SECTION 13: DATA PROTECTION

13.1 INTRODUCTION

During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about job applicants, employees, workers, contractors, interns, and former employees and we recognise the need to treat it in an appropriate and lawful manner, in accordance with the General Data Protection Regulation ((EU) 2016/679) (GDPR). The purpose of this policy is to make you aware of how we will handle your personal data.

13.2 DATA PROTECTION PRINCIPLES

We will comply with data protection law. This states that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way;
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
3. Adequate and relevant to the purposes we have told you about and limited only to those purposes;
4. Accurate and kept up to date;
5. Kept only as long as necessary for the purposes we have told you about;
6. Kept securely.

"Personal data" means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

"Sensitive Personal data" means any special categories of personal data which specifically include generic data, and biometric data. This category of data requires a higher level of protection.

"**Criminal Records data"** means information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

"Processing" means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

13.3 FAIR AND LAWFUL PROCESSING

We will only process your personal data where you have given your consent or where the processing is necessary to comply with our legal obligations. In other cases, processing may be necessary for the protection of your vital interests, for our legitimate interests or the legitimate interests of others (including you).

"Special categories" of particularly sensitive personal information require higher levels of protection. We are required to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. To carry out our legal obligations and in line with our data protection compliance.
2. To assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information in relation to legal claims or to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

13.4 HOW WE ARE LIKELY TO USE YOUR PERSONAL DATA

We will process data about staff for legal, personnel, administrative and management purposes and to enable the Company to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits in connection with your employment.

We may process sensitive personal data relating to staff including, as appropriate:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
- the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- in order to comply with legal requirements and obligations to third parties.

13.5 PROCESSING FOR LIMITED PURPOSES

We will only process your personal data for the specific purpose or purposes notified to you or for any other purposes specifically permitted by the GDPR.

13.6 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Your personal data will only be processed to the extent that it is necessary for the specific purposes notified to you.

13.7 ACCURATE DATA

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please notify the Company if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

13.8 DATA RETENTION

We will not keep your personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

13.9 PROCESSING IN LINE WITH YOUR RIGHTS

You have the right to:

- Request access to any personal data we hold about you.
- Prevent the processing of your data for direct-marketing purposes.
- Ask to have inaccurate data held about you amended.
- Prevent processing that is likely to cause unwarranted substantial damage or distress to you or anyone else.
- Object to any decision that significantly affects you being taken solely by a computer or other automated process.

•

13.10 DATA SECURITY

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if they agree to comply with those procedures and policies, or if they put in place adequate measures.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

13.11 INDIVIDUAL RESPONSIBILITIES

You may have access to the personal data of other individuals, including our clients, in the course of your [employment, contract, volunteer period, internship or apprenticeship]. Where this is the case, we rely on you to help meet our data protection obligations by complying with all policies and processes.

13.12 TRAINING

In order to ensure that data protection is understood and complied with, awareness training will be provided to all individuals as part of the induction process and at regular intervals thereafter.

13.13 PROVIDING INFORMATION TO THIRD PARTIES

We will not disclose your personal data to a third party without your consent unless we are satisfied that they are legally entitled to the data. Where we do disclose your personal data to a third party, we will have regard to the eight data protection principles.

13.14 SUBJECT ACCESS REQUESTS

Individuals have the right to make a data subject access request (DSAR) and obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information

The Company will comply with DSAR free of charge. Where necessary, the Company may request specific criteria or parameters for what data is being requested to ensure that search is not unfounded, excessive or repetitive. In instances where a request becomes excessive or further copies are requested the Company have the right to charge a reasonable administrative fee.

The Company are obligated to provide the information requested within one of month of receipt of the request. Where the request is complex or numerous, the Company can extend this by a further two months by notifying you within one month of receipt of the request.

13.15 RETENTION & DELETION

In the course of carrying out business, creates and holds a wide range of personal data records (data records). There is no requirement to retain data records permanently and data will only be collected, processed and stored where it is relevant and necessary to do so.

Retention periods have been established following assessment of our records to set out the length of time that our data records will be retained and the processes for disposing of records at the end of the retention period.

Assessment was undertaken to:

- Determine their value as a course of information about the Company, its operations, employee and client relationships and the environment within which we work;
- Assess their importance as evidence of business activities and decisions;
- Establish whether there are any legal or regulatory retention requirements

Records will be destroyed in a timely and controlled manner which reduces, so far as is possible, the risk of an unauthorised third party using the data to any individual's detriment and in accordance with the retention periods established.

Every individual is responsible for undertaking any training and/or awareness sessions in relation to data protection and to ensuring the security and disposal of records obtained and processed by them within their role. Each individual must ensure they familiarise themselves with relevant Company policies and act in accordance with them.

13.16 DATA BREACHES

A personal data breach is defined as a security incident that has affected the confidentiality, integrity or availability of personal data. There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If you consider that this policy has not been followed in respect of personal data about yourself or others you should raise the matter with your manager immediately.

It will be necessary for the Company to report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

Registered Address: 6th Floor, 60 Gracechurch Street, London EC3V 0HR
Company number: Registered in England and Wales, number 07434350