
# Personal Data Protection

# Policy and Guidelines

# Charoen Pokphand Group

## Contents

# Personal Data Protection Policy and Guidelines

# Charoen Pokphand Group

## 1. Intent

Charoen Pokphand Group respects and values the human right to the protection of Personal Data owned by all directors, management, staff, customers, suppliers and business partners. Thus, Charoen Pokphand Group shall protect all Personal Data from possible misuse, and maintain such data security based on international laws and standards.

## 2. Scope

This Personal Data Protection Policy and Guidelines apply to Charoen Pokphand Group, (hereafter "the Group") which includes Charoen Pokphand Group Co., Ltd., and all of its subsidiary companies. The term "company" hereafter refers to any such company individually that has adopted this Personal Data Protection Policy and Guidelines. This document shall be reviewed at least once a year, or as conditions require.

## 3. Objectives

3.1 To ensure the security, reliability and protection of Personal Data owned by all directors, management, staff, customers, suppliers and business partners in every transaction with the Group.

3.2 To prevent the damage caused by misuse of Personal Data, as well as misuse of such data for monetary gain

## 4. Roles and Responsibilities

### 4.1 Board of Directors

4.1.1 Ensure that the Personal Data Protection Policy and Guidelines are in place.

4.1.2 Ensure that the policy and guidelines are properly implemented.

### 4.2 Management

4.2.1 Establish rules and procedures to suit the nature of the business, while remaining consistent with the Policy and Guidelines, relevant local data protection laws where the company operates, and international data protection standards.

4.2.2 Ensure that the organizational structure and related functions are in place.

4.2.3 Ensure there are selection procedures when hiring third parties with standardized data protection systems to handle Personal Data on behalf of the company.

4.2.4 Monitor the effective implementation of policy, guidelines, and regulations and identify areas for improvement, in addition to ensuring regular performance reports related to this Policy and Guidelines.

### 4.3 Data Protection Officer

4.3.1 Monitor and review the processing of Personal Data by the company to ensure compliance with the relevant data privacy laws, including to arrange awareness campaigns and training programs on the proper usage of Personal Data.

4.3.2 Advise and recommend the Board of Directors, management, and staff on the proper usage of Personal Data under the relevant local data protection laws.

4.3.3 Serve as the contact point for issues related to Personal Data and protection of the rights of data subjects, including coordinating and cooperating with the Office of the Personal Data Protection Commission.

4.3.4 Ensure the confidentiality of Personal Data obtained over the course of performing their duties.

### 4.4 Staff

4.4.1 Handle Personal Data with care, as well as maintain strict compliance with the relevant laws, rules and regulations.

4.4.2 Notify the Data Protection Officer in collecting Personal Data immediately in the event of any data breach

4.4.3 Notify the company through the relevant whistleblowing channels, if any failure to comply with this policy is found.

## 5. Guidelines

### 5.1 Collection of Personal Data

5.1.1 Collect Personal Data only according to the purpose notified to the Data Subject.

5.1.2 Do not collect Sensitive Personal Data that may cause discrimination or unfair bias to the data subject without their explicit consent, except if it is controlled under the law.

### 5.2 Storage of Personal Data

5.2.1 Security measures are required for all Personal Data storage locations to prevent the unauthorized access, use, modification, and disposal of said data, as well as to prevent Personal Data leak threats.

5.2.2 All Personal Data storage locations, including internal and Third-Parties, must have internationally-accepted data protection systems, and must only store Personal Data as appropriate for their intended usage in compliance with the relevant local data protection laws.

### 5.3 Transfer of Personal Data

5.3.1 Transfers of Personal Data require the consent or request to transfer from the Data Subject.

5.3.2 Transfers of Personal Data to a destination country are permitted under any of the following conditions:

1) The Data Subject has provided consent on the transfer and has been informed that the data protection standards at the destination country may be inadequate.
2) The Data Subject has requested the data transfer, or meets an obligation to a contract in which the Data Subject is a party.
3) The Data Subject is incapable of giving their consent, but the data transfer is necessary to prevent or suppress danger to the life, body, or health of the data subject.

### 5.4 Data Subject Rights

5.4.1 The Data Subject has the right to access or request a copy of their Personal Data.

5.4.2 The Data Subject has the right to request information on how their Personal Data was collected if no consent was provided.

5.4.3 The Data Subject has the right to notify the company in order to modify or change their Personal Data if they are inaccurate.

5.4.4 The Data Subject has the right to delete or destroy their Personal Data, or request the anonymization of the data, in accordance with relevant local data protection laws.

5.4.5 The Data Subject has the right to request the transfer of their Personal Data from one data controller to another controller.

5.4.6 The Data Subject has the right to restrict the usage of their Personal Data, in accordance with relevant local data protection laws.

5.4.7 The Data Subject has the right to object to the collection, usage or disclosure of their Personal Data.

5.4.8 The Data Subject has the right to file a complaint if the data usage is found to have infringed the stated purpose of collection.

### 5.5 Use or Disclosure of Personal Data

5.5.1 Do not use or disclose Personal Data that is different from the purposes set out by this Policy, in addition to disclosing to third parties, except if it is permitted under relevant local data protection laws.

5.5.2 All internal and Third Parties are prohibited from using Personal Data for illegal purposes, and must strictly adhere to guidelines contained in this Policy, including relevant local data protection laws in respective countries where the Group operates.

### 5.6 Disposal of Personal Data

5.6.1 In the event where stored Personal Data is not relevant or finished serving its purpose, or if the Data Subject has objected to or withdrew consent to the processing of their Personal Data, the said data shall be securely disposed of to prevent any potential data leakage.

5.6.2 Dispose and delete any stored Personal Data once the usage period has expired as initially agreed in the purpose of collection, except if required to comply with the relevant local data protection laws

### 5.7 Control of Personal Data

As a Data Controller, the Group must ensure the proper use of Personal Data by complying and applying the following data protection principles set out below:

1) The Data Subject is informed of the purpose of collecting their Personal Data, as well as their terms and rights, including to request their consent (if any) prior to collection, processing or disclosure.
2) Personal Data are collected, processed, and disclosed only as specified in the purpose notified to the Data Subject.
3) Measures are in place to prevent the use or disclosure of Personal Data without permission.
4) Security measures are established for the collection, use, disclosure and transfer of Personal Data, as well as ensure that the measures are properly

reviewed and updated to be compliant with the relevant local data protection laws.

5) Personal Data may only be modified or disposed of on request of the Data Subject.
6) Personal Data must be monitored and reviewed before deletion or destruction in the following cases:
    - The data storage period expires.
    - The data is irrelevant or unnecessary in relation to the purpose it was originally collected for.
    - The data subject requests the removal of their Personal Data or withdraws their consent.
7) Rights and restrictions on access to Personal Data are established.
8) Data subjects could access and review the list of all Personal Data collected by the company when requested.
9) Data Protection Officers and the Data Subject are informed immediately of any data breach.

### 5.8 Processing of Personal Data

The Group will ensure that, regardless if Personal Data is processed internally or by Third parties, the Group shall take appropriate actions with the aim of preventing such person from using or disclosing such Personal Data unlawfully or without authorization. These actions include the following:

1) Personal Data are collected, processed or disclosed only as specifically instructed by the Data Controller.
2) Data security measures are established to prevent the loss or the unauthorized use, modification and disclosure of Personal Data.
3) Records of all Personal Data usage are created and maintained on a regular basis.
4) Data Controllers are informed immediately of any data breach

### 5.9 Privacy Protection

In compliance with relevant local data protection law requirements, all of the Group's companies are required to provide a Privacy Notice to inform data subjects on the collection of their Personal Data. The Privacy Notice should contain at least the following details:

5.9.1 The target groups and Personal Data Sources the company may collect Personal Data from, including customers, suppliers, employees, job applicants, share/securities holders, and third parties.

5.9.2 The purpose of collecting Personal Data from the Data Subject, and method of collection.

5.9.3 The types of Personal Data to be collected, including name, physical address, telephone number, email address, IP address etc.

5.9.4 The length of time the Personal Data is stored by the company.

5.9.5 The rights entitled to the Data Subject.

5.9.6 The option for Data Subject to confirm or withdraw their consent to the storage of their Personal Data.

5.9.7 The measures to maintain the security of the Data Subject's Personal Data.

5.9.8 The contact information of the Data Controller or the Data Protection Officer (if available), so Data Subjects may contact for inquiries related to the website's use of personal data or exercise their rights.

5.9.9 The outside persons or juristic persons that may have access to the Personal Data.

5.9.10 The company's Cookie Policy, if the company collects Personal Data through a website or application.

## 6. Training

The Company shall communicate the Personal Data Protection Policy and Guidelines and cascade it through training programs, conferences, and other appropriate channels to its directors,

management, and staff. The effectiveness of such training and communications programs shall be evaluated on a regular basis.

## 7. Whistleblowing

In case a violation of this Personal Data Protection Policy and Guidelines is found, a report must be filed by following the procedure stated in the Whistleblowing Policy and Guidelines. The information of complainant or whistleblower will be protected and the information will be kept confidential during the investigation and after the completion of the investigation process.

## 8. Policy Advice

In case of suspicion on the action that may violate laws, regulations and this Personal Data Protection Policy and Guidelines, the employee can seek advice from her or his supervisors; team or persons responsible for protecting personal data within the Company, the Compliance Department or Legal Department before making any decision or carrying out any action.

## 9. Penalties

In the event of an investigation, all employees must fully cooperate with internal and external entities. If an employee violates or fails to comply with this Policy and Guidelines, either directly or indirectly, the employee will be subject to disciplinary action in accordance with Company's regulations.

## 10. Related Laws, Regulations, and Policies

10.1 Relevant local data protection laws in countries where the Group operates

10.2 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

10.3 Guidelines for the Regulation of Computerized Personal Data Files by the Office of the United Nations High Commissioner for Human Rights (OHCHR)

## 11. Appendix

The following appendix is attached to this Policy and Guidelines:

11.1 Appendix A: Definitions

# Appendix A

# Definitions

**Personal Data**

Any data of a living person that enables the identification of such person, whether directly or indirectly (excluding data of deceased persons).

**Data Controller**

A person or a juristic person having the power and duties to make decisions regarding the collection, usage or disclosure of Personal Data.

**Data Processor**

A person or a juristic person who operates in relation to the collection, usage or disclosure of Personal Data, pursuant to the orders given by or on behalf of a Data Controller, whereby such person or juristic person is not the Data Controller.

**Data Subject**

The person identified by the Personal Data.

**Sensitive Personal Data**

A specific set of Personal Data that is prohibited from collection without explicit consent from the Data Subject due to the risk of improper discriminatory use, and therefore must be treated with extra security. This includes ethnicity, race, skin color, political opinions, religious beliefs, sexual orientation, criminal convictions, personal health information, disability and trade union membership, genetic and biometric data, as well any other data classified as such under relevant local data protection laws.

**Personal Data Source**

The initial location where the Data Subject has provided Personal Data to the company, which includes the following cases:

- Contacting the company for business or any other inquiries, or submitting a comment through the company's website, application, telephone, email, in person or other method
- Participating in the company's promotional marketing campaigns, sweepstakes, and other related events

- Receiving a service provided through the company website, application or an e-Commerce service provider
- Accessing personal data from publicly-available sources, including business sources, commercial sources and social media, regardless if the Data Subject has disclosed these sources in person or has permitted the above sources to disclose them on their behalf
- Accessing personal data from third-parties, including from family members, emergency contacts, beneficiaries, job guarantors, employment websites, reference persons, state agencies, educational institutions, securities depositories, banks or bond dealers, regardless if the Data Subject has disclosed these sources in person or has permitted another person to disclose them on their behalf
- Providing supporting documents for a business or work contract with the company
- Providing supporting documents for a job application at the company
- Appearing in captured videos or images through CCTV cameras within company premises
- Visiting the company website, regardless if it is intentionally or not

**Third-parties**

Natural or juristic persons outside the Data Subject, Data Controller and Data Processor who are authorized to process Personal Data on behalf of the Group

**Data Protection Officer (DPO)**

The person appointed to advise and monitor Data Controllers and Data Processors to ensure compliance with relevant local data protection laws.

**Privacy Notice**

A document that inform the Data Subject on how the company gathers, uses, discloses and manages their Personal Data.

**Cookie**

a unique file created by a website stored on the user's computer or mobile device, and designed to collect the user's personal information, activities or preferences for the purpose of improving user experience while using the website.