

LEITFADEN · CLOUD-MIGRATION

Cloud-Migration: Entscheidungsrahmen für KMU

Welche Workloads wohin gehören, wie Sie Anbieter neutral vergleichen und warum die Exit-Strategie vor dem ersten Umzug steht.

DAS ERHALTEN SIE

- Workload-Kategorisierung nach den 7 R
- Neutraler Anbietervergleich: Azure, AWS, OCI, Hetzner
- TCO-Kostenmodell und Governance-Grundlagen
- Compliance- und Exit-Checkliste

AUF EINEN BLICK

Für	**Geschäftsleitung, IT-Leitung, Projektverantwortliche**
Zeitbedarf	**ca. 2–3 Stunden Workshop**
Stand	**16. November 2026**
Version	**2.0**

Unverbindliche Praxishilfe – keine Rechtsberatung, kein Audit

1 Ausgangspunkt: Warum und was migrieren?

> Eine Migration beginnt mit Workload-Verständnis, Abhängigkeiten, Sicherheitsanforderungen und Kostenannahmen – nicht mit dem Anlegen einer virtuellen Maschine.

Klären Sie zuerst das Ziel: Ablösung alter Hardware, mehr Flexibilität, Standortunabhängigkeit, geringerer Betriebsaufwand oder bessere Ausfallsicherheit. Jedes Ziel führt zu anderen Entscheidungen. Nicht jede Anwendung gehört in die Cloud, und nicht jede sollte unverändert verschoben werden.

Workload-Steckbrief (je Anwendung)

- Geschäftsprozess, Eigentümer und Schutzbedarf
- Technik: Betriebssystem, Datenbank, Lizenzen, Schnittstellen
- Abhängigkeiten: Identität, Dateiablagen, andere Anwendungen, Hardware (Dongles, Scanner, Maschinen)
- Anforderungen an Latenz, Bandbreite, Verfügbarkeit, Datenstandort
- Aktuelle Kosten und geplante Restlaufzeit

2 Die 7 R: Strategie je Workload

Strategie	Bedeutung	Typisch für
Rehost (Lift & Shift)	Unverändert als VM in die Cloud	Schneller Rechenzentrums-Exit, stabile Anwendungen
Relocate	Ganze Virtualisierungsumgebung verschieben	Größere VM-Bestände mit kompatibler Cloud-Plattform
Replatform	Kleine Anpassungen, z. B. verwaltete Datenbank statt eigener	Weniger Betriebsaufwand ohne Neuentwicklung
Refactor	Umbau auf Cloud-native Dienste	Eigenentwicklungen mit Wachstumsbedarf
Repurchase / Replace	Durch SaaS ersetzen	E-Mail, Telefonie, CRM, Standardsoftware
Retain	Bewusst lokal belassen	Latenzkritische Produktion, Maschinenanbindung, Spezialhardware
Retire	Abschalten	Ungenutzte oder doppelte Anwendungen

Hybrid ist der Normalfall

Gerade in Produktion und Logistik bleiben Maschinen- und Robotersteuerungen sowie zeitkritische Datenwege meist vor Ort. Planen Sie die sichere Verbindung zwischen Standort und Cloud von Anfang an mit.

3 Anbieter neutral vergleichen

Die folgende Übersicht beschreibt typische Stärken und Prüfpunkte, keine Rangfolge. Leistungsumfang, Regionen und Preise ändern sich laufend; prüfen Sie den aktuellen Stand direkt beim Anbieter.

Anbieter	Typische Stärken	Prüfen Sie besonders
Microsoft Azure	Enge Integration mit Microsoft 365 und Entra ID; breites PaaS-Angebot; Rechenzentrumsregionen in Deutschland	Lizenzmodelle (z. B. Windows Server/SQL), Kostenkontrolle, Komplexität der Governance
Amazon Web Services	Sehr breite Dienstpalette, ausgereifte Automatisierung; Region in Frankfurt	Kostenstruktur (u. a. Datentransfer), benötigtes Know-how
Oracle Cloud Infrastructure	Stärken bei Oracle-Datenbanken und -Anwendungen; Region in Frankfurt	Ökosystem und Partnerverfügbarkeit für Ihre übrigen Anwendungen
Hetzner	Deutscher Anbieter mit Rechenzentren in Deutschland; einfache, transparente IaaS-Angebote	Weniger verwaltete Plattformdienste – mehr Eigenbetrieb nötig

Bewertungskriterien (gewichten Sie selbst)

Kriterium	Leitfrage	Gewicht
Datenstandort & Recht	EU-Region? Auftragsverarbeitungsvertrag? Drittlandübermittlung?	___ %
Identität & Integration	Passt der Dienst zu Ihrer Benutzerverwaltung und Ihren Anwendungen?	___ %
Betriebskompetenz	Können Sie oder Ihr Dienstleister die Plattform sicher betreiben?	___ %
Kosten (TCO)	Gesamtkosten über 3–5 Jahre inkl. Betrieb und Datenverkehr	___ %
Nachweise	Z. B. BSI C5-Testat, ISO/IEC 27001 – für die genutzten Dienste?	___ %
Exit-Fähigkeit	Daten und Konfiguration exportierbar? Offene Formate?	___ %

4 Kostenmodell (TCO)

Vergleichen Sie nicht Serverpreis gegen VM-Preis, sondern Gesamtkosten über denselben Zeitraum.

Heute (vor Ort)	Künftig (Cloud)
Hardware und Abschreibung, Ersatzteile	Rechen-, Speicher- und Datenbankdienste (nutzungsabhängig)
Strom, Kühlung, Raum, USV	Datentransfer, öffentliche IP-Adressen, Snapshots
Software-Lizenzen und Wartung	Lizenzmodell in der Cloud (eigene Lizenzen mitnehmen?)
Backup-Hardware und -Software	Backup und Disaster Recovery in der Cloud
Personalaufwand Betrieb	Personalaufwand für Governance, Kostenkontrolle, Sicherheit

Heute (vor Ort)	Künftig (Cloud)
—	Migrationsprojekt, Schulung, Parallelbetrieb

Häufige Kostenfallen

Dauerhaft laufende, überdimensionierte Ressourcen; vergessene Testumgebungen und Snapshots; Datentransfer aus der Cloud; fehlende Budgets und Alarme. Setzen Sie Budgets und Kostenalarme ab dem ersten Tag.

5 Governance, Identität und Netzwerk

Landing Zone

- Struktur aus Abonnements/Konten nach Umgebung (Produktion, Test)
- Einheitliche Namen und Tags (Kostenstelle, Eigentümer)
- Richtlinien: erlaubte Regionen, Pflicht-Verschlüsselung

Identität

- Zentrale Identität mit MFA, keine lokalen Einzelkonten
- Rollen nach minimalen Rechten
- Notfallzugänge (Break-Glass) dokumentiert

Netzwerk

- Verbindung Standort ↔ Cloud per VPN oder Direktverbindung
- Hub-and-Spoke mit zentraler Firewall
- Keine Verwaltungsports öffentlich erreichbar

Betrieb

- Monitoring, Protokollierung und Alarmierung
- Backup und Wiederherstellung getestet
- Patch- und Änderungsprozess definiert

Compliance

- Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abschließen; Unterauftragsverarbeiter prüfen.
- Datenstandort und mögliche Drittlandübermittlungen bewerten und dokumentieren.
- Verzeichnis von Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung bei Bedarf aktualisieren.
- Nachweise des Anbieters (z. B. BSI C5, ISO/IEC 27001) für die tatsächlich genutzten Dienste anfordern.

Exit-Strategie – vor dem Umzug festlegen

Dokumentieren Sie, wie Daten, Konfigurationen und Backups in offenen Formaten exportiert werden, wie lange ein Wechsel dauert und welche Abhängigkeiten von proprietären Diensten bestehen. Der EU Data Act stärkt seit September 2025 die Rechte von Kunden beim Wechsel von Cloud-Anbietern; die vertragliche und technische Umsetzung bleibt dennoch Ihre Aufgabe.

6 Migrationsplan und Checkliste

Phase	Inhalt
1. Bewerten	Workload-Steckbriefe, Strategie nach den 7 R, Anbieterauswahl, TCO
2. Vorbereiten	Landing Zone, Identität, Netzwerkverbindung, Backup, Monitoring
3. Pilot	Unkritische Anwendung migrieren, Abläufe und Kosten messen
4. Migrieren	In Wellen nach Abhängigkeiten; Rückfallplan und Wartungsfenster je Welle
5. Optimieren	Größen anpassen, Reservierungen prüfen, Altsysteme abschalten

	Prüfpunkt	Verantwortlich	Termin / Nachweis
VOR DER MIGRATION			
☐	Ziele und Erfolgskriterien sind schriftlich vereinbart.	_____	_____
☐	Jeder Workload hat Steckbrief und Strategie.	_____	_____
☐	TCO-Vergleich über 3–5 Jahre liegt vor.	_____	_____
☐	AVV und Datenstandort sind geprüft.	_____	_____
☐	Exit-Strategie ist dokumentiert.	_____	_____
WÄHREND UND DANACH			
☐	Rückfallplan je Migrationswelle ist getestet.	_____	_____
☐	Budgets und Kostenalarme sind aktiv.	_____	_____
☐	Backup und Restore in der Cloud sind getestet.	_____	_____
☐	Altsysteme sind sicher abgeschaltet und Daten gelöscht.	_____	_____

Quellen & weiterführende Referenzen

- BSI: Cloud Computing Compliance Criteria Catalogue (C5), bsi.bund.de
- Verordnung (EU) 2016/679 (DSGVO), insbesondere Art. 28 und Kapitel V
- Verordnung (EU) 2023/2854 (EU Data Act), Kapitel VI „Wechsel zwischen Datenverarbeitungsdiensten“
- Dokumentation der Anbieter zu Regionen, Landing Zones und Migrationsmethodik: Microsoft Cloud Adoption Framework, AWS Prescriptive Guidance, Oracle Cloud Infrastructure, Hetzner
- KONTORIT Wissen: „IT-Grundschutz für KMU“ und „Netzwerk-Design“ (kontorit.de/whitepaper)

Unterstützung gewünscht? KONTORIT begleitet kleine und mittlere Unternehmen in Hamburg bei Bestandsaufnahme, Umsetzung und Betrieb. Anfrage: **kontorit.de/kontakt** · E-Mail: **support@kontorit.de**

Dieses Dokument ist eine allgemeine, unverbindliche Orientierungshilfe. Es ersetzt keine individuelle Beratung, kein Sicherheitsaudit, keine Rechts- oder Steuerberatung und keinen Zertifizierungsnachweis. Produktfunktionen, Lizenzen und rechtliche Anforderungen ändern sich; prüfen Sie den aktuellen Stand anhand der genannten Quellen und Ihrer konkreten Umgebung. Genannte Marken gehören ihren jeweiligen Inhabern. © 2026 KONTORIT · Stand 16. November 2026 · Version 2.0