Participation People

Playful in practice
Serious about solutions

Data Protection Policy

Introduction

Purpose

The Company collects and processes personal data relating to our current, past and prospective workforce to manage the employment relationship both during employment and after it ends. We recognise the need to treat that information in an appropriate and lawful manner. We are committed to protecting the privacy and security of employees' personal data. This policy sets out the Company's commitment to complying with our data protection obligations, individuals' rights and obligations in relation to the processing of personal data whilst working for or on behalf of the Company, and the basis on which we will process any personal data we collect or that is provided to us.

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.

This policy does not form part of any employee's contract of employment and may be amended at any time. It applies to all staff, including prospective, current and former staff members of the Company. Any breach of this policy will be taken seriously and may result in disciplinary action.

The Company has appointed as its data protection officer Temi Oluwadare and James Rimmer, Programme Managers. Their role is to inform and advise the Company on its data protection obligations and to oversee compliance with the Company's data protection policies, procedures and obligations. They can be contacted at dataprotection@participationpeople.com.

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 an individual who can be identified from that data (or from that data and other information in our possession).

"**Processing**" is any activity that involves use of personal data whether or not by automated means, 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, physical or mental health, sexual orientation, genetic data 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

When processing personal data, the Company will comply 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 and will not further process that data in a manner incompatible with those purposes
- Personal data processed by the Company will be adequate, relevant and limited to what is necessary for the purposes for which it is processed
- The company keeps accurate personal data that, where necessary, is kept up to date and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay
- The company ensures personal data is not kept in a form which permits identification of the individual for any longer than is necessary for the purposes for which it is processed
- The company ensures personal data is processed in a manner that ensures appropriate data security. It adopts appropriate measures to make sure that personal data is protected against unauthorised or unlawful processing and accidental loss, destruction or damage

The Company tells individuals about their rights, how it complies with its data protection obligations, how it collects and uses personal data, the reasons for processing personal data and the legal basis for processing in its privacy notices.

The Company will only use personal information for the purposes for which it was collected unless it reasonably considers that it needs to use it for another reason and that reason is compatible with the original purpose. If the Company needs to use personal information for an unrelated purpose, it will notify the relevant individuals and explain the legal basis which allows it to do so.

Where the Company processes special categories of personal data or criminal records data this is done in accordance with its separate policy on processing this type of data and ensures appropriate additional safeguards are in place in compliance with the Company's data protection obligations.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in an employee's personal file (in hard copy or electronic format, or both), in the Company's HR management systems and in other IT systems (including the Company's email system). 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 General Data Protection Regulation (UK GDPR) and is registered with the Information Commissioner's Office.

Individual Rights

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

- Access and obtain a copy of the personal data we hold about them on request (also known as a subject access request)
- Require the Company to correct inaccurate or incomplete personal data
- Require the Company to delete or stop processing their personal data where there is no good reason for the Company continuing to process it or where they have exercised their right to object to processing (see below).
- Object to the processing of their personal data where the Company is relying on its legitimate interests (or those of a third party) as the legal ground for processing.
- Request the restriction of processing of their personal data. This enables them to ask the Company to suspend the processing of their personal data, for example, if they want the Company to establish its accuracy or the reason for processing it.

To ask the Company to take any of these steps, the individual should send the request to dataprotection@participationpeople.com.

In some cases, the Company may need to ask for proof of identification and/or require the individual to specify the information or processing activities to which the request relates before a request can be processed. The Company will inform the individual if it needs to verify their identity and the required documents.

The Company will normally respond to a request within a period of one month from the date it is received. However, in some cases, such as where the Company processes large amounts of the individual's personal data, 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 the Company receives a subject access request it will provide the individual with a copy of the personal data requested. 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 may charge a reasonable fee.

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. An individual will not normally have to pay a fee to access their personal information or to exercise any of the other rights listed above. However the Company may charge a reasonable fee if a subject access request is clearly unfounded or excessive. A subject access request is likely to be manifestly unfounded 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 or not it will respond to it.

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

If an individual believes that the Company has not complied with their data protection rights, they have the right to complain at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Data Security

The Company takes the security of HR-related personal data seriously.

The Company has internal policies and controls to prevent personal data from being lost, accidentally destroyed, misused or disclosed and to ensure that it is not accessed except by the Company's employees and other staff when necessary to properly perform their duties.

All data will be held securely in locked cupboards in the appropriate office, which will only be accessed by the CEO, Programme Manager Universal and Programme Manager Specialist and Targeted. Details will be stored on the Company's encrypted Google Drive, which those aforementioned can only access, hosted on European servers, encrypted to 256-bit.

Where the Company engages third parties to process personal data on its behalf, such parties do so based on written instructions. They are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure data security. The Company will ensure the third party provides adequate guarantees in terms of expert knowledge, reliability and resources to implement appropriate technical and organisational measures to ensure personal data is processed in accordance with both companies' data protection obligations. It will have in place a contract or other legal arrangement with the third party setting out the type of personal data that will be processed, the duration of the processing, the nature and purposes of the processing, the categories of data subjects, the obligations and rights of the Company, the specific tasks and responsibilities of the third party and the requirements around returning or deleting the personal data after completion of the contract.

Impact Assessments

Some of the processing that the Company carries out may result in risks to privacy. When appropriate, including where processing is likely to result in a high risk to an individual's 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 nature and severity of the risks for individuals and the measures that can be put in place to mitigate those risks. Where the impact assessment indicates the processing involves a high risk that cannot be mitigated by appropriate measures in terms of available technology and costs of implementation we shall consult the supervisory authority prior to the processing.

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's Office without undue delay and, where feasible, within 72 hours of discovery. The Company will record all data breaches regardless of their effect.

Where appropriate and if the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals without undue delay 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 European Economic Area.

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 their bank details.

Individuals may have access to the personal data of other individuals and of our young people, suppliers 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 its young people, suppliers and clients.

Individuals who have access to personal data are required:

- to access only personal data that they have authority to access and only for authorised purposes
- not to disclose personal data except to individuals (whether inside or outside the Company) who have appropriate authorisation strictly on a need to know basis
- to keep data secure and to comply with all rules, policies and guidance provided by the Company relating to data security and data protection including 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
- to notify, immediately in the event they become aware of or suspect there has been a personal data breach
- to notify, immediately in the event they receive any request from an individual exercising their rights set out above

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

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.