Data Protection Policy

This policy applies to the processing of personal data in manual and electronic records kept by the Company in connection with its human resources function as described below. It also covers the Company's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Company makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies.

Where third parties process data on behalf of the Company, the Company will ensure that the third party takes such measures in order to maintain the Company's commitment to protecting data. In line with current data protection legislation, the Company understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Data Protection Policy

Types of data held

Personal data is kept in personnel files or within the Company's HR systems. The following types of data may be held by the Company, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades
- conduct issues such as letters of concern, disciplinary proceedings
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details

Relevant individuals should refer to the Company's Privacy Notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Health Records

The Company holds health records on all employees and these are used to assess the health, wellbeing and welfare of the workforce and to highlight any issues which may require further investigation. Records can include details of sickness absence, medical conditions, disabilities, and prescribed medication. Data under this heading will only be used by appropriate management and will not be revealed to other employees unless those employees are responsible for health records in the normal course of their duties.

Employees have the right to request that the Company does not keep health records on them. All such requests must be made in writing and addressed to the Data Protection Coordinator.

The Data Protection Principles

All personal data obtained and held by the Company will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing

- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant data protection procedures for international transferring of personal data.

The Rights of Data Subjects

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data

Procedures

The Company has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it appoints or employs employees with specific responsibilities for the processing and controlling of data, and the reviewing and auditing of its data protection systems and procedures
- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects data. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially
- it can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the Company

- it recognises the importance of seeking individuals' consent, where applicable, for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The Company understands that consent must be freely given, specific, informed and unambiguous. The Company will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time
- it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences
- it is aware of the implications international transfer of personal data internationally
- when any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it will be securely deleted and disposed of

Subject Access Requests (SAR)

Relevant individuals have a right to be informed whether the Company processes personal data relating to them and to access the data that the Company holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from [insert name]. The request should be made to [insert details]
- the Company will not charge for the supply of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- the Company will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where the SAR is complex and/or numerous requests are made. If such additional time is required, the relevant induvial making the request shall be informed.

Relevant individuals must inform the Company immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. The Company will take immediate steps to rectify the information.

Data disclosures

The Company may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties

- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security

The Company adopts procedures designed to maintain the security of data when it is stored and transported. In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- refrain from sending emails containing sensitive work-related information to their personal email address
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by a senior manager or Director. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow the Company's rules on data security may be dealt with via the Company's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers

The Company does not normally transfer personal data to any recipients outside of the EEA.

If the Company is required to transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA this will only take place if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority
- The transfer is made with the informed consent of the relevant individual
- The transfer is necessary for the performance of a contract between the relevant individual and the Company (or for pre-contractual steps taken at the request of the relevant individual)
- The transfer is necessary for the conduct of legal claims
- The transfer is necessary to protect the vital interests of the relevant individual or other individuals where the relevant individual is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who can show a legitimate interest in accessing the register

Data Breach Notification

All personal data breaches must be reported immediately to a Company Director.

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of employee data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Company must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

Data Protection Policy

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of employee data subjects, the Company must ensure that all affected employee data subjects are informed of the breach directly and without undue delay.

Data breach notifications shall include the following information:

- The categories and approximate number of employee data subjects concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the Company contact point where more information can be obtained
- The likely consequences of the breach
- Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects

Data protection Co-ordinator

To ensure the implementation of this policy the Company has designated the Office Manager as Data Protection Coordinator. All enquiries relating to the holding of personal data should be referred to them in the first instance.

Consequences of breach of this policy

Any breach of this Policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

Dated: 4th February 2024

Christopher Knollys

Managing Director
Cableduct Limited