sa construction group

Reg No: 2017/287927/07

No. 6 HEATH CIRCLE, BLACKHEATH, 7580
POSTNET SUITE #9, PRIVATE BAG X04, KUILSRIVER, 7579
Tel: (021) 905 7338 Fax2mail: 086 604 2000
www.sa-construction.co.za

POPI POLICY

INTRODUCTION

The purpose of this policy is for SA Construction (Pty) Ltd to comply with the Protection of Personal Information Act, No.4 of 2013 (hereinafter referred to as the "POPI Act" or "the Act").

The POPI Act requires the Company to:

- Sufficiently inform employees/candidates/applicants and work-seekers (data subjects) of the purpose for which the company will process their personal information.
- Protect any information assets from threats, whether internal or external, deliberate or accidental to ensure business continuation/sustainability, minimize business damage and maximize business opportunities.

This policy sets out a compliance framework and establishes measures and standards for the protection and processing of personal information within the Company. It further provides principles regarding the right of an individual's (data -subject) privacy and to reasonable safeguarding of their personal information.

POLICY APPLICATION

This policy and its principles apply to the company's owners, management, employees as well as all branches, business units and divisions of the company. It further applies to all those acting on behalf of the company.

The policy's guiding principles find application in various situations and it's important that it be read in conjunction with the Act and the Promotion of Access to Information Act no. 2 of 2000.

The legal duty to comply with the Act and its provisions is required in any situation where there is processing of:

- Personal information.
- Entered into a record.
- By or for a responsible person
- Who is domiciled in South Africa.

The Act does not apply in situations where the processing of personal information is concluded in the course of purely personal or household activities, or where the personal information has been de-identified

DATA SUBJECTS & THEIR RIGHTS

It is imperative for the company's employees, clients and customers to be ensured that where appropriate, the company will make all parties aware of the rights as conferred upon them as data subjects.

The company will ensure that it gives effect to the following rights namely:

1. **The Right to Access Personal Information**

   The data subject has the right to establish whether the company holds personal information related to him/her. This includes, but is not limited to, the right to request access to that information.

2. **The Right to have certain Personal Information Corrected or Deleted**

   The data subject has the right to request, where reasonable and necessary, that his or her personal information be corrected or deleted. This includes instances where the company is no longer privy to information of the data subject.

3. **The Right that the Data Subject has to object to the Processing of certain Personal Information**

   It is to be borne in mind that the data subject has the right, be it on reasonable grounds, to object to the processing of his/her personal information.

   Should a data subject object to the processing of certain personal information, the company will be required to give due consideration to the request and the requirements of the Act. The company may, however, cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of personal information.

4. **The Right to Object to Direct Marketing**

   The data subject has the definite right to object to the processing of any of his/her personal information for the purposes of direct marketing by means of any unsolicited electronic communication

(i.e. telemarketers contacting the data subject my means of telephonic calls, SMS's or emails).

5. **The Right to Complain to the relevant Information Regulator**

   The data subject has the right to submit a reasonable complaint to the company's duly appointed Information Regulator regarding an alleged infringement of any of the rights protected under the Act and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her personal information.

6. **The Right to be Informed**

   The data subject has the right to be informed that his/her personal information is being collected by the company. Furthermore, the data subject has the right to be notified in any situation where the company has reasonable grounds to believe that the personal information of the data subject has been accessed or retained by an unauthorized person (i.e. server has been hacked and information compromised).

GUIDING PRINCIPLES

The company, its employees and all persons acting on behalf of the company will at all times be required to abide by, be subject to, and act in accordance with the following principles:

1. **Accountability**

   It is extremely important to note that failing to comply with the Act could potentially damage the company's reputation or expose the company to a civil claim for damages incurred. The protection of personal information rests on the shoulder of all employees and should not be taken lightly. The company will ensure that the provisions of the Act and the guiding principles as outlined in this policy are complied with.

   Furthermore, the company will take appropriate steps, which may include, but are not limited to disciplinary actions, against those employees who through their intentional or negligent actions and or omissions, fail to comply with the principles and responsivities outlined in this policy.

2. **Processing Limitations**

   The company will ensure that the personal information of its data subjects is processed in a way that is fair, lawful, in a non-excessive manner, with the necessary and informed consent of the data subject and only for a specifically defined purpose.

   The company will set out to inform the relevant data subject of the reasons for collecting his/her personal information and obtain written consent prior to the processing of the information. The company will under no circumstances distribute or share personal information between separate legal entities, associated companies, or organizations or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

   Where the company deems appropriate, the data subject will be informed of the possibility that his/her personal information will be shared with 3rd parties and be provided with reasons for doing so.

3. **Specification**

   All of the company's departments/divisions and operations must be informed by what is known as the "principle of transparency". The company will process personal information only for **specific, explicitly defined and legitimate reasons.** The company will be responsible for ensuring that its data subjects are made aware prior to the collecting or recording of personal information.

4. **Further Limitations**

   It is to be borne in mind that any and all personal information will not be processed for a secondary purpose unless that said processing is compatible with the original purpose for which it was collected. Thus, where the company seeks to process personal information it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary process is not compatible with the original purpose, the company will first obtain additional consent from the data subject.

5. **Quality of Information Collected**

   The company will take the necessary steps to ensure that all personal information collected is complete, accurate, and not misleading.

Where personal information is collected from 3rd parties, the company will take reasonable steps to ensure that the information is correct by verifying the accuracy of the information directly with the data subject.

6. **Open Communication**

The company will take reasonable steps to ensure that data subjects are always notified that their personal information is being collected – including the purpose for which it is being collected and processed. The company will ensure that it goes further to establish a facility (electronic help desk or provide an email address or phone number) for data subjects who wish to enquire whether the company holds related personal information, or request access to related personal information, or request the company to update or correct personal information, or issue a complaint concerning the access or processing of personal information.

7. **Necessary Security Safeguards**

The company will manage the security of its filing system to ensure that personal information is adequately protected. Security controls will be implemented in order to minimize any risk of loss, unauthorized access, disclosure, interference, modification or destruction.

The company will ensure to continuously review its security controls which will include inter alia, regular testing of protocols and measures put in place to combat cyber-attacks on the company's IT network (i.e. server).

The company will ensure that all paper and electronic records comprising of personal information are securely stored and only made accessible to authorized individuals.

All new employees will be required to sign contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included in said contracts to reduce the risk of unauthorized disclosures of personal information for which the company is responsible. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contract containing the relevant consent and confidentiality clauses.

8. **Data Subject Participation**

A data subject may as aforementioned, request the correction or deletion of his/her personal information held by the company. The company will ensure that it provides a facility for data subjects who wish to request the correction or deletion of their personal information.

CORPORATE GOVERNANCE OFFICER (INFORMATION OFFICER)

The Company will appoint a Corporate Governance Officer (hereinafter referred as a "CGO") and where necessary, a Corporate Governance Assistant to assist the CGO –

The company's CGO is responsible for ensuring compliance with the Act.

Where no CGO is appointed, the head of the company will automatically assume the role of the CGO. Consideration will be given on an annual basis to the re appointment or replacement of the CGO and the reappointment of the CGO's Assistant. Once appointed, the company will be responsible for registering the Information Officer with the South African Information Regulator under the Act prior to performing his/her duties.

DUTIES & RESPONSIBILITIES

The company's CGO will be responsible for the following:

- Take the necessary steps to ensure that the company's compliance with the Act.
- Keeping the owners of the company updated about the company's information protection responsibilities under the Act
- Analyzing privacy regulations and aligning such regulations with the company's personal information and the processing of such information.
- To ensure that regular POPI audits are scheduled and conducted.
- Ensure that it is at all times for the data subjects of the company to conveniently update their information or lodge a complaint.

sa construction group

Reg No: 2017/287927/07

No. 6 HEATH CIRCLE, BLACKHEATH, 7580
POSTNET SUITE #9, PRIVATE BAG X04, KUILSRIVER, 7579
Tel: (021) 905 7338 Fax2mail: 086 604 2000
www.sa-construction.co.za

- To approve any contracts entered into with 3rd parties which may have an impact on the personal information held by the company.
- To ensure that those acting on behalf of the company are fully acquainted with the risks associated with the processing of personal information and that they remain informed about the company's security controls.
- To address employees on questions related to the Act.
- To work with the Information Regulator in relation to any ongoing investigations related to the breach of any personal information.

POPI AUDIT

The CGO along with a consultant from Danshaw Consulting will schedule a full and comprehensive POPIA audit. The purpose of the audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Redefine the purpose for gathering and processing of personal information.
- Ensuring that the processing parameters are adequately limited.
- Ensure that any new data subjects are made fully aware of the processing of personal information.
- Verify the quality and security of personal information.
- Monitor the extent of compliance with the Act and this policy.
- Monitor the effectiveness of all internal controls established to manage the organizations POPI related compliance risk.

DISCIPLINARY ACTION

In matters where a POPI complaint or infringement has been finalized, the company may recommend any appropriate administrative, legal and/or disciplinary action be taken against any employee reasonably suspected of being implicated in any non-complaint activity as aforementioned.

In cases where the company is dealing with ignorance or minor negligence, the company will undertake to provide further awareness training to the employee, however, any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the organization may summarily dismiss the employee.

It is to be borne in mind that disciplinary procedures will only commence where there is sufficient evidence to support an employee's gross negligence. Examples of immediate action to be taken subsequent to an investigation include, but are not limited to:

- Upon recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation, and
- Recovery of funds and assets to limit further prejudice or damages caused.

STORAGE OF DOCUMENTS – HARD COPIES

1. **<u>The Basic Conditions of Employment Act, No 75 of 1997</u>**

   The Basic Conditions of Employment Act (hereinafter referred to as the "BCEA") requires a retention period of 3 years for the documents as mentioned below:

- Section 29(4) – Written particulars of an employee after termination of employment.
- Section 31 – Employee's name and occupation, time worked by each employee, remuneration paid to each employee and date of birth of any employee under the age of 18 years.

2. **<u>Employment Equity Act, No 55 of 1998:</u>**

   Section 26 and the General Administrative Regulations of 2009 (Regulation 3(2)) requires the retention period of 3 years for the documents as mentioned below:

   - Any record in respect of the company's workforce, employment equity and other records relevant to compliance with the Act.

3. **<u>Labour Relations Act, No 66 of 1995:</u>**

Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:

- The relevant Bargaining Council must retain books of accounts, supporting vouchers, income and expenditure statements, balance sheets, reports by auditors and minutes of all meetings.
- Registered Trade Unions and registered employer's organizations must retain books of accounts, supporting vouchers, income and expenditure statements, balance sheets, reports by auditors and minutes of all meetings.
- Registered Trade Unions and employer's organizations must retain the ballot papers.
- Employers must retain all collective agreements and arbitration awards.

- Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents as mentioned below:
  - Registered Trade Unions and Registered Employer's Organizations must retain a list of its members.
  - An employer must retain prescribed details of any past or present strike, lock-out or protest action involving its employees.
  - Records of each employee specifying the nature of any disciplinary actions/transgressions, the actions taken by the employer and the reasons for the actions.

4. **<u>Unemployment Insurance Act, No 63 of 2002:</u>**

The Act, applies to all employees and employers except:

- Workers working less than 24 hours a month.
- Learners.
- Public servants.
- Foreigners working on a contract basis.
- Workers who get a monthly pension.
- Workers who only earn commission.
- Section 56(2) (c) requires a retention period of 5 years, from the date of submission for the documentation as mentioned below:

Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration, and address where the employee is employed.

ELECTRONIC STORAGE OF DOCUMENTS

The electronic storage of information – important documents and information must be referred to and discussed with the designated IT officer (internal or external). He/she will be responsible for the indexing, storage and retrieval of electronic documents containing personal information.

If documents are scanned, the hard copy must also be retained for as long as the information is used for 1 year after the date of scanning, with the exception of documents pertaining to employees. Any and all documents containing information on the written particulars of an employee, including an employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18; must be retained for a period of 3 years after termination of employment.

Sec 51 of the Electronic Communications Act No 25 of 2005 (hereinafter referred to as the "ECT Act") requires that personal information and the purpose for which the data was/is collected must be kept by the individual who electronically requests, collects, collates, processes or stores the information and a record of any 3rd party to whom the information was disclosed must be retained for a period of 1 year for as long as the information is used. The Act further requires that all personal information which becomes obsolete must be destroyed.

DESTRUCTION OF DOCUMENTS

sa construction group

Reg No: 2017/287927/07

No. 6 HEATH CIRCLE, BLACKHEATH, 7580
POSTNET SUITE #9, PRIVATE BAG X04, KUILSRIVER, 7579
Tel: (021) 905 7338 Fax2mail: 086 604 2000
www.sa-construction.co.za

Each department within the company is responsible for attending to the destruction of its documents, this must be done on a regular basis. Files must be checked in order to ensure that they may be destroyed and also to ascertain if there are important original documents in the file. All original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

After the process as aforementioned, the manager of the department shall, in writing, authorize the removal and destruction of the documents.

The documents are then to be made available for collection by the necessary removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information. Alternatively, documents may be stored off-site, in storage facilities approved by the company.

CONSENT

WHEREAS IT IS AGREED THAT,

By signature hereunder, all parties irrevocably agree to abide by the terms and conditions as set out in this agreement as well as you irrevocably agree and acknowledge that all information provided, whether personal or otherwise, may be used and processed by the company and such use may include placing such information in the public domain.

Further it is specifically agreed that the company will use its best endeavors and take all reasonable precautions to ensure that any information provided, is only used for the purposes it has been provided. It is agreed that such information may be placed in the public domain and by signature hereunder, all parties acknowledge that they have read all of the terms in this policy and that they understand and agree to be bound by the terms and conditions as set out in this agreement.

PRIVACY POLICY

Privacy Policy
Last updated: August 31, 2021

This Privacy Policy describes Our policies and procedures on the collection, use and disclosure of Your information when You use the Service and tells You about Your privacy rights and how the law protects You.

We use Your Personal data to provide and improve the Service. By using the Service, You agree to the collection and use of information in accordance with this Privacy Policy. This Privacy Policy has been created with the help of the Privacy Policy Generator.

Interpretation and Definitions

Interpretation

The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

Account means a unique account created for You to access our Service or parts of our Service.

Company (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to SA Construction Group Companies (SA Construction (Pty) Ltd, Nejeni Construction and Project Management (Pty) Ltd, Umdla Civils (Pty) Ltd, WeConstruct (Pty) Ltd, Sidinga Suppliers (Pty) Ltd, Blackheath, Western Cape.

Cookies are small files that are placed on Your computer, mobile device or any other device by a website, containing the details of Your browsing history on that website among its many uses.

Country refers to: South Africa

Device means any device that can access the Service such as a computer, a cellphone or a digital tablet.

sa construction group

Reg No: 2017/287927/07

No. 6 HEATH CIRCLE, BLACKHEATH, 7580
POSTNET SUITE #9, PRIVATE BAG X04, KUILSRIVER, 7579
Tel: (021) 905 7338 Fax2mail: 086 604 2000
www.sa-construction.co.za

Personal Data is any information that relates to an identified or identifiable individual.
Service refers to the Website.
Service Provider means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, to provide the Service on behalf of the Company, to perform services related to the Service or to assist the Company in analyzing how the Service is used.
Usage Data refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
Website refers to SA Construction Group Company websites, accessible from http://www.sa-construction.co.za
You means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.

Collecting and Using Your Personal Data
Types of Data Collected
Personal Data
While using Our Service, We may ask You to provide Us with certain personally identifiable information that can be used to contact or identify You. Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Usage Data

Usage Data
Usage Data is collected automatically when using the Service.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Tracking Technologies and Cookies
We use Cookies and similar tracking technologies to track the activity on Our Service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze Our Service. The technologies We use may include:

- *Cookies or Browser Cookies*. A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service. Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.
- *Flash Cookies*. Certain features of our Service may use local stored objects (or Flash Cookies) to collect and store information about Your preferences or Your activity on our Service. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies. For more information on how You can delete Flash Cookies, please read "Where can I change the settings for disabling, or deleting local shared objects?" available at https://helpx.adobe.com/flash-player/kb/disable-local-shared-objects-

flash.html#main_Where_can_I_change_the_settings_for_disabling__or_deleting_local_shared_objects_

- *Web Beacons*. Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, 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).

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser. Learn more about cookies: Cookies: What Do They Do?.

We use both Session and Persistent Cookies for the purposes set out below:

Necessary / Essential Cookies
Type: Session Cookies
Administered by: Us
Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

Cookies Policy / Notice Acceptance Cookies

Type: Persistent Cookies
Administered by: Us
Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

Functionality Cookies

Type: Persistent Cookies
Administered by: Us
Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

For more information about the cookies we use and your choices regarding cookies, please visit our Cookies Policy or the Cookies section of our Privacy Policy.

Use of Your Personal Data
The Company may use Personal Data for the following purposes:

a) To provide and maintain our Service, including to monitor the usage of our Service.

b) To manage Your Account: to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.

c) For the performance of a contract: the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.

d) To contact You: To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted

services, including the security updates, when necessary or reasonable for their implementation.

e) To provide You with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.

f) To manage Your requests: To attend and manage Your requests to Us.

g) For business transfers: We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.

h) For other purposes: We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience.

We may share Your personal information in the following situations:

a) With Service Providers: We may share Your personal information with Service Providers to monitor and analyze the use of our Service, to contact You.
b) For business transfers: We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.
c) With Affiliates: We may share Your information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
d) With business partners: We may share Your information with Our business partners to offer You certain products, services or promotions.
e) With other users: when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside.
f) With Your consent: We may disclose Your personal information for any other purpose with Your consent.

Retention of Your Personal Data

The Company will retain Your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Transfer of Your Personal Data

Your information, including Personal Data, is processed at the Company's operating offices and in any other places where the parties involved in

the processing are located. It means that this information may be transferred to — and maintained on — computers located outside of Your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from Your jurisdiction.

Your consent to this Privacy Policy followed by Your submission of such information represents Your agreement to that transfer.

The Company will take all steps reasonably necessary to ensure that Your data is treated securely and in accordance with this Privacy Policy and no transfer of Your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of Your data and other personal information.

Disclosure of Your Personal Data

Business Transactions

If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.

Law enforcement

Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Other legal requirements

The Company may disclose Your Personal Data in the good faith belief that such action is necessary to:

Comply with a legal obligation

Protect and defend the rights or property of the Company

Prevent or investigate possible wrongdoing in connection with the Service

Protect the personal safety of Users of the Service or the public

Protect against legal liability

Security of Your Personal Data

The security of Your Personal Data is important to Us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While We strive to use commercially acceptable means to protect Your Personal Data, We cannot guarantee its absolute security.

Children's Privacy

Our Service does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 13 without verification of parental consent, We take steps to remove that information from Our servers.

If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, We may require Your parent's consent before We collect and use that information.

Links to Other Websites

Our Service may contain links to other websites that are not operated by Us. If You click on a third party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Reg No: 2017/287927/07

No. 6 HEATH CIRCLE, BLACKHEATH, 7580
POSTNET SUITE #9, PRIVATE BAG X04, KUILSRIVER, 7579
Tel: (021) 905 7338 Fax2mail: 086 604 2000
www.sa-construction.co.za

Changes to this Privacy Policy

We may update Our Privacy Policy from time to time. We will notify You of any changes by posting the new Privacy Policy on this page.

We will let You know via email and/or a prominent notice on Our Service, prior to the change becoming effective and update the "Last updated" date at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions about this Privacy Policy, You can contact us:

By email: lizinda@sa-construction.co.za