



PRIVACY POLICY

Broadstairs Consulting Ltd (trading as “**BroadStairs**”) takes your privacy very seriously. Please read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

This privacy policy applies to all and any data we process which will include if you are an employee of one of our clients, in which case, we will specify below the personal data we will collect.

We collect, use and are responsible for certain personal data about you. When we do so we are subject to the UK General Data Protection Regulation (*UK GDPR*). We are also subject to the EU General Data Protection Regulation (*EU GDPR*) in relation to services we offer in the European Economic Area (*EEA*).

KEY TERMS

It would be helpful to start by explaining some key terms used in this policy:

We, us, our: BroadStairs, part of The WayFinders Group

Personal data: any information relating to an identified or identifiable individual.

Special category personal data: personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership.

Genetic and biometric data (when processed to uniquely identify an individual): data concerning health, sex life or sexual orientation and information about criminal convictions and offences.

Data subject: the individual who the personal data relates to.

PERSONAL DATA WE COLLECT

We may collect and use the following personal data about you:

- your name, title and contact information, including email address and telephone number and company/organisation details such as ID or employee number;
- information to check and verify your identity such as your date of birth;
- your gender;
- location and address data;
- employment records;
- your personal or professional interests;

- your professional online presence such as your LinkedIn profile;
- information about how you use our website, IT, communication and other systems;
- your responses to questionnaires, surveys, competitions and promotions;
- special category personal data.

We may collect and use this personal data to provide services to you or your employer. If you do not provide personal data we ask for, it may delay or prevent us from providing services to you or your employer. In this case, we may have to cancel a service, but we will notify you if this is the case at the time.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

HOW YOUR PERSONAL DATA IS COLLECTED

We collect most of this personal data directly from you in person, by telephone, text or email and/or via our website. This includes personal data you provide when you:

- apply for our services;
- fill in one of our questionnaires;
- subscribe to our publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey;
- give us feedback or contact us.

However, we may also collect information:

- from publicly accessible sources based inside the UK such as Companies House;
- directly from a third party who could be based inside or outside of the UK or the EEA such as:
- analytics providers such as Google;
- advertising networks such as Google, Facebook or LinkedIn;
- search information providers such as Google;
- from a third party with your consent such as your bank; [and]
- from cookies, server logs and other similar technologies on our website; for more information on our use of cookies, please see our cookie policy [(below)].

Our questionnaires are hosted on sites used by recognised providers whose services and features adhere to the high privacy bar and data protection standards required of data processors by the UK GDPR and the EU GDPR.

HOW AND WHY WE USE YOUR PERSONAL DATA

Under data protection law, we can only use your personal data if we have a proper reason such as:

- where you have given consent;
- to comply with our legal and regulatory obligations;
- for the performance of a contract we are about to enter into or have entered into with you or to take steps at your request before entering into a contract; or
- for our legitimate interests or those of a third party.

A legitimate interest is when we have a business or commercial reason to use your information, so long as this is not overridden by your own rights and interests. We will carry out an assessment when relying on legitimate interests, to balance our interests against your own.

The table below explains what we use your personal data for and why:

What we use your personal data for	Our reasons for using your personal data
Providing services to you.	To perform our contract with you or to take steps at your request before entering into a contract.
Providing services to your employer.	To perform our contract with your employer.
Preventing and detecting fraud against you or us.	For our legitimate interests or those of a third party, ie, to minimise fraud that could be damaging for you and/or us.
Activities necessary to comply with professional, legal and regulatory obligations that apply to our business such as under health and safety law.	To comply with our legal and regulatory obligations.
Ensuring business policies are adhered to such as policies covering security and internet use.	For our legitimate interests or those of a third party, ie, to make sure we are following our own internal procedures so we can deliver the best service to you.
Statistical analysis to help us manage our business such as in relation to our financial performance, customer base, product range or other efficiency measures.	For our legitimate interests or those of a third party, ie, to be as efficient as we can so we can deliver the best service to you at the best price.
Preventing unauthorised access and modifications to systems.	For our legitimate interests or those of a third party, ie, to prevent and detect criminal activity

	that could be damaging for you and/or us. To comply with our legal and regulatory obligations.
Updating and enhancing customer records.	To perform our contract with you or to take steps at your request before entering into a contract. To comply with our legal and regulatory obligations. For our legitimate interests or those of a third party such as making sure that we can keep in touch with our customers about existing services and new services.
Statutory returns.	To comply with our legal and regulatory obligations.
Ensuring safe working practices, staff administration and assessments.	To comply with our legal and regulatory obligations. For our legitimate interests or those of a third party such as to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you.
Marketing our services to: existing and former customers; - third parties who have previously expressed an interest in our services; third parties with whom we have had no previous dealings.	For our legitimate interests or those of a third party, ie, to promote our business to existing and former customers.
External audits and quality checks such as for ISO and the audit of our accounts.	For our legitimate interests or those of a third party, ie, to maintain our accreditations so we can demonstrate we operate at the highest standards.

Where we process special category personal data, we will also ensure we are permitted to do so under data protection laws such as:

- we have your explicit consent;
- the processing is necessary to protect your (or someone else’s) vital interests where you are physically or legally incapable of giving consent; or
- the processing is necessary to establish, exercise or defend legal claims.

MARKETING

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

We have a legitimate interest in using your personal data for marketing purposes (see above ‘**How and why we use your personal data**’). This means we do not usually 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 by using the ‘unsubscribe’ link in our marketing emails.

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

We will always treat your personal data with the utmost respect and never sell it with other organisations for marketing purposes.

WHO WE SHARE YOUR PERSONAL DATA WITH

We routinely share personal data with:

- third parties we use to help deliver our services to you;
- other third parties we use to help us run our business such as marketing agencies, website hosts, lawyers, auditors, insurers and brokers;
- HM Revenue & Customs, regulators and other authorities;
- our bank(s).

If you are an employee of one of our clients and you have completed one of our questionnaires, we may share your personal data within external third parties, principally our client/your employer, in an anonymised and typically aggregated form. We do not provide our client/your employer with raw data, but with a report based on the data that we have collected. This will typically include only aggregated data; the only time that we will share non-aggregated data is if we want to quote from a survey response in a report that we make to our client/your employer. In these circumstances the quote would be anonymised and we would also ensure that it is not possible to ascertain who made the comment from what we disclose. The overriding principle that we work to is that no-one should be identifiable, and no individual or group can be put at risk from retaliation as a result of what we present. We will only retain survey data for as long as reasonably necessary to fulfil the purposes we collected it for, namely, to provide a report to our client/your employer. Within three months of us reporting to our client/your employer, we will remove the survey data from our server.

We only allow our service providers to handle your personal data if we are satisfied that 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 such as in relation to ISO 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 (see '**How to contact us**' below).

WHERE YOUR PERSONAL DATA IS HELD

Personal data may be held at our offices, on our servers (Google) and those of our third party agencies, service providers, representatives and agents as described above (see above: '**Who we share your personal data with**').

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

HOW LONG PERSONAL DATA WILL BE KEPT

We will keep your personal data while you have an account with us or we are providing services to you. Thereafter, we will keep your personal data for as long as is necessary:

- 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.

We will not keep your personal data for longer than necessary. Different retention periods apply for different types of personal data. When it is no longer necessary to keep your personal data, we will delete or anonymise it.

TRANSFERRING YOUR PERSONAL DATA OUT OF THE UK AND EEA

To deliver services to you, it is sometimes necessary for us to share your personal data outside the UK/EEA such as:

- with your and our service providers and/or our affiliated companies located outside the UK/EEA;
- if you are based outside the UK/EEA;
- 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/EEA where:

- the UK government or, where the EU GDPR applies, the European Commission 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.

ADEQUACY DECISION

We may transfer your personal data to certain countries, based on 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 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.

TRANSFERS WITH APPROPRIATE SAFEGUARDS

Where there is no adequacy decision, we may transfer your personal data to another country 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.

TRANSFERS UNDER AN EXCEPTION

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

- 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; or
- 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 we seek to transfer your personal data on this ground.

FURTHER INFORMATION

If you would like further information about data transferred outside the UK/EEA, please contact us (see '**How to contact us**' below).

YOUR RIGHTS

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

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.
Erasure (also known as the right to be forgotten)	The right to require us to delete your personal data in certain situations.
Restriction of 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	The right to object: 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 such as 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).

If you would like to exercise any of those rights, please:

- email, call or write to us — see below: '**How to contact us**';
- provide enough information to identify yourself such as your full name and address and any additional identity information we may reasonably request from you; and
- let us know what right you want to exercise and the information to which your request relates.

KEEPING YOUR PERSONAL DATA SECURE

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 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.

HOW TO COMPLAIN

Please contact us if you have any query or concern about our use of your information (see below '**How to contact us**'). We hope we will be able to resolve any issues you may have.

You also have the right to lodge a complaint with the Information Commissioner (www.ico.org.uk) or any relevant European data protection supervisory authority.

THIRD-PARTY LINKS

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

HOW TO CONTACT US

You can contact us by post or email if you have any questions about this privacy policy or the information we hold about you, to exercise a right under data protection law or to make a complaint. Our contact details are shown below:

FAO: Director
Broadstairs Consulting Ltd
42A High Street
Broadstairs
Kent, CT10 1JT

info@charttheuncharted.com

CHANGES TO THIS PRIVACY POLICY

We keep our privacy policy under regular review. This privacy policy was published on 3 July 2024 and was last updated on 3 July 2024. We may change this privacy notice from time to time, when we do so we will post a new version to this website.