



Privacy Policy 2025

Threpoly "Privacy Policy" version 1.0

Last Updated: 18th October 2024

We at Threpoly take your privacy and our responsibilities very seriously. Please read this privacy policy carefully as it contains important information on who we are and how and why we collect and process your personal data.

It also explains your rights in relation to your personal data and how to contact us or a supervisory authority in the event you have a complaint.

We collect, process and are responsible for certain items of your personal data. When we do so we are subject to the Data Protection Act 2018. The United Kingdom is considered as a third country by the European Union with regard to the General Data Protection Regulation (GDPR) and therefore the provisions of the Data Protection Act 2018 are considered equal.

Key Terms

"We", "Us", "Our", "Company", "Prospect", "Supplier" - Are all taken to mean Threpoly Limited.

"You", "Customer", "Data Subject" - Are all taken to mean the individual who the personal data being collected and/or processed is related to.

"Personal Data" - Means any item of data which can wholly identify an individual or partially identify an individual when combined with another item of personal data.

"Special Categories of Personal Data" - Means personal data which is considered to be of a heightened sensitivity. This includes ethnicity, religious affiliations, trade union membership, political opinions, genetic information, biometric data, sexual history and history of health. A full list can be found on the Information Commissioner's Office website.

"Processing" - Means the storage, access, manipulation, use, deletion or transfer of personal data.

"Data Protection Officer" - A nominated member of our team who is responsible for Data Protection and provides guidance to our business on how to adhere to our legislative responsibilities.

Personal Data We Collect

Through interaction with our marketing activities or as a customer of ours, we may collect the following information from you:

- Your Name, Job Title, Telephone Address and Email Address.
- Payment information such as credit card details or Direct Debit credentials.
- Cookie data.
- Your response to surveys, competitions and promotions.
- Your IP address, location, language preferences and timezone.

This data is collected for the sole purpose of marketing, selling and providing the Threpoly service. Without this information we may not be able to fulfil orders or provide an advertised service in its complete form.

How we Collect Personal Data

Personal data can be collected via a number of different methods. In all cases, we employ validation and other measures to ensure accuracy to the best of our ability.

Source	What is Collected
You	<p>Information about you as a primary account holder or the person conducting a trial of our service - Name, Email Address, Title, Telephone Number.</p> <p>Payment information in order to pay for our service - Credit Card Information, Direct Debit Credentials.</p> <p>When you raise a support ticket or any other electronic communication with us and copy other members of your team or colleagues, we will automatically collect their Email Addresses and Names.</p>
Other Service Users	<p>If you have been added as an additional user of the service we will collect your Name and Email address.</p>
Website and Social Media Pages	<p>Tracking information so that we can analyse prospect behaviour and the popularity of our marketing activities.</p> <p>Any submissions made on our website requesting contact, downloading a marketing resource or submission of other forms such as questionnaires or competition. We would collect Name, Email Address, Job Title and Telephone Number.</p>

Our Service	We collect security tracking information - Logon time, location, IP address and timezone.

Why We Collect Your Personal Data

The Data Protection Act 2018 specifies the reasons for which we can collect and process personal data.

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Activity	Legal Basis
Providing Services and Trials to You	Contract.
Preventing or Detecting Fraud Against both Parties.	Legitimate Interests.
Screening for Emargos or other Sanctions.	Legal Obligation.
Gathering and Providing Information required by Investigative or Regulatory Bodies.	Legal Obligation.
Ensuring Business Processes are	Legitimate Interests.

Adhered to.	
Updating and Enhancing Customer Records.	Contract.
Statutory Returns.	Contract.
Ensuring the Confidentiality of Commercially Sensitive Information.	Legitimate Interests.
Statistical analysis to help us manage our business.	Legitimate Interests and Legal Obligation.
Preventing Unauthorised Access and Modification to our Systems.	Legitimate Interests and Legal Obligation.
Ensuring Safe Working Practices, Staff Administration and Assessments.	Legitimate Interests and Legal Obligation.
External Audits and Quality Checks.	Legitimate Interests and Legal Obligation.
Marketing Our Service to Former Customers.	Consent and/or Legitimate Interests.
Marketing Our Service to Customers.	Consent and/or Legitimate Interests.
Marketing Our Service to Prospects Who Have Shown an Interest in Our Service.	Consent and/or Legitimate Interests.
Marketing Our Service to Prospects Who We Have Had No Previous Dealings.	Consent and/or Legitimate Interests.

Special Categories of Personal Data

Threpolys conducts no activity which requires the collection or processing of Special Categories of Personal Data.

Marketing Activities

We may use your personal data to send you updates (by email, direct online messaging or telephone) about our products and services, including exclusive offers, promotions or new products and services.

We have a legitimate interest in using your personal data for marketing purposes (see above). This means we do not always need your consent to send you marketing information. However, where consent is needed, we will ask for this separately and clearly.

You have the right to opt out of receiving marketing communications at any time:

- Contact us at info@threpoly.com.
- Use the unsubscribe link in emails.
- Updating your marketing preferences by contacting us.

We may ask you to confirm or update your marketing preferences if you ask us to provide further products and services in the future, or if there are changes in the law, regulation, or the structure of our business.

Personal Data Sharing and Transfers

We routinely share personal data with:

- Third parties we use to help deliver our products and services to you, e.g. vendors, strategic partners, resellers, payment service providers.
- Other third parties we use to help us run our business, e.g. marketing agencies or website hosts.
- Third parties approved by you, e.g. social media sites you choose to link your account to or third party payment providers.
- Our insurers and brokers

We only allow our service providers to handle your personal data if we are satisfied they take appropriate measures to protect your personal data. We also impose contractual obligations on service providers to ensure they can only use your personal data to provide services to us and to you.

We may also need to:

- Share personal data with external auditors, e.g. in relation to ISO accreditation and the audit of our accounts.
- Disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.
- share some personal data with other parties, such as potential buyers of some or all of our business or during a restructuring—usually, information will be

anonymised but this may not always be possible, however, the recipient of the information will be bound by confidentiality obligations.

If you would like more information about who we share our data with and why, please contact us using the information at the end of this policy.

We will not share your personal data with any other third party.

Transferring Personal Data Outside of the UK

To deliver services to you, it is sometimes necessary for us to share your personal data outside the UK, e.g.:

- With your and our service providers located outside the UK.
- If you are based outside the UK.
- Where there is a European and/or international dimension to the services we are providing to you.

Under data protection law, we can only transfer your personal data to a country or international organisation outside the UK where.

- The UK government has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'adequacy decision');
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- A specific exception applies under data protection law.

These are explained below.

We may transfer your personal data to certain countries, on the basis of an adequacy decision. These include:

- All European Union countries, plus Iceland, Liechtenstein and Norway (collectively known as the 'EEA'); Gibraltar; and
- Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The list of countries that benefit from adequacy decisions will change from time to time. We will always seek to rely on an adequacy decision, where one exists.

Other countries or international organisations we are likely to transfer personal data to do not have the benefit of an adequacy decision. This does not necessarily mean they provide poor protection for personal data, but we must look at alternative grounds for

transferring the personal data, such as ensuring appropriate safeguards are in place or relying on an exception, as explained below.

Where there is no adequacy decision, we may transfer your personal data to another country or international organisation if we are satisfied the transfer complies with data protection law, appropriate safeguards are in place, and enforceable rights and effective legal remedies are available for data subjects.

The safeguards will usually include using legally-approved standard data protection contract clauses.

To obtain a copy of the standard data protection contract clauses and further information about relevant safeguards, please contact us.

In the absence of an adequacy decision or appropriate safeguards, we may transfer personal data to a third country or international organisation where an exception applies under relevant data protection law, e.g.:

- You have explicitly consented to the proposed transfer after having been informed of the possible risks.
- The transfer is necessary for the performance of a contract between us or to take pre-contract measures at your request.
- The transfer is necessary for a contract in your interests, between us and another person.
- The transfer is necessary to establish, exercise or defend legal claims.

We may also transfer information for the purpose of our compelling legitimate interests, so long as those interests are not overridden by your interests, rights and freedoms. Specific conditions apply to such transfers and we will provide relevant information if and when we seek to transfer your personal data on this ground.

Personal Data Storage

Personal data may be held at our offices and those of our third party agencies, service providers (including cloud based service providers), representatives and agents as described above.

Some of these third parties may be based outside the UK. For more information, including on how we safeguard your personal data when this happens, see below: "Transferring your personal data out of the UK".

Personal Data Retention

We will keep your personal data while you have an active subscription with us or we are providing products and services to you. Thereafter, we will keep your personal data for five years:

- To respond to any questions, complaints or claims made by you or on your behalf;
- To show that we treated you fairly;
- To keep records required by law.
- To market to you under our legitimate interests unless you have expressly removed this consent.

When it is no longer necessary to keep your personal data, we will delete or anonymise it.

Cookies

Cookies are small files that a site or its service provider transfers to your computer's hard drive through your Web browser (if you allow) that enables the Website's or a service provider's system to recognise your browser and capture and remember certain information. They are also used to help us understand your preferences based on previous or current site activity, which enables us to provide you with improved services and to enable us to understand the use of our Website better. We also use cookies to help us compile aggregate data about site traffic and site interaction so that we can offer better site experiences and tools in the future. This helps us to ensure that our Website is up to date and relevant to your interests and needs.

A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us. You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the Website.

Types of cookies we use:

- Traffic Log Cookies.
- Analytics Cookies.
- Social Media Cookies.
- Shopping cart functionality.
- Advertisement performance assessment and conversion tracking.
- Remarketing advertising.
- IP Tracking.

All Cookies used by and on our Website are used in accordance with current English/Welsh and EU Cookie Laws.

Your Rights

You have the following rights, which you can exercise free of charge:

Right	Detail
Access.	The right to be provided with a copy of your personal data.
Rectification.	The right to require us to correct any mistakes in your personal data.
Erase.	The right to require us to delete your personal data—in certain situations.
Restrict Processing.	The right to require us to restrict processing of your personal data in certain circumstances, eg if you contest the accuracy of the data.
Data Portability.	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party - in certain situations.
To Object.	<p>The right to object:</p> <ul style="list-style-type: none">• At any time to your personal data being processed for direct marketing (including profiling);• In certain other situations to our continued processing of your personal data, eg processing carried out for the purpose of our legitimate interests.
Not to be Subject to Automated Individual Decision Making.	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you.

For further information on each of those rights, including the circumstances in which they apply, please contact us (see 'How to contact us' below) or see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights.

If you would like to exercise any of those rights:

- Please email or write to us - see below.
- Provide enough information to identify yourself (e.g. your full name, address and customer or matter reference number) and any additional identity information we may reasonably request from you.
- Let us know what right you want to exercise and the information to which your request relates.

Personal Data Security

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality. We continually test our systems and are ISO 27001 certified, which means we follow top industry standards for information security.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

If you want detailed information from Get Safe Online on how to protect your information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

Contact and Data Protection Officer

Our Data Protection Officer is Chris Payne, who can be contacted using the email address - chris.payne@threpoly.com.

If you have any questions about this Privacy Policy, please contact our Data Protection Officer using the detail above. If you wish to exercise any of your rights under the Data Protection Act 2018, please contact Threpoly at:

Threpoly Limited,
167-169 Great Portland Street,
5th Floor,
London,
W1W 5PF,
United Kingdom.

info@threpoly.com

You also have the right to lodge a complaint with the Information Commissioner . The Information Commissioner may be contacted at <https://ico.org.uk/make-a-complaint> or telephone: 0303 123 1113.