Chailease Holding Company Limited
Personal Information Protection Policy

Confidential document

Approved by the Board of Directors on August 12, 2020

Approved by the Board of Directors on May 28, 2021

Article 1 Purpose

In order to strengthen the personal information protection and management system of Chailease Holding Company Limited (hereinafter referred to as "the Company") and its subsidiaries, reduce operational risks, and protect the rights of data subjects, the Company hereby promulgates “Chailease Holding Company Limited Personal Information Protection Policy” (hereinafter referred to as “this Policy”) in accordance with the provisions of the Republic of China Personal Data Protection Act, to establish a consistent standards of conduct of the Company and its subsidiaries.

Article 2 Scope of application

The Policy applies to the Company and its subsidiaries, affiliates and branches (hereinafter collectively referred to as “Subsidiaries” or “Subsidiary”) and the employees of the aforementioned companies or branches, unless otherwise provided by other applicable laws and regulations. Employees of the Company and Subsidiaries are still bound to fulfill their obligations with regard to personal information protection even after the employment relationship has been terminated.

Contract/temporary staff assigned to provide service at the Company's and Subsidiaries' premises by human resource agencies or manufacturers, suppliers, and their employees or contingent workers that do business with the Company or its Subsidiaries shall also comply with this policy under the Personal Information Protection Act.

In compliance with local laws and regulations, Subsidiaries shall implement this Policy and other measures consistent with the Company. If the Policy does not conflict but vary with the laws and regulations of personal information protection of the country or jurisdiction where a Subsidiary is registered, the Subsidiary should choose the stricter standards as the basis for compliance. If the Policy conflicts with the local laws, regulations or the requirements of the competent authorities of the place where the Subsidiaries are registered, a Subsidiary shall notify the Company and its responsible officer of such regulatory conflict and seek to resolve such conflicts.

Article 3 Organization and Responsibilities

The Legal Division of the Company is the dedicated unit for personal information protection and management system. The dedicated unit shall be given full authority to coordinate and supervise the protection and management of personal information.

The dedicated unit shall report to the board of directors at least every year. If there is any serious violation of the laws and regulations on personal information protection, the dedicated unit shall report to the board of directors immediately.

Article 4 Definitions

The terms used herein denote the following meanings:

1. "personal data" refers to the personal data defined in accordance with the Personal Data Protection Act of the Republic of China and its enforcement rules and relevant business laws;
2. "personal data file" refers to a collection of personal data structured to facilitate data retrieval and management by automated or non-automated means;
3. "collection" refers to the act of collecting personal data in any way;
4. "processing" refers to 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;
5. "use" refers to the act of using personal data via any methods other than processing;
6. "cross-border transfer" refers to the cross-border processing or use of personal data;
7. "Personal data protection management system" refers to the establishment, operation, supervision, inspection, maintenance and improvement of the structure and system of personal data protection management.
8. "Incidents of personal data infringement" refers to use of personal data without authorization or illegal collection, processing, use of personal data or other infringement of the rights of the parties.

Article 5 The collection, processing and use of personal data

The collection, processing and use of personal data shall be carried out by the Company and its Subsidiaries in a way that respects the data subject's rights and interest, shall not exceed the necessary scope of specific purposes, and shall have legitimate and reasonable connections with the purposes of

collection in the following manner:

1. The collection or processing of personal data shall be for specific purposes and on one of the following bases:

    a. where it is expressly required by law;

    b. where there is a contractual or quasi-contractual relationship between the non-government agency and the data subject, and proper security measures have been adopted to ensure the security of the personal data;

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

    d. where consent has been given by the data subject;

    e. where it is necessary for furthering public interest;

    f. where the rights and interests of the data subject will not be infringed upon.

    The Companies and its Subsidiaries shall, on its own initiative or upon the request of the data subject, erase or cease processing or using the personal data when it becomes aware of, or upon being notified by the data subject, that the processing or use of the personal data should be prohibited.

2. The Companies and its Subsidiaries shall expressly inform the data subject of the following information when colleting their personal data unless it meets the requirements specified in Item 4 of this Article:

    a. the name of the Companies or the Subsidiaries;

    b. the purpose of the collection;

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

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

    e. the data subject's rights under this Article and the methods for exercising such rights; and

    f. the data subject's rights and interests that will be affected if he/she elects not to provide his/her personal data.

3. The Companies and its Subsidiaries shall, before processing or using the personal data collected in accordance was not provided by the data subject, inform the data subject of its source of data. The obligation to inform may be performed at the time of the first use of the personal data towards the data subject.

4. The Company and its Subsidiaries 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:
    a. where it is expressly required by law;
    b. where it is necessary for furthering public interests;
    c. where it is to prevent harm on life, body, freedom, or property of the data subject;
    d. where it is to prevent material harm on the rights and interests of others;
    e. where consent has been given by the data subject; or
    f. where it is for the data subject's rights and interests.
5. When the Companies or its Subsidiaries uses personal data for marketing purpose pursuant to the preceding paragraph, upon the data subject's objection to such use, the Companies or its Subsidiaries shall cease using the data subject's personal data for marketing. When using the data subject’s personal data for marketing purpose for the first time, the Companies or its Subsidiaries shall provide the data subject of the ways that he/she can object to such use, and the agency shall pay for the fees therefrom.
6. Upon the request of a data subject, the Companies or its Subsidiaries 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:
    a. where national security, diplomatic or military secrets, overall economic interests or other material national interests may be harmed;
    b. where a government agency may be prevented from performing its statutory duties; or
    c. where the material interests of the data collectors or any third parties may be adversely affected.
7. The Companies or its Subsidiaries 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.
8. In the event of a dispute regarding the accuracy of the personal data, the Companies and its Subsidiaries 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 to by the data subject in writing, and the dispute has been recorded.
9. When the specific purpose of data collection no longer exists, or upon expiration of the relevant

time period, the government or non-government agency 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 to by the data subject in writing.

10. the Companies and its Subsidiaries 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 this Policy.

Article 6 Education and Training

The Company and its Subsidiaries shall conduct education and training sessions supplemented by actual cases to enable all employees to understand and strengthen the personal information protection and management system.

Article 7 Notification mechanisms

Each Subsidiary shall be responsible for the collection, processing, utilization and holding of personal data. The unit responsible for personal data protection of each Subsidiary shall implement personal information protection system in accordance with this Policy and the relevant regulations.

Each Subsidiary shall allocate personal data protection management personnel and incorporate the operation of the personal data protection management system into the supervision and internal control system. If any major violation of laws and regulations related to the protection of personal data is found, it shall be reported to the responsible unit for personal data management of the Company immediately.

Article 8 Record Keeping

The Company and its Subsidiaries shall duly establish relevant record or file safekeeping procedures related to the collection, processing and use of personal data, including but not limited to files or relevant transaction records, and transaction monitoring records and filing materials.

Article 9 Notification of Data Subjects

If any personal data is stolen, disclosed, altered, or otherwise infringed upon due to a violation of this

Policy by the Company or its Subsidiaries, the data subject shall be notified via appropriate means after the relevant facts have been clarified.

Article 10 Policy Violation Procedure

If the personnel of the Company or its Subsidiaries violate the provisions of this Policy and causes personal data to be illegally collected, processed, used, or otherwise infringe on the rights of data subjects, the personnel and his/her supervisors punished in accordance with the Company's work rules and relevant regulations base on the severity of the circumstances. The Company or its Subsidiaries shall also review the Company's existing work regulations, procedures, inspection mechanisms, and education and training advocacy on a case-by-case basis to evaluate whether they are adequate or should be further strengthened.

If the aforementioned violation is determined by the court that the Company should be liable for damages, in addition to compensating in accordance with the law, the company may also initiate civil and criminal proceedings against the personnel who violated this Policy (whether or not he/she has resigned).

Article 11 Internal and Independent Third Party Audit

The auditing unit of the Company and its Subsidiaries shall, in accordance with the regulations, assess whether the personal information protection systems meet regulatory requirements and have duly implemented. Each Subsidiary may, in accordance with actual needs, engage an independent third party to examine the matters specified in the preceding paragraph and provide an audit opinion.

Article 12 Personal Data Processing Measures

Each subsidiary shall establish the "Personal Data Processing Measures" in accordance with this Policy and authorize the general manager of each subsidiary to approve and revise the processing measures.

Article 13 Miscellaneous

Matters not covered in this Policy shall be handled in accordance with the provisions of the Republic of China Personal Data Protection Act.

Article 14 Approved Level

This Policy, including its amendments, is effective upon approval of the Board of Directors.