

TZE Privacy Protection Policy

1. Introduction

As a global leading new energy photovoltaic enterprise, TCL Zhonghuan Renewable Energy Technology Co.,Ltd. and its subsidiaries (referred to as "TZE", "we", "us" and "the company") have always practiced the concepts of privacy protection and data security, actively responded to international privacy protection regulations and standards, committed to responsible data processing and management, and endeavored to work together with all stakeholders to realize the co-creation of corporate value, social value and data security value.

2. Scope

We will ensure that the Privacy Protection Policy is effectively implemented within TZE and its subsidiaries, and that the policy applies to all of the company's employees, production operations, products and services, and encourage more partners, including suppliers, to comply with this policy.

3. Commitments

TZE attaches great importance to the privacy of our employees, customers, partners and suppliers. We are committed to providing our users with a secure, transparent and protected data processing environment. We adhere to strict data privacy protection principles, and firmly oppose any unauthorized access, use or disclosure of data to ensure that users' personal information is fully protected. We are committed to complying with all relevant privacy protection laws and regulations to ensure that users enjoy the right to know, access, rectification and deletion in order to safeguard their privacy rights, and to ensure that the products and services provided by the company do not involve any invasion of privacy or data abuse.

The company has built a comprehensive information security management system to support the privacy protection of employees, customers, partners and suppliers, and has integrated the information security and privacy protection policy system into the overall risk and compliance management of the whole company. 2023, all IT infrastructure and information systems of the headquarter have been certified by the ISO 27001 system; in order to ensure that the system operates efficiently and effectively, the company conducts monthly audits of the To ensure the effective operation of the system, the company conducts internal audits of the information security management system and privacy protection compliance on a monthly basis, conducts system vulnerability scanning and industrial control traffic analysis on a quarterly basis, conducts cybersecurity attack and defense drills on a semi-annual basis, and conducts external third-party audits of the information security management system and privacy

protection compliance on a yearly basis, so as to ensure the effectiveness of the company's information security management system and privacy protection policy.

4. Strategy

4.1 Management Structure

The company has established a Digital Transformation Committee (hereinafter referred to as the "Digital Committee"), which is responsible for formulating the overall digital strategy and guiding principles, with the General Manager serving as the main person responsible for the Committee (the person in charge of the highest decision-making level), as the top person in charge of digital strategy, data privacy and cybersecurity. The Information Security Technology Group under the Data Committee is responsible for implementing the company's policies and systems related to information security and privacy protection, 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 Private Information

During human resource management, business cooperation and customer service, the company will collect necessary information about its employees, partners, suppliers and customers:

(1) For employees, the company will collect information including name, gender, date of birth, ID number, contact information, address, position, salary, bank account, internet usage traces, real-time traffic and face;

(2) For partners and suppliers, the company will collect information including company name, contact name, contact details and bank account;

(3) For customers, the company will collect information such as name, contact information, ID number, photo and license plate number.

We formulate and make public our Privacy Statement to inform our customers and other information collectors about TZE's privacy practices, including the nature of the information to be collected; the purposes for which the information is to be used; how the information collectors may collect, use, retain and process private data at their own discretion (we provide users with the option to opt out of the collection of information or to accept the collection of information, we open up access channels for users' personal information, transfer their data to other service providers upon the request of information collectors, etc.); requirements for sharing, transferring and disclosing users' personal information to third parties (private and public sector), etc. We provide users with the option to refuse or accept the collection of information, provide users with access to their personal information, transfer their data to other service providers at the

request of the party from whom the information was collected, etc.); requirements to share, transfer and disclose the user's personal information to third parties (private and public sector), etc.

All private information is collected with the prior authorization of the person concerned, is kept strictly confidential, is restricted to the use of the relevant department, and will not be used for any other purpose without consent. We closely track and monitor the secondary use of personal information to prevent any incident of information leakage and strictly safeguard information security.

4.3 Privacy Information Preservation

The company's retention period for private information varies according to different targets and circumstances:

(1) For candidates for employment, if they are not on board, their private information is kept only during the recruitment period; the private information of current and former employees is kept during the performance of their duties and stored for more than two years after termination.

(2) Partners' and suppliers' private information is stored during the period of cooperation and for five years after termination.

(3) Private information of customers is stored during the business relationship and for two years after termination.

If there are legal requirements or unresolved legal matters, the information retention period will be extended until the relevant matters are resolved.

4.4 Privacy Information Protection

The company protects the security of private information through physical and technical means:

(1) In terms of physical protection, all files and servers where private information is stored are located in a secure office space and access is restricted to authorized personnel.

(2) In terms of technical protection, we use security equipment (such as firewalls) to protect electronic data, and encrypt the transmission of private information through a document encryption system designated by the company to ensure security and traceability during transmission.

4.5 Privacy Information Destruction

When the retention period of the private information of employees, partners, suppliers and customers expires or when the parties concerned with the information

request the deletion of their private information, the company will securely destroy or anonymize their private information. The destruction of private information is carried out by a professional destruction organization, and the forms of destruction may include physical destruction, data erasure, and other compliant methods, depending on the type of private information.

4.6 Third-Party Disclosures

The company does not sell or rent personal information about parties to third parties. The sharing of personal information to private entities is permitted only with the express consent of the party to whom the information relates, when necessary to provide products or services, or in the event of a merger, acquisition or sale of assets by the company, and to ensure that information protection measures are in place.

The company may disclose personal information to government agencies, law enforcement or other public entities as required by laws and regulations, especially in cases involving national security, public safety, legal proceedings or other legal requirements, and the company is obligated to cooperate with investigations and disclose necessary personal information.

4.7 Information Access and Updates

Information related parties have the right to access and update their personal information and may request that the company delete inaccurate or outdated information. Relevant parties can exercise these rights by contacting the person in charge of privacy protection designated by the company.

4.8 Complaints and Penalties

We continue to improve our existing internal reporting and communication mechanisms and channels for employees, partners, suppliers and other relevant parties to report privacy protection related issues, and establish an effective monitoring mechanism to review and improve our privacy protection practices on a regular basis. We encourage any relevant parties to report any privacy violations to us, either directly to the supervisor, the Audit Department, or through the following phone numbers and email addresses.

Tel: 022-23789766-8022

E-mail: jubao@tzeco.com

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

We will strictly keep the personal information of the informant confidential, and effectively protect the legitimate rights of the informant, the company is strictly prohibited from engaging in any direct or indirect discrimination, difficulties,

suppression or retaliation against the informant and other behaviors.

For any violation of this policy as well as information security and privacy protection related laws and regulations, we take a zero-tolerance attitude, conduct timely investigations and corrective actions on violations, and according to the degree and scope of the impact of the incident, for the department and personnel responsible for the appropriate disciplinary action.

4.9 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 operating procedures.

5. Policy Review and Revision

This policy was approved by the company's General Manager in July 2024 and this Privacy Policy will be updated and revised in due course or at least every three years.

This policy is published on TZE's website for all stakeholders to review, and the implementation of the policy will be disclosed annually in the company's Sustainability Report.

TCL Zhonghuan Renewable Energy Technology Co., Ltd.
General Manager SHEN Haoping
July 2024