**Applicant Privacy Notice**

The data controller processing your data is Optivo. We’re registered as a data controller with the Information Commissioner’s Office and are committed to ensuring that the personal data we process is handled in accordance with data protection legislation.We have a Data Protection Officer who can be contacted via dataprotection@optivo.org.uk.

As part of any recruitment process, Optivo collects and processes personal data of job applicants who apply for roles with us. We’re committed to being transparent about how we collect and use data and to meeting our data protection obligations.

By registering to use our online recruitment system and submitting a job application to us, you agree to the terms of this Data Privacy Statement and for your personal information (which might include sensitive personal information) to be processed and held by Optivo and by selected third parties, however any data shared with us will remain inside the EEA.

We use a people process management software solution that is hosted by Jobsgopublic. They’ve got a privacy policy that’s accessible from your Jobsgopublic account.

**What information do we collect?**

We’ll collect a range of information about you. This includes:

* your name, address and contact details, including email address and telephone number;
* your date of birth;
* Identifiers issued by public bodies e.g. NI 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 we need to make reasonable adjustments during the recruitment process;
* information about your entitlement to work in the UK; and
* Equal opportunities monitoring information, including gender, information about your ethnic origin, gender identification, sexual orientation, health, and religion or belief.

We collect 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.

We’ll also collect personal data about you from third parties, such as references supplied by former employers, including information from employment background check providers and information from criminal records checks (where applicable). We’ll seek information from third parties only once a job offer to you has been made and will inform you before we do this.

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

**Why do we process personal data?**

In some cases, we need to process data at your request prior to entering into a contract with you. For example this could include sharing core information from your application with the interview panel.

We’ll also need to process your data in order to enter into a contract with you.

In some cases we need to process data to ensure the information you provide meets our legal obligations. These include:

* Checks to ensure a successful applicant's eligibility to work in the UK before employment starts.
* Perform criminal records checks from the Disclosure and Barring Service (for applicable roles).
* Perform professional registrations and qualifications checks (for applicable roles).

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

We process health information if we need to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out our obligations and exercise specific rights in relation to employment.

We process other special categories of data, such as information about ethnic origin, sexual orientation, health, religion or belief, age, gender or marital status, this is done for the purposes of monitoring our policies in meeting our obligations under the Equality Act 2010, and to provide anonymised statistical reporting, this equal opportunities monitoring is done with the explicit consent of job applicants, which can be withdrawn at any time. This data is collected separately from other information and isn’t used in the recruitment decision-making process.

For some roles, we’re obliged to seek information about criminal convictions and offences. Where we do this, it’s because it’s necessary for us to carry out our obligations and exercise specific rights in relation to employment.

If your application is unsuccessful, we’ll keep your personal data on file in case there are future employment opportunities for which you may be suited. We’ll only keep this data for the retention periods defined in our retention schedules and set out below.

**What’s the legal basis for processing your data?**

Our purpose for processing this information is to assess your suitability for a role you have applied for and to help us develop and improve our recruitment process.

The lawful basis we rely on for processing your personal data is article 6(1)(b) of the GDPR, which relates to processing necessary to perform a contract or to take steps at your request, before entering a contract.

If you provide us with any information about reasonable adjustments you require under the Equality Act 2010 the lawful basis we rely on for processing this information is article 6(1)(c) to comply with our legal obligations under the Act.

The lawful basis we rely on to process any information you provide as part of your application which is special category data, such as health, religious or ethnicity information is article 9(2)(b) of the GDPR, which relates to our obligations in employment and the safeguarding of your fundamental rights. And Schedule 1 part 1(1) of the DPA2018 which again relates to processing for employment purposes.

We process information about applicant criminal convictions and offences. The lawful basis we rely to process this data are Article 6(1)(e) for the performance of our public task. In addition we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a).

**Who has access to data?**

Access to the information you provide to us shall be restricted to authorised users only and is treated in the strictest confidence and shall only be used for the purposes of processing your application and for processing of the aforementioned anonymous statistics. In order for us to process your application your information will normally only be shared internally for the purposes of the recruitment exercise. This includes members of the People 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. On occasion, for specific roles, we may invite a resident panel member to assist in the recruitment exercise and we would share your C.V. or Application Form and supporting documents with them.

We won’t share your data with other third parties, unless your application for employment is successful and we make you an offer of employment. We’ll then share your applicable data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service (if applicable) to obtain necessary criminal records checks. Some of your data may be shared with government bodies such as UK Visa and Immigration (UKVI) to ensure we can demonstrate compliance.

If your application is successful we’ll also share relevant health data (where necessary) with our Occupational Health provider for the purposes of ensuring we meet our employment obligations.

We won’t transfer your data outside the European Economic Area.

**How do we protect data?**

We take IT security very seriously. We’ve got 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.

Application Security

Jobsgopublic employs extensive security measures to protect against the loss, misuse, and unauthorised alteration of data security includes the following standard features \*

* Protection against improper logins
* Role based permissions are utilised to ensure that data is only accessible to those with appropriate access rights.
* Enforced segregation of duties including secondary controls and restrictions are applied to privileged accounts
* All data is encrypted including backups
* Once data has reached our retention limits the disposition rules will be invoked and relevant data is disposed of securely.

\*note this is not an exhaustive list

Third Parties

Where we engage third parties to process personal data on our behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

**For how long do we keep data?**

If your application for employment is unsuccessful, we’ll hold your job application and other information supplied on file for 6 months after the end of the relevant recruitment process.

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 are detailed in our privacy policy for staff, a copy of which is available at the point of offer.

**Your rights**

As a data subject, you have a number of rights. You can:

* access and obtain a copy of your data on request;
* require us to change incorrect or incomplete data;
* require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
* object to the processing of your data where we’re relying on our legitimate interests as the legal ground for processing; and
* Ask us to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override our legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact us at peoplesupport@optivo.org.uk. You can make a subject access request by contacting us via <https://www.optivo.org.uk/about-us/transparency.aspx>

If you believe we’ve not complied with your data protection rights please contact our Data Protection Officer. If you remain unhappy with our response you can complain to the Information Commissioner at www.ico.org.uk.

**What if you do not provide personal data?**

You’re under no statutory or contractual obligation to provide data to us during the recruitment process. However, if you don’t provide the information, we may not be able to process your application properly or at all.

You’re under no obligation to provide information for equal opportunities monitoring purposes and there’s no consequences for your application if you choose not to provide such information.

**Automated decision-making**

We don’t use automated decision-making in any of our recruitment processes.