Data Protection Policy

Introduction

We may have to collect and use information about people with whom we work. These may include members, current, past and prospective employees, clients, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Data Protection Act 2018 to ensure this.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.

To this end, we fully endorse and adhere to the Principles of Data Protection as set out in the Data Protection Act 2018.

The principles of data protection

The Act stipulates that anyone processing personal data must comply with Eight Principles of good practice. These Principles are legally enforceable.

The Principles require that personal information:

1. shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. shall be accurate and where necessary, kept up to date;
5. shall not be kept for longer than is necessary for that purpose or those purposes;
6. shall be processed in accordance with the rights of data subjects under the Act;
7. shall be kept secure i.e. protected by an appropriate degree of security;
8. shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any **personal data**. It also makes a distinction between personal data and **"sensitive" personal data**.

Personal data is defined as data relating to a living individual who can be identified from:

1. that data;
2. that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.

Sensitive personal data is defined as personal data consisting of information as to:

1. racial or ethnic origin;
2. religion or other beliefs;
3. trade union membership;
4. physical or mental health or condition;
5. sexual life;
6. criminal proceedings or convictions.

Handling of personal/sensitive information

We will, through appropriate management and the use of strict criteria and controls,:

1. observe fully conditions regarding the fair collection and use of personal information;
2. meet our legal obligations to specify the purpose for which information is used;
3. collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
4. ensure the quality of information used;
5. apply strict checks to determine the length of time information is held;
6. shall be accurate and where necessary, kept up to date;
7. shall not be kept for longer than is necessary for that purpose or those purposes;
8. shall be processed in accordance with the rights of data subjects under the Act;
9. shall be kept secure i.e. protected by an appropriate degree of security;

In addition, we will ensure that:

1. everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
2. methods of handling personal information are regularly assessed and evaluated;

All members of staff are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff must take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

1. paper files and other records or documents containing personal/sensitive data are kept in a secure environment;

2. personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
3. individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or Directors must:

1. ensure that they and all of their staff who have access to personal data held or processed for or on behalf of us, are aware of this policy and are fully aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Company and that individual, company, partner or firm;
2. allow data protection audits by us of data held on our behalf (if requested);
3. indemnify us against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by us will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by us.

Implementation

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

Auditing and Monitoring

All staff members with the potential to access confidential personal information should be aware that monitoring and auditing of access is being carried out, and so full compliance to our Data Protection Policy is required. More details can be found in Confidentiality Audit Procedure

Subject Access Requests (SAR)

All individuals who are the subject of personal data held by Facts and Dimensions Ltd are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.

If an individual contacts the company requesting this information, this is called a RTA (Rights To Access Request).

Rights to Access requests from individuals should ideally be made by email, addressed to the data controller at Facts and Dimensions Ltd, Ross Building, Adastral Park, Martlesham Heath, Ipswich, IP5 3RE. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals may be charged £10 per subject access request. The data controller will aim to provide the relevant data within a month.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Internal Personal Information

How long do we keep staff records for, under GDPR?

We don't store all staff records forever. This depends on whose data we're keeping and how long we've stored it for already.

See Information Retention Periods for Types of Records for full details of retention periods for information types.

Current staff

GDPR doesn't set out any minimum or maximum time limits for keeping staff data. But it does state that we shouldn't keep personal data for longer than you need to.

The length of time we'll keep data for will depend on the reason why we've collected it. For example, if we collect an employee's contact number to use in case of emergency, it's not necessary to keep this once the employee leaves.

However, there are legal requirements we must follow:

- **Working time records:** Keep for *2 years* from the date the records refer to.
- **Payroll records:** Keep for *3 years* from the end of the tax year that they relate to.
- **Maternity, Paternity or Shared Parental Pay records:** Keep for *3 years* after the end of the tax year that the payment stopped.

Former staff

After an employee leaves, we can not delete their records right away. We might need them to defend ourself against a tribunal or court claim.

Generally, an employee can make a claim to an employment tribunal within three months of their employment ending. But depending on the claim, the limit can be six months or longer.

If an employee claims that we've breached their contract, they might take us to the civil courts. They can do this within six years of the alleged breach.

As a result, we keep personal data, performance appraisals and employment contracts for six years after an employee leaves.

Former employees, or anyone we hold data on, can request their data with a Subject Access Request (SAR - See above) to see what data we hold on them.

Job applicants

We collect a lot of information from job applicants including CV's, cover letters and interview notes.

We hold onto this data for 6 months, even if the applicant was unsuccessful, as they could log a discrimination claim against us within this time.

In order to hold a CV on file, and continue to be GDPR compliant, we'll need to get consent from applicants and make sure their information is up-to-date.

Client Personal Information

GDPR Article 5(1)(e) says:

1. Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')"

Guide to the General Data Protection Regulation (GDPR)

At a glance:

- You must not keep personal data for longer than you need it.
- You need to consider, and be able to justify, how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy, setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Checklist for Retaining Client Information

- We know what personal data we hold and why we need it, as detailed in the Information Asset Register.
- Facts & Dimensions Ltd Policy is that we do not hold this Customer Information for more than *2 years*, without validation.
- All Customer information is audited bi-annually to ensure the above checklist is valid, and erase, anonymisation, or pseudonymisation is performed as is appropriate to ongoing use.
- We have a Rights of Access policy (and Rights of Access Request Form) for any individuals' requests for the data that we hold about them, and any requests for erasure under, "the right to be forgotten."

Customer Information can contain: names, business addresses, business telephone, and email. Access Level set in Secure Data Access List