One Risk Africa (PTY) Ltd

Data Protection and Protection of Personal Data Policy

Contents

1. INTRODUCTION

Contemporary communication channels such as the Internet, intranets and email play an essential part in accessing and exchanging information. This allows for faster and more effective communication than in the past.

One Risk Africa (Pty) Ltd strives to protect the personal rights of any individual/group whose personal data it processes – including its employees, customers, suppliers and other contractual partners or interested persons.

In this context, *One Risk Africa (Pty) Ltd* has drafted and accepted the following principles that relates to data protection and personal data privacy to ensure compliance with the Protection of Personal Information Act No. 4 of 2013.

2. OBJECTIVES

These principles have the objective of defining security standards for processing, storing and transferring personal data within *One Risk Africa (Pty) Ltd* in order to ensure adequate protection of personal rights of the affected data subjects.

3. SCOPE

These principles govern all data privacy isues. It applies to the processing of the personal data of any individual/group whose personal data are processed within *One Risk Africa (Pty) Ltd,* including employees, customers, suppliers, other contractual partners, interested persons and other parties.

4. DEFINITIONS

Consent is any freely given, informed declaration by the data subject that he/she accepts the processing of his/her personal data.

Data protection/privacy is the sum of all actions taken to protect the personal rights of data subjects when handling their personal data.

Data subjects are all individuals/groups whose personal data are processed within *One Risk Africa (Pty) Ltd,* including current, future and former employees, customers, suppliers and other contractual partners or interested persons.

Information Officer is the person officially named to monitor internal data protection. He/she reports to the management of *One Risk Africa (Pty) Ltd.*

Personal data are any information relating to an identified or identifiable individual/group. An individual/group is identifiable if he/she/it can be directly or indirectly identified.

Processing of personal data is any operation performed in respect of personal data – such as collection, receipt, recording, storage, updating, modification, alteration, retrieval, use, transmission or deletion. This definition will also apply to the word “processed” when used in this context.

Transfer of personal data is the forwarding of personal data, its distribution or all other forms of transfer to third parties. This definition also applies to the words "transferred" and "transferring" when used in this context.

5. GENERAL PRINCIPLES FOR PROCESSING PERSONAL DATA

5.1 Permissibility of Data Processing

The processing of personal data is permitted only if the data subject has consented thereto.

Consent shall be declared whereby the data subject must be informed in advance about the purpose of such processing of personal data and the possible transfer of personal data to third parties. The declaration of consent must be highlighted when included as part of other statements so as to be clear to the data subject.

5.2 Intended Purpose

Personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed contrary to such intended purpose.

5.3 Further Processing of Data

Data transferred from one division within *One Risk Africa (Pty) Ltd* to another division is in accordance with the purpose for which the data was collected and is considered as further processing and storing of this data.

5.4 Data Quality

Personal data must be factually correct and, as far as necessary, up-to-date. Appropriate and reasonable measures should be undertaken to correct or delete incorrect or incomplete data.

5.5 Confidentiality of Data Processing

Only authorised staff is allowed to be involved in the processing of personal data. It is prohibited for them to use such data for their own private purposes or to make it accessible to any unauthorised entity. Unauthorised in this context also means the use of personal data by employees who do not need access to such data to fulfil their employment duties.

5.6 Data Security

One Risk Africa (Pty) Ltd shall implement appropriate technical and organisational measures to ensure the necessary data security. These measures refer in particular to computers (servers), networks and communication links, and applications; they are embedded in the IT security management system of *One Risk Africa (Pty) Ltd.*

One Risk Africa (Pty) Ltd network administration seeks to promote a level of security and privacy. Thus users should be aware that the data they create on the corporate system remain the property of *One Risk Africa (Pty) Ltd*. All work-related documents must be saved in the "user personal drive" folder that is linked to the network server in order to ensure that the content is part of the backup procedure that runs every evening. For security and network maintenance purposes, authorised individuals (IT technicians) within *One Risk Africa (Pty) Ltd* will monitor equipment, systems and network traffic at any time.

5.7 Computer Equipment

All email facilities are provided for business purposes only. All user activity on the Intranet and internet is subject to logging codes.

Laptops, tablets and mobile phones are the main repositories of information and every reasonable precaution must be taken to prevent their unauthorised use.

All computer equipment is the property of *One Risk Africa (Pty) Ltd* and is password protected. It is recommended that passwords are changed on a monthly basis. Passwords are not to be communicated to anybody, for whatever reason.

If one of the above devices are stolen or lost, it is automatically assumed that the device has been compromised. The IT Department needs to be informed to be able to disable any access to the system. Within 24 hours, a report must be submitted to the Chief Operating Officer describing the stolen equipment, the circumstances of it being stolen and the precautions that had or had not been taken. In the case of a mobile phone, the service provider needs to be informed to be able to disable the "SIM" card and blacklist the phone to prevent any further use.

6. RIGHTS OF THE DATA SUBJECT

6.1 Information Right

Each data subject, with adequate proof of identity, has the right to demand information about the type of personal data concerning him/her/it that is processed by *One Risk Africa (Pty) Ltd*. This information should be provided to the data subject. The data subject may address any such application for information to the office or dedicated Information Officer.

6.2 Correction Claim

If the stored personal data are incorrect or incomplete, the data subject may require correction. Data subjects are responsible for providing only correct personal data to *One Risk Africa (Pty) Ltd*. In addition, data subjects shall inform *One Risk Africa (Pty) Ltd* of any relevant changes (e.g. changes of address or name).

7. PROCEDURAL RULES

7.1 Implementation within *One Risk Acceptances (Pty) Ltd*

The managers of the different divisions within *One Risk Africa (Pty) Ltd* are responsible to ensure that this Policy is implemented, which includes in particular providing information to the employees in their division. Should additional training be required, the Information Officer and/or Training Officer should be approached.

7.2 Information Officer

An Information Officer will be appointed to monitor compliance with this Policy. The appointed Information Officer is Rudo van Niekerk, within the Compliance Department.

7.3 Questions and Complaints/Remedies

Data subjects may contact the Information Officer with any questions and complaints regarding the processing of personal data at telephone number +27 (0) 11 706 4331 or alternatively rudo@oneriskafrica.co.za. Such questions and complaints will be treated confidentially.