
# DATA PROTECTION POLICY

**Contents**

## 1. INTRODUCTION

StarLife Assurance Company Limited ("the Company") needs to gather and use certain information about individuals. These individuals are known as data subjects and may include customers, suppliers, business contacts, employees, directors, shareholders and other people whom the Company has a relationship with or may need to contact.

The information obtained from these data subjects is protected by law and the Company is obliged to ensure compliance. To this end, the Company is committed to:

a. Restricting and monitoring access to sensitive data;
b. Developing transparent data collection procedures;
c. Training employees in online privacy and security measures;
d. Building secure networks to protect online data from cyber-attacks;
e. Establishing clear procedures for reporting privacy breaches or data misuse;
f. Including contract clauses and communicating statements on how the Company handles data;
g. Establishing data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.); and
h. Communicating its data protection provisions on its website.

To the extent possible, the provisions of this Policy shall apply to all information belonging to the Company in whatever form (whether oral, written, pictorial or electronic media) containing, without limitation, material of technical, operational, administrative, economic, planning, business, financial or legal nature and any intellectual property of any kind.

## 2. OBJECTIVES

This Policy is designed to ensure that the Company:

a. Complies with the data protection legislation and follow best practice;
b. Protect the rights of stakeholders and other interested parties, including but not limited to employees, customers and partners;
c. Has in place proper procedures for the safe storage, handling, and lawful processing of individuals' data; and
d. Protects itself from the risk of data breach and data security risks, including:
    i. **Breaches of confidentiality:** Where data is given out inappropriately; and
    ii. **Reputational Damage**: Where the Company could suffer if hackers successfully gained access to sensitive data.

## 3. DATA PROTECTION LEGISLATION

The Data Protection Act, 2012 (Act 843) provides how the Company must collect, handle and store personal information. The Act requires that personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The rules apply regardless of whether the data is stored electronically, on paper or on other materials.

## 4. PERSONAL DATA

Personal Data is defined as information about an individual who can be identified from the data, or from data or other information in the possession of, or likely to come into the possession of the Company. Personal Data relating to identifiable individuals, will include:

a. Names of individuals
b. Postal addresses
c. Email addresses
d. Telephone numbers
e. Any other information relating to individuals

Generally, the Company shall collect Personal Data directly from the data subject. However, the Company may collect Personal Data indirectly where,

a. the data is contained in a public record;
b. the data subject has deliberately made the data public;
c. the data subject has consented to the collection of the information from another source;
d. the collection of the data from another source is not likely to prejudice a legitimate interest of the data subject;
e. the collection of the data from another source is necessary:
    i. for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;
    ii. for the enforcement of a law which imposes a pecuniary penalty;
    iii. for the enforcement of a law which concerns revenue collection;
    iv. for the conduct of proceedings before any court or tribunal that have commenced or are reasonably contemplated;
    v. for the protection of national security; or
    vi. for the protection of the interests of a responsible or third party to whom the information is supplied;
f. compliance would prejudice a lawful purpose for the collection; or
g. compliance is not reasonably practicable.

## 5. DATA PROTECTION PRINCIPLES

The Company collects information in a transparent way and only with the full cooperation and knowledge of the data subject. The Company whilst processing data, shall take into account the privacy of the data subject by applying the following principles:

**a. Accountability:** The Company shall ensure that Personal Data is processed:

i. without infringing the privacy rights of the data subject;
ii. in a lawful manner; and
iii. in a reasonable manner.

Where the data is in respect of foreign data subjects sent into Ghana for processing, the Company shall ensure that the data is processed in compliance with data protection legislation of the country of the data subject. The Company shall not transfer data to organizations or countries that do not have adequate data protection guidelines.

**b. Lawfulness of Processing:** Personal Data must be processed only if the purpose for which it is processed is necessary, relevant and not excessive. The Company shall not process Personal Data without the prior consent of the data subject unless the processing is:

i. necessary for the purpose of the employment, insurance or other contract to which the data subject is a party;
ii. authorised or required by law;
iii. to protect a legitimate interest of the data subject;
iv. necessary for the proper performance of a statutory duty; or
v. necessary to pursue the legitimate interest of the Company or a third party to whom the data is supplied.

Additionally, the Company shall not retain Personal Data for a period longer than is necessary to achieve the purpose for which it is collected and processed.

Personal Data shall only be processed by a third party upon the Company's prior written authorization. The third party shall be obliged to treat the data as confidential. In this vain, the Company shall ensure that Non-Disclosure Agreements are executed or specific confidentiality/ data protection clauses are contained in contracts where third parties will be supplied with data.

**c. Specification of Purpose:** The Company shall collect data for a purpose which is specific, explicitly defined, lawful and related to its business activities. Hence, the data subject must at all times be informed of the purpose for which the data is collected.

**d. Compatibility of further Processing with Purpose of Collection:** The Company shall ensure that any further processing of Personal Data shall be for the original specific purpose for which it was obtained.

**e. Quality of Information:** The Company shall ensure at all times that data is accurate, complete, up-to-date and not misleading having regard to the purpose of collection or processing.

**f. Openness:** The Company shall ensure that the data subject is at all times informed of;

i. the nature of the data being collected;
ii. the name and address of the Company;
iii. the purpose for which the data is required;
iv. whether or not the supply of the data by the data subject is discretionary or mandatory;
v. the consequences of failure to provide the data;
vi. the authorised requirement for the collection of the information or the requirement by law for its collection;
vii. the recipients of the data, if any;
viii. the nature or category of the data; and
ix. the existence of the right of access to and the right to request rectification of the data collected before the collection.

Where data is collected from a third party, the Company shall ensure the data subject is given the information specified above before or as soon as practicable after the collection of the data.

g. **Data Security Safeguards:** The Company shall take necessary steps to secure the integrity of Personal Data in its possession or control through the adoption of appropriate, reasonable, technical and organisational measures to prevent loss of, damage to or unauthorised destruction; an unlawful access to or unauthorised processing of Personal Data.

   Where the Company engages a third party to process Personal Data, the Company shall ensure that the third party establishes and complies with the data protection requirements in this Policy and under law.

   Where the Company has reasonable grounds to believe that the Personal Data has been accessed or acquired by an unauthorised person, the Company shall notify the Data Protection Commission and the data subject as soon as reasonably practicable. The Company shall then take steps to restore the integrity of the information system.

h. **Data Subject Participation:** The Company shall upon request by the data subject and upon proof of identity;
   i. confirm whether or not it holds personal data about that data subject;
   ii. provide details of the personal data it holds, including data about the identity of any third party who has or has had access to the information;
   iii. correct data held on the data subject; and
   iv. modify, erase, reduce or correct data in its custody.

The Company is mandated to notify the data subject of the action taken as a result of the request.

### 5.1 Exception

Personal Data is exempt from the data protection principles if it consists of a reference given in confidence by the Company for the purposes of:

a. education, training or employment of data subject,
b. the appointment to an office of the data subject, or
c. the provision of any service by the data subject.

## 6. SPECIAL PERSONAL DATA

The Company shall not process special personal data unless the processing is necessary and the consent of the data subject has been obtained. Special Personal Data consists of information about an individual that relates to:

i. the race, colour, ethnic or tribal origin;
ii. the political opinion;
iii. the religious beliefs or other beliefs of a similar nature;
iv. the physical, medical, mental health or mental condition or deoxyribonucleic acid (DNA);
v. sexual orientation;
vi. commission or alleged commission of an offence; or

vii. proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in the proceedings.

## 7. RESPONSIBILITIES

Employees and all third parties who deal with the Company have some responsibility for ensuring that data is collected, stored and handled appropriately and must therefore ensure that data is handled and processed in accordance with this Policy.

However, the following persons have key areas of responsibility:

7.1 The **Board of Directors:** shall be ultimately responsible for ensuring that the Company meets its legal obligations as pertains to data protection.

7.2 The **Head, Data Management Unit** shall be responsible for:

a. Keeping the Board of Directors updated about data protection responsibilities, risks and issues;
b. Reviewing all data protection procedures and related issues;
c. Arranging data protection training for Employees and other stakeholders;
d. Addressing data protection concerns from data subjects such as Employees and Customers;
e. Dealing with requests from individuals to inspect the data the Company holds about them; and
f. Actively participating in reviewing and approving contracts or agreements with third parties that may handle the Company's sensitive data.

7.3 The **Head, MIS** shall be responsible for:

a. Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
b. Performing regular checks and scans to ensure security hardware and software is functioning properly;
c. Implementing appropriate remedial measures to restore the integrity of data which is lost, corrupted or compromised; and
d. Evaluating any third party services which the Company intends to use for data storage or processing.

7.4 The **Head, Marketing** shall be responsible for:

a. Approving any data protection statements attached to communications such as emails, advertisements, publications and letters;
b. Addressing any data protection queries from journalists or media outlets upon the prior approval of the Executive Management; and
c. Where necessary working with other Employees to ensure marketing initiatives comply with data protection principles.

## 8. GENERAL GUIDELINES

8.1 The Company shall;

i. Grant access to data covered under this Policy only on a “need to know” basis to enable Employees perform their work;
ii. Provide training to all Employees to help them understand their responsibilities when handling data;

iii. Ensure Employees keep all data secure, by taking precautions and following the guidelines contained in this Policy and such other guidelines pertaining to data handling that may be issued from time to time;

iv. Use strong and encrypted passwords to secure data. Employees must never share Passwords;

v. Ensure that Personal Data is not disclosed to unauthorised persons, either within or outside the Company;

vi. Ensure that Personal Data is regularly reviewed and updated and if found to be out of date and no longer required, deleted and disposed of

8.2 The Company shall not share data informally. When access to confidential information is required, Employees, customers and other third parties shall request from the appropriate authority in writing.

8.3 Employees must request assistance from the Head, MIS or Head, Data Management if they are unsure about any aspect of data protection.

## 9. DATA STORAGE

These rules describe how and where data should be safely stored. Responsibility for, and questions about data storage should be directed to the Head, MIS or the Head, Data Management Unit.

### 9.1 Data Stored on Paper

When data is stored on paper, it must be stored in a secure place where unauthorised persons cannot access. Among others:

a. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
b. Employees must make sure paper and print outs are not left where unauthorised persons can see them, for instance on a printer.
c. Data print outs should be shredded and disposed of securely when no longer required.

These guidelines apply to data that is usually stored electronically but has been printed for one reason or the other.

### 9.2 Electronically Stored Data

When data is stored electronically, it shall be protected from unauthorised access, accidental deletion and malicious hacking attempts. Among others,

a. Data shall be protected by strong passwords that are changed regularly and never shared between Employees.
b. If data is stored on removable media (like CD, DVD, External Drive, etc.), these shall be kept locked away securely when not in use.
c. Data shall only be stored on designated drives and servers, and shall only be uploaded to approve cloud computing services.
d. Servers containing Personal Data shall be sited in a secure location away from the general office space.
e. Data shall be backed up frequently and tested regularly, in line with the Company's standard backup procedures.
f. Data shall not be saved directly to mobile devices such as tablets or smartphones.
g. All servers and computers containing data shall be protected by approved security software and firewalls.

## 10. DATA USE

Personal Data is of no value to the Company unless the Company can make use of it. However, it is when Personal Data is assessed and used that it can be at the greater risk of loss, corruption or theft.

When working with Personal Data, Employees shall ensure the screens of their computers are always locked when unattended. Also, Personal data shall not be shared informally and must be encrypted before being transferred electronically outside the Company.

## 11. DATA ACCURACY

The law requires the Company to take reasonable steps to ensure data is kept accurate and up-to-date. The Company shall therefore put in place appropriate measures to ensure that data is accurate at all times. It is the responsibility of all Employees to take reasonable steps to ensure that data is kept as accurate and up-to-date as possible.

Data should be held in as few places as necessary. Employees shall not create any unnecessary additional data sets. Further, Employees shall take every opportunity to ensure that data is updated. For instance, by confirming a Customer's details when they call or visit the office.

The Company shall also make it easy for data subjects to update the information which the Company holds about them. Data shall be updated as inaccuracies are discovered.

## 12. DISCLOSURE WITHOUT DATA SUBJECT'S CONSENT

The Company shall disclose Personal Data to law enforcement agencies without the consent of the data subject upon satisfaction that the request is legitimate and upon prior approval of Executive Management and/ or the Board, if necessary.

## 13. PROCESSING PERSONAL DATA FOR DIRECT MARKETING

The Company shall not provide, use, obtain, procure or provide information related to a data subjects for the purposes of direct marketing without the prior written consent of the data subject. Direct marketing includes communication by whatever means of advertising or marketing material which is directed to particular individuals.

The Company shall comply with all written notices from a data subject precluding the Company from processing his/her Personal Data for the purposes of direct marketing.

## 14. REGISTRATION AS DATA CONTROLLER

The Company shall register, and keep renewed its registration with the Data Protection Commission.

## 15. RECORDS RETENTION

The Company through the MIS Department shall keep the records of the Company for a period not less than 6 years from the date of the last transaction or correspondence with a data subject.

## 16. CONSEQUENCES OF NON-COMPLIANCE

The principles contained in this Policy shall be strictly complied with. Any breach of this Policy shall result in the following:

a. In the case of an Employee or Director, disciplinary action resulting in termination of employment or appointment and or legal action for damages; and

b. In any other case, termination of contract, legal action for breach of contract, if any and damages and regulatory redress where the third party is registered with the Data Protection Commission.

## 17. DISPOSAL OF COMPUTER HARDWARE

Staff of M.I.S department have to access computer equipment on a yearly basis and advise management on the need to dispose them primarily because:

a. They are no longer in working order and repair is not a feasible or available option.

b. The computer is inadequate to serve the purpose required, usually because it is old and has become under-equipped to function with the upgraded software and increased processing demands.

c. The department has found itself with a surplus of computers, possibly due to its replacement policy or strategy.

**Methods of disposal**

1. Where the computer is in working order but inadequate for the designated purpose, it is expected that as far as is practicable the first consideration will be for internal re-assignment.

2. Thus it will be assigned to other departmental functions for which the capacity is appropriate.

3. Secondly, reasonable effort must be made to see if there is any other department that may wish to make use of the equipment.

4. Equipment with residual value but which are inadequate for the business of the Company may be sold to members of the department or outside bodies, subject to the Company's financial guidelines.

5. Where equipment has little resale value, consideration should be given to donating it to a charitable endeavour.

6. 5. If the equipment cannot be used, it should be scrapped for parts or disposed of in accordance with the Company's policy and procedures for disposal.

7. All movement of equipment must be recorded in the Asset Register record, which indicates the information to be recorded over the disposal process.

## 18. REVIEW

This Policy shall be reviewed as and when it becomes necessary but not less than once in every two (2) years to ensure that it is current and relevant. All Employees and Directors will be provided with the most recent version.

Additionally, the Head of Compliance shall deliver the amended Data Protection Policy to all other stakeholders indicating which section(s) have been amended

## APPENDIX: DOCUMENT INFORMATION

| | |
|---|---|
| Document Name: | Data Protection Policy |
| Version | 1.0 |
| Prepared By: | Legal & Compliance –June, 2017<br>Data Management Unit |
| Reviewed By: | Executive Management –28th June, 2017 |
| Approved by: | Board ICT & Innovation Committee- 16th October, 2017 |
| Approved by: | Board of Directors- 20th December, 2017 |