Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of BMS Accountants Ltd. (hereinafter referred to as "the Company"). This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), and the Irish Data Protection (Amendment) Act (2003).

Rationale

The Company must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by the Company in relation to its staff, service providers and clients in the course of its activities. The Company makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Scope

The policy covers both personal and sensitive personal data held in relation to data subjects by the Company. The policy applies equally to personal data held in manual and automated form.

All Personal and Sensitive Personal Data will be treated with equal care by the Company. Both categories will be equally referred-to as Personal Data in this policy, unless specifically stated otherwise.

This policy should be read in conjunction with the associated Subject Access Request procedure, the Data Retention and Destruction Policy, the Data Retention Periods List and the Data Loss Notification procedure.

BMS Accountants as a Data Controller/Data Processor

In the course of its daily organisational activities, the Company acquires processes and stores personal data in relation to:

- Employees of the Company
- Customers of the Company
- Third party service providers engaged by the Company

In accordance with the Irish Data Protection legislation, this data must be acquired and managed fairly. Not all staff members will be expected to be experts in Data Protection legislation. However, the Company is committed to ensuring that its' staff have sufficient awareness of the legislation in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the Data Protection Officer is informed, and in order that appropriate corrective action is taken.

Due to the nature of the services provided by the Company, there is regular and active exchange of personal data between the Company and the Data Subjects of the Data Controllers. In addition, the Company exchanges personal data with Data Controllers on the Data Subjects' behalf.

This is consistent with the Company's obligations under the terms of its contract with its Data Controllers.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a Company staff member is unsure whether such data can be disclosed.

In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

Subject Access Requests

Any formal, written request by a Data Subject for a copy of their personal data (a Subject Access Request) will be referred, as soon as possible, to the Data Protection Officer, and will be processed as soon as possible.

It is intended that by complying with these guidelines, the Company will adhere to best practice regarding the applicable Data Protection legislation.

Third-Party processors

The Company does not currently engage third party processors to process any personal data. If the need arises the Company will in each case ensure, a formal, written contract is in place with the Processor, outlining their obligations in relation to the Personal Data, the specific purpose or purposes for which they are engaged, and the understanding that they will process the data in compliance with the Irish Data Protection legislation.

Consent - Marketing

It is important that customers/business contacts understand that we **do not** share their data with any one for the purposes of marketing.

Personal information will not be shared with a third party for any reason without prior consent.

Data Breach

In case of a personal Data Breach you will be informed of same within 72 hours of the breach becoming known. The Data Protection Officer will notify the Data Protection Commissioner.

The Data Protection Principles

The following key principles are enshrined in the Irish legislation and are fundamental to the Company's Data Protection policy.

In its capacity as Data Controller/Data Processor, The Company ensures that all data shall:

1. ... be obtained and processed fairly and lawfully.

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the Data Controller
- The purpose(s) for which the data is being collected
- The person(s) to whom the data may be disclosed by the Data Controller
- Any other information that is necessary so that the processing may be fair.

The Company will meet this obligation in the following way.

- Where possible, the informed consent of the Data Subject will be sought before their data is processed;
- Where it is not possible to seek consent, The Company will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Where the Company intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view;
- Processing of the personal data will be carried out only as part of the Company's lawful activities, and the Company will safeguard the rights and freedoms of the Data Subject;
- The Data Subject's data will not be disclosed to a third party other than to a party contracted to the Company and operating on its behalf.

2. .... be obtained only for one or more specified, legitimate purposes.

The Company will obtain data for purposes which are specific, lawful and clearly stated. A Data Subject will have the right to question the purpose(s) for which the Company holds their data, and the Company will be able to clearly state that purpose or purposes.

3. ..... not be further processed in a manner incompatible with the specified purpose(s).

Any use of the data by the Company will be compatible with the purposes for which the data was acquired.

4. .... be kept safe and secure.

The Company will employ high standards of security in order to protect the personal data under its care. Appropriate security measures will be taken to protect against unauthorised access to, or alteration, destruction or disclosure of any personal data held by The Company in its capacity as Data Controller.

Access to and management of staff and customer records is limited to those staff members who have appropriate authorisation and password access.

5. ... be kept accurate, complete and up-to-date where necessary.

The Company will:

- ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- conduct periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. The Company conducts a review of sample data every six months to ensure accuracy; Staff contact details and details on next-of-kin are reviewed and updated every two years.
- conduct regular assessments in order to establish the need to keep certain Personal Data.

6. ***... be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed.***

The Company will ensure that the data it processes in relation to Data Subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. ***... not be kept for longer than is necessary to satisfy the specified purpose(s).***

The Company has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, the Company undertakes to destroy, erase or otherwise put this data beyond use.

8. ***... be managed and stored in such a manner that, in the event a Data Subject submits a valid Subject Access Request seeking a copy of their Personal Data, this data can be readily retrieved and provided to them.***

The Company has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, the Company's staff engage in active and regular exchanges of information with Data Subjects. Where a formal request is submitted by a Data Subject in relation to the data held by the Company, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which the Company must respond to the Data Subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

The Company's staff will ensure that, where necessary, such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than 40 days from receipt of the request.

Implementation

As a Data Controller, the Company ensures that any entity which processes Personal Data on its behalf (a Data Processor) does so in a manner compliant with the Data Protection legislation.

Failure of a Data Processor to manage the Company's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts.

Failure of the Company's staff to process Personal Data in compliance with this policy may result in disciplinary proceedings.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply within this Policy.

Data	This includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is processed on computer. Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information which relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of the Data Controller. (If in doubt, [The Company] refers to the definition issued by the Article 29 Working Party, and updated from time to time.)
Sensitive Personal Data	A particular category of Personal data, relating to: Racial or Ethnic Origin, Political Opinions, Religious, Ideological or Philosophical beliefs, Trade Union membership, Information relating to mental or physical health, information in relation to one's Sexual Orientation, information in relation to commission of a crime and information relating to conviction for a criminal offence.
Data Controller	A person or entity who, either alone or with others, controls the content and use of Personal Data by determining the purposes and means by which that Personal Data is processed.
Data Subject	A living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes Personal Data on behalf of a Data Controller on the basis of a formal, written contract, but who is not an employee of the Data Controller, processing such Data in the course of his/her employment.
Data Protection Officer	A person appointed by [The Company] to monitor compliance with the appropriate Data Protection legislation, to deal with Subject Access Requests, and to respond to Data Protection queries from staff members and service recipients
Relevant Filing System	Any set of information in relation to living individuals which is not processed by means of equipment operating automatically (computers), and that is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a manner that specific information relating to an individual is readily retrievable.