

Management Regulations for Personal Data Protection

Article 1

Ennoconn Corporation (hereinafter referred to as the “Company”) establishes the Management Regulations for Personal Data Protection (hereinafter referred to as the “Regulations”) to comply with the Personal Data Protection Act and other applicable laws and regulations. The Regulations govern the collection, processing, and use of personal data to prevent infringement of personal rights and to promote the reasonable use of personal data.

Article 2

The terms used in the Regulations are defined as follows:

1. **Personal Data:** Refers to information relating to a natural person, including name, date of birth, national identification number, passport number, characteristics, fingerprints, marital status, family, education, occupation, medical records, medical treatment, genetic information, sex life, health examinations, criminal records, contact information, financial status, social activities, and any other information that may directly or indirectly identify the individual.
2. **Personal Data File:** Refers to a collection of personal data established in a systematic manner that can be retrieved and organized by automated machines or other non-automated methods.
3. **Collection:** Refers to obtaining personal data by any means.
4. **Processing:** Refers to the recording, input, storage, editing, correction, duplication, retrieval, deletion, output, connection, or internal transmission of personal data for the purpose of establishing or using personal data files.
5. **Use:** Refers to any use of collected personal data other than processing.
6. **International Transfer:** Refers to the cross-border processing or use of personal data.
7. **Government Agency:** Refers to a central or local government agency or administrative legal entity that exercises public authority in accordance with law.
8. **Non-Government Agency:** Refers to any natural person, legal person, or other organization other than those specified in the preceding subparagraph.
9. **Data Subject:** Refers to the individual to whom the personal data pertains, as well as vendors, financial institutions, and other parties that have business dealings with the Company.

Article 3

The following rights exercised by data subjects with respect to their personal data under the Regulations shall not be waived in advance or restricted by special agreement:

1. The right to inquire about or request access to personal data.
2. The right to request a copy of personal data.
3. The right to request supplementation or correction.
4. The right to request cessation of collection, processing, or use.
5. The right to request deletion.
6. Where technically feasible, the right to request the transfer of personal data to a designated third party or service providers.

Article 4

When the Company commissions others to collect, process, or utilize personal data, it shall exercise appropriate supervision over the commissioned party, regularly verify the execution status of the commissioned party, and record the verification results:

1. The scope, categories, specific purposes, and duration of the intended collection, processing, or utilization of personal data.
2. The measures adopted by the commissioned party pursuant to Article 20, Paragraph 2.
3. Where sub-commissioning is involved, the designated sub-commissioned party.
4. Matters that shall be reported to the Company and remedial measures that shall be taken if the commissioned party or its employees violate the Regulations, other personal data protection laws, or related regulations.
5. Any reserved instructions retained by the Company with respect to the commissioned party.
6. Upon termination or rescission of the commission relationship, the return of personal data carriers, and the deletion of personal data held by the commissioned party via storage methods as part of fulfilling the commission contract.

Article 5

The Company's collection, processing, or utilization of personal data shall respect the rights and interests of the data subject, be conducted in accordance with the principles of honesty and good faith, shall not exceed the necessary scope of specific purposes, and shall bear a legitimate and reasonable nexus to the purposes of collection.

Article 6

The Company shall properly manage the personal data it collects, processes, and uses in accordance with personal data protection laws and internal management rules. In principle, the Company shall not arbitrarily provide, disclose, or make personal data available to any third party. However, where necessary for the performance of legal obligations, compliance with lawful requests from government agencies, or the assertion, exercise, or protection of the Company's legal rights and interests, the Company may disclose personal data to government agencies or non-government agencies third parties within the necessary scope of the specific purpose.

Before providing personal data to a third party, the Company shall first verify the identity of the third party, notify the data subject in accordance with law, and obtain the data subject's consent, unless otherwise provided by law or where notification may be exempted by law. The Company shall disclose only the necessary and minimum amount of personal data, and shall require third parties to properly manage personal data in accordance with applicable laws and contractual arrangements. Third parties shall not process, use, or further disclose personal data beyond the specific purpose of the commissioned matters.

Article 7

The Company shall not collect, process, or utilize data regarding personal medical history, medical treatment, genetics, sexual life, health examinations, and criminal records. However, this restriction does not apply under any of the following circumstances:

1. Where expressly provided by law.
2. Where necessary for a government agency to perform its statutory duties or for a non-government agency to fulfill its statutory obligations, and appropriate security measures are adopted either before or after such activities.
3. Where the data subject has made the personal data public, or where the personal data has otherwise been lawfully disclosed.
4. Where a government agency or academic research institution requires the data for medical, health, or crime prevention purposes for statistics or academic research, and the data has been processed by the provider or disclosed by the collector in a manner that does not allow identification of a specific data subject.
5. Where necessary to assist a government agency in performing statutory duties or a non-government agency in fulfilling statutory obligations, and appropriate security measures are adopted either before or after such activities.
6. Where the data subject has provided written consent. However, this shall not apply if the collection, processing, or use exceeds the necessary scope of the specific

purpose, if other laws prohibit reliance solely on the data subject's written consent, or if the consent is given against the data subject's will.

Article 8

When collecting personal data from a data subject, the Company shall explicitly inform the data subject of the following matters:

1. The name of the government or non-government agency.
2. The purpose of collection.
3. The categories of personal data.
4. The period, region, recipients, and methods of personal data utilization.
5. The rights the data subject may exercise under Article 3 and the methods for doing so.
6. Unless otherwise permitted by applicable laws and regulations, the Company shall obtain the data subject's prior consent before collecting, processing, or using personal data (opt-in consent). The data subject may, according to different specific purposes, consent to, refuse, withdraw consent, or opt out of such collection, processing, or use (opt-out option).
7. The data subject's freedom to choose whether to provide personal data, and the impact on their rights and interests if they choose not to provide it.

Notification specified in the preceding paragraph may be waived under any of the following circumstances:

1. Legally exempt from notification.
2. The collection of personal data is necessary for a government agency to execute statutory duties or for a non-government agency to fulfill legal obligations.
3. Notification would impede the execution of statutory duties by a government agency.
4. Notification would prejudice public interests.
5. The contents to be notified are already known to the data subject.
6. The collection of personal data is for non-profit purposes and clearly bears no adverse impact on the data subject.

Article 9

When the Company collects personal data that was not provided by the data subject, it shall inform the data subject of the source of the personal data and the matters listed in Items 1 to 5 of Paragraph 1 of the preceding Article prior to processing or utilization. Notification may be waived under any of the following circumstances:

1. Any of the circumstances listed in Paragraph 2 of the preceding Article apply.
2. Personal data that has been disclosed by the data subject themselves or otherwise legally disclosed.
3. Notification cannot be made to the data subject or their legal representative.
4. Necessary for statistics or academic research based on public interest, provided that the data has been processed by the provider or disclosed by the collector in a manner that renders specific data subjects unidentifiable.
5. Mass media operators collect personal data for the public interest purpose of news reporting.

Article 10

Upon request by a data subject, the Company shall respond to inquiries, provide review, or produce copies regarding the collected personal data. Decisions on such requests shall be made within 15 days; when necessary, this may be extended for a period not exceeding 15 days, and the reasons for extension shall be notified to the requestor in writing. However, this does not apply under any of the following circumstances:

1. Prejudice to national security, diplomatic and military secrets, overall economic interests, or other major national interests.
2. Impediment to the execution of statutory duties by a government agency.
3. Prejudice to the major interests of the collecting agency or a third party.

Article 11

The Company shall maintain the accuracy of personal data and shall correct or supplement it proactively or upon the request of the data subject. If the accuracy of personal data is disputed, the Company shall proactively or upon request cease processing or utilizing it. However, this restriction does not apply if it is necessary for the execution of duties or business operations, or if written consent has been obtained from the data subject and the dispute has been noted.

The Company's retention period for personal data shall not exceed the reasonable period necessary for the specific purpose, and in principle shall not exceed five years. When the specific purpose for collecting personal data ceases to exist or the retention period expires, the Company shall, either proactively or upon request by the data subject, delete, cease processing, or cease using the personal data. However, this restriction shall not apply where processing or use is necessary for the performance of duties or business, or where the data subject has provided written consent.

If a data subject believes that personal data has been collected, processed, or utilized in violation of the Regulations, the Company shall, proactively or upon request, delete, or cease the collection, processing, or utilization of said personal data.

Personal data that was not corrected or supplemented due to reasons attributable to the Company shall, after correction or supplementation, be notified to the recipients to whom the data was previously provided for utilization.

When processing the aforementioned requests from data subjects, decisions shall be made within 30 days; when necessary, this may be extended for a period not exceeding 30 days, and the reasons for extension shall be notified to the requestor in writing.

Article 12

In the event that personal data held by the Company is stolen, leaked, altered, or otherwise compromised, the Company shall conduct an investigation, notify the data subject via appropriate means, and pursue relevant liabilities.

Article 13

The handling unit of the Company may charge necessary cost fees to individuals who inquire about, request review of, or request the production of copies of personal data.

Article 14

The Company's collection or processing of personal data shall be for specific purposes and must satisfy one of the following conditions:

1. Explicitly mandated by law.
2. Contractual or quasi-contractual relationship with the data subject, where appropriate security measures have been implemented.
3. Personal data that has been disclosed by the data subject themselves or otherwise legally disclosed.
4. Necessary for statistics or academic research by academic research institutions based on public interest, provided that the data has been processed by the provider or disclosed by the collector in a manner that renders specific data subjects unidentifiable.
5. With the consent of the data subject.
6. Necessary to advance public interest.
7. Personal data obtained from generally available sources, unless the data subject has a more worthy overriding interest in prohibiting the processing or utilization of said data.

8. No infringement on the rights and interests of the data subject. When the collector or processor becomes aware or is notified by the data subject that processing or utilization should be prohibited pursuant to the proviso of Item 7 of the preceding paragraph, they shall, proactively or upon request, delete, or cease the processing or utilization of said personal data.

Article 15

The Company's utilization of personal data shall be within the necessary scope of the specific purpose of collection. However, utilization outside the specific purpose may be permitted under any of the following circumstances:

1. Explicitly mandated by law.
2. Necessary to advance public interest.
3. Necessary to avert danger to the life, body, freedom, or property of the data subject.
4. Necessary to prevent major harm to the rights and interests of others.
5. Necessary for statistics or academic research by government agencies or academic research institutions based on public interest, provided that the data has been processed by the provider or disclosed by the collector in a manner that renders specific data subjects unidentifiable.
6. With the consent of the data subject.
7. Beneficial to the rights and interests of the data subject. When personal data is used for marketing pursuant to the preceding paragraph, if the data subject objects to receiving marketing, the Company shall immediately cease using their personal data for marketing. During the first marketing instance, the Company shall provide the data subject with a method to refuse marketing and shall bear the necessary expenses.

Article 16

The Company shall prohibit the international transfer of personal data under any of the following circumstances:

1. Where major national interests are involved.
2. Where international treaties or agreements have special provisions.
3. Where the recipient country lacks comprehensive regulations for personal data protection, risking infringement on the rights and interests of the data subject.
4. Where personal data is transferred to a third country (region) via indirect methods to circumvent the Regulations.

Article 17

Personnel across all units of the Company shall cooperate with central competent authorities or municipal/county/city governments in conducting security maintenance audits of data files, data processing methods upon business termination, international transfer restrictions, or other routine business inspections. Personnel participating in inspections who become privy to others' data through such inspections shall bear a duty of confidentiality.

Article 18

All units of the Company that object to demands, enforcement, seizure, or duplication actions taken by central competent authorities or municipal/county/city governments shall immediately submit a request to the Company's legal department to assist in filing an objection or initiating administrative litigation for remedy, thereby safeguarding the Company's rights and interests.

Article 19

The Company, as a holder of personal data files, shall adopt appropriate security measures to prevent personal data from being stolen, altered, damaged, destroyed, or leaked.

Article 20

To prevent personal data from being stolen, altered, damaged, destroyed, or leaked, the Company shall adopt appropriate technical and organizational security maintenance measures.

The measures specified in the preceding paragraph may include the following items, based on the principle of keeping a proper proportion to the personal data protection objectives intended to be achieved:

1. Allocation of management personnel and adequate resources.
2. Defining the scope of personal data.
3. Personal data risk assessment and management mechanisms.
4. Incident prevention, notification, and response mechanisms.
5. Internal management procedures for the collection, processing, and utilization of personal data.
6. Data security management and personnel management.
7. Awareness propagation and education/training.
8. Device security management.
9. Data security audit mechanisms.
10. Preservation of usage records, tracking logs, and evidence.

11. Continuous overall improvement of personal data security maintenance.

Article 21

Execution shall comply with the personal data file security maintenance plan or personal data handling methods after business termination prescribed by the central competent authority (Industrial Development Administration, Ministry of Economic Affairs).

Article 22

The Regulations shall be implemented after approval by the Board of Directors, and the same shall apply to any amendments hereto.