Data Protection Policy

Introduction

Gooch Maloney & Partners Limited is a registered person under the Data Protection Act and the General Data Protection Regulations 2018 and as such is subject to scrutiny by the Information Commissioners Office. The basis of the legislation is to formalise the procedures which should be followed when businesses process or store personal data. Data may essentially be held in an electronic or manual form but under the legislation, a business must provide access to data on request, only use data when positive consent to its use has been given by the relevant person, delete data upon request and ensure that any data when held or used is processed in a fair manner & with sound business justification for doing so.

Under the legislation, individuals (data subjects) have the right to add information to their records, have inaccurate data amended or deleted and to stop relevant information from 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 eg: electronic profiling in order to shortlist job applications.

A business must respond to request for information within a reasonable time and Gooch Maloney & Partners Limited have set internal deadlines of 21 days for responding.

There are both criminal and civil penalties for non-compliance with the legislation. 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. Eg: 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 our business under the legislation and written agreements will be in place documenting exactly what responsibilities each party accepts.

Any personal data will not be transmitted outside the European Economic Area as it is understood that global protection may not be provided.

Impact upon our Company

We must appoint a Data Controller. For this purpose the Directors of the company will act with full responsibility in that capacity on a day to day basis but ultimately, decision making on policy & procedures implementation will be with Graham Hole

- Any issues arising which may give rise to DPA impact must be referred to a Director of the firm at the earliest possible opportunity.
- Any data gathered by staff must be for specific purposes and not be more intrusive than is reasonable in order 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 must 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 prior positive consent.
- Issuing of Newsletters to relevant individuals must be upon the basis of such positive consent being in our possession.
- Ensuring that whenever a data collection event happens we will have in place adequate methods of recording.
- Knowledge of the legislation 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 that processes are in place and evidence of such monitoring taking place.
- Ensuring that we do not breach the regulations on interventionary protection.

IN PRACTICE

How do we collect information?

- For clients we collect information at the first meeting which we hold on a database and as part of this process the client gives appropriate consent to our holding their data. This information will be added to throughout the period of time 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 eg: 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 and will include relevant ID and family contact details for emergencies
- It should be noted that data collection is often by word of mouth. Staff can record on hard copy or electronic notes, the telephone conversation & the nature of the data.

Note; The nature of our business means that we must have certain data from clients in order to fulfil our compliance work for those clients and in the event of not receiving positive consent on use, staff must report the facts to a Director but it is unlikely that we would be in a position to continue working for that client. That decision must only be taken by a Director.

Obtaining Consent

- Under no circumstances whatsoever should personal data be given to any third party without prior written consent (including consent by e-mail as a last resort) 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).
- 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 or cross referencing to a known valid signature eg; on a tax return
- We will seek to obtain all necessary release consents within 5 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 staff at the Company will be maintained on individual staff record files and available only to Directors.
- Payroll details held on computer will be password protected and payroll details will be retained in files within a secure environment.
- Data held on the computer network will be backed up within the hosted server or server onto the installed mirror hard drive instantaneously and daily back ups will be made after the end of each working day.
- Mobile Data eg; Laptops & USB memory sticks will all be password protected
- Passwords will be changed on a regular basis & upon single event changes eg; changes in staff

Usage

- Confidentiality of client data including any data relating to clients employees or agents is restricted to staff of the Company. It is subject to the separate Confidentiality Agreement which is encompassed within each Contract of Employment
- Data relating to employees of the Company is restricted in access to the Directors.
- Consent will be obtained as stated above prior to release of data to third parties.
- Data will only be used for the purpose of 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

- All individuals have a right to request that data is deleted as appropriate. This is generally referred to as the "Right to be Forgotten"
- 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 or by statutory requirements. There may well be justifiable reporting needs in respect of certain data where deletion is not possible simply because an individual requests it.eg compliance with Anti Money Laundering Regulations or at the Order of the Courts
- Data relating to Company staff will be maintained for a period of time based upon a reasonable business need to retain them which for purposes of future references shall not extend beyond 3 years.

General Awareness

- Any matter relating to data protection must be referred to a Director in the first instance but checks on good practice can be accessed via the Data Protection website https://ico.org.uk/
- A copy of the draft codes of practice are available from the website and a copy is available within the Company from the Directors.
- 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.ie; end to end encryption.
- Transmission of any data to clients or with clients consent must be achieved through the use of pdf files which may not be secure and for which the client can specify a paasword
- Any confidential information handed to the Directors for onward transmission to the Pension Auto-enrolment Company should be in a sealed envelope and as such will not be accessed by anyone prior to despatch.
- 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.
- Staff are involved in annual reviews of progress and are already shared as between individuals and Directors on an open basis.