PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

1. PREAMBLE

1.1 Our firm has implemented a Data Privacy and Cyber Security Management framework in line with South African Protection of Personal Information Act 4 of 2013 ("POPIA").

1.2 Our firm's Data Privacy Terms and Conditions apply to all external and internal parties with whom we interact, including but not limited to clients, visitors to our offices, visitors to our website, our own employees and other users of our legal services.

1.3 "Processing" of information encompasses a wide range of activities starting with the initial obtaining of personal information, the use and retention of that information, as well as access, disclosure of same and ending with its disposal.

1.4 As a data subject of our firm, by providing us with your personal information and engaging with the firm, you agree to our Data Privacy Terms and Conditions and authorise us to process such information as set out herein.

1.5 In delivering our legal services, our firm respects the privacy of your personal information, and we have implemented reasonable measures to ensure that the processing of your personal information is aligned to the requirements of the POPIA.

1.6 In this document we explain how and when we process personal information.

1.7 If you have questions arising from the processing of information that are not specifically listed herein, you may contact our firm's Information Officer, Nicole Scholtz, on - nicole@goldlaw.co.za for assistance.

1.8 The firm's data security mitigation measures are provided for in the following Internal and External Policies:

Data Privacy Terms and Conditions	External policy made available to our firm's data subjects via our firm's website and from the information officer: nicole@goldlaw.co.za
Data Classification Policy	Internal policy
Internal IT and Email Usage Policy	Internal policy
Data Incident Reporting Policy	Internal policy
Payments Policy	Internal policy
Employee Data Consent and Accountability Declaration	Internal declaration
Conflict of Interest Policy	Internal policy
Data Archiving and Record Keeping Policy	Internal policy
Client Consent **Once off engagement** **Ongoing engagement**	External consent to be signed by every client of the firm at onboarding
Supplier Consent **Once off engagement** **Ongoing engagement**	External consent to be signed by every supplier, of the firm irrespective of the supply
Professional Associates' Declaration (ongoing association)	External declaration to be signed by professional associates who engage with the firm on an ongoing basis
Professional Associates' Declaration (once off association)	External declaration to be signed by professional associates who engage with the firm on an once office basis
Third Party Operator's Agreement and-Non-Disclosure	External agreement to be signed by suppliers who process data on behalf of the firm

The firm's Business Continuity Plan	Internal plan
PAIA Manual	External manual made available to our firm's data subjects via the firm's website and by the information officer - nicole@goldlaw.co.za
Our firm's website Usage Policy	External policy published on our firm's website - **goldbergdevilliers.co.za**
Updated email disclaimers	Embedded on emails sent from the firm

1.8 Our firm may review and update our Data Privacy Terms and Conditions, and other Policies associated thereto from time to time.

2. INTRODUCTION

2.1 Our firm mainly specialises in the delivery of the following legal services (but not exclusively):

2.1.1 Labour Law;

2.1.2 Corporate And Commercial Law;

2.1.3 Dispute Resolution (Litigation, Arbitration And Mediation);

2.1.4 Alternative Dispute Resolution;

2.1.5 Property Law And Conveyancing (Including Mortgage Bond Registrations);

2.1.6 Road Accident Rund (Raf) Claims;

2.1.7 The Administration Of Deceased Estates;

2.1.8 Trust Services;

2.1.9 Legal Correspondent Services; and

2.1.10 Debt Recoveries

2.2 Our firm operates from one branch which is situated in the Central, Gqeberha area.

2.3 In delivering legal services, our firm has to collect and process personal information as and when required, including but not limited to:

2.3.1 Complying with Regulatory requirements, in terms of the Legal Practice Council, the Consumer Protection Act and the Financial Intelligence Centre Act – amongst others;

2.3.2 The management of client enquiries, instructions or transactions in which we act or have received instruction or are involved with in any way on a professional basis;

2.3.3 Some information when you browse our website, but we will not record any of your personal details from the website unless you specifically subscribe or engage with us directly from the website. These details are recorded in our website terms and conditions.

2.4 We may collect or obtain your personal information:

2.4.1 Directly from you;

2.4.2 In the course of our business relationship with you;

2.4.3 In the course of providing our services to you;

2.4.4 When you make your personal information public;

2.4.5 When you visit and/or interact with our website or our social media platforms;

2.4.6 When you register to access our services including but not limited to newsletters, information updates and similar services and products that we offer;

2.4.7 When you visit our offices; and

2.4.8 From third parties involved in your transaction.

2.5 We may record personal information about you, such as records of your communications and interactions with us, including, but not limited to, your email and other communications with us, your details supplied for delivery of our services or goods (such as invoicing and other such information) or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with you during the course of digital or 'in person' marketing campaigns.

2.6 We treat your personal information confidentially and only use, share, record or delete it as is required by law, as part of our service delivery to you and/or as lawfully instructed by you.

2.7 We primarily use your personal information only for the purpose for which it was originally or primarily collected.

2.8 We will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest for you or for us and is closely related to the original or primary purpose for which your personal information was collected.

3 OBJECTIVE OF THESE TERMS AND CONDITIONS

3.1 Although it is not possible to ensure 100% mitigation against data breaches, the objective of our firm's Data Privacy Terms and Conditions is to ensure adherence by our firm and all employees associated with our firm to the provisions within POPIA together with its Regulations.

3.2 It is a priority for our firm to continue to create Management direction and high-level objectives for regulating the manner in which personal information is processed and to provide for remedies in cases where personal information is not handled accordingly.

3.3 Further purposes of the policy, this shall include:

3.3.1 The supplementation of all our firm's Policies and procedures to align it with South African laws;

3.3.2 General compliance with the requirements of POPIA;

3.3.3 The identification and codification of documents and ensuring adequate protection and maintaining the accuracy of documents where required;

3.3.4 Providing a set framework and unified policy regarding the methods and procedures for the retention and destruction of documents and personal information;

3.3.5 Ensuring that data subjects' Consent is obtained as provided for in POPIA;

3.3.6 Ensuring that our firm's data subjects' information is not unlawfully shared with third parties unless Consent for such sharing is obtained or that such sharing is lawful;

3.3.7 Protecting all of our firm's data subjects from harm;

3.3.8 To stop identity fraud;

3.3.9 Ensuring records that are no longer required or documents that are of no value are destroyed properly and in accordance with the data retention schedule; and

3.3.10 Aiding employees in understanding the requirements relating to the protection of personal information and the retention and destruction of documents.

4 POPIA CORE PRINCIPLES

In our quest to ensure that we protect, as far as we are able to do so, our data subjects' privacy, our firm fully commits as follows:

4.1 To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.

4.2 To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.

4.3 To ensure that the requirements of the POPIA legislation are upheld within our firm. In terms of sections 8, 17 and 18 of POPIA, our firm adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribes to a process of accountability and openness throughout its operations.

4.4 In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, to only collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for our operations and to process the personal information obtained from clients, employees, visitors and services suppliers only for the purpose for which it was obtained in the first place.

4.5 Not to process personal information obtained from clients, our employees, visitors and service suppliers in an insensitive, derogative, discriminatory or wrongful way that can intrude on the privacy of the particular data subject.

4.6 In terms of the provisions contained within sections 23 to 25 of POPIA, to allow all data subjects of our firm the right to request access to certain personal information and correction or deletion of personal information within the specifications of the POPIA. Data subjects should refer to FORMS 1 & 2 attached hereto for these purposes.

4.7 Not to request, or process information related to race, religion, medical situation, political preference, trade union membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented thereto. Our firm will also not process information of children unless the specific consent provisions contained within POPIA have been complied with.

4.8 In terms of the provisions contained within section 16 of POPIA, to continue to take steps to ensure that data subjects' information is recorded and retained accurately.

4.9 Not to provide any documentation to a third party or service provider without the express consent of the data subject except where it is necessary for the proper execution of the service, as expected by the data subject.

4.10 To keep effective record of personal information and not to retain information for a period longer than required.

4.11 In terms of sections 19 to 22 of POPIA, to ensure the integrity and confidentiality of personal information in our possession is maintained and to I provide the necessary security of data and keep it in accordance with prescribed legislation.

5 COLLECTION AND PROCESSING OF PERSONAL INFORMATION

We may subject your personal information to processing during the course of various activities, including:

5.1 The general operation of our firm;

5.2 Analysis, evaluation, review and collation of information in order to determine potential disputes, render legal services, provide legal advice and preparing or reviewing opinions, responding to correspondence, reports, publications, documents relating to our services and any other documents and records;

5.3 Compliance with the law and specifically fraud prevention and the combatting of money laundering;

5.4 Transfer of information to our service providers and operators;

5.5 For recruitment purposes;

5.6 For relationship management and marketing purposes in relation to our services (including, but not limited to, processing that is necessary for the development and improvement of our services), for accounts management, and for marketing activities in order to establish, maintain and/or improve our relationship with you;

5.7 In addition, we may process your personal information for statistical purposes and for internal management and management reporting purposes, including but not limited to: conducting internal audits, conducting internal investigations, implementing internal business controls, providing central processing facilities, for insurance purposes and for management reporting analysis;

5.8 We may process your personal information for safety and security purposes;

5.9 We may share certain personal information with other institutions as part of our service rendering or as legally required, such as sharing information with the Receiver of Revenue, local authorities, the courts, sheriffs and the like. We only share such personal information as may be required for purposes of fulfilling our service mandate or as prescribed by law.

5.10 Collection of personal information from another source may be necessary –

5.10.1 To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

5.10.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

5.10.3 For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

5.10.4 In the interest of national security;

5.10.5 To maintain the legitimate interests of our firm or of a third party to whom the information is supplied;

5.10.6 Where compliance would prejudice a lawful purpose of the collection;

5.10.7 Where compliance is not reasonably practicable in the circumstances of a particular contract.

5.11 Our firm often collects personal information from other parties involved in our transactions as various role players often share clients in a single transaction.

5.12 Most of our communications are done electronically via the internet, per email and other electronic methods and we recognise the international risk of data and email breaches.

5.13 To ensure that lawful conditions exist surrounding our data subject's information, we accept that all our South African based data subjects' Constitutional Right to Privacy is of utmost importance and that our data subjects based in other parts of the world are equally entitled to rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based.

5.14 As such, we are committed to comply with South Africa's POPIA provisions and to the education of our data subjects in respect of their rights to privacy and to make operational amendments as may be necessary.

6 CONSENT

6.1 When our data subjects' information is collected, processed or shared by our firm, it will be for the purposes of delivering services or to comply with statutory requirements.

6.2 In doing so, we explain the reasons for the collection of information from the particular data subject/s and obtain the required Consents to process, if the Consent is necessary, and where required, for the sharing of the information pursuant to such explanation.

6.3 We may process the following categories of Personal Information about you:

6.3.1 Personal details: name, identity number / passport number and photograph;

6.3.2 Demographic information: gender; date of birth / age; nationality; salutation; title; language preferences;

6.3.3 Contact details: correspondence address; telephone number; email address; details of your public social media profile(s);

6.3.4 Transactional details: details of individuals transacting with us;

6.3.5 Personal Information included in correspondence, documents, evidence or other materials that we process while providing our services;

6.3.6 Attendance records: details of meetings and other events organised by us that you have attended;

6.3.7 Consent records: records of any Consents you may have given, together with the date and time, the means of Consent and any related information;

6.3.8 Payment details: billing address; payment method; bank account number; invoice records; payment records; SWIFT details; payment amount; payment date;

6.3.9 Data relating to your visits to our website: your device type; operating system; browser type; browser settings; IP address; language settings; dates and times of connecting to a website; and other technical communications information;

6.3.10 Your employer details: where you interact with us in your capacity as an employee of an organisation, the name, address, telephone number and email address of your employer, to the extent relevant.

6.4 Our firm understands the importance of obtaining our data subjects' Consent, where necessary, to share their information and possibly using the information for limited marketing purposes.

6.5 If personal information is used for any other reason than the original reason it was collected, the specific Consent for such purpose will be obtained from the data subject.

6.6 Further processing of personal information must be compatible with purpose of collection, unless the data subject has consented to such further processing.

6.7 Where personal information is transferred to a third party for further processing, the further processing must be compatible with the purpose for which it was initially collected, unless the data subject has Consented to such further processing or it is permitted in terms of POPIA.

6.8 If personal information is to be used for any other purpose, the further Consent of the data subject must be obtained. Where this is not possible, the Information Officer should be consulted.

6.9 Our firm does not use information for any purpose other than what it was collected for.

6.10 If special personal information is collected, processed and stored for any reason from any of our firm's data subjects, a specific Consent for such collection will first be obtained.

6.11 There are instances in which this specific Consent will not be required:

6.11.1 If collection and processing are carried out with the prior Consent of the data subject;

6.11.2 If collection and processing are necessary for the establishment, exercise or defence of a right or obligation in law;

6.11.3 If collection and processing are for historical, statistical or research purposes;

6.11.4 If we are obliged to collect and process your information in terms of regulation.

6.12 Our standard documentation now reflects the Consent mentioned herein and in compliance with the POPIA.

7 STORAGE OF INFORMATION

7.1 Management of our firm and all employees of our firm remain aware of the risks facing data subjects with the storage of personal and special personal information on our firm's software systems as well as filing copies of the physical information sheets containing personal information physically in our office.

7.2 Our firm stores personal information in its possession:

7.2.1 At our business premises, in the form of hard copies, where necessary;

7.2.2 On our firm's physical and cloud-based servers; or

7.2.3 On the servers of third-party service providers, such as IT systems or hosting service providers.

7.3 Our firm will continuously take reasonable technical and organisational measures to secure the integrity of data in our possession. This includes adopting technological standards to prevent unauthorised access to or disclosure of data, and protect information of data subjects from misuse, loss, alternation and destruction.

7.4 Periodical reviews of our firm's personal information practices and processes regarding collection, storage and technical security measures will be conducted.

7.5 Our firm will ensure that the contracts between itself and third-party service providers and/or contractors and sub-contractors are updated regularly to secure the integrity and confidentiality of personal information in our possession.

7.6 Our firm shall retain records of the personal information that it has collected for the minimum period as required by law, unless the client or data subject in question has furnished their consent or as long as reasonably necessary.

7.7 To ensure that our best attempts are made to minimize data subjects from suffering loss of personal information, misuse or unauthorised alteration of information, unauthorized access or disclosure of personal information generally, we will:

7.7.1 Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.

7.7.2 Monitor the latest internet developments to ensure that the systems evolve as required. Our firm tests our systems regularly to ensure that our security mechanisms are up to date.

7.7.3 Continue to review our internal policies and third-party agreements, where necessary, to ensure that they comply with POPIA and the Regulations, in line with our firm's general Data Privacy Terms.

7.8 Our firm is subject to the record keeping requirements provided in many South African laws, including but not limited to: the Legal Practice Act, the Financial Intelligence Centre Act, the Income Tax Act and The Companies Act of South Africa. To this end and to be sure that we comply with regulatory record keeping duties, our firm has developed and implemented our RECORD KEEPING AND ARCHIVING POLICY, which is reviewed annually.

7.9 It is further specifically recorded that any documents provided to our offices and forming part of the pleadings in litigious matters are filed at the relevant court, whereafter such documents become public documents and may be accessed by third parties.

8 DISPOSAL OF DATA SUBJECTS' INFORMATION

8.1 As provided for in our firm's RECORD KEEPING AND ARCHIVNG POLICY, our firm commits to its responsibility to ensure that records that are no longer needed or are of no value are disposed of when necessary.

8.2 These rules apply to all documents and information which are collected, processed or stored by our firm and include, but are not limited to, documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

8.3 Our firm's RECORD KEEPING AND ARCHIVING POLICY determines when and how information and communications with and to our clients are kept and stored and when information would be destroyed including, but not exclusively limited to:

8.3.1 How emails are stored and when emails are deleted;

8.3.2 How client data is stored, on which software systems and when these are destroyed;

8.3.3 How physical copies of information and communications are stored and when these are destroyed;

8.3.4 How our software and hardware products are monitored and that appropriate rules are implemented with regards to storage of data subjects' information hereon.

8.4 As a matter of course, we do not discard or dispose of the telephone numbers, email addresses of data subjects and electronic communications with data subjects with whom we have previously dealt but will do so on request by the data subject.

8.5 However, since our firm recognizes that most of the information which it collects, processes and shares with other role players in transactions is personal in nature, we do not let information lie around and keep strict controls in respect of access to our software systems.

8.6 For this reason, we will dispose of information securely when no longer required or when being requested by the data subject.

8.7 Our firm acknowledges that electronic devices and media hold vast amounts of information, some of which can linger indefinitely, and we follow the following rules strictly:

8.7.1 Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited at refuse tips.

8.7.2 Our firm will ensure that all electrical waste, electronic equipment and data on disk drives are physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.

8.7.3 Our firm will also ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.

8.7.4 In the event that a third party is used for data destruction purposes, our firm's Information Officer will ensure that such third party also complies with our rules and any other applicable legislation.

8.8 Our firm may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings and we undertake to notify employees of applicable documents where the destruction has been suspended to which they have access.

8.9 In the event that a document and/or information is no longer required to be stored in accordance with either legislation or in line with our own rules, it should be deleted and destroyed.

8.10 Our firm's Information Officer will give direction where there is uncertainty regarding the retention and destruction of a document and/or information.

9. OUR FIRM'S DATA SUBJECT'S RIGHTS

9.1 Our firm recognises that our data subjects have the right to request that our firm confirms, free of charge, whether or not it holds personal information about the data subject and request the firm to provide a record, or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information at a prescribed fee.

9.2 All of our firm's data subjects or such competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, provided that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information is not affected.

9.3 Any of our data subjects may object, at any time, to the processing of personal information–

9.3.1 In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

9.3.2 For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

9.4 All of our data subjects, having provided adequate proof of identity, have the right to–

9.4.1 Request us to confirm, free of charge, whether we hold personal information about the data subject; and

9.4.2 Request a record or a description of the personal information about the data subject held by us including information about the identity of all third-parties, or categories of third-parties, who have, or have had, access to the information – within a reasonable time; at a prescribed fee as determined by our firm's Information Officer; in a reasonable manner and format; and in a form that is generally understandable.

9.5 Our data subjects may, in the prescribed manner, request our firm to –

9.5.1 correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

9.5.2 destroy or delete a record of personal information about the data subject that our firm is no longer authorised to retain.

9.6 Upon receipt of a request referred to in clause 9.5, our firm will, as soon as reasonably practicable –

9.6.1 correct the information;

9.6.2 destroy or delete the information;

9.6.3 provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or

9.6.4

9.6.5 if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

9.7 Our firm will inform the data subject, who made a request, as set out in clause 9.5, of the action taken as a result of the request.

9.8 All users will comply with our firm's data subject access request policy and PAIA manual in respect of any access to personal information requests by data subjects.

9.9 Our firm will provide credible proof to the client/data subject of the action that has been taken in response to the request. If any changes to the personal information will have an impact on any decisions to be made about the data subject/client, the firm will inform all third parties to whom the information has been disclosed, including any credit bureaus, of such changes.

9.10 Please refer to **ANNEXED FORM 1** of the POPIA Regulations attached hereto should you wish to object to the processing of your Personal Information.

9.11 Please refer to **ANNEXED FORM 2** of the POPIA Regulations attached hereto should you wish to request for the correction or deletion of your Personal Information.

10 CYBER TECHNOLOGY

10.1 Standard Anti-Virus rules

10.1.1 In order to ensure that our firm's IT systems are not misused and in accordance with our firm's INTERNAL IT AND INTERNET USAGE POLICY as well as our firm's BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN, everyone who uses or has access to our systems have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

10.1.1.1 Information will be protected against any unauthorized access as far as reasonably possible;

10.1.1.2 Confidentiality of information will be assured as far as reasonably possible;

10.1.1.3 Integrity of information will be preserved as far as reasonably possible;

10.1.1.4 Availability of information for business processes will be maintained;

10.1.1.5 Compliance with applicable laws and regulations to which our firm is subject will be ensured by our Information Officer as far as reasonably possible.

10.1.2 Every user of our IT systems takes responsible for exercising good judgment regarding reasonable personal use.

10.1.3 Management of our firm is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into our firm's programs (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

10.1.4 Our firm's employees are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from our firm's networks, stop using the infected computer immediately and notify the IT Coordinator.

10.1.5 It is further worth noting that our firm's users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments.

10.1.6 Our firm has entered into confidentially agreements with every staff member to ensure full confidentiality in respect of all of our clients' affairs, including our clients' Personal Information.

10.1.7 Employees are trained to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.

10.1.8 The digital work profiles and privileges of staff who have left our employ are properly terminated.

10.1.9 All employees have received and will continue to receive internal training in respect of such viruses and how to identify them and what to do if a virus is suspected.

10.2 IT Access Control

10.2.1 Only authorized employees may log into our firm's IT system and software packages, and these are password controlled.

10.2.2 All employees of our firm exercise caution in allowing unauthorized access to a password and our firm's IT Coordinator ensures that the passwords are reviewed and renewed from time to time by the External IT Service Provider- in particular where GOOGLE based products are used and linked (such as Facebook, WhatsApp and GMAIL based domains).

10.3 Email Rules

10.3.1 Most of our firm's digital communications are conducted via email and instant messaging (IM).

10.3.2 Given that email and IM may contain extremely sensitive and confidential information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware.

10.3.3 The misuse of email and IM can pose many legal, privacy and security risks, so it is important for users of our firm's services to be aware of the appropriate use of electronic communications.

10.3.4 Ourfirm's employees are further prohibited from using email for personal use in accordance with the Internal IT and Email Usage Policy.

10.3.5 Our firm has implemented an INTERNAL IT AND EMAIL USAGE POLICY in order to set out rules for employees to follow and to create the necessary framework and accountability in the event of misuse or negligence.

10.4 Our firm's rules related to handheld devices

10.4.1 Insofar as the use of personal devices is concerned, our firm has implemented internal rules related to the corporate usage of personal devices, within the INTERNAL IT AND INTERNET USAGE POLICY which shall address the risks associated with:

10.4.1.1 Loss, disclosure, corruption or manipulation of corporate data on personally owned devices;
10.4.1.2 Incidents involving threats to, or compromise of, the firm's IT infrastructure and other information assets (e.g. malware infection or hacking);
10.4.1.3 Non-compliance with applicable laws, regulations and obligations (e.g. privacy or piracy);
10.4.1.4 Intellectual property rights for corporate information created, stored, processed or communicated on these devices in the course of work.

10.4.2 Management reserves the right not to authorize individuals, or to withdraw the authorization, if they deem access to personal information on the employees personal device not to be appropriate and in the best interests of the organization.

10.4.3 Our firm safeguards the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices like PC's and Notebooks and our firm's Information Officer and the IT department ensures that:

10.4.3.1 Our firm's users of handheld devices diligently protect their devices from loss and disclosure of private information belonging to or maintained by our firm and that this is achieved with constant awareness training.

10.4.3.2 Before connecting a mobile handheld device to the network at our firm, users are expected to ensure it is on the list of approved devices issued by the IT support wherever necessary.

10.4.3.3 In the event of a security incident or if suspicion exists that the security of our firm's systems has been breached, the person in our firm who becomes aware of the breach shall notify the IT Coordinator immediately together with our firm's Information Officer, especially when a mobile device may have been lost or stolen.

10.4.4 The siting of the equipment should ensure that routine and emergency maintenance of the equipment should be possible to be carried out effectively. Such maintenance should be carried out in accordance with the supplier's recommended service intervals and specifications.

10.4.5 Movements of equipment should be tracked.

10.4.6 Adequate contacts with other authorities including utilities, emergency services, health and safety departments, should be in place.

10.4.7 Decommissioning / disposal of IT and non-IT equipment should be done, and measures should be deployed to ensure that no advertent or inadvertent loss of data / violation of any regulatory compliance take place.

10.5 Tracking Technologies and Cookies

10.5.1 Cookies and similar tracking technologies are used to track the activity on our firm's website and to store certain information.

10.5.2 Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyse the efficiency of the website. The technologies which may be used to track may include:

10.5.2.1 Cookies or Browser Cookies. A cookie is a small file which may be placed on a data subject's device. Data subjects can instruct their browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if this function of our website is not accepted, data subjects may not be able to use some parts of the website. Unless the browser settings have been adjusted, our website may use Cookies.

10.5.2.2 Flash Cookies. Certain features of the website may use local stored objects (or Flash Cookies) to collect and store information about data subjects' preferences or activity on the website. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies. For more information on how

Flash Cookies can be deleted the following process can be followed: "Where can I change the settings for disabling or deleting local shared objects" available at:

https://helpx.adobe.com/flashplayer/kb/disable-local-shared-objects.

10.5.2.3 Web Beacons. Certain sections of the website and emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit our firm access for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

10.5.3 Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on data subjects' personal computer or mobile device even when offline, while Session Cookies are deleted as soon as data subjects' web browsers are closed.

10.6 Physical access control

10.6.1 All of our firm's premises that include computers and other types of information technology resources will, as far as reasonably possible, be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats.

10.6.2 This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, , security guards, and fire protection.

11 THIRD PARTY OPERATORS

11.1 In order for our firm to operate efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to our service delivery.

11.2 Operators (i.e. third parties which may process personal information on behalf of our firm) include marketing database companies, recruitment agencies, psychometric assessment centres, document management warehouses, external consultants and software providers.

11.3 Our firm will implement the following key obligations in respect of operators:

11.3.1 The operator may not process personal information on behalf of our firm without the knowledge and authorisation of our firm;

11.3.2 Our firm will ensure that the operator implements the security measures required in terms of our Data Privacy Terms and Conditions;

11.3.3 There will be a written contract in place between our firm and the operator, THE THIRD-PARTY OPERATOR'S NON-DISCLOSURE AGREEMENT which requires the operator to maintain the confidentiality and integrity of personal information processed on behalf of our firm; and

11.3.4 If the third party is located outside of South Africa, our firm will comply with the requirements in POPIA in respect of transborder transfers of personal information.

11.4 In the event that personal information has been compromised, or if there is a reasonable belief that a compromise has occurred, our firm (or an operator processing personal information on its behalf) will notify the Information Regulator and the relevant data subjects (if their contact details are available).

11.5 As referenced in clauses 1 to 5 above, where necessary we will obtain Consent from the particular data subject.

11.6 These OPERATORS' AGREEMENTS are necessary in order to ensure that the third-party operator treats the personal information of our data subjects responsibly and in accordance with the provisions contained in the POPI Act and Regulations thereto.

11.7 When we present our OPERATORS' AGREEMENTS to a third-party for signature, we usually request copies of the third-party operators' POPIA Policy, rules, internet rules and details of the third-party's Information Officer.

12 BANKING DETAILS

12.1 It is a known fact that South African businesses are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of transactions.

12.2 Our data subjects are open to large amounts of damages and losses if emails are intercepted, and banking details are fraudulently amended without the data subject's knowledge.

12.3 We have implemented an INTERNAL PAYMENTS POLICY which has been circulated to all employees and in accordance with which our employees are formally held liable when not following our rules as well as clear warnings within all our correspondences (emails and physical letters) warning data subjects of the risks of email hacking and interceptions.

12.4 In the event that banking details are sent to data subjects or received from data subjects for purposes of payment, the banking must be confirmed with a telephone call.

12.5 It is recorded that, in certain instances, data subjects' bank details are to be shared with relevant third parties but in such event, all care shall be taken.

13 DIRECT MARKETING

13.1 Our firm does not share data subjects' information with third-parties for the sole purpose of using the information for direct marketing.

13.2 Our firm may send out marketing and information emails out to our database of existing clients from time to time.

13.3 We will always ensure that the required OPTING OUT/UNSUBSCRIBE options which allow the recipients of the emails to request a removal of their details from these bulk emails are clearly implemented.

13.4 Management of our firm will, from time to time, send necessary information to the firm's client base and to this end, the directors will discuss and update the firm's direct marketing strategies.

13.5 We may utilise the Personal Information of an existing client of the firm for the purposes of providing our client with information regarding services that may be of interest to the client (direct electronic marketing).

13.6 New clients of the firm must be given an opportunity to opt in to receiving direct marketing material by electronic communication at the time that their personal information was collected.

13.7 Our firm may only approach clients using their Personal Information if we have obtained their Personal Information in the context of providing legal services to them, and we may then only market legal and ancillary services to them.

13.8 Our firm may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

13.9 Should our firm receive consent to send direct electronic marketing to a non-client of the firm, such direct electronic marketing material must have an opt-out option.

13.10 If you currently receive marketing information from us which you would prefer not to receive in the future, please email us at nicole@goldlaw.co.za.

13.11 Our firm does not make "cold calls" and our number should not appear on our data subjects' devices as "spam".

14 DATA CLASSIFICATION

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

14.1 Our firm considers most, if not all of our data subjects' information as confidential. However, certain information is inherently available on public domains and certain information is proprietary to our firm.

14.2 In accordance with our firm's DATA CLASSIFICATION POLICY, all of our firm's employees share in the responsibility for ensuring that our information assets receive an appropriate level of protection as set out hereunder:

14.2.1 Our firm's Directors, in consultation with the IT Coordinator, are responsible for assigning classifications to information assets according to the standard information classification system presented below.

14.2.2 Where practicable, the information category shall be embedded in the information itself.

14.2.3 All employees of our firm shall be guided by the information category in their security-related handling of all information.

14.2.4 All information entrusted to us from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

Information Description	Examples	Category
Public Data	Information which is not confidential and can be made public without any implications for our firm	Marketing brochures widely distributed Information widely available in the public domain, including publicly available web site areas. Financial reports required by regulatory authorities. Newsletters for external transmission
Proprietary Data	Information, which is restricted to management, approved internal access and protected from external access. Unauthorized access could influence our firm's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in client confidence. Information integrity is vital.	Passwords and information on corporate security procedures Know-how used to process client information Standard Operating Procedures used in all parts of our firm's activities All software codes developed by our firm whether used internally or externally
Confidential Data	Information, which is collected and used by our firm in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data Accounting data and internal financial reports Confidential client business data and confidential contracts Non-disclosure agreements with clients/ vendors Firm business plans. Email and telephone communications with clients and suppliers Transactional documentation related to a matter in which a client is involved Client FICA information Client POPIA information Employee POPIA information

15 INFORMATION OFFICER

15.1 Our firm's appointed Information Officer is:

NICOLE SCHOLTZ

Postal address: P O Box 1282, Port Eizabeth, 6000
Registered address: Pembridge House, 13 Bird Street, Central, Gqeberha, 6001
Physical Address: Pembridge House, 13 Bird Street, Central, Gqeberha, 6001
Tel: 041 501 9800

EMAIL: nicole@goldlaw.co.za

15.2 Our Information Officer is duly appointed by Management of our firm. She refers to the Information Regulator's Guidance Note in order to ensure that she fulfils her duties as required in terms of section 55 of POPIA. InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf

15.3 The general responsibilities of our firm's Information Officer include the following:

15.3.1 To ensure that a compliance framework is developed, implemented, monitored and maintained;

15.3.2 To ensure that a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

15.3.3 That a Manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of PAIA, as amended;

15.3.4 That internal measures are developed together with adequate systems to process requests for information or access thereto;

15.3.5 That internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator;

15.3.6 That, upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time;

15.3.7 To ensure that the INCIDENT RESPONSE POLICY is circulated to all employees and that data incidents are properly managed when they occur;

15.3.8 To encourage compliance, by all employees with the conditions for the lawful processing of personal information;

15.3.9 To work with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the firm.

15.3.10 To ensure continuous data backups and test those backups regularly for data integrity and reliability.

15.3.11 To review policy rules regularly, document the results, and update the policy as needed;

15.3.12 To continuously update information security policies and network diagrams;

15.3.13 To ensure that critical operational applications and data are secure by patching known vulnerabilities with the latest fixes or software updates; and

15.3.14 To perform continuous computer vulnerability assessments and audits.

15.3.15 Registration of Information Officers with the Regulator is not only the prerequisite for an Information Officer to take up their duties in terms of POPIA but is a compulsory requirement for every person identified and appointed by the firm as Information Officer.

15.4 Annual filing requirements:

15.4.1 The Information Officer must annually, in terms of section 32 of PAIA, submit to the Regulator a report regarding:

15.4.1.1 The number of requests for access received; the number of requests for access granted in full; the number of requests for access granted in terms of section 46 of PAIA;

15.4.1.2 The number of requests for access refused in full and refused partially and the number of times each provision of PAIA was relied on to refuse access in full or partially;

15.4.1.3 The number of cases in which the periods stipulated in section 25(1) of PAIA were extended in terms of section 26 (1) of PAIA;

15.4.1.4 The number of internal appeals lodged with the relevant authority and the number of cases in which, as a result of an internal appeal, access was given to a record;

15.4.1.5 The number of internal appeals which were lodged on the ground that a request for access was regarded as having been refused in terms of section 27 of PAIA;

15.4.1.6 The number of applications to a court which were lodged on the ground that an internal appeal was regarded as having been dismissed in terms of section 77 (7) of PAIA.

15.4.2 The Regulator may, annually, request an Information Officer of a private body, in terms of section 83 (4) of PAIA, to furnish to the Regulator with information about requests for access to records of that body.

15.5 Delegation of duties to a Deputy Information Officers:

15.5.1 An Information Officer(s) of both a public or private body may, subject to legislation and policies governing the employment of personnel of the body concerned, delegate any power or duty conferred or imposed on him or her to a Deputy Information Officer of that body in terms of section 56(b) of POPIA and section 17(3) of PAIA;

15.5.2 Only an employee of a body can be delegated as a Deputy Information Officer;

15.5.3 At the time of drafting these terms and conditions, the firm had not formally appointed a Deputy Information Officer, and these clauses are inserted herein for purposes of future reference when and if the firm appoints such a Deputy.

15.5.4 The delegation referred to above must be in writing, using the template provided in the Information Regulator's Guideline – InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf;

15.5.5 The delegation of any powers or duties and responsibilities to a Deputy Information Officer does not prohibit an Information Officer from exercising the powers or performing the duty that he or she has delegated to a Deputy Information Officer;

15.5.6 Any power, duties and responsibilities delegated to a Deputy Information Officer should be exercised or performed subject to such conditions as an Information Officer may consider necessary;

15.5.7 Any conditions of delegation, as conferred on the Deputy Information Officer, should ensure that the body is as accessible as reasonably possible for data subjects or requesters;

15.5.8 An Information Officer of a body must ensure that he or she reserves his or her rights in the aforesaid delegation to exercise the powers or to perform the duties and responsibilities concerned himself or herself; and withdraw or amend the aforesaid delegation at any time;

15.5.9 An Information Officer must be aware that any right or privilege acquired, or any obligation or liability incurred as a result of a delegation of any powers, duties and responsibilities is not affected by any subsequent withdrawal or amendment of the decision to delegate;

15.5.10 Depending on the circumstances of the case, the obligation or liability incurred as a result of any delegation of any powers, duties and responsibilities may be imposed on either the Information Officer or our firm in so far as POPIA is concerned in line with section 17(6)(b) of PAIA;

15.5.11 To ensure a level of accountability by a delegated Deputy Information Officer, bodies are encouraged to ensure that such duties and responsibilities or any power delegated to a Deputy Information Officer is part of his or her job description;

15.5.12 Despite the above-mentioned delegation of a Deputy Information Officer, an Information Officer retains the accountability and responsibility for the functions delegated to the Deputy Information Officer;

15.5.13 To ensure accessibility of the body, the Deputy Information Officer(s) of a multinational entity must be based within the Republic.

15.6 The data breach responsibilities of our firm's Information Officer include the following:

15.6.1 Ascertaining whether personal data was breached;

15.6.2 Assessing the scope and impact by referring to the following:

15.6.2.1 Estimated number of data subjects whose personal data was possibly breached;

15.6.2.2 Determining the possible types of personal data that were breached; and

15.6.2.3 Listing the security measures that were already in place to prevent the breach from happening.

15.6.3 Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:

15.6.3.1 The Information Regulator;

15.6.3.2 Any data subject of the firm who may require notification.

15.6.4 Communication should include the following:

15.6.4.1.1 Contact details of Information Officer;

15.6.4.1.2 Details of the breach;

15.6.4.1.3 Likely impact;

15.6.4.1.4 Actions already in place, and those being initiated to minimise the impact of the data breach; and

15.6.4.1.5 Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

15.7 Review and monitor

15.7.1 Once the personal data breach has been contained, our firm will conduct a review of existing measures in place and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.

15.7.2 All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

16. AVAILABILITY AND REVISION

16.1 A copy of this Policy is made available on our firm's website https://www.goldbergdevilliers.co.za/ and in possession of our Information Officer - nicole@goldlaw.co.za and at our Gqeberha office.

16.2 This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.

Goldberg & de Villiers Inc.
Attorneys, Notaries & Conveyancers

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

ANNEXURE A

CYBER SECURITY MEASURES IN PLACE

THE FIRM'S CYBER SECURITY MEASURES

KONDURA TECHNOLOGIES
multi technical services

www.kondura.co.za

VAT NO.: 4280280472
CC REGISTRATION: 2014/024421/07
PROPRIETOR: JOCOTE (PTY) LTD.

26 September 2025

GOLDBERG & DE VILLIERS
Pembridge House
13 Bird Street
PORT ELIZABETH

Disaster Recovery Requirements

Server restores has been done in a lab environment, we make use of Veeam Backup and Replication so the entire Virtual Server is backed up and encrypted, we can restore and start the Virtual Server on any Host Server.

To restore any data the actual server is mounted, and we can extract a single file or the entire server, therefore any restore tests serves as data backup integrity.

Their physical host is on a Next Business Day hardware Warranty, so recovery is dependent on when the server fails and if it is hardware related, the actual Data restore could take up to 24hrs due to the size of data.

TYPE OF CYBER SECURITY MEASURES	WRITTEN SUMMARY OF MEASURES * I would prefer these measures on a letterhead please	WHO CONTROLS THE UPDATING	HAS A CYBER AUDIT BEEN DONE	HAVE CYBER INCIDENTS BEEN PICKED UP
FIREWALL	Arista	Automatically	Carnegie Penetration Tests are performed monthly	None
ANTI VIRUS	ESET End Point Security	Automatically	None	None Known
DOUBLE AUTHENTICATION	Bitlock / Eset Encryption Key	Kondura Technologies	None	None
DEVICES PRIVACY SETTINGS ACTIVATED	Software Default Policy	Automatically	None	
EMAIL BACK UPS	Microsoft 365	Kondura Technologies	None	None
SYSTEM BACK UPS	Veeam	Kondura Technologies	Yes	None
SSL ENCRYPTION	N/A	N/A	N/A	N/A
PASSWORD MANAGEMENT	Kondura Technologies CC	Kondura Technologies	None	None

041 450 6288
info@kondura.co.za

193 Cape Road
Mill Park,
Port Elizabeth
6001

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

KONDURA TECHNOLOGIES
multi technical services

www.kondura.co.za

VAT NO.: 4230180472
CO REGISTRATION: 2014/094431/07
PROPRIETOR: JOCOTE (PTY) LTD

SOFTWARE UPDATES	Microsoft	Automatic	None	None

1. Please can I have a list of operating systems/applications and programs on which the firm relies?

PLEASE SPECIFY THE SOFTWARE SYSTEM	COMPANY WHO SUPPORTS YOU	CONTACT DETAILS OF COMPANY WHO SUPPORTS YOU	BACK UPS	Notes
FOR EMAILS	Kondura Technologies	Claude Botha – 073 764 7693	Yes	Microsoft Exchange
OPERATING SYSTEM	Kondura Technologies	Claude Botha – 073 764 7693	Yes	
BACK UPS	Kondura Technologies	Claude Botha – 073 764 7693	Yes – External Hard Drive & NAS	Encrypted
MARKETING	GAIA Marketing	Bev Gaia - 083 657 5671		
DEEDS OFFICE SEARCHES	Searchworks Windeed	Call Centre – 0860 34 0000 LexisNexis – Jade Snygans - 0614901234		Web Based Web Based
TENANT SEARCHES	Windeed	LexisNexis – Jade Snygans – 0614901234		Web Based
ACCOUNTS	Dye & Durham - GhostPractice	Teegan Kleynhans – 082 619 3567	Yes	SQL Databased
HR	BDO - Accountants	Bernadette Zeelie – 073 600 7762		Simple Pay System
KYC + FICA	Lexis KYC	LexisNexis – Jade Snygans - 0614901234		Web Based
SPECIFY OTHER	Lexis Convey	LexisNexis – Chantel Meyer - 083 500 6222	Yes	SQL Database

Claude Botha
Director
Kondura Technologies

041 450 6288
info@kondura.co.za

193 Cape Road
Mill Park,
Port Elizabeth
6001

MECER Lenovo VEEAM Office 365

Information and Communication Technology
Disaster Recovery Policy

1. MANDATE OF THE IDSS

It is the mandate of the IDSS (Internet and Digital Service Suppliers to the firm) to ensure business recovery and availability of critical operational data, confidential and proprietary data during or after a loss of normal business operations.

2. OBJECTIVE OF THE POLICY

2.1. The objective of this policy is to provide a plan that responds to a disaster that destroys or severely cripples the IDSS services.

2.2. The intent is to restore critical business operations as quickly as is practical with the latest and most up-to-date data available.

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

---

3. APPLICABILITY OF THE POLICY

This policy applies to the IDSS Division of the Company.

4. TERMS AND DEFINITIONS

Term	Definition
Disaster Recovery	Disaster Recovery (DR) is the restoration of systems and infrastructure back to agreed service levels following a disaster. This may be temporary in the first instance, requiring full-service restoration later.
Risk Assessment	Risk Assessment: The overall process of risk analysis and risk evaluation.

5. ACRONYMS

COBIT: Control Objectives for Information Technology.
IDSS: Information and Communication Technology.
IDSSSC: Information and Communication Technology Steering Committee.
ITIL: Information Technology Infrastructure Library.

6. REFERENCES

6.1. International Guidelines Control Objectives for Information Technology (COBIT).
6.2. International Standards:
6.2.1. Information Technology Infrastructure Library (ITIL).
6.2.2. ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management.
6.2.3. ISO24762 (ISO 24762) Disaster Recovery Services.
6.3. National Policy
6.3.1. Constitution of the Republic of South Africa, Act 108 of 1996.
6.3.2. The Electronic Communications and Transactions (ECT) Act 25 of 2002.
6.3.3. National Strategic Intelligence Act 2 of 2000 applicable for South Africa.
6.3.4. Regulation of Interception of Communications Act 70 or 2002.
6.3.5. State Information Technology Act 88 of 1998.

7. POLICY STATEMENT

This policy is developed to guide the IDSS of the firm in the recovery of data, information, computing and network services in the event that a disaster destroys all or part of the firm's buildings.

8. INFORMATION BACKUP

8.1. Backups shall be scheduled to run after working hours.
8.2. There shall be daily, weekly and monthly backups.
8.3. Backup copies shall be taken to the safe or storage area within the first hour of the business day of the morning after finished backup process.
8.4. Backup strategy or procedure shall specify the exact time on which the backup is scheduled to start running, and on when the backup copies shall be taken to the safe or storage area.
8.5. Backup procedures are documented in writing and updated on regular basis as changes are required.
8.6. There shall be a system administrator assigned to perform the system backups.
8.7. The system administrator shall inspect the backup log to verify the success of the backup and troubleshoot hardware and or software problem related to backup procedure.
8.8. An electronic log of each backup performed will be created by the system administrator and mailed to IDSS monthly for monitoring.
8.9. Log files shall be analysed and for any errors, corrective measures shall be taken every time before taking the backup tapes for safe storage.
8.10. Access to the backup copies in a safe or storage area shall be limited to the system administrators doing the backups.
8.11. Users shall be responsible for ensuring that all essential business information under their control is backed-up.
8.12. Monthly backup copies for staff personnel records will be retained for an indefinite time period (five years).
8.13. Adequate backup facilities should be in place to ensure proper functioning of backup process.

9. EXCLUSIONS

9.1. Restorations are not intended for the following purposes:
9.1.1. Personal data such as photos, videos, music and unofficial e-mail accounts.
9.1.2. Application programs not officially supported by IDSS.
9.1.3. Exceptionally large images (scanned or digitized material) and large video files.
9.1.4. Any lost data not beyond the scope.

10. ROLES AND RESPONSIBILITIES

10.1. The IDSS shall ensure essential business information is backed up at appropriate time intervals.
10.2. The system administrator shall ensure information is backed up as regularly as agreed.
10.3. In support of this policy, all the employees must support and comply with the controls that have been put in place by the IDSS.
10.4. Users shall be responsible for saving official files to the specified network shares.

11. DISASTER RECOVERY STRATEGIES

11.1. The IDSS shall ensure that every server is backed up regularly.
11.2. The turnaround time to receive a backup tape for recovery is maximum 2 hours.
11.3. The system administrator will initiate data recovery processes for the data that has been destroyed by the disaster.
11.4. The restoration time will depend on the amount of data to be retrieved.
11.5. A minimum level of backup information, together with accurate and complete records of the backup copies and documented restoration procedures, should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at main site.
11.6. Backup information should be given an appropriate level of physical and environmental protection, consistent with the standards applied at the main site.
11.7. Backup media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.
11.8. Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the recovery time that has been allotted in the operational procedures for recovery.

12. INITIATION OF DATA RECOVERY PROCEDURES THE IDSS

12.1. **Recovery Actions**

12.1.1. Prepare a detailed assessment of extent of damage; in particular assess extent of damage to network or telecommunications infrastructure in the server room.
12.1.2. Locate and validate relevant backup media if Information Systems are affected.
12.1.3. Call external support contractors (if appropriate) and advise them of extent of damage.
12.1.4. Assess likely duration of disruption to critical services and consider relocating essential users to an alternative site.
12.1.5. Ascertain if there is serviceable computer equipment in critical service areas. Locate backup media and schedules.
12.1.6. Update events log.
12.1.7. Review initial assessment.
12.1.8. Make decisions regarding recovery actions or implementation of manual procedures.
12.1.9. Secure funding if necessary.
12.1.10. Decide on personnel needed for next phase of recovery.
12.1.11. Make initial announcement to Company employees on affected systems.

12.2. **Full Recovery Actions**

12.2.1. Continue installation of replacement equipment (if necessary) with assistance as necessary from external service providers.
12.2.2. Restore from backup media.
12.2.3. Check that critical areas can access the network and take remedial action as necessary.
12.2.4. As systems become operational, the IDSS division will consult with employees to confirm that systems are fully functional before users are granted access.
12.2.5. Prepare and release further external statements if service to clients are affected.
12.2.6. When recovery is complete:
12.2.7. Prepare final report for senior management;
12.2.8. Review actions taken and lessons learnt; and
12.2.9. Update plan

Goldberg & de Villiers Inc.
Attorneys, Notaries & Conveyancers

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

ANNEXURE B

THESE FORMS ARE TO BE DIGITISED AND PUBLISHED ON THE FIRM'S WEBSITE ALONGSIDE THIS POLICY

REGULATED FORM 1

documents (dsd.gov.za)

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 2]

Note:

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 is applicable.*

FORM 1
OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017 [Regulation 2(1)]

Note:

1. Affidavits or other documentary evidence in support of the objection must 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.

Reference Number....

A	DETAILS OF DATA SUBJECT
Name and surname of data subject:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name and surname of responsible party (if the responsible party is a natural):	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
Name of public or private body (if the responsible party is not a natural person):	
Business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
C	REASONS FOR OBJECTION (Please provide detailed reasons for the objection)

Signed at ..... this ..... day of .....20.....

.....
Signature of data subject (applicant)

Goldberg & de Villiers Inc.
Attorneys, Notaries & Conveyancers

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

REGULATED FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYINGORDELETIONOFRECORDOFPERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 3]

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. *Complete as is applicable.*

FORM 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 NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017 [Regulation 3(2)]

Note:

1. Affidavits or other documentary evidence in support of the request must 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.

Reference Number....
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 possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Surname:	
Full names:	
Identity number:	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name and surname of responsible party(if the responsible party is a natural person):	
Residential, postal or business address:	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
Name of public or private body (if the responsible party is not a natural person):	
Business address:	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	

C	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT/*DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY. *(Please provide detailed reasons for the request)*

* Delete whichever is not applicable

Signed at ..... this ..... day of .....20.....

.....
Signature of Data subject

Goldberg & de Villiers Inc.
Attorneys, Notaries & Conveyancers

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

REGULATED FORM 3

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 6]

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname/ registered name of data subject	
Unique identifier/Identity number	
Residential, postal, or business address:	
	Code
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ registered name of responsible party or designated person	
Responsible party signature	
Unique identifier/Identity number	
Residential, postal, or business address:	
	Code
Contact number(s):	
Fax number/E-mail address:	
C	**GOODS OR SERVICES** (Specify goods or services being marketed)
D	**MARKETING METHOD** (Specify marketing method, i.e., email)

My signature below confirms that I have consented to received direct marketing pertaining to the goods or services specified above by the means of the marketing method specified.

Signed at _____ this _____ day of _____ 20_____

_____

Signature of data subject/designated person

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

DEFINITIONS

1. **"Biometrics":** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
2. **"Child":** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;
3. **"Competent person":** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
4. **"Data subject":** means the person to whom personal information relates and for the purposes of our firm, this will include but not be limited to our clients, employees, external service suppliers and all associates of our firm;
5. **"Direct marketing":** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – a) Promoting or offering to supply, in the ordinary course of business our firm, our legal services to the data subject; or b) Requesting the data subject to make a donation of any kind for any reason;
6. **"Electronic communication":** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
7. **"Filing system":** means any structured set of personal information which in the case of our firm consists of physical files kept in the offices of our firm together with the data filed on the various software systems used by our firm;
8. **"Information Officer":** of our firm will mean **NICOLE SCHOLTZ;**
9. **"Operator":** means a person or entity who processes personal information for our firm in terms of a contract or mandate, without coming under the direct authority of our firm;
10. **"Our firm":** for purposes of these Data Privacy Terms and Conditions means:

BUSINESS NAME	**GOLDBERG AND DE VILLIERS INCORPORATED**
REGISTRATION NUMBER	**1999/005587/21**
BUSINESS ADDRESS	**PEMBRIDGE HOUSE, 13 BIRD STREET, CENTRAL, GQEBERHA, 6001**

with all employees in our firm, whether permanent or temporary, who constitute the firm included insofar as their obligations are concerned and contained in this Policy and all other Data Privacy Policies associated with this Policy.

11. **"Person":** means a natural person or a juristic person;
12. **"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: Information relating to the education or the medical, financial, criminal or employment history of the person; Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person; The biometric information of the person; The personal opinions, views or preferences of the person; Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature; The views or opinions of another individual about the person; and The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
13. **"Private body"** means—
    13.1 a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
    13.2 a partnership which carries or has carried on any trade, business or profession; or
    13.3 any former or existing juristic person, but excludes a public body
14. **"Processing":** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –
    14.1 The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
    14.2 Dissemination by means of transmission, distribution or making available in any other form; or
    14.3 Merging, linking, as well as restriction, degradation, erasure or destruction of information;
15. **"Promotion of Access to Information Act":** means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000);
16. **"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.
17. **"Record":** means any recorded information –

17.1 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 visuals images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

17.2 In the possession or under the control of our firm; and

17.3 Regardless of when it came into existence;

18. **"Regulator":** – means the Information Regulator established in terms of Section 39 of the POPIA;

19. **"Restriction":** means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

20. **"Special personal information":** means personal information as referred to in Section 26 of the POPIA which includes 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;

21. **"This Act":** means the Protection of Personal Information Act, No. 4 of 2013.

22. **"Unique identifier":** means any identifier that is assigned to a data subject and is used by our firm for the purposes of the operations of our firm and that uniquely identifies that data subject in relation to our firm.

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2026

IMPLEMENTATION RESOLUTION
V1 – Implemented 01 July 2026

Management of the firm acknowledges the need to analyse and mitigate the wide variety of risks to which the firm is exposed and has put together the Data Privacy Terms and Conditions in order to mitigate the cyber risks associated with the firm's operations and to enhance the firm's crisis and disaster mitigation measures in the event of these risks occurring.

To this end, Management of the firm resolves that:

1. These Data Privacy Terms and Conditions are implemented on signature hereof;
2. These Data Privacy Terms and Conditions shall be circulated to all employees within 30 days after implementation;
3. Training for employees will be arranged prior to implementation;
4. The IT department shall continue to be engaged with regard to the data security risks.

MANAGING DIRECTOR	**SIGNATURE**
TRACEY MOUTON