

Privacy Policy

Last updated October 6, 2026

Contents

Summary of key points

1. What information do we collect?
2. How do we process your information?
3. What legal bases do we rely on to process your information?
4. When and with whom do we share your personal information?
5. How long do we keep your information?
6. How do we keep your information safe?
7. Do we collect information from minors?
8. What are your privacy rights?
9. Controls for do-not-track features
10. Do we make updates to this notice?
11. How can you contact us about this notice?
12. How can you review, update, or delete the data we collect from you?

This Privacy Notice for Zulu Code (Pty) Ltd ('we', 'us' or 'our') describes how and why we might access, collect, store, use and/or share ('process') your personal information when you use our services ('Services'), including when you:

- visit our website at cutq.co.za, or any website of ours that links to this Privacy Notice;
- download and use our mobile application (CutQ), or any other application of ours that links to this Privacy Notice;
- use CutQ to find and book beauty, grooming and wellness services, or to list and run a business that offers them; or
- engage with us in other related ways, such as contacting our support.

We are the responsible party for your personal information under the Protection of Personal Information Act 4 of 2013 ('POPIA').

Questions or concerns? Reading this Privacy Notice will help you understand your privacy rights and choices. We are responsible for making decisions about how your personal information is processed. If you do not agree with our policies and practices, please do not use our Services. If you still have any questions or concerns, please contact us at info@cutq.co.za.

Summary of key points

This summary provides key points from our Privacy Notice. You can find out more about any of these topics by following the link after each key point or by using the contents above.

What personal information do we process? When you visit, use or navigate our Services, we may process personal information depending on how you interact with us and the Services, the choices you make, and

the features you use. [Learn more about personal information you disclose to us.](#)

Do we process any sensitive personal information? Only if you choose to be verified. To confirm that a person is real and that a business is registered, we process a live selfie and identity-document details through a trusted identity partner, only when you ask for it and after you have consented. [Learn more about verification information.](#)

Do we collect any information from third parties? Only when you ask us to. If you verify your identity or your business we receive the result of the check from our identity partner. If you link a TikTok account we receive your public profile details and follower counts from TikTok.

How do we process your information? We process your information to provide, improve and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your information for other purposes with your consent. We process your information only when we have a valid legal reason to do so. [Learn more about how we process your information.](#)

In what situations and with which parties do we share personal information? We share information with the businesses you book with, and with the service providers that help us run CutQ. We do not sell your personal information. [Learn more about when and with whom we share your personal information.](#)

How do we keep your information safe? We have adequate organisational and technical processes and procedures in place to protect your personal information. However, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals or other unauthorised third parties will not be able to defeat our security and improperly collect, access, steal or modify your information. [Learn more about how we keep your information safe.](#)

What are your rights? Under POPIA you have the right to access, correct and delete your personal information, to object to its processing and to complain to the Information Regulator. [Learn more about your privacy rights.](#)

How do you exercise your rights? The easiest way to exercise your rights is by emailing us at info@cutq.co.za. You can also update or delete your account in the app at any time. We will consider and act upon any request in accordance with applicable data protection laws.

1. What information do we collect?

Personal information you disclose to us

In short: We collect personal information that you provide to us.

We collect personal information that you voluntarily provide to us when you register on the Services, make or manage a booking, set up a business, participate in activities on the Services, or otherwise when you contact us.

Personal information provided by you. The personal information that we collect depends on the context of your interactions with us and the Services, the choices you make, and the features you use. The personal information we collect may include the following:

- names
- phone numbers
- email addresses
- passwords
- profile photos
- booking details and notes
- reviews and review photos
- messages you send through the Services
- if you run a business: your business name, address, services, prices, opening hours, photos and the names and contact details of staff you invite

Sensitive information. When it is necessary and with your consent, we process the following categories of sensitive information, only if you choose to verify your identity: biometric information (a live selfie, used to confirm that you are a real person and that you match your identity document) and identity document information (the type and issuing country of your identity document, and whether you are over 18). See ['Verification information'](#) below for exactly what we keep.

Payment data. All payments on CutQ are processed by our payment provider, Paystack. If you pay for a business subscription, or pay a booking deposit to a business, you enter your card or bank details on Paystack's secure page, and Paystack processes and stores them. We do not receive or store your card number, security code or online banking details; we receive only the result of each payment, the amount, the payment channel, Paystack's fee and a reference. You can find Paystack's privacy notice on its website.

Deposits and payouts. If a business asks for a deposit to secure a booking, the deposit is paid to that business through Paystack; we record the booking it belongs to, the amount, when it was paid, and whether it was refunded or kept. A business that takes deposits registers the bank account Paystack should pay into. We send the bank name, account holder and account number to Paystack once, over an encrypted connection, and keep only the bank name, the account holder, the last four digits of the account number and Paystack's reference for the account. Where the account holder is a person, these details are personal information and are processed to pay the business what customers have paid it.

Messages. If you use in-app messaging, we collect the messages you send and receive, when each message was sent and read, and the booking it relates to. Messaging is available only while you have a booking with a business, and a business cannot see your phone number through it. If a conversation is reported, the reported messages are reviewed by us.

Verification information. If you choose to verify your identity or your business, our identity partner (Didit) asks you for a live selfie and, for an ID check, images of your identity document (an ID card, passport or

driver's licence); for a business check, your CIPC certificate or registry extract. The images are processed by the partner and deleted by them after the check. We receive and keep only the result of the check, the document type and issuing country, whether you are over 18, and a one-way hash of your ID number that is used solely to stop the same identity from being used for more than one account. We do not keep your ID number, your date of birth or the images themselves. The partner may keep a face template to prevent one face from verifying several accounts. If you link a TikTok account, we receive your TikTok username, display name and public follower and like counts from TikTok, and hold a token that lets us refresh those counts until you unlink the account.

Information collected automatically

Device and log data. When you use the Services, our servers and service providers automatically record technical information such as your IP address, device type, operating system and app version, and the time of your requests. We use it to keep the Services secure, to prevent abuse and to fix problems. We do not use advertising or analytics software, and we do not track you across other apps or websites.

Application data. If you use our app, we also may collect the following information if you choose to provide us with access or permission:

- **Geolocation information.** We may request access or permission to use your device's location while you are using the app, to show businesses near you. If you wish to change our access or permissions, you may do so in your device's settings.
- **Camera and photos.** We may request access to your camera and photo library so that you can add a profile, portfolio or review photo, take a live selfie for identity verification, photograph an identity or business document, or scan a check-in code. If you wish to change our access or permissions, you may do so in your device's settings.
- **Push notifications.** We may request to send you push notifications about your bookings, messages and account. If you wish to opt out from receiving these types of communications, you may turn them off in your device's settings.

All personal information that you provide to us must be true, complete and accurate, and you must notify us of any changes to such personal information.

Google Maps Platform

Address search and maps in the Services use Google Maps Platform. When you search for an address or place, the text you type is sent to Google to return suggestions, and Google's privacy policy applies to that information.

2. How do we process your information?

In short: We process your information to provide, improve and administer our Services, communicate with you, for security and fraud prevention, and to comply with law. We may also process your

information for other purposes only with your prior explicit consent.

We process your personal information for a variety of reasons, depending on how you interact with our Services, including:

- **To facilitate account creation and authentication and otherwise manage user accounts.** We may process your information so you can create and log in to your account, as well as keep your account in working order.
- **To provide the Services.** We may process your information to show businesses and their services, and to let you book, reschedule and cancel appointments, or, if you run a business, to receive and manage bookings.
- **To manage business subscriptions.** We may process your information to run your free trial, take subscription payments through Paystack and manage cancellations.
- **To respond to user inquiries and offer support.** We may process your information to respond to your inquiries and solve any potential issues you might have with the Services.
- **To request feedback.** We may process your information when necessary to request feedback, such as a review after an appointment, and to contact you about your use of our Services.
- **To protect our Services.** We may process your information as part of our efforts to keep our Services safe and secure, including fraud monitoring and prevention.
- **To save or protect an individual's vital interest.** We may process your information when necessary to save or protect an individual's vital interest, such as to prevent harm.
- **To let you and businesses message each other.** We may process your messages so that you and a business you have booked with can communicate in the app about that booking.
- **To verify identities and businesses.** We may process your information to confirm that a person is who they say they are and that a business is registered, and to show a verification badge, so that customers and businesses can trust one another.
- **To keep the community safe.** We may process reports, blocks and, when a conversation is reported, the reported messages, to investigate misuse and enforce our legal terms.
- **To send you notifications.** We may process your information to send you push notifications, emails and in-app notices about your bookings, messages and account.

3. What legal bases do we rely on to process your information?

In short: We only process your personal information when we have a valid legal reason to do so under POPIA.

Section 11 of POPIA lists the grounds on which personal information may be processed. We rely on the following:

- **Consent.** We may process your information if you have given us permission (i.e. consent) to use your personal information for a specific purpose, such as identity verification. You can withdraw your consent at any time.
- **Performance of a contract.** We may process your personal information when it is necessary to perform our agreement with you, including providing our Services, or to take steps at your request before entering into one.
- **Legal obligations.** We may process your information where it is necessary for compliance with our legal obligations, such as to cooperate with a law enforcement body or regulatory agency, exercise or defend our legal rights, or disclose your information as evidence in litigation in which we are involved.
- **Legitimate interests.** We may process your information when it is reasonably necessary for our legitimate interests, or those of a third party to whom it is supplied, and those interests are not outweighed by your interests and rights. For example, to diagnose problems, prevent fraud and misuse, and keep the Services secure.
- **Your legitimate interests.** We may process your information where it protects a legitimate interest of yours, such as situations involving potential threats to your safety.

4. When and with whom do we share your personal information?

In short: We may share information in specific situations described in this section and/or with the following third parties. We do not sell your personal information.

We may need to share your personal information in the following situations:

- **Businesses you book with.** When you make a booking, the business (its owners and the staff member assigned to you) sees your name, the booking details and any notes you add. Your phone number and email address are shared only if you choose to provide them, for example in a walk-in booking, or when you choose to contact a business on WhatsApp, in which case WhatsApp (Meta) receives your phone number and message under its own privacy policy.
- **Public profile content.** If you run a business, your business profile (name, address, services, prices, opening hours and photos) is shown publicly on CutQ. If you write a review, the review, your rating and any review photos are shown publicly on the business's profile.
- **People you share a booking with.** If you use 'Share this booking', anyone with the link can see the service, the business and its address, the appointment time and the live status of that booking until the link expires or you revoke it.
- **Identity verification partners.** Dikit processes selfies and documents on our behalf to verify identities and businesses. TikTok provides your public profile details and follower counts if you choose to link a TikTok account.

- **Service providers.** We share information with vendors that process it on our behalf and only as needed to run the Services: Supabase (database, authentication and file storage, hosted in the European Union), Paystack (subscription payments, booking deposits, refunds and payouts to businesses' bank accounts), Resend (email), Google (maps, places, geocoding and push notifications through Firebase) and Netlify (website hosting).
- **Businesses you pay a deposit to.** When you pay a booking deposit, the business sees that the deposit was paid, the amount and the booking it belongs to. It does not see your card or bank details.
- **Legal requirements.** We may disclose your information where we are legally required to do so, for example in response to a court order or a lawful request from a public authority.
- **Business transfers.** We may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing or acquisition of all or a portion of our business to another company.

Transfers outside South Africa

Our database, authentication and file storage are hosted by Supabase in Frankfurt, Germany, and some of our other service providers process information in other countries. Where we transfer your personal information outside South Africa, we do so only as section 72 of POPIA allows: to countries with laws that provide an adequate level of protection, such as the European Union's General Data Protection Regulation, or under written agreements that require the recipient to protect your information to a standard substantially similar to POPIA.

5. How long do we keep your information?

In short: We keep your information for as long as necessary to fulfil the purposes outlined in this Privacy Notice unless otherwise required by law.

We will only keep your personal information for as long as it is necessary for the purposes set out in this Privacy Notice, unless a longer retention period is required or permitted by law (such as tax, accounting or other legal requirements). No purpose in this notice will require us keeping your personal information for longer than twelve (12) months past the termination of the user's account. Records of payments, deposits and refunds are kept for five (5) years from the date of the transaction, as South African tax law requires, and are then deleted.

Messages are kept for twelve (12) months from the date they were sent and are then deleted. When you delete your account your messages are no longer linked to you, but the other party's copy of the conversation remains until that period ends. Verification results are valid for twelve (12) months, after which you may verify again; the one-way hash of your ID number is kept for as long as your account exists so that the same identity cannot be used for more than one account, and a record of when verification was attempted (the date and type of check only) is kept to enforce attempt limits. When you delete your account we delete your verification records and booking share links and ask our identity partner to delete any verification session it still holds.

When we have no ongoing legitimate business need to process your personal information, we will either delete or de-identify such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible.

6. How do we keep your information safe?

In short: We aim to protect your personal information through a system of organisational and technical security measures.

We have implemented appropriate and reasonable technical and organisational security measures designed to protect the security of any personal information we process, including encryption in transit and access controls that limit each user to their own information. Card and bank details are entered only on Paystack's pages and never pass through our servers, apps or website; Paystack is certified to the Payment Card Industry Data Security Standard. Payment records in our systems hold amounts, dates and references, and bank account records hold only the last four digits of the account number. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that hackers, cybercriminals or other unauthorised third parties will not be able to defeat our security and improperly collect, access, steal or modify your information. Although we will do our best to protect your personal information, transmission of personal information to and from our Services is at your own risk. You should only access the Services within a secure environment.

If we have reasonable grounds to believe that your personal information has been accessed or acquired by an unauthorised person, we will notify you and the Information Regulator as required by section 22 of POPIA.

7. Do we collect information from minors?

In short: We do not knowingly collect data from or market to children under 18 years of age.

The Services are only for people who are 18 or older. We do not knowingly collect, solicit data from, or market to children under 18 years of age, nor do we knowingly sell such personal information. By using the Services, you represent that you are at least 18. If we learn that personal information from users less than 18 years of age has been collected, we will deactivate the account and take reasonable measures to promptly delete such data from our records. If you become aware of any data we may have collected from children under age 18, please contact us at info@cutq.co.za.

8. What are your privacy rights?

In short: You may review, change or delete your account at any time, and you have the rights POPIA gives you.

Under POPIA you have the right to:

- ask whether we hold personal information about you, and request a copy of it;
- ask us to correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully, or that we are no longer authorised to keep;
- object, on reasonable grounds, to the processing of your personal information, and to object at any time to its use for direct marketing;
- withdraw your consent where we rely on it;
- not be subject to a decision based solely on automated processing that has legal consequences for you or affects you to a substantial degree; and
- complain to the Information Regulator.

To make a request, email us at info@cutq.co.za. We may need to confirm your identity before we act on it. We will consider and act upon any request in accordance with POPIA and the Promotion of Access to Information Act 2 of 2000.

Withdrawing your consent: If we are relying on your consent to process your personal information, you have the right to withdraw your consent at any time by contacting us using the contact details provided in this document. This will not affect the lawfulness of the processing before its withdrawal, nor, when applicable law allows, will it affect the processing of your personal information conducted in reliance on lawful processing grounds other than consent.

Account information

If you would at any time like to review or change the information in your account or terminate your account, you can:

- log in to the app and update your profile; or
- delete your account from within the app (Delete account, in your profile). This cancels your upcoming bookings and removes your profile photos, verification records and booking share links. If you own a business with an active subscription, it is cancelled too.

Upon your request to terminate your account, we will deactivate or delete your account and information from our active databases. However, we may retain some information in our files to prevent fraud, troubleshoot problems, assist with any investigations, enforce our legal terms and/or comply with applicable legal requirements.

The Information Regulator

If you are unsatisfied with the manner in which we address any complaint with regard to our processing of personal information, you can contact the Information Regulator (South Africa):

- General enquiries: enquiries@inforegulator.org.za

- Complaints (complete POPIA/PAIA form 5): PAIAComplaints@info regulator.org.za and POPIAComplaints@info regulator.org.za

9. Controls for do-not-track features

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ('DNT') feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. We do not track you across other websites or apps, and we do not use advertising or analytics cookies (see our [Cookie Policy](#)), so the Services behave the same whether or not DNT is switched on.

10. Do we make updates to this notice?

In short: Yes, we will update this notice as necessary to stay compliant with relevant laws.

We may update this Privacy Notice from time to time. The updated version will be indicated by an updated 'Last updated' date at the top of this Privacy Notice. If we make material changes to this Privacy Notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this Privacy Notice frequently to be informed of how we are protecting your information.

11. How can you contact us about this notice?

If you have questions or comments about this notice, you may email us at info@cutq.co.za or contact us by post at:

Zulu Code (Pty) Ltd
Boksburg, Johannesburg, Gauteng 1459
South Africa

12. How can you review, update, or delete the data we collect from you?

You have the right to request access to the personal information we collect from you, details about how we have processed it, correct inaccuracies, or delete your personal information. You may also have the right to withdraw your consent to our processing of your personal information. These rights may be limited in some circumstances by applicable law. To request to review, update or delete your personal information, email us at info@cutq.co.za, or delete your account from within the app.