TCL Zhonghuan Renewable Energy Technology Co., Ltd.

Privacy Protection Policy

1. Introduction

As a global leader in the new energy photovoltaic (PV) industry, TCL Zhonghuan Renewable Energy Technology Co., Ltd. and its subsidiaries (hereinafter referred to as “TCL Zhonghuan”, “we” or “the Company”) have consistently put the philosophy of privacy protection and data security into practice. We actively respond to international privacy protection laws and standards, commit to conducting data processing and management in a responsible manner, and are committed to working alongside all stakeholders to jointly create corporate, social and data security value.

2. Scope

This Policy applies to TCL Zhonghuan’ s headquarters and all of its wholly-owned and controlled subsidiaries. All directors, senior management and employees of the Company are required to comply strictly with this Policy. At the same time, we encourage external strategic partners, upstream suppliers and downstream channel partners to comply with this Policy.

3. Commitments

TCL Zhonghuan attaches great importance to the privacy protection of its employees, customers, partners and suppliers (hereinafter collectively referred to as “data subjects”). We commit to providing data subjects with a secure, transparent and protected data processing environment. We adhere to strict data privacy protection principles, firmly oppose any unauthorized access to, use of or disclosure of data, and ensure that data subjects’ personal information is fully protected.

We are committed to complying with all relevant privacy protection laws and regulations, ensuring that data subjects enjoy the rights to be informed, to access, to rectify and to erase their information, so as to safeguard their privacy rights, and ensuring that the products and services provided by the Company do not involve any privacy infringement or data misuse.

The Company has built a robust information security management system to support the privacy protection of data subjects, and has incorporated its information security and privacy protection policy system into the Company's overall risk and compliance management.

In 2023, all of the Company's IT infrastructure and information systems obtained ISO 27001 certification. To ensure the effective operation of the system, the Company conducts monthly internal audits of the information security management system and of privacy protection compliance, performs quarterly system vulnerability scans and industrial control traffic analysis, conducts a cybersecurity attack and defense drill every six months, and carries out an annual external third-party audit of the information security management system and privacy protection compliance, so as to ensure the effectiveness of the Company's information security management system and privacy protection policy.

Using 2023 as the base year, the Company commits to achieving, by 2030, the core control targets of maintaining the validity of its information security management system certification each year and keeping the rate of major information security incidents at zero each year, so as to continuously strengthen its information security risk prevention and control capabilities.

4. Strategies

4.1 Management Structure

The Company has established the Digital Transformation Committee (hereinafter referred to as the "DTC"), which is responsible for formulating the overall digitalization strategy and guiding principles. The General Manager serves as the primary responsible person of the Committee (the person in charge at the highest decision-making level) and as the person ultimately responsible for the digitalization strategy, data privacy and cybersecurity. The DTC has established an Information Security Technology Team, which is responsible for implementing the Company's information security and privacy protection policies and systems, monitoring information security and privacy management, and ensuring the Company's compliance in data processing, information sharing and privacy protection.

4.2 Collection and Use of Privacy Information

In the course of human resources management, business cooperation and customer service, the Company collects the necessary information of employees, partners, suppliers and customers:

(1) For employees, the Company collects information including name, gender, date of birth, ID number, contact details, address, position, salary, bank account, network usage records, real-time traffic and facial data;

(2) For partners and suppliers, the Company collects information such as company name, contact person's name, contact details and bank account;

(3) For customers, the Company collects information such as name, contact details, ID number, photo and vehicle license plate number.

We have formulated and made public the Privacy Statement to inform customers and other parties whose information is collected of Zhonghuan's privacy protection practices, including the nature of the information to be collected; the purposes for which the information is used; and the fact that the parties whose information is collected may decide for themselves how their private data is collected, used, retained and processed (we provide users with the option to refuse or accept the collection of information, provide users with channels to access their personal information, and transfer their data to other service providers at the request of the parties whose information is collected); as well as the requirements for sharing, transferring and disclosing users' personal information to third parties (in both the private and public sectors). All collection of privacy information is authorized in advance by the relevant persons, kept strictly confidential, and used only by the relevant departments; it will not be used for other purposes without consent. We closely track and monitor the secondary use of personal information, prevent any information leakage incidents, and strictly safeguard information security.

4.3 Retention of Privacy Information

The Company's retention periods for privacy information vary according to the different subjects and circumstances:

(1) For job candidates who are not hired, their personal privacy information is retained only during the recruitment period; the privacy information of current and former employees is retained during their term of employment and stored for more than two years after they leave.

(2) The privacy information of partners and suppliers is retained during the cooperation period and for five years after its termination.

(3) The privacy information of customers is retained during the business relationship and for two years after its termination.

Where required by law or where there are unresolved legal matters, the retention period will be extended until the relevant matters are resolved.

4.4 Privacy Information Protection Measures

The Company protects the security of privacy information through physical and technical means:

(1) In terms of physical protection, all archives and servers storing privacy information are located in secure office premises and accessible only to authorized personnel.

(2) In terms of technical protection, security devices (such as firewalls) are used to protect electronic data, and privacy information is transmitted in encrypted form through the Company's designated document encryption system, so as to ensure security and traceability during transmission.

4.5 Cross-Border Data Transfer

When transferring data subjects' privacy information overseas for business needs, the Company will strictly comply with the cross-border data transfer laws and regulations applicable in China and the relevant countries and regions, complete the necessary security assessment, filing or certification procedures, and sign the corresponding data protection agreements with overseas recipients, clearly defining the data protection responsibilities and obligations of both parties. We conduct cross-border data transfers only where there is a lawful basis and where adequate security safeguards (such as data encryption and access control) are in place, so as to ensure that privacy information receives, throughout its cross-border flow, a level of protection no lower than that stipulated in this Policy.

4.6 Destruction of Privacy Information

When the retention period for the privacy information of employees, partners, suppliers and customers expires, or when the relevant party requests the deletion of their privacy information, the Company will securely destroy or anonymize such privacy information. The destruction of privacy information is carried out by a professional destruction

organization, and the form of destruction may, depending on the type of privacy information, include physical destruction, data erasure and other compliant methods.

4.7 Third-Party Disclosure

The Company will not sell or rent the personal information of relevant parties to third parties. Personal information may be shared with private entities only with the explicit consent of the relevant party, where necessary to provide products or services, or in the event of a merger, acquisition or sale of assets by the Company, and with appropriate information protection measures in place.

In accordance with laws and regulations, the Company may disclose personal information to government agencies, law enforcement authorities or other public entities, particularly in matters involving national security, public safety, legal proceedings or as otherwise provided by law, where the Company is obliged to cooperate with investigations and disclose the necessary personal information.

4.8 Information Access and Update

Relevant parties have the right to access and update their personal information, and may request that the Company delete inaccurate or outdated information. Relevant parties may exercise these rights by contacting the Company's designated privacy protection officer.

4.9 Complaints and Penalties

We continuously improve our existing internal reporting and communication mechanisms and channels through which employees, partners, suppliers and other relevant parties can report privacy protection-related issues, and we have established effective oversight mechanisms to regularly review and improve our privacy protection practices. We encourage any relevant party to report any privacy infringement to us, either directly to a supervisor or to the Company's Audit Department, or through the telephone number or email address below.

Tel: 022-23789766-8022

Email: jubao@tzeco.com

Address: No. 10 Haitai South Road, Huayuan Industrial Park, Xiqing District, Tianjin

The Company supports anonymous reporting and commits to keeping whistleblowers' personal information strictly confidential and effectively safeguarding their lawful rights.

The Company strictly prohibits any direct or indirect discrimination, obstruction, suppression or retaliation against whistleblowers.

For any violation of this Policy or of the laws and regulations relating to information security and privacy protection, we adopt a zero-tolerance approach, promptly conducting investigations and taking corrective action against unlawful or non-compliant conduct, and imposing corresponding disciplinary sanctions on the responsible departments and personnel according to the degree and scope of the impact caused by the incident.

4.10 Education and Training

The Company regularly organizes privacy protection training for all employees to ensure that they fully understand and comply with the Company's privacy protection policies and operational procedures.

5. Policy Review and Revision

The Board of Directors is the highest decision-making and supervisory body for the Company's privacy protection management. The issuance of this Policy and the commitments contained herein has been endorsed by the Company's senior management. The Company shall formally review this Policy at least once a year. The review shall take into account changes in applicable laws, regulations and regulatory requirements; updates to international standards and industry guidelines; changes in customer requirements; and adjustments to the Company's relevant internal policies. Based on the review results and actual needs, the Company shall revise this Policy as appropriate to ensure that it remains current and applicable.

This Policy is published on TCL Zhonghuan's official website for reference by all stakeholders. Its implementation and the related key performance indicators are disclosed annually in the Company's sustainability report.