PROC-K3 — Betrieb

Verantwortlich: R-OPS + R-COMP (bei DSGVO-relevanten Vorfällen) **Bezugsnormen:** ISO 9001 §8.7, §10.2 · DSGVO Art. 33, 34 · ISO 27001 A.12, A.16, A.17

Incident-Response

Klasse	Beispiele	DSGVO-Meldepflicht	Mandanten-Info
P0 Kritisch	Datenabfluss bestätigt, mehrere Mandanten	Ja, 72 h	„unverzüglich"
P1 Hoch	Pipeline-Down > 4 h, kein Datenabfluss	Bewerten	im selben Werktag
P2 Mittel	Bug mit fachlichem Fehler in einer Akte	Nein	nur betroffener Mandant
P3 Niedrig	Performance-Degradation, einzelne Fehler	Nein	Nein

Schritte: Detect → Contain → Investigate → Communicate (DSGVO 72 h falls P0 + personenbezogene Daten) → Recover → Post-Mortem (binnen 7 Tagen, blameless).

Eskalations-Kette: R-OPS → R-COMP (binnen 30 min bei P0/P1) → R-GF (binnen 1 h bei P0) → Aufsichtsbehörde BayLDA (72 h) → Mandanten (unverzüglich).

Backup, Disaster Recovery & Archivierung

Komponente	Mechanismus	Retention
Tägliches Backup	Cron 02:00 UTC, rsync verschlüsselt, getrennter Storage	30 d täglich + 12 Mo wöchentlich + 5 J monatlich
Restore-Drill	vierteljährlich Stichprobe-Workspace	Bericht in `audits/AUDIT-09/05_review_log.md`
DR-Konzept	RTO 4 h, RPO 24 h, Failover Helsinki → Frankfurt	Annual DR-Drill
10-Jahres-Archiv	Append-only Object-Storage mit SHA-256-Hash	nach Inverkehrbringen der Maschine

Wartung & Fernzugriff

Zugang-Typ	Erlaubt?
Logs lesen, systemd-Restart	ohne Mandant-OK
Mandanten-Workspace-Inhalte lesen / ändern	nur mit Portal-Approval des Koordinators (zeitbegrenzter Token 4 h)
Verschlüsselungs-Schlüssel-Zugriff	nur DR-Eskalation, GF-Freigabe

Architektur: **Bastion-Host** (einzige SSH-Tür, Key + 2FA) + **Portal-Approval** für Schreibzugriff + **Notarized Log** aller Sessions. Default ist Read-Only.

Notfall-Eskalation (wenn Mandant nicht erreichbar): R-GF + R-COMP-Dokumentation + Post-faktische Mandanten-Info + Post-Mortem.

Records

- `state.audit.incidents` (10 Jahre)
- Post-Mortem-PDFs (10 Jahre)
- Aufsichtsbehörden-Meldungen (10 Jahre, gesonderte Vertraulichkeit)
- SSH-Session-Logs Bastion + Notarized Log (5 Jahre)
- `state.audit.wartung_approvals[]` (5 Jahre)
- Backup-Logs (1 Jahr)
- Restore-Drill-Berichte (dauerhaft)

KPI

KPI	Soll
MTTD bei monitorbar	≤ 30 min
MTTR bei P1	≤ 4 h
DSGVO-Melde-Quote rechtzeitig	100 %
Post-Mortem bei P0/P1	100 %
Backup-Erfolgsquote	≥ 99 %
Notfall-Eskalationen Wartung	≤ 2 / Jahr