

MostlyQR security pack

Security questionnaire answers, sub-processors, SLA and continuity commitment - Mostly Tiny Ltd

Last updated: 2026-10-06

Security questionnaire (CAIQ-Lite / SIG-Lite)

These are our answers to the questions in the CSA CAIQ-Lite and the Shared Assessments SIG-Lite that apply to a small SaaS company. They describe MostlyQR, run by Mostly Tiny Ltd (company 17282011, England and Wales). Where something is not in place yet we say so, and say what is planned. Questions we have not covered: security@mostlytiny.io.

Company and scope [SIG: Enterprise risk management]

- Who provides the service? Mostly Tiny Ltd, a small UK software company. MostlyQR is one of its products; all of them share the same infrastructure and controls.
- What does the service do with customer data? It stores customers' codes, destinations, hosted pages and forms, and records scan analytics about the people who scan their codes. For scan data and form submissions we act as the customer's processor under our Data Processing Agreement (mostlyqr.com/legal/dpa).
- Do you hold a SOC 2 report or ISO 27001 certificate? No. Neither audit has been carried out. A SOC 2 Type I readiness programme is planned; we will publish the report on mostlyqr.com/security when one exists.
- Has the service had an independent penetration test? Not yet. When one is commissioned, a summary will be published on mostlyqr.com/security.

Data residency and hosting [CAIQ DSP / SIG: Cloud hosting]

- Where is customer data stored? The database — codes and their destinations, hosted pages and form submissions, scan analytics and account records — is Google Cloud Firestore in the EU multi-region eur3 (Belgium and the Netherlands). Server functions, which process requests, run in Google Cloud region europe-west2 (London, United Kingdom). Uploaded files (logos, images and print assets) are stored in Google Cloud Storage in us-east1 (United States). Sign-in uses Firebase Authentication, which Google runs only in the United States, and an account signed in with a Mostly Tiny account is held by Mostly Tiny ID, whose database is in Google Cloud's US multi-region nam5. The scan map's latest scan location for each code and a short trail of recent ones are kept by Vekta, our map and location-data service, which runs on Cloudflare (Workers, Durable Objects and R2). Transfers to Google LLC in the United States rely on the UK Extension to the EU-US Data Privacy Framework (and, for data under the EU GDPR, on the EU-US Data Privacy Framework), to both of which Google LLC is certified; personal data under the EU GDPR reaches our servers in the UK under the European Commission's adequacy decision for the UK (Implementing Decision (EU) 2021/1772, as amended by Implementing Decision (EU) 2025/2574).
- Which providers run the infrastructure? Google Cloud / Firebase (hosting, database, storage, functions, sign-in) and Cloudflare (DNS, CDN and security in front of the mqr.sh scan domain and the status page; and hosting and storage for Vekta, the service that keeps the scan map's latest locations). The full list of sub-processors, with locations, is at mostlyqr.com/legal/subprocessors.
- Is the scan domain separated from the application? Yes. Scans are served from a dedicated domain (mqr.sh) and hosting target, separate from mostlyqr.com, so a customer's destination can never run in the application's origin.
- Do you notify customers of new sub-processors? Yes — at least 30 days before an addition or replacement, by email and on the sub-processor list, with a right to object (DPA, "Sub-processors").

Encryption [CAIQ CEK / SIG: Data security]

- Is data encrypted in transit? Yes. All MostlyQR endpoints — mostlyqr.com, mqr.sh and the REST API — are served over HTTPS (TLS).
- Is data encrypted at rest? Yes, by the platform: Google Cloud encrypts all data at rest by default (Google-managed keys).
- Customer-managed keys (BYOK)? No.
- How are API keys stored? Only a SHA-256 hash of each key is stored; the full key is shown once at creation, compared in constant time, and displayed afterwards only as a masked prefix and last four characters.

Identity and access management [CAIQ IAM / SIG: Access control]

- How do customers sign in? Passwordless: an email sign-in link, or "Sign in with Mostly Tiny" through our identity service (id.mostlytiny.io). MostlyQR stores no passwords.
- Single sign-on (SAML) and SCIM? Yes, on Business and Enterprise. SAML 2.0 single sign-on runs through our identity service, Mostly Tiny ID, with any SAML 2.0 identity provider (tested with Okta, Microsoft Entra ID and Google). An organisation is linked to its MostlyQR workspaces: its SSO can be required for sign-in, and SCIM provisions and deprovisions MostlyQR seats (deprovisioning also ends the person's MostlyQR sessions).
- Multi-factor authentication? Yes. A workspace owner or admin can require two-factor sign-in for every seat; a second factor is a passkey verified at Mostly Tiny ID or sign-in through the organisation's linked SSO. A member without one is sent to enrol before reaching the workspace, and an admin can only turn the requirement on from a two-factor session of their own.
- Role-based access? Yes. Each workspace has four roles: owner, admin, member (can create and edit codes) and viewer (read-only). Only owners and admins manage members and settings; only the owner changes roles.
- Audit log? Yes. Code changes (create, edit destination, delete) and membership and security-policy changes (invites, joins, removals, role changes, SCIM provisioning, policy changes) are recorded in an append-only workspace log that owners and admins can view, export as CSV and stream to a SIEM as signed webhooks.
- Tenant isolation? Every record belongs to one workspace, and database security rules plus server-side role checks restrict reads and writes to that workspace's members. A verified custom domain only ever serves its own workspace's codes.
- API access? REST API keys are per workspace, available on paid plans, revocable at any time, and rate-limited to 120 requests per minute per key.

Application and interface security [CAIQ AIS / SIG: Application security]

- Malware and phishing protection? Yes. Every destination — and every routing-rule destination and hosted-page link — is checked against Google Web Risk plus our own heuristics. Free-plan and new accounts are checked before a change is saved; all accounts are checked again on every change and re-scanned every 24 hours. A blocked code stops redirecting, shows a neutral warning page with a way to report it, and its owner is emailed.
- Abuse reporting? Yes, at mostlyqr.com/report and abuse@mostlytiny.io, under our Acceptable Use Policy.
- Bot protection on public forms? Yes. The contact and support forms are protected by Cloudflare Turnstile.
- Secure development? Every change runs automated unit and end-to-end tests in CI, and a deploy gate refuses a release whose recorded test run does not match the code being deployed. Production releases go out from the main branch only.
- Dependency vulnerability scanning? Yes. GitHub Dependabot watches the dependencies of every product and opens update pull requests weekly, and Dependabot security alerts are enabled.
- Security headers (HSTS, CSP)? Yes. HSTS is served on all our web hosting (max-age one year).

mostlyqr.com also sends X-Content-Type-Options (nosniff), a Referrer-Policy (strict-origin-when-cross-origin) and frame protection (a Content Security Policy frame-ancestors rule). A full Content Security Policy runs in report-only mode while we tune it; enforcing it is planned.

Business continuity and resilience [CAIQ BCR / SIG: Business resiliency]

- What happens to printed codes if a customer cancels or downgrades? They keep working. A redirect depends only on the code's own status, never on the plan: codes over the new plan's limit are frozen (read-only) and keep redirecting to their last destination.
- And if MostlyQR itself shut down? Codes keep working for as long as MostlyQR operates. If that ever changes, customers get at least 12 months' notice and a full export of every code's destination, and can point their own custom domain at another provider so codes printed on it keep working under their control; we use reasonable endeavours to transfer the redirect service to a successor. For Enterprise and annual Business contracts we are adding a contractual commitment that, while MostlyQR operates, codes keep resolving (read-only) for at least two years after the contract ends (pending legal review).
- Can customers take their data with them? Yes: the REST API lists every code with its destination and scan analytics, serialized campaigns export as a file, and the redirect-table export (Settings -> Export) produces the whole table in one file. A custom domain can be pointed at another provider at any time.
- Monitoring and availability? Scans, the website, the API, hosted pages and analytics are checked every 60 seconds from two independent regions by status.mostlytiny.io, which publishes live status, incidents and uptime history and lets customers subscribe to notifications.
- Service level? 99.9% monthly uptime for code scans. Service credits apply to Enterprise contracts (or an order form that includes the SLA); on other plans, Business included, 99.9% is our published objective and the status page is public, without credits — see mostlyqr.com/sla.
- Backups? Yes. The database runs on Google Cloud's replicated multi-region storage, with point-in-time recovery (a 7-day window) and a daily backup schedule whose backups are retained for 14 days.

Logging, monitoring and incident response [CAIQ LOG, SEF / SIG: Incident management]

- Do you log security-relevant events? Yes. Server functions write structured logs (for example blocked destinations and cross-tenant attempts) to Google Cloud Logging, and front-end errors are captured by our product analytics.
- How are incidents communicated? On status.mostlytiny.io/mostlyqr: an incident is published with updates at least every 30 minutes (15 for critical incidents) until resolved, following our incident-communication playbook.
- Do you notify customers of personal-data breaches? Yes — without undue delay after becoming aware of a breach affecting their data, with the information they need for their own obligations (DPA, "Personal data breaches").
- How can researchers report a vulnerability? security@mostlytiny.io, published in [/.well-known/security.txt](https://well-known/security.txt). We have no paid bug bounty.

Privacy and data lifecycle [CAIQ DSP / SIG: Privacy]

- What scan data is recorded? On paid plans: time, country and region, browser, operating system and device type, language, referring page, routing outcome, an approximate location rounded to about 1 km, and a salted one-way hash of the IP address. The full IP address, full browser string and city are never stored. On the free plan only a scan count and last-scan time.
- How long is it kept? For the life of the account, within the plan's analytics limits, or until the customer deletes the code. Per-code scan trails on the map expire after 30 days.
- What happens when a customer deletes their account? All workspace data is deleted — scan events, pages and form submissions, API keys, integrations, serialized data and uploaded files. Codes are tombstoned (kept only as a reserved, empty record) so a printed code can never be re-registered by

someone else; they then show "This code is no longer active".

- Is customer data used for anything else? No. We do not sell it or combine it with other customers' data (DPA, "Subject-matter").

People and policies [CAIQ HRS, GRC / SIG: Human resources, Governance]

- Written information-security policies and staff training? Not yet formalised. Access to production is limited to the company's founder; written policies, access reviews and training are part of the planned SOC 2 readiness programme.
- Confidentiality? Everyone we authorise to process customer data is bound by confidentiality (DPA, "Confidentiality").
- Customer audits? We answer written questions and share documentation, and allow audits as set out in our DPA ("Information and audits").

Sub-processors

The third parties that process personal data for MostlyQR customers, as published at mostlyqr.com/legal/subprocessors (our Data Processing Agreement is at mostlyqr.com/legal/dpa).

- Google Cloud and Firebase (Google) — MostlyQR - database (codes and destinations, hosted pages, form submissions, scan analytics and account records), server functions, and uploaded logos, images and print assets. Location: database in the EU (eur3 multi-region: Belgium and the Netherlands, with a witness replica in Finland); server functions in the UK (europe-west2, London); uploaded logos, images and print assets in the United States (us-east1).
- Google Cloud and Firebase (Google) — MostlyPDF - database (account, usage and billing records), file processing, and the files you upload and their outputs. Location: database in the United States (nam5 multi-region); file processing, uploaded files and outputs in the UK (europe-west2, London).
- Google Cloud and Firebase (Google) — MostlyRender - database (account, templates and usage records), rendering, uploads and rendered outputs. Location: database in the United States (nam5 multi-region); rendering, uploads and rendered outputs in the UK (europe-west2, London).
- Google Cloud and Firebase (Google) — MostlyPrivacy - database (documents, websites, consent records and privacy requests), server functions, and stored files (document and consent-log exports, banner logos). Location: database in the United States (nam5 multi-region); server functions in the UK (europe-west2, London); stored files in the United States (us-east1).
- Google Cloud and Firebase (Google) — Mostly Tiny ID - database (accounts, organisations, single sign-on and SCIM records, wallet ledger) and server functions. Location: database in the United States (nam5 multi-region); server functions in the UK (europe-west2, London).
- Firebase Authentication (Google) - sign-in for every product (email address, sign-in records, and the IP address and browser used to sign in). Location: United States (Google runs it only in the United States).
- Firebase Hosting (Google) - serving every product's website and app files (sees visitors' IP addresses). Location: Google's global network.
- Stripe - payments and billing records for every paid product. Location: United States and EU.
- Resend - transactional email (sign-in links, receipts, notifications) for every product. Location: United States.
- Cloudflare - DNS, CDN and security; bot checks (Turnstile); approximate location for mqr.sh scan links; status.mostlytiny.io; hosting and storage for Vekta, the service behind MostlyQR's scan map. Location: global edge network.
- PostHog (EU Cloud) - product analytics inside our apps, only with consent. Location: EU (Germany).
- Fathom Analytics - cookie-free website statistics. Location: Canada (UK and EU adequacy decisions).
- Anthropic - the MostlyPDF AI assistant (text is deleted within 30 days and not used for training). Location: United States.
- Google Web Risk and Safe Browsing - malware and phishing checks on MostlyQR destinations (the

destination address only). Location: United States.

MostlyQR Service Level Agreement

This Service Level Agreement ("SLA") sets out the availability we commit to for MostlyQR code scans, how we measure it, and the service credits you receive if we miss it. It applies to business customers on a MostlyQR Enterprise contract, and to any other customer whose order form says that it includes this SLA. On every other plan, Business included, the same target is our published objective and the status page is open to you, but no service credits are due. This SLA takes effect on 1 November 2026.

1. What is covered

The covered service is MostlyQR code scans: a request to a MostlyQR short link being answered by our redirect service — with a redirect to the code's current destination, or with the page our redirect service shows for that code before the redirect (a passcode prompt, or a request to share the scanner's location for a location-based rule). This is the component called "QR code scans" on our status page. Short links on a custom domain that MostlyQR serves for you are answered by the same redirect service and are covered in the same way.

Not covered by the service credits below: the website, the dashboard, the builder, the REST API, scan analytics, and hosted pages — the digital business cards, link pages, landing pages and forms published at mostlyqr.com/p/..., including when a code opens one. We monitor all of them on the same status page and work to the same standard, but scan redirects are what your printed codes depend on, so they are what this SLA guarantees.

2. Our commitment

We will make the covered service available at least 99.9% of the time in each calendar month (UTC). That allows about 43 minutes of downtime in a 30-day month.

3. How availability is measured

- What we probe. Our status service (status.mostlytiny.io) sends a real scan to a dedicated canary code on mqr.sh from two independent network regions, and checks that it is answered with the expected redirect. Custom domains are served by the same redirect service but are not probed separately, so the measurement is the one taken on mqr.sh.
- How often. Each region checks every 60 seconds. While an outage is confirmed, checks back off and run less often (at most every 5 minutes) until the service recovers.
- When downtime starts and ends. A failure counts only once it is confirmed: three consecutive failed checks, seen in both regions. Downtime runs from that confirmation — the minutes of the three checks that confirmed it are not counted — until the service is confirmed working again (two consecutive successful checks). A failure seen from one region only is investigated but not counted, because it usually means a problem with that region's network rather than with MostlyQR.
- How a minute is weighted. A major outage counts as a full minute of downtime, a partial outage (some scans failing) as 0.3 of a minute, and degraded performance (slow but working) as no downtime. Because we probe a single canary code, our monitoring itself records scans as either working or down; a partial outage is recorded only when we declare one in a published incident on the status page.
- Incidents and corrections. What we publish on the status page feeds the measurement too. A published incident that declares the "QR code scans" component down counts as downtime even when our probe did not see it. Our operators can also correct the record when the probe is wrong — for example a false alarm caused by the monitoring itself — either for a past period or by setting the component's state directly while an event is under way. A correction takes precedence over both the probe and any published incident for the minutes it covers, so it can reduce counted downtime. Every correction is logged with who made it, when, the period and state it covers, and a written reason, and that log is kept for at least 24 months. If you make a claim, we will show you every correction that affects the period you claim for, with its reason; if we cannot show a reason for a correction that reduced your downtime, we will disregard that

correction for your claim. Raw probe checks are kept for 14 days; the per-minute record built from them, and the correction log, are kept for the whole claim period.

- Monthly Uptime Percentage = $100\% \times (1 - \text{downtime minutes} \div \text{eligible minutes})$. Eligible minutes are all the minutes in the month, minus any minutes in an excluded event (section 5) and any minutes in which our own monitoring could not take a measurement. Unmeasured minutes are never counted as available.
- The same measurement drives the public uptime history on the status page (<https://status.mostlytiny.io/mostlyqr>), which publishes a 90-day uptime figure for each component once 30 days have passed since its first day of measurements, so you can check our arithmetic. If your own monitoring disagrees with ours, send us your data with your claim and we will review both.

4. Service credits

If the Monthly Uptime Percentage falls below the commitment, you are entitled to a credit against the MostlyQR fees for the affected month (one twelfth of the annual fee on an annual plan):

Monthly Uptime Percentage | Service credit

Less than 99.9% but at least 99.0% | 10% of the monthly fee

Less than 99.0% but at least 95.0% | 25% of the monthly fee

Less than 95.0% | 50% of the monthly fee

- How to claim. Ask through MostlyQR support (support@mostlyqr.com) within 30 days after the end of the affected month. Tell us the account and the dates and times you were affected.
- How it is paid. We apply the credit to your next invoice. Credits are capped at 50% of the fees for the affected month and cannot be transferred. They have no cash value, except that if your contract ends, an unused credit for the final month is refunded.
- Service credits are your sole and exclusive remedy for our failure to meet this SLA, except where the law does not allow our liability to be limited in that way.

5. What is excluded

Downtime does not count against the commitment when it is caused by:

- your destination being down, slow or blocking visitors — MostlyQR still redirects correctly to it;
- your own DNS for a custom domain being changed, expired or misconfigured, or a certificate we cannot renew because the domain no longer points at MostlyQR;
- a code, page or account that we suspended or disabled under our Terms of Service or Acceptable Use Policy, or because the law requires it;
- your breach of the Terms, or traffic you send that exceeds your plan's documented limits;
- features labelled beta, preview or experimental;
- events beyond our reasonable control (force majeure), such as a failure of the public internet outside our and our providers' networks. A failure of our own hosting or network providers (Google Cloud, Cloudflare) is not excluded.

We do not schedule maintenance that takes scan redirects offline: under our maintenance policy the scan redirect never closes for maintenance, so planned maintenance windows elsewhere in the product never count as scan downtime.

6. Status and incident communication

- Live status, incidents, maintenance windows and uptime history: <https://status.mostlytiny.io/mostlyqr>
- You can subscribe there to email notifications for MostlyQR, or for the "QR code scans" component only.
- During an incident we post updates at least every 30 minutes (every 15 minutes for a critical incident) until it is resolved.

7. Changes

We may update this SLA. We will not reduce the commitment or the credits during a term you have already paid for, and we give at least 30 days' notice of any change that is less favourable to you.

Continuity commitment (codes outlive your contract)

Status: approved; it takes effect from 2026-11-01 as part of our Terms.

Continuity after your subscription ends. If you are a business customer on an Enterprise plan or an annual Business plan, or on any plan whose order form includes this continuity commitment, then when your paid subscription or order-form term ends — because it expires or because either of us ends it, other than for your material breach — Mostly Tiny Ltd will keep every short link and dynamic QR code you created redirecting for at least two years after the end date, for as long as we operate the service, at no further charge. Ending your subscription does not require you to delete your account, and your account stays open on our free plan unless you choose to delete it.

During that period, codes beyond the limits of the plan you are then on are read-only: you cannot change their destinations or routing rules, and analytics beyond a scan count may stop. On a plan without routing (such as our free plan), each code redirects to its last saved default destination; on a plan with routing, its saved routing rules keep applying. Before and after the end date you can export your redirect table (every code with its destination) from your dashboard and point any custom domain you own at another provider.

If we ever decide to discontinue the service, we will give you at least 12 months' notice, keep your codes resolving and your redirect-table export available throughout that notice period, and let you point any custom domain you own at another provider so that the codes printed on it keep working under your control. We will also use reasonable endeavours to transfer the redirect service, including our short-link domain, to a successor that takes on this commitment.

This commitment does not cover: a code you delete; your codes if you delete your account or ask us to erase your data, because that removes your codes and they stop redirecting (export your redirect table first); or a code we disable because its destination breaches our Acceptable Use Policy or the law, or that we must disable by law.