TERRAMED LIMITED – PRIVACY POLICY

Issue Date: 18 November 2026
Version: 2026
Supersedes: February 2024
Company Registration Number: 15484367

Introduction

TerraMed Limited ("TerraMed", "we", "us" or "our") is committed to protecting personal data and respecting the privacy of individuals who interact with our business.

As a UK-based supplier of medical devices, healthcare consumables and related products to NHS organisations, private healthcare providers and other customers, we recognise the importance of responsible information management, confidentiality and data security.

This Privacy Policy explains how we collect, use, store, share and protect personal data, and outlines the rights individuals have in relation to their information.

We process personal data in accordance with applicable UK data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Data (Use and Access) Act 2025 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), as amended.

This Policy applies to personal data collected through our website, business communications, customer and supplier relationships, procurement activities and other business operations.

1. Data Controller and Contact Information

TerraMed Limited is the data controller responsible for determining the purposes and means of processing personal data covered by this Policy, except where we expressly act as a data processor on behalf of another organisation.

Our registered business details are:

TerraMed Limited
Suite 7, Innovation House
Molly Millars Close
Wokingham, Berkshire, RG41 2RX
United Kingdom

Company Registration Number: 15484367
Email: management@terramed.co.uk
Website: https://terramed.co.uk

All privacy-related enquiries, data protection requests and complaints may be directed to the email address above.

2. Personal Data We Collect

We collect and process personal data that is reasonably necessary for legitimate business operations, contractual relationships, regulatory compliance and communications.

Depending on the nature of our relationship with an individual, this may include:

2.1. Identity and Professional Information

Names, job titles, employers, departments, professional roles and other business-related identification information.

2.2. Contact Information

Business addresses, postal addresses, telephone numbers, email addresses and other contact details provided during business communications.

2.3. Commercial and Transaction Information

Information relating to quotations, purchase orders, invoices, payments, delivery arrangements, customer accounts, supplier relationships and transaction histories.

2.4. Financial Information

Relevant payment information, bank account details, billing records and other financial information required for legitimate business transactions, accounting or compliance purposes.

2.5. Technical and Website Information

Internet Protocol (IP) addresses, browser and device information, website access records, diagnostic information and data collected through cookies or similar technologies where applicable.

2.6. Communication and Enquiry Information

Information contained in emails, telephone communications, website enquiries, requests for quotations, customer service correspondence, complaints and feedback.

2.7. Marketing and Preference Information

Business communication preferences, marketing preferences and records of consent or objections where applicable.

2.8. Regulatory and Compliance Information

Information reasonably required for supplier due diligence, product safety investigations, regulatory compliance, fraud prevention or the management of contractual and legal obligations.

We do not generally seek to collect special category personal data, such as medical records or information about an individual's health, through ordinary website enquiries or commercial transactions.

Where such information is exceptionally required, including in connection with a medical device safety incident, we will process it only where an appropriate lawful basis, an applicable special category condition and relevant safeguards are in place.

3. How We Collect Personal Data

We may obtain personal data through the following channels:

- **Direct interactions:** Information provided when individuals contact us, request quotations, place orders, supply goods or services, or communicate with our representatives.
- **Website interactions:** Information submitted through website forms, email links and other electronic communication channels.
- **Business relationships:** Information supplied by customers, suppliers, distributors, manufacturers and other commercial partners.
- **Third-party sources:** Relevant professional or commercial information received from business partners, procurement platforms, professional directories, public registers or other legitimate sources.
- **Technical systems:** Information generated through website hosting, security systems, communications platforms and related business technology.

Where personal data is obtained indirectly, we will provide relevant privacy information where required by applicable law.

4. How We Use Personal Data

We process personal data only for specified, legitimate purposes and where an appropriate legal basis exists.

Our principal processing activities include:

4.1. Customer and Supplier Relationships

To establish, maintain and administer commercial relationships, communicate with business contacts, assess suppliers and manage ongoing business requirements.

4.2. Quotations, Orders and Deliveries

To respond to product enquiries, prepare quotations, process orders, arrange deliveries, issue invoices and manage associated transactions.

4.3. Contractual Administration

To negotiate, enter into, perform and administer contractual arrangements and related business obligations.

4.4. Legal and Regulatory Compliance

To satisfy applicable accounting, taxation, healthcare product, procurement, regulatory and other legal requirements.

4.5. Product Quality and Safety

To manage product documentation, traceability, complaints, safety notifications, investigations, recalls and other quality-related matters where necessary.

4.6. Customer Service and Communications

To respond to enquiries, provide product information, address complaints and maintain appropriate records of business correspondence.

4.7. Business Development and Marketing

To communicate relevant information about our products, services and business activities in accordance with applicable direct marketing and electronic communications legislation.

4.8. Security and Business Administration

To protect our information systems, prevent fraud, maintain business records, manage operational risks and safeguard confidential information.

4.9. Business Improvement

To evaluate business performance, maintain service quality, improve internal processes and support legitimate operational planning.

We will not process personal data for materially incompatible purposes unless permitted by law and, where required, appropriate additional information or consent is provided.

5. Lawful Bases for Processing

Under the UK GDPR, we rely on one or more of the following lawful bases, depending on the specific processing activity.

5.1. Contractual Necessity

Where processing is necessary to perform a contract with an individual or to take steps at that individual's request before entering into a contract.

Where a contract is with a corporate customer or supplier, our processing of its representatives' personal data will generally rely on legitimate interests rather than contractual necessity.

5.2. Legal Obligation

Where processing is necessary to comply with applicable laws, regulations, statutory reporting duties or other legal requirements.

5.3. Legitimate Interests

Where processing is necessary for our legitimate business interests, provided those interests are not overridden by the rights and freedoms of the individuals concerned.

These interests may include managing customer and supplier relationships, responding to business enquiries, maintaining business security, preventing fraud, administering contracts and improving operational efficiency.

We assess the necessity and proportionality of processing activities where legitimate interests are relied upon.

5.4. Consent

Where consent is required by law, including for certain marketing communications or non-essential cookies and similar technologies.

Individuals may withdraw their consent at any time. Withdrawal does not affect the lawfulness of processing carried out before consent was withdrawn.

6. Sharing and Disclosure of Personal Data

We may disclose personal data to third parties where reasonably necessary for legitimate business purposes or to satisfy legal obligations.

Recipients may include:

6.1. Group Companies

Companies within Zeela Group where appropriate for legitimate business administration, shared services, operational support or other lawful purposes.

6.2. Service Providers

External organisations providing services such as information technology, website hosting, cloud infrastructure, accounting systems, communications, logistics, payment processing and administrative support.

6.3. Professional Advisers

Legal advisers, accountants, auditors, insurers, bankers and other professional service providers acting within their professional or contractual responsibilities.

6.4. Commercial Partners

Manufacturers, distributors, logistics providers and other business partners where necessary for fulfilling orders, managing supply chains or providing requested services.

6.5. Regulatory and Public Authorities

Relevant regulatory bodies, government departments, law enforcement agencies, courts and other authorities where disclosure is required or permitted by law.

These may include healthcare regulators and public procurement authorities where relevant to our obligations.

6.6. Corporate Transactions

Potential purchasers, investors, advisers or other relevant parties in connection with a proposed or completed merger, acquisition, restructuring or transfer of business assets, subject to appropriate confidentiality and legal safeguards.

We do not sell personal data to third parties for their independent marketing purposes.

Where third parties process personal data on our behalf, we require appropriate contractual arrangements and safeguards in accordance with applicable data protection requirements.

7. International Transfers of Personal Data

Some of our service providers, commercial partners or technology systems may operate outside the United Kingdom.

Where personal data is transferred internationally and the transfer is subject to UK GDPR restrictions, we will ensure that an appropriate legal mechanism is available.

Depending on the circumstances, this may include:

- Transfers to countries or organisations covered by applicable UK adequacy regulations.
- The use of the UK International Data Transfer Agreement (IDTA).
- The UK Addendum to the European Commission's Standard Contractual Clauses.
- Other legally recognised safeguards or exceptions permitted under applicable UK data protection legislation.

Where required, we will assess relevant risks and implement appropriate supplementary protections.

Individuals may request further information about applicable transfer safeguards by contacting management@terramed.co.uk.

8. Data Security and Confidentiality

We recognise the importance of protecting personal data against unauthorised access, unlawful processing, accidental loss, destruction, alteration and disclosure.

We apply technical and organisational security measures proportionate to the nature, sensitivity and risks associated with the information processed.

These measures include, where appropriate:

- Access restrictions based on legitimate business requirements.
- Authentication and account security controls.
- Appropriate encryption and secure data transmission arrangements.
- System maintenance, monitoring and protective security measures.
- Data backup, recovery and business continuity arrangements.
- Confidentiality obligations for relevant employees, contractors and service providers.
- Procedures for identifying, investigating and responding to information security incidents.

Access to personal data is limited to authorised individuals who require the information for legitimate purposes.

Although we take appropriate precautions, no electronic storage or transmission system can be guaranteed to be entirely secure.

Where a personal data breach occurs, we will assess the incident and notify the Information Commissioner's Office (ICO) and affected individuals where required by applicable law.

9. Data Retention

We retain personal data only for as long as reasonably necessary to fulfil the purposes for which it was collected, including applicable legal, accounting, taxation, regulatory and contractual requirements.

Retention periods are determined by reference to the nature of the information, the relevant processing purpose, statutory requirements and any legitimate need to preserve records.

In particular:

- **Commercial and contractual records:** Retained for the duration of the relevant relationship and any additional period reasonably necessary for legal, regulatory or contractual purposes.
- **Accounting and financial records:** Retained in accordance with applicable statutory record-keeping requirements, commonly including periods of six years where relevant.
- **Enquiries and correspondence:** Retained for as long as reasonably necessary to manage communications, maintain appropriate business records and resolve any related matters.
- **Marketing information:** Retained while there is an appropriate lawful basis for processing, subject to applicable consent, objection and suppression requirements.
- **Technical and security records:** Retained for periods proportionate to their operational, security and compliance purposes.
- **Product quality and regulatory records:** Retained in accordance with applicable medical device, product safety, traceability and other regulatory requirements.

Records may be retained for longer periods where necessary to establish, exercise or defend legal claims, comply with legal obligations or address ongoing investigations.

When personal data is no longer required, it will be securely deleted, anonymised or otherwise disposed of as appropriate.

10. Cookies and Website Technologies

Our website may use cookies and similar technologies to support website functionality, maintain security and assist with technical operation or performance assessment.

Cookies are small files stored on a user's device that may enable websites to remember information or recognise particular interactions.

Cookies and related technologies may include:

- **Strictly necessary technologies:** Required for essential website functions, security or the delivery of services requested by users.
- **Functional technologies:** Used to support website preferences or additional functionality where implemented.
- **Analytics and performance technologies:** Used, where implemented, to understand website performance and visitor interactions.
- **Third-party technologies:** Technologies associated with externally provided website services, where applicable.

We will provide relevant information about technologies used on our website and obtain consent where required under applicable law.

Technologies that require consent will not be deployed before the necessary consent has been obtained.

Users may also manage or restrict cookies through their browser settings, although disabling certain technologies may affect website functionality.

11. Direct Marketing and Business Communications

We may communicate with existing and prospective business customers, suppliers and professional contacts concerning our products, services and business activities.

Marketing communications will be conducted in accordance with the UK GDPR and PECR, including applicable rules for business-to-business marketing.

Where legally required, we will obtain consent before sending electronic marketing communications.

Where the law permits processing based on legitimate interests, we will consider the nature of the relationship, the reasonable expectations of the individual and their data protection rights.

Recipients may object to direct marketing at any time by contacting management@terramed.co.uk or using an unsubscribe mechanism where provided.

We will respect valid marketing objections and may retain limited suppression information to ensure that the relevant preferences continue to be observed.

12. Your Data Protection Rights

Individuals have rights under applicable data protection legislation, subject to relevant conditions, limitations and exemptions.

These include:

12.1. Right of Access

The right to request confirmation of whether personal data is being processed and to obtain access to that information.

12.2. Right to Rectification

The right to request correction of inaccurate personal data or completion of incomplete information.

12.3. Right to Erasure

The right to request deletion of personal data where the applicable legal conditions are satisfied.

12.4. Right to Restrict Processing

The right to request that processing be restricted in certain circumstances.

12.5. Right to Data Portability

The right, where applicable, to receive personal data in a structured, commonly used and machine-readable format and to request its transfer to another controller.

12.6. Right to Object

The right to object to certain processing based on legitimate interests or public task grounds.

Individuals have the right to object at any time to the processing of their personal data for direct marketing purposes.

12.7. Right to Withdraw Consent

Where processing relies on consent, the right to withdraw that consent at any time without affecting prior lawful processing.

12.8. Rights Relating to Automated Decision-Making

Rights under applicable law concerning qualifying solely automated decisions, including the right to receive relevant information and to exercise applicable safeguards.

To exercise any of these rights, please contact: **management@terramed.co.uk**

We will respond to valid requests without undue delay and normally within one calendar month, subject to legally permitted extensions, applicable exemptions and any lawful adjustments to the response period.

We may request reasonable information to verify identity or clarify the scope of a request where permitted by law.

Requests are generally handled without charge, although applicable legislation permits fees or refusal in limited circumstances.

13. Automated Decision-Making and Profiling

TerraMed does not generally use automated decision-making or profiling to determine significant outcomes for individuals in its ordinary customer and supplier relationships.

Where automated tools are used for routine operational or administrative purposes, their use remains subject to applicable data protection requirements.

Should we introduce qualifying solely automated decision-making processes that produce legal or similarly significant effects on individuals, we will ensure that appropriate transparency, safeguards and individual rights are provided in accordance with applicable law.

14. Children and Vulnerable Individuals

Our website and commercial services are primarily intended for healthcare organisations, business customers, suppliers and professional users.

They are not specifically directed towards children.

We do not intentionally seek personal data from children through ordinary commercial enquiries.

Where we become aware that personal data has been collected inappropriately, we will take reasonable steps to address the matter in accordance with applicable law.

15. Data Protection Complaints

We encourage individuals to contact us directly if they have concerns about how their personal data is collected, used, stored or disclosed.

Complaints may be submitted to: **management@terramed.co.uk**

In accordance with applicable data protection legislation, including the Data (Use and Access) Act 2025, we will:

- Provide a clear and accessible means of raising a data protection complaint.
- Acknowledge complaints within 30 days of receipt.
- Take appropriate steps to investigate the matters raised.
- Keep complainants reasonably informed of progress.
- Communicate the outcome without undue delay.

Individuals also have the right to raise concerns with the Information Commissioner's Office (ICO), the UK's independent data protection regulator.

Information Commissioner's Office
Website: https://ico.org.uk
Telephone: 0303 123 1113

We encourage individuals to contact us first so that we have an opportunity to investigate and resolve their concerns, without restricting their statutory rights.

16. Changes to This Privacy Policy

We may revise this Privacy Policy periodically to reflect developments in our business operations, legal requirements, regulatory guidance or data processing activities.

The current version will be made available through our website.

Where changes materially affect individuals' rights or the purposes for which their personal data is processed, we will provide additional information or notifications where required by applicable law.

We recommend reviewing this Policy periodically to remain informed about how we handle personal data.

17. Contact Us

For questions, requests or concerns relating to this Privacy Policy, data protection or the processing of personal data, please contact:

TERRAMED LIMITED
Suite 7, Innovation House
Molly Millars Close
Wokingham, Berkshire, RG41 2RX
United Kingdom

Company Registration Number: 15484367
Email: management@terramed.co.uk
Website: https://terramed.co.uk