

Recruitment Candidate Privacy Notice

What is the purpose of this document?

The DPO Centre is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. This Recruitment Candidate Privacy Notice makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise (whether as an employee, worker or contractor), and how long it will usually be retained for.

When we refer to Data Protection Legislation it means the Data Protection Act 2018, GDPR (United Kingdom General Data Protection Regulation) (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation implemented in connection with the aforementioned legislation.

Where data is processed of applicants in the European Union, it also includes the EU General Data Protection Regulation (EU GDPR). This includes any replacement legislation coming into effect from time to time.

Data Protection Principles

We will comply with data protection law and principles, which means that your data will be:

- Used lawfully, fairly and in a transparent way
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- Relevant to the purposes we have told you about and limited only to those purposes
- Accurate and kept up to date
- Kept only as long as necessary for the purposes we have told you about
- Kept securely

The kind of information we hold about you

In connection with your application to work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in the application form and pre-screening questions
- The information you have provided to us in your curriculum vitae and covering letter
- Any information you provided in an email during the recruitment process
- Any information you provide us during an interview
- Test scores for those candidates who complete an assessment
- Overall candidate scores for all the personal and professional attributes of a candidate when considering them for the position they are applying for, throughout all interview stages

We may also collect, store and use sensitive information about your health, including any medical condition(s), health and sickness records provided to us during the recruitment process.

How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, the candidate
- The relevant recruitment agency, from which we collect the information you provided on your curriculum vitae as part of the application process with them
- The relevant recruitment platform; VidCruiter, LinkedIn, and Indeed, from which you have submitted an application
- Third party service reports for example, where an Occupational Health Assessment is required but only once we have discussed this with you

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require details on a certification or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

How we use particularly sensitive personal information

If you disclose sensitive personal information during the shortlisting or interview process, we will use your particularly sensitive personal information in the following ways:

- To consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during an interview or as part of the role you are applying for.

The record will be stored in a secure, access restricted, digital folder for no longer than 6 months from receipt.

Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Information about criminal convictions

For certain roles, we might request you to undertake Disclosure and Barring Service (DBS) checks or in Scotland, a Disclosure Scotland check. We use the DBS checking service certificate to help assess the suitability of applicants for positions of trust.

The DPO Centre complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificate information.

We will not keep any photocopy or other image of the certificate. However, we may keep a record of the date of issue of certificate, the name of the subject, the type of certificate requested, the position for which the certificate was requested, the unique reference number of the certificate and the details of the recruitment decision taken.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data sharing

We also use 3rd party recruitment platforms and job boards for posting of advertisements on our behalf. If applying via one of the online recruitment boards, your details will be processed by them as The Controller. You can find a copy of their privacy policy on their respective websites. If you apply directly, your details will not be uploaded to any recruitment portal. If you wish for your application to be reviewed outside the chosen platform, please notify us of this in your cover email to us.

Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

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.

Data retention

How long will you use my information for?

We will retain your personal information for a period of 12 months after we have communicated to you our decision about whether to appoint you to the role. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

Rights of access, correction, erasure and restriction

Your rights in connection with personal information

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

- **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below)
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes
- **Request the restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it
- **Request the transfer** of your personal information to another party

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our DPO in writing at dpo@dpocentre.com.

Data Protection Officer



We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO at dpo@dpocentre.com. You have the right to make a complaint at any time to relevant supervisory authority for data protection issues.

This policy was last updated on 06/10/2022

Head Office

The DPO Centre Ltd
50 Liverpool Street
London EC2M 7PR

www.dpocentre.com

Outsourced Data Protection
 +44 (0) 203 797 1289
 hello@dpocentre.com

Company Information

VAT 275 6943 57
CRN 10874595