



## **Data Protection**

### **Privacy Notice for candidates**

This notice informs you of how and why your personal data will be used, namely for the purposes of a recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation ((EU) 2016/679) (GDPR).

Channing Hammond Associates is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about you. You are seeing this privacy notice because you are applying, or considering applying, for work through us.

#### **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 other way.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and up to date.
- Kept securely and only as long as necessary for the purposes we have told you about.

#### **The kind of information we hold about you in connection with your application for work with our client, data we will collect, store, and use:**

- The information you have provided to us in your curriculum vitae and covering letter and as requested in our Recruitment Briefing Papers. This includes name, title, address, telephone number, personal email address, employment history, notice period, reference details and qualifications. We may also ask you about information on any employment restrictions and links to our client.
- Any information you provide to us during an interview with us or our client.
- The results of any assessments or tests carried out as part of the recruitment process.
- Interview and assessment reports on your assessment and testing outcomes.

**We may also collect, store and use the following “special categories” of more sensitive personal information:**

- Information about your race or ethnicity, religious beliefs, sexual orientation, gender and age profile.
- Information relating to any disability; pregnancy and marital or civil partnerships.

**How is your personal information collected? We collect personal information about candidates from the following sources:**

- You, the candidate.
- Your named referees, from whom we collect confirmation of past employment details, including job title, start and finish date. We also ask for comments on your ability to do the job that you have applied for as per the job description provided.

**How we will use information about you? We will use the personal information we collect about you to:**

- Assess your skills, qualifications, and suitability for the work or role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our recruitment processes.
- Comply with legal or regulatory requirements.

Having received your CV and supporting statement, we will then process that information to enable our client to decide whether you meet the requirements to be longlisted for the role.

How we use particularly sensitive personal information We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- We will use information about your race or national or ethnic origin, religious, beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

**Automated decision making**

We do not use automated decision making in any part of our recruitment process.

**Data sharing**

Why might you share my personal information with third parties?

We will only share your personal information with third parties, such as our client, for the purposes of processing your application. All our third-party clients are required to take appropriate security measures to protect your personal information in line with our policies. We only permit our clients to process your personal data for specified purposes and in accordance with our instructions.

## **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, and third party clients 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 6 months after we have communicated to you our client's 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 procedure and applicable laws and regulations.

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 and 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 equal opportunities monitoring or 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 the Data Protection Officer  
[enquiries@channinghammondassociates.co.uk](mailto:enquiries@channinghammondassociates.co.uk)

#### **Data Protection Officer**

We have appointed Anna Hammond; Joint Managing Director as the Data Protection Officer and she is responsible for overseeing compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Data Protection Officer. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.