

## PRIVACY POLICY

### 1. OBJECTIVE

- 1.1 At HDK Architects (Pty) Ltd, we are committed to processing your Personal Information in compliance with the Protection of Personal Information Act 4 of 2013 ("POPIA").

### 2. DEFINITIONS

- 2.1 "Personal Information:" "Information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person."
- 2.2 "Data Subject:" "The person to whom Personal Information relates."
- 2.3 "Responsible Party:" For purposes of this Notice, the Responsible Party is **HDK Architects (Pty) Ltd**.
- 2.4 "Consent:" "Voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information."
- 2.5 "Processing:" "Any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information."
- 2.6 "Record:" "Any recorded information..."
- 2.7 "Regulator:" "Information Regulator established in terms of Section 39."
- 2.8 "Special Personal Information:" Personal Information of a data subject relating to their religious or philosophical beliefs; race of ethnic origin; trade union

membership; political persuasion; health or sex life; biometric information and criminal behavior (to an extent).

### 3. GENERAL

- 3.1 We strive to treat all client information as strictly confidential.
- 3.2 No Personal Information regarding a client may at any time or by any means be divulged to an outsider by an employee.
- 3.3 No employee may request, gather or store any Personal Information from or regarding a client, unless this is done for business purposes and takes place with the full knowledge and Consent of the client concerned. The information collected and processed will only be used for the specified purpose for which it was intended, as set out at the time of instruction.
- 3.4 We undertake to provide access, upon request, to our clients and employees to their own Records, in terms of the provisions of POPIA, and where sufficient proof of identity has been shown upon such request.
- 3.5 Where a client wishes to correct/update their Records, we will request proof of the corrected/updated information before rectifying our documents to reflect the change. Proper record will also be kept of the client's request to amend the details of their Record held by us, including the date of the request for the change as well as the change itself.
- 3.6 Where necessary, relevant and in the interest of properly carrying out our instructions and / or mandate, third parties will be notified of changes to the details of a client.
- 3.7 Where a Data Subject requests a Record or description of the Personal Information we hold, as well as that information to which third parties have access, we will attend to such a request within a reasonable time; at a prescribed fee (if any); in a reasonable manner and format; and in a form that is generally understandable.

#### 4. INFORMATION OFFICER

4.1 The details of our Information Officer are as follows:

4.1.1 Information Officer:                   Roan Hugo  
[roan@hdkarch.co.za](mailto:roan@hdkarch.co.za)  
073 157 3999

4.2 For any queries, requests or complaints related to the Processing of Personal Information, please contact our Information Officer.

#### 5. INCIDENT MANAGEMENT PROCESS

5.1 The Processing of data, particularly by electronic means, is always accompanied by a certain element of risk. Although we do everything in our power to safeguard the Personal Information entrusted to us, security breaches are still a possibility.

5.2 Where we have become aware of a data security breach / have reasonable grounds to believe that there has been a data security breach, this will be reported to the Information Regulator, as well as the Data Subject concerned, as soon as reasonably possible after becoming aware of the compromise / possible compromise, and we will provide enough information to allow the Data Subject to take action against any potential consequences.

#### 6. RESEARCH REGARDING EMPLOYMENT APPLICATIONS

6.1 All applicants / prospective employees of HDK Architects (Pty) Ltd are required to furnish certain details, within the ambit of the definition of "Personal Information," necessary for the consideration of their applications, including but not limited to, details of previous employment / work experience, identity numbers and contact details, for the purposes of background and reference checks.

6.2 Applicants / prospective employees confirm that the details of any and all references provided to us are so furnished with the express Consent of the named person.

#### 7. EMPLOYEE COGNISANCE OF POLICY

- 7.1 Employees of HDK Architects (Pty) Ltd, as part of their conditions of employment, attend a training workshop centered on dealing with the Personal Information of our clients in line with the provisions of POPIA.
- 7.2 Each employee, therefore, is aware of the requirements for lawful Processing of Personal Information and has undertaken to treat all client information as strictly confidential, both during and after their employment period.
- 7.3 Our Information Officer is responsible for updating and informing the employees of any relevant new regulations pertaining to POPIA and ensuring that they carry out their duties in line therewith.

## 8. DOCUMENTS CONTAINING PERSONAL INFORMATION

### 8.1 COMPUTERS

- 8.1.1 Only authorised employees (architects and support staff) hold passwords and access to the company's computers and printers.
- 8.1.2 By virtue of our internal privacy policy, these passwords are not shared with other computer users / divulged to any other person, except the authorised head of division.
- 8.1.3 Passwords and all physical and digital access to our Records are immediately removed by our IT agents upon an employee's termination of service.

### 7.1 REMOVAL OF DOCUMENTS FROM OFFICE

- 7.1.1 No files and/or documents containing the Personal Information of any client or employee may leave the premises without the prior approval of the head of department.
- 7.1.2 Such approval is only granted where the documents are removed exclusively for work purposes and the head of department is satisfied that the file/document will not fall into the hands of unauthorised persons.

- 7.1.3 Any document that leaves the office building is placed in a sealed envelope with the complete details of the addressee, as well as a return address in the case of non-delivery.
- 7.1.4 Where documents are sent by courier, the services of a reliable/reputable courier company are utilised the documents are handed to the courier service in a sealed envelope.
- 7.1.5 Any document containing Personal Information of a client / employee is only handed to a person who is not in our service where such a person has received a direct instruction to handle the document or to the person whose information is contained in the document.

## 7.2 REMOTE COMPUTERS

- 7.2.1 Where employees are, for any reason, required to work from home, remote access is granted to such employees (architects and support staff), with the requisite security safeguards (passwords, anti-virus, firewall, etc.) in place to ensure that no unauthorised person gains access to our main frame.
- 7.2.2 Employees are required to obtain prior authorisation from their head of department before removing his/her computer, or any component thereof, from the building.

## 9. RESTRICTION OF ACCESS TO OFFICES

- 9.1 All documents containing Personal Information, including all documents created and stored in electronic format, are kept within the premises known as 27 Willie van Schoor Drive, Office 1, Tygervalley Chambers 5, Bellville, Cape Town.
- 9.2 All existing client files are on a daily basis kept in our locked safe and all other files are kept in the respective division's filing cabinets.
- 9.3 Documents in closed files are kept in the archives / storeroom, which is kept locked. The key is kept in a safe place and is only handed to authorised persons.

- 9.4 When closed files are destroyed after expiry of the prescribed period, the Information Officer ensures that the documents are shredded or otherwise properly destroyed.

## 10. ACCESS TO MAIN BUILDING

- 10.1 Both the front door and the security gate are locked at all times. The receptionist only grants access to authorised persons.
- 10.2 Documents containing Personal Information are not kept in the foyer, unless inside a sealed envelope.
- 10.3 Non-employees/visitors are not permitted to leave the foyer area of the office building to enter the rest of the building, unless accompanied by an employee, to ensure that the visitor does not gain access to any documents and/or information which does not apply to him/her.
- 10.4 Outside office hours, the building is kept locked at all times.

## 11. RISK

- 11.1 The Information Officer attends, on an annual basis, to an update on our risk analysis report and data security safeguards, including the relevant measures pertaining to our physical, digital, operational and administrative security.
- 11.2 Where necessary, the relevant aspects of our security is updated to ensure the strongest possible security measures are in place.

## 12. SUB-CONTRACTORS

- 12.1 There are a number of instances where we, with the prior consent of the client, must make use of a sub-contractor, for example, building or compliance contractors.
- 12.2 Where a sub-contractor handles client information in a manner contrary to the provisions of our privacy and POPIA policies, or there are reasonable grounds to

believe that a sub-contractor has handled client information in a manner contrary to the provisions of our privacy and POPIA policies, this will be reported to the Data Subject concerned, as well as to the Information Regulator, by our Information Officer.

### 13. BACK-UP SUPPORT

All information stored on our system is regularly backed up.