RERIS®
INSURANCE BROKERS
AUTHORISED FSP

Tel. (+27) 015-516-1599
(+27) 015-962-0022
admin@reris.info

Office No 4-33 Songozwi Street
Louis Trichardt 0920
www.reris.info

PROTECTION OF PERSONAL INFORMATION POLICY

FOR

RERIS INSURANCE BROKERS ("RERIS")

PROTECTION OF PERSONAL INFORMATION POLICY

1. Introduction

1.1. Reris Insurance Brokers ("Reris") an authorised financial services provider.

1.2. The Protection of Personal information Act, 4 of 2013 ("the POPI Act"), has eight conditions that require that personal information (PI) of both individuals and juristic entities is sufficiently protected and also used in a manner that facilitates transparency around the following:

1.2.1 **What** is done with the personal information;

1.2.2 **Why** and **how** it is processed (i.e. this covers all phases of a typical information management lifecycle – from collection, to usage, sharing, disposal, archiving, etc.);

1.2.3 **Who** the personal information is shared with (i.e. third parties – both localy and internationally, other legal entities – sometimes within the same group or company, etc.); and

1.2.4 **What types** of personal information is processed and for what purpose.

1.3. With the enactment of the POPI Act, RERIS is required to bring all of its policies and procedures in line with the letter, spirit and relevance of the POPI Act in order to:

1.3.1. Promote the protection of personal information of our data subjects;

1.3.2. Introduce certain conditions establishing minimum requirements for the processing of personal information;

1.3.3. Provide for the rights of persons regarding unsolicited electronic communications and automated decision making; and

1.3.4. Regulate the flow of personal information within our Group of Companies and across the borders of the Republic.

1.4. The POPI Act requires RERIS to ensure that all personal information collected and processed is protected from various unauthorised access and criminal activity such as fraud, identity theft, unauthorised advertising, unauthorised distribution, etc.

1.5. This POPI Act applies to the processing of personal information:

1.5.1. Entered in a record by or for a responsible party by making use of automated or non- automated means; and

1.5.2. Where RERIS is:

1.5.2.1. Domiciled in the Republic; or

1.5.2.2. Not domiciled in the Republic but makes use of automated or non-automated means in the Republic.

2. Policy objectives

2.1. This policy aims to give effect to give to the eight information protection principles:

2.1.1. Accountability – RERIS must ensure that the principles of the POPI Act are complied with. This includes assigning of responsibility to an individual or function to provide oversight on compliance with the principles of the policy.

2.1.2. Processing Information – RERIS must process information in a fair and lawful manner, with the consent of persons or unless otherwise authorised by legislation.

3. Definitions

3.1. **Data subject** means a customer, employee and/or contractor whose personal information is collected and processed by RERIS.

3.2. **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;

3.3. **Personal information** means information relating to an identifiable, living, natural person and a company, including, but not limited to:

3.3.1. Information relating to the race, gender, sex, pregnancy, marital Status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

3.3.2. Information relating to the education or the medical, financial, criminal or employment history of the person;

3.3.3. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

3.3.4. The biometric information of the person;

3.3.5. The personal opinions, views or preferences of the person;

3.3.6. 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;

3.3.7. The views or opinions of another individual about the person; and

3.3.8. 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.

3.4. **Processing** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: -

3.4.1. The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

3.4.2. Dissemination by means of transmission, distribution or making available in any other form; or

3.4.3. Merging, linking, as well as restriction, degradation, erasure or destruction of information.

3.5. **Special personal information** means-

3.5.1. The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

3.5.2. The criminal behaviour of a data subject if that information relates to –

3.5.2.1. The alleged commission by a data subject of any offence; or

3.5.2.2. Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3.6. **Responsible party** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

4. Exclusions

4.1. This policy does not apply to the processing of personal information that has been de-identified to the extent that it cannot be re-identified again.

4.2. De-identified information is information that should not be capable of being:

4.2.1. Used or manipulated by a reasonably foreseeable method to identify the data subject; or

4.2.2. Linked by a reasonably foreseeable method to other information that identifies the data subject.

5. Data subjects' rights

5.1. A data subject has the following rights:

5.1.1. The right to be informed that:

5.1.1.1. Personal information is being collected; and

5.1.1.2. Personal information has been accessed or obtained by an unauthorised person;

5.1.2. The right to enquire whether RERIS holds personal information and to request access to that information as provided for in terms of paragraph 12.1 of this policy;

5.1.3. The right to request the correction, destruction or deletion of personal information as provided for in terms of paragraph 12.1. of this policy;

5.1.4. A data subject may object at any time, to the processing of personal information:

5.1.4.1. If the reason for such processing is in terms of paragraphs 6.2.1.4, 6.2.1.5 and 6.2.1.6 of this policy, on reasonable grounds relating to his or her particular situation, unless legislation provides for such processing; or

5.1.4.2. For purposes of direct marketing by means of unsolicited electronic communications and related policies in subsidiaries;

5.1.4.3. Once the data subject has objected in writing to the processing of personal information, RERIS may no longer process the personal information.

5.1.5. The right not to be subject to a decision which is based solely on the basis of the automated processing of personal information intended to result in legal consequences for the data subject, (for example, sending a bulk SMS requiring confirmation from our customers);

5.1.6. The right to submit a complaint to the Regulator regarding the alleged interference with the protection of personal information;

5.1.7. The right to institute civil proceedings regarding the alleged interference with the protection of personal information; and

5.1.8. The right to withdraw consent. The data subject may withdraw his, her consent, at any time, provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information will not be affected.

6. Processing limitations

6.1. Conditions for lawful processing of personal information.

6.1.1. RERIS may only use a data subject's personal information for the purpose for which it was collected. Therefore, processing of personal information must only be done to the extent necessary and consented to by the data subject to achieve the purpose of the processing.

6.2. Consent, justification and objection.

6.2.1. Personal information may only be processed if:

6.2.1.1. The data subject consents to the processing;

6.2.1.2. Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

6.2.1.3. Processing complies with an obligation imposed by law on RERIS;

6.2.1.4. Processing protects a legitimate interest of the data subject;

6.2.1.5. Processing is necessary for the proper performance of a public law duty by a public body; or

6.2.1.6. Processing is necessary for pursuing the legitimate interests of RERIS or of a third party to whom the information is supplied.

6.2.2. RERIS must be able to provide proof of the data subject's consent to the Regulator upon request. For example, a completed and signed marketing options declaration form, a recording of the data subject's consent over the telephone or an opt-in SMS received from the data subject.

6.3. Collection directly from data subject.

6.3.1. Personal information must be collected directly from the data subject unless:

6.3.1.1. The information is contained in or derived from a public record or has deliberately been made public (for example unrestricted Social Media accounts) by the data subject;

6.3.1.2. Collection of the information from another source would not prejudice a legitimate interest of the data subject;

6.3.1.3. Collection of the information from another source is necessary:

6.3.1.4. To comply with an obligation imposed by law;

6.3.1.4.1. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; and

6.3.1.4.2. In the interests of national security.

6.3.1.5. Compliance would prejudice a lawful purpose of the collection; or

6.3.1.6. Compliance is not reasonably practicable in the circumstances of the particular case.

7. Further processing limitation

7.1. Further processing of personal information must be done in accordance with or be compatible with the purpose for which it was collected if:

7.1.1. The data subject has consented to the further processing of the information;

7.1.2. The information is available in or derived from a public record or has deliberately been made public by the data subject;

7.1.3. Further processing is necessary:

7.1.3.1. To avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;

7.1.3.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue for the benefit of SARS;

7.1.3.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

7.1.3.4. In the interests of national security.

7.1.4. The information is used for historical, statistical or research purposes and RERIS ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

7.2. In order to assess whether further processing is compatible with the purpose of collection, RERIS must take account of:

7.2.1. The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

7.2.2. The nature of the information concerned;

7.2.3. The consequences of the intended further processing for the data subject;

7.2.4. The manner in which the information has been collected; and

7.2.5. Any contractual rights and obligations between the parties.

8. Quality of information

8.1. RERIS must take reasonable steps to ensure that personal information is complete, accurate and that it is updated regularly.

9. Purpose specific

9.1. Collection for specific purpose.

9.1.1. Personal information may only be collected for a specific, detailed, defined and lawful purpose which is related to a function or activity of RERIS.

9.1.2. The data subject must be made aware of the purpose of the collection of the information.

9.2. Retention and restriction of records.

9.2.1. Subject to paragraphs 9.2.1.2 and 9.2.3, records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

9.2.1.1. Retention of the record is required or authorised in terms of any law (see the retention of records policy and accompanying schedules);

9.2.1.2. Retention of the record is required by a contract between the parties thereto; or

9.2.1.3. The data subject has consented to the retention of the record for an extended period of time.

9.2.2. RERIS must properly destroy documentation and/or delete a record of personal information or de-identify it as soon as reasonably practicable after RERIS is no longer authorised to retain the record.

9.2.3. RERIS must restrict processing of personal information if:

9.2.3.1. Its accuracy is contested by the data subject, for a period enabling RERIS to verify the accuracy of the information;

9.2.3.2. RERIS no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof, in which case, such records may not be kept for longer than 5 years unless regulated by legislation;

9.2.3.3. The data subject opposes its destruction or deletion and requests the restriction of its use instead; or

9.2.3.4. The data subject requests to transmit the personal data into another automated processing system (for example change from email to SMS).

9.2.4. Where processing of personal information is restricted pursuant to paragraph 9.2.3, RERIS must inform the data subject before lifting the restriction on processing.

10. Openness

10.1. Notification to the data subject when collecting personal information.

10.1.1. If personal information is collected, RERIS must take steps to ensure that the data subject is aware of:

10.1.1.1. The information being collected and where the information is not collected directly from the data subject, the source from which the information is collected;

10.1.1.2. The name and address of RERIS;

10.1.1.3. The purpose for which the information is being collected;

10.1.1.4. Whether or not the supply of the information by that data subject is voluntary or mandatory;

10.1.1.5. The consequences of failure to provide the information;

10.1.1.6. Any particular law authorising or requiring the collection of the information;

10.1.1.7. The fact that, where applicable, RERIS intends to transfer the information to a third-party country or international organization and the level of protection afforded to the information by that third-party country or international organisation;

10.1.1.8. The data subject's right to lodge a complaint to the Regulator and the contact details of the Regulator.

10.1.2. The steps referred to above must be taken before the information is collected if the personal information is collected directly from the data subject.

10.1.3. In the event that RERIS has previously taken the above steps then, RERIS need not repeat these steps in relation to the subsequent collection of the same information or similar information and if the purpose of collection of the information has not changed.

10.1.4. It is not necessary for RERIS to comply with the requirements in paragraph 10.1.1 if:

10.1.4.1. The data subject has provided consent for the non-compliance; and

10.1.4.2. The information will not be used in a form in which the data subject may be identified.

11. Security safeguard

11.1. Security measures on integrity and confidentiality of personal information.

11.1.1. RERIS must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

11.1.1.1. Loss of, damage to or unauthorised destruction of personal information; and

11.1.1.2. Unlawful access to or processing of personal information.

11.1.2. In order to give effect to paragraph 11.1.1, RERIS must take reasonable measures to:

11.1.2.1. Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

11.1.2.2. Establish and maintain appropriate safeguards against the risks identified;

11.1.2.3. Regularly verify that the safeguards are effectively implemented; and

11.1.2.4. Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

11.1.3. RERIS must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

11.2. Third party operator obligations.

11.2.1. An operator or anyone processing personal information on behalf of RERIS, must process such information in accordance with the related contract's management policy and the guidelines on outsourcing agreements and other related subsidiary policies.

11.3. Process of notification of security compromises.

11.3.1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the operator must notify RERIS immediately within 24 hours of the suspected unauthorised access.

11.3.2. The RERIS must notify:

11.3.2.1. The Regulator; and

11.3.2.2. The data subject, unless the identity of such data subject cannot be established.

11.3.3. The above notification must be in writing and communicated to the data subject in at least one of the following ways:

11.3.3.1. Mailed to the data subject's last known physical or postal address;

11.3.3.2. Sent by e-mail to the data subject's last known e-mail address; placed in a prominent position on RERIS's website;

11.3.3.3. Published in the news media; or

11.3.3.4. As may be directed by the Regulator.

11.3.4. The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the suspected unauthorised access, including:

11.3.4.1. A description of the possible consequences of the security compromise;

11.3.4.2. A description of the measures that RERIS intends to take or has taken to address the security compromise;

11.3.4.3. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

11.3.4.4. If known to RERIS, the identity of the unauthorized person who may have accessed or acquired the personal information.

11.3.5. RERIS may only delay notification of the data subject if the South African Police Service (SAPS) or any other regulator or the Regulator determines that notification will impede a criminal investigation by the SAPS or that regulator.

12. Data subject requests

12.1. Request to access to personal information.

12.1.1. A data subject may request access to his/her personal information held by RERIS by completing the Access to Information Request Form available on the RERIS external website and providing adequate identification.

12.1.2. The data subject has the right to request RERIS:

12.1.2.1. To confirm, free of charge, whether or not RERIS holds personal information about the data subject; and

12.1.2.2. To furnish him/her with the record or a description of the data subject's personal information held by RERIS, including information about the identity of all third parties, who have, or have had, access to the information:

12.1.2.2.1. Within a reasonable time (no longer than 30 days);

12.1.2.2.2. In a reasonable manner and format; and

12.1.2.2.3. In a format that is understandable.

12.1.3. RERIS may or must refuse, as the case may be, to disclose any information requested.

12.1.4. If a request for access to personal information is made to RERIS and part of that information may or must be refused in terms of paragraph 12.1.3, every other part must be disclosed.

12.2. Correction of personal information.

12.2.1. A data subject may request RERIS:

12.2.1.1. To correct or delete personal information about the data subject in its possession that is:

12.2.1.1.1. Inaccurate,

12.2.1.1.2. Irrelevant,

12.2.1.1.3. Excessive,

12.2.1.1.4. Out of date,

12.2.1.1.5. Incomplete,

12.2.1.1.6. Misleading or

12.2.1.1.7. Obtained unlawfully; or

12.2.1.2. To destroy or delete a record of personal information about the data subject that RERIS is no longer authorised to retain.

12.2.2. On receipt of a request, RERIS must, within 30 days:

12.2.2.1. Correct the information;

12.2.2.2. Destroy or delete the information;

12.2.2.3. Provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or

12.2.2.4. Where agreement cannot be reached between RERIS and the data subject, and if the data subject so requests, take such reasonable steps, to attach a notice to the data subject's information recording that a correction of the information has been requested but has not been made.

12.2.3. If RERIS has attached a notice referred to under paragraph 12.2.2 and that notice results in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, RERIS must inform each person or body to whom the personal information has been disclosed of that notice.

12.2.4. RERIS must notify a data subject, who has made a request in terms of paragraph 12.2.1, of the action taken as a result of the request.

13. Processing of special personal information

13.1. Prohibition on processing of special personal information.

13.1.1. Unless the provisions of paragraph 13.2 are complied with, RERIS may not process personal information concerning:

13.1.1.1. The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

13.1.1.2. The criminal behaviour of a data subject if such information relates to: -

12.2.4.1.1. The alleged commission by a data subject of any offence; or

12.2.4.1.2. Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

13.2. General authorisation concerning special personal information.

13.2.1. The prohibition on processing personal information, specified in paragraph 13.1 of this policy, does not apply if the:

13.2.1.1. Processing is carried out with the consent of a data subject;

13.2.1.2. Processing is necessary for the establishment, exercise or defence of a right or obligation in law;

13.2.1.3. Information has deliberately been made public by the data subject (for example, unrestricted Social Media); or

13.2.1.4. Provisions of paragraph 13.3 of this policy are, as the case may be, complied with.

13.3. Authorisation of data subject's special personal information concerning:

13.3.1. Religious or philosophical beliefs.

13.3.1.1. RERIS may not process this personal information as only spiritual or religious organisations to which the data subject belongs are permitted to process such personal information.

13.3.1.2. RERIS may not supply this personal information to third parties without the consent of the data subject.

13.3.2. Race or ethnic origin.

13.3.2.1. Processing may only be done to:

13.3.2.1.1. Identify data subjects and only when this is essential for that purpose; and

13.3.2.1.2. Comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination (for example compliance with the Employment Equity Act).

13.3.3. Trade union membership.

13.3.3.1. Processing may only be done if a data subject's personal information relating to his or her membership or affiliation with a trade union or the trade union federation to which that trade union belongs is necessary to achieve the aims of the trade union or trade union federation.

13.3.3.2. In the cases referred to under 13.3.3.1, no personal information may be supplied to third parties without the consent of the data subject.

13.3.4. Political persuasion.

13.3.4.1. RERIS may not process a data subject's personal information relating to his, her or its political persuasion.

13.3.5. Health or sex life.

13.3.5.1. RERIS may not process a data subject's personal information relating to his or her health or sex life unless processing is done by:

13.3.5.1.1. Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing; the performance of an insurance or medical scheme agreement; or the enforcement of any contractual rights and obligations; or

13.3.5.1.2. Administrative bodies, pension and provident funds, employers or institutions working for them, if such processing is necessary for the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

13.3.5.2. In the cases referred to under paragraph 13.3.5.2, the information may only be processed by RERIS and other responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between RERIS and the data subject.

13.3.5.3. In processing personal information relating to the health or sex life of a data subject, RERIS must at all times, treat such personal information with confidentiality unless RERIS is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information.

13.3.6. Criminal behaviour or biometric information.

13.3.6.1. The processing must be carried out by the SAPS, prosecutors and courts of law or by responsible parties who have obtained that information in accordance with the law (for example, attorneys).

13.3.6.2. The processing of information concerning personnel in the service of RERIS must take place in accordance with the rules established in compliance with labour legislation.

14. Processing of personal information of children

14.1. A child is a person who is under the age of eighteen (18) years.

14.1.1. RERIS may not process personal information concerning a child without the prior consent of the child's parent or legal guardian;

14.1.2. RERIS may not, under any circumstances, collect or process personal information concerning a child for direct marketing purposes.

15. Rights of data subjects direct marketing

15.1. Direct marketing by means of unsolicited electronic communications.

15.1.1. RERIS may not process personal information of a data subject (customer/lead) for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail unless the data subject:

15.1.1.1. In the case of a customer:

15.1.1.1.1. The customer has given his or her explicit consent to receive direct marketing and the customer's consent is obtained when the personal information is collected during the conclusion of the sale;

15.1.1.1.2. The customer's consent must be requested in the prescribed manner and form.

15.1.1.1.3. The content of the direct marketing is limited to similar goods/services sold by RERIS; and

15.1.1.1.4. The customer must be given a reasonable opportunity to object to receipt of direct marketing both when the data was first collected (during the sale) and on each occasion when direct marketing is made to the customer.

15.1.1.2. In the case of a lead/prospective customer:

15.1.1.2.1. RERIS must first get the lead's contact details to approach the lead for consent. Unless these contact details were in the public domain, such as a telephone directory, merely obtaining the contact details (for example through a company that sells data lists) could be an infringement of the POPI Act.

15.1.1.2.2. A lead who has not withheld consent may be approached only once in order to request the consent of that lead/prospective customer.

15.1.1.2.3. The lead must be given a reasonable opportunity to object to receipt of direct marketing.

15.1.1.2.4. In the event that the lead gives his/her consent to receive direct marketing, then the lead must be given a reasonable opportunity to object to receipt of direct marketing on each occasion when direct marketing is made to the lead.

15.1.2. Any communication for the purpose of direct marketing must contain:

15.1.2.1. Details of the identity of the sender or the person on whose behalf the communication has been sent; and

15.1.2.2. An address or other contact details to which the customer may send a request to stop receiving such communication.

16. Transborder information flows

16.1. Transfers of personal information outside the Republic of South Africa.

16.1.1. RERIS may not transfer personal information about a data subject to a third party who is in a foreign country unless

16.1.1.1. That third party is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection;

16.1.1.2. The data subject consents to the transfer;

16.1.1.3. The transfer is necessary for the performance of a contract between the data subject and RERIS; or

16.1.1.4. The transfer is for the benefit of the data subject, and

15.1.2.2.1. It is not practical to obtain the consent of the data subject to that transfer; and

15.1.2.2.2. If it were reasonably practical to obtain such consent, the data subject would be likely to give it.

17. Administrative fines

17.1. Administrative fines.

17.1.1. If RERIS is alleged to have committed an offence in terms of the POPI Act, the Regulator may deliver, by hand, to RERIS an infringement notice. This notice must immediately be forwarded to the Information Protection Officer.

17.1.2. The information protection officer must, within 30 days of receipt of the infringement notice by RERIS, respond to the Regulator as required in terms of the infringement Notice.

18. Offences and penalties

18.1. RERIS shall be guilty of an offence if:

18.1.1. It fails to comply with an enforcement notice;

18.1.2. In compliance with an information notice served by the Regulator,

18.1.2.1. Makes a statement knowing it to be false; or

18.1.2.2. Recklessly makes a statement which is false, in a material respect.

18.2. Any person (employee) is guilty of an offence if:

18.2.1. He/she knowingly or recklessly, without the consent of RERIS, obtains or discloses or offers to sell personal information of a data subject such as account number, ID, bank statements and address details.

18.3. Penalties.

18.3.1. The maximum penalty for a person (including RERIS) who is found guilty of an offence in terms of the POPI Act is a fine of up to R10 million or imprisonment for a period of up to 10 years, or both.

19. Authority and mandate

19.1. The Protection of Personal Information Policy is approved by way of approved resolution of RERIS' directors. The management is responsible for the adherence to and implementation of this Protection of Personal Information Policy.