OUR DATA PROTECTION POLICY

In the course of your work and interaction with us, we could collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example names and addresses.

The UK's data protection legislation, including the UK General Data Protection Regulations (UK GDPR) contains strict principles and legal conditions which must be followed before and during the processing of any personal information.

Everyone has a responsibility to comply with the principles and legal conditions provided by the data protection legislation, including the UK GDPR. Failure to meet those responsibilities is likely to lead to serious consequences. We all want to avoid that.

We are committed not only to the letter of law, but also to the spirit of the law. It's really important to us that we handle all personal data correctly, lawfully and in a fair way. And that we respect the legal rights, privacy and trust of all the people we deal with.

This Policy sets out our obligations, here at Astrantia People Consulting Limited, relating to data protection and the rights of our customers, clients, agents, contractors, business contacts, suppliers and any other parties working on our behalf, in respect of their personal data under data protection law.

Information you need to know about us
For clarity, our company is registered in England and Wales and our registered office is Westbury House, Steam Mills, Midsomer Norton BA3 2JY.

Our Data Protection Officer is Sam Baker. Sam is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures and/or guidelines.

If you have any questions relating to this Policy, or to Data Protection Law and how that applies to Astrantia People Consulting Limited, you should contact Sam. Her contact details are at the end of this Policy.

Here's a few examples of the type of query she can help with:

- if you're unsure about the lawful basis on which personal data is collected, held, and/or processed;
- if you have a query relating to the retention period for any type of personal data;
- if you have a question about our privacy notices or policy documentation;
- if you need assistance in dealing with, or are submitting data subject access requests;
- if you suspect, or know, a personal data breach has happened; or
- if you're unsure about our data security processes and the steps we take to protect personal data.

Definitions
You'll find some terminology included in this policy that relates specifically to terms used in the legislation. We've provided definitions for those below.

Consent: the consent of the data subject which must be a freely given,

	specific, informed, and an unambiguous indication of the data subject's wishes, signifying their agreement to the processing of personal data relating to them.
Data Breach:	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Data Controller:	a natural or legal person or organisation that determines the means and the purpose of processing the personal data.
Data Processor	a natural or legal person or organisation that processes personal data on behalf of a data controller.
Data Subject:	a living, identified, or identifiable natural person whose personal data is held by us.
Data Protection Legislation:	includes (i) the Data Protection Act 2018, (ii) the UK General Data Protection Regulation **(UK GDPR)** and any national implementing laws, regulations and secondary legislation, for so long as the UK GDPR is effective in the UK, and the E-Privacy Directive (and its proposed replacement), once it becomes law.
Personal data:	any information that identifies a living, identified, or identifiable natural person (data subject) who can be identified, directly or indirectly, in particular by reference to an identifier e.g. name, location data, identification number etc. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous or the identity has been permanently removed making it impossible to link back to the data subject.
Processing:	any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.
Special categories of personal data:	any personal data which reveals a data subject's ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.
Criminal records data:	information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

What are the UK GDPR principles?

Astrantia People Consulting Limited is a data controller. This means that we are required by law to

make sure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the UK GDPR principles.

In brief, the principles say that:

- personal data must be processed in a lawful, fair and transparent way;
- the purpose for which the personal information is collected must be specific, explicit and legitimate;
- collected personal data must be adequate and relevant to meet the identified purpose;
- the information must be accurate and kept up to date;
- personal data should not be kept in a form which allows identification of a data subject for longer than is necessary for the purposes for which it is used; and
- personal data must be kept confidential and secure and only processed by authorised people.

Other rules under the UK GDPR include:

- The transfer of personal data to a country or organisation outside the UK should only take place if appropriate safeguarding measures are in place to protect the security of that data.
- The data subject must be permitted to exercise their rights in relation to their personal data.

Astrantia People Consulting Limited must comply with these principles and rules at all times in our information-handling practices. We are committed doing that and to making sure these principles and rules are followed. We take the security and protection of data very seriously.

What are the lawful reasons under which we would expect you to process personal data?

Whilst carrying out our work activities we are likely to process personal data. Astrantia People Consulting Limited will only expect to process personal data where the business has a lawful basis to do that. That may be any one of the following reasons or a combination of:

- consent has been obtained from the data subject to process their personal data for specified purposes;
- we need to perform the contract we have entered into with the data subject, either for employment or commercial purposes;
- we need to comply with a legal obligation; or
- it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where we may need to process the data subject's personal information. These include:

- where we need to protect the data subject's interests (or someone else's interests); or
- where it is needed in the public interest or for other official purposes.

We will always make sure we keep a documentary record of the legal basis we're relying on for each processing activity we perform.

Privacy Notices - Personal data must be processed in a lawful, fair and transparent way

Before we begin collecting or processing personal data directly from a data subject we will make sure that an appropriate privacy notice has been issued. Different notices are used for employment and commercial purposes. The content of the privacy notice must provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must also

explain how, when and for how long we propose to process the data subject's personal information. We need to include information around the data subject's rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where we intend to collect data indirectly from a third party or a public source (i.e. electoral register), we must ensure that a privacy notice is issued to the data subject within a reasonable period of obtaining the personal data and no later than one month after. If the data is used to communicate with the individual, then at the latest, it should be issued when the first communication takes place or, if disclosure to someone else is envisaged, a privacy notice should be issued, at the latest, when the data is disclosed.

We will only use data collected indirectly if we have evidence that it has been collected in accordance with the UK GDPR principles.

Purpose Limitation - The purpose for which the personal information is collected must be specific, explicit and legitimate
When we collect personal information we will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason we have previously identified, we will usually stop processing that information. However, in limited circumstances we can continue to process the information, provided that our new reason is lawful.

Adequate and relevant - The collected personal data must be adequate and relevant to meet the identified purpose
We will only process personal data where we have been authorised to do so because it relates to our work or we have been delegated temporary responsibility to process the information. We will not collect, store or use unnecessary personal data. We will make sure personal data is deleted, erased or removed in line with our Data Retention Policy. We will not process or use personal data for non-work related purposes.

We'll review our records on a regular basis to make sure we don't hold out-of-date or irrelevant information and to check there are lawful reasons for us to continue to hold that information.

Accurate and kept up to date - The information must be accurate and kept up-to-date
If personal information changes, for example a Client changes their address, we ask them to let us know as soon as is practicable so that our records can be updated. We won't be responsible for any inaccurate personal data held on our systems where someone has failed to notify us of a change to their circumstances.

Kept for longer than is necessary - The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used
Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. Any data we decide we don't need to hold will be destroyed in accordance with our Data Retention Policy.

Kept confidential and secure - The personal data must be kept confidential and secure and only processed by authorised personnel
To achieve this we will:

- have in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or

destruction of, or damage to data.

- use code words or passwords before releasing personal information.
- only transmit personal information between locations by e-mail if a secure network is in place.
- make sure that any personal data is held and kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- make sure that, when working on personal information as part of the work we do, we observe the terms of this policy and the data protection legislation, in particular in matters of data security.
- dispose any hard copy personal information securely.
- make sure data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in a secure location in the workplace.
- make sure that data held on computers are stored confidentially e.g. password protection, encryption or coding.
- have network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

Transfer to another country - Transfer of personal data to countries or organisations outside of the UK should only take place if appropriate safeguarding measures are in place to protect the security of that data

We do not generally have a need to transfer data outside of the UK. However, if we are asked to transfer personal data to a country or organisation outside of the UK we won't do that until we can confirm it's done in a legally compliant manner.

Direct Marketing

We are subject to specific rules under the UK GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing. We'll make sure there is an opportunity to request that.

The data subject rights - The data subject must be permitted to exercise their rights in relation to their personal data

Under the UK GDPR, data subjects have some legal rights regarding how their personal data is processed. At any time a data subject can ask us to take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Withdraw their consent if consent was the legal basis for processing
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

There are different rules and timeframes that apply to each of these rights.

Data Subject Access

Anyone has the right to request access to any personal data we hold about them. Although we don't employ people directly, we may hold limited personal data relating to clients, customers, suppliers, or

individuals whose information is shared with us as part of the HR-related work we do.

In most cases, the information we receive from our clients is anonymised or aggregated. Where we do hold identifiable personal data, this is limited to what is necessary for us to be able to deliver our services, such as business-contact details or information provided directly by clients.

Anyone whose personal data we process may submit a data subject access request. If we receive a request, we will respond in line with the responsibilities we have as set out in Data Protection Law. We will provide access unless an exemption applies.

For clarity, we do not normally charge a fee for responding to a data subject access request. However, in line with UK GDPR, we may charge a reasonable fee if a request meets the definition of being manifestly unfounded, excessive, or repetitive, or where additional copies of information are requested.

Correction of Personal Data
Data subjects have the right to ask us to correct any personal data that is inaccurate or incomplete. If we receive a request, we'll make the necessary amendments. We'll contact the data subject to confirm that, within one month of receipt of their request. We can extend that timescale to two months if the request is complex. If any personal data that is to be corrected has been disclosed to a third party, we will make all reasonable effort to contact them to inform them of the request.

Erasure of Personal Data
Data subjects have the right to ask us to erase their personal data in the following circumstances:

- when it's no longer necessary for us to hold that data for the purpose it was originally collected or processed;
- they want to withdraw their consent to us holding and processing their personal data;
- they object to us holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so)
- personal data has been processed unlawfully; or
- personal data needs to be erased in order for us to comply with our legal obligations.

We will act on all the requests we receive, unless we have reasonable grounds to refuse them. In that instance, we'll contact the data subject to confirm that, within one month of receipt of their request. We can extend that timescale to two months if the request is complicated. If any personal data that is to be erased has been disclosed to a third party, we will make all reasonable effort to contact them to inform them of the request.

Objecting to the processing of data
Data subjects have the right to object to us processing their personal data for legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

- When we receive a request for legitimate interests, we'll stop processing their data immediately, unless we can demonstrate that our legitimate interests overrides their interests, rights and freedoms, or that the processing is necessary for legal purposes.

- When we receive a request for direct marketing purposes, we'll stop processing their personal data promptly.

- When we receive a request for scientific and/or historical research and statistical purposes, we'll expect that, as set out in UK GDPR, to demonstrate the grounds relating to their particular situation. We may refuse a request if the information is needed for research that serves the public interest.

Restriction of Personal Data Processing
Data subjects may ask us to stop processing their personal data If we receive a request, we'll only keep the amount of personal data relating to the data subject, that is necessary to make sure the personal data in question is not processed further. If any personal data that is to be restricted has been disclosed to a third party, we will make all reasonable effort to contact them to inform them of the request.

Categories of information
During the course of our work, we may be required to process personal data which falls into different categories, general personal data and special categories of personal data. All data will be processed in accordance with our responsibilities and obligations, and in a confidential manner. However, where that data is classed as a special category, extra care will be taken to ensure the privacy and security of that data.

This means that we will maintain a high level of security and only share this data with those who are also authorised to process that data.

We may need to process special categories of information in connection with customers and other third parties. There may also be circumstances where we need to process information in relation to assist with legal claims or to protect a data subject's interests (or someone else's) or process information in relation to criminal convictions. We'll do this with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force in our business.

When we seek consent
In limited circumstances we may need consent from a data subject to process personal data or special categories of data. As a result, it may be necessary to ask a data subject to provide written consent to allow the processing of special categories of personal data. In that situation, we will provide details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

We will not force anyone to provide written consent. Giving consent will always be a decision made by free will and choice. It is not a contractual condition. Consent can be withdrawn at any time without any reason provided. We will not subject a data subject to a sanction or detriment as a consequence of withdrawing consent.

Exemptions
In limited circumstances there are certain categories of personal data which are exempt from the UK GDPR regime. These include:

- confidential references that are given by a company to third parties or received by a company from third parties.
- management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).

- data which is required by law to be publicly available.
- documents subject to legal professional privilege.

Action to be taken in the event of a data protection breach
We have more detailed information in our Data Breach Policy, however here's a summary of the key steps we'd take in a situation like this.

In the event of an actual or suspected security incident or data breach, we will:
- undertake an initial assessment;
- contain the breach;
- assess what we can do to recover the data and/or limit any further damage;
- establish who needs to be notified of the situation;
- determine the best course of action to resolve or remedy the situation
- record what has happened and any/all steps taken.

The Data Protection Officer will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Record keeping
As Astrantia People Consulting has less than 250 employees, we only need to document processing activities that:
- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data.

Training
All employees of Astrantia People Consulting Limited, that handle personal information of individuals must have a basic understanding of the data protection legislation, including the UK GDPR. We will regularly review all data processing activities to make sure we are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Automated processing and decision making
From time to time we may use computer programmes to process data and make automated decisions. Where automated processing or decision making does take place and the effect of that processing impacts on the freedoms and legitimate interests of the data subject, then in certain circumstances the data subject can request for human intervention. This means that they can ask for a human to review the machine-made outcome/decision.

Sharing personal data
We will always make sure that personal data is only shared with authorised persons and is shared of the reason we've communicated. Extra care and security will be taken when sharing special categories of data or transferring data outside of Astrantia People Consulting Limited to a third party.

If you do have any questions or require any further information about any aspects of this Policy, or about the procedure we follow, please do contact Sam Baker, Director of Astrantia People Consulting Limited by email at sam@astrantiapeople.co.uk

This Policy was last reviewed and updated: April 2026.

Other associated policies and reference documents:

- Data Breach Policy
- Data Breach Register
- Data Breach Report Form
- Data Retention Policy
- IT and Cyber Security Policy