bibly.run

SECURITY OVERVIEW · MAY 2026

How we protect your race data.

A plain-English summary of the security behind bibly.run.

LAST FULL AUDIT	AUDIT CADENCE	PAYMENTS	HOSTING
May 2026	Weekly + Monthly	Stripe	Supabase
Clean — 0 findings	Automated	PCI-DSS Level 1	SOC 2 Type II

OUR APPROACH

Security as a daily discipline.

Bibly handles two things organisers care about most: runner registration data and event payments. Security is built in, not bolted on. The platform runs on industry-standard infrastructure and is audited continuously — both by automated checks and through human review.

HOW WE PROTECT YOUR DATA

Six layers, one promise.

Payments	Card and payment data is processed by Stripe, a PCI-DSS Level 1 certified provider. Bibly never stores raw card numbers — they are tokenised by Stripe before they ever reach our systems.
Database access	Every database query runs under row-level security: runners only see their own registrations, organisers only see their own events, and admin access is restricted and audited. Sensitive fields (bank details, payout information) are protected by stricter rules and never exposed to public or runner-level requests.
Encryption	All traffic to bibly.run is encrypted with TLS 1.2+, and our domain enforces HTTPS via HSTS. The full Bibly stack — front-end, API, database, and storage — is HTTPS-only.

Authentication	User logins are handled by Supabase Auth with bcrypt-hashed passwords, JWT-based session tokens, and per-role access scopes.
Browser hardening	Bibly sets a strict Content Security Policy that locks down where scripts, images, and connections can originate from. The policy is narrowed to our specific Supabase project — never a wildcard — so a compromise of an unrelated service can't reach our app.
Hosting	Bibly runs on Lovable (application hosting) and Supabase (database, auth, storage). Both providers carry SOC 2 Type II attestations. Cloudflare sits in front of the domain to mitigate DDoS and bot traffic.

CONTINUOUS AUDITING

How we stay clean over time.

Security gets quietly worse as code changes and new features ship. To prevent drift, Bibly is audited on an automated, recurring schedule:

Cadence	What's checked	Outcome
Weekly	Live response headers, TLS, database access rules, recent code changes, secret scan	Quiet pass, or alert to founder
Monthly	Full audit — every database table, all user roles tested for cross-account access, dependency vulnerabilities, repository review	Scored report with action items
Quarterly	Threat-model review, new attack-surface analysis, compliance posture	Plan adjustments
Ad-hoc	Triggered by major changes (new payment method, new integration, vendor disclosure)	Targeted deep dive

Each audit produces a versioned report. Findings are triaged by severity and tracked to closure.

WHAT WE'VE SHIPPED

Recent security work.

Our most recent audit (May 2026) was completed end-to-end. Highlights:

Database row-level security

Hardened access controls on organiser profiles, payment settings, and race data so that sensitive fields (bank account numbers, payout configuration, internal review notes) cannot be retrieved by public or runner-level requests.

Narrowed Content Security Policy

Replaced wildcard domain entries with the exact Supabase project host. Reduces the blast radius of any hypothetical compromise of an unrelated Supabase project.

HSTS preload-ready configuration

Configured the app to emit HSTS only on HTTPS responses with the preload directive, in line with RFC 6797 §7.2. Submission to the browser-vendor preload list is in progress.

Recurring audit automation

Weekly and monthly audits are now automated end-to-end, with score tracking and alerting.

RESPONSIBLE DISCLOSURE

Found something? Tell us.

If you believe you've found a security issue affecting Bibly, we want to hear about it. Please email security@bibly.run with a description of the issue and steps to reproduce. We aim to acknowledge reports within 48 hours and resolve confirmed issues promptly. We do not pursue legal action against researchers acting in good faith within the scope described on our website.

WHAT WE HOLD

Runner data, by default minimal.

We collect only the information needed to register a runner for an event and process payment:

- Name, contact email and phone — to communicate event information
- Emergency contact — shared with organisers as required for safety
- Date of birth and category — for race-category placement and age-graded results
- Payment confirmation token from Stripe — never the underlying card details
- Optional: dietary requirements, medical notes, T-shirt size — only when the event requests them

Runners can request export or deletion of their data at any time by emailing privacy@bibly.run. Organisers are bound by our data-processing terms when handling runner information.

SHARED RESPONSIBILITY

Security is a partnership.

Bibly secures the platform. Organisers secure their accounts and how they use data. Runners secure their own credentials. Here's how it splits:

	Bibly	Organiser	Runner
Platform availability & infrastructure security	●		
Application-level access controls (row-level security)	●		
Payment processing security (PCI-DSS via Stripe)	●		
Database backups and disaster recovery	●		
Continuous auditing & monitoring	●		
Strong organiser account password & 2FA		●	
Sharing organiser dashboards only with trusted staff		●	
Handling exported runner data lawfully (GDPR / HK PDPO)		●	
Strong runner account password			●
Keeping contact details up to date			●

Bib. Run. Repeat.

Questions? security@bibly.run · www.bibly.run · #BibRunRepeat