SECURITY, PRIVACY, AND PROCUREMENT

Simple8 Security Pack

A concise review package for service architecture, model operation, data flow, retention, access, incident handling, and customer responsibility.

Simple8 operates its service and model infrastructure in Germany. Customer content is processed to create and deliver the requested language version and is not used to train shared models.

Simple8 GmbH | Version 1.0 | 2026

Scope and product contract

- One source text, one supported locale, and exactly one language mode per request.
- Plain Language and Easy Language are separate modes.
- The output remains in the selected source language.
- All 24 documented locales use the same explicit request contract.
- Generated content is a reviewable draft and requires accountable human approval before publication.

Infrastructure location

Simple8 service and model infrastructure is operated in Germany. The documented processing path applies to every supported content locale. Infrastructure location does not limit language availability.

External model providers

Customer content is not sent to OpenAI, Anthropic, Google, Microsoft, or another external model API for generation. The Simple8 security review separates model processing from non-model infrastructure and service providers.

Data flow

1. **Customer system or browser.** The user or connected system sends source content, locale, and mode over encrypted transport.
2. **Simple8 service in Germany.** The service validates the request, applies access and usage controls, and creates or retrieves the result.
3. **Model operation in Germany.** The selected language version is generated within the managed processing environment.
4. **Reviewable response.** The result returns with request, locale, mode, status, and cache metadata needed by the workflow.
5. **Customer-controlled review and publication.** The customer decides whether the draft is approved, stored, integrated, or published.

Data categories

Category	Purpose	Control
Account and project data	Contract, access, and administration	Role and project controls
Request content	Create the selected language version	Purpose-limited processing
Result and cache data	Deliver or reuse matching content	Tenant isolation and invalidation controls
Security logs	Protect, monitor, and investigate	Restricted operational access
Usage records	Capacity, limits, and billing	No source or output text in analytics events

Retention, cache, and deletion

Account data, request logs, cached content, usage records, and backups are separate categories. Production agreements document the applicable retention period and available controls for each category.

- Matching cache requests are isolated by customer, source content, locale, mode, and relevant model version.
- Cache behavior and cache status are visible in the technical contract.
- Shorter contractual retention can be agreed where workflow and operating requirements allow it.
- Deletion, invalidation, export, and backup treatment are documented for production.
- Customer content is not used to train or fine-tune shared models.

Customer responsibilities

Use public, representative content in the public demo. Apply the agreed production process before sending personal, confidential, medical, legal, or otherwise protected content.

Access, encryption, and operations

- TLS protects data in transit.
- Production data stores use encryption at rest.
- Internal access follows role-based and least-privilege controls.
- Customer credentials can be scoped, rotated, and revoked.
- Production access and security events are reviewed.
- Operational logging supports incident investigation without placing protected content in analytics events.

Availability and incidents

The public status page shows current component state, planned maintenance, and incident communication. Production service commitments and remedies are defined in the applicable plan or contract.

Incident communication includes

- Timestamp and affected components
- Observed customer impact
- Mitigation and current state
- Resolution and follow-up action

Procurement evidence index

Evidence	Purpose	Review owner
Security overview	Architecture and control summary	Security and IT
Data-flow description	Processing path and responsibilities	Privacy and architecture
AVV/DPA terms	Controller and processor obligations	Legal and privacy
Technical and organizational measures	Control design	Security
Subprocessor list	Relevant service providers	Privacy and procurement
Retention and deletion policy	Data lifecycle	Privacy and operations
Model and training policy	Model operation and content use	AI governance
SLA and incident process	Availability and response	Operations and legal
Accessibility statement	Digital accessibility	Accessibility and legal

Assurance boundary

A hosting location or control statement does not by itself establish certification, legal compliance, or suitability for a specific risk. Customers should review the current contract package and apply their own legal, privacy, security, accessibility, and AI-governance assessment.

Security review checklist

- Confirm the exact production architecture and relevant providers.
- Confirm the data categories used by the selected workflow.
- Confirm retention, cache, deletion, and backup terms.
- Confirm account, API-key, role, and support-access controls.
- Confirm incident, maintenance, and service-level terms.
- Confirm whether protected content is in scope for the agreed environment.
- Confirm reviewer ownership and publication responsibility.
- Confirm accessibility and AI-governance responsibilities.

Contact

Security and procurement questions: hallo@simple8.de
Company and registration details: simple8.de/imprint