

Sino Biopharmaceutical Limited

Privacy Policy

1. Purpose

Sino Biopharmaceutical Limited together with its subsidiaries (hereinafter referred to as "SBP Group", "the Group") attach high priority to information security and privacy protection in its daily operations, as well as for customers and business partners. The Policy defines the principles and practices adopted by the Company in all data processing activities, to ensure compliant management and secure utilization of personal data.

2. Applicability

The Policy applies to all operational activities of the Company, including business operations, cooperation with suppliers and other third-party partners, and internal management covering all employees.

Suppliers and other third-party partners shall undergo capability assessments covering data security, cybersecurity and related domains. Cooperation agreements shall incorporate security clauses and non-disclosure agreements with standards equivalent to or more stringent than those stipulated in the Policy. All employees shall comply with the Policy and the explicit requirements set out in the Code of Employee Conduct, and sign information non-disclosure agreements.

3. Basic Principles

The Company strictly complies with applicable laws, regulations, domestic and international standards and regulatory requirements, including the *Personal Information Protection Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Cybersecurity Law of the People's Republic of China*, and *Information Security Technology – Personal Information Security Specifications*. Corresponding security controls are implemented to safeguard personal data, and the Group continuously optimizes its data security management framework and information systems.

4. Definitions

- **Personal Information:** All information recorded electronically or by other means that relates to an identified or identifiable natural person, excluding anonymized information.
- **Data Subject:** The natural person to whom personal data pertains.

- **Data Processing:** Activities including the collection, transmission, storage, processing, utilization, provision and public disclosure of data.

5. Data Collection and Processing

The Company adheres to the principles of minimization and necessity. It clearly informs data subjects of the purposes and methods for collecting and using personal information, and collects and processes personal data only upon voluntary consent from data subjects.

Personal data collected by the Company shall serve legitimate business or operational management needs, consistent with the scope agreed under contractual and privacy agreements, and no excessive data collection shall be conducted. Where relevant business activities cease or data collection is no longer required, the Company shall immediately suspend data collection and delete or anonymize stored personal data upon expiry of the retention period.

For business operation purposes, the Company collects and processes directly identifiable personal information including but not limited to name, date of birth, contact details, ID number, health information, biometric data, physiological health data, education and employment information, and emergency contact information.

Subject to explicit consent from data subjects, the Company may collect and use personal information from third parties such as cooperative clinical trial institutions and hospitals. The Company verifies the legality of personal information sources in accordance with arrangements with third parties and processes such information in compliance with relevant laws and regulations.

Within the scope of routine business activities, the Company processes and uses personal data based on the purposes specified herein, or where permitted or required by applicable information security legislation, while upholding the minimization principle. Key purposes for utilizing personal information include pharmaceutical research and development, product and service procurement, customer relationship management, business contract execution, network equipment and service administration, human resource management, and regulatory compliance obligations.

6. Data Sharing

The Company may disclose personal information to third parties including suppliers, service providers, business partners and affiliated companies to conduct business activities, deliver services and satisfy legal and regulatory requirements. For such disclosures, the Company enters into data confidentiality contracts with third parties pursuant to the Policy and applicable laws to fully protect personal information. During cooperation, the Company imposes strict requirements on third parties to process personal information only within the scope, manner

and methods specified under the Policy, signed contracts, entrustment objectives and privacy agreements.

In the event of corporate transactions such as mergers, acquisitions or asset transfers that necessitate the transfer of personal information to third parties amid business development, the Company will notify relevant parties promptly via notifications, announcements or other channels. The Company will require the receiving third party to use and protect personal information in line with the Policy and applicable laws and regulations. Meanwhile, the Company will continue to ensure personal information is protected to standards no less stringent than those set out in the Policy in accordance with relevant laws and regulations.

The Company reserves the right to disclose personal information as required by law if such disclosure is necessary to comply with regulatory mandates, government requests, court orders or judicial proceedings, or to protect the safety, rights or property of customers, the public, the Group or other individuals.

The Company may use and disclose personal information in other ways with consent obtained from the relevant data subjects.

7. Data Security

The Company has established a dedicated information security team to oversee Group-wide information security management, data development, privacy protection and informatization development. The Compliance Department monitors privacy compliance performance across all business segments. Heads of each business unit are accountable for data compliance within their respective departments and supplier cooperation arrangements, and internal reviews and supplier audits will be conducted where necessary to prevent unauthorized collection and exploitation of private data. All employees shall strictly abide by confidentiality obligations in respect of corporate information, materials, achievements, and non-public information of third parties including customers and distributors.

The Company's privacy risk management forms an integral component of its enterprise risk management system, enabling effective identification, assessment and mitigation of privacy risks throughout daily operations.

From a technical perspective, the Company implements data classification and grading, encrypted storage, access permission controls, limited data retention cycles, firewalls and other safeguards to protect personal information against unauthorized access, leakage, tampering or destruction.

The Internal Audit Team conducts regular inspections on the implementation of this Privacy Policy to identify and remediate potential privacy risks and ensure effective enforcement of

the Policy. Where appropriate, the Company engages independent third-party institutions to evaluate and audit its privacy policies and data processing practices to verify alignment with applicable laws, regulations and international standards.

The Company adopts a zero-tolerance stance against violations of this Privacy Policy. Any breach will result in serious disciplinary actions including but not limited to internal sanctions and termination of employment. Relevant training will be delivered to clarify specific disciplinary consequences for non-compliance, ensuring all employees understand and adhere to the Policy. Data subjects with inquiries or complaints regarding the Company's data processing activities may contact the Company via sjjcb@cttq.com.

8. Cross-border Data Transmission

Prior to transferring personal data overseas, the Company shall fully satisfy all regulatory requirements governing cross-border information transmission and obtain consent from the relevant data subjects. Overseas data retention periods shall comply with both the laws of the People's Republic of China and the jurisdiction of the receiving party.

9. Children's Privacy

The Company does not proactively collect personal data of children under the age of 14. If personal data of minors under 14 is collected inadvertently, such data will be deleted immediately and relevant services suspended.

10. Data Subject Rights

Subject to applicable legal provisions, data subjects are entitled to the following rights:

- Right of Access: To access, inspect and obtain copies of stored personal data relating to themselves;
- Right of Rectification: To correct, update and supplement their personal data;
- Right of Erasure: To request the Company to delete their personal data;
- Right of Consent Withdrawal: To adjust the scope of authorization or withdraw previously granted consent;
- Right of Data Portability: To request the transfer of their personal data to a designated alternative data processor;
- Other rights conferred by applicable legislation.

11. Supplementary Provisions

The Policy shall take effect upon issuance. The Company reserves the right to revise the Policy when applicable laws and regulations are amended or when material changes occur to product or service functions. Matters not covered herein, or provisions conflicting with national laws, regulations and regulatory documents, shall be governed by the official legal requirements of the state. The Company reserves the sole right of interpretation of the Policy.