McCORMICK PROPERTY DEVELOPMENT PROPRIETARY LIMITED

PRIVACY POLICY

[PUBLIC DOCUMENT]

1. INTRODUCTION

This privacy policy is applicable to McCormick Property Development Proprietary Limited ("**MPD**"). MPD is committed to sound business practices in compliance with relevant legislation, which, for purposes of this policy, includes the Protection of Personal Information Act, no 4 of 2013 ("**POPI**") read with section 14 of the Constitution of the Republic of South Africa. POPI aims to protect personal information (which is information which identifies a data subject, such as information relating to race and gender, contact details, financial information, medical information, educational information, employment or criminal history). MPD has appointed an Information Officer, whose details are as follows:

Name: Ananda Booysen

Email address: ananda@expreit.co.za

Telephone number: (012) 660 3020

2. PURPOSE, SCOPE AND OBJECTIVES

2.1 This policy will set out the manner in which personal information (as defined in POPI) is collected, managed, stored, used and protected by MPD. This policy applies to MPD and all of its employees.

2.2 The objectives of this policy are to:

- process personal information lawfully in terms of POPI;
- provide a guideline as to the manner in which MPD processes and protects personal information;
- adopt good practices in terms of processing of personal information;
- protect MPD from the consequences of breaching its responsibilities in terms of POPI;
- display the commitment of MPD to uphold and respect information privacy.

3. DEFINITIONS

3.1 **"data subject"** means the person (natural or juristic) who the personal information is about;

3.2 **"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 race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of a person;

- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to a person;
- the biometric information of a person;
- the personal opinions, views or preferences of a person;
- correspondence sent by a person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about a person; or
- the name of a person if it appears with other personal information relating to such person or if the disclosure of the name itself would reveal information about a person.

The format of the information is irrelevant and POPI applies to all personal information, irrespective of its form (i.e. paper or hard copy, electronic, audio, video).

3.3 **"processing"** or "**data processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

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

It therefore includes reading a file, emailing information to someone, deleting or editing documents, saving documents to a USB, or transferring documents from one device to another. It covers all the different ways in which a responsible party handles personal information in both physical and electronic format.

3.4 **"responsible party"** means the company, body or person which, alone or in conjunction with others, determines the purpose of and means for processing personal information (and thus is responsible for the collection and processing of personal information - in this case, MPD).

3.5 **"special personal information"** means a subcategory of personal information that is considered sensitive information and can be used to unfairly discriminate against a person, such as:

- information regarding 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
- information regarding the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject.

In terms of POPI, a responsible party cannot use special personal information without authorisation.

4. TYPE OF INFORMATION PROCESSED

MPD generally collects and processes the following types of personal information:

- Identity documents and/or company registration documents (as applicable) of, inter alia, employees, representatives of service providers and job applicants;
- Personal details of service providers, job applicants and employees (including but not limited to name, surname and ID number);
- Contact details, including email addresses, telephone numbers, and physical addresses of representatives of service providers;
- Employee data, including salary, disciplinary records, banking details, account numbers, tax information;
- Information held by the deeds office, including property ownership profiles of properties owned by MPD and its business partners or potential business partners.

5. LAWFUL PROCESSING

As prescribed by sections 8 – 25 of POPI, MPD undertakes to comply with the following 8 conditions or principles for the lawful processing of personal information:

5.1 Accountability

The responsible person must comply with POPI. MPD takes responsibility and remains accountable for personal information in its possession and processed by it. MPD will ensure that the conditions for lawful processing are given effect to and complied with.

5.2 Processing limitation

The responsible party must have a good reason for processing personal information.

5.2.1 MPD undertakes to process personal information:

- lawfully, in accordance with POPI;
- in a reasonable manner that does not infringe the privacy of the data subject; and
- in a manner that is adequate, relevant and not excessive so as to infringe on the data subject's right to privacy and exceed the purpose for which it was processed.

5.2.2 Personal information will only be processed if:

- the data subject (or a competent person, where the data subject is a child) consents thereto, alternatively, if the data subject has entered into a contract with MPD (in which instance express consent would not be required);
- processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party. The data subject is forewarned that if it withdraws its consent or objects to the processing of its personal information where it is necessary to process the data subject's personal information, the data subject may be excluded from any affected rights or benefits in terms of a contract and where such consent is operationally material to the continuation of the contract, the contract may be terminated;
- processing complies with an obligation or duty which is required or imposed by law (such as the Employment Equity Act, the Deeds Registries Act etc);
- processing protects a legitimate interest of the data subject; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

5.2.3 Personal information will be collected directly from the data subject, unless:

- the information is contained in or derived from a public record or has deliberately been made public by the data subject;
- the data subject (or a competent person, where the data subject is a child) has consented to the collection of the information from another source;
- collection of the information from another source would not prejudice a legitimate interest of the data subject;
- collection of the information from another source is necessary:
  - to uphold and enforce the law by any public body;
  - to comply with an obligation imposed by law or to enforce legislation;
  - for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
  - in the interests of national security; or
  - to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;
- collecting the information directly from the data subject would prejudice a lawful purpose of the collection; or
- collecting the information directly from the data subject is not reasonably practicable in the circumstances of the particular case.

5.3 Purpose specification

The data subject must know the reason the responsible party is processing their personal information.

5.3.1 MPD will collect personal information for the following and/or related purposes:

- References of an employee or job applicant, for purposes of employment;
- Ensuring quality of delivery of services to clients;
- Complying with contracts with various parties;
- Confirmation of employment;
- Debt collection, including tracing in the event of default on payment;
- Compliance with legislation;
- Vetting of employees;
- Due diligence with building owners;
- Assisting in treating customers fairly, by having complete and up to date information about the customer;
- Effective communication with clients and suppliers, to avoid misunderstandings or failure to communicate as a result of incorrect information;
- Detection and prevention of fraud, crime, money laundering or other criminal activities;
- Audit and record keeping purposes;
- Completion of application forms and contractual documents.

5.3.2 Once personal information, processed and stored by MPD, has been retained for the full term as dictated by MPD or as required by law or industry standard or becomes in any way redundant, MPD will destroy or delete the record of personal information in a manner that prevents its reconstruction in an intelligible form.

5.4 Further processing limitation

The responsible party must ensure that if personal information is processed again it must be used for the original purpose they informed the data subject about. MPD undertakes to carry out any further processing of personal information (further processing being processing of information already collected previously) in accordance or compatible with the purpose for which it was collected originally.

5.5 Information quality

The responsible party must use its best endeavours to ensure that the personal information it processes is accurate and complete. MPD will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where

necessary. Data subjects are however required to ensure that any personal information that is provided is complete, accurate, not misleading and consistently updated where necessary.

5.6 Openness

The responsible party must process personal information in a way that allows the data subject to know what is happening to their personal information.

5.6.1 MPD will ensure that all the documentation of processing operations under its responsibility will be stored and preserved for the required duration and purpose.

5.6.2 If personal information is collected, MPD will take reasonable steps to ensure that the data subject is aware (whether by means of contract, email notification or statement on its website) of all of the following (to the extent applicable):

- the information being collected or the source from which it is collected;
- the name and address of the responsible party;
- the purpose for which the information is being collected;
- whether or not the supply of the information by that data subject is voluntary or mandatory;
- the consequences of failure to provide the personal information;
- any particular law authorising or requiring the collection of the personal information;
- the responsible party intending to transfer the information to another country or international organisation, for instance where information is stored on a cloud server based in a foreign country, that the level of protection afforded to the information by that other country or international organisation is adequate;
- any further relevant information.

5.7 Security safeguards

The responsible party must provide appropriate and reasonable security measures for personal information.

5.7.1 MPD undertakes to secure the integrity and confidentiality of personal information in its possession or under its control. This is done by taking appropriate, reasonable technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal information, and unlawful access thereto (by either a third party or internally by someone within MPD) or unlawful processing thereof.

5.7.2 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, MPD will as soon as reasonably possible after the discovery of the compromise notify:

- the Information Regulator; and
- the data subject, unless the identity of such data subject cannot be established.

5.7.3 MPD has put in place the following adequate safeguards to secure the integrity and confidentiality of personal information:

- Physical access security to the head office building;
- Alarm system to the head office building;
- Password protection on all employee computer logins;
- Anti-virus on all employee computers;
- Firewalls on all employee computers;
- Encryption on all employee computers;
- Secure back-ups of information, stored in a secure location, which is encrypted;
- Regular IT audits to ensure adequate data protection;
- This privacy policy to be complied with by all employees.

5.7.4 MPD conducts periodic risk assessments regarding the processing of personal information, to determine the level of internal and external risks, as well as to implement measures to mitigate and minimise any risks identified.

5.8 Data subject participation

The responsible party must communicate with the data subject about processing and must allow the data subject to correct or update their personal information.

If you have any questions or concerns regarding this policy, your personal information held by MPD, the correction or deletion of personal information or updating your personal information held by MPD, you should contact MPD by sending an email to ananda@expreit.co.za, alternatively contacting us at 012 660 3020 or visiting our office located at 204 Von Willich Avenue, Clubview, Centurion, Pretoria. Data subjects also have the following rights in terms of POPI: to request access to their personal information; to request correction or deletion of personal information; to object to the processing of personal information; and to submit a complaint to the Information Regulator. If you are not satisfied with how MPD has handled your personal information, you may lodge a complaint with the Information Regulator by completing the prescribed POPI form 5 and submitting it via email to POPIAComplaints@inforegulator.org.za.

6. COLLECTION OF INFORMATION

MPD collects personal information in any of the following manners:

- Voluntary disclosure via multiple sources;
- Telephonically;
- Credit bureau systems;
- Deeds office;
- Email;
- Application forms;
- Agreements (service agreements or other agreements).

7. STORAGE AND RETENTION OF RECORDS

All records containing personal information will be stored or kept in a secure location, at the head office in Centurion, which has restricted access and is kept in a facility secure from arson or theft. Records which are stored electronically are protected with an encrypted password and backed-up on a secure platform. Any records stored at the shopping centres within the MPD portfolio are kept in an access controlled office, which has centre security. MPD maintains a retention schedule which specifies minimum retention periods for different categories of records (for example, HR files, service agreements, and financial records). Once the relevant period expires, records are securely destroyed or de-identified unless a longer period is required by law.

8. DESTRUCTION

Further to paragraph 5.3.2, all records containing personal information will be destroyed or de-identified when the personal information becomes obsolete and is no longer required to achieve its intended purpose or upon request by a data subject, provided the responsible party is no longer authorised to retain such personal information in terms of section 14 of POPI. Where MPD is involved in or anticipates that it may be involved in litigation, MPD may place a hold on the destruction of any document that may contain personal information in order to preserve any potential evidence.

9. DIRECT MARKETING

In accordance with section 69 of POPI, MPD will not engage in direct marketing by electronic communications (such as SMS or email) without the required consent. Existing customers will always be given a reasonable opportunity to opt out of receiving further direct marketing communications.

10. TRAINING OF STAFF

This policy will be made available to all employees of MPD. MPD trains the (relevant) staff

on this policy in order to protect the confidentially, security, accuracy and integrity of all personal information in its possession or under its control.

11. PRIOR AUTHORISATION

In accordance with POPI, prior authorisation must be obtained from the Information Regulator before processing any personal information which falls into any of the following categories:

11.1 any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection and with the aim of linking the information together with information processed by other responsible parties (e.g using an ID number initially collected for due diligence business purposes and later linked to a credit provider);

11.2 criminal history of any third parties;

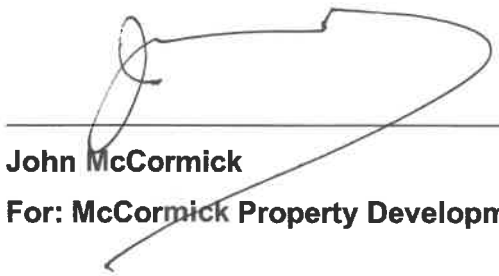
11.3 for the purposes of credit reporting; or

11.4 transferring special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

In the event that MPD processes any personal information in any of the above categories (which requires prior authorisation from the Information Regulator), it is the responsibility of the information officer to obtain such authorisation.

12. APPROVAL OF THIS POLICY

This policy was approved and will be reviewed at least annually, or whenever there is a material change in the law or in MPD's processing activities.



John McCormick
For: McCormick Property Development Proprietary Limited