Job Candidate Privacy Policy

Introduction

The Institute of Directors (IoD) is committed to protecting the privacy and security of candidates' personal data. This policy describes how we collect and use personal data about you during and after the recruitment process in accordance with the EU General Data Protection Regulation (GDPR).

Scope

Our approach to managing your personal data is that we will:

- comply with relevant data protection legislation and all other applicable laws;
- be open and transparent about how we use your personal data;
- only collect personal data that may be required as part of the recruitment process;
- make sure you can access and exercise your other rights under data protection legislation;
- protect your personal data and keep it secure; and
- train our staff on the importance of privacy and making them aware of the correct processes to follow in relation to privacy and the handling of personal data.

This notice applies to candidates that apply for advertised job vacancies with the IoD.

Purpose

The IoD is a "data controller" in respect of the personal data it collects and holds about you as part of the recruitment process. As a data controller, we are responsible for deciding and advising you:

- what data we collect;
- how we use it;
- how we store it;
- when it will be deleted.

Types of Personal Information

Personal data means any information about a living individual from which that person can be identified. The categories of personal data we may collect and hold about you may include:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
- Personal details such as date of birth, gender and nationality;
- CV's or cover letters or any other supplementary document included as part of the application process where requested or not;
- Information about your right to work in the UK;
- Information regarding your work history, qualifications, professional memberships, education, experience, or employment references;
- Photographs if included on CVs or otherwise on supplementary document submitted as part of the recruitment process; and
- The results of any personality profiling assessment that we may carry out as part of the recruitment process.

We may also collect, store and use the following special categories of more sensitive personal data, which could include:

- Information about whether or not you have a disability for which we need to make reasonable adjustments as part of the recruitment process; and
- Information about criminal convictions and offences (where the nature of the job requires this).

More information about how we treat special categories of personal data is set out below.

Personal data collection

We may collect this information in a variety of ways. For example, data might be collected through application forms; your CV; from correspondence with you; or through interviews, meetings or other assessments.

We may collect personal data about you from third parties, such as references supplied by former employers or agencies and information from criminal records checks permitted by law.

Personal Data Storage

Your personal data will be stored in a range of different places, including in our recruitment files, in our HR system, and in other IT systems (including its email system).

Personal Data Processing

Under the GDPR, a data controller should only collect your personal data if it has a valid purpose for doing so that falls into one of the prescribed categories set out in the GDPR. The purposes for which we process your data are set out below.

The IoD requires personal data about you in order to take steps to enter into a contract with you and will retain that personal data in order to perform that contract.

The IoD has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the IoD 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.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the UK before employment starts.

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.

For some roles, we are obliged to seek information about criminal convictions and offences. Where we seek this information, we do so because it is necessary for us to carry out our obligations and

exercise specific rights in relation to employment to establish whether or not an individual has committed an unlawful act or been involved in dishonesty or other improper conduct.

Where it is necessary to collect and process any special categories of sensitive personal data, we will ensure it is handled confidentially and will limit access to the information to the individuals who require it for the purposes of which it is being requested / processed.

If you have any questions as to why we hold any type of personal data about you that is not covered in this policy, please contact the Data Protection Officer at gdpr@iod.com or a member of the HR team at hr@iod.com

Personal Data Sharing

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR Team, relevant hiring managers and interviewers involved in the recruitment process, and IT staff if access to the data is necessary for the performance of their roles.

We will only share your data with third parties for the purposes of assessing your application for employment. This will be with authorised third parties that have been engaged by the IoD such as professional advisors, external consultants, recruitment agencies etc. If you are successful in your application and we make an offer of employment, we will ask for your nominated referees and contact them in order to obtain references for you and we will use your name within that correspondence, and we may contact the Disclosure and Barring Service to undertake necessary criminal records checks (if required for the nature of the role).

Your data will not be transferred outside the European Economic Area (EEA).

Personal Data Security

We take the security of your data very seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where we engage third parties to process personal data on our behalf or we share personal data with third parties, those third parties will do so only upon written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

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

Personal Data Retention

We will not hold your personal data longer than we need it. If unsuccessful, generally we keep the majority of your information for the duration of the recruitment process plus an additional 12 months thereafter. If you are successful in your application, information collected as part of 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

You also have the following rights when it comes to our handling of your data:

- Right of access – you have the right to request a copy of the personal data we have on you and to request supporting information explaining how the personal data is used
- Right of rectification – you have the right to request that we rectify inaccurate personal data about you
- Right of erasure – you have the right to request that we erase all personal data about you (please note that we may be able to reject or restrict the request in some circumstances, depending on the information we hold and our lawful reason to keep it)
- Right to restrict processing – in some situations, you have the right to request that we do not use the personal data you have provided (e.g. if you believe it to be inaccurate)
- Right to object– you have the right to object to certain processing of your personal data (unless we have overriding compelling grounds to continue processing)
- Right to data portability – where we are relying on your consent to use your information, you have the right to require us to provide you with a copy of your information for your use or transfer to another service provider.

If you would like to exercise any of these rights, please contact the IoD's DPO at gdpr@iod.com.

If you believe that the data controller has not complied with your data protection rights, you can complain to the Information Commissioner. Contact details for the ICO can be found at https://ico.org.uk/

Automated processing

We do not generally make any recruitment decisions based solely on automated decision-making. In the event that we do ever use automated decision-making that could have a significant impact on you, we will let you know in advance and give you an opportunity to object.

If you fail to provide personal data

You are under no statutory or contractual obligation to provide data to the IoD during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all. If your application is successful, it will be a condition of any job offer that you provide evidence of your right to work in the UK and satisfactory references.
You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.