

# Silver Planet Life Investment Taxation Solutions Limited

## Data Protection Policy

### **Introduction**

This document is a statement of the Company's Data Protection Policy. The details are below. This policy is not part of your employment contract and it is not legally binding except where it is a statement of the law.

### **About the Data Protection Act**

The Data Protection Act 1984 is concerned about information about individuals. This covers all aspects of the Company's operation, including suppliers, customers, shareholders and employees.

The Act is concerned with "personal information" which is defined as:

- about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature, and
- identifies a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession.

The Act applies to personal information that is subject to 'processing'. For the purposes of the Act, the term 'processing' applies to a comprehensive range of activities. It includes the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

Anyone who "processes data" is called a "data controller". A data controller is required to comply with the eight principles of good information handling (the Data Protection Principles):

These principles require the data controller to:

1. process personal data fairly and lawfully.
2. obtain personal data only for one or more specified and lawful purposes and to ensure that such data is not processed in a manner which is incompatible with the purpose or purposes for which it was obtained.
3. ensure that personal data is adequate, relevant and not excessive for the purpose or purposes for which it is held.
4. ensure that personal data is accurate and, where necessary, kept up to date.
5. ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. process personal data in accordance with the rights of the individuals to whom the information relates.
7. ensure that personal data is kept secure.
8. ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which the information is to be sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

The Act also lays down rules concerning the processing of 'sensitive personal data'; that is data that consists of information about an employee's:

- racial or ethnic origins;
- political opinions;
- religious beliefs;
- trade union membership (or non-membership);
- physical or mental health or condition;
- sex life or sexual orientation;
- criminal (or alleged criminal) activities;
- criminal proceedings, criminal convictions (or any sentences imposed by the courts).

Sensitive personal data must not be held on an employee's personal file without his or her express consent - unless held in compliance with an employer's legal obligations (for example under health and safety legislation) or to protect the employee's vital interests (for example under the Sex Discrimination Act 1975).

The Act requires that the Company must register that it is processing information held on a computer or in some manual filing systems about living individuals on the Information Commissioner's Register.

**The Company's policy on Data Protection**

The Company will register with the Information Commissioner under the Data Protection Act and will fulfil its legal commitments with regard to the Data Protection Principles and the retention of personal data about individuals.

The Company will only collect and retain that information that it needs to carry out its legitimate activities and will hold that information confidentially.

Where the Company needs to obtain and hold "sensitive data", it will only do so with the express permission of the individuals concerned and will hold that data securely.

Where personal data is no longer required, it will be removed from the relevant files and deleted or destroyed.

**Employee's responsibilities on Data Protection**

Every employee has a personal responsibility to comply with the requirements of the Act and the Company policy. It is, therefore, the responsibility of every employee within the terms and to the fullest extent of the Act to protect any personal data that they hold or are responsible for on behalf of the Company and to uphold the legal requirements placed on the Company for Data Protection.

Any employee who is found to have revealed or disclosed any personal data to any unauthorised person or organisation will be in breach of Company policy and will be subject to disciplinary action, which may, dependent on the nature of the disclosure be regarded as Gross Misconduct. Such disclosure may also be treated as a criminal offence.

*This document is a statement of the relevant law where appropriate together with the Company's policies on the subject. The Company reserves the right to amend any non-statutory parts of this policy.*

*This document was current as at 04/11/2009. New Employment legislation and case law means that this document will become out of date and will need reviewing and amending, preferably every 12 months.*