

**GUARDRISK  
PUBLIC PRIVACY  
POLICY**

**July 2026**

**Policy Reference: 0055**

**Policy Owner: Chief Risk Officer**

## Table of Contents

|          |                                                                                      |           |
|----------|--------------------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>ABOUT.....</b>                                                                    | <b>5</b>  |
| <b>2</b> | <b>INFORMATION DISCLOSURE.....</b>                                                   | <b>6</b>  |
| 2.1      | WHAT IS PERSONAL INFORMATION?.....                                                   | 6         |
| 2.2      | WHAT IS SPECIAL PERSONAL INFORMATION? .....                                          | 7         |
| 2.3      | HOW DOES GUARDRISK COLLECT PERSONAL INFORMATION? .....                               | 8         |
| 2.4      | WHAT TYPE OF PERSONAL INFORMATION DOES GUARDRISK COLLECT?.....                       | 8         |
| 2.5      | POTENTIAL CONSEQUENCES OF REFUSING TO PROVIDE PERSONAL INFORMATION.....              | 9         |
| 2.6      | WHEN WILL WE PROCESS YOUR PERSONAL INFORMATION? .....                                | 9         |
| 2.7      | WHEN WILL WE PROCESS YOUR SPECIAL PERSONAL INFORMATION?.....                         | 9         |
| 2.8      | PERSONAL INFORMATION IN THE PUBLIC DOMAIN .....                                      | 10        |
| 2.9      | REASONS FOR PROCESSING YOUR PERSONAL INFORMATION .....                               | 10        |
| 2.10     | PROCESSING INFORMATION OF A CHILD.....                                               | 12        |
| 2.11     | WHO IS RESPONSIBLE FOR PROCESSING YOUR PERSONAL INFORMATION?.....                    | 13        |
| 2.12     | LAWFUL BASIS AND YOU AGREEING TO THIS PRIVACY POLICY .....                           | 13        |
| 2.13     | OBTAINING PERSONAL INFORMATION ABOUT CLIENTS .....                                   | 14        |
| 2.14     | RETENTION OF DATA .....                                                              | 16        |
| 2.15     | PROCESSING INFORMATION ABOUT PERSONS RELATED TO A JURISTIC PERSON.....               | 16        |
| 2.16     | FAILING TO PROVIDE PERSONAL INFORMATION.....                                         | 16        |
| 2.17     | DIRECT ELECTRONIC MARKETING .....                                                    | 17        |
| <b>3</b> | <b>AUTOMATED DECISION MAKING, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE .....</b> | <b>17</b> |
| 3.1      | APPLICATION OF ADM .....                                                             | 17        |
| 3.2      | LEGAL BASES AND YOUR RIGHTS .....                                                    | 18        |
| 3.3      | GOOD PRACTICE MEASURES.....                                                          | 18        |
| 3.4      | ENSURING FAIRNESS AND ACCOUNTABILITY.....                                            | 18        |
| <b>4</b> | <b>COOKIE NOTICE.....</b>                                                            | <b>18</b> |

|           |                                                                                    |           |
|-----------|------------------------------------------------------------------------------------|-----------|
| 4.1       | WHAT ARE COOKIES? .....                                                            | 18        |
| 4.2       | WHAT HAPPENS IF YOU DISABLE YOUR COOKIE FUNCTIONALITY? .....                       | 19        |
| 4.3       | TYPES OF COOKIES WE USE? .....                                                     | 19        |
| 4.4       | WHAT WE USE COOKIES FOR? .....                                                     | 19        |
| 4.5       | MANAGE YOUR COOKIE PREFERENCE .....                                                | 19        |
| 4.6       | WHY DO WE USE COOKIES? .....                                                       | 20        |
| 4.7       | IS YOUR PERSONAL INFORMATION AT RISK? .....                                        | 20        |
| <b>5</b>  | <b>WEB BEACONS .....</b>                                                           | <b>20</b> |
| <b>6</b>  | <b>COLLECTING INFORMATION FROM YOUR BROWSER .....</b>                              | <b>20</b> |
| <b>7</b>  | <b>CLOSE CIRCUIT TELEVISION (CCTV) FOOTAGE .....</b>                               | <b>21</b> |
| <b>8</b>  | <b>LOCATION SERVICES .....</b>                                                     | <b>21</b> |
| <b>9</b>  | <b>CONFIDENTIALITY AND SECURITY .....</b>                                          | <b>21</b> |
| 9.1       | ROUTINE PRECAUTIONS .....                                                          | 21        |
| <b>10</b> | <b>YOUR PERSONAL INFORMATION .....</b>                                             | <b>22</b> |
| 10.1      | SECURING PERSONAL INFORMATION .....                                                | 22        |
| 10.2      | MANAGING DATA PRIVACY AT GUARDRISK GROUP BOARD LEVEL AND REPORTING FREQUENCY<br>22 |           |
| 10.3      | EMPLOYEE TRAINING ON CYBER SECURITY AND DATA PRIVACY .....                         | 23        |
| 10.4      | CENTRALISED CYBER SECURITY AND DATA SECURITY FUNCTIONS AND COORDINATION .....      | 23        |
| 10.5      | THIRD PARTIES .....                                                                | 23        |
| 10.6      | SHARING YOUR INFORMATION .....                                                     | 23        |
| 10.7      | CROSS BORDER SHARING .....                                                         | 25        |
| 10.8      | COMMUNICATION THROUGH DIGITAL CHANNELS .....                                       | 26        |
| <b>11</b> | <b>RIGHTS OF DATA SUBJECTS .....</b>                                               | <b>26</b> |
| <b>12</b> | <b>CHANGES TO PRIVACY POLICY .....</b>                                             | <b>27</b> |
| <b>13</b> | <b>WHICH LAWS APPLY? .....</b>                                                     | <b>27</b> |

|                                                       |           |
|-------------------------------------------------------|-----------|
| <b>14 GET IN TOUCH - COMPLIMENTS OR REQUESTS.....</b> | <b>28</b> |
| <b>15 COMPLAINTS .....</b>                            | <b>30</b> |

## 1 ABOUT

This Privacy Policy governs the manner in which Guardrisk Group ('we', 'our', 'us', 'Guardrisk') treats your personal information, that is collected electronically when you use our website, which can be found at ([www.guardrisk.co.za](http://www.guardrisk.co.za)) to apply online for certain products and services, contact us electronically or register for one of the services or products we offer on the website. This policy sets out the processing in accordance with the Protection of Personal Information Act ('POPIA') and other relevant laws.

The Privacy Policy applies to any website, mobile application, form, document, product or service, which can be found on our website at <https://guardrisk.co.za> which references this Privacy Policy. It also supplements any other privacy policies which may apply in respect of Momentum Group's and/or Guardrisk's entities' processing of personal information.

This policy explains why we collect such personal information, what personal information is collected, and what we do (and do not do) with it. It also explains how you can change your personal information.

We respect your privacy and your personal information and for this reason, we will take all reasonable measures, in accordance with this Policy, to protect your personal information to keep it confidential, even when you are no longer our client. We will maintain the confidentiality of your personal information and comply with the Protection of Personal Information Act 4 of 2013 (POPIA) in South Africa, the other related Data Protection Laws, regardless of which jurisdiction it originated from.

This policy applies to South African entities within the Guardrisk Group of companies, its subsidiaries, operating divisions, business units, licensed entities, management-controlled entities and activities. Each subsidiary not located in South Africa will apply their relevant Data Protection law in their jurisdiction, and that specific Privacy Policy can be accessed for that related information.

Guardrisk operates a cell captive insurance business model. Depending on the product or service provided, Guardrisk may process personal information as a Responsible Party Operator in terms of POPIA.

Guardrisk comprises of companies that provide, among others (but may not be limited to), the following products, and services:

- Claims Processing

- Claims Administration
- Financial services
- Health benefits
- Insurance products
- Payment products and services
- Advanced Analytics
- Insights and Research

Personal information may be processed on behalf of insurers, cell owners, underwriting management agencies (UMAs), binder holders, administrators, reinsurers, claims service providers and other authorised parties involved in the provision and administration of insurance products.

Guardrisk will only share personal information where there is a lawful basis to do so and where appropriate contractual, confidentiality and information security safeguards have been implemented.

Where another party is the Responsible Party, Guardrisk may process personal information solely on the documented instructions of that party and in accordance with applicable laws.

**We briefly outline these principles below:**

- We will only collect, disclose, collate, process, share and store ('use') your personal information with your express written permission, unless legally required to do so, and will only use such information for the lawful purpose for which it is required.
- We will disclose in writing, the specific purpose for which we use, request and store your personal information. We will also keep a record of that personal information and the specific purpose for which we collect it.

**Applicable audience for this policy:**

- A visitor to our website(s)
- Any user of our applications and/or;
- A client who has any product or service or requested any product or service that we provide.

## **2 INFORMATION DISCLOSURE**

### **2.1 What is personal information?**

Personal information refers to any information that identifies you or specifically relates to you. Personal information includes, but is not limited to, the following information about you:

- Your marital status (like married, single, divorced); your national origin; your age; your language; birth; education.
- Your financial information, which may include your financial history and information (like your income or your buying, investing and banking behaviour based on, amongst others, account transactions).
- Your identifying number (like an account number, identity number or passport number).
- Your e-mail address; location information; physical address (like residential address, work address or your physical location); and telephone number (including your cellular number, home landline or office work number).
- Your online identifiers such as social media profiles.
- Your biometric information (like fingerprints, selfies, photos, face recognition, signature or voice).
- Your race and/or gender.
- Your physical health; mental health; well-being; disability; religion; belief; conscience; culture (this also includes physical health tests and results based on wearable fitness devices).
- Your medical history (like your HIV / AIDS status and any medical history disclosed or obtained); criminal history; employment history.
- Your personal views, preferences and opinions.
- Your confidential correspondence; and / or
- Another's views or opinions about you and your name also constitute your personal information.
- CCTV footage (on our physical office premises and branches).

But excludes:

- Information that has been anonymised so that it does not identify a specific person;
- Permanently de-identified information that does not relate or cannot be traced back to you specifically;
- Non-personal statistical information collected and compiled by us.

## **2.2 What is Special Personal Information?**

Special personal information is personal information about the following:

- Your religious and your philosophical beliefs (for example where you enter a competition, and you are requested to express your philosophical view).

- Your race (like where you apply for a product or service where the statistical information must be recorded).
- Your ethnic origin.
- Your trade union membership.
- Your political beliefs.
- Your health (Like where you apply for an insurance policy or medical/health related products).
- Your biometric information (like to verify your identity); and / or
- Your criminal behaviour and alleged commission of an offence (like to prevent money laundering as required by law or when you apply for employment or enter into a relationship with us).

### **2.3 How does Guardrisk collect Personal Information?**

The company collects information either directly from you, the data subject, the employer or through financial services intermediaries. In certain instances, Guardrisk may appoint third parties to collect information on its behalf. The source from which personal information was obtained, if not directly from the data subject, will be disclosed. We may monitor and record any telephone calls that you make to us, unless you specifically request us not to.

### **2.4 What type of Personal Information does Guardrisk collect?**

Personal information collected by Guardrisk can include, but not limited to, and depending on the transaction, a data subject's name, contact, birth date, identity number, gender, employment details, voice recordings, email correspondence, marital, family, policy, location information, online identifier, bank account, medical or health information.

When personal information is collected, the company will indicate the purpose for the collection and whether the information required is compulsory or voluntary. This is indicated on the application forms. Should you have any queries around the reason for collection of the mandatory information; you can consult your advisor.

Third parties may be used to aid in the collection of such information. This information will be restricted to only the required information pertaining to the benefit of your product.

We will also collect your information where you have only partially completed and/or abandoned any information which you began to apply to our website and/or other online forms. Given that we already

consider you a customer at this stage, we may use this information to contact you in order to remind you to complete outstanding information.

## **2.5 Potential consequences of refusing to provide personal information**

Where we require personal information in order to provide you with our products and services (and benefits), your failure to provide us with the necessary information, may result in Guardrisk being unable to provide you with our products and services or assisting in claims. Where such services include financial advice, the appropriateness of the advice may be compromised if you do not provide complete and accurate information. You are responsible for informing Guardrisk if your information changes.

## **2.6 When will we process your Personal Information?**

We will only process your personal information for lawful purposes relating to our business if the following circumstances apply:

- You have consented thereto (where applicable), and/or
- A person legally authorised by you, the law or a court, has consented thereto, and/or
- It is necessary to conclude or perform under a contract we have with you, and/or
- The law requires or permits it (Please refer to our PAIA manual for applicable laws available here, and/or
- It is required to protect or pursue your, our or a third party's legitimate interest; and/or
- You are a child, and a competent person (such as a parent or guardian) has consented thereto on your behalf, and/or

## **2.7 When will we process your special personal information?**

We may process your special personal information in the following circumstances:

- If you have consented to the processing thereto, and/or
- If the processing is needed to create, use or protect a right or obligation in law, and/or
- If the processing is for statistical or research purposes, and/or
- If the special personal information was made public by you, and/or
- If the processing is required by law, and/or
- If racial information is processed and the processing is required to identify you; and/or

- If health information is processed, and the processing is to determine your insurance risk, or to comply with an insurance policy, or to enforce an insurance right or obligation, and/or
- If we do sanctions screening (against any sanctions list, we may in our sole discretion determine) and we may find reports of alleged criminal conduct or proceedings in this regard.

## **2.8 Personal Information in the Public Domain**

Any information or personal information that any data subject makes known on any social media platform or any other media or internet publications remains information made public by the data subject and cannot be protected by Guardrisk and is not protected under the scope of POPIA. We encourage all clients who engage with us not to do so publicly on chatrooms or social media public forms as that information cannot be protected. The privacy policies of the specific platforms used for engagement will be the applicable to the protection regarding such data. Our formal channels such as our websites, call centres and mobile apps are the only platforms that can be managed, governed, and secured by Guardrisk and covered by this Privacy Policy.

## **2.9 Reasons for processing your personal information**

We may use or process any products or services information, or optional information that you provide to us for the purposes that you indicated when you agreed to provide it to us. Processing includes gathering your personal information, disclosing it, and combining it with other personal information. We generally collect and process your personal information for various for the following reasons:

- Products or services purposes such as:
  - Payment processing services providers, merchants, banks and other persons that assist with the processing of your payment instructions.
  - Third parties including, administrators, insurers, brokers, other financial institutions or other organisations that assist with insurance and assurance underwriting, the providing of insurance policies and products, the assessment of insurance and assurance claims, and other related purposes.
  - Trustees, executors or curators appointed by a court of law.
  - Cheque verification service providers.
  - Our service providers, agents and sub-contractors such as couriers and other persons we use to offer and provide products and services to you.
  - Our joint venture partners; and/or

- To process payment instruments (such as a cheque) and payment instructions (such as a debit order or a stop order deduction).
- To conduct affordability assessments, credit assessments and credit scoring (where applicable);
- To develop credit models and credit tools.
- To open, manage and maintain your accounts/policies, contracts, agreements, or relationship with us.
- To disclose and obtain personal information from registered credit bureaux regarding your credit history.
- To enable us to deliver goods, documents, or notices to you.
- For security and identity verification, and to check the accuracy of your personal information.
- To allow the allocation of health benefits where applicable.
- To communicate with you and carry out your instructions and requests.
- For customer satisfaction surveys, promotional and other competitions.
- For insurance and assurance underwriting and administration.
- To process or consider or assess insurance or assurance claims.
- To provide insurance and assurance policies and products, and related services.
- To enable you to participate in and make use of value-added products and services.
- To assess our lending and insurance risks; and/or
- For any other related purposes.
- Marketing purposes such as:
  - Marketing to customers,
  - Marketing to prospects, and
  - Running promotional competitions for business.

*Please refer to section 2.17 for more detail on Marketing*

- Business purposes such as:
  - Managing employees in general,
  - Internal/ External Audit.
  - Accounting, and
  - Business planning and due diligence, and joint ventures, disposals of business, or other proposed and actual transactions.

- Legal purposes such as:
  - Law enforcement and fraud prevention agencies, and other persons tasked with the prevention and prosecution of crime.
  - Regulatory authorities, industry ombudsmen, government departments, and local and international tax authorities.
  - Courts of law or tribunals.

We may use your usage information for the purposes described above and to:

- Remember your information so that you will not have to re-enter it during your visit or the next time you access the website;
- Monitor website usage metrics such as total number of visitors and pages accessed; and
- Tracking your entries, submissions, and status in any promotions or other activities in connection with your usage of the website.

## **2.10 Processing Information of a child**

Protecting privacy of children – Guardrisk takes the privacy of children very serious. Children under the age of 18 years should obtain consent of a competent person acting on their behalf, before providing / submitting any personal information about themselves to Guardrisk or any of their websites.

We will not require children under this age to provide any personal information other than that which is reasonably necessary to use.

If we determine that a user is under the age of 18, we will not use or maintain his/her personal information without the consent of a competent person acting on their behalf.

A child is a person who is defined as a child by a country's legislation, and who has not been recognised as an adult by the courts. We process the personal information of children if the law permits this. We will only process the personal information of children if any one or more of the following applies:

- A person with the ability to sign legal agreements has consented to the processing, being the parent or guardian or a competent person acting on behalf of the child.
- The processing is needed to create, use or protect a right or obligation in law, such as where the child is an heir in a will, a beneficiary of a trust, a beneficiary of an insurance policy or an insured person in terms of an insurance policy.

- The child's personal information was made public by the child, with the consent of a person who can sign legal agreements.
- The processing is for statistical or research purposes and all legal conditions are met.
- Where the child is an heir in a will, if required to give effect to the will.
- Where the child is a beneficiary of a trust, if required to give effect to the trust deed.
- Where the child is legally old enough to open a bank account without assistance from their parent or guardian.
- Where the child is legally old enough to sign a document as a witness without assistance from their parent or guardian.
- Where the child benefits from a bank account such as an investment or savings account; and/or
- Where the child is an insured person or beneficiary of an insurance policy, if required to give effect to the policy.

## **2.11 Who is responsible for processing your personal information?**

- Guardrisk is the responsible party for all personal information that is collected and used for the purposes POPIA laws, principles, and regulations.
- Selected third parties who provide Guardrisk with services, including companies that provide us with technical support and assistance.
- Guardrisk does make use of selected appointed operators who may be responsible for the execution of specific functions. Guardrisk will always ensure that all the required legal documentation has been established and that your data is treated with confidentiality and in accordance with applicable laws.

## **2.12 Lawful basis and you agreeing to this Privacy Policy**

The supply of your Personal Information is voluntary; however, you acknowledge that we cannot make certain products or services available to you if you do not wish to supply such Personal Information.

We collect personal information inter alia in the following instances:

- in the course of executing our statutory functions;
- via this website;
- during your attendance at Guardrisk's premises;
- in connection with business transactions and services you initiate with us;
- when you are requesting access to information on our record; and/or

- where we are legally obliged to as part of a contractual agreement, statutory measure or as otherwise required by law.

We will take appropriate and reasonable technical and organisational steps to prevent any unauthorised access to, or disclosure of your personal information. We may also process your personal information where it is necessary to perform in terms of a contract with you or where it is necessary to comply with a legal or regulatory obligation.

### **2.13 Obtaining personal information about clients**

We collect information about you:

- Directly from you.
- Based on your use of our products, services, or service channels (such as our websites, applications).
- Based on how you engage or interact with us, such as on social media, and through e-mails, letters, telephone calls, and surveys.
- From public sources (such as newspapers); and
- From third parties for the purposes of conducting our business (such as partners, reward partners, list providers, our customer loyalty rewards programmes' retail and online partners, or our service providers).

If the law requires us to do so, we will ask for your consent before collecting personal information about you from third parties. The third parties from whom we may collect your personal information include, but are not limited to, the following:

- Members of the Guardrisk Group, any connected companies, subsidiary companies, its associates, cessionaries, delegates, assignees, affiliates or successors in title and/or appointed third parties (such as its authorised agents, partners, contractors and suppliers) for any of the purposes identified in this Privacy Policy.
- Your spouse, dependants, partners, employer, joint applicant or account holder and other similar sources.
- People you have authorised to share your personal information, such as a person that makes a travel booking on your behalf, or a medical practitioner for insurance purposes.
- Attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements.

- Payment processing services providers, merchants, banks and other persons that assist with the processing of your payment instructions.
- Insurers, brokers, other financial institutions or other organisations that assist with insurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims, and other related purposes.
- Law enforcement and fraud prevention agencies, and other persons tasked with the prevention and prosecution of crime.
- Regulatory authorities, industry ombudsmen, government departments, and local and international tax authorities.
- Credit bureau.
- Trustees, executors or curators appointed by a court of law.
- Third-party integration software service providers to provide data about you based on consent and/or acknowledgement that you have provided.
- Cheque verification service providers.
- Our service providers, agents and sub-contractors such as couriers and other persons we use to offer and provide products and services to you.
- Courts of law or tribunals.
- Participating partners, whether retail or online, in our customer loyalty reward programmes.
- Suppliers in the delivery of our wallet and payment services.
- Our joint venture partners.
- Marketing list providers.
- Digital data transformation or aggregation services which you have authorised to collect activity, health or other digital data streams and share with us.
- If you are a juristic person, such as a company or close corporation, we may collect and use personal information relating to the juristic person's directors, officers, employees, beneficial owners, partners, shareholders, members, authorised signatories, representatives, agents, payers, payees, customers, guarantors. Spouses of guarantors, sureties, spouses of sureties, other security providers and other persons related to the juristic person. These are related persons.
- If you provide the personal information of a related person to us, you warrant that the related person is aware that you are sharing their personal information with us, and that the related person has consented thereto.

- We will process the personal information of related persons as stated in this Privacy Policy, thus references to “you” or “your” in this Privacy Policy will include related persons with the necessary amendments.

## **2.14 Retention of data**

All client data including correspondence, voice recordings and documentation will be retained for as long as you remain a client. If the client relationship should terminate the data will not be retained for longer than what is legally required or required to be kept for evidence purposes and is in line with retention specified as per POPIA and other legislation in line with your specific product or service. Some laws may prohibit us from deleting certain data at the point of termination.

Please also refer to Data Subject rights in terms of deletion of data records below 11.

## **2.15 Processing Information about Persons Related to a Juristic Person**

- If you are a juristic person, such as a company or close corporation, we may collect and use personal information relating to the juristic person’s directors, officers, employees, beneficial owners, partners, shareholders, members, authorised signatories, representatives, agents, payers, payees, customers, guarantors, spouses of guarantors, sureties, spouses of sureties, other security providers and other persons related to the juristic person. These are related persons.
- If you provide the personal information of a related person to us, you warrant that the related person is aware that you are sharing their personal information with us, and that the related person has consented thereto.
- We will process the personal information of related persons as stated in this Privacy Policy, thus references to “you” or “your” in this Privacy Policy will include related persons with the necessary amendments.

## **2.16 Failing to provide Personal Information**

A data subject may refuse to provide personal information. Failing to provide personal information may result in not being able to provide a quote on a product or service or accuracy on quotations. It may also result in a delay in the processing of claims or may negatively affect the outcome of the claim. In order to engage in any contract for any product or service it is mandatory to provide a specified list of personal information (truthfully and accurately) in line with minimality requirements and failing to provide said information may result in decline or refusal of product or service offerings or a delay in a service offering or processing of a claim or outcome of a claim.

## **2.17 Direct Electronic Marketing**

If we are legally permitted to do so, Guardrisk may use your personal or other information to tell you about products, services and special offers from the company or the Momentum Group. To receive this information, you have to opt-in, and you can opt out from receiving such information at any time, at no cost to you.

We will use your personal information to market financial, insurance, investments and other related products and services to you, but not share your information with any third-parties external to Momentum Group for any marketing purposes. We will do this in electronic channels such as SMS, email and/or social media channels. If you are not our customer, or in any other instances where the law requires, we will only market to you by electronic communications with your consent or on your request. In all cases, you can request us to stop sending marketing communications to you at any time, at no cost to you. Neither Guardrisk nor the Momentum Group will ever sell any data to any third party for the purposes of marketing or any other reason.

*Please note that neither Guardrisk nor the Momentum Group have control over Direct Electronic Marketing sent out by Independent Financial Advisors and therefore cannot ensure no contact from independent companies.*

## **3 AUTOMATED DECISION MAKING, MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE**

In our commitment to transparency and accountability, this section of our privacy policy explains our use of Automated Decision Making (ADM) technologies, including profiling, in providing our products or services to you. ADM refers to decisions made solely based on the automated processing of personal information using software, algorithms, artificial intelligence or machine learning that do not involve human intervention.

### **3.1 Application of ADM**

We may use ADM to provide you with products and/or services. Guardrisk may use automated processing, predictive modelling, fraud detection technologies, sanctions screening and risk assessment tools to support underwriting, pricing, claims assessment, anti-money laundering controls and fraud prevention activities. Automated processing is not used as the sole basis for decisions and human review is required by law or business policy.

### 3.2 Legal bases and your rights

We ground our use of ADM on a valid legal basis under applicable data protection law, depending on the nature of the personal information involved. When ADM leads to decisions affecting you, you have rights to:

- Request human intervention,
- Contest decisions made by ADM, and
- Express your point of view.

### 3.3 Good practice measures

To ensure the integrity and fairness of our ADM processes, we have adopted several best practices:

- **Quality assurance and algorithmic auditing:** Regular checks and audits confirm our systems and algorithms function fairly and accurately, avoiding unfair bias or discrimination.
- **Data minimisation and anonymisation:** We apply strict data retention policies and use anonymisation or pseudonymisation techniques where appropriate.
- **Human intervention:** We offer clear avenues for appealing automated decisions, including providing details for human review and a direct contact point for queries.

### 3.4 Ensuring fairness and accountability

Our commitment to these practices underlines our dedication to fairness, privacy, and respect for your rights in using ADM and profiling technologies. We continually review and refine these measures to align with best practices and legal standards.

For more detailed information on your rights and how we implement ADM and profiling in our operations, please contact our information officer (details in section 14 below). We aim to enhance your experience while safeguarding your rights and data privacy in every interaction with our services.

## 4 COOKIE NOTICE

### 4.1 What are cookies?

A cookie is a small text file stored on your device by the website you are visiting. It helps the website to remember information about your device and how you use the website. We use this information to make your visit to our site as easy and useful as possible.

For more on cookies visit: <https://cookielaawinfo.com/> and <https://allaboutcookies.org>

## **4.2 What happens if you disable your cookie functionality?**

Clearing or disabling cookies may limit your website functionality, and your functionality once you've logged in. You can limit the collection of your information by disabling cookies on your browser. You may also be able to modify your browser settings to require your permission each time a site attempts to set a cookie.

However, our website(s) (and many other websites) rely on cookies to enable certain functionality. If you choose to disable cookies, some of the services available on our website may not work properly.

## **4.3 Types of cookies we use?**

There are two main types of cookies, i.e.

- Session cookies
  - When you close your browser, some cookies are deleted. These are called session cookies.
- Persistent cookies
  - Other cookies are stored on your device until they expire, or you choose to delete them. They are called persistent cookies. These cookies are sent back to us each time you visit our site.

## **4.4 What we use cookies for?**

We use cookies for session management, user device identification and classification, traffic routing, and analytics.

## **4.5 Manage your cookie preference**

By using our website(s), you consent to the placement of cookies on your device. If you prefer not to use cookies while visiting any of our websites, you can adjust the settings in your browser accordingly. For more information on how to manage your browser cookie settings, visit one of the following options:

[Chrome;](#)

[Safari;](#)

[Firefox;](#)

[Edge](#)

#### **4.6 Why do we use cookies?**

Our website(s) utilises Google Analytics, which is a web analytics service provided by Google. This enables website owners and app developers to track and analyse visitor behaviour and interactions with their digital properties. It provides insights into website traffic, user demographics, user behaviour, and conversion rates, among other metrics, to help website owners make informed decisions when optimising their digital presence.

By making use of Google Analytics, the website(s) is capable of identifying returning users and analysing their usage patterns, without personally identifying individual visitors. The information collected by the cookie(s) about the website(s) usage will be transmitted to and stored by Google. Google uses this information to evaluate website usage, prepare website activity reports, and offer other services related to website activity and internet usage.

These insights allow us to improve content and build better features that enhance your experience.

If you want to learn more about cookies, please visit the [All about Cookies website](#) which provides instructions on how to remove cookies from your device.

#### **4.7 Is your personal information at risk?**

No, we will never save any personal information, including login details or other personal information that is on your computer.

### **5 WEB BEACONS**

Our website(s) may contain electronic image requests (called a single-pixel gif or web beacon request) that allows us to count page views and to access cookies. Any electronic image viewed as part of a webpage (including an ad banner) can act as a web beacon. Our web beacons do not collect, gather, monitor or share any of your personal information. We merely use them to compile anonymous information about our website.

### **6 COLLECTING INFORMATION FROM YOUR BROWSER**

We automatically receive and record Internet usage information on our server logs from your browser, such as your Internet Protocol address (IP Address), browsing habits, click patterns, version of software installed, system type, screen resolution, colour capabilities, plug-ins, language settings, cookie preferences, search engine keywords, JavaScript enablement, the content and pages that you

access on the website, and the dates and times that you visit the website, paths taken, and time spent on sites and pages within the website (usage information). Please note that other websites visited before entering our website might place personal information within your URL during a visit to it, and we have no control over such websites. Accordingly, a subsequent website collects URL information may log some personal information.

## **7 CLOSE CIRCUIT TELEVISION (CCTV) FOOTAGE**

We use CCTV monitoring to assist in protecting the company's employees and property. CCTV monitoring is only used to monitor public areas in the company. The information from the CCTV monitoring is only used for security and law enforcement, and to ensure public safety.

The use of CCTV to monitor public areas will be done in a way that does not violate the rights of anyone who enters the company's public areas. By entering any of the Guardrisk or Momentum Group buildings, you consent to being recorded.

The information and images collected from CCTV monitoring will be kept in a secure manner and only people who are authorised will have access. The images and information collected by the CCTV belongs to the company.

## **8 LOCATION SERVICES**

We use location services for specific products and services through our websites and applications. The location services will only be switched on with the prior consent of the user. The use of location services is set out in the purpose of collection of data.

## **9 CONFIDENTIALITY AND SECURITY**

### **9.1 Routine Precautions**

Guardrisk and the Momentum Group has physical, technological and procedural security safeguards in place and will use its best endeavours to protect your personal information.

Personal information refers to information that identifies or relates specifically to you, which for example include:

- Your name
- Age

- Gender
- Identity number
- Your assets and liabilities
- Your income
- Your employment details
- Payment records
- Your contact details
- Your marital status
- Family information
- Bank account information
- Medical or health information
- Fitness activity data
- Your policy information

Any information about what you buy, where you shop, where you bank, how you invest, your health behaviour, your health transactions and all related information will also be regarded as personal information.

In short, any information that we know about you will be regarded as your personal information.

## **10 YOUR PERSONAL INFORMATION**

### **10.1 Securing personal information**

Guardrisk will take all reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information. The company will store all the personal information in secured environments, for example on secured servers in a protected data centre.

### **10.2 Managing Data Privacy at Guardrisk Group Board Level and Reporting Frequency**

The Guardrisk Group Audit and Risk Committee (ARC) is a sub-committee of the Board that is accountable to address and manage the risk of data privacy and cyber security. The ARC follows the board cycle and convenes on a quarterly basis. The Guardrisk Group Chief Risk Officer is the risk representative on ARC for data privacy, data security and cyber security through the support of the Momentum Group Chief Privacy Officer. The Guardrisk Group Chief Operating Officer provides guidance and input regarding appropriate business risk management.

### **10.3 Employee Training on Cyber Security and Data Privacy**

Employee Training on Cyber Security and Data Privacy forms part of ongoing compliance training. Cyber Security training is currently further required as a basic compliance training that all employees must complete. As part of the Data Privacy management, there is a specific focus on training, awareness as well as communication that will cover data privacy, data security and more detailed cyber security training as mandatory compliance training to all staff. The POPIA management programme is actively managed at Momentum Group level with participation of all business entities and subsidiaries of Momentum Group, including Guardrisk.

### **10.4 Centralised Cyber Security and Data Security Functions and Coordination**

To deal with Cyber Security and Data Privacy, two separate centralised functions exist within Guardrisk. The IT Security environment includes managing cyber security as a capability and the Data Management environment deals with the aspects of data privacy and extended data security and privacy which is enabled through IT security.

These two functions report into the Group Exco and is coordinated to work closely together to ensure coordinated efforts to best deliver on the relevant requirements.

### **10.5 Third Parties**

We do not exercise control over affiliate parties' privacy policies - Personal information and third parties. Because we are not responsible for any representations or information or warranties or content on any website of an affiliate party (including websites linked to this website or websites facilitated by us), we do not exercise control over affiliate parties' privacy policies, and you should refer to the privacy policy of any such affiliate party to see how such party protects your privacy.

### **10.6 Sharing your Information**

Your privacy is important to us. We will therefore not sell, rent or provide your personal information to unauthorised entities or other third parties, for their independent use, without your consent or the execution of the contract between Guardrisk and yourself requires us to do so.

We may disclose your personal information to the following third parties:

- Other companies in the Guardrisk Group of companies.
- Reinsurers.
- Underwriting management agencies.

- Binder holders.
- Cell owners.
- Loss adjusters.
- Claims assessors.
- Medical practitioners.
- Legal advisers.
- Investigators.
- Fraud prevention organisations.
- Service providers supporting policy administration and claims administration.
- Selected third parties to provide us with services, including companies that provide us with technical support and assistance in respect of the website, companies that provide back-office services, companies that provide hosting services or, that track the website's activities and analytics, and companies engaged to market and distribute Guardrisk Group products and/or services and conduct research on our behalf.
- Professional advisers, judicial, regulatory and law enforcement bodies; and
- A third party that acquires all or part of our assets or shares, or that succeeds us in carrying on all or a part of our business, whether by merger, acquisition, re-organisation or otherwise.
- In order for us to ensure that we meet your needs, we may collect and analyse your personal information and combine all the information that we have about you to compile a profile of you in order for us to personalise and tailor our services to meet your specific needs.
- Once we have collected and analysed your personal information, we may send you promotional material or details which we think may be of interest to you. If any of this promotional information relates to products, promotions, news or services of an affiliate party, and if you indicate that you would like more details, we may inform the affiliate party to contact you directly. We will, however, only inform an affiliate party to contact you directly if you have indicated that this is agreeable to you.

If at any stage, after you have given us your consent, you no longer wish us to use or share your personal information with an affiliate party; you may at any stage withdraw your consent. By choosing to withdraw your consent with affiliated third parties there may be an impact on our offering to you, and it will be explained to you on your request to withdraw your consent.

In any scenario, we will satisfy ourselves that we have a lawful basis on which to share the information and we will document our decision making. Should access to your information be requested in terms

of the Promotion of Access to Information Act. No. 2 of 2000 ("PAIA"), we will notify you of such request in accordance with the terms of PAIA.

On rare occasions, we may be required to disclose your Personal Information due to legal or regulatory requirements. In such instances, we reserve the right to disclose your Personal Information as required in order to comply with our legal obligations, including but not limited to complying with court orders, warrants, subpoenas, service of process requirements or discovery requests.

We may also disclose data about our users to law enforcement officers or others, in the good faith belief that such disclosure is reasonably necessary to enforce this Privacy Policy, respond to claims that any content violates the rights of third-parties, or protect the rights, property, or our personal safety or the personal safety of our employees, clients or the general public.

### **10.7 Cross Border Sharing**

We will only transfer your personal information to third parties in another country in any one or more of the following circumstances:

- Where your personal information will be adequately protected under the other country's laws or an agreement with the third-party recipient; and/or
- Where the transfer is necessary to enter into, or perform, under a contract with you or a contract with a third party that is in your interest; and/or
- Where you have consented to the transfer; and/or
- where it is not reasonably practical to obtain your consent, and the transfer is in your interest. This transfer will happen within the requirements and safeguards of the law.
- Where possible, the party processing your personal information in the other country will agree to apply the same level of protection as available by law in your country, or if the other country's laws provide better protection, the other country's laws would be agreed to and applied.
- An example of us transferring your personal information to another country would be when you make payments if you purchase goods or services in a foreign country.

**PLEASE NOTE:** As the Guardrisk Group operates in several countries, your personal information may be shared within the Guardrisk Group entities in other countries and processed in those countries in order to deliver on the contractual obligations.

## 10.8 Communication through digital channels

Guardrisk may communicate with clients, policyholders, brokers, intermediaries and service providers through approved digital communication platforms including email, WhatsApp, portal services and collaboration platforms.

Such communications may involve the processing of personal information necessary to provide services and support legitimate business activities.

Users remain responsible for protecting access to their own devices and accounts.

## 11 RIGHTS OF DATA SUBJECTS

You have the ability to exercise your rights in terms of POPIA by visiting our website [here](#) and scroll down to “Online POPIA Request”. By clicking on the “Online POPIA Request” button, you can follow the prompts and submit your requests in terms of the below, please ensure that you select Guardrisk as your product.

In terms of data privacy laws, you have certain rights including the right to –

- review, or request access or copies of your Personal Information which is within our custody and control together with details about how we use that information. If you think any of the Personal Information that we hold about you is inaccurate, you may also request that we correct or rectify it;
- in certain circumstances, to require us to stop processing your Personal Information;
- to request that we delete or erase Personal Information in certain circumstances (such as in accordance with local data retention legal obligations);
- withdraw any consent to processing that you have given us and prevent further processing if there is no other legitimate ground upon which we can process your Personal Information;
- restrict processing: you can require certain Personal Information to be marked as restricted for processing in certain circumstances;
- data portability i.e., you can ask us to transmit the Personal Information that you have provided to us to a third party;
- object to automated decision-making, including profiling; and
- lodge a complaint with the relevant data protection regulator if you think we are in breach of any applicable data protection legislation.

In relation to all of these rights, please email us at the email address set out in paragraph 14 below. Please note that we may, where permitted under applicable law, charge a small administrative fee and/or request proof of identity. We will respond to your requests within all applicable timeframes.

In certain circumstances (for example where required or permitted by law), we might not be able to provide you with access to some of your Personal Information, but where appropriate we will notify you of the reasons for this. You have the right to be informed in writing by the company in writing as soon as reasonably possible of any breach or suspected breach. The notification must contain enough information to allow the data subject to take protective measures against the potential consequences of the breach.

You also have a duty to inform us of any changes to your personal information; it is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relation with us.

## **12 CHANGES TO PRIVACY POLICY**

Perusing amendments to the policy. Our right to amend this Privacy Policy. We reserve the right, in our sole discretion to amend (including without limitation, by the addition of new terms and conditions) this Privacy Policy from time to time. You agree to review the Privacy Policy whenever you visit this website for any such amendments. Save as expressly provided to the contrary in this Privacy Policy, the amended version of the Privacy Policy shall supersede and replace all previous versions thereof.

## **13 WHICH LAWS APPLY?**

This Privacy Policy will be governed by and construed and interpreted in accordance with the laws of South Africa. To the extent that a court has jurisdiction over any dispute which may arise out of or in connection with this Privacy Policy, we both submit to the jurisdiction of the South African courts.

## 14 GET IN TOUCH - COMPLIMENTS OR REQUESTS

Contact details of the POPIA Information Officer of Momentum Group

|                                 |                                                 |
|---------------------------------|-------------------------------------------------|
| Name of the Information Officer | Jeanine Norden                                  |
| Postal Address                  | PO BOX 7400<br>Centurion<br>0046                |
| Physical Address                | 268 West Ave<br>Die Hoewes<br>Centurion<br>0157 |
| Email Address                   | dataprivacy@mmltd.co.za                         |

General contact details of Momentum Group

|                   |                                                 |
|-------------------|-------------------------------------------------|
| Postal Address    | PO BOX 7400<br>Centurion<br>0046                |
| Physical Address  | 268 West Ave<br>Die Hoewes<br>Centurion<br>0157 |
| Telephone Number  | +27 (0) 12 065 0445                             |
| Internet site URL | www.momentumgrouppltd.co.za                     |

Contact details of the POPIA Deputy Information Officer of Guardrisk

|                                        |                                                            |
|----------------------------------------|------------------------------------------------------------|
| Name of the Deputy Information Officer | Nalisha Sivanarain                                         |
| Postal Address                         | PO BOX 786015<br>Sandton<br>2146                           |
| Physical Address                       | The Marc<br>Tower 2<br>129 Rivonia Road<br>Sandton<br>2196 |
| Email Address                          | dataprivacy@mmltd.co.za                                    |

General contact details of Guardrisk

|                   |                                                                 |
|-------------------|-----------------------------------------------------------------|
| Postal Address    | PO BOX 786015<br>Sandton<br>2146                                |
| Physical Address  | The Marc<br>Tower 2<br>129 Rivonia Road<br>Sandton<br>2196      |
| Telephone Number  | +27 (0) 11 669 1000                                             |
| Internet site URL | <a href="https://guardrisk.co.za/">https://guardrisk.co.za/</a> |

## 15 COMPLAINTS

Should you believe that Guardrisk has utilised your personal information contrary to Applicable Laws, you undertake to first attempt to resolve any concerns with Guardrisk. If you are not satisfied with such process, you may have the right to lodge a complaint with the Information Regulator, using the contact details listed below:

The Information Regulator (South Africa)

Woodmead North Office Park

54 Maxwell Drive

Woodmead

Johannesburg

2191

Phone: 010 023 5200 or (tollfree) 0800 017 160

Complaints email: [POPIAComplaints@inforegulator.org.za](mailto:POPIAComplaints@inforegulator.org.za)

General enquiries email: [enquiries@inforegulator.org.za](mailto:enquiries@inforegulator.org.za)

Website: <https://inforegulator.org.za/>