other related matters of the use for the personal data.

5.3.3 Each department should meet one of the circumstances below if the situation of personal data utilization is other than the specific purpose:

5.3.3.1 where it is expressly required by law;

5.3.3.2 where it is necessary for furthering public interests;

5.3.3.3 where it is to prevent harm on life, body, freedom, or property of the data subject;

5.3.3.4 where it is to prevent material harm on the rights and interests of others;

5.3.3.5 where it is necessary for statistics gathering or academic research by a government agency or an academic institution for public interests; provided that such data, as provided by the data provider or disclosed by the data collector, may not lead to the identification of a specific data subject;

5.3.3.6 where consent has been given by the data subject according to clause 5.1.3 and 5.1.4; or

5.3.3.7 where it is for the data subject's rights and interests.

5.3.4 When each department requires the use of personal data outside of the specific purpose, it should follow this procedure. It should be approved the head of the department, and coordinated with relevant authority and responsibility unit. The use of personal data outside of the specific purpose should be recorded in written form.

5.3.5 Marketing

5.3.5.1 When Delta Group uses personal data for marketing activities, if the data subjects express refusal, Delta Group should immediately stop using the data subjects' personal data file for marketing.

5.3.5.2 If the data has been provided to a third party, the third party should be informed to make corrections. At the first time of marketing, a free method for the data subjects to express their refusal for marketing should be provided.

5.3.6 Cross-border Transfer

5.3.6.1 When Delta Group transfers personal data internationally, in principle, the following circumstances are not allowed:

- A. Violates major national interests;
- B. Violates international agreements, treaties or special provisions.
- C. The country receiving the personal data lacks proper regulations on protection of personal data and the data subjects' rights and interests may consequently be harmed;
- D. The cross-border transfer of the personal data to a third country (territory) is carried out to circumvent the relevant laws and regulations of personal data.
- E. Violates technical requirements for data transmission of Delta Group.

5.3.6.2 When Delta Group conducts operations related to cross-border transfer, it should take appropriate security protection measures, properly keep records of cross-border related operations of personal data, and perform its supervisory and management responsibilities. Delta Group should also consult the relevant authority and responsibility unit to ensure compliance with the relevant laws and regulations of the transmitting country, receiving country and the international organization of the international transmission.

5.4 Outsource others to process

When Delta Group outsources others to collect, process, or use all or part of personal data, it should sign for approval in accordance with the approval authority and a formal contract

with an external unit to ensure appropriate personal data protection and control measures. Make sure that the protection and measures also meet the information security standards required by Delta Group and conduct appropriate management and supervision. Details of outsourcing others to process, please refer to “Personal Data Outsourced Processing Procedures”

6. Rights of Data subjects

6.1 Data subjects could claim the rights to inquire or request reading, make copies, supplement or correct, stop collecting, processing or using, and delete their personal data. Please refer to “Data Subject's Rights Management Procedure”. To protect rights of data subjects, Delta Group should follow regulations below:

6.1.1 Provide channels for the data subjects to exercise their rights.

6.1.2 Confirm the identity of the data subjects.

6.1.3 Please check whether the exercise of the rights of data subjects will jeopardize national security, diplomatic and military secrets, overall economic interests, or other important national interests; hinder the performance of statutory duties by public agencies; hinder the major interest of the collection agency or a third party circumstance. Refuse the exercise of rights if the afore-mentioned happens.

6.1.4 The data subject's request should be responded within the prescribed time limit. For detailed deadlines, please refer to “Data Subject's Rights Management Procedure”.

7. Awareness Promotion and Education Training

7.1 Delta Group should conduct internal education training and awareness promotion for personal data protection according with actual needs, so employees could understand related laws, various regulations, and their scope of responsibility. For the method and content of education training, please refer to “Personnel Management, Education, and Training Regulations”

8. Audit System

8.1 Delta Group should form an internal control and audit system for personal data protection, and check the management of personal data files. For the detail content of internal control and audit system, please refer to “Personal Data Protection System and Organization Bylaws”

9. References

9.1 Delta Group Personal Data Protection Management Policy

9.2 Delta Group Privacy Policy

9.3 Personal Data Outsourced Processing Procedures

9.4 Data Subject's Rights Management Procedure

9.5 Personnel Management, Education, and Training Regulations

9.6 Personal Data Protection System and Organization Bylaws

10. Announcement and Implementation

10.1 If there is a need to update, add or modify this procedure, the Personal Data Protection Team should draft, and it will take effect after the chairman's approval.

10.2 If the applicable laws and regulations in each regional branch of the Delta Group are different from this procedure, relevant regulations or procedures shall be formed separately to ensure compliance with local laws and regulations.

11. Attachments

11.1 Personal data collection, processing or use consent form template (PIMS-ENG-04-01-001)

11.2 Personal data inventory list (PIMS-ENG-04-01-002)

11.3 Personal data inventory exclusion list (PIMS-ENG-04-01-003)