Fitipower Integrated Technology Inc.

Personal Data and Privacy Protection Management Guidelines

Chapter I – General Provisions

Article 1 Purpose

These Guidelines are established to implement the Personal Data Protection Act (PDPA) and related privacy protection laws, ensuring our company lawfully, reasonably, and securely manages the full lifecycle of personal data — including collection, processing, use, transmission, storage, and eventual deletion — while respecting individuals' privacy rights.

Article 2 Legal Basis

These Guidelines are based on the PDPA, its enforcement rules, and related privacy protection principles.

Article 3 Scope of Application

These Guidelines apply to all personal data and privacy management operations involving the company, its affiliates, employees, clients, suppliers, contractors, and other business partners.

Article 4 Definitions

All terms used herein follow the definitions in the PDPA, including but not limited to: personal data, processing, use, data subject, international transfer, privacy risk assessment, and de-identification.

Chapter II – Organization, Responsibilities, and Policies

Article 5 Personal Data Protection Management Organization

The company establishes a "Personal Data and Privacy Oversight Committee" composed of heads of HR, IT, and audit departments, responsible for：

- Drafting, revising, and promoting personal data and privacy protection policies。
- Assessing and managing privacy risks。
- Planning and conducting privacy and data protection training。
- Reporting, responding to, and investigating data and privacy incidents。
- Conducting internal audits and following up on improvement actions。
- Acting as the main point of contact for authorities and data subjects on privacy matters。

Article 6 Responsible Department

- HR Department: Manages employee personal data and handles data subject rights requests.
- IT Department: Implements, maintains, and responds to technical and physical security measures。
- Business Department: As data collectors, they are responsible for lawful data collection, processing, and use within their scope, and for implementing these Guidelines。
- Legal Department: Provides compliance advice and contract review support。
- Audit Department: Independently monitors and evaluates compliance with these Guidelines。

Article 7 Policy Statement

The company is committed to establishing and maintaining a data and privacy management system that meets legal requirements, ensuring that privacy protection is embedded in all business processes through ongoing training, risk management, and technological reinforcement, and strives for continual

improvement。

Chapter III Operational Content

Article 8 – Legality and Minimization Principle

Personal data must be collected, processed, and used in accordance with the PDPA, based on specific, clear, and lawful purposes, and limited to the minimum necessary to achieve those purposes。

Article 9 – Duty to Inform and Transparency

When collecting personal data, the following information must be clearly and intelligibly disclosed to data subjects (Privacy Notice)：

- Name of the data collector。
- Purpose of collection。
- Categories of personal data。
- Duration, region, target, and method of use。
- Rights and methods of exercising rights under the PDPA。
- When the data subject has the freedom to choose whether to provide personal data, the impact on their rights and interests if they choose not to provide it。

Exceptions permitted by law apply as regulated。

Article 10 Consent Management

- Consent for collection, processing, or use of personal data must be voluntary, specific, informed, and explicit, obtained in writing or other recordable formats, using the company's standard “Consent to Personal Data Collection” form。
- Consent must also be obtained separately for use beyond the original specified purpose。
- Mechanisms must be established to prove consent was obtained and allow withdrawal of consent at any time。

Article 11 Protection of Sensitive Data

Sensitive personal data (e.g., medical records, genetics, sexual life, health checkups, criminal records) must not be collected, processed, or used unless legally authorized or based on explicit written consent, and must be protected with stricter measures such as encryption, access segregation, and additional approval layers。

Article 13 Rights of Data Subjects

Data subjects may exercise the following rights under the law and cannot be contractually waived：

- Request to access or review data。
- Request copies。
- Request correction or supplement。
- Request cessation of collection, processing, or use。
- Request deletion。

Article 14 Handling of Rights Requests

- Data subjects must submit a “Personal Data Rights Request Form” with identification documents。

- The responsible department (usually HR or the original collector) must respond within legal timeframes (15 days for access/review, 30 days for other requests), extendable once if needed。
- Approval or denial must be provided in writing. Denials must include reasons。
- Reasonable costs may be charged for copies。

Article 15 Data Security Measures

To prevent theft, alteration, damage, loss, or leakage, security measures should be based on the sensitivity and volume of data：

- Physical Security: Access controls for storage areas or devices (e.g., locks, entry systems)。
- Technical Security：

  -Encryption during transmission and storage (e.g., SSL/TLS, AES)。

  - Access controls with least-privilege principle。

  - Deployment of firewalls, antivirus software, intrusion detection systems。

  - Logging access activities and regular audit reviews。
- Administrative Controls：

  - Employee confidentiality agreements。

  - Privacy and security training。

  - Regular data backup and recovery tests。

Article 16 Restrictions on International Transfer

Personal data may only be transferred internationally if the recipient location provides equivalent protection levels, or through legal mechanisms such as consent, standard contractual clauses, or international certifications。

Article 17 Outsourcing Management

When outsourcing data processing, contracts must clearly define confidentiality, security, audit, and liability clauses. The company must regularly monitor compliance。

Article 18 Incident Reporting and Response

- Any personnel discovering or suspecting a breach (e.g., data leakage, theft, alteration, damage, loss) must report immediately to their supervisor and the oversight committee。
- The committee shall initiate the response process：

  Containment: Immediate actions to prevent further damage (e.g., system isolation, password resets)。

  Assessment: Determine scope, root cause, and impact through analysis。

  Notification: Decide whether to notify authorities or data subjects and execute as required。

  Remediation: Implement corrective and preventive measures。
- The entire process must be documented using the “Personal Data Security Incident Report Form.”。

Article 19 Privacy Impact Assessment (PIA)

- A PIA must be conducted before：

  Introducing new technologies or systems handling personal data。

  Launching new processes involving large-scale or sensitive data。

  Changing the scope or method of personal data use。

- The PIA should evaluate potential privacy risks and propose mitigation strategies, with reports submitted to the oversight committee。

Article 20 Training

The oversight committee must plan and conduct at least one company-wide training annually on personal data and privacy awareness, with records maintained。

Article 21 Internal Audit and Continuous Improvement

- The audit department shall include PDPA compliance in the annual audit plan。
- Audit results must be reviewed by management; non-conformities must be addressed with corrective plans and tracked to completion。
- The Guidelines must be reviewed in light of regulatory, technological, and business changes to ensure their ongoing relevance, adequacy, and effectiveness。

Chapter IV Supplementary Provisions

Article 22 Enforcement and Revisions

These Guidelines shall take effect upon board approval. Revisions follow the same process。

Originally enacted on December 29, 2014。

First revision: October 30, 2025。

Article 23 Related Forms

一、Consent to Personal Data Collection

二、Personal Data Rights Request Form

三、Personal Data Security Incident Report Form

四、Privacy Impact Assessment Checklist

Consent Form for the Collection of Personal Data

1. Purpose

To handle employee recruitment, employment, HR management, salary payments, labor and health insurance, employee benefits, tax declarations, and other legal obligations, our company collects, processes, and uses your personal data in accordance with the Personal Data Protection Act and related regulations. This statement is provided to protect your rights.

2. Purpose of Data Collection

The purposes for which we collect your personal data include but are not limited to:

- Employee recruitment and hiring evaluation
- Employment registration, labor/health insurance, and pension filing
- Salary disbursement and income tax filing
- Performance review, reassignment, promotion, and separation procedures
- Application of benefit programs (e.g., group insurance, staff trips, health check-ups)
- Compliance with laws or government requests
- Emergency contact or disaster response purposes

3. Categories of Personal Data Collected

We may collect the following types of personal data:

- Basic information (name, gender, date of birth, ID number, nationality, photo)
- Contact information (address, phone number, email)
- Family details (emergency contact, spouse, children)
- Education and employment background
- Bank account (for salary deposit)
- Social insurance information (labor/health insurance, pension)
- Health information (health reports, vaccination records)

4. Duration, Region, Recipients, and Method of Use

- Duration: During the necessary period for stated purposes or statutory retention.
- Region: Taiwan and other business operation locations.
- Recipients: The Company, affiliates, governmental authorities, lawful partners.
- Method: Collected, processed, transferred, and used in paper or electronic form.

5. Rights of the Data Subject

According to Article 3 of the Personal Data Protection Act, you have the right to:

- Inquire or request to review your data
- Request copies
- Request correction or supplementation
- Request to stop collection, processing, or use
- Request deletion

6. Consequences of Failing to Provide Data

If you fail to provide necessary data, employment procedures, salary disbursement, or insurance applications may be affected, and your rights may be compromised.

7. Data Security and Protection

We have implemented reasonable security measures and internal controls to protect your personal data from unauthorized access, disclosure, alteration, or destruction.

8. Contact Information

If you have any questions regarding this statement, please contact:

- Department： HR Department
- Phone：
- Email：
- Address：

9. Consent and Signature

I have read and understood the above statement and agree that the company may collect, process, and use my personal data as described herein.

Employee Signature_____

Date：**_____**

Personal Data Rights Request Form

Item	Content
Applicant Information	
Name	
Phone Number	
Email	
Requested Action(s)	□Access or Review □Request a Copy □Supplement or Correct □Cease Collection/Processing/Use □Deletion
Reason for Request	
Attachments	□Identity Document □Proof of Authorization
Signature	
Date	

Personal Data Security Incident Report Form

Item	Content
Reporting Department	
Date & Time	
Type of Incident	□Unauthorized Access □Data Breach □Loss or Theft □Accidental Disclosure □System Vulnerability □Other：_____
Incident Description	
Affected Data	□Name□Contact Info□ID No. □Financial Info□Health Data □Other：_____
Initial Response	
Signature	
Date	

Privacy Impact Assessment Checklist

1. Basic Information

Project Name		Project Manager	
Lead Department		Assessment Date	
Project Summary			
Assessors			

2. Assessment Initiation Review（If any of the following items is marked “Yes,” a full assessment is required）

No	Checklist Item	Y	N	Remarks
1	Does the project involve the collection, processing, or use of personal data？	☐	☐	
2	Does it involve the processing of sensitive personal data (e.g., health, biometric, criminal records)？	☐	☐	
3	Does it use new technologies (e.g., facial recognition, AI analytics, behavioral tracking) for data processing？	☐	☐	
4	Does it involve large-scale or systematic monitoring or analysis (e.g., employee behavior analysis, customer profiling)？	☐	☐	
5	Does it involve international transfer of personal data？	☐	☐	
6	Does it involve sharing personal data with third parties or outsourcing processing？	☐	☐	
7	Will the personal data be used for new purposes other than the original collection purpose？	☐	☐	

3. Privacy Principles Compliance Assessment

Category	Assessment Item	Y	N	N/A	Risk Description and Mitigation Measures
Legality and Purpose Specification	1. Is there a clear and lawful purpose for data collection？	☐	☐	☐	
	2. Was a clear privacy notice/information disclosure prepared before collection？	☐	☐	☐	
Data Minimization	3. Are the categories of personal data collected limited to the minimum necessary to achieve the purpose？	☐	☐	☐	
	4. Is the data retention period set and aligned with the purpose？	☐	☐	☐	

Data Subject Rights	5. Is there a mechanism to ensure the exercise of data subject rights (access, correction, deletion, etc.)？	☐	☐	☐	
	6. Is the opt-out mechanism easy to find and use？	☐	☐	☐	
Consent Management	7. If consent is required, is it obtained voluntarily, explicitly, and recordably？	☐	☐	☐	
	8. Can data subjects easily withdraw their consent？	☐	☐	☐	
Data Security	9. Are technical security measures planned to match data sensitivity (e.g., encryption, anonymization)？	☐	☐	☐	
	10. Are physical and administrative security measures planned (e.g., access control, confidentiality agreements)?	☐	☐	☐	
Third Parties and Transfers	11. If involving third parties, are confidentiality and security responsibilities clearly defined in contracts？	☐	☐	☐	
	12. If involving international transfers, is the legal basis sufficient？	☐	☐	☐	

4. Risk Rating and Recommended Actions

Identified High-Risk Item	Risk Level (High / Medium / Low)	Recommended Actions and Mitigation Measures	Responsible Person	Completion Deadline

5. Assessment Conclusion and Approval

Overall Risk Level	☐ High Risk： Mitigation measures must be implemented and approved by the General Manager
	☐ Medium Risk： Mitigation measures recommended; approval by the Oversight Committee
	☐ Low Risk： Acceptable risk; project may proceed as planned

Assessment Conclusion：

☐ Approved for Implementation: Risks have been adequately identified and mitigated。

☐ Not Approved: The project presents significant privacy deficiencies and requires redesign before reassessment。

Assessor's Signature：_____ Department Head：_____

Oversight Committee / General Manager Approval：

_____