# Data Protection Policy

This policy applies to all companies within the Relyon Group.

For the purposes of the administration and the management of the business the Company needs to retain and process certain personal and sensitive personal data about its employees and clients.

To comply with the law, information (as defined by the Data Protection Act) must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, The Company must comply with the Data Protection principles which are set out in the Data Protection Act 1998.

The act applies to all types of personal information, which is stored on computers or held in written copy. It sets out eight Data protection principles, which every individual handling such personal data must comply with.

## Principles of the Data Protection Act

The Data Protection principles in summary are:-

- The information to be contained in personal data shall be obtained and processed fairly and lawfully
- Personal Data shall be held for one or more specified and lawful purposes and data held for any purpose(s) shall not be used or disclosed in any manner incompatible with those purposes
- Personal data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose
- Personal Data shall be accurate and where necessary, kept up to date
- Personal data held for any purpose shall not be kept longer than is necessary for that purpose
- Personal data shall be processed in accordance with the data subject's rights
- Personal data shall be kept safe from unauthorised access, accidental loss or destruction
- Personal data shall not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The Company and all staff who process or have access to personal information must ensure that the data protection principles under the Act are followed and fully implemented.

The Company will ensure that all appropriate security measures shall be taken against unauthorised access to, alteration, disclosure or destruction of personal data.

## Employee Data

The Company aims to only process and retain information which is relevant to the employment relationship (potential, current or past).

Personal data processed and retained by the Company may relate to,

- Recruitment, promotion and career development
- Pay and remuneration including payroll, tax, national insurance and other deductions from pay
- Pension and other benefits
- Appraisals and performance reviews
- Disciplinary and Grievance procedures followed

(this is not an exhaustive list)

Sensitive personal data processed and retained by the Company may relate to;

- Sickness (pay and leave)
- Absence
- Equal opportunities monitoring
- Any obligation arising under the Disability Discrimination Act
- Maternity, Paternity. Adoption, Parental leave entitlements
- Pension
- Capability

(this is not an exhaustive list)

Further the Company may process and retain personal data or sensitive personal data where is required to do so under any statute.

## Accessing Employee Data

The Company upon request will confirm what personal data they hold in relation to an employee.

Subject to any statutory exemptions all Employees shall be entitled to request access any personal data or sensitive personal data the Company have retained in relation to the requesting individual only. Such a request is known as a "subject access request".

Any employee shall also be able to request the Company amend or correct inaccurate information retained.

An employee wishing to make such a request must provide details in writing to their line manager outlining the disclosure sought and over what period of time.

Any request will be subject to administration fee. The fee will be reasonable given the nature of the request but normally not exceed £10 per request.

The Company will process any request without unreasonable delay and in any event within 40 days of the Company having receipt of the written request, the administration charge and any additional information which the Company reasonably requires in order to locate the information. No obligation upon the Company to provide the information arises until these conditions have been fulfilled.

Where the requesting employee has failed to provide sufficient information to readily identify the data sought the Company may write back requesting further details.

The information will be supplied by way of a copy, except where the supply of a copy in permanent form is not possible or would involve disproportionate effort, or the Employee agrees otherwise.

Any information not related to the individual will be redacted prior to the documentation being sent to the employee to review.

The Company shall provide access to the information unless doing so would infringe upon the rights of any third party or any legal exemption applies.

## Retention of Data

The Company will hold the minimum personal data and sensitive personal data necessary to enable it to perform its functions.

The Company may retain records relating to an individual's employment with the Company for a period of up to seven years from the date of termination of employment where necessary.

The Company will keep some items of information for longer than others. The retention period will never be for longer than is necessary and in line with current good practice and statutory requirements.

Records retained will be kept in a secure location. The erasure or destruction of information which is out of date will be conducted in such a way as to preserve the confidentiality of the information.

The purpose for which the Company holds any information about Employees after the end of employment is for use solely in relation to residual employment related matters including, but not limited to;

- the provision of job references,
- processing applications for re-employment,
- matters relating to retirement benefits
- the fulfilment of contractual or statutory obligations.

## Employees Duties

In connection with their own personal data all employees have a duty to;

- check that any information that they provide to the Company in connection with their employment is accurate and up to date;
- inform the Company of any changes or errors in information which they have provided e.g. change of address (the Company cannot be held accountable for errors arising from changes about which it has not been informed).

In connection with other staff members, clients and anyone who's personal information may be provided to the Company, all Employee are responsible for ensuring;

- any personal data which they hold is kept securely;
- any personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised Employee, client or other third party.

Where disclosure to a third party is a necessity Employees should ensure that the appropriate consent is in place before any information is released.

All personal data should be accessible only by those who need to use it and should be kept;

- in a secure environment
- be password protected if computerised
- Only kept on any portable storage device where absolutely necessary and if that device itself is kept in a secure environment.

## Disciplinary

The Company expects that all its Employees will comply fully with this Policy and the Principles of the Data Protection legislation.

Disciplinary action may be taken against any employee who breaches any of the instructions or procedures in this policy.

The Company is committed to the highest standards of confidentiality in relation to all its Employees and clients. As such any breaches of this procedure will be regarded as a serious matter and could lead to dismissal.