

# Cloud-Beschaffungen:

Besonderheiten bei Vergabe-,  
IT-Vertrags- und Datenschutzrecht

Varinia Iber | Dr. Fabian Bader

## Ausgangslage und Relevanz: Standard mit neuen Risiken

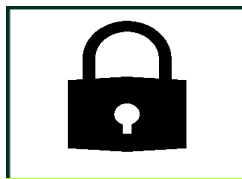
- **Cloud ist zentraler Baustein der Verwaltungsdigitalisierung**
- **Cloud ist politisch gewollt**
  - Digitale Souveränität
  - Standardisierung und Nachnutzung (z. B. Deutsche Verwaltungscloud → FITKO)
- **Zielbild: Souveränität, Kontrollierbarkeit, Exit-Fähigkeit**
- **Cloud-Beschaffungen im rechtlichen Kontext:**



Vergaberecht



IT-Vertragsrecht



DSGVO

# Teil 1: IT-Vertrag und Datenschutz

# Kernrisiken der Cloud

Cloud bedeutet die Auslagerung von Daten, Infrastruktur und Kontrolle. Das ist mit zentralen Risiken verbunden:

01

## Reduzierte Transparenz

- eingeschränkte Einsicht in technische Abläufe
- komplexe Unterauftragnehmerstrukturen
- faktische „Black-Box“-Systeme

02

## Abhängigkeit (Vendor Lock-in)

- proprietäre Technologien und Datenformate
- hohe Wechselkosten (technisch und wirtschaftlich)
- eingeschränkte Portabilität von Daten und Anwendungen

03

## Drittlands- und Zugriffsrisiken

- Zugriffsmöglichkeiten ausländischer Behörden trotz EU-Hosting
- rechtliche Bindungen des Anbieters (z. B. US-Recht)
- begrenzte/erschwererte Durchsetzbarkeit europäischer Schutzstandards

# IT-Vertragsrechtliche Gestaltung als Steuerungselement

## Struktur des Vertragswerkes:

- **Hauptvertrag als Steuerungsebene**
  - klare Governance-Regeln, Verantwortlichkeiten, Eskalationsmechanismen
- **ggf. Technischen Anlagen** verbindlich integrieren
  - API-Spezifikationen, Datenformate, Interoperabilitätsanforderungen, IT-Sicherheits- und Architekturvorgaben
- **ggf. Angebotsbestandteile des Anbieters**
  - beispielsweise Konzepte, technische Beschreibungen etc.
  - nur einbeziehen, soweit geprüft und freigegeben



Wichtig: Rangfolge der Vertragsdokumente definieren!

# IT-Vertragsrechtliche Gestaltung als Steuerungselement

## Wesentliche Regelungsbereiche des Cloud-Vertrages:

- **Leistungsbeschreibung**
  - funktional und messbar (inkl. Update-/Release-Zyklen)
- **Service Level + Sanktionen**
  - Verfügbarkeit, Performance, Datensicherung
  - klare Rechtsfolgen: Vertragsstrafen/Gutschriften, Kündigungsrechte
- **Datenschutz**
  - AVV nach Art. 28 DSGVO
  - Datenlokation + Drittlandtransfer inkl. Schutzmaßnahmen
- **Unterauftragsverhältnisse** (vollständige Transparenz + Zustimmungsvorbehalte/Wechselkontrolle)
- **Auditrechte und Berichtspflichten** (echte Prüfbarkeit, Zugriff auf Nachweise, Zertifizierungen, ggf. Vor-Ort-Prüfung)
- **Exit-Regelungen** (Fristen, Formate, Unterstützungspflichten)

Standardisierung: Nutzung der EVB-IT Cloud als Ausgangspunkt, aber Anpassung erforderlich !



Kontrollfrage: „Ist die Regelung praktisch überprüfbar und durchsetzbar?“ Ziel: Vermeidung von „Papier-Compliance“

# Datenschutzrechtliche Kernanforderungen

- **Abgrenzung: Verantwortlicher vs. Auftragsverarbeiter**
  - Verantwortlicher: entscheidet über Zwecke und Mittel (Art. 4 Nr. 7 DSGVO)
  - Auftragsverarbeiter: verarbeitet Daten weisungsgebunden (Art. 4 Nr. 8 DSGVO)
  - Cloud-Anbieter regelmäßig: Auftragsverarbeiter – aber nicht immer eindeutig
- **Art. 28 DSGVO oder Art. 26 DSGVO – Mindestanforderungen einhalten**

## Kontrollfragen für die Praxis:

- Verfolgt der Anbieter eigene Zwecke mit den Daten?
- Hat er Entscheidungsspielraum über wesentliche Mittel?

Wenn ja:

➡ gemeinsame Verantwortlichkeit zumindest prüfen

gsrechten und Auditrechten, pauschale Regelung zu

on Subdienstleistern (Subprozessoren); Mischformen: teilweise

# Drittlandzugriffe als strukturelles Risiko

- Grundsatz: **Übermittlung in Drittländer nur bei angemessenem Schutzniveau** (Art. 44 ff. DSGVO)
  - Angemessenheitsbeschluss (Art. 45 DSGVO) z.B. Schweiz, Japan, Vereinigtes Königreich, USA (Data Privacy Framework)
  - Geeignete Garantien (Art. 46 DSGVO) z.B. Standardvertragsklauseln, Binding Corporate Rules
  - Ausnahmen für Einzelfälle (Art. 49 DSGVO) z.B. Einwilligung, wichtige öffentliche Interessen etc.
- **Problematisch** sind **Zugriffsmöglichkeiten trotz EU-Hosting** aufgrund Konzernstrukturen internationaler Anbieter sowie Zugriffspflichten nach Drittlandrecht
  - ➔ Transparenz über Konzern- und Unterauftragnehmerstrukturen
  - ➔ Informations- und Abwehripflichten vereinbaren
- Position der Datenschutzkonferenz (DSK): **„Souveräne Cloud“ oder „Confidential Cloud“ sind kein rechtlicher Maßstab.** Entscheidend ist die effektive Verhinderung unzulässiger Zugriffe.
  - ➔ Fokus auf Schlüsselkontrolle, Verschlüsselung, Zugriffskonzepte

# Data Act: Paradigmenwechsel für Cloud-Verträge

01

## **Regelung des Wechsels von Cloud-Anbietern** (Art. 23 ff.):

- Anbieterwechsel (Exit) muss technisch und wirtschaftlich möglich sein
- Rechte und Pflichten der Parteien während des Wechsels
- Schrittweise Abschaffung von Wechselentgelten

02

## **Interoperabilität** (Art. 33 ff.)

- Standardisierte Schnittstellen
- offene Datenformate
- Multi-Cloud-Fähigkeit

03

## **Drittlandzugriffe** (Art. 32): **Anbieter** müssen **unrechtmäßige Drittlandzugriffe verhindern**

### **Relevanz für öffentliche Auftraggeber:**

- Erleichterung von Anbieter-Wechsels und Reduzierung von Lock-in-Effekten
- Konkrete Vorgaben zu den technischen Anforderungen definieren
- Berücksichtigung bei Vertragsgestaltung

# Teil 2: Vergaberechtliche Besonderheiten

# Zentrale Stellschrauben bei Cloud-Vergaben

## Bedarfsdefinition

- Markterkundung
- Leistungsbeschreibung und Produktneutralität
- Wahl der Verfahrensart

## Angemessene Datenschutzerfordernisse

- Sicherstellung datenschutzrechtlicher Vorgaben
- ohne ungerechtfertigte Marktverengung

## Eignungs-/Zuschlagskriterien

- Zertifizierungen im Bereich IT-Sicherheit
- Konzeptionelle Zuschlagskriterien



# Bedarfsdefinition

- **Markterkundung:**
  - Technische Machbarkeit, Vendor Lock-In (bei Bestandslösung)?
- **Leistungsbeschreibung:**
  - Ist-Situation beschreiben (z. B. relevante Schnittstellen)
    - ➡ Kalkulationsrelevanz
    - ➡ Vermeidung unzulässigen Wettbewerbsvorteils beim Bestandsanbieter
  - Produktneutralität
  - Sonderfall: Microsoft-Konditionenverträge, z. B. MS-Office, Azure Cloudleistungen
    - ➡ zwar Händlerwettbewerb, jedoch verbunden mit Produktspezifikation
    - ➡ sach- u. auftragsbezogene Rechtfertigung inkl. Dokumentation
- **Verfahrensart:**
  - Offenes Verfahren oder wettbewerbliches Verfahren (VV mit TWB, Wettbewerblicher Dialog)?
    - ➡ Kontrollfrage: „Kann ich die Leistung/Ausschreibungsbedingungen so eindeutig beschreiben, dass keinerlei Verhandlungen und Gespräche mit den Bietern nötig sind?“

# Angemessene Datenschutzerfordernungen im Verfahren

## • Anforderungen bzgl. Drittstaatenübermittlung:

- VK Baden-Württemberg, Beschl. v. 13.07.2022 – 1 VK 23/22: Latente Zugriffsmöglichkeit durch Konzernmutter von UA in nicht sicherem Drittstaat ist Datenschutzverstoß
- OLG Karlsruhe, Beschl. v. 07.09.2022 – 15 Verg8/22: Keine Datenübermittlung allein aufgrund Konzernbindung; der öffentliche Auftraggeber darf grundsätzlich auf das Leistungsversprechen des Bieters vertrauen  
➡ Pauschalen Ausschluss vermeiden (bei Drittlandtransfer Angemessenheitsbeschlüsse prüfen)

## • AVV u. TOMs – Festlegung während oder nach Vergabeverfahren?

- Option 1: Mit Angebotsabgabe nur Zusicherung der Abschlussbereitschaft  
➡ Vorteil: Flexibilität  
Nachteil: Risiko nachgelagerter Verhandlungen
- Option 2: Abschluss AVV mit Zuschlagserteilung, Einreichung TOMs mit Angebotsabgabe  
➡ Vorteil: Gewissheit bei Datenschutzniveau  
Nachteil: Konsequenzen bei Nichteinreichung (Nachforderung/Ausschluss)



Option 2 Empfehlung bei Gewissheit über Entstehung Auftragsverarbeitungsverhältnis

# Eignungs-/Zuschlagskriterien

- **Eignungskriterien/Zertifizierungen:**

- ISO/IEC 27001 nach internationalem Standard
- ISO 27001 auf Basis von IT-Grundschutz (BSI)
- Testat nach dem Kriterienkatalog C5 des BSI
  - ➡ Marktverengung u. Sach- u. Auftragsbezug beachten
  - ➡ Ggf. milderes Mittel: Eigenerklärung zur Einholung bis Auftragsbeginn

- **Konzeptionelle Zuschlagskriterien:**

- Ausnutzung gesetzlicher Umsetzungsspielräume u. kluge Delegation auf Bieterseite
  - ➡ Data Act gibt „Ob“, aber nicht „Wie“ der Umsetzung vor

Beispiele konzeptioneller Zuschlagskriterien:

- „Exit-Strategie und Vermeidung eines Lock-Ins für den Auftraggeber“
- „Interoperabilität der angebotenen Lösung“