

PRIVACY POLICY

ONESOURCE PRIVACY POLICY

1. Purpose

At OneSource Specialty Pharma Limited ("OneSource", "we", "us" or "the Company"), we are committed to protecting the privacy and security of personal data entrusted to us by employees, job applicants, customers, suppliers, vendors, contractors, consultants, business partners, clinical trial participants, website users, and other individuals with whom we interact.

This Privacy Policy establishes the principles and requirements governing the collection, use, processing, storage, disclosure, transfer, retention, and protection of personal data in compliance with applicable data protection laws, including the Digital Personal Data Protection Act, 2023 (India), the General Data Protection Regulation (GDPR), and other applicable privacy regulations.

OneSource maintains a strict zero-tolerance approach towards unauthorised access, misuse, unlawful disclosure, alteration, loss, destruction, or processing of personal data.

2. Scope and Applicability

This policy is applicable to OneSource's entire operations, including suppliers and third-party vendors involved with OneSource. All suppliers, contractors, consultants, and third-party service providers shall comply with privacy and data protection requirements equivalent to those established in this Policy and shall be subject to appropriate contractual safeguards.

3. Privacy Governance and Accountability

Privacy and data protection risks form an integral part of our enterprise-wide risk management and compliance framework. Privacy risks are periodically identified, assessed, monitored, reported, and mitigated through established governance mechanisms.

A Data Protection Officer (DPO), supported by a cross-functional privacy governance team, is responsible for overseeing compliance with this Policy, responding to privacy-related concerns, coordinating investigations, and monitoring implementation of privacy controls across the organisation.

4. Principles of Personal Data Processing

OneSource processes personal data in accordance with the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability
- Privacy by design and by default

5. Legal Basis for Processing

Where required by applicable law, OneSource processes personal data based on one or more of the following legal grounds:

- Consent of the individual;

- Performance of a contract;
- Compliance with legal or regulatory obligations;
- Protection of vital interests;
- Legitimate business interests that do not override individual rights;
- Scientific, medical, clinical, or research purposes permitted under applicable laws.

Where consent is required, personal data shall not be collected, used, retained, processed, or disclosed unless valid consent has been obtained.

6. Categories of Personal Data Collected

Depending on the nature of the relationship, OneSource may collect and process:

Employees, Contractors, and Applicants

- Identification information
- Contact details
- Employment records
- Educational and professional qualifications
- Payroll and benefits information
- Emergency contact details
- Information required for regulatory compliance

Customers, Vendors, and Business Partners

- Contact information
- Business information
- Contractual and financial information
- Communication records

Patients and Clinical Trial Participants

- Health information
- Medical history
- Diagnostic information
- Biometric information
- Research-related information

Website Users

- IP addresses
- Device identifiers
- Browser information
- Website usage information

- Cookie-related information

7. Purposes of Processing

Personal data may be processed for:

- Recruitment and employment administration;
- Compensation and benefits management;
- Customer relationship management;
- Contract administration;
- Regulatory and legal compliance;
- Clinical research and pharmacovigilance activities;
- Product quality and patient safety activities;
- Vendor and supplier management;
- Information security monitoring;
- Business operations and continuity;
- Website administration and improvement;
- Protection of company assets and interests;
- Any other legitimate purpose permitted by applicable law.

8. Protection Against Secondary Use

Personal data collected by OneSource shall be used only for the specific, explicit, and lawful purposes for which it was collected or for other compatible purposes permitted under applicable law. Personal data shall not be processed, disclosed, or used for unrelated or secondary purposes without an appropriate legal basis, including obtaining additional consent where required by applicable law.

9. Customer Privacy Rights and Choice

OneSource is committed to ensuring individuals maintain control over their personal data.

Where applicable, individuals may:

- Provide or withhold consent for processing activities;
- Withdraw consent at any time;
- Opt out of processing based on consent or legitimate interests, subject to legal or contractual limitations;
- Control preferences regarding communications and use of personal information.

Withdrawal of consent shall not affect the lawfulness of processing conducted before such withdrawal.

10. Cookies and Similar Technologies

OneSource may use cookies, web beacons, internet tags, and similar technologies on its websites and digital platforms to enhance user experience, improve website functionality, maintain security, and analyze website usage. These technologies may collect information such as IP addresses, browser type,

device information, website activity, and user preferences. Where required by applicable law, users will be provided with the option to provide or withdraw consent for non-essential cookies. Users may also manage cookie preferences through their browser settings; however, disabling certain cookies may affect website functionality and user experience.

11. Disclosure of Personal Data

Personal data may be disclosed only where necessary and lawful, including to:

- OneSource affiliates and group entities;
- Pivot Path and authorized service providers;
- Regulatory authorities and government agencies;
- Auditors, legal advisors, and professional consultants;
- Clinical research organizations and research partners;
- Information technology service providers;
- Potential acquirers or successors during mergers, acquisitions, or corporate restructuring activities.

All disclosures shall be subject to appropriate confidentiality, privacy, and security obligations. Personal data shall not be sold to third parties.

12. Cross-Border Transfers

Where personal data is transferred across national borders, OneSource shall implement appropriate safeguards and comply with applicable legal, regulatory, and contractual requirements governing international data transfers.

13. Security and Confidentiality

OneSource implements appropriate technical, organisational, physical, and administrative safeguards to protect personal data, including:

- Role-based access controls;
- Encryption and secure transmission mechanisms;
- Network security controls;
- Monitoring and intrusion detection systems;
- Secure backup and recovery procedures;

These measures are designed to preserve the confidentiality, integrity, and availability of personal data.

14. Data Retention

Personal data shall be retained only for as long as necessary to fulfil the purpose for which it was collected and to satisfy legal, regulatory, contractual, scientific, business, or operational requirements.

Upon expiry of applicable retention periods, personal data shall be securely deleted, anonymised, archived, or otherwise disposed of in accordance with approved procedures and applicable laws.

15. Data Breach Management

OneSource maintains documented incident response and breach management procedures.

In the event of an actual or suspected personal data breach:

- The incident shall be promptly investigated;
- Appropriate containment and remediation measures shall be implemented;
- Impact assessments shall be conducted;
- Affected individuals and competent authorities shall be notified where required by law;
- Corrective and preventive actions shall be implemented.

16. Rights of Data Principals / Data Subjects

Subject to applicable laws, individuals may:

- Request access to personal data held by OneSource;
- Obtain information regarding processing activities;
- Request correction of inaccurate or incomplete information;
- Request deletion of personal data;
- Request restriction of processing;
- Object to processing where permitted by law;
- Withdraw consent;
- Request transfer of personal data to themselves or another service provider in a structured, commonly used, and machine-readable format where applicable;
- Nominate another individual to exercise rights on their behalf where permitted by law;
- Lodge complaints regarding privacy practices.

Requests shall generally be processed without charge unless permitted otherwise under applicable law.

17. Privacy Awareness

OneSource conducts periodic awareness programmes on cybersecurity and data protection for its employees. This Policy shall be published and updated on the company's official website.

18. Monitoring, Audits, and Compliance

OneSource monitors compliance with this Policy through periodic reviews and assessments.

The Company may conduct:

- Internal privacy and data protection audits;
- Internal audits/Compliance assessments;
- Independent third-party audits and reviews;

Findings arising from such reviews shall be addressed through corrective and preventive actions.

19. Violations and Disciplinary Actions

Violation of this Policy may result in corrective actions, disciplinary measures up to and including termination of employment or contractual engagement, recovery of damages where appropriate, and legal or regulatory action.

OneSource maintains a zero-tolerance approach towards intentional misuse, unauthorised disclosure, or unlawful processing of personal data.

20. Contact and Grievance Redressal

Questions, concerns, complaints, or requests relating to privacy and personal data may be directed to:

Data Protection Officer (DPO)

To ensure transparency in data protection, we have appointed a Data Protection Officer (DPO), in compliance with various legislations, who is supported by a cross-functional governance team. Individuals may contact our DPO, Ms. Tintu at Data.Protection@onesourcecdmo.com.

21. Periodic Review

This Policy shall be reviewed at least annually and whenever required due to changes in applicable laws, regulations, organisational structure, technologies, business operations, or industry best practices. Revisions shall be documented, approved, communicated, and incorporated into relevant training and awareness programmes.

Glossary of Key Terms

Term	Definition
Consent	Freely given, informed, and unambiguous agreement by the data subject for the processing of their personal data
Cookies	Small data files stored on a user's device by websites to remember preference or track activity for analytics and performance
Cross-Border Data Transfer	The transfer of personal data outside the country where it was originally collected, subject to applicable privacy safeguards
Data Breach	Any unauthorized access, disclosure, or loss of personal data. It requires notification and remediation under applicable laws
Data Protection Officer/ Office (DPO)	The designated individual/ team responsible for ensuring compliance with data protection obligations and addressing privacy-related queries or concerns
Data Subject	Any individual whose personal data is collected or processed (such as patients, employees, healthcare professionals)
Internet Tags	Small pieces of code or metadata used online to classify, track, or describe information. They can serve different purposes depending on context, ranging from organizing content to monitoring user activity.
Personal Data	Information that identifies or can be used to identify an individual, such as name, email address, contact information, health records and IP address
Right to Withdraw	The data subject's right to request access to their data or request its deletion under applicable laws
Web beacon	Tiny, often invisible tracking tools embedded in websites or emails that monitor user activity. They are also known as tracking pixels, pixel tags, clear GIFs, or web bugs

Version Control Sheet

Version Number	Date of Board Meeting	Remarks
V1	Approved and adopted in the Board Meeting held on July 24, 2026	Adopted in line with requirements of ESG parameters