Next Generation Cloud

Cloud Services Anbieter, Best Practices und Drittstaatentransfer

15. IT-Rechtstag

5.5.2021

Nino Tlapak

DORDA

WE DELIVER CLARITY.

Agenda

1. Einleitung
2. Aufbau Cloud-Verträge
3. Inhalt Cloud-Verträge
4. Implikationen beim Drittstaatentransfer
5. Fazit: Showstopper erkennen und Risiken verringern

Einleitung

Wesensmerkmale der Cloud

- Die Cloud ist…
  - IT-Infrastruktur, die über ein Rechnernetz zur Verfügung gestellt
- Charakteristika
  - hohe Skalierbarkeit durch geteilte Ressourcen
  - Elastizität
  - häufig bedarfsbasierte Nutzung/Abrechnung
- verschiedene Erscheinungsformen
  - Datastorage, SaaS, PaaS, IaaS

Einleitung

Cloudsourcing ≠ Outsourcing

- **Outsourcing**: Kunde "mietet" IT-Infrastrukturen, die nur von ihm genutzt werden
  - idR individuell verhandelter Vertrag

- **Cloudsourcing**: mehrere Kunden teilen sich eine gemeinsame, beim Anbieter idR an mehreren Standorten betriebene Infrastruktur
  - idR Massenprodukt
  - auf Basis von standardisierten Verträgen des Cloud Providers
  - meist nur wenig Verhandlungsspielraum für den Kunden
    - Veränderung durch Aktivität im regulierten Umfeld erkennbar

Einleitung

Ausgangslage – Rechtliche Herausforderungen

- kaum gesetzliche (Sonder-)Bestimmungen
  - allgemeines Zivilrecht
    - Vertragsgestaltung und -auslegung
    - Gewährleistung / Haftung
  - Unternehmensrecht
    - zB Mängelrüge
  - Immaterialgüterrecht
    - Rechteeinräumung/Lizenzierung
  - Datenschutzrecht
    - bei Verarbeitung personenbezogener Daten in der Cloud
- ausländische Sondergesetze (zB CLOUD Act)

Einleitung

Ausgangslage – Praktische Herausforderungen

- häufig unverhandelte Verträge/AGB, von der einen Seite erstellt und von der anderen unreflektiert übernommen
  - geringer(er) Spielraum für Vertragsverhandlungen
  - "*take it or leave it*"
- "*Grauzone*" zwischen technischen und rechtlichen Themen
- rasante faktische und rechtliche Entwicklung
  - laufend neue Technologien: Blockchain, etc
  - ständig rechtliche Neuerungen: DSGVO, Urheberrechtsnovelle, etc
  - ausländische Besonderheiten (zB CLOUD Act)
  - Weiterentwicklung durch Rsp (zB Schrems II)

Aufbau Cloud-Verträge

Klassischer Aufbau

- Präambel
- Leistungsbeschreibung (meist in Anlagen)
- Nutzungsrechte und sonstige IP
- Verfügbarkeit, Wartung, Updates, SLA (meist in Anlagen)
- Einsatz von Subunternehmen
- Datenschutz und -sicherheit (meist in Anlagen)
- Kommerzielle Bestimmungen (Order Form)
- Haftung und Gewährleistung
- Laufzeit und Kündigung
- Anwendbares Recht und Gerichtsstand

Aufbau Cloud-Verträge

Regelmäßig fehlende Inhalte

- effektive Audit- und Kontrollrechte
- Steuerungsmöglichkeit bei Subunternehmen
- Change Prozesse
- (ausreichende) Haftung für Datenverlust / DSGVO Verstöße
- Nachwirkung / Beendigungsunterstützung
- branchenspezifische must haves
  - vor allem Aufsichtsrecht und datenschutzrechtliche Besonderheiten

Aufbau Cloud-Verträge

Wesentliche rechtliche Fragestellungen

- anwendbares Recht?
  - Anbieter bringen in ihren Verträgen bzw AGB meist ihr eigenes Recht (oft US-Recht) zur Anwendung
- vertragsrechtliche Einordung der Cloud?
  - zwischen Miete und Dienstleistung, ggf Werkvertrag
- Leistungsumfang und Pflichten des Anbieters? Qualität? Preis?
  - teilweise nur rudimentär festgelegt

  → Risiko für den Kunden, da keine Berufung auf eine bestimmte Qualität
- Umfang von Gewährleistung und Haftung?
  - meist SLC als "*sole and exclusive remedy*"
- Datenschutz?
- Beendigungsmöglichkeiten?

Inhalt Cloudverträge

Rechtliche Einordnung – klassischerweise Mietvertrag

- Überlassung von Standardsoftware
  - für einen breiten Anwenderkreis zugeschnitten
  - keine Anpassung an die Wünsche des Kunden (kein "Customizing")
  - keine Zusatzprogrammierungen
- zeitlich begrenzte Nutzung durch den Kunden
  - Rechteeinräumung auf bestimmte Zeit oder
  - Rechteeinräumung auf unbestimmte Zeit mit Kündigungsmöglichkeit und Rückgabeverpflichtung (OGH 1 Ob 229/14d)
- idR laufendes Entgelt

Inhalt Cloudverträge

Gewährleistung und Haftung - Problemaufriss

- Cloud nie 100% fehlerfrei
  - Serviceausfälle
  - Nicht-Verfügbarkeit
  - Systemstillstand
  - Fehler in der SaaS-Applikation
  - Hackerangriff mangels ausreichender Sicherheitsmaßnahmen
- Mängel können beim Kunden rasch zu hohen Schäden führen
  - Geschäftsstillstand
  - fehlerhafte Geschäftsabwicklung
  - Datenverlust und -verstöße
  - negative PR

Inhalt Cloudverträge

Gewährleistung und Haftung

- Gewährleistung häufig vertraglich eingeschränkt
  - oft kaum (brauchbare) Servicelevels
    - nur Reaktions-, aber keine Behebungszeiten
    - "*best effort*", "*commercially reasonable*"
  - bei Massenprodukten oft niedrige Service Levels Credits vorgesehen
    - "*sole and exclusive remedy*"
  - Anbieter behalten sich meist vor, Wartungsfenster zu setzen
    - meist Abstellen auf internationale Feiertage

- Bei Fehlern in der Praxis daher
  - rechtzeitig in richtiger Form, begründet und über richtigen Kanal melden
  - intern sauber dokumentieren
  - Eskalation auf Projektebene

Inhalt Cloudverträge

Gewährleistung und Haftung

- umfassende Haftungseinschränkung im Vertrag bzw den AGB
  - vor allem bei US-Anbietern
  - Vorsicht: Besonderheiten englischer Vertragssprache
- Einschränkungen hinsichtlich Art der Schadenszufügung und des Schadens, Höhe als auch Dauer der Verjährungsfrist
  - zusätzlich betragliche Beschränkung (meist Jahresentgelt)
  - tlw sogar expliziter Ausschluss bei Strafen, Datenverlust, etc
- häufig Beweisschwierigkeiten
  - konkreter Schaden kann oft schwer beziffert werden (zB Datenverlust)

Inhalt Cloudverträge

Stolperfalle: Datenrückgabe/Zugriff nach Vertragsbeendigung

- sinnvolle Datenrückgabe; oder
  - Datenformat
  - Löschpflicht des Providers

- nachgelagerter Zugriff
  - Datenhosting im EU-Ausland → prozessrechtliche Durchsetzung?
  - Lösung: Zugriff für bestimmte Zeit nach Vertragsbeendigung
    - meist 60 bis 180 Tage
    - Wichtig: unabhängig von Kündigungsgrund
    - meist ungeregelt: Unterstützung? Kosten?

Implikationen beim Drittlandstransfer

Datenschutzrechtliche Ausgangslage

- Cloud Anbieter ist Auftragsverarbeiter im Sinne der DSGVO
  - **Vereinbarung nach Art 28 DSGVO** verpflichtend
- bei Cloud Provider außerhalb der EU: zusätzlich
  - Angemessenheitsbeschluss oder
  - Standarddatenschutzklauseln (Vorlagen der EU Kommission)
    - Schrems II: supplementary measures?
- Kunde bleibt datenschutzrechtlicher Verantwortlicher
  - haftet den Betroffenen für verursachten Schaden (Art 82 Abs 2)
    - auch wenn Schaden durch Cloud Anbieter verursacht
    - Kunde kann sich beim Provider regressieren (Art 82 Abs 5)
  - potentielle Geldstrafen nach Art 83 gegen den Kunden
    - Verletzung von Prüfung- und Weisungspflichten
    - nicht sorgfältige Auswahl / nicht ausreichende Überwachung des Auftragsverarbeiters (Auswahl-/Überwachungsverschulden)

Implikationen beim Drittlandstransfer

Kritische / fehlende Klauseln in der Praxis

- eingeschränkte bzw fehlende Steuerungsmöglichkeit für Subunternehmen
  - keine Offenlegung sämtlicher Subs
  - eingeschränkte/fehlende Widerspruchsmöglichkeit bei Austausch
- eingeschränkte Auditrechte
  - sowohl für den Kunden als auch dessen Prüfer
- wenig bis kein Support bei Betroffenenrechten
  - oftmals nur Abstellen auf verfügbare Funktionen der Cloud
  - meist gegen gesondertes Entgelt
- wenig Kooperationsbereitschaft mit zuständigen Behörden
- Zusage konkreter IT-Sicherheitsmaßnahmen
  - statt Einhaltung des laufend weiterentwickelten Stands der Technik

Implikationen beim Drittlandstransfer

Exkurs: Einsatz und Steuerung von Subunternehmen

- Steuerungsmöglichkeit nicht nur aufsichts- sondern auch datenschutzrechtlich zwingend
- konkrete schriftliche Genehmigung nicht praxistauglich
  - Zahlreiche Subunternehmen innerhalb der Cloud
- **daher**: Informations-, Widerspruchs- und Kündigungsrecht
  - vorherige Information bei Austausch oder Hinzuziehen neuer Subunternehmen durch den Cloud-Provider
  - Widerspruchsrecht des Kunden (tlw verhandelbar mit wichtigem Grund)
  - Sonderkündigungsrecht für den Kunden
- Achtung: Erstreckung der Audit- und Weisungsrechte auf die Subunternehmen zwingend erforderlich
  - Überbindung sämtlicher Vertragsinhalte von Cloud-Provider an alle Subunternehmen

Implikationen beim Drittlandstransfer

Der Fall des EU-US Privacy Shield – Auswirkung auf SCC

- EU SCC weiterhin gültig
  - Hintergrund: Klauseln treffen keine Aussage zu Datenschutzniveau
- **aber** gleiche Prüfpflicht des Verantwortlichen wie bisher
  - Welchen Schutz bieten SCC im konkreten Fall?
  - Welche Garantien sieht der Sitzstaat des Empfängers vor?
  - Sind EU SCC ausreichend oder weitere Maßnahmen erforderlich?
- Prüfung erfolgt in der Praxis kaum
  - hätte in der Vergangenheit wohl bereits zu Anpassungsbedarf geführt
- für USA hat EuGH detaillierte Prüfung vorgenommen
  - Ergebnis: unveränderte EU SCC nicht ausreichend

Implikationen beim Drittlandstransfer

Lösungsansätze bei Cloud-Verträgen

- vertragliche Überbindung rechtlicher Verpflichtungen
  - Datenschutz
  - Auditrechte (für Kunde und dessen Prüfer)
  - Spezialmaterie : Bankgeheimnis, EBA Guidelines
- strenge Geheimhaltungs- und Vertraulichkeitsregelungen
  - unter Berücksichtigung branchenspezifischer Besonderheiten
- Vereinbarung umfassender (Daten-)Sicherheitsmaßnahmen
  - zB Verschlüsselung und Pseudonymisierung

  ➔ Wenn Daten nicht zugänglich sind/Provider keinen Schlüssel hat, wird das Risiko faktisch minimiert!

Implikationen beim Drittlandstransfer

Supplementary Measures in der Praxis

- Informationspflichten für Anbieter, wenn eine US-Behörde Datenzugriff verlangt
  - Vorsicht: teilweise Gag-Order (Info unzulässig) möglich
- Pflicht des Anbieters, Rechtsmittel voll auszuschöpfen
  - Kunden Äußerungsmöglichkeiten geben
  - Informationsaustausch und laufende Updates
- Zusage, dass keine Backdoors implementiert sind
- rasche Beendigungsmöglichkeit des Vertrages
  - kurze Kündigungsfristen
  - ggfs Recht zur Kündigung aus wichtigem Grund bei Änderungen

Implikationen beim Drittlandstransfer

Begleitmaßnahmen zur Risikomitigierung

- Prüfung des Cloud Anbieters
  - zB Zertifizierungen und Einhaltung von Standards (zB ISO)
- Dokumentation für potentielle Verfahren
  - Sorgfaltsverstoß? Auswahlverschulden?
- laufende Kontrolle des Anbieters
  - Umfang und Ausmaß der Reports und Audits
  - Kostentreiber!
  - sofortige Reaktion und Eskalation bei Datenschutzverstößen
- Vorsicht bei "europäischen" Cloud-Lösungen
  - Einschränkung der Funktionalität möglich
  - oftmals nur data-at-rest innerhalb EU/EWR
  - idR Zugriff durch US Tochter bei Wartung möglich
    - follow the sun Support sonst faktisch nicht möglich

Fazit: Showstopper erkennen und Risiken verringern

Häufige No-Gos

- fehlende Steuerungsmöglichkeit
  - insbesondere bei Subunternehmen
- kein effektives Audit- oder Kontrollrecht
- "*falsches*" Lizenzmodell
  - hohe Kosten und/oder brach liegende Lizenzen
- fehlende Informations- und Abwehrpflichten bei US-Zugriffen
  - drohender DSGVO- als auch Geheimhaltungsverstoß
- unverhandelte Kündigungsfristen
  - entweder zu kurz, um Alternativlösung einzusetzen; oder
  - zu lange und damit monetäres Thema

Ansprechpartner

Mag Nino Tlapak, LL.M.

- Partner bei DORDA
- Universität Wien, Mag iur 2012
- Universität Wien, Universitätslehrgang Medien- und Informationsrecht, LL.M. (IT-Law) 2013
- Fachliche Schwerpunkte: Datenschutz, Cybersecurity, IT-Verträge mit Schwerpunkt auf Outsourcing und Cloud-Verträge
- Empfohlen als Next Generation Lawyer im Bereich TMT und Data Privacy im renommierten internationalen Handbuch "Legal 500" sowie als Up and Coming in "Chambers Europe"
- PrivacyConnect Co-Chair Vienna
- Vortragender für Datenschutzrecht bei Master-Lehrgängen an der Universität Wien, FH Technikum Wien und FH Campus Wien sowie der Donau Universität Krems ("Datenschutz und Privacy")
- Mitglied der Interessensgemeinschaften "www.it-law.at" und "Privacyofficers.at"

Kontakt

Mag Nino Tlapak, LLM
T: +43 1 533 47 95 – 23
E: nino.tlapak@dorda.at

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien

International Law Office - Information Technology Award for Austria 2014, 2015, 2016, 2017, 2018 & 2019
International Law Office - E-Commerce Award for Austria 2012 & 2013
Managing IP Awards – Austrian Firm of the Year for Copyright & Design 2020