1 CLINITHINK JOB APPLICANT PRIVACY NOTICE

Data controller: Martin Deleay, CFO

IT Security Officer: Phil Davies, CIO

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

Should you sign up for or make use of other parts of the Clinithink Websites then you will be subject to the Websites' Privacy Policy and the Websites' Terms of Use.

2 WHAT INFORMATION DO WE COLLECT?

The Company collects a range of information about you. 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 the Company needs to make reasonable adjustments during the recruitment process
- information about your entitlement to work in the location of the job vacancy

The Company may 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, including online tests.

The Company may also collect personal data about you from third parties, such as references supplied by former employers. The Company 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.

3 WHY DO WE PROCESS PERSONAL DATA?

The Company needs to process data to take steps at your request prior to entering into a contract with you. It may also need to process your data to enter into a contract with you.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the location of the job vacancy before employment starts.

The Company 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 Company to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The Company may also need to process data from job applicants to respond to and defend against legal claims.

The Company may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. The Company processes such information to carry out its obligations and exercise specific rights in relation to employment.

The Company will not use your data for any purpose other than the recruitment exercise for which you have applied.

4 WHO HAS ACCESS TO DATA?

Your information may 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.

The Company will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The Company will then share your data with former employers to obtain references for you.

If you are a resident in the European Economic Area (EEA) your data may be transferred internally within Clinithink between the UK and the US as part of the recruitment process. Your data may be transferred to countries outside the European Economic Area (EEA) as part of undertaking the recruitment process. Data transferred outside the UK, internally within Clinithink, is subject to the Company's Information Security Policy and following relevant third party vetting to ensure adequate controls and safeguards are in place for that third party to handle personal information. When we engage in such transfers, we will ensure our arrangements are governed by relevant legal mechanisms and safeguards, including entering into data processing agreements and where required standard contractual clauses designed to ensure that your personal information is protected, on terms approved for this by the European Commission.

If you are resident in the United States your data may be transferred internally within Clinithink between the US and the UK as part of the recruitment process. Data transferred outside the US, internally within Clinithink, is subject to the Company's Information Security Policy and following relevant third party vetting to ensure adequate controls and safeguards are in place for that third party to handle personal information.

5 HOW DO WE PROTECT DATA?

The Company 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. Where the Company engages third parties to process personal data on its 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.

6 HOW LONG DO WE KEEP DATA?

If your application for employment is unsuccessful, the Company will hold your data on file for 12 months after the end of the relevant recruitment process. At the end of that period 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

7 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 the Company to change incorrect or incomplete data
- require the Company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing
- in certain circumstances you can ask the Company to restrict processing of your data
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing
- ask the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the Company's legitimate grounds for processing data

If you would like to exercise any of these rights, please contact the HR Manager.

If you believe that the Company has not complied with your data protection rights, you can complain to the relevant regulatory body for the location of the job vacancy.

8 WHAT IF YOU DO NOT PROVIDE PERSONAL DATA?

You are under no statutory or contractual obligation to provide data to the Company during the recruitment process. However, if you do not provide the information, the Company may not be able to process your application properly or at all.

9 AUTOMATED DECISION-MAKING

Recruitment decisions are not based on automated decision-making.