GO SHLIACH

Security & Privacy at Go Shliach

What we hold, what we never hold, and who can see it.

PREPARED FOR

Written for shluchim, their boards, and the donors who ask.

UPDATED

August 2026

QUESTIONS

hello@goshliach.com

Go Shliach is one system used by many Chabad houses, and it handles the two things an organization can least afford to lose: the trust of its donors and the record of their giving. This is the plain account of how both are protected — beginning with the inventory.

IN YOUR WORKSPACE

The gift

Amount, date, fund, and the receipt you issued for it.

The donor

Name, address, contact details, and the notes your office keeps.

Your operations

Households, pledges, programs, deposits, and communications.

Your team

Who has an account, what role they hold, and when they signed in.

NEVER REACHES US

Card numbers

Never received, never transmitted, never stored — not encrypted, not hashed, not there.

Security codes

The CVV on the back of a donor's card never passes through Go Shliach.

Bank credentials

No donor or organization banking logins are held by us.

Another Chabad house's data

Your workspace cannot read theirs, and theirs cannot read yours.

Every Chabad house is a sealed workspace

Many organizations use Go Shliach. No two of them can see each other's records.

That separation is not a filter the application remembers to apply. It is enforced by the database itself, using a mechanism called row-level security. Every record — every contact, donation, receipt, pledge, program, deposit and note — carries the organization it belongs to, and a policy attached to each table checks the membership of the person asking before a single row is returned.

The check is not optional and cannot be skipped from the application side. A request for rows outside your workspace does not come back empty as a courtesy; it is refused one level below the application, by the database engine itself.

This is a deliberate choice about where to put the guarantee. The common alternative is to filter by organization in application code — which works right up until one query out of several hundred is written without the filter. Putting the rule in the database means the wrong query returns nothing rather than someone else's donors.

The same policies also account for the state of the organization. A workspace that has been suspended, closed, or frozen stops accepting writes at the database level too, not merely in the interface.

> If a developer shipped a bug tomorrow that asked the database for "all donations," the database would still hand back only yours.

Card numbers never reach us

When a donor gives online, their card details go from their browser straight to Stripe. They do not pass through Go Shliach.

Stripe is certified at PCI DSS Level 1 — the highest level defined for handling payment card data, and the same standard the major banks and national retailers are held to. They handle the card. We handle the record of the gift.

So the split is clean: Stripe knows the card, Go Shliach knows that Mrs. Cohen gave $360 to the Purim campaign on the fourth of March and was sent receipt 1042.

Payment notifications coming back from Stripe are verified by signature before they are believed. A message claiming "this donation succeeded" that was not actually signed by Stripe is rejected, so a forged notification cannot create a donation record or a receipt in your books.

> There is no card number inside Go Shliach to steal. The one kind of data that gets taken for money is not in our possession at all.

Getting into an account

Accounts are created deliberately, protected by a second factor if you want one, and revocable the moment something feels wrong.

Invite only

Nobody signs themselves up into your workspace. An account exists because someone with authority in your organization invited that person by email, and invitations expire — an old invite left sitting in an inbox stops working.

Passwords are never stored in readable form

Passwords are one-way hashed by the authentication service. They are not stored, logged, or visible to us — nobody at Go Shliach can look up or tell you your password, which is exactly the property you want.

Two-factor authentication

Available on every account, using a standard authenticator app. Turning it on means a stolen password alone is not enough to get in.

Remembered devices, stored as hashes

So your staff is not typing a code every morning, a device can be remembered for up to 30 days. The cookie that does it is HTTP-only, secure, same-site strict, and bound to one person — and only a hash of it is kept, so a stolen copy of the database yields hashes, not usable cookies.

Revocation on demand

A password reset or a forced sign-out ends existing sessions, and remembered devices can be revoked for an account in one action — the thing you need when a laptop goes missing.

Who can see what inside your workspace

Six roles, matched to how a Chabad house office actually divides its work — and enforced in two places, not one.

Owner and admin hold the keys: settings, billing, members. Staff run the CRM day to day — contacts, households, programs, campaigns, communications. Bookkeeper works the money: payments, receipts, deposits, bills, categories. Volunteer logs visits and follow-ups. Viewer reads.

The important detail is that a role is not only an interface. Every restriction is applied twice: once by the application, so a person sees a clear message rather than a confusing error, and

again by the database policies described above, so the restriction holds even if a request never goes through the interface at all.

> A volunteer who is handed a laptop that is already signed in still cannot open your donation history.

A record of who did what

Administrative actions are written down as they happen, with enough detail to reconstruct them later.

What each entry records

Who acted and under which email, what they did, which record they did it to, the values before and after the change, the IP address, the browser, and the timestamp.

Support access is not quiet

If the Go Shliach team needs to enter your workspace to fix a problem, that entry is logged like any other action. There is no silent mode.

Signing in as a user is deliberate and visible

The tool that lets support see exactly what you see is restricted to platform administrators, uses a single-use token, is recorded in the audit log, and shows a persistent banner for the whole session so it is obvious it is happening.

Deleting an organization is recorded too

A database trigger writes the audit entry, so the record of the deletion does not depend on the code path that performed it.

> You can answer “who saw this, and when?” with a record rather than a reassurance.

Hardening in the software

The measures below are the ones that stop an attack reaching your data through the website rather than through the database.

A strict content security policy

Every page declares what it is allowed to load and run. Scripts must come from us and carry a per-request token; plugins are refused outright; and any insecure request is upgraded to HTTPS. This is the control that blunts an injected-script attack.

The app cannot be framed

No other website may embed a signed-in Go Shliach page inside itself, which is what clickjacking depends on. The single exception is a published form's embed view — the one page designed to live on your own website — and it is matched by an exact pattern, not a loose prefix.

Incoming webhooks are verified

Messages from payment, email and mailbox providers are checked against their signatures before being acted on. Scheduled jobs authenticate with their own secret. An unsigned or wrongly signed request is discarded.

Public endpoints are rate limited

Submissions to public hosted forms are limited per address, so a public form cannot be used to flood your workspace with junk.

Input is validated on the server

What the browser sends is checked again on the server against a schema before it reaches the database. Client-side validation is a convenience; it is never the gate.

How your records are stored

Encrypted in transit and at rest, on managed infrastructure, backed up automatically.

In transit and at rest

Every connection is encrypted with TLS. The stored data is encrypted on disk.

Independently audited infrastructure

The managed database platform underneath Go Shliach holds a SOC 2 Type II report. That certification belongs to the infrastructure provider. Go Shliach has not completed its own SOC 2 audit and does not claim one.

Backed up

Automated backups run against the database so a hardware failure is not a loss of your history.

Kept in one place

Your records are not scattered across a dozen third-party tools that each need their own review. The fewer places donor data lives, the fewer places it can leak from.

What we will not do with your data

The commitments below are not conditional on a plan, a price, or a future change of ownership.

We do not sell it

Not to data brokers, not to fundraising vendors, not at any price.

We do not share your donor list

Not with another Chabad house, not with any umbrella organization, not with a third party.

We do not train AI on it

Your donors' records are not training material.

We do not advertise to your donors

They are your relationships. We have no business with them.

It stays yours

Leaving should be as available as joining, or the promises above are worth less than they look.

Export

Your records export to CSV on request — contacts, donations, receipts and the rest, in a format you can open in a spreadsheet or load into another system.

Deletion

We will delete your organization's data on request, subject only to the tax, legal, billing and fraud-prevention retention your own organization and ours are bound by. Where something must be retained, we will tell you what and why.

No hostage-taking

Access to your own records is not a lever we use in a billing dispute. A workspace that is frozen for non-payment becomes read-only, not sealed shut.

If you find a security problem

We would much rather hear about a weakness from you than read about it later.

Write to hello@goshliach.com with what you found and how to reproduce it. We will confirm we received it, tell you what we found when we have looked, and let you know when it is fixed.

We will not threaten or pursue anyone who reports a genuine problem in good faith and does not access, alter, or keep data belonging to another organization while investigating it.

An honest word about limits

No system is unbreakable, and a vendor who tells you otherwise is selling something.

So here is the other side of the ledger, plainly. Go Shliach has not completed a SOC 2 audit of its own; the report referenced above belongs to the infrastructure underneath us. We do not publish a third-party penetration test. We do not offer a contractual uptime guarantee. If any of those are requirements for your board, we would rather you know now than discover it during a review.

What we can tell you plainly is this. We hold less than you would expect. What we do hold is separated at the database level rather than by application code that could forget. Access is scoped by role and recorded when it is used. And the category of data that is actually worth stealing — payment card numbers — is never in our hands.

If a board member or a donor has a question this document does not answer, write to us. We would rather answer it than have you guess.

If this leaves a question unanswered, ask it.

We would rather answer a board's question directly than have anyone guess. Write to hello@goshliach.com.

This document describes how Go Shliach is built and operated as of the date on the cover. It is a description of our practices, not a warranty or a certification. The SOC 2 Type II report referenced above belongs to the managed infrastructure provider underneath Go Shliach; Go Shliach has not completed an audit of its own and does not claim one.