# PRIVACY POLICY

| | |
|---|---|
| **BUSINESS NAME** | David Newham Property Management (Pty) Ltd |
| **TRADING AS** | David Newham Property Management (Pty) Ltd |
| **REGISTRATION NUMBER** | 1973/015042/07 |
| **BUSINESS ADDRESS** | Level 6, West Wing, Cento Building, Bella Rosa Office Park, 21 Durbanville Avenue, Bellville, Western Cape |
| **BUSINESS TELEPHONE NUMBER** | +27(0)21 948 0934 |

## PROTECTION OF PERSONAL INFORMATION

DNPM has dedicated policies and procedures in place to protect all personal information collected, processed and used by DNPM to ensure full adherence to all requirements prescribed by the Protection of Personal Information Act ("POPIA"). The information you share with us as a Data Subject allows us to provide you with the best experience with our products and services, or as a stakeholder.

## PURPOSE OF THIS POLICY

This Privacy Notice describes how DNPM collects, uses, discloses, retains and protects your personal information, as prescribed with the POPIA and other relevant laws. Any and all information collected will be kept strictly confidential. We will not disclose your personal information to anyone, unless we obtain your consent, or unless it is required or permitted by law or a regulatory authority. It will not be sold, loaned or otherwise disclosed to any organisation. We may retain any information for purposes of ongoing business relationships or to communicate directly with you. We will store and keep your personal information according to the retention (holding) periods defined by law for legitimate business purposes and will take reasonably practicable steps to make sure that it is kept up to date and deleted and archived according to our defined retention schedules.

## PROCESS OF COLLECTING PERSONAL INFORMATION

DNPM uses different methods to collect information from and about you. Your personal information may either be collected by us or provided by you. When personal information is obtained from Third Parties, DNPM will either secure the Data Subject's consent or process it without consent only when legally permissible. We will only collect your personal information by lawful and fair means and, where appropriate with your knowledge or consent.

Subsequently, DNPM must take reasonable steps to ensure that the Data Subject is aware of the following :

- The specific information being collected and purpose of such information being collected.
- If such information is not collected directly from the Data Subject, then the source from which it was collected.
- The reasons attached to the collection of the Data Subject's personal information.
- The legal obligations that are imposed on DNPM in terms of collecting the Data Subject's personal information.
- The consequences attached if the Data Subject fails to provide the requested personal information.

DNPM processes personal information for various reasons. Before or at the time of collecting your personal information, we will identify the purpose(s) for which the information is being collected. Personal information is used as is appropriate in the normal course of business to provide the products and services. We may retain any information for purposes of ongoing business relationships or to communicate directly with you. The reasons for processing of information is including but not limited to the following:

- To manage information, products and/or services requested by data subjects;
- To help us identify data subjects when they contact us;
- To improve the quality of our services;
- Marketing purposes.

**STORAGE OF PERSONAL INFORMATION**

The storage of personal information shall not be retained beyond the period necessary for the fulfilment of the specific purpose for which it was collected or subsequently processed, subject to exceptional circumstances. These exceptions include instances where:

- retention is mandated or authorised by statute;
- reasonably required by DNPM for legitimate functions or activities, dictated by contractual obligations;
- subject to the explicit consent of the Data Subject or a competent person acting on behalf of a child.

POPIA permits extended retention for historical, statistical, or research endeavours, contingent upon the implementation of appropriate measures. Once the authorised retention

period expires, then DNPM will promptly destroy, delete, or de-identify the information securely.

Personal information should be safely stored. When personal information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to personal information that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Where such information is classified as secret access to the environment, should be restricted and locked.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or photocopier.
- Printouts that contain personal information should be shredded immediately and disposed of securely when no longer required.

When personal information is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts. DNPM will ensure the following:

- All computers and electronic storage require access control passwords;
- All electronic access must be logged;
- Personal information should only be stored on designated drivers and servers, and should only be uploaded to approved cloud computing services;
- If personal information is stored on removable media (like a memory stick, external hard drive, CD or DVD) the files should be encrypted, password protected and the media should be locked away securely when not being used;
- USB drives (memory sticks) that are found or have been handled out as promotional item should not be plugged into any computer as these devices may contain hidden malware or viruses;
- All lost or stolen devices (including removable media) must immediately be reported to the line manager;
- Electronic files that contain personal information should be backed up frequently. Those backups should be tested regularly in line with the DNPM's standard backup procedures, which include cloud base backup and manual local backup;
- All servers, computers and other electronic devices containing personal information should be protected by anti-virus software, with embedded firewall.

Third Party service providers gaining access to Data Subject's personal information, by way of mandate, will be in accordance with the provisions of this Policy and adherence to the requirements of POPIA. DNPM ensures that such usage by a Third-Party service provider will

implement and maintain security measures equivalent to or exceeding those employed by DNPM to safeguard the personal information of the Data Subject. Personal information may be processed within South Africa or in other jurisdictions where DNPM or its Third-Party service providers provided that such processing meets the standards of protection prescribed by law regardless of its location.

**DNPM's RESPONSIBILITIES**

Everyone who works for or with DNPM has some responsibility for ensuring that the personal information of data subjects is processed appropriately to ensure the confidentiality, integrity and availability thereof.

Each Information End User, Information Owner, business unit and team that handles personal information must ensure that it is processed in line with this Policy and POPIA.

These people have key areas of responsibility:

The information Officer is responsible for:

- Encouraging compliance for the lawful processing of personal information and the provisions of POPIA;
- Engaging and working with Information Regulator concerning investigations;
- Developing, implementing, maintaining and reviewing this Policy;
- Conducting personal information assessments to ensure that adequate measures and standards exist to comply with conditions for the lawful processing of personal information;
- Developing, monitoring, maintaining and making available the manual as prescribed by PAIA, as well as ensuring compliance with section 51 of PAIA by including the postal and street address, phone and fax number, and, if available, electronic mail address of the head of DNPM or his delegated Information Officer;
- Ensuring internal measures are developed together with adequate systems to process requests for information or access;
- Conducting internal POPIA awareness sessions;
- Delegation of his or her powers and duties to one or more Deputy Information Officers to ensure compliance;
- Registering DNPM's details of the Information Officer and Deputy Information Officer with the Information Regulator, following the Information Regulator's guidelines:
- Classifying personal information in line with DNPM's latest FICA RMCP;

- Maintaining internal procedures to support the effective handling and security of personal information.
- Reviewing all personal information protection procedures and related policies, in line with an agreed schedule and make recommendations to the Deputy Information Officer and /or DNPM's Legal Risk & Compliance Officer in terms of the DNPM's RCMP; and
- Ensuring that all employees, consultants and others that report to the Information Owner are made aware of and are instructed to comply with this and all other relevant policies.

The Deputy Information Officer is responsible for:

- Keeping the Information Officer updated about information assets and personal information protection responsibilities, risks and issues;
- Reviewing all personal information protection procedures and related policies, in line with an agreed schedule;
- Arranging personal information protection training and advice for the people covered by this Policy;
- Checking and approving any contracts or agreements with third parties that may process personal information on behalf of DNPM, if applicable;
- Dealing with requests from data subjects who want to see the personal information that DNPM holds about them (also called "data subject access requests"). The identity of anyone making a data subject request must be verified before disclosing any personal information;
- Ensuring all ICT assets used for processing personal information meets security standards;
- Performing regular checks and scans to ensure security hardware and software is functioning properly. This function may be performed by DNPM's IT specialist;
- Evaluating any third-party services DNPM is considering using to process personal information. For instance, cloud computing services.

The Information Officer and/ or the CEO of the organisation is responsible for:

- Approving any personal information protection statement attached to communication such as e-mails and letters; and
- Approving any personal information protection statement included in any Lease Agreement and/ or Addenda thereto.

**PROVISION OF PERSONAL INFORMATION TO THIRD PARTY SERVICE PROVIDERS**

- Internal disclosure

  In general, personal information is shared within DNPM where legally permitted for reasonable and appropriate business purposes. However, access within DNPM's organisation is restricted to those employees or third parties who need access to carry out their assigned functions. DNPM may share information within its group structure as well as with agents and contractors where necessary and in line with this policy.

- External disclosure

  External disclosure is made pursuant to an agreement or as permitted or required by law (e.g. FICA) or legal process, or with the consent of Data Subject. The Company may process the information in line with the purpose it was gathered for.

- POPIA allows personal information to be shared if it involves national security or criminal activities without the consent of the Data Subject. Under these circumstances the request for personal information will be disclosed. However, the Deputy Information Officer will ensure that the request is legitimate and in line with POPIA, seeking assistance from DNPM's legal representatives where necessary.

**ENFORCEMENT**

- Non-compliance

  Non -compliance with this Policy by DNPM's employees will be dealt with in accordance with the Disciplinary Code/ Regulations of DNPM. Consequences may include disciplinary action up and to termination of employment, and/or legal proceedings to recover any loss or damage to DNPM, including the recovery of any fines or administrative penalties imposed by the Information Regulator in terms of POPIA.

- Data breach

  Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, DNPM will notify the Information Regulator and the affected Data Subject (unless the identity of such Data Subject cannot be established) and address the data breach in accordance with the terms of POPIA.

  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.

**RIGHTS OF THE DATA SUBJECT**

- The Data Subject has the right to know what personal information DNPM hold about the Data Subject;
- What personal information was sent to the service providers or any other third parties;
- Data Subject can request DNPM to update, correct, or delete personal information that is outdated, incorrect, incomplete, irrelevant, or excessive;
- Data Subject may object to the processing of their personal information on reasonable grounds;
- DNPM also reserves the right to refuse a request for the deletion of personal information of the Data Subject if its retention is required by law or necessary for the protection of DNPM's legal rights;
- Data Subject have the right to unsubscribed from any direct marketing communications from DNPM;
- DNPM reserves the right to terminate any existing contractual agreements in the event of the Data Subject requests the deletion of all personal information held by DNPM, as the processing of the personal information is a prerequisite for the fulfilment of these agreements.
- Data Subject has the right to submit complaints to the Information Regulator regarding to how your personal information has been handled improperly, illegally, or in a way that interferes with their rights under POPIA and if not unhappy with the decision of the adjudicator, can follow dual procedure under the POPIA; and
- To institute legal proceedings on how and what personal information is held.

**DATA SUBJECT REQUESTS FOR INFORMATION**

Upon request we will furnish you with details of the personal information we hold about you. You may submit your request using **Form2 Correction or Deletion of Personal Information** which is attached below. Should you believe that any information we hold about you is incorrect, please inform us using Form 2 and we will correct it.

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, DNPM shall notify:

- The Regulator; and

- 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.

**CHANGES AND AMENDMENTS**

Upon reviewing our policies on an annual basis, DNPM ensures that we adhere to all the requirements prescribed by legislation. DNPM reserves the right to alter and/or amend this Policy and any information herein. Please consult the platform where you have obtained this policy regularly to keep update of any changes as whilst DNPM may notify The Data Subject such alteration and/ or amendments it cannot always ensure that such notice is always received.. The rights and obligations between the Data Subject and DNPM is governed by this Policy with respect to each instance of access and use of DNPM's On-line Platform.

**CONTACT INFORMATION**

Any questions, queries, or requests for further information about this Policy can be directed to the Information Officer, alternatively:

- DNPM: Contact Number: 021 948 0934
- On-line Platform page on www.dnpg.co.za
- Sedick Moerat

| | |
|---|---|
| CEO | Means the DNPM's Chief Executive Officer , and including an acting CEO |
| Data Subject | Means the identifiable natural/juristic person to whom personal information relates |
| Deputy Information Officer | Means Mr. Thomas Dods, in his role as a financial account of DNPM |
| FICA | Means the Financial Intelligence Centre Act, 28 of 2001 (as amended) together with any regulations thereto |
| Information assets | Means the assets the organisation uses to create, store, transmit, delete and/or destroy information to support its business activities |

| | |
|---|---|
| | as well as the information systems with which that information is processed. All electronic information and non-electronic information created or used to support business activities regardless of form or medium, for example, paper documents, electronic files, voice communication, text messages, photographic or video images.<br><br>All applications, devices and other systems with which DNPM processes its information, for example telephones, fax machines, printers, voicemail, e-mail, instant messaging, smartphones and other mobile devices ("ICT assets"). |
| Information custodian | Means the person responsible for defining and implementing security measures and controls for Information and Communication Technology assets ("ICT assets") |
| Information end user | Means a person that interacts with information assets and ICT assets for purpose of performing an authorised task. |
| Information Officer | Means the person appointed as DNPM's Legal Advisor, who also fulfil the role of Legal Risk & Compliance Officer in terms of DNPM's RMCP in terms of FICA. |
| Information owner | Means a person responsible for, or dependent upon the business process associated with an information asset. |
| PAIA | The Promotion of Access to Information Act, 2 of 2000. |
| Personal information | "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-<br>a) Information relating to race, gender, sex, pregnancy, marital status, national, ethic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of person;<br>b) Information relating to the education or medical, financial, criminal or employment history of the person;<br>c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;<br>d) The biometric information of the person; |

| | |
|---|---|
| | e) The personal opinions, views or preferences of the person;<br>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;<br>g) The views or opinions of another individual about the person; and<br>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. |
| Processing | Means any operation or activity or any set operations, whether or not by automatic means, concerning personal information, including:<br>a) The collection, receipt recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;<br>b) Dissemination by means of transmission, distribution or making available in any other form; or<br>c) Merging, linking, as well as restriction, degradation, erasure or destruction of information. |
| RMCP | Means the organisation's Risk Management & Compliance Programme, as prescribed by the FICA |
| Special personal information | Means personal information as referred to in Section 26 of POPIA |
| POPIA | Protection of Personal Information Act, 4 of 2013 |