# Trina Solar Co., Ltd

# Personal Data Protection Management Policy

| | |
|---|---|
| **Responsible Department:** | **Information Security Department, Compliance Management Department** |
| **Supporting Department:** | **Legal Department, Human Resources Department** |
| **Approved By:** | **GRC** |
| **Document No.:** | **TSL-CM-008** |
| **Effective Date:** | **2024-08-12** |

# 1. Purpose

This Policy is established to respect and protect the privacy rights of individuals, to ensure that the purpose of personal data collection, retention, use, processing, transfer, provision, public disclosure, deletion, and other activities align with the intentions of the personal data subjects and comply with the requirements of laws and regulations.

# 2. Scope

This Policy applies to the personal data protection and compliance management of Trina Solar Co., Ltd. (hereinafter referred to as the “Company”), its branches, and subsidiaries. For entities outside of the Chinese mainland, the implementation shall be based on the principles outlined in this Policy, along with relevant provisions of applicable laws and regulations.

This Policy is formulated in accordance with the applicable personal data protection requirements (including but not limited to the Chinese Personal Information Protection Law, the European General Data Protection Regulation, the California Consumer Protection Act, and other legal and regulatory requirements) where the Company operates.

The Company shall require all third parties, such as suppliers, contractors, consultants, or vendors who access, handle, use, operate, and store Trina Solar's personal data to comply with the requirements outlined in this Policy.

# 3. Definition

| Description | Definition |
|---|---|
| **Personal Data** | All kinds of information recorded electronically or by other means relating to an identified or identifiable natural person, excluding information that has been anonymized. |
| **Sensitive Personal Data** | Personal data that, once leaked or illegally used, can easily lead to the infringement of a natural person's human dignity or jeopardize his or her personal or property safety, including information on biometrics, racial origin, religious beliefs, specific identities, medical and health care, financial accounts, traces, and personal data on minors under the age of 14. |
| **Personal Data Subject(s)** | The specific natural persons who can be identified by personal data, including customers, suppliers, employees, etc. |
| **Personal Data Processor(s)** | Organs, enterprises, public institutions, social organizations, and other organizations that collect, store, use, process, transfer, provide, disclose, and delete personal data. |

| | |
|---|---|
| **Handle** | The operations performed on Personal Data, including but not limited to the collection, storage, use, processing, transfer, provision, disclosure, deletion, and disposal of such data. |
| **Collect** | Any act of capturing Personal Data. |
| **Use** | Any act of using Personal Data. |
| **Process** | A series of processing activities for Personal Data, including but not limited to collection, identification, screening, classification, sorting, analysis, reconstruction, storage, transmission, retrieval, and display. |
| **Provide** | The acts of a Personal Data Processor entrusting a third party to handle Personal Data and other acts of handling Personal Data for certain interests. |

# 4. Content of Management

## 4.1 Basic Principles of Personal Data Protection

1. **Principle of Consistency of Authority and Responsibility.** The Personal Data Processor shall be responsible for the handling of Personal Data and the damage caused to the legitimate rights and interests of the Personal Data Subjects.

2. **Principle of Explicit Purpose.** The purpose of Personal Data handling should be lawful, legitimate, necessary, and clear.

3. **Principle of Informed Consent.** The purpose, method, scope, and rules of Personal Data handling shall be clearly stated to the Personal Data Subjects, seeking their authorization and consent or having other legal grounds.

4. **Principle of Minimum Necessity.** Unless otherwise agreed with the Personal Data Subject or there are other legal grounds, only the minimum types and amount of Personal Data necessary to fulfill the authorized purpose shall be handled. Once the intended purpose has been achieved, the Personal Data shall be promptly deleted or anonymized as agreed.

5. **Principle of Openness and Transparency.** The scope, purpose, and rules for handling Personal Data shall be disclosed in a clear, understandable, and reasonable manner, and shall be subject to external supervision.

6. **Principle of Security Assurance.** Security capabilities that are proportionate to the security risks faced shall be established, along with adequate administrative measures and technical safeguards, to ensure the confidentiality, integrity, and availability of Personal Data.

7. **Principle of Subject Participation.** Personal Data Subjects shall be provided with methods to access and correct their Personal Data, withdraw consent, and deactivate their accounts.

## 4.2 Collection of Personal Data

1. The types of Personal Data collected by the Company typically include, but are not limited to the individual's name, photo, identification number, phone number, email address, and mailing address, depending on the specific context and purpose of collection. Prior to collecting any Personal Data, the Company shall inform the Personal Data Subjects clearly about the nature of the Personal Data being collected, the purpose of collection, the methods used, the scope of handling, and any third parties involved.

2. All activities involving Personal Data Collection shall be conducted for lawful, legitimate, explicit, and reasonable purposes, using lawful means.

3. All activities involving Personal Data Collection shall have a valid legal basis. Personal Data Subjects shall be informed about the purpose of the data handling, the methods used, the types of Personal Data collected, and the retention period. The Personal Data collected shall be limited to the minimum necessary to achieve the stated purpose of handling. The specific legal basis may vary depending on Personal Data Subjects, handling purpose, method, and applicable legal provisions of Personal Data. The Company may handle Personal Data only under any of the following circumstances:

    1) obtaining the individual's opt-in consent;

    2) handling Personal Data as necessary for the conclusion and performance of contracts with customers/suppliers;

    3) handling employees' Personal Data as necessary for the conclusion and performance of contracts signed with employees, or necessary for the implementation of human resource management in accordance with labor rules formulated and collective contracts signed in compliance with applicable laws;

    4) necessary for the performance of statutory duties or obligations;

    5) necessary for responding to public health emergencies or protecting an individual's life, health, and property safety in urgent situations;

    6) other legal ground as prescribed by relevant laws.

4. Collection and Handling of Sensitive Personal Data

1) Sensitive Personal Data may only be collected and handled when there is a specific purpose, a clear necessity, and strict protective measures are in place.

2) The collection and handling of Personal Data shall obtain the Personal Data Subject's separate consent or have other legal ground; If laws or regulations mandate written consent for handling such Personal Data, those requirements will take precedence.

3) Personal Data Subjects should be informed of the necessity of handling Sensitive Personal Data and the impact on their rights and interests, unless disclosure is mandated by law.

5. When the circumstances related to the collection and handling of Personal Data change, the Personal Data Subject's consent must be re-obtained or an alternative legal ground must be provided.

## 4.3 Retention of Personal Data

1. Personal Data collected shall be safeguarded with suitable technical and administrative measures to prevent leaks, destruction, alterations, or unauthorized access, and ensure its security and confidentiality.

2. The roles and responsibilities of personnel managing Personal Data must be clearly defined, with increased supervision and management to prevent unauthorized access.

3. While storing Personal Data, the Company shall ensure that the data remains accurate, complete, and up-to-date.

4. A reasonable retention period for Personal Data shall be established and communicated to Personal Data Subjects, ensuring that it aligns with the minimum duration required to fulfill the purpose or comply with applicable laws and regulations.

## 4.4 Use of Personal Data

1. When using Personal Data, the Company shall strictly comply with laws and regulations, clearly define the purpose of use, and limit usage to the scope authorized by the Personal Data Subject or within legally justified boundaries.

2. Personal Data must not be used for illegal activities, trading, or any purposes that violate laws and regulations.

3. The Company shall implement classified and graded management measures for Personal Data based on its data classification and grading processes, ensuring that personnel may only access and use Personal Data within their authorized scope.

4. If the authorized use of Personal Data exceeds its original scope, or if the purpose for using that Personal Data changes, the Company shall re-obtain consent from the Personal Data Subject or have other legal grounds.

## 4.5 Cross-border Transfers of Personal Data

To ensure that the cross-border transfer of Personal Data aligns with the original purpose for which it was collected, handled, and used, the Company shall re-obtain the Personal Data Subject's separate consent or have other legal grounds. The Company shall also implement appropriate safeguards in accordance with this Policy and the applicable laws and regulations governing cross-border transfers of Personal Data in the jurisdictions where the Company operates and conducts business.

## 4.6 Provision of Personal Data

**1. Entrusting the Handling of Personal Data**

1) When the Company entrusts a third party to handle Personal Data, it shall establish agreements with the entrusted party on the purpose, duration, methods, types of Personal Data involved, protection measures, and the rights and obligations of both parties. The Company shall supervise the entrusted party's Personal Data handling activities.

2) Without the Company's consent, the entrusted processor shall not subcontract the handling of Personal Data to another party. The entrusted processor shall handle Personal Data in accordance with the agreement and shall not handle Personal Data beyond the agreed-upon handling purpose, methods, etc.

2. **Transfer of Personal Data.** If the Company needs to transfer Personal Data due to reasons such as mergers, divisions, dissolution, or bankruptcy, it shall notify the Personal Data Subject of the name or contact information of the recipient and obtain the Personal Data Subject's separate consent. The recipient shall continue to fulfill the obligations of the Personal Data Processor.

3. **Disclosure and Sharing of Personal Data with Third Parties**. If the Company discloses or shares its handled Personal Data with third parties, it shall inform the Personal Data Subject of the recipient's name, contact information, purpose and method of disclosure, and type of Personal Data involved, and obtain separate consent or have other legal grounds. The recipient shall handle Personal Data within the scope of the above purposes, methods, and types of Personal Data. Any changes to the original purposes or methods of handling require renewed consent from the Personal Data Subject or other legal grounds.

4. **Public Disclosure of Personal Data.** The Company shall not publicly disclose the Personal Data handled by the Company unless it has obtained the consent of the Personal Data Subject or has other legal grounds clearly stipulated by laws and regulations.

## 4.7 Deletion of Personal Data

1. The Company shall dispose of Personal Data within a specified timeframe once the purpose of its collection has been fulfilled, is deemed unachievable, or when it is no longer necessary for handling, and take reasonable measures to ensure that Personal Data cannot be recovered or reused.

2. If the retention period required by laws or regulations has not yet expired, or if it is technically impossible to delete Personal Data, the Company shall stop all handling activities except for storing the Personal Data and taking necessary security measures to protect it.

## 4.8 Rights of Personal Data Subjects

**The Company shall protect the legitimate rights and interests of customers and other Personal Data Subjects in accordance with applicable laws.** Upon verifying the identity of the Personal Data Subject, the Personal Data Processor shall promptly respond to the rights exercised by the Personal Data Subject and provide an appropriate response along with a reasonable explanation within the timeframe established by applicable laws and regulations:

1. Request information about how their Personal Data is handled;

2. Request access to view and copy their Personal Data;

3. Request correction or supplementation of their Personal Data;

4. Request deletion of their Personal Data;
5. Withdrawal consent (opt-out);
6. Request a copy of their Personal Data;
7. Request transfer of their Personal Data to another designated Personal Data Processor, subject to compliance with applicable laws, regulations, and conditions stipulated by the national cyberspace administration.

## 4.9 Management Supervision and Evaluation

1. The Company regularly conducts training and awareness programs on personal data protection (including but not limited to relevant laws, regulations, norms, standards, and management systems pertaining to personal data protection).
2. The Company regularly performs personal data security assessments and risk evaluations to promptly identify and resolve personal data security issues.
3. The Company shall promptly address personal data security incidents and notify the relevant Personal Data Subjects concerned in a timely manner.
4. The Company has established a personal data protection supervision mechanism, embedding this Policy and management procedures into the group-wide risk and compliance management system, and regularly carries out personal data protection supervision and evaluations to promptly identify and resolve any issues related to personal data protection.
5. The Company's Audit and Supervision Department accepts and handles complaints and reports related to personal data protection, and investigates and handles illegal personal data handling activities.

   Phone: +86 519-85176933
   Email: IA@trinasolar.com
   Address: Trina Solar's Audit and Supervision Department,
   No. 2, Tianhe Road, Xinbei District, Changzhou City,
   Jiangsu Province (Zip Code 213031)

   
   

6. **The Company maintains a "zero tolerance" policy for violations of personal data protection**. Any violation of applicable laws, this Policy and other systems and procedures related to personal data protection of the Company, resulting in any administrative penalties, disputes, economic losses, damage

to brand reputation, or other negative impacts shall be subject to penalties including verbal or written warnings, termination of employment contracts, recovery of improper gains, and demands for compensation for losses, based on the severity and circumstances of the violation. If the violation constitutes a criminal offense, the Company shall refer the matter to the appropriate authorities for legal liability in accordance with the law.

7. The Company shall regularly conduct internal and external audits of the compliance of this Policy in accordance with the requirements of relevant applicable laws, regulations, policies, and other requirements, as well as the Company's business operations, and shall promptly adjust and update this policy accordingly.

## 5. Revision Record

| Document No. | Version | Responsible person for drafting/revising | Effective Date | Revision Details and Reason |
|---|---|---|---|---|
| TSL-CM-008 | V01 | Information Security Department, Compliance Management Department | 2024-08-12 | New version release |

## 6. Special Instructions

The Information Security Department and the Compliance Management Department are responsible for interpreting and updating this Policy. This Policy is valid for two years. Once the new version of the policy is released, the old version is automatically invalidated.