
New Sudan Insurance Co. Ltd

Data Protection Policy

January 2025



Content

1.	Introduction	Page 3
2.	Data Protection Principles	Page 3
3.	Lawful Processing	Page 3
4.	Data Minimization and Control	Page 4
5.	Accountability	Page 4
6.	Use of Processors	Page 5
7.	Company Measures	Page 5
8.	Role of the Data Protection Officer	Page 6
9.	Procedures for Staff	Page 6
10.	Rights of Data Subjects	Page 7
11.	Reporting of Breaches	Page 8



Introduction

New Sudan Insurance Company Ltd (NESICO) a corporation organized under the laws of the New Sudan Company Act 2012 duly organized to transact business in the Republic of South Sudan

The security and management of data is important to ensure that we can function effectively and successfully for the benefit of our staffs and clients.

In doing so, it is essential that client's privacy is protected through the lawful and appropriate use and handling of their personal information.

The use of all personal data by NESICO is governed by:

- The Transitional Constitution of the Republic of South Sudan

Every member of staff has a responsibility to adhere to this Data Protection Policy.

1. DATA PROTECTION PRINCIPLES

These require that all personal data be:

- processed in a **lawful, fair** and **transparent** manner.
- collected only for **specific, explicit** and **limited** purposes ('purpose limitation').
- **adequate, relevant** and **not excessive** ('data minimization').
- **accurate** and kept **up-to-date** where necessary.
- kept for **no longer than necessary** ('retention').
- The Data Processing Register will be reviewed at least every 12 months by the handler with the involvement of the Management
- handled with appropriate **security** and **confidentiality**.

We are committed to upholding the Data Protection Principles. All personal data under our control must be processed in accordance with these principles.

2. LAWFUL PROCESSING

1. All processing of personal data must meet one of the six lawful bases defined below:
 - Where we have the **consent** of the data subject
 - Where it is in our **legitimate interests** and this is not overridden by the rights and freedoms of the data subject.
 - Where necessary to meet a **legal obligation**.
 - Where necessary to fulfil a **contract**, or pre-contractual obligations.



NEW SUDAN INSURANCE COMPANY LTD.

Nimra Talata, Block 1, PO Box 260, Juba, South Sudan

Tel: 0925 955 000, 0919 123 678, 0925 478 766

Email: nesi@nesico.com

- Where we are protecting someone's **vital interests**.
 - Where we are fulfilling a **public task**, or acting under official authority.
2. Where processing is based on consent, the data subject has the option to easily withdraw their consent.
 3. Where electronic direct marketing communications are being sent, the recipient should have the option to opt-out in each communication sent, and this choice should be recognized and adhered to by us.

3. DATA MINIMISATION AND CONTROL

1. Data collection processes will be regularly reviewed by the Management to ensure that personal data collected and processed is kept to a minimum.
2. We will keep the personal data that we collect, use and share to the minimum amount required to be adequate for its purpose.
3. Where we do not have a legal obligation to retain some personal data, we will consider whether there is a business need to hold it.
4. We will retain personal data only for as long as it is necessary to meet its purpose. Our approach to retaining and erasing data no longer required will be specified in the retention policy and schedule. This schedule will be reviewed annually.
5. In the case of sharing personal data with any third party, only the data that is necessary to fulfil the purpose of sharing will be disclosed.
6. Anonymization and Pseudonymisation of personal data stored or transferred should be considered where doing so is a possibility.

4. ACCOUNTABILITY

1. NESICO will maintain a Data Processing Register as maybe required by relevant laws to document regular processing activities.
2. The 'Data Protection Officer' (DPO) has the specific responsibility of overseeing data protection and ensuring that we comply with the data protection principles and relevant legislation.
3. The DPO will ensure that the Data Processing Register is kept up to date and demonstrates how the data protection principles are adhered to by our activities. Individual members of staff have a



NEW SUDAN INSURANCE COMPANY LTD.

Nimra Talata, Block 1, PO Box 260, Juba, South Sudan

Tel: 0925 955 000, 0919 123 678, 0925 478 766

Email: nesi@nesico.com

duty to contribute to ensure that the measures outlined in the Register are accurately reflected in our practice.

4. The Management monitors our compliance with relevant policies and regulatory requirements in respect of data protection as part of our Data Management Strategy.
5. All employees, services providers, Brokers and agents who will be handling personal data on behalf of NESICO will be appropriately trained and supervised where necessary.
6. The collection, storage, use and sharing of personal data will be regularly reviewed by the Data Protection Officer, the Management.
7. We will adhere to relevant codes of conduct where they have been identified and discussed as appropriate.

5. USE OF PROCESSORS

1. NESICO must only appoint processors who can provide sufficient guarantees around compliance with the relevant laws and that the rights of data subjects will be protected.
2. Where a processor can demonstrate that they adhere to approved codes of conduct or certification schemes, this should be taken into consideration for choice of supplier.
3. Where NESICO uses a processor, a written contract must be in place (plus any additional requirements that we determine). Processors can only act on the instruction of NESICO.

6. COMPANY MEASURES

1. All devices owned by NESICO will have hardware encryption set up by default where possible, including laptops, mobile devices and removable media.
2. All staffs, Service Providers, Brokers, Agents, Surveyors, Loss Adjustors or anyone else working on behalf of NESICO and handling personal data are bound by the data this Policy.
3. Where any Services Providers, Brokers, Agents, Surveyor, Loss Adjustors, or anyone else working on behalf of NESICO fails in their obligations under this Policy, they shall indemnify NESICO against any cost, liabilities, damages, loss, claims or proceedings that may arise from that failure.

7. ROLE OF THE DATA PROTECTION OFFICER

1. The Data Protection Officer role is assigned to a member of staff on



NEW SUDAN INSURANCE COMPANY LTD.

Nimra Talata, Block 1, PO Box 260, Juba, South Sudan

Tel: 0925 955 000, 0919 123 678, 0925 478 766

Email: nesi@nesico.com

a voluntary basis i.e. we are not legally obliged to have a DPO. We have chosen to do so as part of demonstrating our accountability and ensuring our compliance with data protection requirements.

2. The DPO assists NESICO to:
 - monitor our internal compliance
 - inform and advise on our data protection obligations
 - provide advice regarding Data Protection Impact Assessments
 - act as a contact point for data subjects and the any Regulatory Authority.
3. The DPO advises the Management and reports to Senior Management and to NESICO's Board of Directors on data protection matters.
4. The DPO is easily accessible as a point of contact for staff for data protection issues and is identified as the point of contact in our privacy notice and other external material.
5. The DPO identifies, organizes and delivers training for staff and meets with new staff during their induction to discuss data protection matters, including this policy.
6. The DPO is required to have appropriate knowledge of data protection law and best practice, and is provided with adequate resources to help them carry out their role. This might include appropriate training and accreditation where identified.
7. The DPO is nominally responsible for carrying out responses to requests made by data subjects, reporting breaches and drawing up policies and procedures.
8. This does not preclude another responsible member of staff for carrying out these duties.

8. PROCEDURES FOR STAFF

While this policy helps us to demonstrate how we seek to comply with data protection legislation and be accountable for our actions,

All members of staff must comply with these procedures for processing or transmitting personal data. In addition, staff should be aware of and adhere to policies around the Acceptable Usage of ICT Systems, and any other guidance issued in relation to cyber security and the use of personal data.

- Always treat people's personal information with integrity and confidentiality. Don't hand out personal details just because someone asks you to.



NEW SUDAN INSURANCE COMPANY LTD.

Nimra Talata, Block 1, PO Box 260, Juba, South Sudan

Tel: 0925 955 000, 0919 123 678, 0925 478 766

Email: nesi@nesico.com

- Where personal data exists as hard copy, it should be stored in a locked box, drawer or cabinet, and not left where anyone could access it.
- The transfer of hard copies should be passed directly to the recipient.
- Staff are issued with encrypted USB devices for the secure transfer of personal data or sensitive information. No other removable media devices should be used to transfer these types of information without permission from the Systems Administrator or Head of Information Management.
- The loss or theft of any device should be reported as soon as possible to the DPO, Systems Administrator or Head of Information Management.
- Take care when connecting to public wi-fi connections, as these can expose your connection to interception. If you're not sure if a connection is secure, do not connect to it.
- If you are thinking of sending marketing to individuals, consult with the DPO first, as there are certain laws that apply to electronic direct marketing. This could include anything that promotes the aims or purpose of NESICO, including promoting an event or seeking engagement.
- Take care to email the intended recipient (especially where email address autocomplete is turned on). Use the 'bcc' field for emailing several people where using 'to' or 'cc' is not needed.
- If you are using your own device to access personal data on Office365 (e.g. Outlook), ensure that your device has a firewall and is password protected.
- If you do have a question or are unsure about any of these procedures, contact the Data Protection Officer or Head of IT.

9. RIGHTS OF DATA SUBJECTS

1. Under data protection laws, data subjects have certain rights:
 - **Right to be informed.** The right to be told how their personal data is used in clear and transparent language.
 - **Right of access.** The right to know and have access to the personal data we hold about them.
 - **Right to data portability.** The right to receive their data in a common and machine-readable electronic format.
 - **Right to be forgotten.** The right to have their personal data erased.
 - **Right to rectification.** The right to have their personal



NEW SUDAN INSURANCE COMPANY LTD.

Nimra Talata, Block 1, PO Box 260, Juba, South Sudan

Tel: 0925 955 000, 0919 123 678, 0925 478 766

Email: nesi@nesico.com

data corrected where it is inaccurate or incomplete.

- **Right to object.** The right to complain and to object to processing.
 - **Right to purpose limitation.** The right to limit the extent of the processing of their personal data.
 - **Rights related to automated decision-making and profiling.** The right not to be subject to decisions without human involvement.
2. We will uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Privacy information will acknowledge these rights and explain how individuals can exercise them. Most rights are not absolute, and the individual will be able to exercise them depending on the circumstances, and exemptions may apply in some cases.
 3. Any request in respect of these rights should preferably be made in writing to nesi@nesico.com, but we will also accept verbal requests.
 4. Requests that are 'manifestly unfounded or excessive' can be refused.
 5. We will take reasonable measures to require individuals to prove their identity where it is not obvious that they are the data subject.
 6. We will respond to the request within one **week** from the date of request or being able to identify the person, unless it is particularly complex (in which case we will respond in no longer than 30 days).
 7. The DPO will ensure that required actions are taken and that the appropriate response is facilitated within the deadline.
 8. The DPO will draw up procedures for responding to requests where necessary, for example, for facilitating Subject Access Requests.

10. REPORTING OF BREACHES

1. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
2. All members of staff should be vigilant and able to identify a suspected personal data breach. A breach could include:
 - loss or theft of devices or data, including information stored on USB drives or on paper
 - hacking or other forms of unauthorized access to a device, email account, or the network
 - disclosing personal data to the wrong person, through



NEW SUDAN INSURANCE COMPANY LTD.

Nimra Talata, Block 1, PO Box 260, Juba, South Sudan

Tel: 0925 955 000, 0919 123 678, 0925 478 766

Email: nesi@nesico.com

wrongly addressed emails, or bulk emails that inappropriately reveal all recipients email addresses

- alteration or destruction of personal data without permission
3. Where a member of staff discovers or suspects a personal data breach, this should be reported to the DPO as soon as possible.
 4. Where there is a likely risk to individuals' rights and freedoms, the DPO will report the personal data breach to the Managing Director within 24 hours of knowledge of the breach.
 5. Where there is also a likely high risk to individuals' rights and freedoms, NESICO will inform those individuals without undue delay.
 6. The DPO will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.