

Protection of Personal Information & Data Protection Policy Document

Version Control	Date	Author
1.0	30-06-2021	M. Besseling
Draft 0.1	04-05-2021	M. Besseling

Background and Applicability.....	3
Your Rights.....	4
Purpose of the Processing of Personal Information	5
For our clients:.....	5
For prospective clients:	5
For employees:.....	5
For vendors, suppliers, and other businesses:	5
Categories of Data Subjects and Categories of Personal Information	6
Clients or Prospective Clients (which may include employees and/or suppliers).....	6
Employees.....	6
Vendors/Suppliers/Other Businesses	7
Recipients of Personal Information.....	7
Condition 1: Accountability	8
Information Officer	9
Condition 2: Processing Limitation	10
Condition 3: Purpose Specification	11
Retention of Personal Information Records	11
Restriction of Personal Information Records	11
Condition 4: Further Processing Limitation	12
Condition 5: Information Quality.....	13
Condition 6: Openness.....	14
Documentation	14
Notification To Data Subject When Collecting Personal Information	14
Condition 7: Security Safeguards	15
Procedures.....	15
Information Security Measures	15
Operators and Data Processors.....	16
Security Compromises	16
Cross Border Transfers of Personal Information	16
Condition 8: Data Subject Participation	17
Objection to the Processing of Personal Information by a Data Subject.....	17
Request for Correction or Deletion of Personal Information	17
Appendix 1	18
Appendix 2	19

Background and Applicability

The Protection of Personal Information Act 4 of 2013 aims:

- to promote the protection of personal information processed by public and private bodies;
- to introduce certain conditions so as to establish minimum requirements for the processing of personal information;
- to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000;
- to provide for the issuing of codes of conduct;
- to provide for the rights of persons regarding unsolicited electronic communications and automated decision making;
- to regulate the flow of personal information across the borders of the Republic; and
- to provide for matters connected therewith.

A copy of the act can be obtained at the following link: <https://www.gov.za/documents/protection-personal-information-act>

Hypasurance Insurance Consultants (“the organisation”), as a company that gathers and processes personally identifiable information as part of our core business and is domiciled in the Republic of South Africa must comply with the provisions of this act.

When you interact with our organisation, either by doing business with us, communicating with us via telephone, fax or email, or visiting our website, the Act grants you certain rights that protect you from the misuse or improper handling of any of your personally identifiable information. In the language of the Act, you become a “data subject” and we, as the responsible party for any of these interactions, must detail the processes we have in place to handle your information, the safeguards we have implemented to protect that information, and the procedures we follow in the event of any breaches or improper access to your information.

As stipulated in the Act, the conditions for lawful processing of personal information by or for a responsible party are the following:

- “Accountability”, as referred to in section 8,
- “Processing limitation”, as referred to in sections 9 to 12,
- “Purpose specification”, as referred to in sections 13 and 14,
- “Further processing limitation”, as referred to in section 15,
- “Information quality”, as referred to in section 16,
- “Openness”, as referred to in sections 17 and 18,
- “Security safeguards”, as referred to in sections 19 to 22; and
- “Data subject participation”, as referred to in sections 23 to 25.

Your Rights

Section 5 of the Act stipulates that you as a data subject enjoy the following rights:

- You have the right to be notified that we are collecting your personal information, and for what purposes.
- You have the right to be notified when an unauthorised party accesses or acquires your information.
- You have the right to establish whether we hold any of your information, and what that information is.
- You have the right to request access to any of your personal information that we hold.
- You have the right to request that we correct, destroy or delete any of your information.
- You have the right to object, on reasonable grounds, to the processing and storage of your information.
- You have the right to, at any time, opt out of us using your personal information to market directly to you.
- You have the right to not be subjected to profiling through the automated processing of your personal information.
- You have the right to submit a complaint to the Regulator regarding any perceived interference or failure in the way we have protected your information.
- You have the right to institute civil proceedings regarding any perceived interference or failure in the way we have protected your information.

Purpose of the Processing of Personal Information

Your personal information may only be processed and stored for a specific purpose or purposes. These purposes are as follows:

For our clients:

- Performing duties in terms of any agreement we have with you as a client.
- Making, or assist in making, insurance decisions with you or regarding your insurance portfolio.
- Communicating with product providers/insurers on your behalf
- Communicating with contractually involved third parties, such as (but not limited to) managing agents, repair services, assessors, and towers.
- Communicating (including direct marketing) with you by email, SMS, letter, telephone or in any other way about our services, unless you have opted out from such communication.
- To analyse your insurance and investment needs so that we can tailor specific solutions to you.
- Carrying out market research, business, and statistical analysis.
- Performing other administrative and operational purposes including the testing of systems.
- Recovering any debt consumers may owe Hypasurance Insurance Consultants
- Complying with regulatory and other obligations we may have as a business, including but not limited to the requirements of the Financial Intelligence Centre Act 38 of 2001, the Financial Advisory and Intermediaries Services Act (FAIS Act) (Act 37 of 2002), the Financial Sector Regulation Act (Act 9 of 2017) and the Short-term Insurance Act (Act 53 of 1998).
- Any other reasonably required purpose relating to our business.

For prospective clients:

- Verifying and updating information.
- Submission of your information to selected product providers for the purposes of exploring insurance product or investment quotes or products.
- Direct marketing, except where you have opted out from receiving such marketing.
- Any other reasonably required purpose relating to the processing of a prospect's personal information reasonably related to the Adept Advisory's business.

For employees:

- Verification of applicant employees' information during recruitment process
- General matters relating to employees, such as for the purposes of administrating or facilitating legislative compliance, pension, medical aid, payroll, disciplinary action or training matters.
- Any other reasonably required purpose relating to the employment or possible employment relationship.

For vendors, suppliers, and other businesses:

- Verifying supplier information and performing checks.

- Purposes relating to the agreement or business relationship or possible agreement or business relationships between the parties.
- Payments.
- Complying with the organisation's regulatory and other obligations.
- Any other reasonably required purpose relating to our business.

Categories of Data Subjects and Categories of Personal Information

Clients or Prospective Clients (which may include employees and/or suppliers)

- postal and/or street address, and any documentary proof thereof.
- title and name.
- contact details, such as phone numbers and e-mail addresses.
- ethnic group.
- employment history.
- age.
- gender.
- marital status.
- nationality.
- language.
- financial information.
- identity details or passport number, and documentation relating thereto.
- bank account details, and documentation relating thereto.
- insurance history, such as previous policies you have held and claims you may have made.
- browsing habits and click patterns on our websites.
- correspondence relating your insurance and/or investment portfolio, and any correspondence relating to the management and administration of such portfolio.

Employees

- name and contact details.
- identity number and identity documents, including passports.
- employment history and references.
- banking and financial details.
- details of payments to third parties to facilitate salary deductions where applicable.
- employment contracts.
- employment equity plans.
- medical aid records.
- pension fund records.

- remuneration/salary records, including payslips.
- performance appraisals.
- disciplinary records.
- leave records.
- training records, and records relating to education and compliance with organisational regulatory obligations.

Vendors/Suppliers/Other Businesses

- name and contact details
- identity and/or company information and directors' information
- banking and financial information
- information about products or services
- payments made or received
- other information not specified, reasonably required to be processed for business operations

Recipients of Personal Information

For the purposes of doing business, Hypasurance Insurance Consultants may be required either contractually or legally to share your personal information – either internally or with other parties.

Notwithstanding the outlined purposes for which we may process and store your personal information, we also may share that information with the following types of parties:

- Any firm, organisation, or person that we use to collect payments and recover debts or to provide a service on its behalf.
- Any firm, organisation, or person that/who provides us with products or services.
- Any payment system we use to facilitate payments and manage the organisation's accounts.
- Regulatory and governmental authorities or ombudsmen, or other authorities, including tax authorities, where we have a duty to share such information.
- Third parties to whom payments are made on behalf of employees.
- Financial institutions from whom payments are received on your behalf.
- Employees, contractors, and temporary staff.
- Agents of the business.

These parties have an equal responsibility to protect your personal information, and you have the right to know who we share your personal information with, for what purposes, and to be supplied with any details you require to contact such party directly.

Condition 1: Accountability

Our organisation needs personal information relating to both individual and juristic persons in order to carry out its business and organisational functions. The way this information is processed and the purpose for which it is processed is determined by Hypasurance Insurance Consultants. We are therefore a Responsible Party for the purposes of POPI and will ensure that your personal information:

- is processed lawfully, fairly and transparently. This includes the providing you appropriate information when your data is collected by Hypasurance Insurance Consultants, in the form of privacy or data collection notices. We must also have a legal basis (for example, consent) to process personal information.
- is processed only for the purposes for which it was collected.
- will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- is adequate, relevant, and not excessive for the purposes for which it was collected.
- is accurate and kept up to date.
- will not be kept for longer than necessary.
- is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that personal information, in both physical and electronic form, are subject to an appropriate level of security when stored, used and communicated by Hypasurance Insurance Consultants, in order to protect against access and acquisition by unauthorised persons and accidental loss, destruction or damage.
- is processed in accordance with your rights, where applicable (see previous section).

The responsible party must ensure that the conditions set out in section 8 of the Act, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

Responsible Party

Name	Hypasurance Insurance Consultants (Pty) Ltd.
Telephone Number	+27 11 678 7564
Physical Address	53 Soutpans Avenue Fairlands 2030 Johannesburg South Africa
Postal Address	PO Box 73247 Fairlands 2030 Johannesburg South Africa
Dedicated Compliance Email Address	compliance@hypasurance.com

Information Officer

Name	Matthew-Isle Besseling
Physical Address	10 Swaeltjie Road Boskruin 2188 Johannesburg South Africa
Telephone Number	+27 72 829 7399
Email Address	matt@hypasurance.co.za
Position	Managing Director

Condition 2: Processing Limitation

Hypasurance Insurance Consultants will always ensure that we process your personal information in a way that is lawful, and in a reasonable manner that does not infringe on your privacy.

We will only process such information in a manner that is proportional to the purposes for which it was supplied, where such a manner is adequate, relevant, and not excessive to those purposes.

We will always request your consent to process your information; where we have received your information from a third party to facilitate our obligations in terms of a contract with you, we will ensure that such third party has received such consent.

You may withdraw your consent to us processing your personal information at any time. However, in such cases, this may prevent us from discharging our obligations in terms of any contractual responsibilities we have to you.

Condition 3: Purpose Specification

We only collect personal information for specifically defined lawful purposes. We have outlined these purposes in the above section titled “Purpose of the Processing of Personal Information”.

We will, prior to collecting such information or as reasonably soon afterwards, make you aware of the purpose of such collection.

For more information, please see Condition 6: Openness below.

Retention of Personal Information Records

As stipulated by the Act, in most cases your personal information must not be retained any longer than is required to facilitate the purpose for which that information was initially provided.

However, we also have legislative obligations that dictate how long we must keep such information, including cases where our contractual relationship may have ended.

Where your personal information was provided to us as part of our business relationship, we will normally store this data for 5 years after the termination of such relationship. However, there are some exceptions to this rule:

1. Where your information is part of a record of a transaction is under investigation or report submitted to the Financial Intelligence Centre.
2. Where your information forms part of an insurance portfolio or products, we will retain this information indefinitely for statistical, research, and historical purposes. In such cases we will endeavour to aggregate (“de-identify”) such information.
3. Where your information is in the form of correspondence with us in the form of email, we will retain these records for a longer period for historical record-keeping purposes.

When we destroy your personal information, we will do so in a manner that will prevent its reconstruction in any form.

Restriction of Personal Information Records

Access to your personal information is restricted, and only authorised employees of our business, other parties to your insurance and investment contracts, and our appointed data processors and service providers are allowed access to it.

In particular, in cases where we have retained your data for longer than the periods stipulated above, we will make sure that your information is securely stored.

For more information, please see Condition 7: Security Safeguards below.

Condition 4: Further Processing Limitation

We do not process your personal information once the original purpose of collecting such information has been fulfilled, except where such information has been aggregated and is no longer personally identifiable or where such processing is required to comply with legal, regulatory, or public health and safety purposes.

Condition 5: Information Quality

We will at all times take reasonably practicable steps to ensure the data we collect and subsequently process is accurate and complete.

Condition 6: Openness

Documentation

Section 17 of the Act stipulates as follows:

“A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section ... 51 of the Promotion of Access to Information Act. “

Section 51 of the Promotion of Access to Information Act indicates that all private bodies must compile and maintain a manual containing various details about the business, including a description of the records held by such body and sufficient detail to facilitate a request for access to a record of the body.

However, in terms of the Notice of 29 June titled “Promotion Of Access To Information Act, 2000 (Act No. 2 Of 2000): Exemption Of Certain Private Bodies From Compiling Manual”, Hypasurance Insurance Consultants is by nature of turnover and number of employees exempted from compiling such a manual until 31 December 2021.

Notwithstanding the above, most of our company records, policies and procedures are available on our website, or failing that, via email request.

Notification To Data Subject When Collecting Personal Information

When collecting your personal information (or as soon afterwards as is reasonably practicable), where a disclosure is not necessary in terms of the Act, we will furnish you with the following information:

- What information we require from you, or where we have collected your personal information from another party, the source of such information
- Our name and address
- The purpose of collecting your information
- Whether or not the supply of your information is voluntary or mandatory
- The consequence of not providing the requested information
- If any legal or regulatory reasons exist for requesting your information
- Further information such as the nature of the information, your further legal rights when supplying such personal information, and who in addition to us will receive it.

In cases where we have made such a disclosure to you before, and we require the same sort of information for the same purpose, we do not need to make such a disclosure again.

Condition 7: Security Safeguards

We will at all times secure the integrity and confidentiality of your personal information under our control by taking appropriate technical and organisation measures to prevent loss, damage or unauthorised destruction of and unlawful access to such information.

Procedures

Hypasurance Insurance Consultants will take steps to identify all reasonably foreseeable internal and external risks to your information and establish and maintain appropriate safeguards to these risks. These safeguards will be regularly verified and monitored to ensure that they are effectively implemented.

Information Security Measures

We undertake to institute and maintain the data protection measures to accomplish the following objectives outlined below. The details given are to be interpreted as examples of how to achieve an adequate data protection level for each objective. We may use alternative measures and adapt to technological security development, as needed, provided that the objectives are achieved.

Access Control of Persons

We shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the data are processed. All workstations are protected by passwords known only to the authorised operator themselves and other authorised persons (such as IT staff).

Data Media Control

We undertake to implement suitable measures to prevent the unauthorized manipulation of media, including reading, copying, alteration or removal of the data media used by Hypasurance Insurance Consultants and containing personal data of clients, prospective clients, employees, and suppliers.

Data Memory Control

We undertake to implement suitable measures to prevent unauthorized input into data memory and the unauthorised reading, alteration, or deletion of stored data.

User Control

We shall implement suitable measures to prevent our data processing systems from being used by unauthorised persons by means of data transmission equipment.

Access Control to Data

Hypasurance Insurance Consultants represents that the persons entitled to use the organisation's data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions (authorisation).

Transmission Control

We shall be obliged to enable the verification and tracing of the locations / destinations to which the personal information is transferred by utilization of the organisation's data communication equipment / devices.

Transport Control

We shall implement suitable measures to prevent personal information from being read, copied, altered, or deleted by unauthorized persons during the transmission thereof or during the transport of the data media.

Organisation Control

We shall maintain our internal organisation in a manner that meets the requirements of this Manual.

Operators and Data Processors

Where data is stored and/or processed by a third party, we will ensure that their security measures equal or exceed those detailed above. In addition, we will only contract third party services for storage or processing of information where those third parties are located in jurisdictions offering equal or greater protections to your personal information than offered under the Act.

We have established Operator/Data Processing agreements with all third parties who store and/or process personal information data on our behalf to ensure that they take all necessary precautions to safeguard your data, and establish and maintain procedures to protect access to and confidentiality of your personal information.

Additionally, these service providers must make available their own POPI Manuals and/or privacy policies that detail how they comply with the requirements of the Act.

The table below outlines our current service providers, the nature of our relationship with them and the purpose for which they store your personal information.

Provider	Nature	Purpose
Broker Engine (Pty) Ltd	Data Processing & Storage	Provision of applications to manage your insurance and investment portfolio, including all documentation and information pertaining thereto.
Afrihost (Pty) Ltd	Data Processing & Storage	Hosting of organisation email accounts

Security Compromises

Where there is reasonable grounds to believe that your information has been accessed or acquired by any unauthorised person, we must as soon as reasonably possible notify you (except where it will impede any legal or criminal investigation) and the Information Regulator. Such notification must be in written or electronic form and may consist of an email, a notification on our website, or a published notice in national media.

The purpose of this is so that you can take protective measures against such compromise of your personal information, and must include possible consequences of the breach, any remedial action taken or intended, the identities of the persons responsible for the breach, and possible measures you can take to mitigate the adverse effects of the breach.

Cross Border Transfers of Personal Information

Your personal information may be transmitted transborder and stored in data servers hosted outside South Africa. We will in all cases ensure that such servers are in countries that offer equal or greater protection of your personal information that that provided by the Act.

We will also endeavour to ensure that our dealers and suppliers make all reasonable efforts to secure said data and personal information.

Condition 8: Data Subject Participation

In terms of the act, you have the right to have access to your personal information, including learning what information we store and the right to ask for a description or record of that information.

That description can also contain information on which third parties have or have had access to that information.

You also have the right to request corrections to your record when the data is out of date, incomplete, inaccurate, excessive, or obtained unlawfully. Upon receiving the request, we will complete the request within a reasonable timeframe except where dictated by law.

When you exercise any of the rights above, we are allowed to levy a fee to cover the costs of retrieving and collating or modifying that information. In such cases, we will provide you with an estimate of this cost and whether we require a deposit before we provide such information.

When we provide you with the requested information, we will do so in a manner and format consistent with the Act.

Objection to the Processing of Personal Information by a Data Subject

Section 11 (3) of the Act provides that you, as a Data Subject, may at any time object to the processing of your personal information in the prescribed form (subject to exceptions contained in POPIA). **We have attached such a form to this manual as Appendix 1.**

Request for Correction or Deletion of Personal Information

Section 24 of the Act provides that you, as a Data Subject, may request for your personal information to be corrected/deleted in the prescribed form. **We have attached such a form to this manual as Appendix 2.**

Appendix 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

(Regulation 2)

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as applicable.

A	DETAILS OF DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique Identifier / Identity Number:	
Residential, postal or business address:	
	Code:
Contact Numbers:	
Fax Number / Email address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname / Registered Name of Responsible Party:	
Residential, postal or business address:	
	Code:
Contact Numbers:	
Fax Number / Email address:	
C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) TO (f) (Please provide detailed reasons for the objection)

Signed at _____ on this _____ day of _____ 20__.

Signature of Data Subject/Designated Person

Appendix 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

(Regulation 3)

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as applicable.

Mark the appropriate box with an "x".

Request for:

	Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.
	Destroying or deletion of a record of personal information about the data subject which is in the possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique Identifier / Identity Number:	
Residential, postal or business address:	
	Code:
Contact Numbers:	
Fax Number / Email address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname / Registered Name of Responsible Party:	
Residential, postal or business address:	
	Code:
Contact Numbers:	
Fax Number / Email address:	
C	INFORMATION TO BE CORRECTED / DELETED / DESTROYED / DESTROYED

D	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTON 24(1) (a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN (please provide detailed reasons for the request).

Signed at _____ on this _____ day of _____ 20__.

Signature of Data Subject/Designated Person

