PRIVACY POLICY OF DANÈL.INC

1. POPI POLICY

(In terms of Protection of Personal Information Act 4 of 2013)

In respect of **DANÈL NORTJE INCORPORATED,** registered with the Information Regulator (South Africa) on the 25th of February 2025 under registration number **5-001495.**

2. DEFINITIONS

The following words or expressions will bear the following meanings in this policy:

- "the/this Act / POPI" shall mean the Protection of Personal Information Act 4 of 2013, as amended.
- "From time to time", together with all relevant regulations published thereunder as effective from 1 July 2021.
- "the/this Policy" shall mean this policy together with all annexures thereto, as amended from time to time.
- "Danèl Nortje/ Danèl.Inc/ the Firm" shall mean Danèl Nortje Incorporated
- "Information Officer" shall mean the appointed Information Officer, currently being **Mrs. Edith de Beer**.
- "Deputy Information Officer" the person, authorized by the Information officer of the Firm to facilitate or assist with any request in terms of this Act and/or policy, currently being Anneke van der Merwe.
- "Responsible Party" This is the firm/company/person that controls the data that is processed. Danèl Nortje Incorporated is a Responsible party.
- "Operator" This is the firm/company/person that processes the data on behalf of the responsible party.
  For instance: if we receive an instruction for a transfer and the Seller, Mr. Shark, lives in Cape Town, then we must use a correspondent attorney, Seaside Attorneys, in Cape Town to assist the Seller to sign the transfer documents on our behalf. In this scenario, Danèl Nortje Incorporated is the Responsible Party and Seaside Attorneys will be the Operator.

- "Data Subject" Any living identifiable person or juristic entity to whom personal information or special personal information relates to. In the scenario above, Ms. Shark, is the data subject because his personal information is collected.
- "Processing information" How we collect, use, store or destroy information. We only collect and process personal information if the data subject has given consent.

3. INTRODUCTION

Danèl Nortje Incorporated is sensitive to the personal nature of the information provided to us and we care about the privacy and security of personal information. We take our responsibility to protect personal information very seriously. This policy explains how we collect, use, store, share and protect personal information. We recognize the importance of protecting privacy in respect of personal information (as defined in the Protection of Personal Information Act 4 of 2013 – POPI Act) collected by us when we provide legal services as per instructions to us by clients.

POPIA regulates how we process (collect, use, store and destroy) personal information and special personal information (data) relating to a living person or existing entity.

We will not use personal information for any other purpose than that set out in this policy and will endeavour to protect personal information that is in our possession from unauthorized alteration, loss, disclosures, or access. We may review and update this policy from time to time. The latest version of this policy is available on request. This policy applies to all external parties with whom we interact, including but not limited to individual clients, representatives of client, visitors to our offices and other users of our legal and other services.

The object of the Act is to give effect to the constitutional right of protection of personal information held by private or public bodies which information is required for the exercise or protection of any rights and matters connected therewith.

We only collect and process personal information if you have given us your consent, in terms of a legal obligation places on us, or, where it is necessary, for the performance of a contract with you. Because of the sensitivity of some personal information, we ensure that the way we process your personal information complies fully with the Protection of Personal Information Act, 4 of 2013 ("POPIA").

This privacy policy applies to any of your personal information that we collect and process within the course of providing our services to you.

4. COLLECTION OF PERSONAL INFORMATION AND SPECIAL PERSONAL INFORMATION

Personal information and special personal information are any information relating to an identifiable living or juristic person.

We may collect or obtain personal information about you:

- Directly from your, or during our relationship with you;
- While providing legal services to you or your organization;
- When you make your personal information public;
- When you visit and / or interact with our website;

In addition to the above, we may create personal information about you such as records of your communications and interactions with us, including but not limited to, your attendance at interviews when applying for a job with us or when you are visiting our offices.

The following personal information may be collected / used / stored / destroyed:

- Information about a person's 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;
- information relating to the education, medical, financial, criminal, or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person;
- biometric information of the person (fingerprints / retinal scan / facial recognition);
- personal opinions, views, or preferences of the person.

The following special personal information may not be collected / used / stored / destroyed without the person's express written consent:

- A person's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information (fingerprints / retinal scan / facial recognition)
- The criminal behaviour of a data subject to the extent that such information relates to the alleged commission by the person of any offence or any proceedings in respect of any offence allegedly committed by that person or the disposal of such proceedings.
- Personal Information relating to a child:

We do not intentionally collect or use personal information of children (persons younger than 18 years) unless with the express consent of a parent or guardian or if the law otherwise allows or requires us to process such personal information.

5. CATEGORIES OF PERSONAL INFORMATION WE MAY PROCESS

We may process the following categories of personal information about you:

- Personal details – your name and photograph;
- Demographic information – gender, date of birth, nationality, title, and language preference;
- Identifier information – passport or identity number, utility provider details, bank account statements; Contact details – correspondence address, telephone number and email address;
- Instruction details – details of the individual instructing Danèl.Inc, personal information included in correspondence, documents, evidence, or other materials that we process while providing legal services;
- Attendance records – details of meetings and other events organized by or on behalf of Danèl.Inc that you have attended;
- Consent records – records of any consents you may have given, together with the date and time, means of consent and any related information;
- Payment details – billing address, payment method, bank account number, payment records, payment amount and date;
- Data relating to your visits to our website – your device type, operating system, browser type, browser settings, IP address, language settings, date, and times of connecting to a website and other technical communication information;
- Employer details – where you interact with us in your capacity as an employee of an organization the name, address, telephone number and email address of your employer, to the extent it is relevant;

6. SENSITIVE PERSONAL INFORMATION

Where we need to process your sensitive personal information, we will do so in the ordinary course of our business, for a legitimate purpose and in accordance with the applicable law.

7. PURPOSES OF PROCESSING AND USING PERSONAL INFORMATION

We will process your personal information in the ordinary course of our legitimate business purposes in providing legal and related services and advice. We will primarily use your personal information only for the purpose for which it was originally or primarily collected. We will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest and is closely related to the original or primary purpose for which the personal information was collected.

We may subject your personal information to processing during various activities, including, without limitation the following:

- Operating our business and providing services to clients
- Analysis, evaluation, review, and collection of information to determine legal issues and potential disputes, provide legal advice and prepare or comment on opinions, agreements, correspondence, reports, documents relating to legal proceedings and other documents and records
- Compliance with applicable law and fraud prevention
- Transfer of information to our service providers and other third parties
- Recruitment
- We may process your personal information for safety and security purposes.

Before any personal information is processed, written consent will be obtained from the data subject.

8. DISCLOSURE OF PERSONAL INFROMATION TO THIRD PARTIES

We may disclose your personal information to our service providers for legitimate business purposes, in accordance with applicable law and subject to applicable professional and regulatory requirements regarding confidentiality.

8.1 In addition, we may disclose your personal information:

- If required by law
- To legal and regulatory authorities, upon request or for the purposes of reporting any actual or suspected breach or applicable law or regulations
- To third party operators
- Where it is necessary for the purposes of or in connection with, actual or threatened legal proceedings or establishment, exercise, or defence of legal rights

- To any relevant party for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution or criminal penalties, including but not limited to safeguarding against, and the prevention of threats to public security.

We require that our service providers (third parties) take appropriate, reasonable, technical, and organizational measures to keep the personal information secure. In addition, they may not use or disclose the personal information for any purpose other than providing the services on our behalf. We enter into agreements (Operator Undertakings) with third parties to further secure the processing of personal information.

Personal information will be provided to our employees to enable them to perform their duties.

We will not sell personal information. No personal information will be disclosed to anyone except as provided in this policy.

9. INTERNATIONAL TRANSFER OF PERSONAL INFORMATION

We may transfer your personal information to recipients outside of the Republic of South Africa. Personal information may be transferred outside of the Republic of South Africa provided that the country to which the data is transferred has adopted a law that provides for an adequate level or protection substantially similar to the POPI act and the third-party undertakes to protect the personal information in line with applicable data protection legislation and the transfer is necessary in order to provide the legal and other related services that are required by Danèl.Inc's clients.

10. DATA SECURITY AND INCIDENT RESPONSE

We implement appropriate, reasonable technical and organizational security measures to protect your personal information that is in our possession against accidental or unlawful destruction, damage, loss, alteration, unauthorized disclosure, unauthorized access, in accordance with applicable law. Access to personal information is restricted to employees which have the necessary unique usernames, passwords, and login credentials. Sharing of this information between employees are prohibited. No external storage devices are allowed. We use electronic and computer safeguards like firewalls and comprehensive antivirus programs, as well as physical and electronic access control to our building and offices, and regular updates of software and programs are done.

Where there are reasonable grounds to believe that your personal information that is in our possession has been accessed or acquired by any unauthorized person, we will notify the relevant regulator and you, unless a public body responsible for detection, prevention or investigation of offences or the relevant regulator informs us that notifying you will impede a criminal investigation.

11. MINIMUM OPERATING STANDARDS

Standards (MOS) in place, as well as a Disaster Recovery Plan, which will also direct our response to a data breach. Because the internet is an open system, the transmission of information via the internet is not completely secure. Although we will implement all reasonable measures to protect your personal information that is in our possession, we cannot guarantee the security of any information transmitted using the internet and we cannot be held liable for any loss or privacy occurring during such transmission.

Full and incremental backups to preserve information assets are performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical. Backup media are stored in a secure, geographically separate location form the original and are isolated from environmental hazards and tested for accuracy on a regular basis.

12. DATA ACCURACY

The personal information provided to Danèl.Inc should be accurate, complete, and up to date. Should personal information change, the onus is on the provider of such information to notify Danèl.Inc of the change and provide Danèl.Inc with the accurate data.

13. DATA ADMINISTRATION

Danèl.Inc will restrict its processing of personal information to data which is sufficient for the fulfilment of the primary purpose and applicable legitimate purpose for which it was collected.

14. DATA RETENTION AND DELETION

Danèl.Inc shall only retain and store personal information for the period for which the data is required to serve its primary purpose or a legitimate interest or for the

period required to comply with an applicable legal requirement or obligation, whichever is the longest.

As Attorneys, we must comply with the Legal Practice Act 28 of 2014. In terms of the Legal Practice Act we must store all information (in electronic and hard-copy format) for a minimum period of 7 (Seven) years once our mandate has been completed and/or the file closed.

All information captured on Lexis Convey, (previously Ghost Convey) and/or Ghost Practice as part of the process to open files and draft documents are backed up electronically. All data stored on the company server is automatically backed up daily. The backed-up data is encrypted and stored in a secure off-site data centre.

On completion of the mandate the supervising attorney checks that the following are in order:

- All finances,
- FICA Documents,
- Documents have been scanned and stored on Ghost Practice,
- Checklists are properly signed off.

The file is then signed off by the attorney. Our accounting department then allocate a dead file number to the file and store the file in archives for safe keeping.

Should the file thereafter be needed, the accounting department retrieves the file from safe keeping in the archives and keep track of where the file is.

Once the relevant time periods for retaining the files have lapsed, the files are destroyed professionally.

15. YOUR LEGAL RIGHTS

You have rights under the South African and other laws to have access to your personal information and to ask us to rectify, erase and restrict the use of your personal information. You also have rights to object to your personal information being used, to ask for the transfer of personal information you have made available to us and to withdraw consent to the use of your personal information.

All your requests will be subject to our obligation to retain it by law or for a legitimate purpose.

16. OUR CONTACT DETAILS

If there are any questions regarding this policy, or if you want to have access to your personal information or if you believe we are using personal information unlawfully, please contact us:

Full Names: **Danèl Nortje Incorporated**

Registration Number: **2020/858389/21**

Physical Address: 13B Queen Street, Irene Estate, Centurion, 0157

Docex: 29 Centurion

Telephone Number: **086 111 4661** l E-mail: info@Danelinc.com

The Information officer is Mrs. Edith de Beer

Her contact details are:

Telephone Number: 086 111 4661 l Email: edith@Danelinc.com

The Deputy Information Officer is Ms. Anneke van der Merwe

Her contact details are:

Telephone Number: 086 111 4661 l E-mail: anneke@Danelinc.com

A complaint may be lodged at the Information Regulator (South Africa) with the following details:

Website: https://www.justuce.gov.za/inforeg/index.html

Address: JD House, 27 Stiemens Street, Braamfontein Johannesburg

PO Box 31533, Braamfontein Johannesburg 2017

Email: complaints.IR@justice.gov.za

17. DISCLAIMER

The information contained herein is for information purposes only and should not be construed as legal advice from any lawyer or representative of our firm.

Professional advice should be sought before any action is taken based on the information contained herein.