CONSORT

Consort Technical Underwriters

Data Privacy Policy (POPI)

CONSORT DATA PRIVACY (POPI POLICY)

COMPANY POLICY

1. Introduction

Consort Technical Underwriting Managers (Pty) Ltd ("Consort") needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards, and how to comply with the law.

2. Why this Policy exists

This data protection policy ensures Consort:

- Complies with data protection law and follow good practice;
- Protects the rights of staff, customers and partners;
- Is open about how it stores and processes individuals' data; and
- Protects itself from the risks of a data breach Privacy law

The Protection of Personal Information Act, 2013 describes how organisations, including Consort, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Consort has made a commitment to respect the privacy rights of individuals by ensuring that their personal information is collected, used and disclosed in such a manner that a reasonable person would consider appropriate in the circumstances.

The Protection of Personal Information Act (POPIA). This Privacy Policy is based on the principles and rules set out in the Act.

Following the Definitions section in this policy document, there are 10 separate policy statements, along with a series of procedural rules which accompany each policy.

3. Definitions

"Broker" means the brokerage organization responsible for abiding by and implementing the policies and procedures in this policy document, and includes the officers and employees of the brokerage.

"Client" means an individual who engages a Broker to acquire or renew a policy of insurance.

"Conditions" means the Conditions of Lawful Processing stipulated in Chapter 3 of the Act, unless the context indicates a contrary meaning:

- Accountability
- Processing limitation
- Purpose specification
- Further processing limitation
- Information quality
- Openness
- Security safeguards
- Data subject participation

"**Data Subject"** means the person to whom personal information relates.

"Operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

"Person" means a natural person or a juristic person.

"Personal Information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
b. information relating to the education or the medical, financial, criminal or employment history of the person;
c. any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
d. the blood type or any other biometric information of the person;
e. the personal opinions, views or preferences of the person;
f. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g. the views or opinions of another individual about the person; and

h. 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

"Privacy Officer / Information Officer" means the individual or individuals appointed from time to time by the Underwriter to be accountable for the Broker's/Insurers/Underwriting Managers compliance with the policies and procedures contained in this policy document.

"Process" means any operational activity concerning personal information including the collection, organisation, storage, modification, communication and destruction of information. (The definition in POPIA is wide and is intended to cover all manner of processing.)

"Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

a. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
b. dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information;

"Public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"Record" means any recorded information:

a. regardless of form or medium, including any of the following:
    i. Writing on any material;
    ii. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
    iii. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    iv. book, map, plan, graph or drawing;
    v. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
b. in the possession or under the control of a responsible party;
c. whether or not it was created by a responsible party; and regardless of when it came into existence;

"Regulator" means the Information Regulator established in terms of the Act; "Responsible Party" means a person who determines the purpose of and means of processing personal information (typically, but not always, the collector of information).

This privacy policy describes how we handle Personal Information that we collect from your application and claim forms, telephone calls, e-mails and other communications with us, as well as from claim investigators, medical professionals, our website, witnesses or other third parties involved in our business dealings with you

4. Policy Scope

This policy applies to:

- The head office of Consort;
- All branches of Consort;
- All staff and volunteers of Consort;
- All contractors, suppliers and other people working on behalf of Consort

It applies to all data that the company holds relating to identifiable individuals and juristic persons.

4. Personal Information that we collect

Depending on your relationship with us (for example, as a consumer policyholder; non-policyholder insured or claimant; witness; commercial broker or appointed representative; or other person relating to our business), Personal Information collected about you and your dependents may include:

General identification and contact information

Your name; address; e-mail and telephone details; gender; marital status; family status; date of birth; passwords; educational background; physical attributes; activity records, such as driving records; photos; employment history, skills and experience; professional licenses and affiliations; relationship to the policyholder, insured or claimant; and date and cause of death, injury or disability.

Identification numbers issued by government bodies or agencies

Identification number (ID); passport number; tax identification number; military identification number; or drivers or other license number.

Financial information and account details

Payment card number; bank account number and account details; credit history and credit score; assets; income; and other financial information.

Medical condition and health status

Current or former physical or mental or medical condition; health status; injury or disability information; medical procedures performed; personal habits (for example, smoking or consumption of alcohol); prescription information; and medical history.

Other sensitive information

In certain cases, we may receive sensitive information about your trade union membership, religious beliefs, political opinions, family medical history or genetic information (for example, if you apply for insurance through a third-party marketing partner that is a trade, religious or political organization). In addition, we may obtain information about your criminal record or civil litigation history in the process of preventing, detecting and investigating fraud. We may also obtain sensitive information if you voluntarily provide it to us (for example, if you express preferences regarding medical treatment based on your religious beliefs).

Telephone recordings

Recordings of telephone calls to our representatives and call centres.

Information to investigate crime, including fraud and money laundering

For example, insurers commonly share information about their previous dealings with policyholders and claimants for this purpose

Information enabling us to provide products and services

Location and identification of property insured (for example, property address, vehicle license plate or identification number); travel plans; age categories of individuals you wish to insure; policy and claim numbers; coverage/peril details; cause of loss; prior accident or loss history; your status as director or partner, or other ownership or management interest in an organization; and other insurance you hold.

Marketing preferences and customer feedback

You may let us know your marketing preferences, enter a contest or prize draw or other sales promotion, or respond to a voluntary customer satisfaction survey.

5. From whom do we collect the Personal Information

Personal information will be collected directly from the data subject, except if:

a. the information is contained in a public record or has deliberately been made public by the data subject;
b. the data subject has consented to the collection of the information from another source;
c. collection of the information from another source would not prejudice a legitimate interest of the data subject;
d. collection of the information from another source is necessary:

   i. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
   ii. to enforce a law imposing a pecuniary penalty;
   iii. to enforce legislation concerning the collection of revenue as defined in local tax legislation;
   iv. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
   v. in the legitimate interests of national security; or
   vi. to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

e. compliance would prejudice a lawful purpose of the collection; or
f. compliance is not reasonably practicable in the circumstances of the particular case.

6. How we use Personal Information

We may use this Personal Information to:

- Communicate with you and others as part of our business.
- Send you important information regarding changes to our policies, other terms and conditions, the Site and other administrative information.
- Make decisions about whether to provide insurance; provide insurance and assistance services, including claim assessment, processing and settlement; and, where applicable, manage claim disputes.
- Assess your eligibility for payment plans, and process your premium and other payments.
- Provide improved quality, training and security (for example, with respect to recorded or monitored phone calls to our contact numbers).
- Prevent, detect and investigate crime, including fraud and money laundering, and analyse and manage other commercial risks.
- Carry out market research and analysis, including satisfaction surveys.
- Provide marketing information to you (including information about other products and services offered by selected third-party partners) in accordance with preferences you have expressed.

- Personalize your experience on the Site by presenting information and advertisements tailored to you.
- Identify you to anyone to whom you send messages through the Site.
- Allow you to participate in contests, prize draws and similar promotions, and to administer these activities. Some of these activities have additional terms and conditions, which could contain additional information about how we use and disclose your Personal Information, so we suggest that you read these carefully.
- Manage our infrastructure and business operations, and comply with internal policies and procedures, including those relating to auditing; finance and accounting; billing and collections; IT systems; data and website hosting; business continuity; and records, document and print management.
- Resolve complaints, and handle requests for data access or correction.
- Comply with applicable laws and regulatory obligations (including laws outside your country of residence), such as those relating to anti-money laundering and anti-terrorism; comply with legal process; and respond to requests from public and governmental authorities (including those outside your country of residence).
- Establish and defend legal rights; protect our operations or those of any of our group companies or insurance business partners, our rights, privacy, safety or property, and/or that of our group companies, you or others; and pursue available remedies or limit our damages.

7. International Transfer of Personal Information

Due to the global nature of our business, for the purposes set out above we may transfer Personal Information to parties located in other countries (including the United Kingdom, United States and other countries that have a different data protection regime than is found in South Africa). We may transfer information internationally to our group companies, service providers, business partners and governmental or public authorities.

8. Sharing of Personal Information

Consort may make Personal Information available to:

Our group companies

Consort and Lombard Insurance Company Limited ("Lombard") are responsible for the management and security of jointly used Personal Information. Access to Personal Information within Lombard is restricted to those individuals who have a need to access the information for our business purposes.

Other insurance and distribution parties

In the course of marketing and providing insurance, and processing claims, Consort may make Personal Information available to third parties such as other insurers; reinsurers; insurance and reinsurance brokers

and other intermediaries and agents; appointed representatives; distributors; affinity marketing partners; and financial institutions, securities firms and other business partners.

Our service providers

External third-party service providers, such as medical professionals, accountants, actuaries, auditors, experts, lawyers and other outside professional advisors; travel and medical assistance providers; call centre service providers; IT systems, support and hosting service providers; printing, advertising, marketing and market research and analysis service providers; banks and financial institutions that service our accounts; third-party claim administrators; document and records management providers; claim investigators and adjusters; construction consultants; engineers; examiners; jury consultants; translators; and similar third-party vendors and outsourced service providers that assist us in carrying out business activities.

Governmental authorities and third parties involved in court action

Consort may also share Personal Information with governmental or other public authorities (including, but not limited to, workers' compensation boards, courts, law enforcement, tax authorities and criminal investigations agencies); and third-party civil legal process participants and their accountants, auditors, lawyers and other advisors and representatives as we believe to be necessary or appropriate:

a. to comply with applicable law, including laws outside your country of residence;
b. to comply with legal process;
c. to respond to requests from public and government authorities including public and government authorities outside your country of residence;
d. to enforce our terms and conditions;
e. to protect our operations or those of any of our group companies;
f. to protect our rights, privacy, safety or property, and/or that of our group companies, you or others; and
g. to allow us to pursue available remedies or limit our damages.

Other Third Parties

We may share Personal Information with payees; emergency providers (fire, police and medical emergency services); retailers; medical networks, organizations and providers; travel carriers; credit bureaus; credit reporting agencies; and other people involved in an incident that is the subject of a claim; as well as purchasers and prospective purchasers or other parties in any actual or proposed reorganization, merger, sale, joint venture, assignment, transfer or other transaction relating to all or any portion of our business, assets or stock. To check information provided, and to detect and prevent fraudulent claims, Personal Information (including details of injuries) may be put on registers of claims and shared with other insurers. We may search these registers when dealing with claims to detect, prevent and investigate fraud.

Personal Information may also be shared by you, on message boards, chat, profile pages and blogs, and other services on the Site to which you are able to post information and materials. Please note that any information you post or disclose through these services will become public information, and may be available to visitors to the Site and to the general public. We urge you to be very careful when deciding to disclose your Personal Information, or any other information, on the Site.

9. Security

Consort will take appropriate technical, physical, legal and organizational measures, which are consistent with applicable privacy and data security laws. Unfortunately, no data transmission over the Internet or data storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any Personal Information you might have with us has been compromised), please immediately notify us. (See the "Who to Contact About Your Personal Information" section below.) When Consort provides Personal Information to a service provider, the service provider will be selected carefully and required to use appropriate measures to protect the confidentiality and security of the Personal Information.

10. Retention of Personal Information

Consort takes reasonable steps to ensure that the Personal Information we process is reliable for its intended use, and as accurate and complete as is necessary to carry out the purposes described in this Privacy Policy. Consort will retain Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law.

11. Marketing Preferences

We will provide you with regular opportunities to tell us your marketing preferences, including in our communications to you. You can also contact us by e-mail at info@consort.co.za or by writing to the Data Protection / Compliance / Information Officer, to tell us your marketing preferences and to opt-out. If you no longer want to receive marketing-related e-mails from Consort on a going-forward basis, you may opt-out of receiving these marketing-related emails by clicking on the link to "unsubscribe" provided in each e-mail or by contacting us at the above addresses.

We aim to comply with your opt-out request(s) within a reasonable time period. Please note that if you opt-out as described above, we will not be able to remove your Personal Information from the databases of third parties with whom we have already shared your Personal Information (i.e., to those to whom we have already provided your Personal Information as of the date on which we respond to your opt-out request). Please also note that if you do opt-out of receiving marketing communications from us, we may still send you other important administrative communications from which you cannot opt-out

12. Access and Correction Requests, Questions and Concerns

In certain countries, an individual may have the right to access, correct, object to the use of, or request deletion or suppression of Personal Information on certain grounds. Please contact us as set out in the "Who to Contact About Your Personal Information" section below with any such requests or if you have any questions or concerns about how we process Personal Information. Please note that some Personal Information may be exempt from access, correction, objection, deletion or suppression rights in accordance with local privacy and data protection laws

13. Other information we may collect through our website

"Other Information" is any information that does not reveal your specific identity, such as:

- Browser information;
- Information collected through cookies, pixel tags and other technologies;

- Demographic information and other information provided by you; and
- Aggregated information
- Other Information

We Collect We and our third-party service providers may collect Other Information in a variety of ways, including:

Through your internet browser:

Certain information is collected by most websites, such as your IP address (i.e., your computer's address on the internet), screen resolution, operating system type (Windows or Mac) and version, internet browser type and version, time of the visit and the page(s) visited. We use this information for purposes such as calculating Site usage levels, helping diagnose server problems, and administering the Site.

Using cookies:

Cookies are pieces of information stored directly on the computer you are using. Cookies allow us to recognize your computer and to collect information such as internet browser type, time spent on the Site, pages visited, language preferences, etc. We may use the information for security purposes, to facilitate navigation, to display information more effectively, to personalize your experience while visiting the Site, or to gather statistical information about the usage of the Site. Cookies further allow us to present to you the advertisements or offers that are most likely to appeal to you. We may also use cookies to track your responses to our advertisements and we may use cookies or other files to track your use of other websites.

Using pixel tags, web beacons, clear GIFs or other similar technologies:

These may be used in connection with some Site pages and HTML-formatted e-mail messages to, among other things, track the actions of Site users and e-mail recipients, measure the success of our marketing campaigns and compile statistics about Site usage and response rates.

From you:

Some information (for example, your location or preferred means of communication) is collected when you voluntarily provide it. Unless combined with Personal Information, this information does not personally identify you.

By aggregating information:

We may aggregate and use certain information (for example, we may aggregate information to calculate the percentage of our users who have a particular telephone area code).

Please note that we may use and disclose Other Information for any purpose, except where we are required to do otherwise under applicable law. If we are required to treat Other Information as Personal Information under applicable law, then, in addition to the uses listed in the "Other Information We Collect" section above, we may use and disclose Other Information for all the purposes for which we use and disclose Personal Information.

14. Who to contact about your personal information

If you have any questions about our use of your Personal Information you can e-mail or write to The Data Protection / Information / Compliance Officer:

Name: Graham Charlton
E-mail address: graham@consort.co.za
Telephone number: (011) 658-1156

15. Changes to this Privacy Policy

We review this Privacy Policy regularly and reserve the right to make changes at any time to take account of changes in our business and legal requirements. We will place updates on our website.

ADDENDUM

POPI ADDENDUM TO CONTRACT OF EMPLOYMENT

With reference to the Protection of Personal Information Act (POPIA) no.4 of 2013 which became effective on 1 July 2021, you are notified of the following in terms of your Personal Information that may not be reflected in our current Contract of Employment

1. For the purpose of this addendum:

    1.1. "Personal Information" means personal information as defined in POPIA and further defined in clause 7;
    1.2. "POPIA" means the Protection of Personal Information Act 4 of 2013, as amended from time to time; and
    1.3. "Processing" means processing as defined in POPIA and "Process" shall have a corresponding meaning;

2. The Company undertakes to comply with POPIA in the Processing of your Personal Information and the Personal Information of your spouse / partner / dependents and emergency contact person/s in terms of this addendum.

3. In terms of POPIA, the Company may not Process your Personal Information without your consent.

4. It is essential for the Company to process your Personal Information for purposes of managing your employment, for disciplinary processes and to process salaries, payments, benefits, access, medical aid membership, retirement fund membership, insurance, service level fulfilment, sales, performance, leave, health and safety, UIF, BEE reporting and tax, most of which are required to enable the Company to comply with applicable law.

5. It will not be possible for the Company to fulfil its obligations in terms of your employment, or to perform the aforementioned activities, without the ability to Process your Personal Information and to disclose same to Third Parties, where the Company has contracted Third Parties to assist the Company with the aforementioned activities. The provision of your Personal Information, on the basis of this addendum, is, therefore, mandatory.

6. By signing this addendum, you consent to the Processing of your Personal Information by the Company, in terms of this addendum, as well as disclosure of such Personal Information to Third Parties, as reasonably required by the Company or to comply with applicable law.

7. Personal Information may include, but is not limited to:

   7.1. Collecting, organising, processing, and storing personal information for the business interests of the Company, as well as for the benefits of the employee and the Company.
   7.2. Utilising personal information for screening, training and development, performance monitoring, career management, administration, employment relationship issues, termination of employment and any other employment-related purposes;
   7.3. Sharing personal information with third parties, such as fund and insurance administrators and government departments. In certain circumstances personal information may be shared across borders when sharing the information with third parties.
   7.4. Distributing relevant personal information when legally required to do so.

8. The parties agree to update, from time to time, any personal information supplied to each other, which may or has changed. The parties cannot be held liable for any loss caused by any of the parties' failure to update and/or correct the personal information supplied to each other, by any of the parties. You may access your Personal Information, as held by the Company, at any reasonable time by notice to the Company.

9. Your Personal Information may be transferred to third countries / cross-border to fulfil the aforementioned activities and to perform back-up tasks. Should the employee's personal information be shared cross border, the personal information will not be subject to less protection than it enjoys in terms of South Africa's data privacy laws

10. The Employee hereby consents to the processing of their Children's personal information, if applicable, as may be necessary for the completion and/or submission of the Employee's Pension / Provident Fund documentation and/or claims.

11. You have the right to file an objection to the Processing of your Personal and / or to submit a complaint to the Information Regulator at https://justice.gov.za/inforeg/contact if you feel that the Company is not complying with its obligations in terms of POPIA

ADDENDUM

DATA BREACH ASSESSMENT REPORT

This template is primarily designed to meet the requirements of assessment of data breaches of personal information as defined by the POPI Act. A data breach involving other kinds of information may require a different approach.

Under the POPI Act, Consort Technical Underwriting Managers (Pty) Ltd must notify affected individuals and prepare a statement for the Information Regulator if the data breach is likely to result in serious harm to any of the individuals whose information was involved.

The purpose of this Report is to:

- enable Consort Technical Underwriting Managers (Pty) Ltd to document its assessment of a data breach;
- to inform the decision of whether to notify affected individuals and/or the Information Regulator; and
- to inform Consort Technical Underwriting Managers (Pty) Ltd.'s review of the data breach and the taking of actions to prevent future breaches.

This assessment must be completed expeditiously and within 30 days if possible.

Description	Details
Description of the breach	[Provide a short description of the breach, including the date and time the breach was discovered and the duration and location of the breach.]
Type of information involved	[Insert the type of information involved.]
How the breach was discovered	[Insert details about how the breach was discovered, and by whom.]
Cause and extent of breach	[Insert details about the cause and the extent of the breach.]
List of affected individuals	[List the affected individuals or describe the class of individuals who are or may be affected by the data breach.]

Is the breach likely to result in serious harm to any of the individuals to whom the harm relates?	[Evaluate whether the breach is likely to result in serious harm to any of the individuals to whom the information relates, having regard to: • the kind of information involved; • the sensitivity of the information; • whether the information is protected by one or more security measures, and the likelihood of those measures being overcome; • the persons, or the kinds of persons, who have obtained, or who could obtain, the information; and • if a security technology or methodology was used in relation to the information and designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information, the likelihood that persons could circumvent the security technology or methodology. Seek advice from the Information Officer if required.]
Remedial action	[Insert details of the steps Consort Technical Underwriting Managers (Pty) Ltd has taken to reduce any potential harm to individuals, e.g. by recovering lost information before it is accessed or changing access controls on compromised systems.]
Is or will the remedial action result in making serious harm no longer likely?	[State whether the remedial action will result in making serious harm no longer likely. If serious harm is no longer likely, Consort Technical Underwriting Managers (Pty) Ltd is not required to prepare a statement to the Information Regulator or to notify affected individuals.]
Who will be notified of the breach?	[Select from the following options.] **[Option 1]** Consort Technical Underwriting Managers (Pty) Ltd has determined that the data breach is likely to result in serious harm to individuals and therefore Consort Technical Underwriting Managers (Pty) Ltd will: • Provide a statement to the Information Regulator containing a description of the breach, the kind of information concerned and the recommended steps for individuals. • Will [select one of the following options] notify all affected individuals / notify affected individuals at risk of serious harm / publish the statement on Consort Technical Underwriting Managers (Pty) Ltd.'s website and publicise it [choose this option only if the first two options are impracticable]

	[Option 2] Consort Technical Underwriting Managers (Pty) Ltd has determined that notification of the data breach is not required because it is not likely to result in a serious risk of harm to any individuals.
Preliminary recommendations	[Include any recommendations on actions that could be undertaken to contain the breach or prevent future breaches of a similar nature – these recommendations will feed into Consort Technical Underwriting Managers (Pty) Ltd.'s comprehensive review of the data breach.]
Names of response team members	[Insert the names and roles of the response team members. The make-up of the response team will be determined by the CEO / MD / KI, having regard to the skills required to respond to the breach.]
Date	[Insert Date.]

ADDENDUM

FORM FOR REPORTING A SUSPECTED INFORMATION SECURITY INCIDENT

Company Name:		**HIGHLY CONFIDENTIAL**

Your Name:	
PC Name: (e.g., XX######)	
Dept/Division:	
Today's Date:	
Tel No:	
Email Address:	

Date of Incident:		**Time of Incident:**	
Who Was Notified?		**Time of Notification:**	
Brief Description of Incident: (include website URLs, suspect name(s), impacted system(s), other relevant data…)			

Did you witness the incident yourself?	☐ Yes	☐ No
Did others witness the incident? (if yes, specify below)	☐ Yes	☐ No
To your knowledge was any of the following involved?	☐ Yes	☐ No
• **Telephone**	☐ Yes	☐ No
• **Fax**	☐ Yes	☐ No
• **Theft**	☐ Yes	☐ No
• **Fraud**	☐ Yes	☐ No
• **Photocopier**	☐ Yes	☐ No
• **Unauthorised Access**	☐ Yes	☐ No
• **Computer Hardware**	☐ Yes	☐ No
• **Customers**	☐ Yes	☐ No
• **Email**	☐ Yes	☐ No
• **Third Parties**	☐ Yes	☐ No
• **Internet Download**	☐ Yes	☐ No
• **Copyright**	☐ Yes	☐ No
• **Virus**	☐ Yes	☐ No
• **Other (Please specify)**	☐ Yes	☐ No

Was any COMPANY Internal or Confidential information compromised?	
Did you report this incident to: (Please circle all applicable)	
Supervisor - Law Enforcement – Director of IT – Internal Auditor – Other (Please Specify)	

Initiated By:		**Date:**	
Reviewed By:		**Date:**	
Approved By (1):		**Date:**	
Approved By (2):		**Date:**	

ADDENDUM

DATA BREACH NOTIFICATION FORM

Data Breach Notification

(**Attention:** Do not transmit the personal data concerned by the data breach with the notification of the violation to the Information Regulator's Office)

Type of notification	☐ Complete notification ☐ Preliminary notification ☐ Complementary / amended notification
ID of notification (Optional - internal ID from your org.)	
Date of previous notification (case complementary notification)	
ID of previously notified breach (case complementary notification)	
Summary of the data breach (summarize the events that occurred)	

1. Company Details

1.1. Contact Details	
Name of the organisation	
Address and any relevant contact details of the organisation	
Name and function of the reporting person	
Reporting person's contact details	
Name and function of the person who can be contacted for more information about the breach	
Email address	
Phone number	

Postal address	
Sector of activity of the organisation	
2.2. Involvement of others outside the responsible party for the service concerned by the data breach	
Name and qualification of the other involved party	

3. Timeline

Date of breach	
Start date of breach	
End date of breach	
Date of awareness of breach	
Means of detection of breach	
Date of notification by Operator	
Reasons for late notification of breach	
Comments on the dates	

4. About the breach

Nature of the incident	☐ Confidentiality ☐ Integrity ☐ Availability
	☐ Device lost or stolen ☐ Paper lost or stolen or left in insecure location ☐ Mail lost or opened ☐ Hacking ☐ Malware (e.g. : ransomware) ☐ Phishing ☐ Incorrect disposal of personal data on paper ☐ E-waste (personal data still present on obsolete device) ☐ Unintended publication ☐ Data of wrong data subject shown ☐ Personal data sent to wrong recipient ☐ Verbal unauthorized disclosure of personal data ☐ Other:

Cause of the breach	☐ Internal non malicious act (breach of policy) ☐ Internal malicious act ☐ External non malicious act ☐ External malicious act ☐ Other:

5. About the breached data

Regular data	☐ Data subject identity (name, surname, date of birth) ☐ National identification number ☐ Contact details ☐ Identification data ☐ Economic and financial data ☐ Official documents ☐ Location data ☐ Genetic or biometric data ☐ Criminal convictions, offence or security measures
Special categories of data	☐ Data revealing racial or ethic origins ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sex life data ☐ Health data ☐ Genetic data ☐ Biometric data ☐ Not yet known ☐ Other:
Approximate number of personal data records concerned by the breach	

6. About the Data Subjects / Affected Party

Type	☐ Employees ☐ Users ☐ Subscribers ☐ Students ☐ Military staff ☐ Customers (current and prospects) ☐ Patients ☐ Minors ☐ Vulnerable individuals ☐ Not yet known ☐ Other:
Detailed description of the concerned data subjects	
Approximate number of persons concerned by the breach	

7. About the measures in place BEFORE the breach

Description of measures in place before the breach	

8. Consequences of the breach

In the event this is a breach of Confidentiality	☐ Larger distribution than necessary or beyond authority consented by data subjects ☐ Data may be linked with other information of the data subjects ☐ Data may be exploited for other purposes and / or unfair manner ☐ Other :
In the event this is a breach of Integrity	☐ Data may have been modified and used even though it is no longer valid ☐ Data may have been modified into otherwise valid data and subsequently used for other ☐ Other :
In the event this is a breach of availability	☐ Loss of the ability to provide a critical service to the affected data subjects ☐ Alteration of the ability to provide a critical service to the data subjects ☐ Other :

8.1. Physical, material or non-material damage or significant consequences to the data subjects	
Nature of the potential impact for the data subject	☐ Loss of control over their personal data ☐ Limitation of their rights ☐ Discrimination ☐ Identity theft ☐ Fraud ☐ Financial lost ☐ Unauthorised reversal of pseudonymisation ☐ Damage to reputation ☐ Loss of confidentiality of personal data protection by professional secrecy ☐ Other (please describe) :
Severity of the potential impacts	☐ Negligible ☐ Limited ☐ Significant ☐ Maximal

9. Action(s) taken

9.2. Communication to data subjects	
Information of data subjects	☐ Yes ☐ No but they will be informed ☐ No they will not be informed ☐ Not defined at this time
Date of when information was given to data subjects if they already have been informed	
Date of future information of the data subjects if they have not been informed yet	☐ Date : ☐ Unknown date of future information of the data subjects
Number of data subjects informed	
Means of communication used to inform the data subject	
Content of the information delivered to the data subjects	*(Submit the content communicated to the data subjects with the notification)*

Reason for not informing data subject	☐ The Responsible Party has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it. ☐ The Responsible Party has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise. ☐ It would involve disproportionate effort to inform each data subject individually.
9.3. Measures taken to address the breach	
Measures taken by the Responsible Party to address the breach	

9.4. Cross border and other notifications	
Is this notification a cross border notification made to your lead supervisory authority ?	☐ Yes ☐ No If yes, precisely list of the countries concerned by the breach:
Has the breach been or will it be notified directly to other concerned Supervisory Authority/ies?	☐ Yes ☐ No If yes, indicate the other(s) Supervisory Authority/ies concerned:
Has the breach been or will it be notified to Data Protection Authorities outside the RSA?	☐ Yes ☐ No If yes, indicate the other(s) Data Protection Authority/ies outside the RSA concerned:
Has the breach been or will it be notified to other regulators because of other legal obligations?	☐ Yes ☒ No If yes, indicate the other(s) regulator(s) notified:

ADDENDUM

DATA BREACH RESPONSE PLAN

This plan defines the steps to be taken in the event of loss of Personal Information, as a result of loss of, damage to, or unauthorised destruction of personal information; and unlawful access to or processing of personal information by an unauthorised entity.

The safekeeping of data whilst working remotely from home is an important consideration, to protect against access by unauthorised persons who might be able to view content on a laptop or cell phone.

A loss can arise from theft or loss of data storage media, such as computers or by cyber-attack. Experts deem the possibility of a cyber-attack to be a question of "when" and not "if" an incident occurs, thus the staff of Consort Technical Underwriting Managers (Pty) Ltd must be alert to the possibility of a breach and report any suspicion of a breach as soon as possible, to Graham Charlton as the Information Officer (IO).

We must be aware of the possible risk of opening suspicious e-mails which might contain malicious links, which can lead to the installation of malware or a ransomware attack. It is felt that the threat of ransomware demand is probably a greater exposure than a cyber hack to steal information.

INCIDENT RESPONSE TEAM (IRT) – Graham Charlton (IO) and Chris Charlton, Shaun van der Merwe of IT Contact details:

Graham Charlton – graham@consort.co.za - Mobile No: 083 233 0439
Chris Charlton – chris@consort.co.za - Mobile No: 083 233 0437
Shaun van der Merwe – shaun@overscore.co.za – Mobile No: 082 900 7227

1. Breach Detection

- Where there are reasonable grounds to believe that personal information has been accessed by an unauthorised person, or otherwise compromised, Graham Charlton must be formally advised immediately by the person who identified the incident.
- The primary requirement is to identify the nature and extent of the incident and contain it, and to ensure the retention of all appropriate evidence. (Form DB1 – Data Breach Incident Report - to be completed by the person identifying the incident)
- A written report of the circumstances relating to the incident must be completed (Form DB2 – Data Breach Assessment Report - to be completed by the Information Officer), once all relevant information has been obtained from the person who identified the event, in conjunction with IT Support and in association with IRT.

2. Breach Containment

- Time and efficiency of response is a key factor in limiting any damage and IRT are to immediately take the necessary steps to secure the environment, contain the incident to prevent any further loss and to preserve any evidence. IRT will document information relating to the incident and perform an initial impact assessment.

3. Notification Requirement

Section 22 of the Protection of Personal Information Act (POPIA), (Notification Security Compromises), defines the steps required to notify the appropriate authorities in the event of a data breach.

- Notification must be given by Craig Ormrod as the Information Officer to the Information Regulator, (Form DB3 – Data Breach Notification form - to be completed by the Information Officer for this purpose). Data subject(s) must be advised once the Information Regulator has confirmed his/her satisfaction that the situation will not be compromised by notification to the data subject(s), and where appropriate, any Law Enforcement Agency should be notified, as soon as reasonably possible, again with the Information Regulator's approval.
- There are conditions applicable in this respect, primarily that notification to the data subject may be delayed if the Regulator or a Public Body, such as SAPS, determines that such notification will impede criminal investigation by any Public Body, or if it is perceived that notification of the breach to the data subject might cause an undesirable result, for example if the data relates to adverse health status, then the data subject's health practitioner or close relative, should be advised.
- The information given to the data subjects must provide sufficient information and be clear and specific, to enable them to understand the possible consequences of the security compromise. It must detail the measures we have taken in our attempt to avoid further compromise and unauthorised access or use of their personal information, and we must make recommendations to the data subjects as to how they can mitigate the possible adverse effects of the of the security compromise.
- Notification to the data subject must be in writing and communicated in at least one of the following ways:

    1. Mail to the data subject's last known postal or physical address
    2. E-Mail to the data subject's last known e-mail address
    3. Prominent notification on our website (www.associatedcompliance.co.za)
    4. Published in the news or appropriate media, or
    5. As may be directed by the Information Regulator

4. Recovery Process

The procedures for the recovery from any incident will be identified once the containment processes have been completed. The means that the process for the recovery of data, if lost, will be confirmed, and activated by the IRT using any available assistance and advice. Decision will be made as to whether a phased approach to the reinstatement of systems will be a requirement or whether the entire system will be brought down and reinstated "in toto" once all issues have been resolved.

5. Post Incident follow up

- (Form DB4 – Data Incident/Breach Register - should be completed at this time by the Information Officer)
- IRT will investigate, identify, and eradicate, where possible, any vulnerabilities which might become apparent during the investigation and handling of the incident
- Interview anybody with insight relating to the occurrence and identify whether there were circumstances enabling the incident which could have been avoided, and install the necessary protections, including refresher training of staff, to prevent a recurrence.
- Ensure that data subjects (and our clients) have been fully informed as to the introduction of any procedures or steps taken which might affect their interaction with us after the incident.

ADDENDUM

DATA SUBJECT ENQUIRY PROTOCOLS

The Protection of Personal Information Act (POPIA) places an important responsibility on parties who collect, store, use and destroy personal information ("responsible parties") and also provides rights and remedies to persons whose personal information is being processed ("data subjects").

We need to collect personal information to effectively carry out our everyday business functions and services and, in some circumstances, to comply with the requirements of the law and/or regulations.

For more information on our processing activities, please refer to our Privacy Statement which is available on our website: www.associatedcompliance.co.za or upon request at our office.

As a responsible party, we are obligated under POPIA to abide by the principles which ensure that personal information shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject.
b. collected for specified and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.
c. adequate, relevant, and limited to what is necessary in relation to the purposes for which the information is processed.
d. accurate and, where necessary, kept up to date.
e. kept for no longer than is necessary for the purposes for which the personal data was processed, or for the agreed upon retention period.
f. processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

As a data subject, you may request access to your personal information that we hold. You may also request that your personal information be corrected or deleted in circumstances where such information has become outdated, is not accurate, is incomplete, misleading, or excessive, if it has not been obtained by lawful means, or if we are no longer entitled to retain the information.

We are obliged, if so requested, to provide confirmation to you on whether or not we hold your personal information, to provide a description of the personal information in question and to confirm the identity of all third parties or the categories of third parties who have received your personal information.

We must comply with any such request from you:

- within a reasonable time period, and
- in a reasonable manner and format; and in a form that is generally understandable.

In accordance with POPIA, we are only obligated to provide access to personal information belonging to you, directly to you, unless you have consented otherwise, and in such a case we will require satisfactory proof of capacity before considering the access request.

Should we refuse to provide personal information to you, this must be based on the same grounds for refusal as allowed under the Promotion of Access to Information Act (PAIA). Our PAIA Manual is available on our website at www.consort.co.za or upon request at our office.

1. Access Request and Objection Procedure

This procedure provides the process for individuals to follow when making a request or a complaint to Consort Technical Underwriters, along with the protocols we will follow when such a request is received.

1.1. The right of access

You have the right to obtain from us, confirmation as to whether or not your personal information is being processed. We are committed to upholding the rights of individuals and have dedicated processes in place for providing access to personal information.

Where requested, we will provide the following information:

- the categories or type of personal data concerned.
- the purpose/s of the processing.
- the recipient/s or categories of recipient/s to whom any personal data has been or will be disclosed.

- If the data has been transferred to a third country or international organisation(s) (and if applicable, the appropriate safeguards used)
- the envisaged period for which the personal data will be stored (or the criteria used to determine that period)
- where the personal data was not collected directly from you, any available information as to its source

1.2. How to make a Data Subject Access Request

You need to make this request in writing using the form provided in Annexure A.
Where a request is received by electronic means, we will provide the requested information in a commonly used electronic form (unless otherwise requested by you).

1.3. What we do when we receive a Data Subject Access Request

1.3.1. Identity Verification

Data subject access requests are passed to our Information officer as soon as received and a record of the request is noted.

The person assigned to the request will use all reasonable measures to verify your identity, as the individual to whom the personal information relates. Where we are unable to do so, we may contact you for further information, or ask you to provide evidence of your identity prior to actioning any request. This is to protect your information and rights.

If a third party, relative or representative is requesting the information on your behalf, we will verify their authority to act for you and again, may contact you to confirm their identity and gain your authorisation prior to actioning any request.

1.3.2. Information Gathering

If you have provided enough information in your request to collate the personal information held about you, we will gather all forms (hard-copy, electronic, etc) and ensure that the information required is provided in an acceptable format. If we do not have enough information to locate your records, we may contact you for further details. This will be done as soon as possible and within the timeframes
set out below.

1.3.3. Information Provision

Once we have collated all the personal information held about you, we will send this to you in writing. The information will be in a concise, transparent, and easily accessible format, using clear and plain language.

1.4. Fees and Timeframes

Whilst we will confirm, free of charge, whether or not we hold personal information about you, should we require, depending on the nature of your request, that you pay us a fee in order to enable us to respond to your request and for the services provided to you, we will:

- provide you with a written estimate of the fee before providing the services; and
- we may require you to pay a deposit for all or part of the fee.

Where the request is made by electronic means, we will provide the information in a commonly used electronic format, unless an alternative format is requested.

We will always aim to provide the requested information at our earliest convenience, but at a maximum, 30 days from the date the request is received. However, where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months. If this is the case, we will write to you within 30 days and keep you informed of the delay and provide the reasons.

1.5. Your other rights

You have the right to request the correction of any inaccurate data held by us. Where we are notified of inaccurate data, and agree that the data is incorrect, we will amend the details as directed by you and make a note on our system of the change and reasons.

We will rectify the errors within 30 days and inform you in writing of the correction and where applicable, provide the details of any third-party to whom the data has been disclosed. Where applicable, we will inform all third parties to whom your personal information was disclosed, of the corrections or updates needed.

In certain circumstances, you may also have the right to request from us, the erasure of personal data or to restrict the processing of personal data where it concerns your personal information; as well as the right to object to such processing

If for any reason, we are unable to act in response to a request for rectification and/or data completion, we will always provide a written explanation to you and inform you of your right to complain to the Information Regulator.

You can use the form and contact details in Annexure A to make such requests.

1.6. Automated Decision-making

We do not employ any automated decision-making.
Exemptions and Refusals

POPIA contains certain exemptions from the provision of personal information. If one or more of these exemptions applies to your request or where we do not act upon the request, we shall inform you at the earliest convenience, or at the latest, within 30 days of receipt of the request.

Where possible, we will provide you with the reasons for not acting and any possibility of lodging a complaint.

1.7. Lodging a complaint

Any complaints or concerns with regards to the way in which we process personal information or the way in which we handle your request or objection may be directed to our Information officer:

Information Officer:	Mr Graham Charlton
Business Address:	Unit 30, Waterford Office Park, Corner Witkoppen and Waterford Drive, Fourways, 2055
Postal Address:	P O Box 520, Banbury, 2164
Email Address:	graham@consort.co.za
Telephone:	011 658 1156

Should we not resolve your complaint or if you remain dissatisfied with our actions, you have the right to lodge a complaint with the Information Regulator.

2. Annexure A

FORM: REQUESTS IN RELATION TO YOUR RIGHTS IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA)

Particulars of the Responsible Party from whom you are requesting access:

Registered Company Name:	Consort Technical Underwriting Managers (Pty) Ltd
Business Address:	Unit 30, Waterford Office Park, Corner Witkoppen and Waterford Drive, Fourways, 2055
Postal Address:	P O Box 520, Banbury, 2164
Telephone:	011 658 1156
Email Address:	graham@consort.co.za

Please note:

All Personal Information collected in this form is for the purposes of assessing and giving effect to your requests.

Affidavits or other documentary evidence as applicable in support of your requests may be attached.

If the space provided for in this form is inadequate, submit information as an Annexure to this form and sign each page.

All completed requests with supporting documentation must be submitted to info@associatedcompliance.co.za

Mark the appropriate request box with an "x" and only complete the relevant sections.

Access request for details of the personal information held by Consort Technical Underwriters about you.	Complete sections A, B, C, G, H
Objection to the processing of your personal information.	Complete sections A, B, D, G, H
Correct or delete personal information about the data subject in the possession or under the control Consort Technical Underwriters that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.	Complete sections A, B, E, G, H
Destroy or delete a record of personal information about the data subject that Consort Technical Underwriters is no longer authorised to retain.	Complete sections A, B, F, G, H

A. DETAILS OF THE DATA SUBJECT (to whom the request relates) *Proof of identification must be attached, for example, copy of ID, Passport. Certified copies must not be older than 3 months.*	
Full Names and Surname / Registered Name if data subject is a juristic person	
ID/Passport number or Registration number if data subject is a juristic person	
Residential, postal, or business address	
Contact number	
Email address	

B. PARTICULARS OF PERSON MAKING REQUEST ON BEHALF OF THE DATA SUBJECT *This section must be completed if the request is made on behalf of a data subject or juristic entity. Proof of capacity must be attached, for example power of attorney, affidavit, authorisation.*	
Full Names and Surname / Registered Name if data subject is a juristic person	
ID/Passport number or Registration number if data subject is a juristic person	
Residential, postal, or business address	
Contact number	
Email address	

C. INFORMATION REQUESTED *Please provide as much detail as possible about the personal information you want, to help us to deal with your request quickly and efficiently.*		
I would like you to:		
Confirm if Consort processes my personal information		
Provide a copy of my personal data held		
Provide an explanation and/or documentation and material relating to the following:		
	The reason / purposes for processing my personal information	
	The categories or type of information being processed	
	The recipients, or categories of recipients of my information	
	The planned retention period of my information, or details of how the retention period is determined	
	Where my personal information is transferred across the borders of South Africa, the security safeguards relating to such transfer	

D. REASONS FOR OBJECTING TO THE PROCESSING OF YOUR PERSONAL INFORMATION	
Provide detailed reasons for objecting to the processing of your personal information	
If known, please provide details of the record to which the objection relates	

E. PERSONAL INFORMATION RECORDS TO BE CORRECTED OR DELETED *This section must be completed if the request is for the correction or deletion of personal information about the data subject in the possession or under the control of Consort, and the information is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.*	
Provide detailed reasons for the correction or deletion	
If known, please provide details of the record to which the correction or deletion relates	

F. PERSONAL INFORMATION RECORDS TO BE DELETED OR DESTROYED *This section must be completed if the request is for the destruction or deletion of a record of personal information about the data subject that Consort is no longer authorised to retain.*	
Provide detailed reasons for the destruction or deletion	
If known, please provide details of the record to which the destruction or deletion relates	

G. MEANS OF CONTACT *Please complete this section to inform us on how you would like to be contacted by marking the appropriate box with an "x" and providing the relevant contact details.* *We will use your preferred contact method to notify you if your request has been granted or denied and the reasons for such denial where applicable.*	
Telephone number	
Email	
Physical address	
Relevant contact details	

3. DECLARATION AND SIGNATURE

I, _____ (full name), confirm that the information provided above is correct and that I am the data subject, or the person duly authorised to act on behalf of the data subject, as noted within this form.
I acknowledge that Consort is obligated to confirm the identity of the data subject and where applicable, the person duly authorised to act on behalf of the data subject. It may be necessary for Consort to contact me to obtain further information in order to action my request.

I understand that my request will not be valid until all the required information as requested by Consort has been received by Consort.

I am aware that whilst Consort provides the information requested without a fee, should I make unfounded, repeated, or excessive requests, Consort may charge a reasonable administrative fee in order to process my request.

Signed at _____ on this _____ day of_____ 20 ____

Signature: _____

ADDENDUM

COMPLAINTS PROTOCOLS

COMPLAINT REGARDING INTERFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION / COMPLAINT REGARDING DETERMINATION OF AN ADJUDICATOR IN TERMS OF SECTION 74 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 7]

Note:

1. Affidavits or other documentary evidence as applicable in support of the request 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. Comp/eta as is applicable.

Mark the appropriate box with an "x".

Complaint regarding:

☐ Alleged interference with the protection of personal information
☐ Determination of an adjudicator.

PART I	**ALLEGED INTEREFERENCE WITH THE PROTECTION OF THE PESONAL INFORMATION IN TERMS OF SECTION 74(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (Act No. 4 of 2013)**
A	**PARTICULARS OF COMPLAINANT**
Name(s) and surname / registered name of data subject	
Unique identifier/identity number	
Residential, postal or business address	
Postal Code	

Contact number(s)	
Fax number/email address	

B	**PARTICULARS OF RESPONSIBLE PARTY INTERFERING WITH PERSONAL INFORMATION**
Name(s) and surname / registered name of responsible party	
Residential, postal or business address	
Postal Code	
Contact number(s)	
Fax number/email address	

C	**REASON FOR COMPLAINT**

PART II	COMPLAINT REGARDING DETERMINATION OF ADJUDICATOR IN TERMS OF SECTION 74(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (Act No. 4 of 2013)
A	**PARTICULARS OF COMPLAINANT**
Name(s) and surname / registered name of data subject	
Unique identifier/identity number	
Residential, postal or business address	
Postal Code	
Contact number(s)	
Fax number/email address	

B	PARTICULARS OF ADJUDICATOR AND RESPONSIBLE PARTY
Name(s) and surname / registered name of responsible party	
Residential, postal or business address	
Postal Code	
Contact number(s)	
Fax number/email address	

C	REASON FOR COMPLAINT