

PRIVACY NOTICE & POLICY

⊕ PRIVACY NOTICE

Deon Ferrier and Associates (Pty)Ltd, hereinafter DFA Solutions, is an ICT solutions company, with a core focus on ICT Security and Managed Services.

Our address and contact details for the purpose of this notice

Physical Address: Suite 7, Burlington Arcade, Cnr Main, Park & Lester Road, Wynberg, Western Cape
Email address: popia@dfasolutions.co.za
Telephone no.: +27 21 761 0532

DFA Solutions needs to gather and use certain information about data subjects. As a company we endeavour to fully comply with the provisions of the Protection of Personal Information Act (POPIA) Act No. 4 of 2013, hereinafter referred to as PoPIA. These can include the personal information of our clients, suppliers, business contacts, employees and other people the company has relationships with.

The PoPIA regulates all companies and entities that process personal information and DFA Solutions regard the protection of personal information as a very important right. Our aim is to ensure that all personal information kept by the company is effectively safeguarded and solely used for the purpose for which it was collected.

The purpose of this privacy notice is to inform you about our privacy policy and our use of the personal information we collect from you when you submit your data to us, use our website or subscribe to our services.

⊕ POLICY

Our Privacy Policy outlines how DFA Solutions manages personal information which it processes for various business requirements and specifically in the rendering of effective services.

TABLE OF CONTENTS

1. DEFINITIONS.....	3
2. PURPOSE	4
3. SCOPE	4
4. DATA COLLECTED, CATEGORIES AND CLASSIFICATION.....	5
5. DATA USAGE.....	7
6. RESPONSIBILITIES	8
7. GENERAL EMPLOYEE GUIDELINES.....	9
8. COLLECTING OF PERSONAL INFORMATION.....	9
9. RETENTION OF PERSONAL INFORMATION	10
10. UTILISATION OF PERSONAL INFORMATION	10
11. THIRD PARTY RESPONSIBILITY	11
12. SAFEGUARDING OF PERSONAL INFORMATION.....	11
13. RIGHT TO ACCESS PERSONAL INFORMATION	12
14. RETENTION OF PERSONAL INFORMATION	12
15. BREACHES OF THE ACT OR POLICY	13
16. MAINTENANCE AND UPDATING OF THIS PRIVACY POLICY.....	13
17. WEBSITE PRIVACY.....	14
18. DATA SUBJECT REQUEST AND COMPLAINTS.....	17

1. DEFINITIONS

For the purpose of this section, this notice and policy subscribes to the definitions as provided for in the Protection of Personal Information Act 4 of 2013, hereinafter referred to as PoPIA. Should there be conflict or substantive difference between definitions, then the definition in PoPIA will prevail and apply, unless this policy explicitly states otherwise.

Data privacy advisor	For the purpose of this policy, a data privacy advisor is any person (<i>internal or external</i>) appointed by the Information Officer to act in advisory capacity in terms of the company's data privacy requirements.
Data subject	Means the identifiable natural/juristic person to whom personal information relates.
Deputy Information Officer.	Means an employee of the company duly appointed by the Information Officer to perform the function of the Deputy Information Officer.
Information assets	<p>Means the assets the company uses to create, store, transmit, or process information to support its business activities as well as the information systems with which that information is processed.</p> <p>It includes:</p> <ul style="list-style-type: none"> • All electronic 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 content. • All applications, devices and other systems with which the organisation processes its information, for example telephones, fax machines, printers, computers, networks, 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 ('ICT') assets.
Information end-user	Means the person that interacts with information assets and ICT assets for the purpose of performing an authorised task.
Information officer	Means a senior employee of the company duly appointed by the company as the Information Officer, failing which the person defined by the Act or relevant Regulations.

Information owner	Means the person responsible for, or dependent upon the business process associated with an information asset.
Personal information	Means information, as defined in the Act, 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, marital status, nationality, age, physical or mental health, disability, belief, culture, language and birth of the person; education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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

2. PURPOSE

This privacy policy ensures that the company:

- (i) Complies with the Protection of Personal Information Act, 2013 (Act 4 of 2013).
- (ii) Protects the rights of data subjects.
- (iii) Is transparent in how it processes personal information.
- (iv) Protects itself from the risks of security breaches.

3. SCOPE

This policy applies to all employees, agents, consultants and any other person or entity executing services on behalf of DFA Solutions. It governs all related activities that involve the processing of personal information for or on behalf of the company.

4. DATA COLLECTED, CATEGORIES AND CLASSIFICATION

The information collected, processed and held by the company has been divided into different categories grouped into various subjects, each of which describes a sub set of data information collected and held. The categories of information are not exhaustive, but are merely meant to give an indication of the information held by DFA Solutions, without specification. A category may therefore contain sub-categories and sub-sets of information, which are not specifically listed.

(i) Companies Act Records

- Documents of incorporation
- Memorandum and Articles of Association
- Minutes of Board of Directors meetings
- Records relating to the appointment of directors/ auditor/ secretary/ public officer and other officers
- Share Register and other statutory registers

(ii) Financial Records

- Annual Financial Statements
- Tax Returns
- Accounting Records
- Banking Records
- Bank Statements
- Paid Cheques - Not Applicable – All payments are done via EFT
- Electronic banking records
- Asset Register
- Rental Agreements
- Invoices
- Customer Details-Vat Numbers-delivery addresses-email addresses-client company details

(iii) Income Tax Records

- PAYE Records
- Documents issued to employees for income tax purposes
- Records of payments made to SARS on behalf of employees
- All other statutory compliance records:
- VAT
- Regional Services Levies
- Skills Development Levies
- UIF
- COID

(iv) Personnel Records

- Employment contracts
- Employment Equity Plan
- Disciplinary records
- Salary records
- SETA records
- Disciplinary code
- Leave records
- Training records
- Training Manuals - All online
- Employee Identity Numbers
- Employee addresses
- Employee names
- Staff administration (employee records and information)
- Staff includes potential and existing staff

(v) Client/Debtor Data

- Client company/trading details-vat numbers, company registration details etc.
- Customer contracts and customer details
- Details regarding the rendering of services according to instructions given by clients
- Keeping of accounts and records
- Complying with tax laws
- Clients include potential and existing clients.

(vi) Vendor/Creditor/Consultant/Sub-Contractor/Agent or other 3rd Party Data

- Client company/trading details-vat numbers, company registration details etc.
- Client and 3rd party professional qualifications and professional body registration details
- Supplier contracts and supplier contact details
- Customer contracts and customer details
- Details regarding the rendering of services according to instructions given by clients
- Keeping of accounts and records
- Complying with tax laws
- Clients include potential and existing clients.

5. Data Usage

DFA Solutions will not intentionally share your information with any other third party or use your data for any purpose other than described herein.

We use the information we collect for the following purposes:

- Accounting process requirements.
- Human Resources management and related employee requirements.
- Physical safeguarding of information assets within the company.
- To identify and authenticate you so you may securely use our Services;
- To provide you with our Services;
- To improve and customize your experience with our Services, such as delivering content and responses tailored to you and the way you interact with our Services;
- To link your Account to connected third-party devices, apps, features, or services when you request this;
- To respond to your requests, inquiries and instructions made through or about our Services;
- With your separate consent, to deliver advertising, including customized advertisements, sponsored content and promotional communications;
- To allow you to interact with and use third-party applications and services;
- To operate, evaluate and improve our Services and our business (including developing new products and services; enhancing and improving our products and services; managing our communications; analysing our products, services and customer base; conducting market research; performing data analytics; and performing accounting, auditing and other internal functions);
- To protect against, identify and prevent fraud and other criminal activity, claims and other liabilities; and
- To comply with and enforce applicable legal requirements, relevant industry standards and our policies, including this Privacy Notice, related policies and procedures.

We may use and combine the information we collect about you with data from other services or features you use, your devices and other sources such as applications, as well as information about your online activities on websites and connected devices over time and across third-party websites, devices, applications and other online features and services for the purposes above.

We may further use the data collected for communication with customers, dealing with enquiries from our sales department and to advise customers of special offers, product updates and discounts. If you have consented to receive marketing communications from us, we may combine information we collect about you from the services with data from other services or features, including to provide you with customised notices or advertisements. All marketing mediums will have an “opt-out” function should you elect to not receive any further notices or marketing communications from us in future. Where a marketing medium excludes an “opt-out” function, please inform us through the procedure provided herein if you wish to not receive any further notices or marketing communications from us in future.

Consent - We require your consent to obtain and use the data. In certain circumstances we might have obtained your information prior to the commencement of data privacy laws. Please note that you may withdraw your consent at any time through the procedure provided herein.

We only maintain your data on our records for as long as we have your consent to do so and as permitted or required by law. Where you elect to withdraw consent or amend your information, we will amend or delete such information on your instruction to do so and within the period required by law in each circumstance and

In general, your information will not will be processed abroad, however certain services may require processing of your data abroad. In these circumstances, we will endeavour to alert you as soon as reasonably possible.

Complaint - You have a right to complain about our use of your information if you think your rights have been infringed by an institution processing your personal information. Please see the section herein addressing complaint procedures.

6. RESPONSIBILITIES

All DFA Solutions employees, agents and consultants have a responsibility to ensure that the personal information of data subjects is collected, stored and processed appropriately to ensure the confidentiality, integrity and the availability thereof.

Each Information End User and Information Owner that handles personal information must ensure that it is handled and processed in line with this policy and the provisions of the PoPIA.

7. GENERAL EMPLOYEE GUIDELINES

- (i) The only people able to access any personal information covered by this policy should be those who need it to successfully complete their duties.
- (ii) Personal information should not be shared informally and must never be shared over social media platforms, including messaging groups such as WhatsApp or similar.
- (iii) Where an employee does not normally have access to specific confidential information, but requires access for the execution of an official duty, such access must be requested from a senior person with authority to provide the requested access.
- (iv) The company will provide training to its employees in order to facilitate the understanding of their responsibilities when handling personal information.
- (v) Employees should keep all personal information secure, by taking sensible precautions and following the guidelines provided herein or from time-to-time.
- (vi) The company must ensure and enforce the use of strong password complexity and any other means of security, such as encryption, Two factor authentication, and so forth.
- (vii) Personal information should not be disclosed to unauthorised individuals, either within the company or to any other external party.
- (viii) Personal information must be reviewed regularly and updated if it is found to be out dated. If no longer required, it should be deleted and disposed of in line with the disposal instructions.
- (ix) Employees should request assistance from the Deputy Information Officer or other senior personnel if they are unsure about any aspect of the protection of personal information.

8. COLLECTING OF PERSONAL INFORMATION

The company only collects information to support its internal business functions and to provide a service to its clients. Personal information is collected directly from data subjects where practical and should be in compliance with PoPIA.

Personal information may be collected through a variety of channels and may include the following:

- Application forms and direct requests;
- Contracts;
- Seminars, Webinars, and similar gatherings;
- Email distribution lists;
- Websites;
- Through surveillance cameras (with facial recognition technology);
- Through third party service providers;
- Social media platforms;
- Responding to questionnaires and surveys;

It is acknowledged that through the services rendered by the company personal information may be collected as an unintentional auxiliary process that is part of the specific service being rendered to the client. In the latter, such personal information will be afforded the same protection under this policy and in strict compliance with the requirements of PoPIA.

9. RETENTION OF PERSONAL INFORMATION

The company may collect and process personal information for the following reasons:

- (i) As requires by law, *example as submissions to SARS under relevant tax laws*;
- (ii) Employment and remuneration and other Human Resources needs;
- (iii) Processing employee benefits;
- (iv) Closing agreements and contracts with clients or vendors;
- (v) Communication; sending and sharing of important information;
- (vi) Register services;
- (vii) Provision of contracted services to clients;
- (viii) Responding to requests or complaints;
- (ix) Consultations;
- (x) Determining and addressing a client's needs;
- (xi) Security background checks (vetting);
- (xii) Rendering accounts, Debt recovery;
- (xiii) Non-disclosure;

It is accepted that this is not an exhaustive list and may be updated from time-to-time to accommodate changes in the business environment that DFA Solutions operates in.

10. UTILISATION OF PERSONAL INFORMATION

DFA Solutions will only use personal information for the intended purposes it was collected for unless the data subject grants consent for additional uses.

As a principle, the company shall only share personal information if it obtained consent from the data subject to share such information. Personal information may be shared with the stakeholders and in the manner as follows:

- (i) South African Revenue Service
- (ii) Medical aids and pension funds
- (iii) Financial institutions, such as banks, for payment and remuneration purposes
- (iv) Business partners, vendors, contractors, or consultants to provide contracted services to clients or to facilitate services;
- (v) In response to a request for information by a legitimate authority in accordance with, or required by any applicable law, regulation, or legal process, or to comply with judicial proceedings;
- (vi) To protect the rights, property, or safety of the company or others; and
- (vii) Where consent in writing has been contained from the data subject for sharing

11. THIRD PARTY RESPONSIBILITY

Any service providers rendering a service on behalf of DFA Solutions are required and expected to implement suitable information protection and security measures aligned with the provisions and requirements of PoPIA. Third parties are not permitted to use personal information for any purpose, other than it was intended for.

12. SAFEGUARDING OF PERSONAL INFORMATION

The company is committed to protect personal information from misuse, loss, theft, unauthorized access, modification, or disclosure. It should be acknowledged that no company can fully secure its systems, but DFA Solutions protects personal information by applying best-practice standards and using various methods, processes and technologies, amongst others:

- Strict access control processes;
- Contractually holding third parties liable to whom personal information is disclosed and requiring them to comply with the provisions of PoPIA;
- Firewalls, Demilitarised Zones (DMZ) and Virtual Private Networks (VPN) tunnels.
- Data encryption and two-factor authentication
- Continuous pro-active security monitoring of all systems and services;
- Physical security controls;
- Continuous patch management;

13. RIGHT TO ACCESS PERSONAL INFORMATION

- (i) A data subject has the right to request the company to disclose, correct, update, block, or delete personal information that it holds.
- (ii) The right in 13(i) is not absolute and may be subject to various factors allowed by law, *such as a legal duty on the company to retain personal information.*
- (iii) The Information Officer will assess the request received from the data subject and ensure that the request is handled in compliance with PoPIA provisions. The Information Officer will acknowledge receipt of any such request within three (3) days of the date of submission.
- (iv) The Information Officer shall respond within forty-eight (48) business hours from the time the request is received, noted that the time is calculated within the business hours of the company. *As an example, if a request is received at 18h00, the forty-eight hour (48hr) response period will be calculated from 08h00 the following business day. If a request is received at 06h00, the forty-eight hour (48hr) response period will be calculated from 08h00 the same business day.* For the purpose of clarity, the company's business hours for the purpose of this policy only, is Monday to Friday, from 8am to 5pm and excluding South African public holidays.
- (v) Where the company processes legally obtained personal information, the data subject may withdraw consent at any time for future processing;
- (vi) The data subject may object to the processing of personal data at any time.
- (vii) On any suspicion that personal information has been unlawfully processed and rights relating to protection of your personal information were violated or that personal information has been compromised, the data subject shall contact the company's listed officer dealing with such requests and if not satisfied with the response, may lodge a complaint with the company's Accounting Officer, alternatively the Information Regulator.
- (viii) In the event of an information breach that the company becomes aware of, the company shall notify the data subject through best effort options, which may include a general public notice where the company does not have the means to directly inform the data subject.

14. RETENTION OF PERSONAL INFORMATION

- a) The company shall retain personal information for as long as it is necessary to fulfil the purposes for which it was collected and to comply with any legislative and or archive requirements where after it shall be deleted/disposed of.
- b) Retention periods may vary depending on the purpose and herein the following criteria will determine retention periods:
 - (i) Legal or contractual, or other obligations to retain personal data;
 - (ii) Data necessary for or as part of an investigation or for litigation purposes; and;
 - (iii) to maintain accurate records management aligned with relevant legislation.

15. BREACHES OF THE ACT OR POLICY

- (i) Breach of this policy or the PoPIA by any employee of the company may lead to disciplinary action instituted against such an employee. Where an employee is found guilty in a disciplinary action taken herein, the employee may be dismissed for a first offence and any costs as a result of the employee's misconduct may be recovered by the company. Disciplinary actions and sanctions herein, must comply with the relevant legislation.
- (ii) Breach of this policy or the PoPIA by an agent, consultant or any entity performing a service on behalf of the company will be regarded as a breach of contract. Where such a breach is not stipulated in the terms of a contract between the company and the party, the provisions herein prevails. The company may immediately and unilaterally cancel the contract without any liability to the company. The company may take any legal actions necessary to recover damages suffered, including reputational damage, from the party in breach of this policy or the PoPIA.

16. MAINTENANCE AND UPDATING OF THIS PRIVACY POLICY

DFA Solutions will maintain and update this Privacy Notice and Privacy Policy and shall publish, on its website, the updated/revised version as and when necessary. The company may also inform data subjects through email and other communications channels about such publications.

It is the responsibility of the data subject to review such notices and publications and determine which action it requires to take based on the revisions/updates made by the company.

17. WEBSITE PRIVACY

By using DFA Solution's website or websites, the data subject (user) is deemed to have accepted the terms and conditions as specified on the website.

The user is able to access other third party sites via links or displayed frames from the company's website. These third party sites are not monitored, maintained or controlled by DFA Solutions and we are not responsible in any way for their content or compliance with privacy laws. The use of such sites and applications is thus subject to the relevant third party's privacy policy statements.

DFA Solutions respects any user's online privacy. Some anonymous information about the user is automatically collected by our website. This information may include: the user's browser type, access times, referring web site addresses and viewed pages/content. This information is collected to generate general aggregate statistics about the use of the company's website and is used to improve our services and your experience with our online platforms.

Our websites also use "cookies". A cookie is a text file that is placed on the user's hard disk by a webserver. Cookies cannot be used to run software, applications, services or deliver viruses or malware to the user's computer. Cookies are uniquely assigned to the user and can only be read by a webserver in the domain that issued the cookie to the user. The user may from time to time be requested to accept or decline cookies. Most web browsers automatically accept cookies, but the user can usually modify the browser settings to decline cookies if the user prefers. If a user chooses to decline cookies, certain automated user experiences may be lost. For example, if a user previously indicated a language preference, when the user returns to the website the default language will apply and not the language the user previously preferred.

DFA Solutions do not intentionally share any user details that may have been obtained, automatically or without the user's knowledge, unless if the user gave consent to share collected information. The company may share anonymous aggregate statistics about users and traffic patterns, but such information will not identify the user or will be declassified.

(a) Use of Cookies

We use the following cookies to give effect to certain user functions, preferences and overall user experiences.

Cookie Name/ID	Domain	Type	Description	Duration
_ga	.dfasolutions.co.za	Analytics	This cookie is installed by Google Analytics. The cookie is used to calculate visitor, session, campaign data and keep track of site usage for the site's analytics report. The cookies store information anonymously and assign a randomly generated number to identify unique visitors.	2 years
_gid	.dfasolutions.co.za	Analytics	This cookie is installed by Google Analytics. The cookie is used to store information of how visitors use a website and helps in creating an analytics report of how the website is doing. The data collected including the number visitors, the source where they have come from, and the pages visited in an anonymous form.	1 day
_gat_gtag_UA_180563844_1	.dfasolutions.co.za	Analytics	This cookie is set by Google and is used to distinguish users.	1 minute
Uvc	.addthis.com	Analytics	The cookie is set by addthis.com to determine the usage of Addthis.com service.	1 year 1 month
__atuvc	dfasolutions.co.za	Functional	This cookie is set by Addthis to make sure you see the updated count if you share a page and return to it before our share count cache is updated.	1 year 1 month
__atuvs	dfasolutions.co.za	Functional	This cookie is set by Addthis to make sure you see the updated count if you share a page and return to it before our share count cache is updated.	30 minutes
PHPSESSID	dfasolutions.co.za	Necessary	This cookie is native to PHP applications. The cookie is used to store and identify a users' unique session ID for the purpose of managing user session on the website. The cookie is a session cookies and is deleted when all the browser windows are closed.	session

(b) Data Collected

We collect the following data through our website:

- Name;
- E-mail;
- City;
- Message;
- Information as described in the cookies in the table at section 17(a)

(c) Data Usage

The aforementioned information collected is utilised by us in order to respond to your enquiries made through our website.

We also use your details to inform you of urgent ICT security notices, or to send you information regarding our services. Whenever your information is used in the latter sense, you as the data subject will have an automatic option to “opt-out”. Where the communication tool does not allow for an automated “opt-out” process, you as the data subject will be notified within the communication of the options available to “opt-out” of such communications.

We will not share your information with any other third party or use your data for any purpose other than described above and such collected information will not be used to make any automated decisions about you.

A users’ information will also be used for correspondence, notices, advertisements, surveys, offers or newsletters to you concerning our services and products. The user will at all times have the option to “opt-out” of such communications.

18. DATA SUBJECT REQUEST AND COMPLAINTS

For the purpose of good governance, the company has elected to address any requests or complaints received in relation to the PoPIA in the following overarching manner:

1. The data subject submits request/complaint to the dedicated official (DPO).
2. The DPO handles the request in terms of the company's data privacy policy, PoPIA and any other relevant legislation.
3. Should the data subject not be satisfied with the response of the DPO, the data subject may escalate such dissatisfaction to the Information Officer. The Information Officer will review the matter and provide feedback to the data subject.
4. Should the data subject still not be satisfied with the outcome/response from the Information Officer, the data subject may lodge a complaint with the Information Regulator.

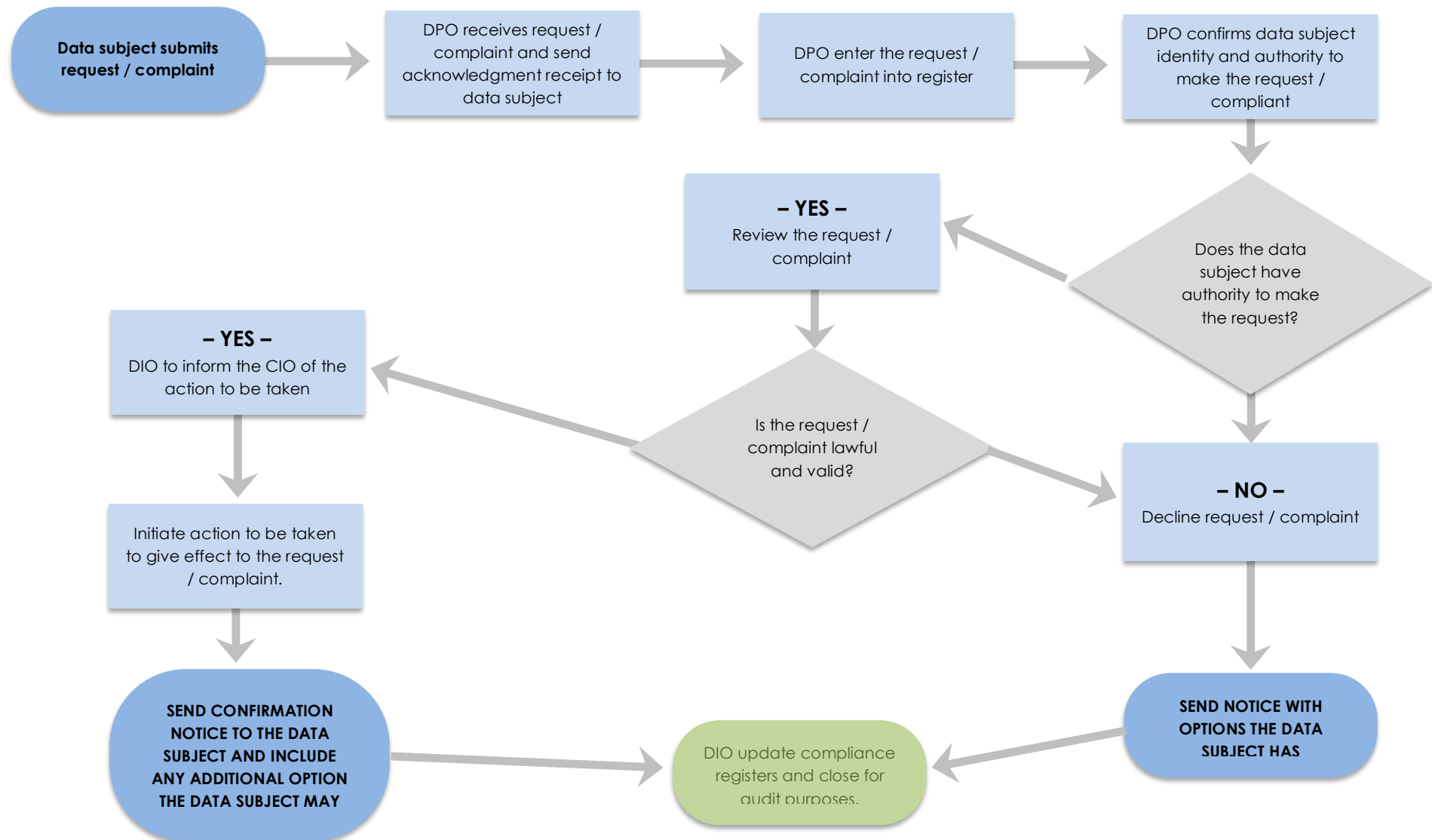
The process flow for submitting requests or complaints are annexed hereinafter. Notwithstanding the proposed steps herein, nothing prohibits the data subject from directly approaching the Information Regulator. The company do however encourage data subjects to first exhaust the internal processes which it endeavours to resolve amicably and responsibly within the framework of the law.

For the purpose of this section the information of the relevant persons is as follow:

1. **Deputy Information Officer: Mr Rodney Daniëls**
Information Officer: Mr Deon Ferrier
Email: popia@dfasolutions.co.za
Telephone: +27 21 761 0532
Website: <https://dfasolutions.co.za>
Street Address: Suite 7, Burlington Arcade, Cnr Main, Park & Lester Road Wynberg, Western Cape
2. **Information Regulator of South Africa (Complaints)**
Email: complaints.IR@justice.gov.za
Website: <https://www.justice.gov.za/infoereg/index.html>
Street Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

Document version	5
Effective date	1 July 2021

ANNEXURE 1 : POPIA REQUEST / COMPLAINT PROCESS



ANNEXURE 2: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Deputy Information Officer or Information Officer of DFA Solutions:

Name	
Contact Number	
Email Address:	

Please Note that DFA Solutions requires proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested and you will be informed accordingly of such reasonable costs

A. Particulars of Data Subject	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Request	
I request DFA Solutions to:	
(a) Inform me whether it holds any of my personal information	<input type="checkbox"/>
(b) Provide me with a record or description of my personal information	<input type="checkbox"/>
(c) Correct or update my personal information	<input type="checkbox"/>
(d) Destroy or delete a record of my personal information	<input type="checkbox"/>
C. Instructions	
<Please insert/attach an additional page if the space provided is not sufficient>	
D. Signature Page	
Signature	
Date	

ANNEXURE 3: PoPIA COMPLAINTS FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please Note that DFA Solutions will require proof of identification prior to processing your request.

Please submit the completed form to the Deputy Information Officer or Information Officer of DFA Solutions:	
Name	
Contact Number	
Email Address:	

We encourage data subjects to use our internal process, as explained in section 18 of the Privacy policy, to resolve complaints, however if you are not satisfied with the outcome and do not wish to follow our internal process, you have the right to lodge your complaint with the Information Regulator. The details of the Information Regulator for the purpose of lodging complaints are provided under section 18 of this policy.

A. Particulars of Complainant	
Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	
B. Details of Complaint	
<Please insert/attach an additional page if the space provided is not sufficient>	
C. Desired Outcome	
<Please insert/attach an additional page if the space provided is not sufficient>	
D. Signature Page	
Signature:	
Date	