Data Protection Policy

Introduction

The Company is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the Company's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR-related personal data. [This policy does not apply to the personal data of clients or other personal data processed for business purposes.]

The Company has appointed Andrew Papadopoulos as its data protection officer. Their role is to inform and advise the Company on its data protection obligations. They can be contacted at andrew.papadopoulos@focuscloud.org. Questions about this policy, or requests for further information, should be directed to the data protection officer.

Definitions

"Personal data" is any information that relates to a living individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

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

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

Data protection principles

The Company processes HR-related personal data in accordance with the following data protection principles:

- The Company processes personal data lawfully, fairly and in a transparent manner.
- The Company collects personal data only for specified, explicit and legitimate purposes.
- The Company processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The Company keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The Company keeps personal data only for the period necessary for processing.
- The Company adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Company tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. If the Company wants to start processing HR-

related data for other reasons, individuals will be informed of this before any processing begins.

HR-related data will not be shared with third parties, except as set out in privacy notices. Where the Company relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the Company processes special categories of personal data or criminal records data to perform obligations, to exercise rights in employment law, or for reasons of substantial public interest, this is done in accordance with a policy on processing special categories of data and criminal records data.

The Company will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

Personal data gathered during the [employment, worker, contractor or volunteer relationship, or apprenticeship or internship] is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Company holds HR-related personal data are contained in its privacy notices to individuals.

The Company keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the UK GDPR.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell them:

- whether their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the UK and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the Company has failed to comply with their data protection rights; and
- whether the Company carries out automated decision-making and the logic involved in any such decision-making.

The Company will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual wants additional copies, the Company will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

To make a subject access request, the individual should use the Company's form for making a subject access request (Appendix 1). In some cases, the Company may need to ask for

proof of identification before the request can be processed. The Company will inform the individual if it needs to verify their identity and the documents it requires.

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the request is complex, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded if it is made with the intention of harassing the Company or causing disruption, or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, the Company will notify them that this is the case and whether it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the Company's legitimate grounds for processing data (where the Company relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether the individual's interests override the Company's legitimate grounds for processing data.

To ask the Company to take any of these steps, the individual should send the request to andrew.papadopoulos@focuscloud.org.

Data security

The Company takes the security of HR-related personal data seriously. The Company has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

Impact assessments

Some of the processing that the Company carries out may result in risks to privacy. Where processing would result in a high risk to individual rights and freedoms, the Company will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.]

Data breaches

If the Company discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers

The Company will not transfer HR-related personal data to countries outside the UK.

Individual responsibilities

Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let the Company know if data provided to the Company changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals [and of our customers and clients] in the course of their [employment, contract, volunteer period, internship or apprenticeship]. Where this is the case, the Company relies on individuals to help meet its data protection obligations to staff [and to customers and clients].

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Company) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Company's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to [name of individual/the data protection officer] immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Company's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Training

The Company will provide training to all individuals about their data protection responsibilities as part of the onboarding process [and at regular intervals thereafter].

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Appendix 1

Subject access request	
Name:	
Daytime telephone number:	
Email:	
Address:	
Employee number:	
By completing this form, you are making a request under the UK General Data Protection Regulation (UK GDPR) for information held about you by the organisation that you are eligible to receive.	
Required information (and any relevant dates): [Example: Emails between "A" and "B" from [date] to [date].]	
By signing below, you indicate that you are the individual named above. The organisation cannot accept requests regarding your personal data from anyone else, including family members, unless evidence is provided of authority to act on your behalf. We may need to contact you for further identifying information before responding to your request. You warrant that you are the individual named and will fully indemnify us for all losses, cost and expenses if you are not. Please return this form to a member of the People team. Please allow 30 days for a reply.	
Data subject's signature:	
Date:	