

28. DATA PROTECTION POLICY

INTRODUCTION

The General Data Protection Regulations (GDPR) is about protecting the rights of all employees with regard to your personal information. In addition to protecting privacy, the GDPR aims to ensure reliability of information and its fair and legitimate use. Subject to certain exemptions the GDPR gives you the right to access any personal information held about you.

The Act covers information, which is recorded as part of a 'relevant filing system', i.e. a set of information in which records are structured, either by reference to you or by reference to criteria relating to you, which would make you or your specific information identifiable. This policy clarifies our approach to protecting personal data.

SCOPE AND PURPOSE - PRINCIPLES OF THE ACT

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for specific, explicit and valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant and adequate to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.
7. Where applicable, comply with the relevant data protection procedures for international transferring of personal data.

THE RIGHTS OF DATA SUBJECTS UNDER THE ACT

The Act grants you to have the right to have a copy of the information that an organisation holds about you. It also allows you to apply to the courts to obtain an order requiring an organisation to correct inaccurate data held, and to seek compensation where damage and distress have been caused as a result of any breach of the Act.

Under certain circumstances, by law you have the right to:

- Be informed about the collection and use of your personal data;
- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- Request the erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it;
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- Request the transfer of your personal information to another party;
- Regulate any automated decision-making and profiling of your personal data; and,
- Object to the processing of your personal data in certain circumstances

COMPANY RESPONSIBILITIES UNDER THE ACT

Management of the Company are responsible for compliance with the Act. We have responsibility for the type of personal data collected and how that data is used. Where we are required to disclose or process personal data we must ensure it is compliant with the Act.

STAFF RESPONSIBILITIES UNDER THE ACT

No member of staff should disclose personal data outside the Organisation's procedures, or use personal data held on others for their own purposes.

THE TYPES OF DATA COVERED BY THE ACT

PERSONAL DATA

The Act is concerned with 'personal data'. That is, information which:

- relates to a living person, and
- identifies an individual either on its own or together with other information that is in the Organisation's possession or that is likely to come into its possession.

The Act relates to all personal information, whether it is kept manually or electronically, that is held in a 'relevant filing system' (as defined above). In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered.

PROCESSING

The Act applies to personal data that is subject to 'processing'. For the purposes of the Act, the term 'processing' includes the initial obtaining of personal data, keeping and using the data, accessing, disclosing and destroying the data.

Examples of personal data likely to be covered by the Act include:

- Details of an employee's home address, telephone number, and any other personal information held on a computer system or in a manual filing system;
- An e-mail about an incident involving a named employee;
- A manager's notebook containing sections on several named employees;
- Meeting notes;
- CVs and other information gathered during recruitment process. You also have the right to ask us to stop processing personal information

References from former employers;

- National Insurance numbers;
- Job title, job descriptions and pay grades;
- Holiday records;
- Internal performance information;
- Medical or health information;
- Sickness absence records;
- Tax codes;
- Terms and conditions of employment; and,
- Training details.

In practice nearly all usable information held about individuals will be covered by the Act.

The data the Company holds will be for management and administrative use only but the Company may, from time to time, need to disclose some data it holds about you to relevant third parties (e.g. parties with which it has a contract for services i.e. legal support/advice, where legally obliged to do so by the Inland Revenue, or where requested to do so by yourself for the purpose of giving a reference).

SENSITIVE PERSONAL DATA

Sensitive data is information concerning your:

- racial or ethnic origin
- political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- physical or mental health or condition
- Sexual orientation
- commission or alleged commission of any offence, or
- Proceedings for any offence committed or alleged to have been committed.

DATA SECURITY

The Company have put in place measures to protect the security of data to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. Failure to follow the Company's rules on data security may be dealt with via the disciplinary policy. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so

CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

REQUEST FOR INFORMATION

You may request information, as defined above, on any normal working day i.e. Monday to Friday inclusive.

All requests must be hand-written quoting your home address and National Insurance number and referring to the General Data Protection Regulations. Requests should be put in a sealed envelope addressed to a Senior Manager/Director/Partner.

The information will be made available within 30 days. If the consent of a third party is necessary, the time limit will run from the time of the receipt of the information or consent.

In the event that the request is manifestly excessive, the Company has the right to refuse a request. Any refusals will be in writing explaining on what grounds refusal has been made along with the right to seek judicial remedy and to make a complaint to the Information Commissioner's Office.

This policy is to be read in conjunction with the Privacy Policy provided to you separately

A handwritten signature in black ink, appearing to be 'MML'.

1.4.26

