# Data Protection Policy - HR Data

## Introduction

The Company is committed to complying with Data Protection legislation and the associated Data Protection principles. As a consequence the Company seeks to operate in a transparent manner in relation to what data it collects, how it uses and processes the personal data of its workforce, and the reasons for such processing.

This policy sets out the Company's commitment to data protection, as well as individual rights and obligations in respect to personal data.

This policy applies to the personal data of candidates for jobs, employees, any other individuals engaged in any other form of work by the Company, and ex-employees. It is a policy in relation to employment-related data only.

The person with responsibility for compliance with data protection legislation within the Company is Mark Robinson. They can be contacted at mark@creative62.com or on 0116 2752831.

If you have any queries about this policy, require further information, wish to make a subject access request or exercise your rights, then such enquiries or contact should be sent to the above individual who is the identified Company contact for such matters.

## Definitions

Criminal records data: means information about an individual's criminal convictions and offences.

Personal data: means any information relating to an individual who can be identified from the information in question.

Processing: means any use that is made of information such as collection, recording, organisation, storage, amendment, disclosure, retrieval, erasure or destruction.

Special categories of personal data: means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data, health, sex life or sexual orientation.

## Data Protection Principles

The Company processes personal data in accordance with the following data protection principles. Personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, up to date;
- kept only for the period necessary for which it is processed; and
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, and accidental loss, destruction or damage.

## Data Management Procedures

The Company maintains a record of its processing activities in a register of the employment-related data it processes.

The Company uses privacy notices to advise individuals of the personal data it processes, the reason for processing it, to whom personal data is disclosed, the legal basis for processing the data, the time period for storage, the individual's rights in respect to the data, and the source of the data.

The Company will update personal data promptly where an individual advises that information relating to them has changed or is inaccurate.

Personal data collected or received by the Company will be held in the individual's personnel file and/or on any electronic system, email system and or HR/payroll system we operate. The duration for which such personal data is held is as set out in the privacy notices issued to individuals.

The Company, in considering the data it processes or might process, will only process data which can be lawfully processed. The Company relies upon the following lawful grounds for processing work-related personal data: processing is necessary for the performance of the employment contract or work contract, or in order to enter into such a contract, or the processing is necessary for compliance with a legal obligation (such as complying with equal opportunities legislation), or it is necessary for the purposes of a legitimate business interest. These matters are set out in the privacy notice issued to all individuals.

All data, including special category data, will only be processed for legitimate purposes, and will be handled confidentially. Access to such data is strictly controlled and only authorised individuals have access to such data.

In addition, data security procedures are followed as set out below in the Data Security section.

All data will be retained during the course of employment (or for the duration of any other type of engagement). Following the termination of the

contract, the data will be retained for a period of up to 6 years following the start of the next tax year, in part due to the need to retain records for certain legal reasons. In respect to applicants for jobs who are unsuccessful their details will be retained for up to 6 months. Other procedural steps relating to data management are set out in this policy.

## Special Category Data

In the event the Company processes special categories of personal data or criminal records data to perform obligations or to exercise rights under employment legislation, this is performed in accordance with this policy, including the procedures it sets out, and in accordance with this section.

The Company only collects data for relevant work-related matters and does not seek to specifically gather or receive special category information unless it is relevant. Such special category data will only be collected for specific legitimate workplace matters and will not be processed in any way incompatible with that purpose.

This essentially means that such information will only be collected, processed and or retained where it is necessary to do so for the purposes of carrying out the obligations and exercising specific rights of the Company or of the individual in question in connection with the field of employment. So for example such processing may be required to comply with the Equality Act 2010, or other pieces of employment legislation or in respect of the law relating to statutory sick pay.

## Individual Rights

You have certain rights in respect to your personal data. These are set out below.

### Subject Access Requests

You have the right to make a subject access request. This may include the following information from the Company:

- confirmation of whether or not your data is processed;
- the purpose of processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed;
- the envisaged period the personal data will be stored or the criteria for determining that period;
- your right to request rectification, erasure, restriction of processing or to object to processing of personal data (see below);
- your right to complain to the Information Commissioner;
- the source of the data where it is not collected from you;

- the existence of any automated decision-making, and meaningful information about the logic involved in any such decision-making; and
- where personal data is transferred to a third country or an international organisation, the appropriate safeguards that apply.

Should you make such a request, the Company would provide you with a copy of the personal data held. If you require further copies, the Company will charge a reasonable fee, which will be based on the administrative cost of providing the further copies.

If you wish to make a subject access request, you should send the request to the Company contact identified above in the Introduction. In some circumstances proof of identification may be needed before the request can be processed. The Company will advise you if your identity needs to be verified and what verification documents are required (this would normally only apply to former staff members, or job applicants).

The Company will respond to a request within one month from the date the request is received. That period can be extended by a further two months where necessary, taking into account the complexity and number of requests. In such circumstances the Company will write to you within one month of receipt of the request advising of the extension and reasons for it.

Where a request is manifestly unfounded or excessive, the Company may charge a reasonable fee, taking into account the administrative cost of responding to the request or refuse to act on the request. A subject access request can be manifestly unfounded or excessive where it is repetitive. In the event you make a request that is manifestly unfounded or excessive, then the Company will advise you accordingly, and will confirm whether or not it will respond to the request.

**Requests for rectification, erasure, restriction of processing, and objections to processing of personal data**

If you wish to request any of the above actions of the Company you should send the request to the Company contact identified above in the Introduction. You should provide as much information as possible in support of your request.

## Data Security

The Company takes the matter of security for HR-related personal data seriously. The Company takes appropriate measures to protect personal data from loss, accidental destruction, improper disclosure or misuse, and to ensure against data breaches or unauthorised access to data. Only authorised individuals in the proper performance of their job roles can access such data.

Where the Company makes use of third parties to process personal data on its behalf, they do so on the grounds of written instruction and authorisation from the Company. In addition they are under a duty of confidentiality and are required to adopt appropriate technical and organisational measures to protect and ensure data security.

## Impact Assessments

In the event processing would be likely to result in a high risk to the rights and freedoms of an individual, the Company will conduct an impact assessment. The assessment will: describe the envisaged processing operations; the purpose of the processing; the necessity and proportionality of the processing operations; assess the risks to the rights and freedoms of individuals; and measures and safeguards to address such risks.

## Data Breaches

In the case of a data breach that poses a risk to the rights and freedoms of individuals, the Company will report it to the Information Commissioner within 72 hours of having become aware of the breach.

All data breaches will be documented. This will include the facts relating to the data breach, its effects and remedial action.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will communicate to the data subjects that there has been a breach. In addition the Company will provide them with appropriate information about the nature of the breach, the appropriate contact in the Company if they require more information, the likely consequences of the breach and the mitigation steps taken to address any adverse effects.

## International data transfers

It may be that your personal data will be transferred outside the European Economic Area (EEA) through the use of cloud storage or similar technology. In such circumstances data will only be transferred to organisations which are covered by an adequacy decision by the EU Commission.

## Individual Responsibilities

You should assist the Company to keep your personal data accurate and up to date.

You should advise the Company as soon as possible if any information you have provided to the Company changes, such as personal details, a change of address or a change in bank details.

Where you have access to personal data relating to others, then you must recognise and comply with your responsibilities under Data Protection legislation.

If you have access to personal data you must:

- only access personal data you have been given authority to access;
- only access personal data for authorised purposes;
- not disclose personal data to others unless they are authorised individuals;
- ensure data is kept secure and retained where it cannot be accessed by unauthorised personnel;
- ensure personal data, or devices containing or that can be used to access personal data, are not removed from the Company's premises without appropriate security measures being used to secure the data and the device (e.g. encryption or password protection);
- only store personal data on authorised devices; and
- comply with the Data Protection Principles (set out above).

You should understand that a breach of this policy may be treated as a disciplinary offence and in cases of a severe breach may be treated as gross misconduct.