



BUILDING WEALTH,
CHANGING LIVES

PUBLIC PRIVACY (POPIA) POLICY

CONTENTS

1.	PURPOSE.....	2
2.	SCOPE	2
3.	DEFINITIONS.....	3
4.	OBJECTIVES.....	4
5.	POLICY	4
6.	PRINCIPALS OF PROTECTION OF PERSONAL INFORMATION	5
7.	COOKIE POLICY	11
8.	LOCATION SERVICES.....	11
9.	SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION.....	11
10.	SHARING OF YOUR PERSONAL INFORMATION AND THIRD PARTIES	13
11.	GOVERNING LAW	15
12.	DOCUMENT CONTROL.....	15
13.	RECORD OF PROCESSING, RETENTION AND DISPOSAL OF PERSONAL INFORMATION .	15
14.	ROLES AND RESPONSIBILITIES	15
14.1.	INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER.....	15
14.2.	HEADS OF DEPARTMENTS	16
14.3.	EMPLOYEES	16
15.	MONITORING AND ENFORCEMENT.....	17
16.	GET IN TOUCH.....	17
17.	COMPLAINTS PROCEDURE.....	18

1. PURPOSE

- 1.1. This Policy governs the manner in which ASI collect, use, share and otherwise process your Personal Information, in line with POPIA.
- 1.2. ASI provides, among others, the following products, and services:
 - 1.2.1. Advisory Services;
 - 1.2.2. Advanced Analytics;
 - 1.2.3. Claims Processing;
 - 1.2.4. Claims Administration;
 - 1.2.5. Financial services;
 - 1.2.6. Health benefits;
 - 1.2.7. Loyalty rewards and benefits;
 - 1.2.8. Short-term and long-term Insurance products;
 - 1.2.9. Investment management services;
 - 1.2.10. Insights and Research;
 - 1.2.11. Administrative/Intermediary Services for Brokerages;
 - 1.2.12. Employee Benefits Advisory and Intermediary Services;
 - 1.2.13. Wellness services; and
 - 1.2.14. Consulting services.
- 1.3. ASI respect your privacy and your Personal Information and for this reason, ASI 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.
- 1.4. ASI will maintain the confidentiality of your Personal Information and comply with the POPIA when processing your Personal Information. ASI briefly outline these principles below:
 - 1.4.1. ASI will only collect, disclose, collate, process 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;
 - 1.4.2. ASI will disclose in writing, the specific purpose for which ASI use, request, and store your Personal Information. ASI will also keep a record of that Personal Information and the specific purpose for which ASI collect it in accordance with the FAIS Act which is a period of 5 (five) year after termination of services.

2. SCOPE

- 2.1. ASI is obliged to inform its Data Subjects as to how their Personal Information is used, disclosed, and destroyed.
- 2.2. ASI guarantees its commitment to protecting its Data Subjects' privacy and ensuring their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.
- 2.3. This Policy applies to all Personal Information processed by, or on behalf of ASI.

3. DEFINITIONS

- 3.1. **"ASI"** means ASI Group of companies who are bound by this policy, its subsidiaries and associated companies;
- 3.2. **"Data Subject/s"** means, for the purpose of this policy, Clients and or prospective clients of ASI;
- 3.3. **"Direct Marketing"** means to approach/contact a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – promoting or offering to supply, in the ordinary course of business, any goods or service to the Data Subject; or requesting a donation of any sort and for any reason from the Data Subject;
- 3.4. **"FAIS"** means, the Financial Advisory and Intermediary Services Act 37 of 2002;
- 3.5. **"Information Officer"** means the head of a private body as contemplated in Section 1, contained in PAIA;
- 3.6. **"PAIA"** means Promotion of Access to Information Act 2 of 2000;
- 3.7. **"Personal Information"** is all information that relates to an identifiable Data Subject. It carries the same definition as Personal Information contained in POPIA being "Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to – information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language and birth of the person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that would reveal the contents of the original correspondence; the views or opinions of another individual regarding the person; and 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";
- 3.8. **"POPIA"** means the Protection of Personal Information Act no 4 of 2013; and
- 3.9. **"Policy"** means this POPIA Policy;

Any other words used in this Policy which are defined in POPIA carries the same meaning in this Policy as in POPIA.

4. OBJECTIVES

- 4.1. This Policy sets out how ASI deals with its Data Subjects' Personal Information and in addition for what purpose said information is used for. This Policy is made available via a publicly access link from our website.
- 4.2. ASI acknowledges that it is mandatory to comply with the provisions of POPIA. . There are eight (8) conditions that shall apply, and which are relevant for the lawful processing of Personal Information:
 - 4.2.1. Accountability;
 - 4.2.2. Processing limitation;
 - 4.2.3. Purpose specification;
 - 4.2.4. Further processing limitation;
 - 4.2.5. Information quality;
 - 4.2.6. Transparency (honesty and integrity); and
 - 4.2.7. Security safeguards; and Data Subject participation.

5. POLICY

- 5.1. In South Africa, the right to privacy is protected in terms of the common law and section 14 of the 1996 Constitution. As with all rights in the Bill of Rights, none are absolute, and can be limited in terms of laws of general application. While the Constitution provides for, among other rights, the right to privacy, the extent of the right to privacy may be limited by application of laws such as PAIA and the Regulation of Interception of Communications and Provision of Communication-related Information Act, 70 of 2002 ("RICA").
- 5.2. Other laws such as the Electronic Communications Act, 25 of 2002, the National Credit Act, 34 of 2005 and the Consumer Protection Act, 68 of 2008, all provide further protection for privacy and confidentiality.
- 5.3. POPIA requires all South African organisations which handle Personal Information, to comply with several important principles regarding privacy, disclosure and trans-border flows of Personal Information to other countries. POPIA places responsibilities on ASI to process Personal Information that it holds, in a fair and proper manner. The processing of such information includes the collection, recording, organising, storage, updating or modification, retrieval, consultation, disclosure, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, including inaccessibility, erasure or destruction of Personal Information.
- 5.4. This Policy sets out ASI's compliance to POPIA.

6. PRINCIPALS OF PROTECTION OF PERSONAL INFORMATION

- 6.1. What is personal information?
 - 6.1.1. 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:
 - 6.1.1.1. Your marital status (married, single, divorced etc.); your national origin; your age; your language; birth; education;
 - 6.1.1.2. Your financial information, which may include your financial history and information (e.g., your income or your buying, investing, and banking behaviour based on, amongst others, account transactions);
 - 6.1.1.3. Your identifying number(s) (an account number, identity number or passport number etc.);
 - 6.1.1.4. Your e-mail address; location information; physical address (residential address, work address or your physical location); and telephone number (including your cellular number, home landline or office work number);
 - 6.1.1.5. Your online identifiers such as social media profiles;
 - 6.1.1.6. Your biometric information (e.g., fingerprints, face recognition, signature, or voice);
 - 6.1.1.7. Your race and/or gender;
 - 6.1.1.8. Your physical health; mental health; well-being; disability; religion; belief; conscience; culture;
 - 6.1.1.9. Your medical history (HIV / AIDS status or any other medical history disclosed or obtained); criminal history; employment history;
 - 6.1.1.10. Your personal views, preferences, and opinions;
 - 6.1.1.11. Your confidential correspondence; and / or
 - 6.1.1.12. Another's views or opinions about you and your name also constitute your Personal Information.
 - 6.2. What is special personal information?
 - 6.2.1. Special Personal Information is Personal Information about the following:
 - 6.2.1.1. Your religious and your philosophical beliefs (for example where you enter a competition, and you are requested to express your philosophical view);
 - 6.2.1.2. Your race (such as where you apply for a product or service where the statistical information must be recorded);
 - 6.2.1.3. Your ethnic origin;
 - 6.2.1.4. Your trade union membership;
 - 6.2.1.5. Your political beliefs;
 - 6.2.1.6. Your health (such as when you apply for an insurance policy or medical/health related products);
 - 6.2.1.7. Your biometric information (to verify your identity); and / or
 - 6.2.1.8. Your criminal behaviour and alleged commission of an offence (e.g., to prevent money laundering as required by law or when you apply for employment or enter into a relationship with us).
 - 6.3. How does ASI collect personal information?
 - 6.3.1. ASI may collect and process the Data Subject's Personal Information as defined in POPIA.
 - 6.3.2. The type of information will depend on the nature of the relationship with the Data Subject and the purpose for which the information is collected and used.
 - 6.3.3. Personal Information will be processed for those purposes only.
 - 6.3.4. Whenever possible, ASI will inform the relevant Data Subject what information they are required to provide to us and what information is optional.

6.3.5. ASI collects information either directly from you, the Data Subject, the employer or through financial services providers such as insurers, underwriting managers or intermediaries. In certain instances, ASI 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.

6.4. What type of personal information does ASI collect?

6.4.1. Personal Information collected by ASI include but are not limited to:

- 6.4.1.1. a Data Subject's name;
- 6.4.1.2. contact number and/or details;
- 6.4.1.3. birth date;
- 6.4.1.4. identity number;
- 6.4.1.5. gender;
- 6.4.1.6. employment details;
- 6.4.1.7. Marital status;
- 6.4.1.8. Family information;
- 6.4.1.9. Policy information;
- 6.4.1.10. location information;
- 6.4.1.11. online identifier;
- 6.4.1.12. bank account details;
- 6.4.1.13. medical or health information; and
- 6.4.1.14. any other information required by ASI to achieve the specified purpose.

6.4.2. When Personal Information is collected, ASI will indicate the purpose for the collection and whether the information required is compulsory or voluntary.

6.5. Lawful Basis Of Collecting Personal Information

6.5.1. ASI may, when required, handle what the POPIA classifies as 'special information', detailing Data Subjects' information such as ethnicity, race, and biometric data in some instances. This data is subject to strict controls, and therefore, ASI is required to adhere to the Act and protect this information efficiently:

- 6.5.1.1. Purpose Limitation - Personal data may only be used for the specific purpose for which it has been initially collected. Subsequent use for other purposes must be compatible with this primary purpose;
- 6.5.1.2. Proportionality - Processing of personal data may not be excessive in relation to the objective pursued by ASI. Data may be collected only to the extent required;
- 6.5.1.3. Direct Collection - Personal data must generally be collected directly from the Data Subject;
- 6.5.1.4. Transparency - The Data Subject must be aware what personal data is processed for which purpose and who is responsible for it;
- 6.5.1.5. Data Quality - Personal data must be collected correctly. Appropriate measures must be taken so that irrelevant or incomplete data is corrected or deleted;
- 6.5.1.6. Security - Appropriate technical and organizational measures must be taken to protect personal data against unauthorized access, accidental loss or destruction and other forms of unlawful processing. Data may be accessible only by persons who have a "need to know"; and
- 6.5.1.7. Deletion - Personal Data that is no longer required must be deleted. The period of time after which data is to be deleted shall be defined and the actual deletion must be ensured. The storage for an indefinite period is not permissible.

- 6.6. When will ASI process your personal information?
 - 6.6.1. ASI will only process your Personal Information for lawful purposes relating to our business if the following conditions are met:
 - 6.6.1.1. The Data Subject consents to the processing – consent is obtained directly from the Data Subject;
 - 6.6.1.2. A person legally authorised by the Data Subject, the law, or a court, has consented thereto;
 - 6.6.1.3. The Personal Information is subject to a contract concluded between the parties or such information is in the public domain;
 - 6.6.1.4. Processing complies with an obligation imposed by law on ASI in respect of but not limited to:
 - 6.6.1.4.1. Protection of Personal Information Act 4 of 2013;
 - 6.6.1.4.2. Electronic Communications Act 25 of 2002 as amended;
 - 6.6.1.4.3. Promotion of Access to Information Act 2 of 200 as amended;
 - 6.6.1.4.4. Income Tax Act 58 of 1962 as amended;
 - 6.6.1.4.5. Value Added Tax Act 89 of 1991 as amended;
 - 6.6.1.4.6. Companies Act 78 of 2008 as amended; and/r
 - 6.6.1.4.7. Any other act or regulation ASI may be governed by.
 - 6.6.1.5. Processing protects a legitimate interest of clients so that ASI can respond to their needs on a timeous basis and provide them with a beneficial service and protection;
 - 6.6.1.6. Processing protects a legitimate interest of suppliers so that ASI can provide them with business opportunities on a timeous basis and relevant information; and
 - 6.6.1.7. Processing protects a legitimate interest of Employees to enable ASI to provide them with the necessary services and protection.
- 6.7. When will ASI process your special personal information?
 - 6.7.1. ASI may process your special Personal Information in the following circumstances:
 - 6.7.1.1. If the Data Subject has consented to the processing thereto.;
 - 6.7.1.2. If the processing is needed to create, use, or protect a right or obligation in law;
 - 6.7.1.3. If the processing is for statistical or research purposes;
 - 6.7.1.4. If the special Personal Information was made public by the Data Subject;
 - 6.7.1.5. If the processing is required by law;
 - 6.7.1.6. If racial information is processed and the processing is required to identify the Data Subject; and/or
 - 6.7.1.7. If health information is processed, and the processing is to determine the Data Subject's financial services risk, or to comply with financial services policy, or to enforce a financial service right or obligation.
- 6.8. Reasons For Processing Your Personal Information
 - 6.8.1. ASI will process your Personal Information for the following reasons:
 - 6.8.1.1. Payment processing on behalf of services providers, merchants, banks, and other persons that assist with the processing of your premium payment instructions;
 - 6.8.1.2. Insurers, intermediary/brokers, other financial institutions, or other organisations that assist with financial services underwriting, the providing of financial services financial services policies and value-add products, the assessment of financial services financial services claims, and other related purposes;
 - 6.8.1.3. Law enforcement and fraud prevention agencies, and other persons tasked with the prevention and prosecution of crime;

- 6.8.1.4. Regulatory authorities, industry ombudsmen, government departments, and local and international tax authorities;
- 6.8.1.5. Credit bureaux;
- 6.8.1.6. Trustees, executors, or curators appointed by a court of law;
- 6.8.1.7. Cheque verification service provider;
- 6.8.1.8. Our service providers, agents, and sub-contractors such as couriers and other persons we use to offer and provide products and services to you;
- 6.8.1.9. Courts of law or tribunals;
- 6.8.1.10. Participating partners, whether retail or online, in our client loyalty reward programmes;
- 6.8.1.11. Our joint venture partners;
- 6.8.1.12. Marketing list providers;
- 6.8.1.13. To process payment instruments (such as a cheque) and payment instructions (such as a debit order or a stop order deduction);
- 6.8.1.14. To conduct affordability assessments, credit assessments and credit scoring (where applicable);
- 6.8.1.15. To open, manage and maintain your accounts/policies, contracts, agreements, or relationship with us;
- 6.8.1.16. To disclose and obtain Personal Information from credit bureaux regarding your credit history;
- 6.8.1.17. To enable us to deliver goods, documents, or notices to you;
- 6.8.1.18. For security and identity verification, and to check the accuracy of your Personal Information;
- 6.8.1.19. To communicate with you and carry out your instructions and requests;
- 6.8.1.20. For client satisfaction surveys, events, promotional and other competitions;
- 6.8.1.21. For financial services, underwriting and administration;
- 6.8.1.22. To process or consider or assess financial services claims.
- 6.8.1.23. To provide financial services policies and products, and related services;
- 6.8.1.24. To enable you to participate in client loyalty reward programmes: determine your qualification for participation, rewards points, rewards level, and monitor your buying behaviour with our rewards partners to allocate the correct points or inform you of appropriate products, goods, and services you may be interested in, or to inform our reward partners about your purchasing behaviour;
- 6.8.1.25. To enable you to participate in and make use of value-added products and services;
- 6.8.1.26. To assess our lending and insurance risks;
- 6.8.1.27. Administrative needs;
- 6.8.1.28. Management of employees, client, and supplier relations;
- 6.8.1.29. For audit and record keeping purposes;
- 6.8.1.30. Compliance with internal policies and procedures, legal and regulatory requirements or when it is otherwise allowed by law;
- 6.8.1.31. Confirming, verifying, and updating Data Subjects' details;
- 6.8.1.32. For the detection and prevention of fraud, money laundering or other malpractice; and/or
- 6.8.1.33. For any other related purposes.

- 6.9. Processing Information Of A Child
 - 6.9.1. Protecting privacy of children – ASI takes the privacy of children very seriously. Children under the age of 18 years should obtain their guardian's consent before providing / submitting any Personal Information about themselves on the ASI website.
 - 6.9.2. We will not require children under this age to provide any Personal Information other than that which is reasonably necessary to use the ASI website.

- 6.9.3. If we determine that a user is under the age of 18, we will not use or maintain his/her Personal Information without the guardian's consent.
- 6.9.4. 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 following applies:
 - 6.9.4.1. A person with the ability to sign legal agreements has consented to the processing, being the parent or guardian of the child;
 - 6.9.4.2. 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;
 - 6.9.4.3. The child's Personal Information was made public by the child, with the consent of a person who can sign legal agreements;
 - 6.9.4.4. The processing is for statistical, or research purposes and all legal conditions are met;
 - 6.9.4.5. Where the child is an heir in a will, if required to give effect to the will;
 - 6.9.4.6. Where the child is a beneficiary of a trust, if required to give effect to the trust deed;
 - 6.9.4.7. Where the child is legally old enough to open a bank account without assistance from their parent or guardian;
 - 6.9.4.8. Where the child is legally old enough to sign a document as a witness without assistance from their parent or guardian;
 - 6.9.4.9. Where the child benefits from a bank account such as an investment or savings account; and/or
 - 6.9.4.10. Where the child is an insured person or beneficiary of an insurance policy, if required to give effect to the policy.
- 6.10. Obtaining Personal Information About Clients
 - 6.10.1. We collect information about you:
 - 6.10.1.1. Directly from you;
 - 6.10.1.2. Based on your use of our products, services, or service channels (such as our websites and applications);
 - 6.10.1.3. Based on how you engage or interact with us, such as on social media, and through e-mails, letters, telephone calls, and surveys;
 - 6.10.1.4. From public sources (such as newspapers); and
 - 6.10.1.5. From third parties for the purposes of conducting our business (such as partners, reward partners, preferred providers, our client loyalty rewards programmes' retail and online partners, or our service providers).
 - 6.10.2. 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:
 - 6.10.2.1. Members of the ASI 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;
 - 6.10.2.2. Your spouse, dependants, partners, employer, joint applicant or account holder and other similar sources;
 - 6.10.2.3. People you have authorised to share your Personal Information, such as a person that makes a car-hire booking on your behalf, or a medical practitioner;

- 6.10.2.4. Attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements;
 - 6.10.2.5. Payment processing services providers, merchants, banks, and other persons that assist with the processing of your premium payment instructions;
 - 6.10.2.6. Insurers, underwriting managers, intermediaries/brokers, other financial institutions, or other organisations that assist with financial services underwriting, the providing of financial services policies and products, the assessment of financial services claims, and other related purposes;
 - 6.10.2.7. Law enforcement and fraud prevention agencies, and other persons tasked with the prevention and prosecution of crime;
 - 6.10.2.8. Regulatory authorities, industry ombudsmen, government departments, and local and international tax authorities;
 - 6.10.2.9. Credit bureaux's;
 - 6.10.2.10. Trustees, executors, or curators appointed by a court of law;
 - 6.10.2.11. Our service providers, agents, and sub-contractors such as couriers and other persons we use to offer and provide products and services to you;
 - 6.10.2.12. Courts of law or tribunals;
 - 6.10.2.13. Participating partners, whether retail or online, in our client loyalty reward programmes;
 - 6.10.2.14. Our joint venture partners;
 - 6.10.2.15. Marketing list providers; and
 - 6.10.2.16. Digital data transformation or aggregation services which you have authorised to collect activity, health or other digital data streams and share with us.
- 6.11. Processing Information About Persons Related To A Juristic Person
- 6.11.1. 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, clients, guarantors, spouses of guarantors, sureties, spouses of sureties, other security providers and other persons related to the juristic person regarded as related persons for purposes of this Policy.
 - 6.11.2. 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.
 - 6.11.3. We will process the Personal Information of related persons as stated in this Policy, thus references to "you" or "your" in this Policy will include related persons with the necessary amendments.
- 6.12. Direct Marketing
- 6.12.1. If permission is given, ASI may use your personal or other information to tell you about products, services and special offers from ASI or other subsidiaries of ASI.
 - 6.12.2. We will use your Personal Information to market events, promotions, financial services and other related products and services to you. We will do this in person, by post, telephone, or electronic channels such as our website, our application, SMS, email, and fax.
 - 6.12.3. If you are not our client, or in any other instances where the law requires, we will only market to you by electronic communications with your consent.
 - 6.12.4. In all cases, you can tell us to stop sending marketing communications to you at any time by clicking the unsubscribe option on the correspondence sent to you or sending an e-mail to customerfeedback@asi.co.za

7. COOKIE POLICY

- 7.1. 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.
- 7.2. There are two main types of cookies, namely:
 - 7.2.1. Session cookies - these are cookies that are only active while you are visiting our site. When you close your browser, these cookies are deleted; and
 - 7.2.2. Persistent cookies – these are cookies that are stored on your device until they expire, or you choose to delete them. These cookies are sent back to us each time you visit our site.
- 7.3. We use cookies for session management, user device identification and classification, traffic routing, and analytics.
- 7.4. Your Personal Information is not at risk by the use of cookies. ASI will never save any Personal Information, including login details or other Personal Information on your electronic devices.
- 7.5. ASI's websites make use of cookies to enhance your web experience. The types of cookies we use, and the purpose thereof are described below. You will always be notified about our use of cookies and have the right to disable certain types or all cookies.
- 7.6. Clearing or disabling cookies may limit your website functionality, and your functionality once you have 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.

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. SECURITY AND CONFIDENTIALITY OF PERSONAL INFORMATION

- 9.1. Information Security
 - 9.1.1. ASI will take all reasonable technical and organisational precautions to prevent the loss, misuse, or alteration of your Personal Information. ASI will store all the Personal Information in secured environments, for example on secured servers in a protected data centre.
 - 9.1.2. ASI's information and communication technologies and systems are critical to ASI's operations. The reliance on such technologies and information (data) housed in such technologies are important to the ASI.

- 9.1.3. To ensure continuity and efficient recovery in the event of a failure of such technologies and resulting loss of said data, ASI has and will continue to engage specific service providers to implement recovery solutions.
- 9.1.4. These security measures are subject to the service providers undertaking to maintain the confidentiality of any Personal Information as defined in POPIA.
- 9.1.5. ASI is legally obliged to provide adequate protection for the Personal Information it holds and to stop unauthorised access and use of Personal Information. ASI will, on an ongoing basis, continue to review its security controls and related processes to ensure that its Data Subject's Personal Information is secure.
- 9.1.6. When ASI contracts with third parties, it imposes appropriate security, privacy, and confidentiality obligations on them to ensure that Personal Information that it remains responsible for, is kept secure.

9.2. How You Can Review And Correct Your Personal Information

- 9.2.1. Data Subjects have the right to access the Personal Information ASI holds about them, and you may request to review your Personal Information contained in ASI's records at any time to correct or update the information.
- 9.2.2. Data Subjects also have the right to request ASI to update, correct or delete their Personal Information on reasonable grounds.
- 9.2.3. If the purpose for which your Personal Information was requested initially does not exist anymore, (if for example you no longer have a contract with us), you may request information held by ASI to be removed. However, ASI can decline your request to delete the information from its records if other legislation requires the continued retention thereof or if it has been de-identified.
- 9.2.4. Once a Data Subject objects to the processing of their Personal Information, ASI may no longer process said Personal Information even though, for reasons described above, such information may continue to be stored on our systems.
- 9.2.5. Where a Data Subject objects to the processing of their Personal Information it may affect the validity of all other agreements between the parties where such processing is a material requirement in such agreements.
- 9.2.6. ASI will take all reasonable steps to confirm the Data Subject's identity before providing details of their Personal Information or making changes to their Personal Information.

9.3. Managing Data Privacy At ASI Board Level And Reporting Frequency

The ASI Executive Committee (EXCO) is a Board-appointed committee that is accountable to address and manage organisational risk, including the risk of data privacy and cyber security. The EXCO follows the board cycle and convenes on a monthly basis. The ASI Business Strategy and Planning Director as well as the Chief Financial officer are the business representatives on EXCO for data privacy, data security and cyber security and provides guidance and input regarding appropriate Risk Management.

- 9.4. Employee Training On Data Privacy And Cyber Security
 - 9.4.1. Employee Training on Cyber Security and Data Privacy forms part of ongoing compliance training.
 - 9.4.2. As part of the POPIA management programme, 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.
 - 9.4.3. The POPIA management programme is actively managed at ASI Group level with participation of all business entities and subsidiaries of ASI.

- 9.5. Centralised Cyber Security And Data Security Functions And Coordination
 - 9.5.1. To deal with Cyber Security and Data Privacy, two separate centralised functions exist within ASI. 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.
 - 9.5.2. These are coordinated to work closely together to ensure coordinated efforts to best deliver on the relevant requirements. ASI will 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.
 - 9.5.3. ASI will take responsible measures to:
 - 9.5.3.1. identify all reasonable predictable internal and external risks to Personal Information in its possession or under its management;
 - 9.5.3.2. establish and maintain appropriate safeguards against the risks identified;
 - 9.5.3.3. regularly verify that the safeguards are effectively implemented; and
 - 9.5.3.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguarding methods.
 - 9.5.4. ASI will 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.

- 9.6. Security Compromises
 - 9.6.1. 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 information officer should be contacted immediately.
 - 9.6.2. The information officer is required to notify the information regulator and the Data Subject.
 - 9.6.3. The notification of a breach of confidentiality should be declared as soon as is reasonably possible upon the discovery of the compromise.
 - 9.6.4. The information officer needs to provide sufficient information to the Data Subject which will enable the Data Subject to take protective measures against the potential consequences of the compromise.

10. SHARING OF YOUR PERSONAL INFORMATION AND THIRD PARTIES

- 10.1. Sharing Of Personal Information
 - 10.1.1. Your privacy is important to us. We will therefore make every attempt not sell, rent, or provide your Personal Information to unauthorised entities or other third parties, for their independent use, without your consent.

- 10.1.2. ASI may disclose Data Subjects Personal Information:
 - 10.1.2.1. Where ASI has a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect our rights;
 - 10.1.2.2. To ASI's suppliers and third-party service providers when necessary to perform any service;
 - 10.1.2.3. To other companies in the ASI Group of companies;
 - 10.1.2.4. To Professional advisers, judicial, regulatory and law enforcement bodies; and/or
 - 10.1.2.5. To a third party that acquires all or part of our assets or shares, or that succeeds ASI in carrying on all or a part of our business, whether by merger, acquisition, re-organisation or otherwise.
- 10.1.3. In order for ASI to ensure that ASI 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 ASI to personalise and tailor our services to meet your specific needs.
 - 10.1.3.1. Once ASI has collected and analysed your Personal Information, ASI may send you promotional material or details which we think may be of interest to you.; and
 - 10.1.3.2. 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, ASI may inform the affiliate party to contact you directly. ASI will, however, only inform an affiliate party to contact you directly if you have indicated that this is agreeable to you.
- 10.1.4. 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 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.
- 10.2. Third Parties
 - 10.2.1. ASI has agreements in place to ensure that our suppliers and third-party service providers comply with confidentiality and privacy conditions.
 - 10.2.2. ASI does not, however:
 - 10.2.2.1. Accept responsibility 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).
 - 10.2.2.2. 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.
- 10.3. Cross Border Sharing
 - 10.3.1. ASI will only transfer your Personal Information to third parties in another country in any one or more of the following circumstances:
 - 10.3.1.1. Where your Personal Information will be adequately protected under the other country's laws or an agreement with the third-party recipient;
 - 10.3.1.2. 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;
 - 10.3.1.3. Where you have consented to the transfer;
 - 10.3.1.4. Where it is not reasonably practical to obtain your consent, and the transfer is in your interest;
 - 10.3.1.5. This transfer will happen within the requirements and safeguards of the law; and
 - 10.3.1.6. 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.

11. GOVERNING LAW

This 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 Policy, all parties submit to the jurisdiction of the South African courts.

12. DOCUMENT CONTROL

We reserve the right, in our sole discretion to amend (including without limitation, by the addition of new terms and conditions) this Policy on an ad hoc basis. You are advised to check the Policy periodically 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. RECORD OF PROCESSING, RETENTION AND DISPOSAL OF PERSONAL INFORMATION

- 13.1. All Personal Information that is collected will be for a specific legal purpose, in accordance with the principles set out this policy.
- 13.2. The 'ASI Information Retention and Disposal Policy' provides guidance on how information will be stored, how long it will be retained for and under what circumstances information should be disposed of or destroyed and the methods that will be used.
- 13.3. The specific purpose for collection and the nature of processing will be identified through one or more of the following mechanisms:
 - 13.3.1. A signed agreement which records such details and the Data Subject's consent; and
 - 13.3.2. An electronic mechanism to record the processing reasons, storage, retention and disposal.

14. ROLES AND RESPONSIBILITIES

- 14.1. Information Officer And Deputy Information Officer
 - 14.1.1. The Information and Deputy Information Officers are responsible for:
 - 14.1.1.1. ensuring that ASI has a POPIA compliance program in place and that all employees and operators, service providers, contractors and agents acting for or on behalf of ASI are aware of this Policy and their obligations in relation to the POPIA compliance program;
 - 14.1.1.2. maintaining notification with the Regulator;
 - 14.1.1.3. handling Data Subject access requests and requests from third parties for Personal Information;
 - 14.1.1.4. promoting and maintaining awareness of POPI and regulations, including training; and
 - 14.1.1.5. investigating losses and unauthorised disclosures of Personal Information.

14.2. Heads Of Departments

14.2.1. The Heads of Department / Business Units are responsible for:

- 14.2.1.1. ensuring their employees and where applicable all operators, service providers, contractors and agents acting for or on behalf of ASI understand the role of the POPIA conditions in their day-to-day work, through onboarding, training, and performance monitoring, and for monitoring compliance within their own areas of responsibility;
- 14.2.1.2. advise employees and where applicable Operators, service providers, contractors and agents acting for or on behalf of ASI in their departments on the implementation of and compliance with POPIA and this Policy and any associated guidance / codes of practice;
- 14.2.1.3. ensure appropriate technical and organisational measures are taken within their departments to ensure against unauthorised or unlawful processing of Personal Information and against accidental loss or destruction of, or damage to, Personal Information;
- 14.2.1.4. keep the Information Officer and Deputy Information Officers informed of changes in the collection, use, and security of Personal Information within their department;
- 14.2.1.5. report any loss of Personal Information to the Information and Deputy Information Officer; and
- 14.2.1.6. ensure the proper completion of all POPI consent forms.

14.3. Employees

14.3.1. The Employees are responsible for:

- 14.3.1.1. processing Personal Information in accordance with POPIA, the POPIA conditions for processing, and any guidelines and instructions issued by ASI from time to time;
- 14.3.1.2. ensuring that they only process Personal Information, which is relevant and accurate and only for the purpose for which it is required;
- 14.3.1.3. ensuring that all special Personal Information will only be processed in line with the provisions set out under POPIA and in accordance with instructions set out by the Information Officer from time to time;
- 14.3.1.4. ensuring that all Personal Information and all records housing such Personal Information are safely retained, stored and archived and/ or destroyed when no longer required;
- 14.3.1.5. complying with all security and monitoring measures to safeguard and protect any Personal Information which he or she may be in possession of;
- 14.3.1.6. ensuring that any transfer of Personal Information to third parties is authorised, lawful and that appropriate and safe transport mechanisms are employed in respect of the Personal Information so transferred such as encryption;
- 14.3.1.7. ensuring that only authorised downloading of electronic Personal Information onto portable devices or the removal of manual Personal Information from our premises, occurs;
- 14.3.1.8. raising any concerns in respect of the processing of Personal Information with the Information Officer or Deputy Information Officer;
- 14.3.1.9. promptly passing on to the Information Officers, all Data Subject access requests and requests from third parties for Personal Information;
- 14.3.1.10. reporting losses or unauthorised disclosures of Personal Information to the Information Officer;
- 14.3.1.11. ensure the Personal Information they provide about themselves is up to date; and
- 14.3.1.12. not attempt to gain access to information that is not necessary to hold, know or process

15. MONITORING AND ENFORCEMENT

- 15.1. All employees will be responsible for the implementation of this policy including the supporting of guidelines, standard operating procedure, notices, consents and appropriate related documents and processes.
- 15.2. Employees who violate the guidelines and standard operating procedures of this policy may be subjected to disciplinary action, being taken against him/her.
- 15.3. Employees will be provided with at least annual POPIA training and will be kept informed of any changes to POPIA as and when required to ensure they remain informed.
- 15.4. The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the processing, collection, or re-identifying of Personal Information shall be directed to the information officer or deputy information officer(s).

16. GET IN TOUCH

The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the processing, collection, or re-identifying of Personal Information shall be directed to the information officer or deputy information officer(s).

CONTACT DETAILS OF THE INFORMATION OFFICER OF ASI

Name of the Information Officer	Benita Porobich
Postal Address	ASI Place, Turnberry Office Park, 48 Grosvenor Road, Bryanston, Sandton, 2191
Physical Address	ASI Place, Turnberry Office Park, 48 Grosvenor Road, Bryanston, Sandton, 2191
Email Address	Benita.Porobich@asi.co.za

GENERAL CONTACT DETAILS OF ASI

Postal Address	ASI Place, Turnberry Office Park, 48 Grosvenor Road, Bryanston, Sandton, 2191
Physical Address	ASI Place, Turnberry Office Park, 48 Grosvenor Road, Bryanston, Sandton, 2191
Telephone Number	+27 86 1 274 377
Internet site URL	www.asi.co.za

17. COMPLAINTS PROCEDURE

- 17.1. Data Subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. ASI takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:
 - 17.1.1. POPIA complaints must be submitted to the Information Officer in writing within a reasonable time of being made aware of the alleged infringement. The Information Officer will acknowledge the complaint within 3 (three) days of receipt thereof and provide the Data Subject with a "POPIA Complaint Form" as per POPIA Form 5;
 - 17.1.2. Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 (one) working day;
 - 17.1.3. The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA;
 - 17.1.4. The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the ASI's Data Subjects;
 - 17.1.5. Where the Information Officer has reason to believe that the Personal Information of Data Subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with ASI's Management Committee where after the affected Data Subjects and the Information Regulator will be informed of this breach depending on the agreed severity;
 - 17.1.6. The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to ASI's governing body within 6 ((six) weeks of receipt of the complaint. In all instances, ASI will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines;

17.1.7. The Information Officer's response to the Data Subject may comprise any of the following:

17.1.7.1. A suggested remedy for the complaint,

17.1.7.2. A dismissal of the complaint and the reasons as to why it was dismissed; and/or

17.1.7.3. An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

17.1.8. Where the Data Subject is not satisfied with the Information Officer's suggested remedies, the Data Subject has the right to file an appeal of the complaint with ASI or alternatively lay a complaint to the Information Regulator. Whose details are hereunder:

JD House, 27 Stiemens Street, Braamfontein, Johannesburg 2001

P. O Box 31533 Braamfontein Johannesburg 2017

Complaints e-mail: PAIAComplaints@inforegulator.org.za

POPIAComplaints@inforegulator.org.za

General enquiries e-mail: enquiries@inforegulator.org.za

17.1.9. The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

FOLLOW US ON
OUR CHANNELS

Scan the QR Code



Your Trusted Independent Employee Benefits & Insurance Advisor

+27 86 1 ASI FSP / +27 86 1 274 377

ASI, a group of authorised financial services providers

• Health • Wellness • Insure • Invest • Retire

BUILDING WEALTH, CHANGING LIVES