OUR DATA PROTECTION POLICY

In the course of your work with Astrantia People Consulting Limited, we're likely to collect, use, transfer or store personal information about employees, clients, customers and suppliers, for example their names and home 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 any 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 and failure to meet those responsibilities are likely to lead to serious consequences. We all want to avoid that.

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.

Data Subject:	a living individual.
Data Controller:	the person or organisation that determines the means and the purpose of processing the personal data.
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:	is any information that identifies a living individual (data subject) either directly or indirectly. 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:	is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.
Special categories of personal data:	this includes 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:	means 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 ensure 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;
- the collected personal data must be adequate and relevant to meet the identified purpose;
- the information must be accurate and kept up to date;
- 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; and
- the personal data must be kept confidential and secure and only processed by authorised personnel.

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 to ensuring that these principles and rules are followed, as 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 (or bases) to process that information. The lawful basis 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;
- where we need to perform the contract we have entered into with the data subject, either for employment or commercial purposes;
- where we need to comply with a legal obligation; or
- where 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 you we 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 ensure that we keep a documentary inventory of the legal basis (or bases) which is being relied on in respect of 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 to the data subject. 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 which you 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 for processing the personal information remains compatible with your original lawful purpose (unless our original lawful basis was 'Consent').

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 and we will make sure that personal data is deleted, erased or removed within the Company's retention guidelines. We will not process or use personal data for non-work related purposes.

Astrantia People Consulting Limited will review its records on a regular basis to make sure we do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

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 that they inform us as soon as practicable so that our records can be updated. Astrantia People Consulting Limited will

not be responsible for any inaccurate personal data held on its systems where someone has failed to notify us of the relevant change in 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 which Astrantia People Consulting Limited decides it does not need to hold for a particular period of time will be destroyed in accordance with its retention of data 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, for example, encryption is used for e-mail.
- 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 continue to 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 requested to transfer personal data to a country or organisation outside of the UK we will not transfer personal data to a country or organisation unless we have in place safeguards to ensure this is done in a legally compliant manner.

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

Under the UK GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that Astrantia People Consulting Limited 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.

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 the privacy notice and at all times 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. This should be processed 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 in order to process personal data or special categories of data. As a result, it may be necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. In that situation, we will provide the data subject with 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 compel a data subject to provide written consent. Giving consent will always be a decision made by free will and choice and 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
A personal data breach will arise whenever:
1) any personal data is lost, destroyed, corrupted or disclosed;
2) if someone accesses the data or passes it on without proper authorisation; or
3) if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, we will:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

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. More detail on the steps we will take are set out in our Data Breach Policy.

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 ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. 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.

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 and we will ensure that data subjects are given this option at

first point of contact. When a data subject exercises their right to reject marketing we will desist immediately from sending further communications.

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: January 2025.

Other associated policies and reference documents:

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