PRIVACY POLICY IN ACCORDANCE WITH THE PROTECTION OF PERSONAL INFORMATION ACT ACT 4 OF 2013

WOLFAARDT ATTORNEYS INC.
2021/673046/21

Wolfaardt INCORPORATED
Attorneys · Notaries · Conveyancers

7 Palm Street, White River, 1240
Tel: (013) 750 0320/30
E-mail: liandi@wolfaardtinc.co.za
Deeds Office Lodgement Number: 12

Docex 9, White River, 1240
www.wolfaardtinc.co.za
Updated on
05/07/2023

TABLE OF CONTENTS

1. INTERPRETATION OF THIS POLICY

For the purposes of this Policy, Personal Information will be understood in accordance with the definition provided in the Protection of Personal Information Act 4 of 2013 ("hereinafter POPIA").

Unless the context indicates a contrary intention an expression which denotes any gender includes the other genders, a natural person, a juristic person and vice versa, the singular includes the plural and vice versa.

Unless inconsistent with the context, the expressions set forth below shall bear the meanings assigned to them hereunder:

POPIA	Protection of Personal Information Act 4 of 2013.
Constitution	Act 108 of 1996.
Requester	The natural or juristic person requesting access to information held by Wolfaardt Attorneys Inc. A requester also refers to the person making a request on behalf of somebody else.
Information Regulator	Means the Information Regulator established in terms of section 39 of POPIA.
Data subject	means the person to whom personal information relates.
Information officer	means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act.
Responsible Party	means Wolfaardt Attorneys Inc.
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;
Mandate	the written mandate given by the data subject to the Firm in terms whereof the data subject authorises the Firm to process its personal information.
Consent	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
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
c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

Personal Information means information relating to a 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, location information, online identifier, or other assignment to the person.
d) The biometric information of the person.
e) The individual 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.

Record means any recorded information, regardless of form or medium or when it came into existence, in the possession of the Responsible Party, whether it was created by the Responsible Party or not, including any of the following-

a) Writing on any material;
b) 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;
c) Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
d) Book, map, plan, graph, or drawing;

e) Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced.

2. INTRODUCTION

Wolfaardt Attorneys Inc. ("hereinafter called the Firm and / or the Business") is committed to protecting the privacy of personal information of our data subjects. The information data subjects share with us, allows us to deliver efficient and effective services.

The Firm has dedicated policies and procedures in place to protect all personal information collected and processed by us to ensure the quality, accuracy and confidentiality of Personal Information in our possession. However, it is impossible to guarantee that your Personal Information shall be 100% secure.

This privacy policy explains how the Firm collects and uses personal information and gives effect to the constitutional right to privacy. The Firm reserves the right to amend this Privacy Policy or add provisions to it at any time by publishing an updated version.

3. THE COLLECTION OF PERSONAL INFORMATION

The Firm collects personal information in various instances, including but not limited to:

3.1. Collecting information from a data subject directly;

3.2. Collecting information from third parties (such as regulators, government authorities and registries, or attorneys representing our clients' counterparties);

3.3. Collecting information as a result of interaction on our social media and the Firm's website.

This information includes, but is not limited to, the person's name, contact details and information regarding the matter with which they need assistance.

4. CONDITIONS FOR PROCESSING OF PERSONAL INFORMATION

In terms of POPIA there are eight lawful conditions for processing Personal Information, namely:

4.1. **Accountability** - as referred to in section 8 of POPIA - The responsible party must ensure that the conditions and all the measures set out in POPIA that give effect to such conditions, are complied with at the time of the determining the purpose and means of the processing.

4.2. **Processing Limitation** - as referred to in sections 9 to 12 of POPIA, Personal Information may only be processed in a fair and lawful manner and only with the consent of the data subject.

4.3. **Purpose Specification** - as referred to in sections 13 and 14 of POPIA, Personal Information may only be processed for specific, explicitly defined and legitimate purposes.

4.4. **Further Processing Limitation** - as referred to in section 15 of POPIA, Personal Information may not be processed for any other reason other than the purpose it was collected for unless it is in accordance with an exemption granted under Section 37.

4.5. **Information Quality** - as referred to in section 16 of POPIA, the responsible party must take reasonable steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary.

4.6. **Openness** - as referred to in sections 17 and 18 of POPIA, he responsible party must take reasonable steps to insure that the data subject whose information is collected is aware that such personal information is being collected by the responsible party and for what purpose the information will be used.

4.7. **Security Safeguard** - as referred to in sections 19 to 22 of POPIA, Personal Information must be kept secure against the risk of loss, unlawful access, interference, modification, unauthorized destruction and disclosure.

4.8. **Data Subject Participation** - as referred to in sections 23 to 25 of POPIA, Data subjects may request whether their personal information is held by the Firm, as well as the correction and/or deletion of any personal information held about them.

5. PROCESSING OF PERSONAL INFORMATION BY THE FIRM

The Firm is committed to process all Personal Information obtained in accordance to the conditions mentioned in paragraph 4 of this Policy. The Firm will not use the Personal Information for any other purpose, save for the purpose to complete said instruction or mandate and will only disclose, transfer and/or hand over the Personal Information to those authorised persons(s) to enable the business to complete its mandate.

The Firm will not retain your Personal Information for longer than is necessary to achieve the purpose for which it was collected, unless required to do so by any act, regulation or bylaw or by an order from a judicial or regulating body such as a court or tribunal.

The Firm processes personal information for various reasons, including but not limited to the following:

a) To maintain client records;
b) General administration;

c) Financial and tax purposes;
d) Legal or contractual purposes;
e) To improve the quality of our services to clients;
f) To help detect and prevent fraud and money laundering under FICA;
g) To help recover debts;
h) Engaging with the public;
i) To provide services to clients;
j) To comply with legal or regulatory obligations;
k) If a data subject has provided their consent; or
l) If the processing is allowed by law.

As prescribed in section 26 of POPIA, the Firm will not process personal information concerning –

a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
b) the criminal behaviour of a data subject.

As prescribed in Section 35, the Firm will only process Personal Information of children if a competent person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child –

a) carried out with the prior consent of a competent person; and
b) is necessary for the establishment, exercise or defence of a right or obligation in law.

6. RECIPIENTS WITH WHOM PERSONAL INFORMATION IS SHARED

In processing your Personal Information, the Firm may share it within the group of companies or with other third parties. These include but are not limited to:

a) Statutory authorities;
b) Law enforcement agencies;
c) Tax authorities;
d) Medical schemes;
e) Employee pension and provident funds;
f) Contractors, vendors, or suppliers;
g) Payment processors;
h) Email management and distribution tools;
i) Data storage providers;
j) Server hosts;
k) Group companies;
l) Agents;
m) Service providers.

7. SECURITY AND SAFEGUARDS

The Firm has identified its security risks and has further taken all reasonable steps to protect and avoid unauthorised access to Personal Information. The Firm has implemented various procedures and software to safeguard Personal Information and routinely reviews its operations in order to ensure that personal information is adequately protected.

In order to give effect to the safeguarding, the Firm has the following measures in place:

7.1. Managing the security of its filing system to ensure that personal information is adequately protected by limiting access to any records and by locking archived files in dedicated areas for safe keeping.

7.2. To ensure that operators that process personal information on behalf of the Firm apply adequate safeguards as outlined above by entering into written service agreements with the operators to pledge their commitment of the lawful processing of Personal Information as required by POPIA.

7.3. All employees will be required to sign a Confidentiality Undertaking in terms POPIA.

7.4. The Firm will ensure that where Personal Information is stored on removable storage medias such as external drives, CDs or DVDs, that these are kept locked away securely when not being used.

7.5. The Firm will ensure that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords will be changed regularly and may not be shared with unauthorized persons.

8. INTELLECTUAL TECHNOLOGY

a. All IT related services are looked after by Octopi Smart Solutions (Pty) Ltd.

b. All documents and applications are located on a Windows 10 desktop PC at Lüneburg & Janse Van Vuuren Inc. at their White River branch and access is controlled by Local User Accounts. All computers and devices are password/PIN protected.

c. The e-mail domain is hosted at Xneelo (Hetzner) ZA Data Centre. SPF, TXT & MX records are in place to prevent/limit e-mail spoofing.

d. E-mails are hosted with Microsoft 365 Exchange Online cloud infrastructure and each user's mailbox is protected by a password. There are better SPAM filters than the original POP/IMAP e-mail accounts. 2 Factor Authentication is setup on Admin and User accounts on Microsoft 365 accounts.

e. The internal network (LAN) is protected from the internet by an onsite router as well as a dedicated firewall. Internet router, firewall and internal network is managed by Octopi Smart Solutions (Pty) Ltd.

f. Remote working happens using Anydesk and TeamViewer remote desktop software. OpenVPN VPN functionality will be enabled in future for even better security, which has secure SSL VPN functionality with a digital certificate for each user working remotely.

g. Bitdefender Endpoint antivirus are installed on all computers and servers to protect against viruses, ransomware and dangerous websites. Antivirus definitions updates happens every hour and program upgrades are installed as soon as it is released. Computers automatically check via the software for updates and once every two weeks via an on-site technician to confirm no other issues arise.

h. Desktop and server operating systems are set to automatically install Windows security updates. Computers are constantly checked to verify that they are fully patched.

i. For disaster recovery, a full server backup is done daily to a Network Attached Storage (NAS) device located off-site. Data backups of users are done daily to the dedicated server and then backups run daily from server to the NAS device. Regular backup logs, checks and restores are done by Octopi Smart Solutions (Pty) Ltd to verify the state of the backups.

8.1 Website

The information provided on the Firm's website is for general guidance only. The information is not intended to constitute legal advice and is used at your own risk. The Firm accepts no responsibility or liability for damages arising from the use of the information.

When making use of the Firm's Website, users may be asked to provide the following Personal Information:

a) First name and Surname
b) Physical address
c) Phone number
d) Company / CC / business name

8.2 Log Files

When you visit the Firm's Website, even if you do not submit a query and/or request to be contacted, we may collect information, such as your IP address, the name of your ISP (Internet Service Provider), your browser, the website from which you visit us, the pages on our website that you visit and in what sequence, the date and length of your visit, and other information concerning your computer's operating system, language settings, and broad demographic information.

This information is aggregated and anonymous data and does not identify you specifically. However, this data may be able to be used to identify the data subject if it is aggregated with other Personal Information that the data subject supplies to the Firm.

This information is not shared with third parties and is used only within the Firm on a need-to-know basis. Any individually identifiable information related to this data will never be used in any way different to that stated above, without explicit permission/consent from the Data Subject.

8.3 Cookies

The Firm uses cookies. A cookie is a small piece of information stored on your computer or smart phone by the web browser. The types of cookies used on the Website are described below:

"Session cookies": These are used to maintain a so-called 'session state' and only lasts for the duration of your use of the Website. A session cookie expires when you close your browser, or if you have not visited the server for a certain period of time. Session cookies are required for the Platform to function optimally, but are not used in any way to identify you personally.

"Permanent cookies": These cookies permanently store a unique code on your computer or smart device hard drive in order to identify you as an individual user. No Personal Information is stored in permanent cookies. You can view permanent cookies by looking in the cookies directory of your browser installation. These permanent cookies are not required for the Firm's website to work, but may enhance your browsing experience.

9. INCIDENT RESPONSE

Where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person, the Firm shall notify:

a. the Regulator; and
b. the data subject, unless the identity of such data subject cannot be established.

The notification will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

10. RETENTION POLICY

In accordance with Section 14(3) of POPIA the Firm will not retain records of Personal Information any longer than is necessary for achieving the purpose for which the information was collected unless the retention of records is required by law.

11. DESTRUCTION OF PERSONAL INFORMATION

When the Data Subject is satisfied that the Firm's mandate is completed and the matter is finalized, all original documentation will be given back to the Data Subject.

The physical file/s will be placed in safe keeping in archives situated on the premises of the Firm, which is locked and a limited set of keys are available to avoid unauthorized access.

Once all periods of retention of records as required by law are fulfilled, the file content will be burned in an appropriate manner by an employee of the Firm.

12. PROCESS OF REQUIRING ACCESS TO THE RECORDS HELD BY THE FIRM

In terms of Sections 23 to 25 of POPIA, Data Subjects may request to access, amend or delete Personal Information that is in the possession of the Firm. However in certain instances the Firm may legally refuse or decline such requests.

A Data Subject may also have the right to object to the processing of their Personal Information or to file a complaint with a Regulator.

If a Data Subject wishes to exercise their rights, they can contact the Firm's Information Officer at the details provided in paragraph 13 of this Policy. A fee for accessing, amending or deleting Personal Information may be charged.

Data subjects are encouraged to update their Personal Information as and when necessary.

13. APPOINTMENT OF INFORMATION OFFICER

The Firm has complied with the requirements of the Act in that it appointed Lucas Cornelius Rudolph Janse van Vuuren as its Information Officer.

The contact details of the Information Officer are as follow:

E-mail:	liandi@wolfaardtinc.co.za
Website:	www.wolfaardtinc.co.za
Physical address:	7 Palm Street White River, 1240
Contact number:	Tel. (013) 750 0320/30
Deputy Information Officer:	Liandi Lloyd

14. INFORMATION AND DEPUTY INFORMATION OFFICERS – DUTIES AND INCIDENT MANAGEMENT

14.1. The general responsibilities of the INFORMATION AND DEPUTY INFORMATION OFFICERS for the FIRM include the following:

14.1.1. The encouragement of compliance, by the Firm, with the conditions for the lawful processing of personal information;

14.1.2. Managing requests made to the Firm pursuant to POPIA;

14.1.3. Working with the Regulator in relation to investigations conducted pursuant to prior authorization required to process certain information of POPIA in relation to the FIRM.

14.1.4. Review policy rules regularly, document the results, and update the policy as needed.

14.1.5. Continuously request Octopi Smart Solutions (Pty) Ltd. to

14.1.5.1. update information security policies and network diagrams.

14.1.5.2. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.

14.1.5.3. Perform continuous computer vulnerability assessments and audits

14.2. The data breach responsibilities of the INFORMATION AND DEPUTY INFORMATION OFFICERS for the FIRM include the following:

14.2.1. Ascertain whether personal data was breached;

14.2.2. Assess the scope and impact by referring to the following:

14.2.2.1. Estimated number of data subjects whose personal data was possibly breached;

14.2.2.2. Determine the possible types of personal data that were breached;

14.2.2.3. List security measures that were already in place to prevent the breach from happening.

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

14.2.3.1. The Information Regulator;

14.2.3.2. Each data subject who may have been affected by a compromise;

14.2.3.3. Management of the FIRM;

14.2.3.4. The IT support team of the FIRM;

14.2.3.5. Communication should include the following:

i. Contact details of INFORMATION AND DEPUTY INFORMATION OFFICERS
ii. Details of the breach,
iii. Likely impact,
iv. Actions already in place, and those being initiated to minimise the impact of the data breach,
v. Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

14.2.4. Review and monitor

14.2.4.1. Once the personal data breach has been contained, the 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.

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

15. THIRD PARTY OPERATORS

The FIRM recognizes that, in fulfilling certain of its contracts with its customers and in order to operate efficiently in fulfilling such contracts, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to the BUSINESS'S service delivery.

To ensure that its OPERATORS adhere to the same standard of data breach risk mitigation as the FIRM, it will where possible enter into an OPERATORS' AGREEMENT with the relevant service supplier with whom either of the FIRM share data subjects' information in order to ensure that the OPERATOR treats the personal information of the particular FIRM'S data subjects responsibly and in accordance with the provisions contained in the Act and Regulations

thereto. The FIRM shall, where possible request copies of the OPERATOR'S POPIA Policy, rules, internet rules, security measures and details of OPERATOR'S Information Officer.

16. BANKING DETAILS

It is a known fact that electronic transmission of banking details poses a particular cyber risk threat which The FIRM recognizes. Organizations who share banking details electronically are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of the transaction. Either of the FIRM'S data subjects are open to large amounts of damages or losses if emails are intercepted and banking details are fraudulently amended without the data subject's knowledge.

To mitigate the risk of internet and email interceptions of banking details, the FIRM has implemented clear warnings within all its correspondences (emails and physical letters) warning data subjects of the risks of email hacking and interceptions. In the event that banking details are physically sent to data subjects or received from data subjects per email or instant messaging platforms for purposes of payment, the banking details will be confirmed with a telephone call and verification of each account will be done. 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 to ensure encryption of emails.

DECLARATION BY THE INFORMATION OFFICER OF WOLFAARDT ATTORNEYS INC..

I, the undersigned,

Lucas Cornelius Rudolph Janse van Vuuren

being the authorized and approved Information Officer of Wolfaardt Attorneys Inc., hereby declare as follows:

1. I have made myself aware of the contents of this document;

2. I will ensure that the processes herein contained are implemented in my FIRM;

3. I will ensure that all staff in my FIRM are trained on the aspects and importance of the protection of personal information as contained herein;

4. I will ensure that this document is updated and reviewed regularly;

SIGNED AT WHITE RIVER ON THIS 5TH DAY OF JULY 2023.

LUCAS CORNELIUS RUDOLPH JANSE VAN VUUREN