mcpgate — Security Whitepaper

*For prospective customers and procurement teams. Version 1.0 · 2026-05-30. Every claim in this document is backed by the internal ISMS (Statement of Applicability v1.0) and verifiable evidence. mcpgate is **aligned with ISO/IEC 27001:2022 Annex A controls — not (yet) certified**; no accredited body has audited the management system.*

---

1. What mcpgate is

mcpgate is a self-hostable AI gateway: it sits between AI clients (e.g. Claude, ChatGPT) and your existing tools (Jira, GitLab, Google Workspace, Slack, …) over the Model Context Protocol. It is a **pass-through** — tool actions land in your own systems; mcpgate holds the minimum data necessary to operate (an encrypted, short-lived PII-pseudonym mapping; OAuth tokens; an audit log).

2. Security architecture (built into the product)

- **Encryption.** OAuth tokens and sensitive data are encrypted at rest (Google Cloud KMS or AES-256-GCM). All traffic is TLS; HSTS is enforced.
- **Authentication & access.** OpenID Connect / OAuth 2.0 with PKCE; per-service authorization; an explicit allow-list guest model; token-gated administration.
- **PII & privacy.** Personal data is pseudonymized before it reaches an LLM and rehydrated only for the actual tool call (mapping encrypted, short TTL). Logs use hashed identifiers — no raw emails or IPs.
- **Auditability.** Sign-ins, tool calls, and admin actions are written to an append-only audit log with hashed identifiers; exportable to your SIEM.
- **Data-leak guardrails.** Destructive actions require explicit confirmation; response sizes are capped; a throughput view surfaces unusual data pulls.

3. Secure development & supply chain

Every release runs through CI with **automated dependency vulnerability scanning** (Renovate, pip-audit, Trivy), **static analysis** (Bandit), and a **security test suite** that must pass before a build ships. Releases are versioned with a public CHANGELOG. Known-but-unfixable advisories are explicitly tracked and risk-accepted, not silently ignored.

4. Hosting & data residency (mcpgate-operated services)

The hosted services (`demo.mcpgate.de` , `mcpgate.de` , the `api.mcpgate.de` feedback relay) run in the **European Union — Hetzner, Falkenstein, Germany** — on infrastructure certified to **ISO/IEC 27001:2022 and BSI C5**. Backups are nightly off-server full-disk images plus daily encrypted database

snapshots, with encryption keys escrowed off the server. **Self-hosted deployments run entirely on your own infrastructure** — see §6.

5. Logging, monitoring & incident response

Structured logging and metrics (Prometheus / Grafana / Loki) cover the operated services. A documented incident-response runbook defines severity levels, containment/eradication/recovery, a **coordinated vulnerability-disclosure** path, and a **GDPR Art. 33/34 breach-notification** procedure (72-hour clock). Report a vulnerability privately to **hello@mcpgate.de**.

6. Shared responsibility (self-hosted model)

Because you host mcpgate, security is shared. The split is framework-neutral and maps onto ISO 27001, SOC 2, and BSI C5. (M = mcpgate software · O = you, the operator · S = shared.)

Area	Resp.	mcpgate provides	You provide
Cryptography (data/tokens at rest, TLS)	M / S	KMS/AES-GCM encryption, HSTS	the key/KMS, TLS termination at your edge
Authentication & access	S	OIDC/OAuth+PKCE, per-service allow-list, admin gating	your IdP, who gets access, the policy
PII & data masking	M	pseudonymization before the LLM, log minimization	controller duties + DPAs with your users
Audit & monitoring	S	append-only audit log + metrics	ship to your SIEM; monitor
Secure development	M	dependency scanning, SAST, security tests on the image	keep your host patched
Backup	S	backup-target guidance (`OPERATIONS.md`)	run + test backups of your deployment
Network security	S	safe binds, reverse-proxy/TLS support	firewall, segmentation, the proxy
Host & physical	O	—	OS hardening, data-centre/cloud security
Configuration & secrets	S	safe defaults + `verify-setup.sh`	your `.env` / secret management

A **full per-control mapping (all 93 ISO 27001:2022 Annex A controls)** is available on request for your certification evidence.

7. Privacy & data protection

mcpgate is built privacy-first: cookie-free marketing site, no third-party tracking, PII pseudonymization as a core feature, GDPR data-subject rights (access, erasure, etc.) supported, defined retention with

automated purges. Data controller for the operated services: Andreas Kruse, Berlin, Germany.

8. Standards alignment

- **ISO/IEC 27001:2022** — the product's security management is built on and aligned with the Annex A controls; an internal ISMS (scope, policy, risk assessment + treatment, Statement of Applicability, records) is maintained and operated. **Not yet certified.**
- The same controls map to **SOC 2** Trust Services Criteria and **BSI C5** with minor relabeling.
- Hosting infrastructure (Hetzner) is independently **ISO 27001:2022 + BSI C5** certified.

9. Contact

- Security reports / questionnaires: **hello@mcpgate.de**
- Full control mapping for your audit: request via the same address.

This document describes capabilities present at the version date. "Aligned with ISO/IEC 27001 Annex A controls, not certified." We will state certification explicitly, with the certificate, once achieved.