TCI Co., Ltd.

Privacy Policy

Adopted by the 3rd Meeting of the Board of Directors of TCI Co., Ltd. in 2026, August 10, 2026

TCI Co., Ltd. has completed ISO/IEC 27001:2022 certification, with the ISMS covering the corporate network, ERP system and data center operations that are critical to business operations. Through these mechanisms, the management system is implemented as sustainable information security governance and is being further extended to subsidiaries, advancing integrated group-wide information security management.

As a biotechnology enterprise founded on research, development and manufacturing, we recognize the confidentiality of personal information and the trust on which it rests, and we understand the importance of data in cross-border operations, digital services and supply chain collaboration. We therefore commit to processing personal information in a lawful, fair and transparent manner, and to establishing a consistent and continuously improving privacy protection mechanism in accordance with the EU General Data Protection Regulation (GDPR), Taiwan's Personal Data Protection Act and its Enforcement Rules, and other relevant regulations.

In this policy, "you" or "data subject" means a natural person having a business or employment relationship with the Company, including employees, customers, suppliers and other stakeholders of the Company.

This policy applies to operations involving the processing of personal information across the business activities of the Company and its overseas subsidiaries and operating sites. In addition, in marketing communications directed at vulnerable market groups (for example children and persons lacking market knowledge), we will make every effort to avoid causing misunderstanding as to the potential benefits of our products or services.

Our Commitments

We commit to processing personal information on the core principles of "minimum necessity" and "purpose limitation", and to incorporating personal information protection and information security risk into our overall risk management and compliance framework, ensuring through institutionalized governance, internal and external review and continuous improvement that protective measures advance in step with operational needs.

- Lawfulness, fairness and transparency: We collect and use personal information within the scope permitted by applicable law and necessary for the stated purposes, and clearly inform data subjects of the purposes and methods of processing.
- Minimum necessity and purpose limitation: We collect and process only the personal information necessary to fulfil specific purposes, avoiding unnecessary or excessive processing.
- Security and resilience: We adopt reasonable and appropriate technical and organizational measures to maintain the confidentiality, integrity and availability of personal information.
- Respect for rights: We safeguard the rights that data subjects enjoy under the GDPR and other applicable laws, and respond in accordance with the prescribed timeframes and procedures.
- Cross-border transfers and third-party management, transparency and continuous improvement: Where data is transferred or processing is outsourced due to cross-border operational needs, we require the parties concerned to adopt corresponding protective measures and to comply with this policy. We periodically review implementation through mechanisms such as internal audit and management review, and propose and implement improvement plans where necessary.

With respect to information security, the Company has obtained ISO/IEC 27001 information security management system certification, and is periodically inspected and verified by an independent third-party certification body.

Our Strategy

Governance and Accountability

We establish a governance framework for privacy protection and information security, clearly defining roles and responsibilities and integrating them into compliance and risk management processes, so that policy implementation, resource allocation and management effectiveness can be supervised and tracked.

Data Minimization and Full Lifecycle Management

We collect, use and retain data in accordance with the principle of minimum necessity. Once the purpose has been achieved or the retention period has expired, we delete the data or take other appropriate measures as

required, so as to reduce the risk of data exposure. We will also make every effort to adopt reasonable technical and management measures to ensure that processing occurs only for the period necessary for the purposes set out in this policy, and that data is retained only for the shortest necessary period.

Information Security and Risk Management

Building on our information security management system, we conduct periodic risk assessments, internal audits and management reviews, propose improvement measures for identified risks and continuously track their effectiveness. The Company has established response and notification mechanisms for personal data security incidents, and fulfils the relevant notification and reporting obligations in accordance with applicable law.

Cross-Border Transfers and Third-Party Management

Within the scope of the purposes set out in this policy and based on cross-border operational needs, personal data may be transferred to other companies within the Company's group and to the countries or regions in which their sites are located. Where necessary, we also cooperate with external advisors, service providers and others, and share data with competent authorities and others in accordance with the applicable purposes and legal procedures. The laws and personal data protection requirements of such countries or regions may differ; we will adopt commensurate protective measures to ensure that a consistent level of protection is maintained throughout cross-border transfer and outsourced processing.

Data Subject Rights and Handling of Requests

The Company provides formal channels for data subjects to exercise their rights, and responds within the timeframes and in accordance with the procedures prescribed by applicable law. Other rights enjoyed by data subjects under the law are likewise safeguarded in accordance with applicable law.

Stakeholder Communication, Education and Positive Impact

Through communication and education we raise awareness of privacy protection among internal and external stakeholders, strengthen data ethics and trust, and disclose in an open and transparent manner the direction of continuous improvement in our policies and management practices.

Transparent Notification

In accordance with the GDPR and applicable laws, we will clearly explain the following matters concerning the processing of personal information, and will provide appropriate supplementary information where necessary:

Data Controller and Data Processor

The data controller is TCI Co., Ltd. Where required for business purposes, third parties such as service providers may be engaged as data processors, and are required to comply with this policy and applicable law.

Purposes of Collecting Personal Information

These include performing contractual relationships or pre-contractual measures, fulfilling obligations required by law or by the competent authorities, and processing necessary for the legitimate interests of the Company or a third party, provided that your rights and freedoms are not infringed.

Categories of Personal Information

These may include basic identification data, contact details, transaction and contract data, and information on the use of online services, all processed in accordance with the principle of minimum necessity.

Period, Scope, Recipients and Means of Use

On a lawful basis, and for business purposes, website operations or the provision of products and services, data may be shared within the group and, where necessary, with competent authorities, external advisors, service providers, parties to litigation or legal proceedings, third parties necessary for the investigation or prevention of crime, or third parties providing advertising, plug-ins or website content. In addition, due to the cross-border nature of our business, personal data may be transferred to the countries or regions in which the Company's group operates. Such countries or regions may have different laws and personal data protection requirements; we will adopt commensurate protective measures to ensure a consistent level of protection during transfer. We will also make every effort to take reasonable measures to process data only for the period necessary to achieve the aforementioned purposes and to retain it only for the shortest necessary period. Once the purpose has been achieved or the retention period has expired, the data will be deleted, anonymized or otherwise appropriately handled as required.

Data Subject Rights

These include the rights to enquire about and review data (and to be provided with a copy), to supplement and

correct data, to restrict or cease processing or to object to processing, and to erasure. However, where an exception provided by law applies, the Company may continue to retain or process the data to the extent necessary.

Freedom to Provide Personal Information and Possible Consequences

You are free to choose whether to provide personal information. However, if you decline to provide it or the information is insufficient, this may affect identity verification, eligibility review, contract performance, statutory filings or other operations necessary to our business, and may consequently affect the provision of services or your rights and interests.