Die Cloud-Exit-Checkliste

32 Punkte für den entspannten Wechsel von AWS/Azure/GCP zu europäischen Anbietern — in der Reihenfolge, in der sie in echten Projekten anfallen. Zum Abhaken gedacht, nicht zum Abheften.

Phase 1 — Bestandsaufnahme (vor jeder Entscheidung)

- ☐ Kosten-Report der letzten 3 Monate exportiert (Cost Explorer / Cost Management)
  Die Rechnung ist die ehrlichste Inventarliste.
- ☐ Vollständiges Service-Inventar erstellt: was läuft, wer nutzt es, wer ist Owner?
- ☐ Abhängigkeiten kartiert: Wer spricht mit welcher Datenbank, Queue, API?
- ☐ Zombie-Infrastruktur markiert (ungenutzte Instanzen, Volumes, IPs, alte Snapshots)
  Erfahrungswert: 5–15 % der Rechnung sind ersatzlos streichbar.
- ☐ Implizite AWS/Azure-API-Nutzung im Code gesucht (SDK-Aufrufe, Instance-Rollen)
- ☐ Datenvolumen erhoben: Datenbanken, Object Storage, Fileshares (für Sync-Planung & Egress-Kosten)

Phase 2 — Recht & Compliance

- ☐ Datenfluss-Karte erstellt: Welche personenbezogenen Daten liegen wo, fließen wohin?
- ☐ CLOUD-Act-Betroffenheit bewertet (US-Anbieter oder US-Mutterkonzern in der Kette?)
- ☐ AV-Verträge & Sub-Prozessoren-Listen der aktuellen Anbieter geprüft
- ☐ Anforderungen gesammelt: DSGVO, NIS2, Branchenstandards, Kundenverträge, Zertifikate
- ☐ Datenschutzbeauftragten / Kanzlei früh eingebunden — nicht erst beim Cutover

Phase 3 — Zielbild & Business Case

- ☐ Service-Mapping erstellt: Für jeden Service ein Ziel (EU-Äquivalent, Self-Hosted oder „bleibt vorerst“)
- ☐ Provider-Auswahl nach Anforderungsprofil (Preis / Compliance / Managed-Bedarf), nicht nach Bauchgefühl
- ☐ Betriebsmodell geklärt: Wer patcht, überwacht, reagiert nachts? (Team / Dienstleister / Managed)
  Die am häufigsten übersprungene Frage.
- ☐ Business Case gerechnet: Einsparung, Migrationskosten inkl. einmaliger Egress-Kosten, Break-even
- ☐ Rollback-Kriterien definiert: Woran erkennen wir, dass wir abbrechen — und wie geht das?

Phase 4 — Aufbau der Zielumgebung

- [ ] Zielumgebung als Infrastructure as Code aufgebaut (Terraform/Ansible), nichts von Hand
- [ ] Security-Baseline umgesetzt: TLS überall, 2FA/SSO, Firewall-Regeln, Least-Privilege-Zugriffe
- [ ] Monitoring & Alerting eingerichtet — vor dem ersten produktiven Byte
- [ ] Backup-Konzept nach 3-2-1 umgesetzt, Offsite bei zweitem EU-Anbieter, append-only/Object-Lock
- [ ] Restore-Test durchgeführt und protokolliert (RTO gemessen, nicht geschätzt)
  Ein Backup ohne Restore-Test ist ein Gerücht.
- [ ] Staging-Umgebung identisch zur Ziel-Produktion aufgebaut

Phase 5 — Migration & Parallelbetrieb

- [ ] Datenbank-Replikation zur Zielumgebung eingerichtet (Lag im Sekundenbereich)
- [ ] Object Storage initial synchronisiert, Delta-Syncs geplant (rclone o. ä.)
- [ ] Lasttest / Traffic-Replay gegen die neue Umgebung gefahren
- [ ] DNS-TTL rechtzeitig gesenkt (Tage vorher, z. B. auf 300 s)
- [ ] Cutover-Drehbuch geschrieben: Schritte, Verantwortliche, Zeitfenster, Abbruchkriterien, Rollback
- [ ] Alte Umgebung nach Cutover eingefroren 2–4 Wochen behalten (nicht sofort kündigen!)

Phase 6 — Nach dem Wechsel

- [ ] Doku & Runbooks übergeben: Deployment, Rollback, Incident-Prozesse
- [ ] Kosten-Monitoring etabliert: monatlicher Blick auf die neue Rechnung (Drift früh erkennen)
- [ ] Regelmäßige Restore-Tests im Kalender (mind. quartalsweise, mit Protokoll)
- [ ] Alt-Accounts aufgeräumt & gekündigt, Datenlöschung dokumentiert, AV-Verträge beendet

Alles abgehakt? Dann sind Sie weiter als die meisten.
Wenn Sie bei einzelnen Punkten Unterstützung möchten: Der Hygge Check liefert Inventar, Business Case und Migrationsplan zum Festpreis — Ergebnis in 2 Wochen. **hyggecloud.de · hallo@hyggecloud.de**

Diese Checkliste ist ein Praxis-Werkzeug, keine Rechtsberatung. Weitergabe ausdrücklich erwünscht. Stand: Juli 2026.