HOW WE USE YOUR DATA FOR RECRUITMENT

Background

This privacy policy covers how we **Stellar Quines** collect, use, store and protect the data that is supplied to us by job applicants and agencies.

Our Commitment to Job applicants

We believe completely in equal opportunities and will treat all applicants fairly with no discrimination.

We never knowingly provide misleading information about the nature of the role. We would never charge a job seeker a fee for the purpose of finding them a role.

We are committed to managing your personal information securely and with respect in accordance with the General Data Protection requirements.

The information we collect may cover the following:

- Contact information (name address, phone number and email address)
- Information from CV or application form or covering letter (education, skills and qualifications)
- Psychometric tests (Saville Holdswoth, Pystech and approved suppliers)
- Health records (Night Worker assessment forms, Health questionnaires) where required as part of the role.
- Occupational health report (Higher level screening required for role) with Access to medical Records consent being given by the applicant
- Disclosure and Barring Record where a requirement for the role
- References from the named referees that the applicant provides and only with the applicants' consent.
- Visa and proof of the right to work in the UK documents
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Salary, annual leave, pension and benefits information.

We may also collect, store and use "special categories" of more sensitive personal data which require a higher level of protection such as Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions. Also information about criminal convictions and offences.

Purpose of collection

The purpose of collecting this information is to find suitable candidates to fulfil a specific role within our Company, and to check that you are legally entitled to legally work in the UK. We collect personal information either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from background check agencies

Where appropriate, we will collect information about criminal convictions as part of the recruitment process. We are allowed to use your personal information in this way to carry out our obligations.

How the information is held.

Most information is transmitted by email and is stored on Dropbox Business, our company server and paper based filing.

Sensitive Personnel information can only be accessed by authorised staff within our Company via our server. Our staff are trained to understand the importance of keeping personal data secure.

Our computers are encrypted and safeguarded by anti-virus software and the regular changing of security passwords. Dropbox Business is certified as being compliant with the most widely accepted security and privacy standards and regulations in the world, such as ISO 27001/2, ISO27018/17 and SOC 2 and meets

the requirements of GDPR. Our company server is password protected and can only be accessed by authorised staff within our Company

The information on candidates for specific roles will be held for 6 months in line with CIPD recommended best practice. After which paper files will be securely shredded and computer records deleted. Only if we have asked, and you have given your consent for the data to be held will this not apply.

Disclosure

We may disclose the information for the purpose of obtaining referees. Where additional information is required the information may be disclosed to the Disclosure and Barring Service, your G.P or an Occupational Health professional only after you have given your consent

You have specific rights in connection with personal information: request access to your personal information; **request correction** of the personal information that we hold about you; **request erasure** of your personal information; **object to processing** of your personal information where we are relying on a legitimate interest; **request the restriction of processing** of your personal information; **request the transfer** of your personal information to another party and the r**ight to withdraw consent.**

Complaints

Privacy complaints are taken very seriously and if you believe that we have breached your privacy you should in the first instance write to **Hannah Forsyth (Company Administrator)** who has responsibility for Data Protection within our Company stating the details of your complaint. We would ask that you provide us with as much detail as possible to allow a thorough investigation. Your complaint will be acknowledged within 24 hours and we aim to resolve any complaint within 5 working days. However, depending on the complexity of the complaint and availability of external agencies it may on occasions take longer.

Should your complaint show that we have breached our duty of care we will report the breach to the Information Commissioner's Office (ICO).

If you are not satisfied by our response you may complain to the ICO. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.