Data Protection Policy

Introduction

Warrens GBC Ltd is a registered person under the Data Protection Act 1998 and is subject to scrutiny by the Data Protection Office. The basis of the act is to formalise the procedures which should be followed when the business process or store personal data. Data may essentially be held in an electronic or manual form but under the Act, a business must provide access to data on request and ensure that any data is processed in a fair and reasonable way.

Under the Act, individuals (data subjects) have the right to add information to their records, have inaccurate data deleted and to stop information being used for marketing purposes. Individuals have a legal right to know what data is held and what if anything that data is used for.

Individuals also have a right to know from where information was obtained and if it has been used for any automated decision-making processes e.g.: electronic profiling to shortlist job applications.

A business must respond to request for information within 40 days.

There are both criminal and civil penalties for non-compliance with the Act. Challenges may also be made against offenders under the Human Rights Act.

What exactly is Sensitive Data?

All businesses have a duty to maintain the highest possible levels of security whilst handling data under schedule 3 of the Data Protection Act.

This category covers areas relating to health, sexuality, religion, ethnicity and trade union membership.

For matters concerning sick pay within a payroll, specific consent is required from the employee to the handling of data; e.g. the reasons for sickness quoted by a doctor on a sick note is sensitive data.

Outsourcing of any data processing to third parties does not relieve obligations of a business under the Act and written agreements should be in place documenting exactly what responsibilities each party accepts.

Any personal data should not be transmitted outside the European Economic Area as global protection may not be provided.

Impact upon our Company

Any issues arising which may give rise to Data Protection Act impact must be referred to a Director of the firm.

- Any information gathered by the staff must be for specific purposes and not be more intrusive than is reasonable for us to fulfil the immediate obligations upon us.
- Wherever possible, data held must be and remain as up to date and accurate as possible.
- Data should not be retained any longer than necessary.
- Processing of data must be in accordance with the rights of the individual(s) concerned.
- Processing of data must be done using appropriate technological measures to ensure access can be restricted if required.
- Any data held must be subject to consent.
- Publishing of statement on DPA within any marketing literature, mailing lists etc used.
- Ensure that whenever a data collection event happens we will have adequate methods of recording.
- Knowledge of the Act is sufficient to ensure that a breach of confidentiality does not arise. Breaches can be transmitted verbally, in written form, e-mail, via a website etc.
- A need to monitor internally to ensure that processes are in place and evidence of such monitoring should be recorded.

IN PRACTICE

How do we collect information?

- For clients, we collect information at the first meeting. This information is held in a database and in the client's file. This information will be added to throughout the period during which we act and in most cases, it may extend beyond then.
- For suppliers, we collect information when we trade with them and this may arise very early in the process e.g. at tender or quote stage.
- For introducers to the Company, we gain information through business cards, introduction letters, incoming mail shots etc.
- For staff recruitment purposes we gain information from applications, CV's and telephone conversations and correspondence which for appointed staff will be added to throughout their working period with the Company.
- It should be noted that data collection is often by word of mouth.

Obtaining Consent

- Under no circumstances whatsoever should personal data be given to any third party without consent from the individual.

An indicative but not exhaustive list of examples is given as Appendix B, but staff must use their best judgement in this area.

- Consent is best obtained in writing from a subject but may be by telephone if we know for certain that the person responding is the subject, (in which case a telephone record must be made), or in person at a meeting (when an authority should be signed at the time).
- Consent by e-mail is not acceptable as we cannot guarantee the security of the sender's equipment.
- Consents sent to us by third parties apparently signed by an individual should not be accepted at face value without double checking with a subject.
- We will seek to obtain all necessary consents within 3 working days of a request for data. This is considered reasonable except where a subject may for any reason be unavailable. In such cases, data must not be transmitted.
- Individuals applying for jobs with the Company will be informed of the use of personal details.

Security

- Security and confidentiality are an inherent part of our work and staff should understand the necessity of such.
- Data relating to the staff at the company will be maintained on individual staff record files and available only to authorised personnel.
- Payroll details held on the computer will be password protected and payroll details held manually will be retained in files within a secure environment.
- Security of client data will be detailed in the office manual including methods of processing data within a secure environment.
- Data held on the computer network will be backed up to the server onto the installed mirror hard drive periodically and a daily back up will be made after the end of each working day.

Usage

- Confidentiality of client data including any data relating to clients, employees or agents is restricted to staff of the company with appropriate authorisation and cause.
- Movement of data outside the company will only take place via secure networks and protected data storage.
- Data relating to employees of the company is restricted in access to the management team.
- Consent will be obtained as stated above prior to the release of data to third parties.
- Data will only be used for answering specific requests and should relate only to information necessarily required.
- Professional judgement and ethics must be observed and utilised in dealing with any sensitive data.

Destruction

- Data relating to clients will be maintained for such periods as are laid down by the professional bodies responsible for the conduct of the company.
- Data relating to company staff will be maintained for a period based upon a reasonable business need to retain them which for purposes of future references shall not extend beyond 5 years.

General Awareness

- Any matter relating to data protection may be referred to a Director in the first instance but checks on good practice can be accessed via the Data Protection website www.gov.uk/data-protection.
- For criminal convictions, it must be clear that spent convictions do not have to be declared unless covered by certain exceptions relating to a specific post.
- We will act for clients on payroll bureau only where consent to hold records has been received by us.
- Where clients request payroll details be despatched by fax we must ensure that the methodology is secure.
- We may from time to time request that applications for posts at the company contain details of ethnicity, sexuality, disability or other characteristics, but this will be only for the promotion of our Equal Opportunities Policy and will be detailed on our application form.
- Staff are involved in annual reviews of progress and information is already shared between individuals and Directors on an open basis.

Appendix A

THIRD PARTY REQUESTS FOR DATA RELATING TO EMPLOYEES

Subject access request

This right is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data;
- and given details of the source of the data (where this is available).

In most cases you must respond to a subject access request promptly and in any event within 40 calendar days of receiving it. However, some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request.

Disclosing data to third parties

Exercise caution when dealing with requests for personal information from outside the Company. Personal data should only be disclosed over the telephone in emergencies.

When dealing with routine type queries from public and official bodies, you need to be convinced that:

- the person is who he/she says he/she is
- the enquiry is genuine
- the data in question is clearly identified.

If in any doubt as to the authenticity of the enquiry, seek advice from a senior member of the company. Unless you are familiar with named staff at bodies such as Local Education Authorities, it is advisable to ask for a main switchboard number to phone them back to ensure the legitimacy of a query. Requests in writing should be on official headed paper. Keep a record of all telephone calls with any other correspondence and a copy of the outgoing letter.

Once the legitimacy of the request is established the requested information should be made available.

Requests from the police

The police do occasionally ask for personal data as part of an inquiry, but they don't have the automatic right to receive information about our staff or students. You should not be pressured into handing over personal information. There is a special process to allow the police to access personal data for certain crime-related purposes.

Requests from other third parties

You should not disclose any information about an individual without written and signed permission from the individual. Do not even confirm that an individual is a client of the firm. You can, without implying that a client of the name given is indeed a client, agree to attempt to pass on a letter or message to them, but do not give out addresses or contact details.

If some third-party claims that it is vital to have an answer or to contact an individual immediately, take their details and seek assistance from a senior member of staff.

Appendix B

Third parties who may request data from us and where consent is required for release include the following:

Inland Revenue
Department for Work & Pensions (formerly DSS)
H. M. Customs & Excise
Other Government Regulatory Bodies
Police/National Criminal Intelligence Service
Banks & Building Societies
Other Lending & Financial Institutions
Credit Agencies
Training Agencies
Colleges & Universities
Previous or Prospective Employers
Professional Organisations
Accountancy Firms
Lawyers/Solicitors
Estate Agencies/Surveyors
Staff Representing Clients
Employment or similar Agencies

The list is indicative and not exhaustive – staff must use the highest levels of discretion and confidentiality in dealing with any requests for data from third parties.

Appendix C

RETENTION PERIODS FOR EMPLOYEE RECORDS

Application Form - Duration of Employment

References Received - Duration of Employment

Payroll & Taxation Information - 9 years

Sickness Records - Duration of Employment

Annual Leave Records - Duration of Employment

Unpaid/Special Leave Records - 3 years

Annual Appraisal Records - 5 years

Notes regarding Promotion, Training & Disciplinary matters - 1 year after end of employment

References given & relevant Information used - 5 years after end of employment

Records relating to Accidents or Injury at work - 12 years after event

The above criteria are for guidance only but if longer periods are considered appropriate then justification must be given.