

TITANDC

Privacy Policy

How TitanDC collects, uses, shares and protects personal information, in terms of the Protection of Personal Information Act, 4 of 2013

Version 3.0 · Approved 9 September 2026

1. Who we are

Titan Development Consultants (Pty) Ltd, trading as TitanDC ("TitanDC", "we", "us"), registration number 1999/021465/07, is an authorised financial services provider, FSP number 8972. We are the "responsible party" for the personal information we process in the course of providing insurance and financial advice, intermediary services and related administration.

	Detail
Information Officer	Johan Geldenhuys, Managing Director (registered with the Information Regulator)
Deputy Information Officer	Dean Geldenhuys, Director
Address	3 Tyger Lake, Office 518, Fifth Floor, 2 Niagara Road, Tygervally, Cape Town, 7530
Telephone	021 200 4000
Email	reception@titandc.co.za (subject line: Privacy request)

2. Our commitment

We process personal information lawfully, for a specific purpose, and only to the extent needed for that purpose. We are open about what we do with it, keep it accurate and secure, allow you to exercise your rights over it, and keep it no longer than necessary. These are the eight conditions for lawful processing in the Act, and this policy explains how we meet each of them.

3. Who this policy applies to

This policy applies to clients and prospective clients, the people insured or nominated under a client's policies (such as dependants, beneficiaries and drivers), trustees and members of community schemes we serve, suppliers, business partners, website visitors and job applicants. Where a client gives us personal information about another person, the client confirms that they are entitled to do so and that the person has been told about this policy.

4. The information we collect

- **Identity and contact details:** name, identity or passport number, date of birth, addresses, telephone numbers, email address, and details of dependants or beneficiaries.
- **Financial details:** income, bank account details for premium collection and claim payments, credit information where a product requires it, tax number, and details of assets, vehicles and property to be insured.
- **Policy and claims information:** existing and previous cover, claims history, loss details, quotes, proposals, records of advice, and correspondence.

- **Special personal information:** health information for life, disability, medical scheme and gap cover applications and claims; and, where an insurer requires it for underwriting or claims, information about criminal convictions or alleged offences. We process special personal information only with your consent, or where the law or the establishment of a right or obligation requires it, and only for the purpose for which it was given.
- **Children's information:** details of minor dependants or beneficiaries, processed with the consent of a parent or guardian and only for the purpose of the relevant cover.
- **Website and technical information:** when you submit the enquiry form on our website, the details you enter are sent to our form provider. The website does not set advertising cookies or run analytics trackers. Hosting and security services may record technical information such as IP addresses to protect the site.

5. Where we get it

Most of the information we hold comes directly from you. We also receive information from insurers, medical schemes and other product suppliers about the cover you hold; from other financial services providers when you move your business to us with your consent; from credit bureaus, identity verification services and public registers where the law or a product supplier requires verification; and from assessors, repairers, medical practitioners and other parties involved in a claim.

6. Why we process it and on what basis

Purpose	Lawful basis
Giving you advice and arranging, administering and renewing your cover	Performance of a contract with you, and steps you ask us to take before entering into one
Submitting and managing claims on your behalf	Performance of a contract; your consent for health and other special information
Verifying your identity and screening for financial crime	Legal obligations under the Financial Intelligence Centre Act and related law
Keeping records of advice and transactions	Legal obligations under FAIS and insurance legislation
Responding to enquiries, complaints and access requests	Legitimate interests and legal obligations
Sending you information about products and services that may interest you	Your consent, or an existing client relationship, which you may withdraw or object to at any time
Protecting our systems, preventing fraud and defending legal claims	Legitimate interests

7. Who we share it with

We share personal information only where it is necessary for the purposes above, and only with parties who are bound to protect it:

- insurers, underwriting managers, medical schemes, gap cover providers, investment and life assurance product suppliers, and their claims assessors, loss adjusters and service providers, to quote, underwrite, administer and pay claims on your cover;
- Titan Direct (Pty) Ltd (registration number 2002/024096/07, FSP 48217), an associated company, where it administers your policy under a binder or administration agreement with your insurer;
- our outsourced compliance officers, auditors, accountants and legal advisers;

- our IT and hosting providers, who store data on our behalf in secured cloud services with multi-factor authentication and off-site backup;
- our website form provider, which receives the details you enter into the enquiry form and stores them for us;
- credit bureaus, identity verification and sanctions screening services, where the law requires;
- the Financial Sector Conduct Authority, the Information Regulator, the FAIS Ombud, the National Financial Ombud Scheme, the Financial Intelligence Centre, SARS, courts and law enforcement, where the law requires or allows.

We do not sell personal information, and we do not share it with third parties for their own marketing.

8. Transfers outside South Africa

Some of our service providers, including cloud hosting and our website form provider, may store or process information on servers outside South Africa. We only permit this where the recipient is subject to a law, binding corporate rules or a contract that provides substantially similar protection to the Act, or where you have consented, as section 72 of the Act requires.

9. Keeping your information accurate

We take reasonable steps to keep personal information complete, accurate, up to date and not misleading. We confirm your details when we give advice, at every renewal and when you make a claim. You are responsible for telling us promptly when your details change, including your contact details, the people insured under your policies, the use of your vehicles and property, and anything that affects your cover. Inaccurate information can affect the validity of a policy or the outcome of a claim.

10. How we protect it

We apply appropriate technical and organisational safeguards: access to client information is limited to staff who need it for their role; our systems require individual logins and multi-factor authentication; data is stored in secured cloud services with off-site backups; paper records are kept in a locked office and disposed of securely; and staff receive training on this policy and on the Act at induction and at least annually. Our IT provider confirms these controls in writing for our compliance reviews. If we become aware of a security compromise affecting your personal information, we will notify the Information Regulator and you as soon as reasonably possible, as section 22 of the Act requires.

11. How long we keep it

We keep records of advice, transactions and client communications for at least five years after the end of the relationship or the last transaction, as FAIS requires, and identity verification records for at least five years as the Financial Intelligence Centre Act requires. Claims records are kept for as long as a claim or a related legal claim could arise. Once the applicable period has passed, records are deleted or destroyed in terms of our Document Retention Policy, unless we are required by law to keep them longer or you have consented to a longer period.

12. Direct marketing

We may tell existing clients about products and services similar to those they already hold. We only send electronic marketing to other people with their consent, which we request once. Every marketing message tells you how to opt out, and you can opt out at any time by contacting us.

13. Your rights

Under the Act you may ask us whether we hold personal information about you and request a copy of it; ask us to correct or delete information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; object to processing that is based on legitimate interests or for direct marketing; withdraw consent where processing is based on consent; and complain to the Information Regulator. Requests for access to records are handled under our PAIA Manual, which is available on our website.

14. How to make a request

Send your request to the Information Officer at the contact details in section 1, marked "Privacy request", and tell us which right you are exercising and what information it concerns. To protect your information, we will verify your identity before acting. We use the forms prescribed by the Information Regulator: Form 1 for objections to processing and Form 2 for correction or deletion; both are available from us and from the Regulator's website.

Step	What happens	When
1	We acknowledge your request in writing and confirm the identity documents we need.	Within 2 working days
2	We confirm what information we hold and, if applicable, the fee for copies as prescribed under PAIA.	Within 10 working days
3	We respond to the request, or explain why we cannot comply and how to escalate.	Within 30 days of a complete request, extendable once by 30 days with notice

Staff who receive a request from a data subject must pass it to the Information Officer on the same day; no personal information may be released or changed on request until the Information Officer has verified the requester and authorised the response.

15. Complaints

If you are not satisfied with how we have handled your personal information or a request, please contact the Information Officer first so that we can put it right. You also have the right to complain to the Information Regulator:

	Information Regulator (South Africa)
Address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal address	P O Box 31533, Braamfontein, Johannesburg, 2017
Telephone	010 023 5200
Email	enquiries@inforegulator.org.za
POPIA complaints	POPIAComplaints@inforegulator.org.za
Website	www.inforegulator.org.za

16. Changes to this policy

We review this policy at least annually and whenever the law or our processing changes. The current version is always available on our website and at our offices. Material changes are communicated to clients.

Version control

Date	Version	Change	Approved by
September 2026	3.0	Current version, replacing Privacy Policy Statement v2.3.	Johan Geldenhuys, Managing Director, on the recommendation of Masthead (compliance officers), 9 September 2026