

Screenzor

Privacy Policy

Last revised: August 17, 2026

1. Who We Are

Screenzor ("Screenzor," "we," "us") is operated by Donald Mzima, based in South Africa. This Privacy Policy explains how we collect, use, and protect personal information when you use screenzor.com, the Screenzor Chrome extension, and related services (together, the "Service").

Contact for privacy matters: legal@screenzor.com.

2. What Data We Collect

- Account data: name, email address, and a securely hashed password (or

third-party sign-in identifier) when you register.

- Billing data: subscription plan and payment status. Card and payment

details are collected and processed directly by our payment processors, Payfast and (from a future date) Paystack — we do not store full card numbers ourselves.

- Usage data: pages visited, features used, approximate location

(derived from IP address), device and browser type, collected via Google Analytics and Google Ads (see our Cookie Policy (<https://screenzor.com/cookie-policy>)).

- Recording content: screen recordings you create. If you record

locally and never upload or share a recording, Screenzor's servers do not receive that content. If you upload a recording (e.g. to generate a shareable link, or to use team workspace features), the video and any associated metadata (title, timestamps, viewers) are stored on our infrastructure as described in Section 11.

- Team/workspace data: for Pro+ team workspaces, the names/emails of

invited members and their access activity.

3. Why We Process Your Data (Legal Bases)

Depending on your location, we rely on one or more of the following legal bases: your consent (e.g. for analytics/advertising cookies, marketing emails); performance of a contract with you (providing the Service you signed up for); our legitimate interests (e.g. securing the Service, improving features); and compliance with a legal obligation (e.g. tax and accounting records).

4. International Data Transfers

Some of our sub-processors (Section 11) store or process data outside South Africa, including in the European Union, United Kingdom, and United States. Where we transfer personal data internationally, we rely on recognized safeguards such as Standard Contractual Clauses, adequacy decisions, or the sub-processor's own certified compliance framework, consistent with section 72 of South Africa's Protection of Personal Information Act (POPIA) and Chapter V of the GDPR.

5. Data Retention

We retain account and recording data for as long as your account is active. Google user data is retained and

deleted as described in Section 9.

If you delete your account in the app (Settings ! Account ! Delete account), we delete your account data from the application database as part of that process, including Google user data associated with the account. As an outer limit, we delete or anonymize remaining personal data within 90 days, except where we must retain records longer to comply with legal, tax, or dispute-resolution obligations.

6. Your Rights

If you are in the EEA/UK: you have the right to access, correct, erase, restrict, or port your data, and to object to processing based on legitimate interests, under the GDPR/UK GDPR.

If you are in South Africa: you have equivalent rights under POPIA, including the right to request access to and correction or deletion of your personal information, and to object to processing for direct marketing.

If you are in California: you have rights under the CCPA/CPRA, including the right to know, delete, correct, and to opt out of the "sale" or "sharing" of personal information (Screenzor does not sell personal information; our use of Google Analytics/Ads may constitute "sharing" for advertising purposes, which you can opt out of via our cookie banner).

If you are in another US state with a comprehensive privacy law (e.g. Virginia, Colorado, Connecticut, Utah), you have similar access, deletion, correction, and opt-out rights under that state's law.

If you are in Canada: you have rights under PIPEDA to access and challenge the accuracy of your personal information.

If you are in Brazil: you have rights under the LGPD, including confirmation of processing, access, correction, anonymization, and deletion.

If you are in Australia: you have rights under the Privacy Act 1988 to access and correct your personal information.

How to Exercise Your Rights

You can delete your Screenzor account and associated cloud data, including Google user data, in the app: Settings ! Account ! Delete account. You can disconnect Google Calendar (and other integration data) under Settings ! Integrations. You may also email legal@screenzor.com with a correction, or deletion request. We will respond within the timeframe required by your local law (for example, 30 days under GDPR, 45 days under the CCPA, or a reasonable period under POPIA), and may need to verify your identity first.

7. Direct Marketing and Email Communications

We will only send you promotional or marketing emails if you have opted in, consistent with POPIA section 69 and Canada's Anti-Spam Legislation (CASL), both of which require opt-in consent. Our marketing emails also comply with the US CAN-SPAM Act's requirements (truthful headers, a working unsubscribe mechanism, and prompt honoring of opt-out requests), even though opt-in consent is our own stricter internal standard beyond what CAN-SPAM itself requires. Every marketing email includes an unsubscribe link, and you can withdraw consent at any time without affecting transactional emails (e.g. billing receipts, security notices).

8. Children's Privacy

Screenzor is not directed at children under 13 for direct, individual sign-up. Where Screenzor is used in a school or classroom setting, our School/Institutional Terms Addendum (<https://screenzor.com/school-institutional-addendum>) governs how student data is handled and places consent obligations on the adopting institution.

9. Google User Data

If you sign in with Google, or optionally connect Google Calendar, Screenzor receives Google user data (such as your email, basic profile information, and calendar/event data you authorize) only to provide and improve Screenzor's features — for example, account sign-in, showing your meetings, and meeting notes. We do not use Google user data for advertising, and we do not sell Google user data. Screenzor's use and transfer of information received from Google APIs complies with the Google API Services User Data Policy (<https://developers.google.com/terms/api-services-user-data-policy>), including the Limited Use requirements.

Service providers listed in Section 12 (including Supabase and our hosting infrastructure) process this information only to operate Screenzor on our behalf. That is not a sale of Google user data and is not use for advertising.

How we protect Google user data

Screenzor protects Google user data with the following controls, which are implemented in the product today:

- Data is encrypted in transit using HTTPS/TLS between your browser or

the Screenzor apps and our servers.

- Data is encrypted at rest using our infrastructure providers'

storage-level encryption (see Section 12).

- Google Calendar refresh tokens are encrypted with AES-256-GCM before

they are stored, and Screenzor's Calendar APIs do not return those tokens to the client.

- Google Calendar OAuth uses PKCE (S256) when connecting a calendar.
- Calendar API routes that read or change a user's Calendar data require a

signed-in user and a valid authentication token. Database row-level security restricts Calendar rows so that an authenticated user can access only their own data.

- Access to user data within Screenzor is limited to what is necessary to

operate and support the Service, as described in our Security Statement (<https://screenzor.com/security-statement>).

How long we keep Google user data

- Google sign-in information (such as your email, name, and profile

photo provided by Google for account sign-in) is kept while your Screenzor account remains active. Disconnecting Google Calendar does not remove your Screenzor sign-in.

- Google Calendar connection data, including OAuth/token material,

selected calendars, and synchronized event copies (titles, times, locations, meeting links, attendee/organizer information, and related provider metadata), is kept while Google Calendar remains connected to your Screenzor account.

When you connect Google Calendar, Screenzor copies events from a recent window on the first sync (currently about 90 days back and 180 days forward) and then keeps those copies updated. That window is how we choose what to sync. It is not an automatic deletion schedule. Synced event copies remain until you disconnect Google Calendar, delete your Screenzor account, or a later sync removes an event that was deleted or cancelled in Google.

Disconnecting Google Calendar

If you disconnect Google Calendar in Settings > Integrations, Screenzor:

- stops future Calendar synchronization;
- revokes Google authorization for the Calendar integration where technically possible;
- removes stored Google Calendar integration data that is no longer required, including synchronized events and related metadata; and
- removes stored Google Calendar refresh-token credentials associated with the integration.

Disconnecting Google Calendar does not delete your Screenzor account, cloud recordings, or notes you created in Screenzor. You can connect Google Calendar again later.

Deleting your Screenzor account

If you delete your Screenzor account, Google user data associated with that account is deleted as part of the same process. That includes Google sign-in identity stored for the account, Google Calendar connections, OAuth/token material, synchronized Calendar events, and related synchronization data.

How to request deletion of Google user data

- Google Calendar data only: Settings ! Integrations ! Disconnect calendar.
- Your whole Screenzor account (including Google user data):
Settings ! Account ! Delete account.
- By email: legal@screenzor.com. We will verify your identity and complete or confirm deletion as described in Section 5 and Section 6.

10. Data Security and Breach Notification

We protect personal data, including Google user data, using the mechanisms described in Section 9 and in our Security Statement (<https://screenzor.com/security-statement>): encryption in transit (HTTPS/TLS), encryption at rest on our infrastructure providers, application-level encryption of Google Calendar refresh tokens, authenticated Calendar API access, and database row-level security. If a data breach occurs that is likely to result in risk to your rights, we will notify affected users and, where required, the relevant regulator (e.g. South Africa's Information Regulator within a reasonable time, or the competent EU supervisory authority within 72 hours) without undue delay. Security researchers who discover a vulnerability should follow our Vulnerability Disclosure Policy (<https://screenzor.com/vulnerability-disclosure-policy>).

11. Contact Us

Questions about this Privacy Policy: legal@screenzor.com.

12. Sub-Processors

We use the following third-party service providers to operate Screenzor. Each processes personal data only as necessary to perform its function for us:

Sub-processor — Purpose — Data involved

Supabase — Authentication, database, file storage — Account data, uploaded recordings, workspace data, Google sign-in

identifiers, and Google Calendar integration data (when connected)

Cloud hosting provider (GCP/Cloudflare) — Infrastructure/hosting — All data in transit/at rest

Google Analytics — Website usage analytics — Usage data, device/browser data

Google Ads — Advertising measurement — Usage data (with consent, see Cookie Policy)

Payfast — Payment processing — Billing data

We review this list periodically; material additions will be reflected here and, where required by law, notified to you in advance.

Last revised: August 17, 2026

We may update this document from time to time. If we make material changes, we will notify you by email and/or a notice on the Screenzor website before the change takes effect. Minor changes will only update the date above.