Company Data Protection Policy

Direct Data Analysis

Data Protection Registration Number: Z3022378

This document is to be read by all persons employed, who also need to sign that they have read and fully understand the data protection policy of Direct Data Analysis.

June 2011

1st June 2011

Data Protection Policy

Introduction

Direct Data Analysis (The Company) is required to collect and store certain personal data as part of its business activities. The Company recognises the importance of the correct and lawful treatment of personal data; it maintains confidence in the organisation and provides for successful operations.

The types of personal data that the Company may require includes information about: members of the public, company employees, etc, who have given permission for data to be collected for survey research and analysis purposes. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

The Company fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for the Company must adhere to these principles.

Any person working with data for or on behalf of Direct Data Analysis needs to be aware of this policy and confirm by signature that they fully understand and will abide by the policy at all times.

Principles

The principles require that personal data shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met;

2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;

3. Be adequate, relevant and not excessive for those purposes;

4. Be accurate and, where necessary, kept up to date;

5. Not be kept for longer than is necessary for that purpose;

6. Be processed in accordance with the data subject's rights;

7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;

8. And not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Satisfaction of principles

In order to meet the requirements of the principles, the Company will:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- take the appropriate technical and organisational security measures to safeguard personal data;
- and ensure that personal data is not transferred abroad without suitable safeguards.

The Company's Designated Data Controller

The Company's Information Compliance Manager is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Company. The Information Compliance Manager is *Phil Woodvine*. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Information Compliance Manager.

Status of the Policy

Any employee who considers that the policy has not been followed in respect of personal data should raise the matter with the Company's Information Compliance Manager in the first instance.

Any breach will be taken seriously and may result in formal action.

Subject Access

All individuals who are the subject of personal data held by the Company 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.
- Be informed what the Company is doing to comply with its obligations under the 1998 Data Protection Act.

Employee Responsibilities

All employees are responsible for:

- Checking that any personal data that is provided to the Company is accurate and up to date.
- Ensuring that any change to information which has been provided, e.g. changes of address, is processed swiftly and accurately.
- Checking any information that the Company may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, employees collect information about other people (e.g. about personal circumstances), they must comply with the Policy and with the Data Protection Procedures which are contained in the Data Protection Manual.

Data Security

The need to ensure that data is kept securely means that precautions **must** be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- Any personal data which they hold is kept securely at all times.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.
- Computer screens are locked to prevent unauthorised viewing when the authorised user is away from the computer.
- No personal data is to be viewed or worked upon in a public area (i.e. on the train).
- Data is not allowed to be stored on employees own personal computers.

Data will be secured in two levels as follows:

1. All devices that hold data (computer, laptop, portable data storage device) are password protected to prevent unauthorised access.
2. Databases, spreadsheets and all other data storage programmes to be password protected. This must be a separate password to that required to access the computer/storage device.

All passwords must contain a mix of letters and numeric and be a minimum of 6 characters long.

Rights to Access Information

Employees and other subjects of personal data held by the Company have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request in writing to the Company's Information Compliance Manager.

The Company reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.

The Company aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days of a written request, unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Subject Consent

The purpose to collect and process data should be communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, then where a person may be identified from the data stored, express consent to process the data must be obtained.

Retention of Data

The Company will keep some forms of information for longer than others. All staff are responsible for ensuring that information is not kept for longer than necessary and need to agree with the client how long data is to be kept.

Upon disposal of data;

- Paper Data: To be shredded and then disposed of securely.
- Electronic data:
  - Portable data stores (for temporary holding or transporting) – data to be deleted and the data store formatted.
  - Computers and laptops – Delete data and then run the 'cleaner' programme installed on the Company's computer.

Employee Understanding of the Policy

I [*insert name of employee here*] confirm that I have read, understand, and will comply with at all times, this Data Protection Policy issued by Direct Data Analysis, and that any breach of the policy may lead to disciplinary action or dismissal from employment.

Signed: …….

Print Name: ……..

Date: ……..