RISCURA

Protection of Personal Information Policy

8 February 2021

More information?

Nevashnee Naidoo | 021 673 6999 | nnaidoo@riscura.com

riscura.com

Contents

1. INTRODUCTION

1.1 The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

1.2 POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

1.3 Through the provision of service, the Company is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

1.4 A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

1.5 Given the importance of privacy, the company is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

2.1 Personal Information

2.1.1 Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

2.1.1.1 race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;

2.1.1.2 information relating to the education or the medical, financial, criminal or employment history of the person;

2.1.1.3 any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.1.1.4 the biometric information of the person;

2.1.1.5 the personal opinions, views or preferences of the person;

2.1.1.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

2.1.1.7 the views or opinions of another individual about the person;

2.1.1.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.2 Data Subject

2.2.1 This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the Company with products or other goods.

2.3 Responsible Party

2.3.1 The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the Company is the responsible party.

2.4 Operator

2.4.1 An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For

example, a third-party service provider that has contracted with the Company to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.5 Information Officer

2.5.1 The Information Officer is responsible for ensuring the Company's compliance with POPIA.

2.5.2 Where no Information Officer is appointed, the head of the Company will be responsible for performing the Information Officer's duties.

2.5.3 Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.6 Processing

2.6.1 The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

2.6.2 the collection, receipt, recording, Company, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.6.3 dissemination by means of transmission, distribution or making available in any other form; or

2.6.4 merging, linking, as well as any restriction, degradation, erasure or destruction of information.

2.7 Record

2.7.1 Means any recorded information, regardless of form or medium, including:

2.7.1.1 Writing on any material;

2.7.1.2 Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

2.7.1.3 Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.7.1.4 Book, map, plan, graph or drawing;

2.7.1.5 Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.8 Filing System

2.8.1 Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.9 Unique Identifier

2.9.1 Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.10 De-Identify

2.10.1 This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.11 Re-Identify

2.11.1 In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.12 Consent

2.12.1 Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

2.13 Direct Marketing

2.13.1 Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

2.13.2 Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

2.13.3 Requesting the data subject to make a donation of any kind for any reason.

2.14 Biometrics

2.14.1 Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

3. POLICY PURPOSE

3.1 The purpose of this policy is to protect the Company from the compliance risks associated with the protection of personal information which includes:

3.1.1 Breaches of confidentiality. For instance, the Company could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.

3.1.2 Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the Company uses information relating to them.

3.1.3 Reputational damage. For instance, the Company could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the Company.

3.2 This policy demonstrates the Company's commitment to protecting the privacy rights of data subjects in the following manner:

3.2.1 Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.

3.2.2 By cultivating a culture that recognises privacy as a valuable human right.

3.2.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

3.2.4 By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the Company.

3.2.5 By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the Company and data subjects.

3.2.6 By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

4.1 This policy and its guiding principles apply to:

4.1.1 The Company's directors

4.1.2 All branches, business units and divisions of the Company

4.1.3 All employees and volunteers

4.1.4 All contractors, suppliers and other persons acting on behalf of the Company

4.1.5 The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the Company's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

4.2 POPIA does not apply in situations where the processing of personal information:

4.2.1 is concluded in the course of purely personal or household activities, or

4.2.2 where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

Where appropriate, the Company will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects.

The Company will ensure that it gives effect to the following seven rights.

5.1 The Right to Access Personal Information

5.1.1 The Company recognises that a data subject has the right to establish whether the Company holds personal information related to him, her or it including the right to request access to that personal information.

5.1.2 An example of a "Personal Information Request Form" can be found in the POPI Procedure document.

5.2 The Right to have Personal Information Corrected or Deleted

5.2.1 The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the Company is no longer authorised to retain the personal information.

5.3 The Right to Object to the Processing of Personal Information

5.3.1 The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

5.3.2 In such circumstances, the Company will give due consideration to the request and the requirements of POPIA. The Company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.4 The Right to Object to Direct Marketing

5.4.1 The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.5 The Right to Complain to the Information Regulator

5.5.1 The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

5.5.2 An example of a "POPI Complaint Form" can be found In the POPI Procedure document

5.6 The Right to be Informed

5.6.1 The data subject has the right to be notified that his, her or its personal information is being collected by the Company.

5.6.2 The data subject also has the right to be notified in any situation where the Company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the Company will always be subject to, and act in accordance with, the following guiding principles:

6.1 Accountability

6.1.1 Failing to comply with POPIA could potentially damage the Company's reputation or expose the Company to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.

6.1.2 The Company will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Company will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

6.2 Processing Limitation

6.2.1 The Company will ensure that personal information under its control is processed:

6.2.1.1 in a fair, lawful and non-excessive manner, and

6.2.1.2 only with the informed consent of the data subject, and

6.2.1.3 only for a specifically defined purpose.

6.2.2 The Company will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.

6.2.3 Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the Company will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.

6.2.4 The Company will under no circumstances distribute or share personal information between separate legal entities, associated Company's (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

6.2.5 Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the Company's business and be provided with the reasons for doing so.

6.2.6 An example of a "POPI Notice and Consent Form" can be found in the POPI Procedure document.

6.3 Purpose Specification

6.3.1 All of the Company's business units and operations must be informed by the principle of transparency.

6.3.2 The Company will process personal information only for specific, explicitly defined and legitimate reasons. The Company will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

6.4 Further Processing Limitation

6.4.1 Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

6.4.2 Therefore, where the Company seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the Company will first obtain additional consent from the data subject.

6.5 Information Quality

6.5.1 The Company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.

6.5.2 The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the Company will put into ensuring its accuracy.

6.5.3 Where personal information is collected or received from third parties, the Company will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

6.6 Open Communication

6.6.1 The Company will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.

6.6.2 The Company will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:

6.6.2.1 Enquire whether the Company holds related personal information, or

6.6.2.2 Request access to related personal information, or

6.6.2.3 Request the Company to update or correct related personal information, or

6.6.2.4 Make a complaint concerning the processing of personal information.

6.7 Security Safeguards

6.7.1 The Company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

6.7.2 Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.

6.7.3 The Company will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company's IT network.

6.7.4 The Company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

6.7.5 All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the Company is responsible.

6.7.6 All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.

6.7.7 The Company's operators and third-party service providers will be required to enter into service level agreements with the Company where both parties pledge their mutual

commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.

6.7.8 An example of "Employee Consent and Confidentiality Clause" for inclusion in the Company's employment contracts can be found in the POPI Procedure document.

6.7.9 An example of an "SLA Confidentiality Clause" for inclusion in the Company's service level agreements can be found in the POPI Procedure document

6.8 Data Subject Participation

6.8.1 A data subject may request the correction or deletion of his, her or its personal information held by the Company.

6.8.2 The Company will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.

6.8.3 Where applicable, the Company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. INFORMATION OFFICERS

7.1 The Company will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

7.2 The Company's Information Officer is responsible for ensuring compliance with POPIA.

7.3 There are no legal requirements under POPIA for a Company to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger companies.

7.4 Where no Information Officer is appointed, the head of the Company will assume the role of the Information Officer.

7.5 Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.

7.6 Once appointed, the Company will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

7.7 An example of an "Information Officer Appointment Letter" can be found in the POPI Procedure document.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1 Governing Body

8.2 Information Officer

8.3 IT Service Provider

8.4 Marketing & Communication Manager

8.5 Employees and other Persons acting on behalf of the Company

Please refer to the POPI Procedure document for more detailed information.

9. POPI AUDIT

9.1 The Company's Information Officer will schedule periodic POPI Audits.

Please refer to the POPI procedure document for more information.

10. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

10.1 Data subjects have the right to:

10.1.1 Request what personal information the Company holds about them and why.

10.1.2 Request access to their personal information.

10.1.3 Be informed how to keep their personal information up to date.

10.2 Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form".

10.3 Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the Company's PAIA Policy.

10.4 The Information Officer will process all requests within a reasonable time.

11. POPI COMPLAINTS PROCEDURE

11.1 Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The Company takes all complaints very seriously and will address all POPI related complaints in accordance with the procedure set out in the POPI Procedure document.:

12. DISCIPLINARY ACTION

12.1 Where a POPI complaint or a POPI infringement investigation has been finalised, the Company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

12.2 In the case of ignorance or minor negligence, the Company will undertake to provide further awareness training to the employee.

12.3 Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the Company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

12.3.1 Examples of immediate actions that may be taken subsequent to an investigation include:

12.3.2 A recommendation to commence with disciplinary action.

12.3.3 A referral to appropriate law enforcement agencies for criminal investigation.

12.3.4 Recovery of funds and assets in order to limit any prejudice or damages caused.