

Information notice for job applicants

Dedalus Southern Africa (Pty) Ltd and Faranani Healthcare Solutions (Pty) (“Dedalus”) attach a great deal of importance to and intends to pay particular attention to protecting your personal information and respecting your privacy.

The aim of this privacy policy (the “**Policy**”) is therefore to inform you of how your personal information is processed when you submit your application for a position within Dedalus (paid employment, internship, etc.).

In this regard, please note that Dedalus is deemed to act as the responsible party under applicable data protection laws, which include the *Protection of Personal Information Act* No. 4 of 2013 (POPI) and the *Promotion of Access to Information Act* No 2 (PAIA) for your personal information (hereinafter referred to as “**we**”, “**us**” and “**our**”). Please refer to Section 7 (“*How can you contact us?*”) below to access the contact details.

The Bill of Rights in the Constitution of South Africa guarantees you a right to privacy. It also provides for a limitation of your right to privacy. This policy takes into account all of these rights and limitations.

1

WHAT PERSONAL DATA DO WE COLLECT?

We collect the following categories of personal information about you:

- Identification data (e.g., surname, first name, date of birth, etc.).
- Professional and educational data (e.g., resume, identity of your current employer (if applicable)).
- Evaluation data regarding your professional skills, including the results of practical tests performed during the recruitment process
- Personal data (i.e., data relating to your personal life, as it appears on your resume or that you voluntarily convey in your exchanges with us, such as your hobbies or your marital status).
- Economic data (e.g., your current salary and salary expectations, etc.).
- Health-related data (e.g., information regarding disability) and other special categories of data (e.g., racial, or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership) if applicable pursuant to local legislation.
- Data related to criminal convictions and offences, if authorized by local laws.
- Gender, race, ethnic origin, and disability (due to the Government’s Black Economic Empowerment (BEE) is a policy to facilitate broader participation in the economy)

The provision of your personal information is voluntary, but in most cases, we will be unable to process your application properly without it. For example, if you refuse to provide us with reasonably

required information regarding your educational and professional background, we will be unable to determine whether your profile meets the needs of the position and will have to reject your application.

In any case, we will inform you when it is mandatory to provide your personal information.

Additionally, if you provide us with personal information belonging to third parties (e.g., contact details for people with whom we can verify your references), you undertake to ensure that such persons have been duly informed of the processing of their personal information in accordance with this policy and, if required, have consented to the processing of their personal information.

The personal information may be collected directly from you or can be provided by third parties (such as, previous employers to verify your references) and/or publicly accessible sources.

2

WHY DO WE USE YOUR PERSONAL DATA?

The table below outlines the purposes that we process your personal information for and, for each purpose, the purpose (legal basis) for the processing operation in question:

PURPOSES	LEGAL BASIS
Processing of your application to: (i) determine the suitability of your profile for the position in question; and (ii) make you an offer if we believe that your profile matches the position that you have applied for.	The legal basis of the processing is the performance of the necessary steps to enter a potential employment contract with you. If special categories of data (such as, religion and philosophical beliefs, race and ethnic origin, political persuasion, sex life, biometric information, data relating to your health, your membership of a trade union) is processed in this context, the legal basis for such processing is the necessity to comply with relevant laws.
Site access and security management, including video surveillance if you are interviewing on our premises	Our legitimate interest is to protect people, premises, and property.
Compliance with the applicable legal framework	Need to comply with a legal obligation that we are subject to.
Management and follow-up of potential disputes	Our legitimate interest is to defend our interests, including through legal action.
Processing your request to receive our job alerts	Your optional consent.

In any case, please note that we will not process your personal information for any other purpose that is incompatible with the above-mentioned purposes.

3

WHO DO WE SHARE YOUR PERSONAL DATA WITH?

In the context of our processing operations, we may communicate your personal information to the following recipients:

- to our service providers, suppliers, agents, and contractors, to the extent that they assist us in carrying out the purposes set out in this policy (e.g., we use IT service providers to host your personal information on our behalf).
- to other entities of the Dedalus Group.
- to competent courts, public authorities, government agencies and law enforcement agencies (including where we are required to comply with legal or regulatory requests).

Regardless of the recipient, we will only disclose your personal information to them on a strictly need-to-know basis and only to the extent required to fulfill the purposes identified in this policy.

We do not sell your personal information. We do not do direct marketing. We will not subject you to decisions which have legal consequences and affect you based on automated processing of your information intended to provide a profile including your performance at work, worthiness, reliability, location, health, and personal preferences.

4

DO WE TRANSFER DATA OUTSIDE SOUTH AFRICA?

In connection with the processing operations described in this policy, we may transfer your personal information outside the South Africa ("ZA"), including to countries that are not generally recognized as providing an adequate level of data protection.

This specifically means that each of the intended transfers is based on one of the following mechanisms at least:

- the provision of an adequate level of protection for the processing of personal information as referred to in section 72 of POPI; or alternatively;
- the conclusion of binding corporate rules or binding agreements which provide an adequate level of protection that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information in the Republic of South Africa, including the standard contractual clauses reproducing the models adopted by the European Commission; or, alternatively;
- the existence of an exemption related to one of the specific situations exhaustively provided for in Applicable Data Protection Laws (e.g. where you have given your consent to such transfer having been informed of the absence of safeguards, where the transfer is necessary for the performance of a contract concluded between you and us, where the transfer is necessary for the conclusion or performance of a contract concluded in your interest

between us and a third party, or where the transfer is necessary for the establishment, exercise or defense of our legal claims, where it is not reasonably practicable to obtain your consent and where if it was practical you would be likely to give consent etc.).

5

HOW LONG DO WE STORE YOUR PERSONAL DATA FOR?

We store your personal information for no longer than is necessary for the purpose of the processing concerned and as required by law.

In other words, this means that the storage periods we apply vary depending on the purpose for which we process the data in question. The table below therefore indicates, for each purpose, the storage period that will be applied to your personal information:

PURPOSES	STORAGE PERIOD
Processing of your application to: (i) determine the suitability of your profile for the position in question; and (ii) make you an offer if we believe that your profile matches the position that you have applied for.	If the application is unsuccessful, the data will be kept until the end of the recruitment process or, at the latest, for 6 months after the end of the process concerned.
Compliance with the applicable legal framework	For the duration of the limitation period of the obligations that we are subject to. Without prejudice to different terms, 7 years – Business and Companies Act
Site access and security management, including video surveillance if you are interviewing on our premises	Video surveillance images will be stored for maximum of 30 days from the date of recording. However, Dedalus reserves the right, in any case, to retain your personal information also for the time strictly necessary to fulfil the regulatory obligations to which the Responsible Party is subject as well as to meet any defensive needs or requests by the Judicial Authorities and/or Law Enforcement Agencies
Management and follow-up of potential disputes	For the duration of the dispute and until all potential remedies have been exhausted
Processing your request to receive our job alerts	Until your consent is withdrawn

We have also defined an archiving policy. This ensures that your personal information is not stored in the active database unnecessarily.

In any case, once the applicable storage period has elapsed, we will irrevocably erase or anonymize your personal information so that you can no longer be identified.

In accordance with the applicable data protection legal framework, particularly POPI and PAIA, you have the following rights as a data subject:

- a) to be notified that personal information about you is being collected as provided for in terms of section 18 POPI; or your personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22 POPI;
- b) to establish whether a responsible party holds personal information of that data subject and to request access to your personal information as provided for in terms of section 23 POPI;
- c) to request, where necessary, the correction, destruction or deletion of your personal information as provided for in terms of section 24 POPI;
- d) to object, on reasonable grounds relating to your particular situation to the processing of your personal information as provided for in terms of section 11(3)(a) POPI;
- e) to object to the processing of your personal information at any time for purposes of direct marketing in terms of section 11(3)(b) POPI; or in terms of section 69(3)(c) POPI;
- f) not to have your personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1) POPI;
- g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of your personal information intended to provide a profile of such person as provided for in terms of section 71 POPI;
- h) to submit a complaint to the Regulator (<https://www.justice.gov.za/infoereg/index.html>; Email address: infoereg@justice.gov.za) regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74 POPI; and
- i) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99 POPI.

However, please note that some of the above rights are subject to specific conditions dictated by the applicable data protection legal framework. So, in the event that your specific situation does not meet these conditions, we will unfortunately be unable to comply with your request.

Our company also has a right to privacy in the same you do, so the protections afforded to you, apply to us *also*. In the course of carrying on its business, Dedalus has expressly authorised the use of video surveillance cameras to secure its physical property. If you do not agree to this video surveillance, do not enter Dedalus property. If you do enter, you consent to this limitation of your right to privacy and the use of video surveillance by Dedalus

To exercise your rights, please contact our information officer using the contact details provided in Section 7 (*How can you contact us?*). To process your request as efficiently as possible, we may ask you for certain additional information to confirm your identity and/or assist in locating the personal information that forms the subject matter of your request.

7

HOW CAN YOU CONTACT US?

If you have any questions or requests regarding our processing operations with your personal information under this policy, including exercising your rights, as outlined above, you may contact us on the following address: rania.kandil@dedalus.com

We also have appointed an information officer ("IO"), which you can contact by e-mail at the following address: dpo.group@dedalus.eu

Current version: [Dedalus – job applicant privacy policy – v. 2]

Last updated: March 2025