FCF Co., Ltd.

Regulations Governing Personal Data Protection

Date of Promulgation: June 8, 2022

Chapter I. General Provisions

Article 1. In order to manage and process the personal data owned by the Company, prevent employees' interests and rights from infringement and promote the reasonable use of personal data, the Company establishes the Regulations in accordance with the "Personal Data Protection Act" and "Enforcement Rules of the Personal Data Protection Act."

Article 2. The terms used herein denote the following meanings:

I. Personal data: A natural person's name, date of birth, ID Card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, healthcare data, genetic data, data concerning a person's sex life , records of physical examination, criminal records, contact information, financial conditions and data concerning a person's social activities and any other information that may be used to directly or indirectly identify the natural person;

II. Personal data file: A collection of personal data structured to facilitate data retrieval and management by automated or non-automated means;

III. Responsible unit: The unit engaged in collection, processing and use of data for the business it takes charge of or in order to execute business;

IV. Unit: Any of the Company's units engaged in administrative management and business;

V. Collection: The act of collecting personal data in any way;

VI. Processing: The act of recording, inputting, storing, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting or internally transferring data for the purpose of establishing or using a personal data file; the Company's internal use and management of the same;

VII. Use: The act of using personal data via any methods other than processing;

VIII. Cross-border transfer: The cross-border processing or use of personal

data;

IX. Government agency: A central or local government agency or administrative entity authorized to exercise public authority pursuant to laws;

X. Employee data: The personal data of employees who are working for the Company, including any data to be needed or maintained during the performance of job duty, including those about job transfer provided by the employees in person and during their performance of job duty, changes in salaries, bonus, performance reward and punishment, changes in educational background and working experience, attendance records, changes in labor insurance, national health insurance and labor pension, training, public announcement, participation in activities, applications and forms.

Article 3. Recipient and Scope

I. Recipient: Any of the Company's personnel and advisors or suppliers dealing business with the Company (including their employees or temporary workers).

II. Scope: The personal data protectable under the Personal Data Protection Act. The relevant requirements are adopted for the purpose of collection, processing, use and cross-border transfer of personal data, in order to ensure personal data safety.

Article 4. Responsible Unit

I. Personnel Unit:

1. Proposal of, amendments to and management of the Regulations Governing Personal Data Protection.
2. Creation, processing, maintenance and custody of employees' personal data.
3. Policy promotion and training related to the Personal Data Protection Act.
4. Liaison for complaints, consultation and reporting on personal data incidents.
5. Other matters related to management of planning and execution of personal data protection.

II. IT Unit:

1. Set up the information security protection network for personal data to prevent personal data from being stolen, tampered, damaged, destroyed or disclosed by hackers and strengthen the control of security measures.

2. Information security damage prevention and crisis management and response mechanism.

III. Internal Audit Unit:

1. Audit various management procedures under the Regulations periodically or from time to time, verify compliance thereof and provide suggestions about improvement.
2. Prepare the audit report based on said audit results in accordance with the SOP for Internal Audit and submit it to the Board of Directors periodically.

Article 5. Responsibilities

I. All of the Company's personnel shall acknowledge and strictly comply with the Regulations, and fully participate in the implementation of programs under the Regulations.

II. The Company's management are responsible for appointing the personal data management owner with the authority to supervise the operations of the Company's personal data management system, and direct and manage the operation of the Company's personal data protection management execution organization to fulfill the compliance with the Personal Data Protection Act.

Chapter II. Collection, Processing and Use of Personal Data

Article 6. The Company shall ensure that the collection, processing and use of personal data are carried out in a way that respects the data subject's rights and interest, in an honest and good-faith manner, without exceeding the necessary scope of specific purposes, and have legitimate and reasonable connections with the purposes of collection.

Article 7. A data subject may exercise the following rights with regard to his/her personal data against the Company pursuant to laws, based on his/her right autonomy in the personal data:

I. the right to make an inquiry of and to review his/her personal data;

II. the right to request a copy of his/her personal data;

III. the right to supplement or correct his/her personal data;

IV. the right to demand the processing or use of, or erase, his/her personal data.

Article 8. Data pertaining to a natural person's healthcare, genetics, sex life, physical examination and criminal records shall not be collected, processed or used unless on any of the following bases:

I. where it is expressly required by law;

II. where it is within the necessary scope for a government agency to

perform its statutory duties or for the Company to fulfill its statutory obligation, provided that proper security and maintenance measures are adopted;

III. where the personal data has been disclosed to the public by the data subject or has been made public lawfully;

IV. where it is necessary for a government agency or an academic institution to collect, process and use the personal data for statistics gathering or academic research for the purpose of healthcare, public health or crime prevention and through specific procedure.

Article 9. Each unit shall expressly inform the data subject of the following information when collecting their personal data:

I. the name of the government or non-government agency (company/unit name);

II. the purpose of the collection;

III. the categories of the personal data to be collected;

IV. the time period, territory, recipients and methods of which the personal data is used;

V. the rights exercisable by the data subjects under Article 3 of the Personal Data Protection Act;

VI. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data. The obligation to inform as prescribed in the preceding paragraph may be waived under any of the following circumstances:

1. where notification may be waived in accordance with the law;
2. where the collection of personal data is necessary for the government agency to perform its statutory duties or the Company to fulfill its statutory obligations;
3. where giving notice will prevent the government agency from performing its statutory duties;
4. where giving notice will harm a third party’s material interest;
5. where the data subject has already known the contents of the notification.

Article 10. Each unit shall, before processing or using the personal data collected in accordance with Article 19 of the Personal Data Protection Act which are not provided by the data subject (i.e., Personal data collected indirectly), inform the data subject of its source of data and other information specified in Sub-paragraphs 1 to 5, Paragraph 1 of the preceding article. The obligation to inform as prescribed in the

preceding paragraph may be exempt under any of the following circumstances:

I. under any of the circumstances provided in Paragraph 6 of the preceding article;
II. where the personal data has been disclosed to the public by the data subject or has been made public lawfully;
III. where it is unable to inform the data subject or his/her statutory representative;
IV. where it is necessary for statistics gathering or academic research in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;
V. where the personal data is collected by mass communication enterprises for the purpose of news reporting for the benefit of public interests. The obligation to inform as prescribed in Paragraph 1 may be performed at the same time of the first use of the personal data towards the data subject.

Article 11. Except for the personal data specified under Paragraph 1, Article 6 of the Personal Data Protection Act, the collection or processing of personal data by the Company shall be for specific purposes and on one of the following bases:

I. where it is expressly required by law;
II. where there is a contractual or quasi-contractual relationship between the Company and the data subject;
III. where the personal data has been disclosed to the public by the data subject or has been made public lawfully;
IV. where it is necessary for statistics gathering or academic research by an academic institution in pursuit of public interests, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;
V. where consent has been given by the data subject in writing;
VI. where it is related to public interest;
VII. where the personal data is obtained from publicly available sources, unless the data subject has an overriding interest in prohibiting the processing or use of such personal data.

The "written consent," as referred to in the preceding subparagraph 5, means a separate declaration of agreement given by a data subject after he/she has been informed by the data collector of any of the purposes other than that

originally specified, the scope of other use and the impact of giving or not giving consent on the rights and interests of the data subject.

I. Article 12. Except for the personal data specified in Paragraph 1, Article 6 of the Personal Data Protection Act, the Company shall use personal data only within the necessary scope of the specific purpose of collection, the use of personal data for another purpose shall be only on any of the following bases: where it is expressly required by law;
II. where it is necessary for furthering public interest;
III. where it is necessary to prevent harm on life, body, freedom or property of the data subject;
IV. where it is necessary to prevent material harm on the rights and interests of others;
V. 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 processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject;
VI. where consent has been given by the data subject in writing;

The "written consent," as referred to in the preceding subparagraph 6, means a separate declaration of agreement given by a data subject after he/she has been informed by the data collector of any of the purposes other than that originally specified, the scope of other use and the impact of giving or not giving consent on the rights and interests of the data subject.

Article 13. If a cross-border transfer of personal data is carried out by the Company under any of the following circumstances, the central government authority in charge of the industry concerned may impose restrictions on such transfer:

I. where major national interests are involved;
II. where an international treaty or agreement so stipulates;
III. where 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.

Chapter III. Response to Data Subjects' Exercise of Interest and Right

Article 14. Upon the request of a data subject, the Company shall reply to the data subject's inquiry, allow the data subject to review the personal data collected, or provide the data subject with a copy thereof except under any of the following circumstances:

I. where national security, diplomatic or military secrets, overall economic

interests or other material national interests may be harmed;

II. where a government agency may be prevented from performing its statutory duties;

III. where the material interests of the data collectors or any third parties may be adversely affected.

Article 15. The Company shall ensure the accuracy of personal data in its possession and correct or supplement such data on its own initiative or upon the request of data subjects.

I. In the event of a dispute regarding the accuracy of the personal data, the Company shall, on its own initiative or upon the request of the data subject, cease processing or using the personal data, unless the processing or use is either necessary for the performance of an official or business duty or has been agreed upon by the data subject in writing, and the dispute has been recorded.

II. When the specific purpose of data collection no longer exists or upon expiration of the relevant time period, the Company shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data, unless the processing or use is either necessary for the performance of an official or business duty, or has been agreed by the data subject in writing.

III. The Company shall, on its own initiative or upon the request of the data subject, erase the personal data collected or cease collecting, processing or using the personal data in the event where the collection, processing or use of the personal data is in violation of the Personal Data Protection Act.

IV. If any failure to correct or supplement any personal data is attributable to the Company, the Company shall notify the persons who have been provided with such personal data after the correction or supplement is made.

Article 16. If any personal data is stolen, disclosed, altered, or otherwise infringed upon due to a violation of the Personal Data Protection Act by the Company, the data subject shall be notified via appropriate means after the relevant facts have been clarified.

Article 17.

I. Where a request is made by a data subject to the Company pursuant to Article 10 of the Personal Data Protection Act, the Company shall determine whether to accept or reject such request within fifteen days; such deadline may be extended by up to fifteen days if necessary and

the data subject shall be notified in writing of the reason for the extension.

II. Where a request is made by a data subject to the Company pursuant to Article 11, the Company shall determine whether to accept or reject such request within thirty days; such deadline may be extended by up to thirty days if necessary, and the data subject shall be notified in writing of the reason for the extension.

Article 18. The Company may charge a fee to cover necessary costs from those who make an inquiry or request to review or obtain copies of the personal data.

Chapter IV. Personal Data Security Management and Maintenance

Article 19. The Company's Personnel Unit is allowed to engage in the act of inputting, storing, compiling/editing, correcting, retrieving, deleting, outputting or transferring data, or processing in any other manners for the purpose of personal data management and shall be responsible for managing and maintaining the data. IT Unit shall take appropriate security measures and establish internal security control mechanism and adequate storage locations to prevent the personal data from being stolen, altered, damaged, destroyed or disclosed and shall undergo the internal audit conducted by the Internal Audit Unit from time to time.

Article 20. The unit accessing personal data shall create the unit's authority of access to personal data, establish the encryption treatment subject to adequate hierarchy of security, improve the data access control and the protection measures for data security to prevent any illegal intrusion, such as a hacker's attack, and shall conduct the internal self-audit and update from time to time.

Article 21. Where any unit suffers any information security hazard, such as intentional destruction or damage to personal data files and negligence in operations, or illegal intrusion, such as a hacker's attack, it shall take appropriate emergency response actions and report the personal data security incident.

Article 22. The Regulations shall be enforced upon promulgation after approval of the Company's President. The same shall apply where the Regulations are amended.