Ching Feng Home Fashions Co., Ltd.

Personal Data Protection Act

Article 1 The Company hereby establishes these Regulations to implement the protection and management of personal data.

Article 2 The term "personal data" as used in these Regulations refers to the data specified in Subparagraph 1, Article 2 of the Personal Data Protection Act (hereinafter referred to as the "PDPA").

Article 3 All departments of the Company shall strictly comply with Article 5 of the PDPA when collecting, processing, or using personal data.

Article 4 Management of Personal Data Use

1. When collecting personal data from the data subject, except as expressly provided by law, the Company shall obtain the consent of the data subject and clearly inform the data subject of the purpose of collection, the categories of personal data, the period, territory, recipients, and methods of use of the personal data.
2. The collection of personal data shall comply with specific purposes and ensure the accuracy, completeness, and timeliness of the data.
3. When collecting personal data, the Company shall comply with the requirements of the PDPA and obtain appropriate authorization and supervision, and shall collect only the necessary fields required. When the collection of personal data has been authorized and consented to, electronic documents shall be encrypted for the data files, while hard-copy documents shall be transmitted and exchanged by sealed or other secure means.
4. When any department requires personnel data for business operations, it shall submit an application to the Human Resources Department and, after obtaining authorization and consent, handle such data in accordance with the "PDPA."
5. For the Company's collection and processing of personal data, except for the data specified in Paragraph 1, Article 6 of the "PDPA," there shall be a specific purpose, and one of the following circumstances shall apply:

   A. Expressly provided by law.

   B. There is a contractual or quasi-contractual relationship with the data subject.

   C. The data subject has made the personal data public by himself/herself or the personal data has otherwise been legally made public.

   D. Written consent has been obtained from the data subject.

E. The personal data is obtained from generally available sources. However, this shall not apply where the data subject has a significant interest that is more worthy of protection in prohibiting the processing or use of such data.

6. For the Company's use of personal data, except for the data specified in Paragraph 1, Article 6 of the "PDPA," such use shall be within the necessary scope of the specific purpose of collection. However, the personal data may be used for purposes other than the specific purpose under any of the following circumstances:

   A. Expressly provided by law.

   B. For the promotion of public interests.

   C. To prevent danger to the life, body, freedom, or property of the data subject.

   D. To prevent material harm to the rights and interests of others.

   E. Written consent has been obtained from the data subject.

7. Unless written consent has been obtained from the data subject or permitted by laws and regulations, personal data shall not be arbitrarily disclosed, sold, or used for purposes other than the specific purpose for which it was collected.

8. Where any department uses personal data for purposes other than the specific purpose in accordance with the proviso of Article 20 of the PDPA, it shall keep a record of the use of the personal data. The use of personal data shall not involve arbitrary linking of databases, nor shall it be abused.

9. For personal data not provided by the data subject, the data subject shall be informed before such data is processed or used, and such notification shall be completed within one year after the implementation of the Personal Data Protection Act. The notification may be made orally, in writing, by telephone, text message, email, fax, electronic document, or by other means sufficient to enable the data subject to know or reasonably become aware thereof.

10. When the specific purpose for which the Company retains personal data ceases to exist, the retention period expires, or the personal data is deleted, or the collection, processing, or use of personal data is ceased upon the request of the data subject, the department responsible for collecting the data shall submit the matter for approval and, upon approval, delete the personal data or cease its processing or use. However, this shall not apply where such action is necessary for the performance of official duties or business operations, or where the data subject has given written consent.

    For personal data that has been deleted or for which the collection, processing, or use has been ceased, the department responsible for the deletion shall maintain accurate records.

11. The use of instant messaging software or external email accounts (such as Yahoo Mail, Gmail, Hotmail, etc.) to transmit or access personal data files is prohibited. When transmitting personal data through the Company's internal email system (webmail), encryption protection shall be applied.

Article 5 Management of Personnel Handling Personal Data:

1. The department responsible for managing personal data files shall prevent personal data from being stolen, altered, damaged, lost, or leaked.
2. To strengthen the access security of information systems containing personal data files, prevent unauthorized access, and maintain the privacy of personal data, when a user is formally authorized to access personal data files, the user's account shall be unique to avoid the sharing of accounts.
3. Personnel who handle or have access to sensitive data shall fully perform their duty of confidentiality, and it shall be confirmed that their user identification accounts are canceled or deactivated upon their resignation or termination of contract.
4. Personnel are prohibited from publicly disclosing any personal data learned in the course of business through social networking websites, blogs, public forums, or other Internet-based means.

Article 6 If the Company encounters any theft, leakage, alteration, or other infringement of personal data as specified in Article 12 of the PDPA, after the facts have been investigated and confirmed, the Company shall notify the data subject of the fact of the personal data infringement and the response measures taken by oral notification, written notice, telephone, text message, email, fax, electronic document, or other means sufficient to enable the data subject to know thereof.

Article 7 Any matters not provided for herein shall be handled in accordance with the relevant provisions of the Personal Data Protection Act.

Article 8 These Regulations shall take effect upon approval by the Board of Directors. The same shall apply to any amendments thereto.

These Personal Data Protection Act were established on November 11, 2019.