

Data Protection Policy

Introduction

Kimal plc holds and processes information about its job applicants, employees, ex-employees, customers / clients, suppliers and other individuals for various purposes, e.g. to operate the payroll and to enable correspondence and communication to those with whom it deals.

To comply with the Data Protection Act 1998 ("the 1998 Act"), information must be collected and used properly, stored safely and not disclosed to unauthorised persons.

Purpose

The purpose of this policy is to ensure that the company complies fully with its legal obligations in relation to the protection of personal data that it holds about or concerning any individual.

All employees and Managers of the company must familiarise themselves fully with its contents and ensure that its terms are applied fully in relation to the handling or "processing" of personal data.

Those employees whose job involves the handling of personal data will receive appropriate training at their induction¹ and, as required during their employment, on the detail of the Data Protection Act 1998 and the procedures for obtaining, retaining, updating, using, transporting, sending and destroying personal data. All of these functions are strictly confidential and any employee handling personal data in breach of the company's data protection policy may face disciplinary charges that may, in serious cases, result in dismissal.

This policy concerns personal data held by the company in relation to any person, whether they are, were or are about to become employees of the company or any customer, supplier or contact. Personal data is described below in more detail, but the concept is very broad and may include any information about any individual, held by the company.

Data protection laws are overseen by the Information Commissioner who has powers to take legal action against businesses or individuals acting unlawfully. Any employee may make themselves individually liable to legal action by the Information Commissioner and/or by any individual whose information they have disclosed in breach of data protection legislation and who suffers loss as a result. There have also been very high profile cases involving loss of data in breach of the legislation giving rise to very real damage to the reputation of the organisations concerned. This policy is designed to prevent such potential damage to the company and its employees and to ensure that personal data processed by the company is dealt with in full compliance with the law.

Definition and Scope

The law contains some important concepts that define the obligations of the company and its employees. Although most employees are not expected to remember detailed legal definitions, a general understanding of the concepts is required to avoid inadvertent breaches and to ensure that employees can take further advice in relation to any particular situation that may give rise to concern. The company has nominated the HR Manager to be responsible for data processing and compliance with data protection legislation. Any questions or concerns relating to the company's or any individual employee's responsibilities should, in the first instance, be referred to the employee's direct line manager.

Summary of Aims

The lawful and correct treatment of personal information is vital to successful operations, and to maintaining confidence in the Company and the individuals with whom it deals. Therefore, the Company will by appropriate management and the strict application of controls will:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- 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;
- ensure the quality of information used;
- determine the length of time information is held;
- ensure that the rights of people about whom information is held can be exercised under the Act. These include, but are not limited to, the right of access to their personal information; the right to correct or request the erasure of information which they regard as incorrect;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

Notification to the Information Commissioner

The Company has an obligation as a Data Controller to notify the Information Commissioner (“IC”) of the purposes for which it processes personal data. Individual data subjects can obtain full details of the Company’s data protection registration/notification with the Information Commissioner from the Company Data Protection Manager or from the Information Commissioner’s website (<http://www.dataprotection.gov.uk>).

Data Protection Principles

The Company, as a Data Controller, must comply with the Data Protection Principles which are set out in the 1998 Act. In summary these state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date
- Not be kept for longer than is necessary for those purposes.
- Be processed in accordance with the data subject’s rights under the 1998 Act, as amended by the Freedom of Information Act 2000.
- Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country or territory has equivalent levels of protection for personal data.

Data Processing

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including the:

- organisation, adaptation or alteration of the information or data,
- retrieval, or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available,
- erasure or destruction of the information or data.

Data Protection Manager

The Company Data Protection Manager is the HR Manager. All queries about the Company policy and all requests for access to personal data should be addressed to the Data Protection Manager (see "Right to Access Personal Data" below).

Responsibilities of individual Data Users

All members of the Company who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with the requirements of the 1998 Act (including the Data Protection Principles) and with the Company's data protection policy (including any procedures and guidelines which may be issued from time to time). A breach of the 1998 Act and/or the Company's data protection policy may result in disciplinary proceedings.

In particular, no member of the Company may, without the prior written authorisation of the Data Protection Manager:

- develop a new computer system for processing personal data;
- use an existing computer system to process personal data for a new purpose;
- create a new manual filing system containing personal data;
- use an existing manual filing system containing personal data for a new purpose.

The above does not apply to databases which are maintained by individual Data Users within the Company for their private domestic uses, for example, private address books. However, individual Data Users should consider whether their private domestic uses fall within the scope of the 1998 Act and whether they will need to register this with the Information Commissioner. If any individual employee has any concerns regarding 'personal databases' they may have, they should consult with the Data Protection Manager.

Data storage Areas

Data may be held in paper records and or in electronic databases. Access to such electronic databases is restricted in the same manner as access to paper based files. However, in addition to other data users the Computer Manager, or the nominated deputy, may have day-to-day access to the electronic databases for the purposes of administering and maintaining the same.

Email

It is permissible and appropriate for the Company to keep records of communications, including electronic communications, which are relevant to an individual's ongoing relationship with the Company provided such records comply with the Data Protection principles.

It is recognised that email is increasingly used for such communications and that such emails will form part of the Company's records. It goes beyond the scope of this policy document to address the appropriate use of email in the proper functioning of the Company, and the limitations and legal implications with this mode of communication. However, employees should be aware that the Company will monitor the use of its electronic communications facilities including email to ensure its proper and authorised use. See the Company's Electronic Communications policy which also includes the

However, all members of the Company need to be aware that the 1998 Act applies to emails which contain personal data about individuals which are sent or received by members of the Company (other than for their own private purposes as opposed to Company purposes. However if such communications are undertaken then individual Data Users should consider whether this private uses falls within the scope of the 1998 Act and thereby they become liable for it to be registered and controlled).

- subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the Company to locate the personal data in the emails;
- the legislation applies to all emails from and to members of the Company which are sent and received for Company purposes, whether or not the emails are sent through the Company email system or on an individual's own email account.

Sensitive Personal Data

The Company may from time to time process "sensitive personal data" relating to individuals with whom it has dealings.

"Sensitive personal data" is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

Currently, the Company envisages the need to process sensitive personal data.

For example,

- data relating to the ethnic origin of employees may be processed for the purposes of equal opportunities monitoring
- Medical records for the provision of healthcare and general welfare of employees and clients
- In exceptional circumstances, the Company may need to process information regarding criminal convictions or alleged offences in connection, e.g. with any disciplinary proceedings or other legal obligations e.g. CRB checks.

In other circumstances, where sensitive personal data is to be held or processed, the Company will seek the explicit consent of the individual in question unless one of the limited exemptions provided in the Data Protection Act 1998 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

Data Security and Disclosure

All members of the Company are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, consult the Company Data Protection Manager.

Personal data must be kept securely and examples of how this may be done will include:

- keeping the data locked in a filing cabinet, drawer or room; or
- if the data is computerised, ensuring that the data is password protected or kept only on disk which is itself kept securely; or
- any other appropriate security measure.

Right to Access Personal Data

Data Subjects have the right under the 1998 Act to access any personal data that is being held about them either in, a form that can be automatically processed (mainly computer records) or in a "relevant filing system" (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible) and to request the correction of such data where it is incorrect.

The Freedom of Information Act 2000 amends the Data Protection Act 1998 in a number of ways, including extending data subjects' right of access to personal information held about them by the Company. Individuals have the right to access personal information held in "unstructured" files, so that even personal data held in a file relating to something else (e.g. a file without the subject's name on the front, or minutes of a meeting) must be disclosed to the data subject under the Data Protection Act provided that the individual data subject can provide sufficient information for the Company to locate the personal data.

An individual who wishes to exercise their right of access must complete the Company "Subject Access Request" form which is available on the company's intranet under HR Documents.

The Company will make a charge of £10 (or such other charge as is permitted from time to time by the Data Protection Act 1998) on each occasion that access is requested and this fee should accompany the Subject Access Request form. In accordance with the 1998 Act, the Company reserves the right to refuse repeated requests where a reasonable period has not elapsed between requests.

The Company will respond to the request for access to personal data within 40 days of the request or payment of the fee, whichever is the later.

If any inaccuracies in data are disclosed by such a request the Data subject should communicate immediately to the Data Protection Manager who shall take appropriate steps to make the necessary amendments if applicable.

Disclosure outside of the EEA

The Company may, from time to time, be required to transfer personal data to countries or territories outside of the European Economic Area in accordance with purposes made known to individual data subjects.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.



Data Subjects' Consent

Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. The Company will consider any objections to the use it makes of personal data but reserves the right to process personal data in order to carry out its functions as permitted by law.

Hard copies taken of this document will not be maintained – to check you are using the latest copy contact the Data Protection Manager Bridget Brooks, bridget_brooks@kimal.co.uk