KVRUN TRUST CENTRE

Security and compliance questionnaire

Last updated 2 November 2026 · kvrun.com/trust

This document sets out where KVRUN LTD's compliance stands and answers the questions security and procurement teams ask most often. The live version at kvrun.com/trust is always current; check it if this copy is more than a few months old.

Compliance status

ISO/IEC 27001

UNDERWAY

We are building our information security management system (ISMS) towards ISO/IEC 27001 certification with the British Assessment Bureau, targeting the Stage 2 audit by the end of January 2027. Our controls are already aligned to the standard. We are not yet certified.

UK GDPR and EU GDPR

COMPLIANT

We act as processor for your content under a Data Processing Addendum. Inference stays in the UK by default.

EU AI Act

COMPLIANT

Article 5 practices are prohibited by our acceptable use policy. Output is machine-marked under Article 50. Every fine-tune keeps an evaluation record.

ISO/IEC 27001 journey

Certification is underway with the British Assessment Bureau, targeting completion of the Stage 2 audit by the end of January 2027. We update the roadmap as each stage completes, and publish the certificate on the trust centre when it is granted.

- **1. Controls aligned to ISO/IEC 27001** — COMPLETE
  Encryption, access control, logging, vendor review and incident response designed against Annex A.
- **2. ISMS scope, policies and risk assessment** — COMPLETE
  ISMS scope defined, policy set written, risks assessed and the Statement of Applicability produced.
- **3. Internal audit and management review** — IN PROGRESS
  Testing the ISMS with an internal audit, then a management review, before the external audits begin.
- **4. Stage 1 audit** — PLANNED
  The British Assessment Bureau, our certification body, reviews our ISMS documentation and readiness.
- **5. Stage 2 audit and certification** — PLANNED
  The British Assessment Bureau tests our controls in operation. We publish the certificate here when it is granted.
  Target: End of January 2027

Company and certifications

Who is the legal entity providing the service?

KVRUN LTD, a company registered in England and Wales under company number 17504024. Registered office: 150 Fulmar Lane, Wellingborough, England, NN8 4AY.

Which security certifications do you hold?

None yet. We are working towards ISO/IEC 27001 certification, and our controls are already aligned to it. We never claim a certification we do not hold, and we will publish the certificate in our trust centre when it is granted.

Where are you in the ISO/IEC 27001 process?

Our ISMS is in place: the scope, policy set, risk assessment and Statement of Applicability are complete. We are now at the internal audit stage, followed by management review. The Stage 1 and Stage 2 external audits come next, as set out in our ISO/IEC 27001 roadmap. We are targeting completion of the Stage 2 audit by the end of January 2027.

Who is your certification body?

The British Assessment Bureau, which will carry out both the Stage 1 and the Stage 2 audits.

Do you have a SOC 2 report?

No. The platform produces evidence that maps to SOC 2 controls, such as per-tenant key isolation for CC6.1 and the continuous audit log for CC7.2. We do not hold a SOC 2 report. SOC 2 is on our longer-term roadmap, but there is no timeline yet.

Do you hold cyber insurance?

Yes. We hold cyber insurance. Details of the cover are available on request.

Who is responsible for security?

Our Security Lead, Atley Hunter, owns the information security programme and the ISO/IEC 27001 ISMS. Reach the security team at compliance@kvrun.com.

Do you have a Data Protection Officer?

We have not appointed a Data Protection Officer. Data protection is overseen by our Security Lead, and all data protection queries go to compliance@kvrun.com.

Will you complete our security questionnaire?

Yes. Most answers are in this questionnaire, which you can download as a PDF from our trust centre (kvrun.com/trust). Send anything else to compliance@kvrun.com and we will answer it in writing.

Can we carry out a security review or audit of kvrun?

Yes, on reasonable notice. We will take part in calls, answer follow-up questions and share supporting documents under NDA. Audit rights for processing of personal data are set out in the Data Processing Addendum.

Data protection and privacy

Are you a controller or a processor of our data?

We are processor for your content: datasets, prompts, outputs and fine-tuned models. We are controller only for the account, billing and usage data we need to run the service. See the privacy policy (kvrun.com/privacy).

Do you offer a Data Processing Addendum?

Yes. It meets Article 28 of the UK GDPR and the EU GDPR and forms part of our terms (kvrun.com/terms). Request a copy from compliance@kvrun.com.

Do you use our data to train models?

No. We do not use your content to train, fine-tune or improve any model, for ourselves or for any other customer. A fine-tuning run uses your data only to produce your own model.

Who owns our data and fine-tuned models?

You do. You keep all rights in your datasets, prompts, outputs and fine-tuned model artifacts. We claim no ownership of them.

Do you use sub-processors?

Yes. The current list is published in the sub-processors table on our trust centre (kvrun.com/trust#sub-processors). Each one is security-reviewed before onboarding and bound by an Article 28 contract. Processing locations and transfer safeguards for each are available from compliance@kvrun.com.

Will you tell us when sub-processors change?

Yes. Team owners get 30 days' notice by email of any material addition or replacement, and you may object on reasonable data protection grounds under the Data Processing Addendum.

How do you handle international transfers?

Where personal data leaves the UK or the EEA, we use Standard Contractual Clauses with the UK Addendum, or rely on an adequacy decision, and add supplementary measures where needed.

How do you support data subject requests?

For your content, we pass on requests we receive and help you, as controller, respond to them. For data we hold as controller, we respond within one month.

Data residency

Where is our data processed?

In the United Kingdom. Inference runs on dedicated GPUs that kvrun operates in London by default, so the inference path stays in the UK. No third party provides our GPU compute.

Where is our data stored?

Object storage and backups are held in a UK region. If you have a specific residency requirement, tell us before you upload data and we will confirm the configuration in writing.

Can we run kvrun in our own cloud account?

Yes. The console can place deployments in your own connected cloud account or on self-hosted infrastructure, so the data stays inside your own environment.

Data retention and deletion

Do you keep our prompts and responses?

Stateless deployments keep no request content on the server. Context in the governed KV cache is held only for the session, and you can erase it at any time.

Can you prove data has been deleted?

Yes. A session is erased by destroying its encryption keys. Every copy, on every storage tier, becomes unreadable at once. Each erasure issues a certificate within a minute.

How long do you keep logs and records?

Security logs for 12 months, or longer when an investigation needs them. Billing records for six years, as tax law requires. Account data for the life of the account, then under our retention schedule.

What happens to our data when the contract ends?

Running deployments and jobs are torn down. You can export your content before the end date. After that we delete or return it under the Data Processing Addendum and our retention schedule. Training instances are already torn down after every job.

Are backups erased too?

Yes. Backups are encrypted, and cryptographic erasure applies to them, so destroying the keys makes the backed-up copies unreadable as well.

Encryption and key management

Is data encrypted in transit?

Yes. Our website and console use TLS, and kvrun.com sends HSTS. A deployment endpoint is served over HTTPS once you attach a custom domain, and we issue and renew its certificate. A new deployment answers over plain HTTP at its IP address until a domain is attached, so attach one before you send sensitive data.

Is data encrypted at rest?

Yes. Every block in the governed KV cache is sealed with AES-256-GCM, on every tier: GPU memory, host memory, local disk and object storage. Local storage on a deployment, where enabled, files held in object storage, backups, and any keys you store with us are also encrypted at rest.

How are encryption keys managed?

Every tenant has its own key hierarchy, with keys unique to the workspace and session. Keys are never shared between tenants. Destroying a key erases the data it protects.

How are API keys protected?

API keys are scoped to a workspace or deployment and stored hashed. A key is shown once, when it is created, and can be rotated at any time from the console.

Tenant isolation and infrastructure

How is our data kept apart from other customers' data?

Each tenant runs on dedicated GPUs, so compute is never shared. Each tenant has its own keys and KV cache, and prefix caching never crosses tenants.

Can another customer reuse our cached context?

No. Cached blocks are encrypted under your keys and are never shared across tenants.

How is network access controlled?

Every deployment has its own firewall and source allowlist. A request from an address outside the allowlist is dropped before it reaches the model, whatever key it carries.

What hardware and software do you run on?

NVIDIA A100 and H100 GPUs operated by kvrun, or GPUs in your own connected cloud account, serving open models such as Qwen, Gemma, Mistral and DeepSeek. The governance layer sits between the serving engine and cache storage, and works with vLLM, SGLang, TensorRT-LLM and llama.cpp.

Access control

How is access to our workspace controlled?

Team owners invite members and assign role-based permissions from the console. Every API request needs a valid deployment key and a source address on that deployment's allowlist.

Do you support single sign-on?

Yes. Single sign-on (SSO) is supported, so your identity provider controls who can sign in to your workspace.

Who at kvrun can access our data?

Only staff who need it to run or support the service, on a least-privilege basis. Staff access to production systems is logged.

Is multi-factor authentication enforced for staff?

Yes. MFA is enforced for every staff account on every system we use.

Logging, monitoring and audit

What do you log?

Every allocation, access, movement and erasure of KV cache data goes to an append-only audit log. Production systems are logged and monitored.

Can we get audit evidence?

Yes. You can export the audit log from the console with one click, mapped to the controls your auditors test.

Incident response

Do you have an incident response plan?

Yes. We have a documented plan for detecting, triaging, containing and recovering from security incidents, and for reviewing them afterwards.

How and when will you tell us about a breach?

We will notify you within 48 hours of becoming aware of a personal data breach affecting your data, so you can meet your own duties. We notify regulators as the law requires, within 72 hours.

How do we report a security issue or vulnerability?

Email compliance@kvrun.com with the details and steps to reproduce. Please give us reasonable time to fix the issue before disclosing it.

Security testing

Do you carry out penetration testing?

Yes. We run internal penetration tests, and an independent third-party penetration test is planned. Once it is complete, we can share a summary of the findings and the fixes under NDA.

Backups and business continuity

How is data backed up?

Backups are encrypted and stored in Wasabi Cloud Storage, in a UK region. Cryptographic erasure applies to backups, so erased data cannot be restored from them.

Do you have business continuity and disaster recovery plans?

Yes. We maintain documented business continuity and disaster recovery plans, with KPIs that we monitor to check they work.

People

Do you screen staff?

Yes. Every member of staff is background-checked before they are given access.

Do staff receive security training?

Yes. All staff complete security training.

Are staff bound by confidentiality?

Yes. All staff sign confidentiality agreements.

AI governance

How do you comply with the EU AI Act?

Practices prohibited under Article 5 are banned by our acceptable use policy (kvrun.com/acceptable-use). AI-generated output is machine-marked under Article 50. Every fine-tune keeps an evaluation record with its weights.

Can you show an evaluation for each fine-tuned model?

Yes. Each training run records an evaluation, which is stored with the weights and mapped to the EU AI Act articles it answers to.

Where do base models come from?

Base models are pulled from established third-party model repositories, and each is subject to its own licence, such as Apache 2.0 or the Gemma Terms.

What uses of the service do you prohibit?

Our acceptable use policy (kvrun.com/acceptable-use) prohibits Article 5 practices and unlawful or harmful uses. We may suspend a team immediately for prohibited or high-risk use.

Contracts and service

Do you offer a service level agreement?

Service levels apply when agreed in a separate written SLA. Contact legal@kvrun.com to discuss one.

What are the termination terms?

Either party can end the agreement on 30 days' notice, or for a material breach that is not fixed within 30 days. You can close your account at any time.

Where can we read your policies?

Our terms of service (kvrun.com/terms), privacy policy (kvrun.com/privacy), acceptable use policy (kvrun.com/acceptable-use) and cookie policy (kvrun.com/cookies) are published in full. The Data Processing Addendum is available on request, and the sub-processor list is published on our trust centre

(kvrun.com/trust#sub-processors).

Sub-processors

Each is security-reviewed before onboarding and bound by an Article 28 contract. Team owners get 30 days' notice of any material change.

Scaleway	Web application hosting
Enigma Net	Infrastructure and networking (UK)
MongoDB Atlas	Database hosting
Wasabi Cloud Storage	Object storage and encrypted backups (UK)
Cloudflare	Edge network, DNS, TLS and website hosting
Hanko	Authentication
Stripe	Payment processing
Google Workspace	Internal email and documents
Atlassian (Jira and Confluence)	Internal ticketing and documentation
HubSpot	Customer relationship management
PostHog	Website analytics (EU cloud), only with consent
Google (Tag Manager and Ads)	Website advertising measurement, only with consent

Contact

Security, data protection and compliance: compliance@kvrun.com

Contracts, terms and abuse reports: legal@kvrun.com

KVRUN LTD, company number 17504024, registered in England and Wales.