
PRIVACY POLICY

PURPOSE

Transparency Solutions Limited respects your privacy and is committed to protecting your Personal Data.

This privacy policy will inform you as to how we look after your Personal Data and tell you about your privacy rights and how the law protects you.

This privacy policy aims to give you information on how we collect and process your Personal Data through your use of our services, including any data you may provide through our website when you sign up or purchase a service.

Our services are not intended for children and we do not knowingly collect data relating to children.

It is important that you read this privacy notice together with any other privacy notice or fair Processing notice that we may provide on specific occasions when we are collecting or Processing Personal Data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

DEFINITIONS

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes sensitive personal data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Processing: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

CERTIFICATIONS

As part of our commitment to demonstrate compliance with current data protection legislation we have obtained ISO9001 and ISO27001 certifications.

PRINCIPLES

All persons who process Personal Data with our permission must endorse and adhere to these principles at all times and especially when they obtain, handle, process, transfer, store or erase Personal Data.

The six fundamental principles of Personal Data Processing are as follows:

1. Fairness, lawfulness and transparency
All Personal Data must be processed fairly, lawfully and transparently.
2. Purpose limitation
All Personal Data must be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner that is incompatible with those purposes.
3. Minimisation
All Personal Data must be adequate, relevant and limited to what is necessary for the purpose for which they are processed.
4. Accuracy
All Personal Data must be accurate and where necessary, kept up to date with regards to the purposes. Every reasonable step to rectify or erase inaccurate Personal Data must be taken without delay.
5. Storage limitation
No Personal Data should be kept in a form which permits identification of a Data Subject for longer than is necessary to achieve the purpose.
6. Integrity and confidentiality
All Personal Data must be processed in a manner that ensures appropriate security of the Personal Data. At the very least, it must always be protected against unauthorised or unlawful Processing, accidental loss, destruction or damage, by using appropriate technical and organisational measures.

As the Data Controller, we are ultimately accountable for each of these principles and are obliged by law to be able to demonstrate compliance at all times. It is for this reason that we are required to take responsibility for the strict adherence to these principles by all of our staff and processors.

We will notify you of any changes that apply to you, where appropriate, in writing.

THE DATA WE COLLECT ABOUT YOU

Personal Data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of Personal Data about you:

1. "Identity Data" includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
2. "Contact Data" includes billing address, delivery address, email address and telephone numbers.
3. "Financial Data" includes bank account and payment card details.

4. “Transaction Data” includes details about payments to and from you and other details of products and services you have purchased from us.
5. “Technical Data” includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.
6. “Profile Data” includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
7. “Usage Data” includes information about how you use our services and website.
8. “Marketing and Communications Data” includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. aggregated data is data which may be derived from your Personal Data but is not considered Personal Data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. 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 notice.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

If you fail to provide Personal Data

Where we need to collect Personal Data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

CONDITIONS FOR PROCESSING DATA

Under data protection legislation the Processing of Personal Data is prohibited unless there is a legitimate legal basis upon which the data is being processed. There are six potential legal bases for Processing.

All persons authorising the Processing of Personal Data must be assured that at least one of the following bases applies:

Legal bases for Personal Data Processing

We have set out below, in a table format, a description of all the ways we plan to use your Personal Data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your Personal Data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your Personal Data where more than one ground has been set out in the table below.

Purpose/Activity	Type of data	Lawful basis for Processing including basis of legitimate interest
To register you as a new customer	(a) Identity	Performance of a contract with you

	(b) Contact	
To process, deliver and perform your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)
To administer and protect our business and our website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our services, website, marketing, customer relationships and experiences	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile	Necessary for our legitimate interests (to develop our products/services and grow our business)

To ensure compliance with GDPR Transparency has undertaken a 'Legitimate Interest Assessment' for both prospects and customers to ensure the privacy rights of these individuals have been given due consideration.

COLLECTING DATA

We use different methods to collect data from and about you, including:

Direct interactions. You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes Personal Data you provide when you:

1. Apply or enquire about our services.
2. Subscribe to our services or publications.
3. Request marketing to be sent to you.
4. Enter a competition, promotion or survey.
5. Give us feedback.
6. Communicate with us via social media (this includes, likes, follows, retweets and any other method of interaction via social media).

Automated technologies or interactions. As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this Personal Data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy for further details.

Third parties or publicly available sources. We may receive Personal Data about you from various third parties and public sources as set out below:

1. Technical Data from the following parties:
 - (i) analytics providers such as Google based outside the EU;
 - (ii) advertising networks; and
 - (iii) search information providers.
2. Contact, Financial and Transaction Data from providers of technical, payment and delivery services.
3. Identity and Contact Data from data brokers or aggregators.
4. Identity and Contact Data from publicly available sources.

HOW WE USE YOUR PERSONAL DATA

We will only use your Personal Data when the law allows us to. Most commonly, we will use your Personal Data in the following circumstances:

1. Where we need to perform the contract that we are about to enter into or have entered into with you.
2. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
3. Where we need to comply with a legal or regulatory obligation.

Generally we do not rely on Consent as a legal basis for Processing your Personal Data other than in relation to sending third party direct marketing communications to you via email or text message.

You have the right to withdraw Consent to marketing at any time by contacting us.

Marketing

We strive to provide you with choices regarding certain Personal Data uses, particularly around marketing and advertising. We have established the following Personal Data control mechanisms:

Promotional offers from us

We may use your Identity, Contact, Technical, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which services and offers may be relevant for you.

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us or if you provided us with your details when you registered for a promotion or completed a survey and, in each case, you have not opted out of receiving that marketing.

Third-party marketing

We will get your express opt-in Consent before we share your Personal Data with any company for marketing purposes.

Opting out

You can ask us or associated third parties to stop sending you marketing messages at any time by contacting us.

Where you opt out of receiving marketing from us, this will not apply to Personal Data provided to us as a result of a service purchase, service experience or other transaction.

Cookies

Our website uses cookies. You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our website may become inaccessible or not function properly.

Change of purpose

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the Processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your Personal Data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Data without your knowledge or Consent, in compliance with the above rules, where this is required or permitted by law.

DISCLOSURE OF YOUR PERSONAL DATA

With regards to the purposes set out in the table in the 'Conditions for Processing Data' section of this policy, we may have to share your Personal Data with the parties set out below:

1. service providers acting as processors who provide IT and system administration services to us;
2. professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services to us;
3. HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of Processing activities in certain circumstances; or
4. third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a

change happens to our business, then the new owners may use your Personal Data in the same way as set out in this privacy notice.

We require all third parties to respect the security of your Personal Data and to treat it in accordance with the law. We do not allow our third-party service providers to use your Personal Data for their own purposes and only permit them to process your Personal Data for specified purposes and in accordance with our instructions.

INTERNATIONAL DATA TRANSFERS

We share your Personal Data with select third parties. This may involve transferring your data outside the European Economic Area (EEA).

Where an external third party is based outside the European Economic Area (EEA), their Processing of your Personal Data will involve a transfer of data outside the EEA.

Whenever we transfer your Personal Data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented by the third party.

Where we use certain service providers, we may use specific contracts approved by the European Commission which give Personal Data the same protection it has in Europe. For further details, see European Commission: Model contracts for the transfer of Personal Data to third countries.

Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to Personal Data shared between Europe and the US. For further details, see European Commission: EU-US Privacy Shield.

Please contact us if you want further information on the specific mechanism used by us when transferring your Personal Data out of the EEA.

INFORMATION SECURITY

We regularly review our approach to information security and stay up to date with developments in the field and emerging threats. To secure the information we hold we are committed to allocating sufficient resources (including time and budget) to ensure that robust and high-quality tools and processes are implemented.

Transparency takes all reasonable steps to protect and maintain the integrity, confidentiality and availability of Personal Data within our control. For the purposes of this policy, organisational and technological security measures are in place to protect and secure against: accidental loss, damage, destruction, theft or unsanctioned disclosure, publication or transfer of Personal Data.

We have put in place appropriate security measures to prevent your Personal Data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your Personal Data to those employees, agents, contractors and other third parties who have a legitimate business reason to access it. They will only process your Personal Data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

BREACH AND INCIDENT REPORTING

Serious breaches will be reported to the relevant supervisory authority by us within 72 hours of us becoming aware of the breach.

THE RIGHTS OF DATA SUBJECTS

All reasonable efforts will be made to verify your identity before carrying out any requests or disclosures of information made by you. These efforts may include the request for additional personal information where necessary.

Under Data Protection Legislation, you have the following rights:

1. Request access to your Personal Data (commonly known as a "data subject access request"). This enables you to receive a copy of the Personal Data we hold about you and to check that we are lawfully Processing it.
2. Request correction of the Personal Data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
3. Request erasure of your Personal Data. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your Personal Data where you have successfully exercised your right to object to Processing (see below), where we may have processed your information unlawfully or where we are required to erase your Personal Data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
4. Object to Processing of your Personal Data where we are relying on a Legitimate Interest (or those of a third party) and there is something about your particular situation which makes you want to object to Processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are Processing your Personal Data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
5. Request restriction of Processing of your Personal Data. This enables you to ask us to suspend the Processing of your Personal Data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
6. Request the transfer of your Personal Data to you or to a third party. We will provide to you, or a third party you have chosen, your Personal Data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided Consent for us to use or where we used the information to perform a contract with you.
7. Withdraw Consent at any time where we are relying on Consent to process your Personal Data. However, this will not affect the lawfulness of any Processing carried out before you withdraw your Consent. If you withdraw your Consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your Consent.

It is important that the Personal Data we hold about you is accurate and current. Please keep us informed if your Personal Data changes during your relationship with us.

DATA RETENTION

How long will you use my Personal Data for?

We will only retain your Personal Data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for Personal Data, we consider the amount, nature, and sensitivity of the Personal Data, the potential risk of harm from unauthorised use or disclosure of your Personal Data, the purposes for which we process your Personal Data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers.

In some circumstances you can ask us to delete your data: see Request erasure below for further information.

In some circumstances we may anonymise your Personal Data (so that it can no longer be associated with you) for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

SUBJECT ACCESS REQUESTS

Making a request

If you wish to make a subject access request to verify the lawfulness and accuracy of the Personal Data we hold about you, you must put your request in writing (letter or e-mail) and submit it to a member of the Senior Management Team.

Your request should be specific about the nature and the type of data you require.

Every attempt will be made to comply with your request in a timely manner and without undue delay.

Upon receipt of the information you are encouraged to check the accuracy of the information and to advise Transparency of any updates that may need to be made.

A fee will not be charged for an access request, except where a request is deemed to be 'manifestly excessive' or you have already been provided with the information.

No fee usually required

You will not have to pay a fee to access your Personal Data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that Personal Data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you of the anticipated time frame for a response and keep you updated.

FURTHER INFORMATION

Any queries or comments about this policy, or any concerns that the policy has not been followed, should be addressed to a member of the Senior Management Team.