grcHero

Privacy Policy

Document ID	**PRIVACY-1.1**	Effective date	**24 Nov 2026**
Version	**1.1**	Operator	**Baraka JM**
Status	**Published**	Contact	**baraka@grchero.dev**
Classification	**Public**		

Questions about this document: baraka@grchero.dev.

Contents

1 Who is responsible 3
2 Data we handle 3
3 Why we use data, and on what basis 4
4 Cookies and similar storage 4
5 Analytics 5
6 AI features and your own AI agents 5
7 Support access 5
8 Who we share data with 6
9 Where data is stored, and transfers outside the EU 6
10 How long we keep it 6
11 Security 7
12 Your rights 7
13 Changes 7

1 Who is responsible

grcHero is built and run by Braintel Innovations, a technology startup based in Salasala, Dar es Salaam, Tanzania (registered with BRELA, business name registration number 724001). Email: baraka@grchero.dev.

We process personal data under the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and Tanzania's Personal Data Protection Act, 2022 (PDPA). This policy gives you the information these laws ask us to give.

We act in two roles:

- For account and service data (who you are and how you use grcHero) we decide why and how it is used, so we are the controller.
- For Your Content (the records you and your members enter in a workspace) the workspace decides why and how, and we process it on its behalf. We offer a data processing agreement for this on request at baraka@grchero.dev.

2 Data we handle

Table 1. Data we handle

Data	Examples	Why
Account	Email, display name, link to your sign-in identity, role, membership, invitations	Create and secure your account and workspace
Sign-in	Credentials and sign-in state, held by the identity service we run ourselves	Check who you are
Sessions	A session identifier and sign-in flow state, in strictly necessary cookies, and session data on our servers	Keep you signed in safely
API tokens	Only a hash of each token, plus when and from where it was last used	Secure automation
Audit records	Who did what and when inside a workspace: person, action, record, time, request reference, and the name of the client or AI agent used	Accountability and security
Usage counts	Daily counters, such as the number of AI requests	Apply limits and run the service
Command line activity	Who ran a scan, when, how they signed in and the version of the command line tool. Never your source code, file paths or findings	Show a workspace how its tool is used
Your Content	Everything entered or uploaded in a workspace, including text read from uploaded files	Provide the service
Guests	An invited external reviewer's verified email and what they viewed in a package	Run external review

Data	Examples	Why
Email	Your address, and which fixed notices we sent	Send invitations and the notices you ask for
Feedback	If you use Share feedback: your message, its kind, your name and email, your workspace name and the page you were on	Improve the product and reply
Support	What you send us	Respond
Visits to public pages	The page path, the referring site's host name, your country and a visitor number that changes every day. See section 5	Learn which public pages are useful
Optional product analytics	Only if you opt in. See section 5	Improve the product

grcHero is meant for people acting for an organisation and is not directed at children. We do not knowingly collect data from children. grcHero is not designed to hold special categories of personal data, such as health data. A workspace is responsible for the personal data it chooses to enter and for having a lawful basis for it.

3 Why we use data, and on what basis

- To provide the service (account, sign-in, workspace, the features you use): performance of the agreement with you.
- To keep the service secure and accountable (sessions, audit records, abuse and error handling): our legitimate interest in running a safe service.
- To count visits to our public pages without a cookie (section 5): our legitimate interest in knowing which pages are useful. Browsers that send Do Not Track or Global Privacy Control are not counted.
- For optional analytics and for AI requests that send content to an outside provider: your consent, given at that time and withdrawable at any time.
- Where the law requires it: legal obligation.

4 Cookies and similar storage

We set two cookies. Both are HttpOnly and SameSite=Lax, and Secure outside local development:

- A session cookie holding your session identifier. It lasts at most 7 days, and ends after 8 hours of inactivity or when you sign out.
- A sign-in cookie holding sign-in flow state. It lasts 10 minutes.

Both are strictly necessary. We use no advertising cookies. Counting visits to public pages sets no cookie and stores nothing in your browser. Your browser's storage holds only your analytics choice and, if you opt in, a random anonymous identifier, plus temporary assistant sharing choices for the current tab session.

5 Analytics

Visits to our public pages. When the operator has switched it on and you open our website, documentation or blog, we count the visit. We record the page path (without anything after a question mark), the host name of the site that referred you, your country as reported by our network provider, and a visitor number that changes every day and cannot be linked from one day to the next. We set no cookie and store nothing in your browser for this. Your IP address and browser details are used briefly on our server to produce the daily number and are not stored or passed to the analytics system. If your browser sends Do Not Track or Global Privacy Control, the visit is not counted. Pages where you sign in or work are never counted this way. The same account is published at grchero.dev/docs/site-analytics. We have not set an automatic deletion period for these counts. They contain no names or addresses.

Product use, if you opt in. Off unless the operator switches it on, and then only after you tick the opt-in, which starts unticked. We honour Do Not Track and Global Privacy Control. Events use fixed names and generic page paths. We collect no file contents, labels, workspace or person identities, session replay or autocapture.

Both run on analytics software we host ourselves, so analytics data does not go to an advertising company.

6 AI features and your own AI agents

Our AI features. When you choose an AI feature and consent to that request, the question and the excerpts you select (limited in size), or for a diagram draft the description you type, or for a diagram improvement your request with the names and connections of the components in that diagram, are sent to the AI provider named in the dialog. That provider may process the request outside the EU. We do not send workspace or person identifiers, whole databases or raw files. The provider's own retention and training terms apply, and we do not promise zero retention. The text you submit and the draft you get back are stored in your workspace so you can review them. Do not include personal data in a request unless you are entitled to.

Your own AI agent. If you connect your own AI agent through the command line tool or MCP, it acts with your sign-in and only within your role. What it writes is a draft until a person accepts it. grcHero records the agent's name as a label in the audit log. What your agent reads and sends to its own provider is between you and that provider. The command line tool analyses your code on your computer. Before a scan it sends us only its version, the workspace and a random request reference.

7 Support access

grcHero staff cannot see the records in your workspace. If you ask for help, we may ask to view it. An owner or admin decides, for a limited time, read only, and can end it at any moment. Every page we open is shown to owners and admins.

8 Who we share data with

We use service providers who act for us. We do not sell personal data.

Table 2. Who we share data with

Provider	What it does	Where
Contabo	Hosts our servers, which run grcHero, the database and the identity service	Data centre in the EU
Cloudflare	Carries traffic to our sites, and stores uploaded evidence files in its R2 object storage	Global network. Storage is set to Western Europe, a preference rather than a guarantee
Resend	Sends our email	Outside the EU possible
An AI provider	Handles an AI request, only after you consent to it	Named in the dialog

If you choose to sign in with GitHub, GitHub acts for itself as the controller of your GitHub account. We receive your verified email and name from it.

We also share data when the law requires it or to protect rights and security. Invited guests see only the package shared with them.

9 Where data is stored, and transfers outside the EU

We run grcHero from Tanzania, so we reach the data from there when we operate and support the service. Our servers are at Contabo in the EU. Uploaded evidence files are in Cloudflare R2 object storage, set to Western Europe. Cloudflare treats that setting as a preference, not a guarantee, so files may be held elsewhere. Traffic to our sites passes through Cloudflare's global network, and our email and any AI request you consent to are handled by providers that may be outside the EU. Where a provider handles personal data outside the EU or the European Economic Area, we rely on a transfer mechanism recognised under EU law, such as the Standard Contractual Clauses or an adequacy decision.

10 How long we keep it

Table 3. How long we keep it

Data	How long
Account data (email, name)	While your account exists. Deleting a workspace does not delete your account, because you may belong to other workspaces. We remove an account when you ask us to
Your Content and audit records	While the workspace exists. A workspace sets its own record retention periods, and nothing is removed automatically. Owners remove records themselves
A deleted workspace	An owner schedules deletion. A 30-day grace period follows, in which any owner can cancel and export data. After that the workspace is removed

Data	How long
A workspace data export file	Private, and removed after 7 days
Backups	Encrypted, taken daily. We keep the newest 7 and overwrite or delete older ones, including encrypted copies kept away from the server, so deleted data can remain in a backup for up to about a week
Sessions	Ended after 8 hours of inactivity, and at most 7 days
Technical logs	Kept in a rotating set, a fixed amount per service (five files of up to 20 MB), then overwritten. They may include network addresses
Feedback notes	Deleted 12 months after we close them, or 24 months after you sent them if never closed
Public page visit counts	In our analytics system with no automatic deletion period. They hold no names or addresses

11 Security

We use tenant isolation in the database, access control, hashed tokens, encrypted backups, private file storage with short-lived links, malware scanning of uploads and audit logging. We hold no security certification and have not published a penetration test result. No system is perfectly secure. If you find a security problem, please tell us at baraka@grchero.dev.

12 Your rights

You may have the right to access your personal data, have it corrected or erased, restrict or object to its use, receive a copy in a usable format, and withdraw consent. You may also complain to Tanzania's Personal Data Protection Commission, or to the data protection authority where you live or work.

To use a right, email baraka@grchero.dev. We reply without undue delay and within one month, a period the law lets us extend for complex requests, in which case we tell you. For data in a customer workspace, the workspace owner is usually the right first contact. Owners can export all workspace data and schedule its deletion themselves in Settings.

13 Changes

We will update this page and its date. For a material change we will tell workspace owners by email, or by a notice in grcHero, at least 30 days before it applies. Earlier versions remain available on the legal page.