



TRUST CENTER / DPA

This is a draft. No clause is binding until it is reviewed and signed. Its security annex and sub-processor annex were corrected on 2026-10-09 to describe production as it is today.

Current version: 2026-09.

[Download PDF](#)

[Accept in your workspace settings](#)

Data Processing Addendum

Last updated: 2026-10-09

This page summarises the CMDash Data Processing Addendum. It is available on request for any CMDash Cloud customer and forms part of the Master Services Agreement when incorporated by reference. A PDF is available for download below, or from `legal@cmdash.com` for a copy with your organization's details pre-filled.

"Legal note. The text on this page — including the Annexes below — is a structural scaffold engineering has assembled from the product's actual mechanisms (see each Annex's own sourcing note); it is DPA available, counsel review pending. Sections and Annex rows marked `[counsel]` are placeholders for counsel's final language, not CMDash's binding legal position. Nothing on this page constitutes legal advice, and no clause here is executable until counsel has reviewed it and it has been signed."

Parties and scope

This Addendum applies between CMDash, Inc. ("Processor") and the customer ("Controller") whenever the Controller uses CMDash Cloud to process personal data. For on-premise deployments where CMDash never receives customer data, the DPA applies only to the limited categories of operational telemetry the Controller opts into (support diagnostics, error reports).

The Addendum is governed by the General Data Protection Regulation (EU) 2016/679 and the UK General Data Protection Regulation, each as amended, along with applicable member-state and successor laws.

GDPR Article 28 obligations

CMDash processes Controller Personal Data only on documented instructions from the Controller, in line with GDPR Article 28(3) and the equivalent UK GDPR provisions. The Addendum sets out:

- the subject matter and duration of processing (as long as the Controller maintains an active subscription, plus a limited post-termination retention window for final export);
- the nature and purpose of processing (provision of the CMDash security-and-compliance platform);
- the categories of data subjects (Controller's personnel, contractors, and any other individuals whose data the Controller imports);
- the rights and obligations of the Controller (retention of overall responsibility for lawful basis, notice, data-subject rights).

CMDash requires all personnel authorised to process Controller Personal Data to be under confidentiality obligations and to undergo security awareness onboarding.

Security measures (Article 32)

CMDash implements the technical and organisational measures described in the [Security overview](#). In summary: encryption in transit and at rest, per-tenant row-level security, role-based access control, audit logging, MFA for administrative access, segregated environments, and a documented incident-response process.

Subprocessors

The Controller grants the Processor general written authorisation to engage subprocessors for the provision of the service. A current, dated list of engaged subprocessors is published at </trust/subprocessors>.

CMDash will notify subscribing Controllers at least 30 days before engaging a new subprocessor or replacing an existing one. The Controller may object on reasonable data-protection grounds; if the parties cannot agree on a resolution within 30 days of the objection, the Controller may terminate the affected part of the service without penalty.

International transfers

Where processing of Controller Personal Data involves a transfer outside the European Economic Area, the United Kingdom, or Switzerland to a jurisdiction that is not the subject of a valid adequacy decision, the parties rely on the European Commission's **Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914 of 4 June 2021), Modules 2 and 3 as applicable, together with the UK Addendum issued by the Information Commissioner's Office where the UK GDPR applies. Swiss data flows follow the same SCCs adapted per FDPIC guidance.

CMDash conducts a Transfer Impact Assessment documenting the relevant supplementary measures (encryption in transit and at rest, audit log coverage, challenge of unlawful access requests) and makes the assessment available to the Controller on request.

Binding Corporate Rules fallback. If the SCCs become invalid or unavailable for a category of transfer, and adequate Binding Corporate Rules are in force for the relevant subprocessor, the parties will rely on those BCRs for the affected transfer until an alternative SCC package is agreed.

SCC module

CMDash processes Controller Personal Data solely on the Controller's instructions and never determines the purposes and means of that processing itself, so the primary relationship this Addendum documents is Controller-to-Processor: **Module Two** of the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914). Module Two, its optional clauses, the governing-law and forum choices in Clause 17/18, and whether a Module Three (processor-to-sub-processor) docking is needed for any subprocessor's own onward transfer are confirmed by counsel before execution — this section states which module applies, not the fully completed clause text. `[counsel]`

Data-subject rights assistance

CMDash provides the Controller with functionality within the CMDash platform to support the Controller's fulfilment of data-subject rights: machine-readable data export (Article 20 portability), user deletion and tenant deletion with cascading removal (Article 17), access logs for access requests (Article 15), and rectification through the standard user-profile editor (Article 16).

Where a data subject contacts CMDash directly with a rights request, CMDash will forward the request to the Controller without undue delay rather than respond on the Controller's behalf.

Personal data breach notification

CMDash will notify the Controller without undue delay and in any case within 72 hours of becoming aware of a Personal Data Breach affecting Controller Personal Data. The notification will describe, to the extent known, the nature of the breach, categories and approximate number of data subjects and records concerned, the likely

consequences, and the measures taken or proposed to address the breach and mitigate its effects.

Audit rights

CMDash makes available to the Controller the information necessary to demonstrate compliance with Article 28, including the SOC 2 report (once published — see [/trust/soc2](#)), the pen-test summary, and any additional evidence reasonably required. Where a Controller requires an on-site audit, CMDash will cooperate in scoping a mutually agreeable review; costs are to be borne by the Controller unless the audit uncovers material non-compliance.

Return or deletion on termination

On termination of the service, CMDash will, at the Controller's election, return or delete Controller Personal Data within 30 days, save where retention is required by applicable law. The current cascade-delete behaviour on tenant offboarding is documented in the SOC 2 control mapping (CC6.5). New evidence attachments, evidence-package archives and data exports are sealed under a per-tenant data key; on offboarding those keys are destroyed first, which makes the sealed objects unreadable. Other files and the database are not sealed with per-tenant keys and are deleted directly. A database backup taken before a key was destroyed still holds that key in wrapped form until the backup ages out.

Annex I — Parties and description of processing

Parties.

	Name	Role
Controller	The customer identified on the applicable order form, or the organization whose CMDash account is used to accept this Addendum	Controller
Processor	CMDash, Inc.	Processor

Subject matter. Provision of the CMDash security-and-compliance dashboard (posture scoring, compliance tracking across NIST CSF, CMMC, SOC 2, and other frameworks, AI-assisted risk narratives, and board-ready reporting) to the Controller and its authorised users.

Duration. For as long as the Controller maintains an active CMDash subscription, plus the post-termination return/deletion window in "Return or deletion on termination" above.

Nature and purpose of processing. Hosting, storage, and processing of the Controller's account, organization, and security-posture data so the CMDash application can compute and display posture scores, track compliance evidence, generate reports, and — where the Controller enables it — produce AI-assisted narratives and suggestions (see the subprocessor list for the AI provider and what it receives).

Categories of data subjects. The Controller's personnel, contractors, and any other individuals whose data the Controller imports into the product (for example, named risk owners, policy approvers, or vendor contacts).

Categories of personal data. Account and identity data (name, work email, role); organization and security-posture data the Controller connects from its own tools; application usage and audit-log data generated by using the product. CMDash does not require the Controller to submit special-category data, and the product is not designed to process it.

Processing operations. Collection, storage, retrieval, structuring, display, and (where the Controller opts in) AI-assisted analysis of the categories above, plus the export and deletion operations described elsewhere in this Addendum. This Annex is a factual scaffold drawn from the product's own mechanisms; counsel confirms it matches the final agreement scope. `[counsel]`

Annex II — Technical and organisational measures

These measures are the ones actually implemented today, as published in full on the Security overview and mapped to SOC 2 Type II criteria in `docs/compliance/soc2-`

`type-ii-controls-mapping.md``; this Annex is a summary of that page, not a separate claim:

- **Identity and access.** Bcrypt-hashed passwords (8-character minimum on register and reset; no breached-password check), TOTP multi-factor authentication with single-use hashed recovery codes, SAML 2.0 SSO and SCIM v2 provisioning for enterprise tenants, and JWT access tokens (15-minute lifetime) with rotating, hashed refresh tokens.
- **Authorisation and tenant isolation.** Row-level security policies, enforced at the database, on every tenant-scoped table; role-based access control (Owner/Admin/Viewer plus custom roles) applied uniformly through per-endpoint guards; every write attributed to an acting user in the audit log.
- **Encryption.** TLS in transit with HSTS. The load balancer's TLS policy currently accepts older protocol versions than the target and is being tightened; this Annex does not commit to a minimum TLS version until that is done. At rest, object storage uses server-side AES-256 with S3-managed keys; the production database is a Lightsail managed PostgreSQL instance whose at-rest encryption mechanism is not documented in CMDash's infrastructure code and is not asserted here. New evidence attachments, evidence-package archives and data exports are additionally sealed with AES-256-GCM under per-tenant data keys. No AWS KMS key protects customer data at rest.
- **Transport and application security.** A strict HTTP response-header set applied independently in both the web application and the API; documented application-security controls covering input validation and dependency management.
- **Logging, monitoring, and incident response.** Structured application and security-event logging, operational metrics and dashboards (automated alerting is written but not yet applied to production), and a documented incident-response process (see "Personal data breach notification" above for the customer-facing commitment it backs).
- **Secrets management.** Production secrets are held in an environment file on each host, outside images and source control; AWS Secrets Manager holds the database credential and the JWT signing secret only.

- **Supply chain.** Container images are scanned and signed (Cosign, release key pair) in the release process before publication; dependencies are tracked and updated through the standard release pipeline.
- **Availability and recovery.** A Lightsail managed PostgreSQL database with automated daily snapshots and point-in-time recovery; application instances distributed across availability zones behind a load balancer. There is a single region (us-east-1), no cross-region backup replication and no secondary region.

See "Encryption in transit and at rest" on the Security overview page for the current state. Counsel confirms this Annex's wording matches what the signed agreement should represent as a guaranteed commitment versus a description of current practice. `[counsel]`

Annex III — Sub-processors

The table below mirrors [/trust/subprocessors](#) — the single source of this list — as of its last review date, **2026-10-09**. That page, not this table, is authoritative if the two ever disagree; this Annex is regenerated from the same

```
`packages/shared/src/subprocessors/catalog.ts` catalog by
`scripts/legal/render-dpa-annex-iii.mjs`.
```

<!-- annex-iii:start (generated by scripts/legal/render-dpa-annex-iii.mjs) →

| Sub-processor | Purpose | Region | Transfer mechanism |
|---------------------------|--|---------------------------|----------------------|
| Amazon Web Services, Inc. | Cloud infrastructure (Lightsail compute, load balancer and managed PostgreSQL database; S3 object storage). For customers who subscribe through AWS Marketplace, AWS also resolves the subscribing AWS account, reports entitlements, and receives hourly usage quantities (AWS Marketplace Metering Service). | United States (us-east-1) | SCCs + AWS DPA |
| GitHub, Inc. (Microsoft) | Container registry (GHCR) and source-code hosting | United States | SCCs + Microsoft DPA |

| Sub-processor | Purpose | Region | Transfer mechanism |
|---------------|---|---|--------------------|
| Stripe, Inc. | Subscription billing and payment processing | United States (EU processing for EEA customers) | SCCs + Stripe DPA |
| Resend, Inc. | Transactional email delivery (password reset, magic link, notifications) | United States | SCCs + Resend DPA |
| PostHog, Inc. | Product analytics for the tenant dashboard (SaaS only — never deployed on-prem) | United States (PostHog Cloud US) | SCCs + PostHog DPA |
| HubSpot, Inc. | CRM sync for marketing leads (contact-form submissions, white-paper requests, quote-builder requests). Disabled by default (<code>`CRM_SYNC_ENABLED=false`</code>); this entry is disclosed regardless of the flag's current value because the capability is shipped and this list must not lag a config change (see #554). | United States | SCCs + HubSpot DPA |

| Sub-processor | Purpose | Region | Transfer mechanism |
|--|--|---|---|
| Google LLC (Google Analytics 4) | <p>Web analytics on the public marketing site (cmdash.com): page views and marketing-funnel events such as pricing and CTA clicks. In the browser, Google Analytics loads only after the visitor accepts the cookie banner (Consent Mode v2; all storage denied by default, no browser requests to Google before consent). On the app sign-up and email-verification pages it can also load to continue a visit that began on the marketing site. Separately, when the operator has configured it, CMDash servers send two conversion events (a marketing form submitted, a free account created) to the Google Analytics Measurement Protocol; those server-side events are not conditioned on the cookie banner and carry a synthetic identifier when the visitor has no Google cookie. Not loaded in the authenticated product screens or in any on-premise deployment.</p> | United States (global collection endpoints) | Consent (cookie banner) for browser analytics + SCCs + Google Ads Data Processing Terms |
| Google LLC (Sign in with Google) | Optional OAuth 2.0 sign-in and sign-up for users who choose "Continue with Google", where the deployment has Google sign-in configured. Not used unless the user clicks it. | United States (global) | User-initiated sign-in (contract) + Google API Services terms |
| Microsoft Corporation (Sign in with Microsoft) | Optional OpenID Connect sign-in and sign-up for users who choose "Continue with Microsoft", where the deployment has Microsoft sign-in configured. Not used unless the user clicks it. | United States (global) | User-initiated sign-in (contract) + Microsoft privacy statement |

| Sub-processor | Purpose | Region | Transfer mechanism |
|--|--|-------------------------------|--|
| Cloudflare, Inc. | Two narrow uses. (1) Turnstile: the bot check on app account sign-up (loaded from challenges.cloudflare.com on the registration page, and verified server-side before an account is created). (2) The 1.1.1.1 DNS-over-HTTPS resolver, used for customer-directed external-exposure DNS lookups (see the exposure-intelligence rows below). Cloudflare is not a CDN, DNS host or proxy for any CMDash site or for application traffic. | Global edge | Legitimate interest (abuse prevention) for Turnstile + SCCs + Cloudflare DPA |
| Google LLC (Google Public DNS) | Fallback DNS-over-HTTPS resolver (dns.google) used for customer-directed external-exposure DNS lookups when the primary resolver fails. | United States (global) | Public DNS query; no customer data beyond the queried name + Google Public DNS terms |
| crt.sh (Certificate Transparency log search) | Customer-directed lookup of the publicly logged TLS certificates for domains a customer registers for exposure monitoring (certificate-transparency monitoring). A failed or malformed answer is recorded as unknown, never as "no new certificates". | Not specified by the operator | Public lookup service; no DPA (query contains only a public domain name) |
| Shodan InternetDB | Customer-directed lookup of the public IP addresses behind domains a customer registers for exposure monitoring (open ports and known vulnerabilities seen by the internet scanner). Runs in the daily IP-reputation sweep for organizations whose plan includes IP reputation; needs no API key. | Not specified by the operator | Public lookup service; no DPA (query contains only a public IP address) |

| Sub-processor | Purpose | Region | Transfer mechanism |
|---|--|---|---|
| GreyNoise
(Community API) | Customer-directed lookup of whether a public IP address of a registered asset is seen scanning or attacking the internet. Runs in the daily IP-reputation sweep for organizations whose plan includes IP reputation; the Community endpoint needs no API key. | Not specified by the operator | Public lookup service; no DPA (query contains only a public IP address) |
| AbuseIPDB | Customer-directed lookup of the abuse-report history of a public IP address of a registered asset. Used only when an AbuseIPDB API key is configured (a key the customer supplies, or one the operator holds). | Not specified by the operator | Customer-directed lookup under the AbuseIPDB terms; no DPA |
| DNS blocklist operators
(SpamCop, UCEPROTECT, Mailspike, PSBL, GBUIDB, blocklist.de and, with a customer-supplied key, Spamhaus ZEN) | Customer-directed check of whether a public mail-sending IP address of a registered asset is listed on a DNS blocklist. These are DNS queries sent through the DNS-over-HTTPS resolvers above; the blocklist operator sees a query for the reversed IP address under its zone. | Not specified by the operators | Public DNS lookup; no DPA (query contains only a public IP address) |
| Anthropic, PBC | Hosted AI model (Claude) for AI-assisted policy drafting, policy-control link autosuggestion, vendor-questionnaire auto-answer, the daily AI risk narrative, AI executive-summary generation, and AI risk-remediation suggestions | United States (data stored in the US); customer API traffic may by default be routed for processing to the US, Europe, Asia, or Australia per the Anthropic DPA | SCCs (Module 2/3) + UK/Swiss Addenda + Anthropic DPA |

<!-- annex-iii:end →

Signature

This Addendum is effective when signed below by an authorised representative of each party, or accepted electronically by an Owner through the Controller's CMDash workspace settings (see ``apps/api/src/legal/legal.service.ts``'s acceptance record — who accepted, when, and from where). The clause text above is a scaffold; counsel confirms final wording before either signature is collected. ``[counsel]``

For the Controller

Signature: _____

Name: _____

Title: _____

Date: _____

For the Processor (CMDash, Inc.)

Signature: _____

Name: _____

Title: _____

Date: _____

Request the DPA for signature

An OWNER can record acceptance of the current version above. To receive the PDF with your organization's details pre-filled, or to negotiate changes, email legal@cmdash.com. We aim for a first response within two business days.