HYBRID
Risk Management

PROTECTION OF PERSONAL INFORMATION (POPI) POLICY

INTRODUCTION

Hybrid Risk Management is an authorised Financial Service Provider hereinafter referred to as “Hybrid”, “The FSP”, “We”, “Us” and “Our”.

We are committed to protecting your privacy and interests by implementing measures with the objective to ensure that your personal information is collected and processed lawfully and that safeguards are in place to prevent loss of, damage to, or unauthorised destruction of data or unlawful access to or processing of personal information.

This policy explains what information we collect and how we obtain, use, process and disclose personal information as is required in terms of the Protection of Personal Information Act (POPIA).

It is our intention that this policy will protect an individual’s personal information from being prejudiced in any way and this policy is consistent with the privacy laws applicable in South Africa.

PERSONAL INFORMATION

We collect and process your personal information primarily to provide you with access to our services and products, for the performance of a policy, as well as to assist us improve our services to you.

Personal information is any information specific to you, which you provide, or which is received by us through our website, mobile application, intermediaries (brokers), helpdesk, or any other channel with your consent.

This information may relate to you as a natural or a juristic person. For example:

- Name & surname
- Race, gender, marital status, ethnic or social origin, age, disability, language & education, criminal history, employment
- Identity number
- Contact information, email, telephone, address
- Vehicle information including information provided by telematics and tracking units
- Correspondence provided by you or an agent acting on your behalf
- Property and asset information including descriptions and use
- Insurance history, claims history, or credit information
- Company information
- Financial information
- Information made public by you

We may collect and process information provided to us, with your consent from your broker or financial advisor, insurers, underwriters, the insurance data sharing system, TransUnion, or insurance administrators. We may also collect and process data relating to your visits to our website and / or app including, but not limited to traffic data, location data, weblogs and other communication data.

By using and/or accessing the Website available at www.hybridrisk.co.za and/or our mobile application and/or products and services, you consent to us collecting and processing your personal information on the basis as set out in this policy.

The Website and App make use of Cookies in order to provide you with relevant content and the best experience possible whilst using the Website and/or App. At any stage during your use of the website and/or App, you may choose to block the Cookies used by us, however this may impact your use or experience of the Website and/or App.

PURPOSE FOR WHICH INFORMATION IS COLLECTED (USE OF INFORMATION)

We collect, store, verify or share personal or other information where relevant, for the following purposes:

- To conclude or propose to conclude an insurance contract
- For underwriting purposes and risk assessment
- Assessing, validating, and processing claims
- Conducting credit reference searches or verification or credit rating
- Confirming and verifying an individual's identity
- For purposes of validating, verifying, or recording claims or insurance history
- For the detection, enforcement, and prevention of fraud, crime, money laundering or other malpractice
- Conducting market or customer satisfaction research to improve our service
- For compliance, reporting, audit, and record keeping purposes
- In connection with legal proceedings, as required by law or to combat fraud
- Follow an individual's instructions
- To Inform a person of services available to them
- To establish if products or services offered by us suits the individual's needs

The collection, and processing of personal Information may be required to assess your risk profile, process claims, provide quotations, comply with reporting, and audit obligations, offer services or to answer any requests or enquiries, relating to a service or product and will only be used where it is relevant.

Personal information collected, is used only for the purpose for which it was intended. Copies of correspondence that may contain personal information, is stored for record-keeping, reference, validation, and back-up purposes.

Information is retained in line with the purpose for which it is collected and to enable us to comply with reporting and audit requirements. Claims, underwriting, and policy information history is stored to provide future information pertaining to underwriting risk, previous claims and losses, payments record, legal requirements and for future cover requirements, variations or amendments to existing cover.

We will not reveal any personal information to a third party unless:

- it is relevant to the purpose for which it has been collected and necessary in terms of the performance of the insurance policy.
- it is necessary for the performance of our functions and services, to conduct our business or deliver our service (for e.g., process your claim)
- we are compelled to comply with legal and regulatory requirements or when it is otherwise allowed by law
- it is in the public interest (for example combating fraud)
- It is information made public by you

- it is necessary to protect or defend our legal rights including the rights of our shareholders, directors, partners, employees, or clients
- the FSP undergoes a change in ownership, for the sole purpose of the new owner being able to continue operating the business and providing the products and services related thereto
- otherwise consent to by you

Third parties may include: Insurers, reinsurers, claims assessors, loss adjustors, contractors, or service providers (where required to perform functions related to the indemnification, reinstatement, repair or replacement of any insured item), Home or roadside assist service providers, TransUnion, investigators, attorneys, courts, tracing agents, police or your broker.

RIGHT TO ACCESS OR CORRECT PERSONAL INFORMATION

You have the right to access your personal information, request corrections, and request identities of third parties who have or had access to your personal information. Such requests can be made in writing to us at the information provided below under contact information.

REVOKING CONSENT AND/OR REQUEST DELETION OF PERSONAL INFORMATION

If you request, we will delete or anonymise your personal data so that it no longer identifies you, unless we are legally allowed or required to maintain certain personal information, including situations where data is required to fulfil our contract or obligations such as the following:

- If you have an active insurance contract, we must maintain your details in order to administer your insurance contract, claims, and obligations. This may also be required in terms of our legal reporting and record keeping requirements or such other as set out under any applicable law and to assist in combating fraud which is in the public interest.
- If there is an unresolved issue relating to your account, such as an outstanding or an unresolved claim, recovery, or dispute.
- Where we are required to retain the personal data for our legal, tax, audit, reporting, and accounting obligations, we will retain the necessary personal data for the period required by applicable law; and/or,
- Where necessary for our legitimate business interests such as fraud prevention or to maintain the security and protection of our clients and stakeholders.

SECURITY SAFEGUARDS

We strive to ensure the security, integrity, and confidentiality of personal information. We will review and update our security measures in accordance with future legislation and technological advances.

Unfortunately, no data transmission over the Internet can be guaranteed to be totally secure, however, we will endeavour to take all reasonable steps to protect the personal information against loss, damage, unauthorized destruction, or unlawful access or processing of personal data.

We will always maintain high standards to ensure the protection and integrity of their systems.

We may engage with other 3rd party organisations to provide support services to us. Such third parties are obliged to respect the confidentiality of any personal information held by us or to which they have access

to in the course of establishing, maintaining, servicing, updating, improving, or developing our systems, databases, portals, and infrastructure.

Our employees are obliged to respect the confidentiality of any personal information held by us. All employees are required to sign an employment contract which includes a confidentiality clause. They are also required to familiarise themselves with and complete training on the Protection of Personal Information Act (POPIA) insofar as it applies to them.

We endeavour to take all reasonable steps to keep secure any personal information which they hold or have access to, and to keep this information accurate and up to date. If at any time, an individual discovers that information gathered about them is incorrect, they may contact the FSP to have the information corrected at the contact information provided below.

CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

According to the POPI Act there are eight conditions that must be complied with to ensure that the processing of personal information is lawful. These conditions include:

1. Accountability
The responsible party must ensure that the conditions set out in Chapter 3 of the POPI Act, and all the measures that give effect to such conditions, are complied with.

2. Processing Limitation
Personal information may only be processed in a lawful and reasonable manner that does not infringe on the privacy of the data subject.

Personal information may only be processed if:

- the data subject (or a competent person, where the data subject is a child), consents to the processing
- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party
- processing complies with an obligation imposed by law on the responsible party
- processing protects a legitimate interest of the data subject
- processing is necessary for the proper implementation of a public duty governed by law
- processing is necessary for pursuing the legitimate interests of the responsible party
- it was obtained directly from the data subject. Data can be collected from a third party when:
    - The data is public record or is deliberately made public by the data subject
    - Consent has been given to do so
    - The legitimate interests of the data subject has not been violated
    - There are also exceptions for those working in court proceedings, law enforcement and public bodies

3. Purpose Specific
Personal information may only be collected for specific, explicitly defined, and legitimate reasons relating to a function or activity of the responsible party. The data subject must be made aware of the purpose of

the collection of personal information. It is therefore important to understand the purpose for which we collect personal information as noted above.

4. Further Processing Limitation
Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

Therefore, if we wish to process existing personal information for a purpose other than the purpose for which it was originally collected, we must first obtain additional consent from the data subject, otherwise we may process data further if:

- The data subject consented
- Information came from a public record
- Law requires further processing
- Processing is related to national security

5. Information Quality
We will take all reasonable steps to ensure that all personal information collected is complete, accurate, not misleading and up to date.

6. Openness
We will maintain the documentation of all processing operations. We will take all reasonable steps to inform data subjects whose information is being collected of:

- The information being collected and where the information is not collected from the data subject, the source from which it is collected;
- The name and address of the responsible party;
- The purpose for which the information is being collected;
- Whether or not the supply of the information by that data subject is voluntary or mandatory;
- The consequences of failure to provide the information;
- Any particular law authorising or requiring the collection of the information;
- The fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation.
- The nature or category of the information
- Their right to access or rectify the information collected
- Their right to object to their personal information being processed (See revoking consent and/or request deletion of personal information above)
- Their right to lodge a complaint with the information regulator (see complaints below)

7. Security Safeguards
The responsible party 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 loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information.

To achieve the abovementioned results, the responsible party must take reasonable measures to:

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

8. Data Subject Participation

A data subject may request whether their personal information is held, as well as the correction or deletion of his or her personal information held by the FSP. The FSP will take all reasonable steps to confirm your identity before providing details of your personal information.

INDEMNITY

By accepting our privacy policy, you indemnify Hybrid Risk Management against any loss, liability, harm, damage (whether direct, indirect or consequential) or expense of any nature whatsoever which may be suffered by you or any third party arising from any third party or service provider's failure to comply with the requirements of the Protection of Personal Information Act or any other relevant law.

CONTACT INFORMATION

Any questions relating to the FSP's POPI policy or the treatment of an individual's personal data may be addressed to the contact details below:

Information officer:	Hendrik Andries (Hendre) Smit
Telephone number:	087 80 80 807
Postal address:	Postnet suite 99, Private bag x5, Strubensvalley,1735
Physical address:	Ruimsig Country office estate, Block D, 129 Hole-in-one avenue, Ruimsig, Gauteng, 1724
Email address:	hendre@hybridrisk.co.za
Website:	www.hybridrisk.co.za

COMPLAINTS

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. All complaints must be submitted to us in writing and will be considered by the Information Officer. Where the data subject is not satisfied with the Information Officer's determination, the data subject has the right to complain to the Information Regulator.

Information Regulator

Tel:	010 023 5200
Email:	enquiries@inforegulator.org.za POPIAComplaints@inforegulator.org.za