ALTRAD

The ingenuity of our people creates endless possibilities

Data protection Manager: Wendy Gould – Senior HRBP

As part of any recruitment process, Altrad collects and processes personal data relating to job applicants. Altrad is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What is personal data?

"Personal data" is any information about a living individual from which they can be identified such as name, ID number, location data, any online identifier (such as IP address), or any factor specific to the physical, physiological, genetic, mental, economic, or social identity of that person. It does not include data where any potential identifiers have been removed (anonymous data) or data held in an unstructured file.

There are "special categories" of more sensitive personal data which are more private in nature and therefore require a higher level of protection, such as genetic data, biometric data, information about sex life or sexual orientation, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health. For the purposes of this notice, personal data relating to criminal convictions will also fall within the description of 'special category' personal data.

When we refer to "processing", this means anything from collecting, using, storing, transferring, disclosing, altering, or destroying personal data.

What information does Altrad collect?

Altrad collects information about you, which is relevant to the recruitment process, and limited to what is necessary for that purpose. This includes:

- your name, address, and contact details, including email address and telephone number.
- details of your qualifications, skills, experience, and employment history.
- information about your current level of remuneration, including benefit entitlements.
- whether or not you have a disability for which Altrad needs to make reasonable adjustments during the recruitment process.
- information about your entitlement to work in the UK; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

Altrad collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment (including online tests).

Altrad
Building 2, Field End Business Park,
Rotherham, S63 0JF, United Kingdom

T +44 (0) 1709 886050
uk.altradservices.com

Altrad will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. Altrad will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does Altrad process personal data?

To pursue our legitimate interests as a business. This may include:

- your contact details such as your name, address, telephone number and personal email address which will be used to communicate with you in relation to the recruitment process.

- your CV, any education history, employment records, professional qualifications and certifications in order for us to consider your suitability for the job you are applying for.

- details of the job role you are applying for any interview notes made by us during or following an interview with you, in order to assess your suitability for that role.

- pay and benefit discussions with you to help determine whether a job offer may be made to you.

- voicemails, emails, correspondence, and other communications created, stored or transmitted by you on or to our computer or communications equipment in order to progress the application through the recruitment process.

- CCTV footage of you onsite for security reasons, for the protection of our property and for health and safety reasons; and

- network and information security data in order for us to take steps to protect your information against loss, theft or unauthorised access.

To comply with our legal obligations or exercise legal rights conferred upon us. This may include:

- checks for eligibility to work in the UK as required by immigration laws, such as passport and visa documentation.

- formal identification documentation relating to you, such as a passport or driving licence, to verify your identity (including your date of birth).

- Disclosure and Barring Service (DBS) checks where we have a legal right or reason for doing so (for further information see section 5 below).

- DVLA checks to validate driving licence information if you are to drive our vehicles as part of the role applied for.

To enable us to perform our legal obligations in respect of employment, social security, social protection law, or as needed in the public interest. This may include:

- special category data such as health information to assess and/or to comply with our obligations under the Equality Act 2010 (for example a requirement to make reasonable adjustments to the recruitment process or your working conditions).

For occupational health reasons or where we are assessing your working capability, subject to appropriate confidentiality safeguards. This may include:

- information about your physical or mental health, or disability status, to assess whether any reasonable adjustments are required for you during the recruitment process and, where you are successful in your application, carrying out any medical assessment required for your role, pension and any insurance benefits.

For statistical purposes in the public interest such as equal opportunities monitoring (for example the collection of information about race, ethnic origin, sex or religion). Any such information shall only be used, once collected, in an anonymised form for statistical purposes and will not be used in relation to your application for employment with us.

For some roles, Altrad has a legal right / reason, to undertake Disclosure and Barring Service (DBS) checks (or in Scotland, a Disclosure Scotland check). Where we do so, we only do so in accordance with our Data Protection Policy, the principles in GDPR, and the prevailing legislation in the area of criminal background checks as updated from time to time. For details on how long we retain criminal convictions information and how it is disposed of, please refer to our DBS policy.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

We may share your personal data and special category personal data with other companies within our group of companies. They may use your personal data as part of our regular reporting activities on performance OR in the context of a business reorganisation or group restructuring exercise OR for systems maintenance support and hosting of data.

Altrad will not share your data with third parties unless your application for employment is successful and it makes you an offer of employment. Altrad will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

We may share your data with our legal and other professional advisers (including accounting and audit services) to provide us with advice in relation to our business, including our legal, financial, and other obligations and claims.

Your data may be transferred outside the European Economic Area (EEA) should this be applicable to your role. Data is transferred outside the EEA on the basis of specify relevant safeguards eg declaration of adequacy, binding corporate rules or other safeguards and link to relevant documents or information if possible.

How does Altrad protect data?

Altrad takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

We limit access to your personal data to those who have a business need to know and they will only process your personal data on our instructions and subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected or actual data security breach and will notify you and the Information Commissioner's Office ("ICO") of a suspected breach where we are legally required to do so.

Whenever we propose using new technologies, or where processing is construed as 'high risk', we are obliged to carry out a data protection impact assessment which allows us to make sure appropriate security measures are always in place in relation to the processing of your personal data.

For how long does Altrad keep data?

If your application for employment is unsuccessful, Altrad will hold your data on file for 12 months after the end of the relevant recruitment process to demonstrate an open and fair recruitment process in defence of a legal claim or to satisfy regulatory requirements. You may ask Altrad to keep your personal data on file for longer consideration for future employment opportunities. At the end of that period, or once you withdraw your consent which you may do at any time, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file [and retained during your employment]. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights.

You may make a formal request for access to personal data and/or special category data that we hold about you at any time. This is known as a Subject Access Request. We will respond to such a request within 1 month. Please note that under the GDPR we are permitted to extend the 1 month time period for responding by an additional 2 months where in our view your request is complex or numerous in nature. We may also charge a reasonable fee based on administrative costs where in our view your request is manifestly unfounded, excessive or is a request for further copies. Alternatively, we may refuse to comply with the request in such circumstances.

Under certain circumstances, by law you also have the right to:

- have your personal data corrected where it is inaccurate.
- have your personal data erased where it is no longer required. Provided that we do not have any continuing lawful reason to continue processing your personal data, we will make reasonable efforts to comply with your request.
- have your personal data be transferred to another person in an appropriate format where we process that data in reliance on your consent and the processing is carried out by automated means.
- withdraw your consent to processing where this is our lawful basis for doing so.
- restrict the processing of your personal data where you believe it is unlawful for us to do so, you have objected to its use and our investigation is pending, or you require us to keep it in connection with legal proceedings; and

to object to the processing of your personal data, where we rely on legitimate business interests as a lawful reason for the processing of your data. You also have the right to object where we are processing your personal data for direct marketing purposes. We have a duty to investigate the matter within a reasonable time and take action where it is deemed necessary. Except for the purposes for which we are sure we can continue to process your personal data; we will temporarily stop processing your personal data in line with your objection until we have investigated the matter. If we agree that your objection is justified in accordance with your rights, we will permanently stop using your data for those purposes. Otherwise, we will provide you with our justification as to why we need to continue using your data. For statistical purposes information such as equal opportunities monitoring (for example the collection of information about race, ethnic origin, sex or religion) may be used, once collected, in an anonymised form and will not be used in relation to your application for employment with us.

We may need to request specific information from you to help us to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. If you withdraw your consent, our use of your personal data which was collected before your withdrawal is still lawful.

You have the right to complain to a supervisory body if you are concerned about the way we have processed your personal data. In the UK this is the ICO – www.ico.org. Although you have the right to complain to the ICO, we encourage you to contact us first with a view to letting us help in resolving any queries or questions.