DATA PROTECTION POLICY

Table of Contents

Background and Overview

The Data Protection Act 1998 (the “Act”) which came into force on 1st March 2000 both replaces and extends the provisions of the Data Protection Act 1984. The Act requires individuals who are responsible for personal data to comply with certain key principles, more specifically relating to data that is held. The Act regulates the processing of information relating to individuals and applies throughout the “lifetime” of the data.

The Act increases the scope of the right of individuals to gain access to data that is held, and which relates directly to them. This covers certain non-automated or “manual” data including data stored on a computerised system and includes archived copies. The Act applies new conditions as to how such manual and automated data can be processed and broadens the definition on what constitutes “sensitive personal data”.

As a result, the Company has an obligation to ensure that it adopts an approach to data protection that is clear, concise and which can easily be implemented, and which recognises the importance of processing data. The definition of "processing" is very wide ranging, and covers virtually all conceivable activities in connection with data including, obtaining, recording, amending, retrieving, disclosing, storing or destroying the data, whether this is undertaken by or on behalf of the Company. Whenever the words "process" or "processing" (or other variation on those words) are used in this policy, they should be interpreted in this way.

The Act clearly defines eight data protection principles which must be complied with when processing any type of personal data.

Providing Personal Data

Personal data can be provided from a variety of sources, including, among others: employees, other personnel, suppliers and from other people with whom the Company may communicate. The Company needs to be able to process personal data concerning its employees in order to be able to manage and operate its business effectively.

The Company will endeavour to ensure that employees understand why personal data is needed, why it is being processed by the Company and to whom it may be disclosed. Employees may have access to their personal data subject to the provisions contained within this policy document.

The processing of personal data may only be for legitimate reasons; for example, statutory information and for operational management and administrative purposes. The Company may only hold personal data which is related either directly or indirectly to the employees’ employment with the Company.

The Company holds data on its employees to form a “Personnel File”. This data may be held in files in either the Human Resources or Payroll/Finance Departments of the Company as appropriate and may be held either electronically on the Human Resources/Payroll systems, or, manually. Manual records generally comprise paper-based records which are held in the Human Resources and/or Payroll/Finance department.

Description of Personal Data

Electronic or manual records held by the Company on its employees may, for example, include the following types of data (this list is not exhaustive, and we will therefore notify you where we are holding any different types of data):

- Name, address, telephone number(s)
- Other contact details
- Employment application/C.V.
- Career History
- Interview notes
- References
- Offer of employment

- References from past employers or personal references
- Job description
- Statement of statutory particulars/Contracts of Employment/Service Agreement
- Medical information/reports and sickness records
- Company benefits
- Trade union, staff association membership
- Disciplinary/grievance records
- Court, tribunal or inquiry proceedings
- Training and development/appraisal records
- Attendance records
- Immigration status and/or racial origin
- Asylum & Immigration records
- Copy of driving licence
- Correspondence between employee and employer pertaining to any of the above/changes relating to any of the above
- Details of any accidents than an employee may have had at work
- Emergency contact information
- Holiday records
- Exit interview forms
- P11d/P45/P60
- Date of commencement of employment
- Bank/building society details
- Salary
- Notice of Tax Coding
- National Insurance Number
- Pension information
- Data required for government departments (e.g. attachments of earnings etc.)
- Motoring and other relevant convictions
- Marriage and partnership details
- Membership of professional bodies

Sensitive Personal Data

What is Sensitive Personal Data?

Some of the data detailed under Description of Personal Data is defined as “sensitive personal data” (as defined under the Act) and may consist of any of the following:

- The racial or ethnic origin of an employee
- An employee’s political opinions
- An employee’s religious beliefs or similar beliefs
- Membership of a Trade Union
- Physical and/or mental health or condition
- Details of an employee’s sex life
- The commission or alleged commission of an offence or, any proceedings for any offence or, any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of a court in relation to such proceedings

Processing

The Act prohibits the processing of sensitive data as defined above without the employee's explicit consent, except in certain permissible circumstances, for example, ethnic monitoring. The Company policy in this regard is that it will obtain the explicit and informed consent of the employee for the processing of sensitive personal data that may include any of the above, save where it is not necessary to do so in accordance with the Act.

"Processing" includes obtaining, keeping, using, accessing, disclosing and destroying of data.

Use of Personal Data

There are a number of legitimate reasons why the Company processes an employee's personal data. This could be for one of a number of purposes, of which the following are examples:

- The administration and payment of an employee's salary, pension and other appropriate benefits
- Performance appraisal or training
- Career planning and personal development
- Communicating with employees
- Maintaining statutory records
- Compliance with legislation in relation to health and safety/other employment related matters and compliance with other Company policies
- The processing of personal data in respect of membership of a pension scheme, for example, processing of contributions, storing and maintaining contact details, making the payment of benefits under the scheme etc.

There may also be other circumstances in which your personal data may be disclosed to a third party, for example, to benefits providers, Company medical and/or legal advisors. This would take place normally having obtained in the first instance consent by the employee. However, there may be circumstances where this may not always be appropriate. For example: in the event of a dispute between the employee and the Company. In such a situation the Company reserves the right to disclose all relevant personal details concerning the employee to its legal advisors for the purpose of protecting the Company's position.

The Eight Data Protection Principles

The Company is required to comply with the following Eight Data Protection Principles with regard to any personal data that is processed.

All personal data must:

- Be fairly and lawfully processed
- Be obtained only for one or more specified and lawful purpose(s), and not further processed in any manner incompatible with such purpose(s)
- Be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed
- Be accurate and, where necessary, kept up to date
- Be kept no longer than necessary for the purpose(s)
- Be processed in accordance with the individual's rights
- Be subject to appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection

Format of Records

Where possible and practical, all records (whether electronic or manual) will be kept in a standard format in chronological order within sub-sections.

Access to Data

Certain employees of the Company will be authorised to establish, access, maintain and destroy records. All files are kept in a secure location and only authorised employees of the Company will have access to appropriate personal data held on employees.

Personnel Records may only be established, accessed and/or maintained by:

- Managing Director
- The Human Resources Director
- Any HR Assistants

Unless particular circumstances dictate otherwise, Payroll records may only be established, and/or maintained by:

- Managing Director
- The Human Resources Director
- The Finance Director
- Financial Controller

Line Managers/the Head of I.T., or where appropriate, personnel authorised by any of the above, may be authorised to access, but not without the express consent of the employee concerned, make any changes to individual personal employment record(s) either in full or in part. E.g Line managers may need to view performance appraisals, training records and/or CVs.

Unless particular circumstances dictate otherwise, Client records may only be established, accessed and/or maintained by:

- Manager Director
- Employees dedicated to working on specific accounts
- (this includes but is not limited to: Business Unit Director / Account Director(s) / Operations Controller / Data Analysists / Account administrators)

- Line Managers/the Head of I.T., or where appropriate, personnel authorised by any of the above, may be authorised to access, but not without the express consent of the Business Unit Director / Account Director specifically allocated to a client, make any changes to client record(s) either in full or in part. E.g. for improvements and development to internal business process and compliance.

Requests for any changes or additions to access files or folders must be authorised (in writing) by one of the following people prior to access being granted:

- Managing Director
- Finance Director
- The Human Resources Director
- Business Unit Director

Employee Rights

Employees/other individuals in respect of whom the Company processes personal data have certain rights. These include:

The right of access – the employee is entitled to request access to their personal data; however, in certain circumstances, not all of the personal data has to be disclosed where an exemption contained in the Act applies.

The right of accuracy and/or legitimacy of personal data. Where an employee believes a record to be inaccurate they are entitled to bring this to the attention of the Company and request that the record be amended. If, following investigation, this challenge is upheld, the employee is entitled to have the record removed or corrected and to receive confirmation. An employee may also challenge why the Company holds certain data.

Retention/Disposal of Employee Records

Employee records covered as part of this policy will be retained for the following specified periods after the employee has left the Company's employment following which they will be destroyed.

Personnel records – 6 years
Payroll records (inc. SMP & SSP) – in accordance with Inland Revenue requirements
Pension records – in accordance with the rules of the scheme
Health & Safety - Permanently
Accident records – 12 years
Unpaid Leave records – 3 years

Should you require further information regarding the Data Protection Policy, please contact the Head of Human Resources.

Data Protection and Grievances/Disciplinary Action

Where it becomes apparent that an employee has (or is suspected of having) contravened any aspect of this Data Protection Policy, then, apart from very minor contraventions, the Company's disciplinary procedure will be invoked. Accordingly, the Company reserves the right to take such action as may be appropriate in the circumstances up to and including dismissal. Depending on the seriousness of the conduct, the employee may be dismissed without notice or pay in lieu of notice. Examples of the type of conduct that could result in dismissal include:

- Any deliberate contravention of one or more of the data protection principles which results in a potential claim for damages against the Company
- Selling (or attempting to sell) personal data relating to an employee of the Company
- Without the Company's express or implied authority, or without the relevant employee's express or implied consent, disclosing personal data relating to any such employee of the Company to a third party

Where an employee believes another employee has infringed his/her data protection rights they are encouraged to bring this to the attention of their line manager in accordance with the Company's grievance procedure.

Policy Acknowledgement

Please acknowledge that you have read and understood this policy by signing below.

I confirm that I have received and read the Company's Data Protection Policy and I acknowledge and understand the contents of the policy.

Signed: …….. Date: ……..

Printed: ……..

Frequently Asked Questions

Who owns the Data Records?
All records are the property of the Company which is responsible for them

Does the Company hold any "secret" records?
The Company may hold certain records that it would be unwilling to disclose and does not have to disclose in accordance with the Act. For example, there may be sensitive documents relating to an employee's promotion or management forecasting which, if disclosed, could cause damage to the Company's interests.

Does the Company need my consent to hold data on me?
Not necessarily. The Company may ask for an employee's consent to hold personal data if the data is defined as being "sensitive", but even in the case of some types of sensitive data, the Act will permit the Company to process that sensitive data if one of the "permitted reasons" contained in the Act applies (e.g. if it is necessary to process the sensitive data in order to perform a legal right imposed on the Company in connection with employment). As such, it will not always be the case that consent is sought or required. Please see policy document for further information.

What should I do if I believe that the data held on me by the Company is inaccurate?
If an employee believes that the data held on them by the Company is inaccurate they should in the first instance bring this to the attention of their Line Manager.

A decision will be made by Human Resources in conjunction with the Line Manager and the employee will be kept informed so that they understand the decision which has been taken and the reasons for it.

In the event that the employee does not agree with the decision which has been taken, they may appeal to the Managing Director whose decision will be final.

For what purpose does the Company hold data on me?
The Company holds data on its employees for a number of legitimate reasons. For example: to enable the Company to pay its employees, to monitor their holiday entitlement, monitor their training and development, contact them as and when necessary, maintain an accurate record of their employment etc.

Do the people who process the data on me understand the need for confidentiality?
The people who have access to employee data have been provided with training in respect of the need for confidentiality. They understand the need to record data accurately, keep it up to date, store and dispose of personal data securely, to keep computer passwords secure and ensure that the information being disclosed is to an individual of the appropriate level and seniority.

Who will have access to data on me?
In addition to those employees who have access to data concerning employees as detailed above, the Company may also provide information to third parties in appropriate circumstances, for example, to the Inland Revenue, the Company's stakeholder pension provider etc.

What will happen if there is an abuse of data processing?
If the Company is made aware of an instance of abuse, it will follow the disciplinary procedure in respect of that employee if appropriate. Any concerns in this regard should be brought to the attention of the Line Manager. In the case of a third party, i.e. someone not an employee of the Company, who is alleged to have been abusing the policy, the Company will take such action as it considers appropriate in the circumstances.

Access to personal records?
Please refer to the attached procedure.

Access to Individual Personal Data

The employee is entitled to request access to their Personnel file and other personal data processed by the Company about them.

The employee is required to give notice in writing to the Head of Human Resources using the attached form. This form is supplied to external data subjects (including former employees and job applicants) as well as existing employees. The Human Resources department will then confirm in writing the date, time and place at which access will be provided on receipt of the written request. Any written request that is made will be dealt with promptly.

Access will normally be provided, where possible, within 28 business days of the written request being received. However, the more comprehensive the search and the more information required, the longer it may take for the Company to provide the information requested.

A fee of £10.00 will be charged prior to access and a cheque for the full amount should be made payable to the Company.

The Company may simply send to the employee requesting their data a copy of the information requested. Alternatively, if the employee asks to see their entire Personnel file, access will be provided in the presence of a member of the Human Resources Department or an appropriate manager delegated by Human Resources for this purpose. This is for the sole purpose of ensuring that no information is inappropriately or inadvertently removed, destroyed or damaged.

Copies of Records

A request may be made for a copy of any, or all, of the contents of the record. In such circumstances, the Company will make a record of which documents if any, have been requested and, where possible, were provided to the employee making the request. Where it would take "disproportionate effort" to supply copies of such information (as described in the Act), the Company reserves the right to refuse to supply such copies.

APPLICATION FOR ACCESS TO PERSONAL DATA

Name:		**Date:**	
Address:			
Telephone No.:			
E-Mail Address:			
Line Manager:			
Relationship to Company **(e.g. Employee, Customer)**			
Relationship **(past or current)**			
What information do you want to be provided? Please provide as much information as possible to enable us to locate the information that you have requested.			
File Search:			
Is the information held in manual files?			
If so, who do you believe has the files?			
What dates do you require the search to cover?	From:		To:
Is the information held in the form of e-mails or in another computerised format?			
Names of authors/recipients of the messages	Authors:		
	Recipients:		
The subject of the mails			
What dates do you believe the messages were sent?	From:		To:

Do you believe the emails to be “live” or in archived or back up form?			
Any other information which may assist our search			
Please complete the above and pass this form to the Head of Human Resources together with a cheque for £10.00 and, except in the case of current employees, a proof of identity.			
Signed:		**Date:**	