root

Privacy Policy

Last updated: 6 November 2026

At Root, we're committed to protecting the privacy of your personal data.

This privacy policy (**Privacy Policy**) is meant to help you understand what data we collect, why we collect it and how you can update, manage, export and delete your data.

> **Personal data** is information that relates to you and may identify you as an individual. This includes your name, contact information, age and gender and certain special categories of data like race, ethnic origin, health information or criminal record.
>
> If you are in South Africa, personal data also applies to information that may be used to identify a juristic person, like a registered company.

We process personal data in line with all applicable laws, including:

- The European Union's General Data Protection Regulation (**GDPR**);
- The UK's GDPR (**UK GDPR**);
- The UK Data Protection Act (**UK Data Protection Act**); and
- South Africa's Protection of Personal Information Act (**POPIA**).

To help you navigate this Privacy Policy:

Section 1 - Who we are and what we do
Section 2 - The personal data we process and how we use it
Section 3 - Who we share personal data with
Section 4 - Data retention, export and deletion
Section 5 - How we protect your data
Section 6 - How we use cookies
Section 7 - Your rights
Section 8 - Contacting us
Section 9 - Contacting the authorities

We update this Privacy Policy occasionally. When we make major updates, we will place a prominent notice visible to site visitors and notify you where possible, however you should always check back here periodically to see if the Privacy Policy has been updated. We will always show the date of the last update at the top of the page for you to know when it was last changed.

We regularly review our compliance with this Privacy Policy. If you have any questions, please contact us by email at privacy@rootplatform.com.

root

1. WHO WE ARE AND WHAT WE DO

a. Who we are:

This Privacy Policy applies to Root Platform Inc., a Delaware, USA corporation and its subsidiaries and affiliates (collectively, **Root** or **we**, **us**, **our**). We operate in various countries around the world, including the United Kingdom and South Africa.

b. What we do:

We believe that the future of insurance is digital, personalised and embedded. Our mission is to grow insurance businesses into this future by providing the infrastructure that makes this possible.

We do this by providing our clients with access to an end-to-end digital insurance platform that enables them to launch, sell and administer insurance products and digital engagement channels fast (the **Root Insurance Platform**).

For more information about our services, see here.

2. THE PERSONAL DATA WE PROCESS AND HOW WE USE IT

Sections of this Privacy Policy may apply differently to you based on the way you interact with Root.

You are either a Site Visitor or a Client, User or End User:

Site Visitor: You are a Site Visitor when you visit and interact with our web sites, web pages, interactive features, blogs and their respective contents at rootplatform.com (or any derivation like root.co.za) (**Our Sites**).

Client: You are a Client when you enter into an agreement relating to you, your Users or your End Users using our services.

User: You are a User when you set up a Root Account and gain access to the Root Insurance Platform at app.rootplatform.com (or any other derivation), because your employer or organisation is a Client. Support and operational staff or other agents of our Clients who gain access to the Root Insurance Platform are Users.

End User: You are an End User if you use any applications built by or on behalf of a Client on the Root Insurance Platform. If you are a policyholder of a Client, you will be an End User.

For each user type we've explained what personal data we collect, why and how we process it:

<table>
<tr><td rowspan="4">Site Visitors</td><td>What personal data do we collect?</td></tr>
<tr><td>When you fill in forms on Our Sites (like our Contact page) or contact us by email or phone, or when you complete any website questionnaires or participate in discussion boards on social media or other platforms associated with Our Sites you directly provide us with:

• Your name and contact details (for example, your phone number or email address)
• Your company name, team and country</td></tr>
<tr><td>How do we use this personal data?</td></tr>
<tr><td>We process this personal data:

• To respond to your requests or questions
• To provide you with information about our company, our services and products, for marketing purposes

The legal basis for collecting and processing this information is your consent. You will be requested to consent when submitting this information in a form or otherwise.

You can withdraw your consent to processing by unsubscribing at any time by following the unsubscribe link at the bottom of the email you receive or contacting us at privacy@rootplatform.com.</td></tr>
<tr><td rowspan="4">Clients</td><td>What personal data do we collect?</td></tr>
<tr><td>When you sign up for Root's services for your organisation, Users and End users, you directly provide us with:

• Your company name and registration number
• Your representatives' names and contact details (phone number or email address)
• Financial information</td></tr>
<tr><td>How do we use this personal data?</td></tr>
<tr><td>We process this personal data:

• To communicate with you about your subscription, our relationship, this Privacy Policy, or our agreement with you</td></tr>
</table>

	• To perform our duties to you in terms of our agreement with you • To enable us to bill you for services • To enhance the safety and security of our Users and services • To perform necessary actions to maintain our services, like answering support queries, troubleshooting software bugs and resolving operational problems • To send communications about our services and products to you These activities are necessary to fulfil the terms of our agreements with Clients, are compatible with such uses or are necessary for Root's and our Clients' legitimate interests.
Users	**What personal data do we collect?**
	When you create and use a Root Account, you directly provide us with: • Your name • Your contact information (email & phone number) • Your login name and password • Chat logs (with support queries)
	How do we use this personal data?
	We process this personal data: • To create/update your individual Root Account • To send non-marketing communications to you • To enhance the safety and security of our Users and services • To perform necessary actions to maintain our services, like answering support queries, troubleshooting software bugs and resolving operational problems These activities are necessary to fulfil the terms of our agreements with Clients, are compatible with such uses or are necessary for Root's and our Clients and Users' legitimate interests in monitoring and improving our customer support services.
End Users	**What personal data do we collect?**
	Information about policyholders and other End Users is uploaded to our services by our Clients and their Users. Clients control what data is processed and the purpose and means of the processing, not Root. We obtain this data from Clients and their Users and process it based on the specific instructions of each Client in their capacity as controller / responsible party.

	This means the information we collect and process for our Clients and their Users as part of our services will vary depending on the insurance products and policies they issue or administer through our services, and how they use our services. Data can also be sourced by Clients from Third Party Services like payments providers or identity verification providers. Each insurance product has a potentially unique range of personal data that is sourced in order to issue and/or administer an insurance policy. This is likely to include: • Your name • Your contact details (email and phone number) • Address • Identity/passport number • Nationality • Age • Gender • Marital status and occupation • Payment information and bank account details* • Claims data • Complaints data *Please note that we use third-party providers to process payments and do not accept payments through our services.
	How do we use this personal data?
	We process the personal data: • To perform our duties to Clients in terms of our agreements with them • To perform necessary actions to maintain our services, like answering support queries, troubleshooting software bugs and resolving operational problems These activities are necessary to fulfil the terms of our agreements with Clients, are compatible with such uses or are necessary for Root's and our Clients and End Users' legitimate interests.

a. Withdrawing consent:

If you have provided your consent to the collection, processing and/or transfer of your personal data, you have the right to fully or partially withdraw your consent. This includes where you want to opt out of some or all marketing communications.

Once you have notified us that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you originally consented unless there is another valid legal ground for processing.

To stop receiving emails from us, click on the "unsubscribe" or "manage email preferences" link in the email you received from us to unsubscribe from some or all of the emails you receive. Alternatively, reach out to us at privacy@rootplatform.com.

3. WHO WE SHARE PERSONAL DATA WITH

Some of our services and features require that we share data with third parties, with our subsidiaries or affiliates, at our Clients' request or for legal reasons.

a. Third parties

These include the third parties or categories of third parties listed below.

- payment processors and facilitators
- identity verification providers
- cloud storage providers
- customer support and communications platform providers
- communications service providers
- customer relationship management platforms
- accountants, consultants, lawyers and other professional service providers
- insurance and financing partners
- marketing partners and marketing platform providers to reach or better understand our Clients and measure advertising effectiveness.

We will only share your personal data with these third party service providers to the extent necessary for them to perform their services for us. We only use service providers we trust, and who have agreed to keep your data secure and confidential and to only use it for the purpose for which we shared it with them. Some of our service providers may be located in other countries. We provide for appropriate safeguards through contracts between our foreign and local service providers and us, including through standard contractual clauses or other approved transfer mechanisms. Third party service providers are not owned or controlled by Root and third parties that have been granted access to information may have their own policies and practices for its collection, use and sharing.

b. Root subsidiaries or affiliates

We share data with our subsidiaries and affiliates to help us provide our services or conduct data processing on our behalf.

c. At the Clients' request or consent

This includes sharing data with:

- **The Client's underwriters or insurers**. For example, where a Client requests that we provide the underwriter of its insurance products with access to its data or data reporting. This can be shared through apps or websites that integrate with our APIs.
- **The Client's business partners or service providers.** If a Client uses third party partners or service providers for its insurance business and requests that we share access to its data or Root Account with them. For example, claims administration providers.

d. Legal reasons

We may share your personal data if we believe we are legally required to do so (e.g. to comply with law enforcement investigations or other legal proceedings), to enforce our contracts and policies or to respond to an emergency that we believe in good faith requires that we disclose personal data.

If there is a change in our company structure or ownership, we may share your data as part of the assets transferred or the due diligence for the transaction. We'll use reasonable endeavours to anonymise your data where possible, and will comply with any applicable confidentiality obligations.

4. DATA RETENTION, EXPORT AND DELETION

a. Retaining data

We only retain your data for as long as necessary for the purposes described above.

This varies depending on the type of data, the category of user you are, the purposes that we collected the data for and whether the data must be retained after an account deletion request for purposes described below.

b. Exporting data

You have the right to access all of your data stored on our platform.

As a Client, you can export a copy of all of your data from the Root Insurance Platform if you want to back it up or use it with a service outside of Root.

For more information on how to export your data, see our Documentation here.

c. Deleting data

If your agreement with us is terminated or you request that we delete your Root Account and/or data by contacting us, we will delete all of your data, data of your policyholders, Users and End Users from the Root Insurance Platform and our servers within 60 days of termination or your request.

We retain your other data for business reasons and to comply with legal and audit obligations. We will not keep it for longer than is necessary.

5. HOW WE PROTECT YOUR DATA

We understand how sensitive policyholder and User information is for your business.

That's why we emphasise privacy and security throughout all system design processes and implement security measures based on the sensitivity of the data we hold.

These measures are in place to protect the data from being disclosed, from loss, misuse and unauthorised access and from being altered or destroyed. They include:

- Encryption to keep your data private while stored and in transit
- Multi-factor authentication and strong password requirements on the application
- Using trusted, SOC 2 certified and ISO27001 compliant AWS data centres for cloud-hosting our platform infrastructure
- Strict access control in accordance with the principle of least privilege, meaning that access to personal data is limited to only Root employees and contractors who need that information to process it
- Regularly tested security incident response procedures

You can find more information about these and our other measures on our Security page.

We proactively monitor our systems for bugs, possible vulnerabilities and attacks and our team is on call 24/7 to address and report incidents. Still, no system is perfect and we could never guarantee that we will never experience a breach of any of our physical, technical or administrative safeguards.

You also have a role to play in keeping personal data safe. For example, you should never share your login credentials for your Root Account with anyone, and should make sure your employees or agents follow the same rule.

If you suspect that we (or you) have had a security breach, please let us know immediately by sending an email to privacy@rootplatform.com and contacting your Root account manager.

We will let you know of any incidents that affect your personal data and we will inform you about how you can help minimise the impact.

6. HOW WE USE COOKIES

Cookies are small data files stored on your device by websites that you visit. They allow websites to track and remember information about your device and how you use the website.

When you visit Our Sites, we collect information from you automatically through cookies.

Our Sites use the following types of cookies:

- **Essential cookies** - Essential cookies are required to enable the basic features of Our Sites, like adjusting your consent preferences. The legal basis for our use of essential cookies is our legitimate interests, namely being able to provide and maintain Our Sites.
- **Analytics cookies** - Analytics cookies are used to understand how Site Visitors interact with Our Sites. These cookies help provide information on metrics like the number of visitors, bounce rate, traffic source etc. and help us improve the way Our Sites work. You will be asked to consent to the use of these cookies and are free to deny your consent.
- **Targeting cookies** - Targeting cookies are used to identify visitors between different websites, for example, content partners and banner networks. Those cookies may be used to build a profile of Site Visitor interests or show relevant ads on other websites. You will be asked to consent to the use of these cookies and are free to deny your consent.
- **Functionality cookies** - Functionality cookies are used to remember Site Visitor information on our Sites, like preferences selected on cookie consent banner. These cookies help ensure website compliance with privacy regulations by remembering your cookie choices. You will be asked to consent to the use of these cookies and are free to deny your consent.

You can block any of these cookies by activating a setting on your browser allowing you to refuse cookies, or by selecting your cookie preferences in the pop-up on our website. You can also delete cookies through your browser settings.

If you turn off cookies, you can continue to use Our Sites, but certain services may not work effectively or at all.

Our Sites may contain links to other websites. This Privacy Policy only applies to Our Sites, so if you click on a link to another website, you should read their privacy or cookie policy.

7. YOUR RIGHTS

We would like to make sure you are fully aware of all of your data protection rights. You have:

- The right to be informed about the collection and use of your personal data.

- The right to access your personal data.
- The right to have inaccurate personal data corrected or completed if it is incomplete.
- The right to have your personal data erased, also known as the 'right to be forgotten'.
- The right to request that we restrict the processing of your personal data.
- The right to receive your personal data for your own purposes across different services, also known as the right to data portability.
- The right to object to us processing your personal data in certain circumstances.
- The right to object to automated decision-making and profiling. You may ask that a human review any automated decisions that we make about you, express your point of view about it, and obtain an explanation of the decision.

You can exercise your rights by contacting us at the addresses below.

If you wish to make a complaint about how we process your personal data, you may submit this to us using the address below. We will acknowledge receipt of your complaint within 30 days and provide you with the outcome of our investigation without undue delay.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

We try to respond to requests within 30 days. Occasionally it may take us longer than 30 days if your request is particularly complex or you have made a number of requests.

We may also charge a reasonable fee if your request is manifestly unfounded, excessive or repetitive or as we're otherwise legally allowed to do, alternatively, we may refuse to comply with your request in these circumstances to the extent we're legally allowed to.

We will let you know if this is the case.

If you are a User or End User, we may be required to redirect your request or complaint to the relevant Client who is your data controller or responsible party for them to respond directly.

8. CONTACTING US

We regularly review our compliance with this Privacy Policy. If you have any questions, please contact us by email at privacy@rootplatform.com, alternatively contact Root's Legal Counsel / Data Protection Officer at ashton@root.co.za.

If you do need to send physical mail, this should be sent to the following addresses:

- **If you are in the United Kingdom, EEA, Middle East, Asia or Oceania:**
  Root Platform, 33 Queen Street, London, England, EC4R 1AP
- **If you are in Africa:**
  Great Westerford, 240 Main Road, Rondebosch, Cape Town, South Africa, 7700
- **Any other country or region:**
  Root Platform, 33 Queen Street, London, England, EC4R 1AP

9. CONTACTING THE AUTHORITIES

You have the right to lodge a complaint with the following authorities:

If you are in the United Kingdom:
The Information Commissioner's Office at 0303 123 1113 or by starting a live chat on the ICO website, if you believe that your personal data is being processed in a manner that is not in compliance with the UK GDPR or UK Data Protection Act.

If you are in the European Union:
A supervisory authority in the Member State where you live or work, or where the infringement took place.

If you are in South Africa:
You have the right to complain to the Information Regulator at inforeg@justice.gov.za if you believe that your personal data is being processed in a manner that is not in compliance with POPIA.