DORDA

WKO Spedition · Logistik

CLOUD VERTRÄGE IN DER PRAXIS

RECHTLICHE STOLPERSTEINE UND PRAKTISCHE LÖSUNGSANSÄTZE

Informationsbroschüre zur Cloud und deren rechtlichen Fragestellungen

V O R W O R T

Cloud-Computing birgt neben klaren wirtschaftlichen Vorteilen durch hohe Skalierbarkeit, geteilte Ressourcen und der bedarfsbasierten Nutzung und Abrechnung auch rechtliche Risiken. Viele lassen sich darauf zurückführen, dass der Markt von US-Anbietern dominiert wird. Dadurch kommt es zu einem Aufeinanderprallen unterschiedlicher Rechts- und Vertragsstrukturen und stellen sich regelmäßig grundlegende datenschutzrechtliche Fragen.

Während der praktische Bedarf und faktische Einsatz von Cloudlösungen aufgrund der Vielfältigkeit der Einsatzmöglichkeiten drastisch zunimmt, fehlt es gleichzeitig an einschlägigen gesetzlichen Regelungen: Wie in vielen Bereichen des IT-Rechts gibt es keine Spezialbestimmungen für Cloud Verträge. Daher kommen die allgemeinen zivilrechtlichen Bestimmungen zur Anwendung. Freilich bestehen aber für gewisse, kritische Bereiche, wie zB den Datenschutz, einschlägige, strenge Bestimmungen. Abgesehen davon ist aufgrund des rasanten und immerwährenden technischen Fortschritts ein hohes Maß an Flexibilität erforderlich, um vertraglich für beide Seiten lebbare Lösungen zu finden und Brücken zwischen den unterschiedlichen Vertragsregimen zu schlagen. Dabei gibt es je nach konkretem Anwendungsbereich und Funktionalität der Cloudlösung, Branche des Kunden und Zugang des Anbieters unterschiedliche Parameter und Spielräume, die bei der Vertragsverhandlung zu berücksichtigen sind. Wiewohl Cloudverträge gerne als unverhandelbare Standards präsentiert werden, gibt es in der Praxis vielmehr in gewissen Bereichen Verhandlungspouvoir, aber auch -bedarf.

Ziel dieser Informationsbroschüre ist es, Ihnen die wesentlichen rechtlichen Rahmenbedingungen und damit einhergehenden Stolpersteine bei Cloudverträgen zu erläutern und sodann praktische Lösungswege zu skizzieren. Da es sich bei cloudbasierten Dienstleistungen in der Regel um Standardprodukte handelt, ist im Sinne eines risikobasierten Ansatzes stets eine Einzelfallabwägung auf Basis des Gesamteindrucks erforderlich. Wo sind Anpassungen wirklich notwendig und nötig? Neben einer belastbaren vertraglichen Basis ist das Augenmerk zudem im selben Ausmaß auch auf die technischen und organisatorischen Implementierungs- und Begleitmaßnahmen zu legen, um Projekte zu ermöglichen. Ein erfolgreiches Cloudsourcing Projekt bedarf daher der frühzeitigen Einbindung und Zusammenarbeit des Projektmanagers mit der Rechts- und IT-Abteilung – je nach Umfang allenfalls unter Einbeziehung externer Experten aus diesen Bereichen.

Inhaltsverzeichnis

1. Einführung

1.1. Unterschiedliche Cloudmodelle

Hinter jeder Cloud-Lösung steht eine externe IT-Infrastruktur, die dem Kunden über ein Rechnernetz eines Dritten ("Cloud-Provider") zur Verfügung gestellt wird. Damit muss diese IT nicht mehr selbst lokal beim Kunden ("*on premise*") betrieben werden. Dabei zeichnet sich die Cloud im Wesentlichen durch (i) hohe Skalierbarkeit durch geteilte Ressourcen, (ii) Elastizität, (iii) bedarfsbasierte Nutzung und Abrechnung und damit (iv) Kosteneffizienz aus. Oftmals wird nicht nur der Betrieb oder die Wartung der IT-Infrastruktur, sondern das gesamte Service samt Speicherung ausgelagert.

Auch der Inhalt der Vereinbarung kann sehr unterschiedlich sein: Neben reinen Hardware- oder Softwarepaketen gibt es auch Mischformen, wo beides gemeinsam angeboten wird. Über eine Cloud werden in der Praxis daher viele unterschiedliche Dienstleistungsmodelle angeboten. Diese reichen von klassischem Datastorage über Software as a Service (SaaS) und Platform as a Service (PaaS) hin zur Infrastructure as a Service (IaaS). Je nachdem, ob über den Dienst nur Einzelne oder unbegrenzt viele Kunden serviciert werden, wird zwischen Private oder Community Cloud und Public Cloud unterschieden. Mischformen als Hybrid Cloud sind dabei ebenso denkbar und kombinieren gegebenenfalls die Vorteile aus beiden Welten.

1.2. Abgrenzung zum klassischen Outsourcing

Beim klassischen Outsourcing mietet der Kunde bestimmte, meist dedizierte (ihm allein zugeordnete) IT-Infrastruktur und zugehörige (Wartungs- und Support-)Leistungen. Ursprünglich wurden diese Leistungen sodann vom Auftraggeber alleine genutzt. Für die Ausgestaltung des Projekts, aber auch der zugehörigen Verträge bietet bzw erfordert das entsprechende Flexibilität: Das Projekt und der Vertrag werden für den konkreten Kunden individuell erstellt und ausgehandelt.

Bei Clouddienstleistungen teilen sich unterschiedliche, oft sogar in verschiedenen Ländern sitzende Kunden eine vom Cloud-Provider in der Regel an mehreren Standorten betriebene IT-Infrastruktur oder Software. Es handelt sich – zumindest bei Public Clouds – um vereinheitlichte Massenprodukte mit vorgegebenen Spezifikationen, die allen Kunden "as is" auf Basis standardisierter Verträge angeboten werden. Naturgemäß besteht bei diesen Dienstleistungen schon aufgrund dieser Ausgangslage nicht nur wenig individueller Anpassungs- sondern damit auch nur beschränkter Verhandlungsspielraum. Das ist bei der Auswahl des konkreten Anbieters und Festlegung des Projektzugangs von Anfang an entsprechend zu berücksichtigen: Üblicherweise sind bei solchen Modellen die konkreten Serviceparameter kaum veränder- und verhandelbar (zB Service Levels und Service Level Credits, Response Time, Security Measures). Das macht aus Sicht des Anbieters auch Sinn: Würde er gegenüber einzelnen Kunden Änderungen in diesen Bereichen zulassen, müsste er gegebenenfalls seine Leistung entsprechend der individuellen Vereinbarung und dementsprechend auch all seine Verträge mit bestehenden Kunden anpassen. Das widerspricht jedoch klar dem intendierten, vereinheitlichten Business Modell. Im Gegenzug profitiert der Kunde aber beim Einheitsansatz vor allem kommerziell von den vereinheitlichten Standards und kontinuierlichen Weiterentwicklung der Services. Statt hohen Kosten für Change Requests Einzelner beteiligen sich alle Kunden gemeinsam mit einem weitaus geringeren Anteil an laufenden Updates und Upgrades. Nicht übersehen werden darf aber, dass es auch bei Standardprodukten in gewissen Bereichen sehr wohl Verhandlungsmöglichkeiten bzw -notwendigkeiten gibt. Diesen Punkten widmen wir uns dann im Folgenden.

Besteht bei einem Kunden Bedarf an Individual- oder Nischenlösungen, sind Public Cloud Lösungen daher nicht die richtige Wahl. Das heißt aber nicht automatisch, dass der Auftraggeber auf dedizierte Systeme und klassisches Outsourcing zurückgreifen muss. In der Praxis haben sich durchaus hybride Projekte, bei denen klassische Outsourcing Elemente mit Private oder Public Cloud Lösungen kombiniert werden, durchgesetzt. So können die Vorteile aus den unterschiedlichen Welten kombiniert werden: Höhere Investitionen und Individualisierung dort, wo es notwendig ist. Standardlösungen für die Bereiche ergänzen, in denen das möglich ist. Damit werden Kosten eingespart.

1.3. Exkurs: Digitalisierungsförderung

Zum Zeitpunkt der Erstellung dieser Informationsbroschüre waren alle Branchen noch von der herrschenden Corona-Virus Pandemie gebeutelt. Als eine Maßnahme zur Unterstützung österreichischer Unternehmen und Erhöhung der Investitionen zur Ankurbelung der Wirtschaft hat die Bundesregierung die aws Investitionsprämie ins Leben gerufen: Damit werden Neu-Investitionen im Bereich Ökologisierung, Digitalisierung und Gesundheit aktuell mit 14% (aber maximal EUR 50 Mio) gefördert (https://www.aws.at/corona-hilfen-des-bundes/aws-investitionspraemie/). Das Projekt muss dafür bis spätestens 28.2.2021 eingereicht, bis zum 1.3.2021 mit der Investition (zB Bestellung, Lieferung, Beginn Umsetzung etc) begonnen und spätestens bis zum 28.2.2022 umgesetzt werden.

Daneben gibt es aber auch sonst laufend unterschiedliche Förderungen und Anlaufstellen für IT-Investitionen – vom Bundesministerium für Digitalisierung und Wirtschaftsstandort über Bund und Länder bis hin zu spezialisierten Digitalhubs. Die aktuell umfangreichste Förderung zur Digitalisierung von Unternehmensprozessen und Aufbau digitaler Geschäftsmodelle ist über das aws möglich (https://www.aws.at/aws-digitalisierung). Für KMU ist KMU Digital 2.1 (https://www.kmudigital.at), digi4KMU (http://noe.gv.at/digi4kmu) oder auch Wien Digital (https://wirtschaftsagentur.at/foerderungen/programme/wien-digital-110) eine potentielle Anlaufstelle für Förderungen.

2. Rechtliche Rahmenbedingungen

2.1. Ausgangslage

Weder für klassisches Outsourcing noch Cloudverträge gibt es gesetzliche Sonderbestimmungen. Dementsprechend greifen die allgemeinen zivil- und unternehmensrechtlichen Regelungen rund um Vertragsgestaltung und -auslegung, Haftung und Gewährleistung. In Bezug auf die Besonderheiten der Lizenzierung und sonstigen Rechteeinräumung kommen das Urhebergesetz und weitere einschlägige immaterialgüterrechtlichen Grundlagen zur Anwendung. Da bei Clouddienstleistungen stets auch der Transfer von Daten und Informationen betroffen ist, sind schlussendlich noch die Datenschutzgrundverordnung ("DSGVO"), nationale Sonderbestimmungen wie das Datenschutzgesetz ("DSG") und die Regelungen des Gesetzes gegen den unlauteren Wettbewerb ("UWG") zum Schutz von betriebs- und Geschäftsgeheimnissen zu beachten. Gerade bei der Auslagerung (wesentlicher) Dienste können für bestimmte Branchen zudem besondere, regulatorische Anforderungen zur Anwendung kommen. Das betrifft vor allem Versicherungen, Banken und den Gesundheitsbereich. Für Spediteure gibt es keine vergleichbaren Spezialbestimmungen. Allerdings führen die verschärften Anforderungen für die regulierten Branchen schleichend zu einer generellen Anhebung der Vertragsstandards und -praxis. Davon profitieren dann auch andere Marktteilnehmer.

Diesen nationalen und/oder europäischen Rechtsgrundlagen stehen die auf den Cloud-Provider lokal anwendbaren Gesetze und Regelungen gegenüber – gerade im IT-Bereich sind somit vor allem US-Recht sowie nach Vollzug des Brexit zukünftig auch die Rechtsordnung des Vereinigten Königreichs relevant. Eine besondere Herausforderung stellen dabei die grundsätzlich unterschiedlichen Herangehensweisen und Regelungsmethoden von kontinentaleuropäisch oder anglo-amerikanisch geprägten Vertragswerken dar. Das beginnt beim grundsätzlichen Aufbau des Vertrages: Während man in Europa in Verträgen auf Grundlage des subsidiär geltenden Gesetzes eher versucht generelle Regelungen zu treffen, sind vor allem US-amerikanisch geprägte Vereinbarungen mehr kasuistisch nach dem Case Law Prinzip gestaltet. Dazu kommt bei Letzteren auch die Angewohnheit umfangreicher Definitionen, die zur Erfassung des Rechtstextes mitgelesen werden müssen. Inhaltlich zeigen sich zahlreiche Abweichungen im Verständnis von (englischen) Rechtsbegriffen wie zB rund um das Thema von Garantien und Gewährleistungen samt entsprechender Terminologie sowie den Umfang der Zusicherungen bei Schlechterfüllung. Gerade im Softwarebereich hat sich eine Überlassung von Leistungen als "as is" – also wie gesehen und ohne weitere Zusicherungen – etabliert. Bei Cloudverträgen kommt es selbst bei der Zusicherung der IP-Compliance – also Nichteingriff in Rechte Dritter – regelmäßig zu Einschränkungen. Auch beim Aufbau und Umfang von Haftungsbeschränkungen bestehen gravierende Abweichungen im Sinne eines viel weiteren Ausschlusses der Verantwortlichkeit. Im IT-Recht versierte Juristen sind dies aber gewohnt – durch den US-Einfluss hat sich in diesem Bereich bereits ein eigener, vom normalen Vertragsverständnis abweichender Anbieterstandard entwickelt.

Um pragmatische Lösungen zu erzielen ist es wichtig, sich auf die wesentlichen Punkte zu konzentrieren. Potentielle Showstopper aus allen Bereichen – technisch, wirtschaftlich und rechtlich – sollten vorab identifiziert und kommuniziert werden. Nach einer ersten Annäherung bei den wesentlichen Punkten macht ein mark-up des Anbieters Sinn. Danach empfiehlt es sich erfahrungsgemäß die Vertragsverhandlungen persönlich bzw virtuell zu führen, um kosten- und zeiteffizient zu einem gemeinsamen Verständnis und daher für beide Seiten lebbaren Ansatz zu kommen. So kann man am besten ausloten, wo doch Verhandlungsspielraum besteht oder man identifizierte Abweichungen einer Risikobewertung zuführen muss.

Die eingangs erwähnte, erforderliche Zusammenarbeit zwischen der Zuständigen für Recht und IT ist gerade bei Cloud Verträgen wichtig und kann zur pragmatischen Lösungsfindung beitragen. So können oft initial als rechtliche Showstopper identifizierte Punkte durch mitigierende technische Maßnahmen abgefangen werden. Das gilt nicht nur für klassische Service Levels, sondern insbesondere auch in Zusammenhang mit dem potentiellen Datentransfer an etwaige Drittländer (siehe dazu im Detail Pkt 3.3.). Umgekehrt können Techniker die Belastbarkeit und praktische Tauglichkeit von vom Cloud-Provider ins Treffen geführte technischen Lösungen, die Rechtsprobleme beseitigen sollen, evaluieren.

2.2. Rechtliche Einordnung von Cloudverträgen

Cloudverträge sind grundsätzlich als Dauerschuldverhältnis ausgestaltet, beinhalten dabei aber – je nach Leistungsumfang – sowohl Dienstleistungs-, Mietvertrags- als auch Werkvertragselemente. In der Praxis hat sich bei solch komplexen Bereichen eine differenzierte Betrachtung durchgesetzt: Statt den Vertrag gesamthaft einem rechtlichen Regime zu unterstellen, wird pro Leistungsbereich eine treffsichere Zuordnung vorgenommen. Daher sind die einzelnen Leistungen dem jeweils passenden Regime zuzuordnen: Schlussendlich kommt es besonders darauf an, ob der Cloud-Provider nur

redliches Bemühen (wie bei einer Dienstleistung, zB Support) oder einen konkreten Erfolg (wie bei einem Werkvertrag, zB Implementierung) schuldet.

Bei den weitverbreiteten Cloud-Verträgen rund um Überlassung von Standardsoftware gegen laufendes Entgelt ist die Hauptleistung mittlerweile regelmäßig als Mietvertrag ausgestaltet, wobei idR eine bestimmte Laufzeit (Befristung) mit automatischer Verlängerung am Markt vorherrschend ist. Alternativ gibt es auch unbefristete Verträge, die mit einer – im Vergleich zu Outsourcingverträgen – meist eher kurzen Kündigungsfrist beendet werden können. Das trifft vor allem auf bloße Datastorage Leistungen zu. Für den Bereich der Softwareüberlassung schuldet der Anbieter im Wesentlichen die (mangelfreie) Zurverfügungstellung der Software und Aufrechterhaltung der Verfügbarkeit durch Updates und laufende Fehlerbehebung. Hier wird also oftmals der im klassischen Softwarebereich getrennte Bereich Lizensierung und Wartung vermischt.

2.3. Aufbau Cloud-Verträge und Verhandlungsstrategie

Die Cloudverträge der großen IT-Anbieter (i) stammen idR aus US-amerikanischer Feder und (ii) sind klassischerweise vielschichtig und komplex aufgebaut: So gibt es meist ein übergeordnetes Enterprise Agreement, das die Lizenzbestimmungen regelt und auf einem Master Service Agreement aufbaut, in dem die wesentlichen Rechte und Pflichten beider Vertragsparteien sowie insbesondere Haftung und Gewährleistung festgelegt sind. Daneben bestehen idR eine separate Auftragsverarbeitungsvereinbarung (Data Processing Agreement, DPA), Security Policy, Service Level Agreement (SLA), spezifische Produktbestimmungen (Product und/oder Service Terms) und allenfalls Bestellformulare (Order Forms). Die erste große Herausforderung ist daher den Gesamtzusammenhang, die unzähligen Verweise und Wechselwirkungen der unterschiedlichen Klauseln zu erfassen. Dabei mangelt es den meisten dieser Vertragssets einer klaren Vorrangregelung, sodass etwaige Lücken oder gar Widersprüche oftmals erst nach gezieltem Ansprechen von Themen aufgedeckt und bereinigt werden können.

Aber auch Verträge von europäischen Anbietern sind idR sehr komplex. Hier besteht oftmals ein zentraler Rahmenvertrag, dem dann die anderen Dokumente untergeordnet sind. Anders als bei US-Verträgen ist hier das Zusammenspiel der Vertragsbestandteile aber vielfach klarer und sind die Themen besser abgegrenzt.

Nicht nur aufgrund des Ineinandergreifens der unterschiedlichen Vertragsteile, sondern auch auf Basis strategischer Überlegungen sind die unterschiedlichen Elemente der Vereinbarung stets gemeinsam zu verhandeln. Nur so können Widersprüche nachhaltig vermieden und gleichzeitig die eigene Verhandlungsposition gestärkt werden. Kommerziell wirkt sich eine getrennte Verhandlung zB von Haupt- und etwaigem Wartungsvertrag (sofern dieser nicht als Leistung integriert ist) idR ebenso negativ aus – etwaige im Hauptvertrag gewonnene Punkte schlagen sich aus Erfahrung dann bei der Service Fee nieder.

Bei sensiblen Projekten, wie zB bei Überlassung einer Vielzahl von Daten, gegebenenfalls sogar besonderer Kategorien (sensible Daten) oder im regulierten Bereich, empfiehlt es sich, die wesentlichen Punkte in einem zentralen Dokument einheitlich zu lösen. Dieser Vertragszusatz oder Amendment sollte dann ausdrücklich den sonstigen Vertragsbestandteilen vorgehen. Damit werden einerseits fehlende oder unzureichende Vorrangklauseln überwunden und andererseits sichergestellt, dass die wesentlichen Vertragsprinzipien auch etwaigen einseitigen Änderungsmöglichkeiten des Anbieters entzogen werden. So finden sich gerade bei Cloud Verträgen in technischen Anlagen, aber

auch in den Datenschutzregeln oft entsprechend einseitige, für den Kunden schwer akzeptierbare Befugnisse.

2.4. Wesentliche Vertragsbestandteile und Verhandlungsspielraum

Wenn im Unternehmen initial die Awareness für den bestehenden Ergänzungs- und Überarbeitungsbedarf von Cloudverträgen geschaffen wurde, ist der erste wesentliche Grundstein gelegt. Das frühzeitige Erkennen und die Schaffung des Verständnisses, dass die wichtigsten Themen klar kommuniziert und mit dem Cloud-Provider Verhandlungen zur Anpassung seiner Vertragsmuster geführt werden müssen, ist die wichtigste Grundvoraussetzung für den Erfolg der Auslagerung. Erfahrungsgemäß nehmen Vertragsverhandlungen im Cloudumfeld bei gröberem Änderungsbedarf doch einige Zeit in Anspruch, da Cloud-Provider typischerweise (i) auf Zeit spielen und (ii) intern selbst mit der (üblicherweise in den USA sitzenden) Muttergesellschaft verhandeln müssen. Falsche Erwartungen und insbesondere eine zu enge Timeline stehen sinnvollen und zielgerichteten Vertragsverhandlungen daher regelmäßig im Weg und sind daher bestmöglich zu vermeiden. Bei Anbietern, die ihre Vertragswerke schon grundlegend an kontinentaleuropäisches Recht, vorzugsweise Deutschland oder Österreich, angepasst haben, können Verhandlungen auch durchaus rascher gehen. Gleiches gilt bei absoluten Standardprodukten mit geringem Anpassungsmöglichkeiten, die auf die absoluten "*must haves*" reduziert sind.

In den Verhandlungsrunden selbst ist sodann ein besonderes Augenmerk auf die folgenden, klassischerweise zumindest in Grundzügen bereits vorhandenen Regelungen zu legen:

- Präambel
  Gerade bei Nischenprodukten, die von einem Anbieter cloudbasierend angeboten werden, ist eine detaillierte Beschreibung der Erfahrung und Professionalität des Cloud-Providers zu begrüßen. Diese wird bei der Vertragsauslegung herangezogen, wenn es um die Feststellung der üblicherweise zu erwartender Qualität und Eigenschaften der Dienstleistungen geht.
- Leistungsbeschreibung
  Je komplexer die angebotenen Dienstleistungen aufgebaut sind, desto detaillierter ist abzugleichen, welche Dienste zu welchem Preis tatsächlich umfasst sind.
- Nutzungsrechte und sonstige IP
  Um Leerkosten für brachliegende Lizenzen zu vermeiden ist vorab zu entscheiden, welches Lizenzmodell sich für welches Einsatzgebiet am besten eignet (siehe dazu im Detail Pkt 2.5.).
- Haftung und Gewährleistung
  Service-Ausfälle, Fehler und damit einhergehende vorübergehende oder dauerhafte Nicht-Verfügbarkeit können beim Kunden rasch zu hohen Schäden führen: Von fehlerhaften Geschäftsabwicklungen über Datenverluste bis hin zum Geschäftsstillstand. Klassischerweise versuchen aber die Cloud-Provider die Haftung und Gewährleistung weitestgehend auszuschließen. Je nach Kritikalität des Services besteht daher gerade hier entsprechend großer Nachbesserungsbedarf: Zu umfassenden Haftungsausschlüssen tritt gerade bei US-Verträgen idR noch eine betragliche Begrenzung sowie umfangreiche Einschränkung hinsichtlich Art der Schadenszufügung, Art des Schadens sowie Höhe und auch Dauer der Verjährungsfrist hinzu.
- Verfügbarkeit – SLA
  Durch die fehlenden Gewährleistungszusagen und eingeschränkten Haftungsbestimmungen ist ein besonderes Augenmerk auf die Ausgestaltung der

Service Levels und zugehörigen Service Level Credits zu legen. Nur so kann die erforderliche Steuerung bei Mängeln und Fehler erfolgen. In der Praxis sind in den Standardverträgen aber meist kaum (brauchbare) Service Levels sowie meist keine oder nur niedrige Service Level Credits vorgesehen. Erfahrungsgemäß besteht hier erst ab einer gewissen Unternehmensgröße des Kunden die Bereitschaft des Cloud-Providers in tiefergreifendere Verhandlungen einzusteigen.

- Wartungsbestimmungen
  Hand in Hand mit den SLA gehen die Bestimmungen rund um den Umfang und die Erreichbarkeit von Wartungs- und Supportleistungen sowie der vorgesehene Zeitraum ihrer Umsetzung (Wartungsfenster).
- Einsatz von Subunternehmen
  Nicht nur die initiale Auswahl von bestimmten Subverarbeitern, sondern insbesondere das Prozedere rund um den Austausch derselben bzw die Hinzuziehung weiterer ist in Bezug auf die erforderliche Überbindung der Vereinbarung zwischen Kunde und Cloud-Provider besonders relevant. Hier besteht idR ein Spannungsverhältnis zwischen den datenschutzrechtlichen Erfordernissen des Kunden und den geschäftlichen Interessen des Anbieters. Letzterer möchte seine Flexibilität möglichst groß halten und einseitig Entscheidungen treffen. In der Praxis sind Informationspflichten und realistische Kündigungsmöglichkeiten des Kunden daher das absolute Minimum.
- Datenschutz und Vertraulichkeit
  Da Clouddienstleistungen klassische Auftragsverarbeitungen im Drittland sind, sind die wesentlichen datenschutzrechtlichen Parameter, Maßnahmen und Garantien mit Fokus auf Art 28 und 46 ff DSGVO zu vereinbaren (siehe dazu im Detail Pkt 3.3.).
- Kommerzielle Bestimmungen
  Neben den Zahlungsbedingungen rund um die Lizenzgebühren sind typischerweise Downtime-Fees, Pönalen, Haftungsbegrenzungen, die Tragung von am Sitzstaat des Kunden anfallenden Abgaben und Steuern sowie SLC stark zu Gunsten des Cloud-Providers ausgestaltet. Gerade das Thema Steuern ist heikel: Der Anbieter sieht regelmäßig vor, dass sämtliche am Sitz des Kunden anfallende Abgaben und Gebühren – insbesondere auch Abzugssteuern – von letzterem zu tragen sind. Die Abzugssteuern sind aber eine Besteuerung des Einkommens des Ausländischen Providers im Inland. Hier würde der Kunde also die fällige Einkommenssteuer des Providers tragen.
- Laufzeit und Kündigung
  Üblicherweise ist eine beschränkte Laufzeit mit automatischer Verlängerung, aber ohne ordentliche Kündigungsmöglichkeit vorgesehen. Alternativ gibt es auch unbefristete Verträge mit Kündigungsmöglichkeiten. Bei größeren Projekten wird manchmal auch eine vorgelagerte Pilotphase mit eingeschränktem Umfang vereinbart, um eine Heranführung des Kunden an die Cloudlösung zu ermöglichen. In jedem Fall ist bei der Vertragsbeendigung drauf zu achten, dass – insbesondere bei fehlendem internen Back-Up beim Kunden – auch nach Vertragsbeendigung oder im Insolvenzfall des Cloud-Providers ein effektiver Zugriff auf die eigenen Daten mitsamt Rücktransfermöglichkeit besteht und genug Zeit zum Umstieg auf ein alternatives System – sei es ein Drittanbieter oder zurück auf die eigene IT-Infrastruktur des Kunden – bleibt.
- Rückführung und Löschung der Daten
  Die Standardverträge der Cloud-Provider sehen idR eine 90 bis 180-tägige Frist zur Rückholung der eigenen Daten vor. Dabei ist meist nur rudimentär festgelegt, ob dies technisch mithilfe der ohnedies im Rahmen der Nutzung der Services zur Verfügung stehenden Tools möglich ist. Je nach Art und Umfang der Daten ist daher frühzeitig intern abzuklären, ob (i) die notwendigen Hilfestellungen und Software

im Leistungsumfang inkludiert (und daher ausreichend lizenziert) sind, (ii) eine Rückführung mithilfe dieser Tools sinnvoll möglich und (iii) innerhalb der Zeit auch umgesetzt werden kann. Aus datenschutzrechtlicher Sicht ist zudem klarzustellen, dass und wann der Anbieter die Daten nach erfolgreicher Rückübernahme nachweisbar und irreversibel löschen muss. Hier ist in der Praxis aufzupassen, dass die beiden gegenläufigen Interessen – Datenspeicherung zur Überleitung und Löschung – so auf einander abgestimmt sind, dass es zu keiner vorzeitigen Beseitigung kommt.

- Anwendbares Recht und Gerichtsstand
  Klassischerweise ist bei Cloudverträgen US, UK, Irisches oder maximal luxemburgisches Recht vorgesehen. Aufgrund fehlender Vollstreckungsabkommen mit den USA und den noch nicht final abschätzbaren Folgen des Brexit ist die Wahl eines EU-Rechts jedenfalls zu bevorzugen. Bei ausländischer Rechtswahl ist es umso wichtiger, ein umfangreiches Mapping mit zwingenden österreichischen Bestimmungen durchzuführen, um diese an den Cloud-Provider vertraglich überbinden zu können.

Obwohl – je nach Umfang und Kritikalität der Auslagerung – relevant, fehlen jedoch die folgenden Regelungen typischerweise in den Standarddokumenten der Cloud-Provider:

- Effektive Audit- und Kontrollrechte;
- (Direkte) Steuerungsmöglichkeiten bei Subunternehmen;
- Resolving Times im Rahmen von SLA;
- Nachwirkung und/oder Beendigungsunterstützung bei Vertragsauflösung;
- Geeignete Garantien zur Eindämmung des Risikos eines Zugriffs durch ausländische Behörden; und
- Branchenspezifische Besonderheiten (zB für Banken, Versicherungen, Life Science).

2.5. Lizenzmodell auf den konkreten Bedarf optimieren

Am vom Cloud-Provider angebotenen Grundset lässt sich aufgrund des zugrundeliegenden Geschäftsmodells nicht rütteln: So erhält der Kunde gegen laufendes Entgelt das nicht-exklusive Recht zur Nutzung der Software, Plattform oder sonstigen Services. In seltenen Fällen kann – so solche Leistungen überhaupt erforderlich sind und angeboten werden – für abgegrenzte Bereiche wie zB zusätzliches Customizing oder Individualprogrammierungen auch ein exklusives Werknutzungsrecht eingeräumt werden. Der Fokus der Vertragsverhandlungen muss jedoch klar auf dem intern in einem ersten Schritt zu erhebendem Bedarf und geplanten Umfang aufbauen:

- Ist die Vertragsdauer bzw Kündigungsfrist für das Projekt geeignet? Ist eine Übergangsfrist vorgesehen? Zu welchen Konditionen ist eine Verlängerung möglich?
- Ist eine weltweite bzw sämtliche Standorte abdeckende Nutzungsmöglichkeit eingeräumt?
- Besteht die Möglichkeit der Nutzung im gesamten Konzern? Ist der spätere Beitritt neuer Konzerngesellschaften sowie das Ausscheiden aus dem Konzern geregelt?
- Können die Services auch durch Dritte im notwendigen Umfang genutzt werden (zB Einbeziehung von Beratern oder Wirtschaftsprüfern; Kunden)?
- Nach welchen Kriterien erfolgt die Abrechnung (Useranzahl; genutzte Kapazitäten; Mischformen)? Welches Konzept passt für das Unternehmen bzw Projekt am besten?
- Welche Leistungen sind abgedeckt; was sind Zusatzleistungen? Was kosten letztere? Welcher Bedarf wird gedeckt – wo bedarf es Zukäufe bei Dritten?

- Wie erfolgt die Lizensierung – direkt oder über einen Dritten Zwischenhändler (Reseller)? Letzteres löst auch vertraglichen Regelungsbedarf aus.
- Wenn es einen Implementierungsbedarf oder eine schrittweise Einführung in das Unternehmen gibt, ist für den Anfang eine Lizensierung nur der absolut notwendigen Grundlizenzen mit kostengünstiger Aufstockmöglichkeit zu empfehlen. Je nach Anbieter sind Testlizenzen oder eben ein Minimumset möglich.
- Vereinbarung von Volumsrabatten bei Erreichung gewisser Lizenzzahlen sowie von "*bad weather conditions*" bei Nichterreichen der Mengenzielen. Damit wird positiv ein wechselseitiger Anreiz bzw für den worst case Preissicherheit geschaffen.

Sobald der benötigte Lizenzbedarf bzw die Struktur erhoben und mit dem Anbieter – auch kommerziell – vereinbart ist, sind die Vertragskonditionen mit dem vereinbarten Nutzungsumfang abzugleichen und erfahrungsgemäß nachzuziehen. Gerade bei der Konzernnutzung – ein Unternehmen erwirbt die Lizenzen für weitere Tochterunternehmen; im Extremfall nicht einmal für sich selbst, sondern als IT-Beschaffungsorganisation nur für die operativen Gesellschaften – besteht regelmäßig Anpassungsbedarf. Auch an diesem Beispiel sieht man, wie wichtig die gemeinsame Verhandlung sämtlicher Vertragsteile ist. Andernfalls entstehen kaum bis nicht sanierbare Lücken, die sich im Ernstfall negativ auswirken können.

3. Schwerpunkt: Datenschutzrechtliche Aspekte

3.1. Datenschutzrechtliche Ausgangslage

Cloud-Provider sind als Auftragsverarbeiter iSd Art 4 Z 8 DSGVO einzuordnen – der Kunde ist und bleibt somit datenschutzrechtlicher Verantwortlicher. Vor der Auswahl eines Auftragsverarbeiters ist dementsprechend eine sorgfältige Prüfung des Cloud-Providers durchzuführen und zu dokumentieren. Dabei kann in der Praxis für den technischen Bereich auf zahlreiche Zertifizierungen und Auditberichte zurückgegriffen werden. Die ebenfalls erforderliche rechtliche Validierung, ob in dem Niederlassungsland des Cloud-Providers die Rechte und Freiheiten der Betroffenen ausreichend gewahrt sind, findet in der Praxis bisher aber de facto nicht statt (für Details siehe dazu unten Pkt 3.3).

Bei Vertragsabschluss ist für die Datenschutz-Compliance zwingend eine Auftragsverarbeitungsvereinbarung abzuschließen. Während die Mindestinhalte nach Art 28 DSGVO in den Standardverträgen der Cloud-Provider üblicherweise bereits abgebildet sind, sind die folgenden Bereiche in der Regel nur rudimentär ausgestaltet. Hier besteht der jeweils ausgeführte Nachjustierungsbedarf:

- <u>Eingeschränkte oder gar fehlende Steuerungsmöglichkeit für Subunternehmen</u>
  In Cloud-Verträgen fehlt regelmäßig die Zusage der Offenlegung sämtlicher eingesetzter und das gesetzlich notwendige Widerspruchsrecht bei Austausch bestehender oder Hinzuziehung neuer Subunternehmen. Auch direkte Weisungs-, Durchgriffs- oder andere Steuerungsrechte sind üblicherweise nicht enthalten. Hier besteht daher dringender Anpassungsbedarf, insbesondere, wenn einzelne Subunternehmen in (unsicheren) Drittstaaten niedergelassen sind (siehe dazu auch Pkt 3.2.).
- <u>Eingeschränkte Auditrechte, Kooperation mit für den Kunden zuständigen Behörden</u>
  Sowohl für den Kunden selbst als auch für die zuständigen Behörden sind standardmäßig starke Einschränkungen vorgesehen. Üblicherweise sieht der Cloud-Provider eine Pflicht zur Vorankündigung, eingeschränkte Betretungs- und Einsichtsrechte oder hohe Kosten vor. Regelmäßig sind individuelle Einsichtsrechte komplett ausgenommen und es werden dem Kunden stattdessen nur standardisiere

Auditberichte zur Verfügung gestellt. Je nachdem, ob solche Auditberichte zertifiziert sind oder nicht und in welcher Branche der Kunde tätig ist, sind diese für die Grundbedürfnisse ausreichend. In regulierten Bereichen, wie bei Banken- und Versicherungen, sind aber jedenfalls auch für den Kunden on-side Audits erforderlich. Unabhängig von der Branche dürfen und können Behördenrechte nicht eingeschränkt werden.

- Übermäßige Kooperation mit US-Behörden
  Vor dem Hintergrund der Niederlassung der meisten Cloud Anbieter bzw ihrer Muttergesellschaften in den USA sind in Cloudverträgen oftmals an den geltenden US-Bestimmungen orientierte Kooperations- und Mitwirkungspflichten bei Anfragen von US-Behörden sowie Compliance mit US-Vorschriften vorgesehen. Im Bereich des Sanktionsrechts ist eine entsprechende Zusage des Kunden unumgänglich, aber auch unschädlich. Hinsichtlich der regelmäßig festgeschriebenen Zusammenarbeit mit US-Behörden bei Datenherausgabeansprüchen stellen sich aber schwerwiegende Themen. So besteht dafür in der DSGVO keine Rechtsgrundlage, was im Ernstfall zu empfindlichen Strafen führen kann (siehe dazu und Lösungsvorschläge in Pkt 3.3.).
- Wenig bis kein Support bei Betroffenenrechten
  Regelmäßig bieten Cloud-Provider zur Erfüllung der Betroffenenrechte nur bestimmte Funktionen oder Tools innerhalb der Services an. Darüber hinaus fehlt oft ein effektives Unterstützungsangebot. In den seltenen Fällen, in denen zusätzlicher Support angeboten wird, ist dieser meist mit vergleichbar hohen Kosten verbunden. Hier ist ein angemessener Ausgleich zu finden, damit der Kunde seinen gesetzlichen Verpflichtungen nachkommen kann, da gerade die Verletzung von Betroffenenrechten in der Praxis der häufigste Auslöser für Beschwerden bei der Datenschutzbehörde ist. Bei wiederholten oder schwerwiegenden Verstößen kann das auch empfindliche Geldstrafen auslösen.
- Zusage konkreter IT-Sicherheitsmaßnahmen statt Zusage der Enthaltung des sich laufend weiterentwickelnden Stands der Technik
  Nicht nur in der Cloud sondern allgemein bei IT-Services versuchen Anbieter statt der erforderlichen Zusage der Einhaltung der angemessenen Sicherheitsmaßnahmen nach Art 32 DSGVO lediglich bestimmte, vorab vereinbarte Maßnahmen zuzusagen. Damit liegt es dann am Kunden, diese mit dem Stand der Technik abzugleichen und zu entscheiden, ob er den Vertrag so abschließen kann. Damit wird die Entscheidung und damit auch das Risiko, ob die getroffenen Maßnahmen datenschutzkonform sind, zur Gänze an den Kunden ausgelagert. Das ist per se schon heikel, da dem Kunden oftmals die notwendige IT-Expertise fehlt. Noch kritischer ist allerdings, dass durch die Vereinbarung gewisser Sicherheitsstandards eine Versteinerung eintritt, die die mit der DSGVO eigentlich intendierte, dynamische Anpassung an den jeweiligen technischen Fortschritt untergraben wird. Hier sehen Anbieter daher regelmäßig vor, dass sie nach eigenem Gutdünken sehr wohl Anpassungen vornehmen können. Der Kunde hat diese wieder zu prüfen und kann maximal den Vertrag kündigen, aber nicht steuernd eingreifen. Auch dadurch kommt es zu einer Risikoverlagerung. Diese Punkte sind in der Praxis wegen des Standardmodells schwer verhandelbar. Dementsprechend ist eine regelmäßige technische Evaluierung sowie eine rasche Reaktion, falls Missstände bekannt werden, notwendig.

Sofern der Cloud-Provider und/oder dessen Subunternehmen auch außerhalb des EWR niedergelassen sind, ist sicherzustellen, dass auch dort das europäische Datenschutzniveau eingehalten wird. Dafür gibt es in Art 46 ff DSGVO unterschiedliche Lösungsansätze, wie solche geeigneten Garantien umgesetzt werden können. In der Praxis sind hier vor allem

Angemessenheitsbeschlüsse der EU-Kommission – wie zB das EU-US Privacy Shield bis zum Juli 2020 – relevant. Damit erklärt die Kommission nach eingehender Prüfung der rechtlichen Rahmenbedingungen den Datenschutzstandard in konkreten Drittstaaten – gegebenenfalls eingeschränkt auf zertifizierte Unternehmen– als gleichwertig mit dem der EU. Zwar ist im Juli 2020 das für die Praxis wichtigste Abkommen, nämlich das Privacy Shield, gekippt worden, wodurch die auf dessen Basis bisher zertifizierten US-Gesellschaften daher nicht mehr als sicher einzustufen sind. Dennoch gibt es aber noch mit einer Vielzahl weiterer Staaten entsprechende Gleichstellungen wie zB für die Schweiz, Kanada, Israel oder Japan. Gibt es keinen Angemessenheitsbeschluss – oder ist ein bestehender nicht verlängert oder aufgehoben worden –besteht daneben auch die Möglichkeit des Abschlusses von Standarddatenschutzklauseln ("SCC") zwischen dem Kunden und dem Cloud-Provider. Mit diesen kann ein Datentransfer zu einem konkreten Unternehmen in einem sonst unsicheren Drittstaat dadurch gerechtfertigt werden, dass es sich vertraglich vorgegebenen Selbstverpflichtungen unterwirft (zu den Besonderheiten für den Abschluss von SCC als Ersatz für die Privacy Shield Zertifizierung für US-Anbieter siehe im Detail Pkt 3.3.).

3.2. Einsatz und Steuerung von Subunternehmen

Aus datenschutzrechtlicher Sicht ist eine effektive Steuerungsmöglichkeit von Subunternehmern zwingend erforderlich: Der Kunde hat als Verantwortlicher sicherzustellen, dass er etwaige Betroffenenansprüche oder Behördenauflagen unverzüglich umsetzen kann. Darüber hinaus muss er auch in der Lage sein, bei etwaigen gesetzlichen Änderungen oder Entwicklung der einschlägigen Rechtsprechung rasch zu reagieren.

Die effektivste Steuerung, nämlich eine schriftliche Vorab-Genehmigung vor Hinzuziehung neuer Subunternehmer, ist in der Cloud aufgrund der Anzahl der involvierten Dienstleister und Datencenter weder praxistauglich noch realistisch erzielbar. Stattdessen stellt man in der Praxis auf eine Kombination aus Informations-, Widerspruchs- und Kündigungsrechten ab: Der Cloud-Provider muss den Kunden als Mindestmaß innerhalb einer angemessenen Frist vor Austausch oder Hinzuziehung eines neuen Subunternehmens informieren. Dem Kunden ist sodann – allenfalls eingeschränkt auf objektivierbare Gründe – ein Widerspruchsrecht eingeräumt. Für den Fall, dass der Cloud-Provider ohne den Subunternehmer nicht mehr in der Lage wäre, die geschuldete Leistung in der vereinbarten Qualität zu erbringen, ist ein Sonderkündigungsrecht zu vereinbaren. Einige Cloud Provider überspringen gleich das Widerrufsrecht und geben dem Kunden stattdessen direkt die Möglichkeit, den Vertrag zu beenden. Hier liegt es also direkt am Kunden, ob er den Subunternehmer akzeptiert oder die Zusammenarbeit auflöst. Dieser Mechanismus ist das absolute Mindestmaß, das vereinbart sein muss. Dabei ist bereits kritisch, dass der Kunde dazu gedrängt wird, den neuen Subunternehmer hinzunehmen und er keine Möglichkeit hat, auf Vertragserfüllung zu bestehen. Dementsprechend ist bei der Verhandlung des finalen Wortlauts sehr sorgfältig vorzugehen.

Zusätzlich zur erforderlichen Nachschärfung bei den Regelungen rund um die Hinzuziehung von Subunternehmen besteht aber auch der Bedarf an entsprechend erweiterten Auditrechten: So muss neben dem Weisungs- auch das Auditrecht explizit auf sämtliche Subunternehmen – sowohl für den Kunden als auch dessen Aufsichtsbehörden – ausgedehnt werden. Es ist daher auch in der Kette sicherzustellen, dass der Cloud-Provider dazu verpflichtet ist, sämtliche oder zumindest die wesentlichen Vertragsinhalte auch an alle Subunternehmen zu überbinden. Damit geht bereits denklogisch die Übernahme einer

vollumfänglichen Haftung für den Einsatz der Subunternehmen durch den Cloud-Provider einher – auch hier ist in der Praxis oftmals Hand anzulegen.

3.3. Besonderheiten bei Cloud-Providern mit Sitz in den USA

Mit der Schrems II Entscheidung des EuGH im Juli 2020 erreichte die bereits seit 2013 andauernde öffentliche Diskussion rund um die Datensicherheit in den USA einen neuen Höhepunkt: Seit 2013 vertritt Max Schrems den Standpunkt, dass in den USA kein ausreichender Schutz für dort gespeicherte personenbezogene Daten vor den Überwachungstätigkeiten der ansässigen Behörden gewährleisteten sei. Der EuGH ist dem mittlerweile bereits zwei Mal gefolgt und hat (i) 2015 das Safe Harbor Abkommen, und (ii) nun auch am 16.7.2020 zu C-311/18 das Privacy Shield Abkommen als dessen Nachfolger für ungültig erklärt. Beide waren sogenannte Angemessenheitsentscheidungen der EU Kommission, mit der eine Datenübermittlung an entsprechend zertifizierte Empfänger in den USA ohne weitere Erfordernisse zugelassen wurden. Inhaltlich hat der EuGH dabei hervorgehoben, dass die bekannten Überwachungsmöglichkeiten nach US-amerikanischen Recht (i) unverhältnismäßig seien und zudem (ii) für potenziell von diesen Programmen erfassten Personen außerhalb der USA keine wirksamen Rechtsbehelfe und Garantien vorsehen.

Daher war es nun kurzfristig notwendig, zur Ermöglichung des Datentransfers zu US-Providern als Alternative die schon erwähnten SCC zu vereinbaren. Viele große Cloud-Provider haben als lessons learnt aus dem Fall von Safe Harbor und der Vorhersehbarkeit der Angreifbarkeit des Privacy Shields diese bereits parallel mit ihren Kunden abgeschlossen. Wo das noch nicht der Fall ist, muss das nun kurzfristig nachgeholt werden. Die Standarddatenschutzklauseln sind nämlich im Gegensatz zu weit verbreiteten Mythen weiterhin aufrecht und gültig, wenn auch anpassungsbedürftig:

Die vom EuGH aufgezeigten datenschutzrechtlichen Risken aufgrund der US-amerikanischen Gesetzgebung sind strukturell. Sie betreffen daher jede Datenüberlassung in die USA unabhängig von Zweck, Umfang oder Rechtsgrundlage. Es ist daher erforderlich, in den SCC zusätzliche (strengere) vertragliche Pflichten vorzusehen, die die vom EuGH erkannten Risken des potentiellen Zugriffs durch US-Behörden mitigieren. Klassischerweise wird die grundsätzliche Kooperation des Cloud-Providers mit US-Behörden – meist überschießend (siehe oben Pkt 3.1) – unter dem Punkt "Third Party Requests" oder im Rahmen der Confidentiality Obligations geregelt. Diese Bestimmungen sind kritisch zu prüfen und durch möglichst frühzeitige Informationspflichten, der Verpflichtung des Cloud Providers sämtliche verfügbare Rechtsmittel auszuschöpfen und gezielte Sonderkündigungsrechte abzufedern.

Alternativ oder auch zusätzlich können auch technische Maßnahmen die Risken mitigieren und damit den Bedenken des EuGH auf faktischer Ebene Rechnung tragen: Bei bloßer Verwendung von anonymisierten Daten greift das Regime der DSGVO nicht. Wo das aus faktischen Gründen kein praktikabler Lösungsansatz ist, kann auch auf eine Verschlüsselung der Daten gesetzt werden. Ist sichergestellt, dass nur der Kunde über den Schlüssel zur Wiederherstellung von Klardaten verfügt, ist argumentierbar, dass selbst im Falle eines Zugriffs durch US-Behörden keine Einsichtsmöglichkeit und damit kein Risiko für den Betroffenen besteht.

4. Conclusio

4.1. Awareness und Verhandlungsstrategie

Sobald im Unternehmen die strukturelle Entscheidung, eine Auslagerung in die Cloud vorzunehmen, getroffen wurde, ist die Schaffung der erforderlichen Awareness bei allen Beteiligten – vom IT-Mitarbeiter über den Projektleiter bis hin zum Management – der notwendige erste Schritt. Dabei sind nicht nur die dargelegten rechtlichen wie auch technischen Stolperfallen sowie Kostenimplikationen zu beleuchten, sondern insbesondere auch die erforderliche Zeit für eine saubere Auswahl des Cloud-Providers, die strukturierten Vertragsverhandlungen und nachfolgendem Roll-Out im Unternehmen einzuplanen. Es sind daher frühzeitig ausreichend Ressourcen, Zeit und Budget zu schaffen und ein zwischen Legal, IT und Projektmanagement eng abgestimmter Zeitplan samt Verhandlungsstrategie festzulegen. Vor der ersten konkreten Kontaktaufnahme mit dem Cloud-Provider sind die zur Verfügung gestellten Standardverträge im Detail zu screenen, um in Zusammenschau mit dem Gesamtprojekt die wichtigsten Showstopper frühzeitig erkennen zu können. Auf dieser Basis lässt sich ein sorgfältiges Konzept zur weiteren Vorgehensweise erstellen. So kann der Fokus auf die wesentlichen Klauseln und zugehörigen kommerziellen Implikationen gelegt und das Risiko, sich durch fehlgeleitete Detaildiskussionen zu verirren, minimiert werden. Bloß kosmetische Vertragsanpassungen durch den Cloud-Provider oder beharrliche überbordende Änderungswünsche durch den Kunden und die damit einhergehenden Zeit- und Kostenimplikationen können so weitgehend vermieden werden.

Die Entscheidung für die Durchführung eines Cloudsourcings setzt somit aufgrund der dargelegten Rahmenbedingungen die Bereitschaft voraus, einem risikobasierten Ansatz zu folgen: Je nach Umfang und Kritikalität der Auslagerung sind mehr oder weniger Anpassungen im Vertrag oder in der Projektumsetzung erforderlich. Klares Ziel ist dabei aber immer ein ausgewogenes Ergebnis mit vertretbaren Restrisiken und sorgfältig ausgewählten mitigierenden Maßnahmen zu erreichen.

4.2. Zusammenfassung der wesentlichsten Showstopper

Selbst dringliche sowie scheinbar unwichtigere, kleinere Projekte oder fehlende eigene Marktmacht sind kein Anlass zur Akzeptanz unverhandelter Standardverträge. Vielmehr sind jedenfalls die folgenden Themen zu adressieren und bei Bedarf entsprechend nachzuverhandeln:

- Etwaig fehlende Steuerungsmöglichkeit
    - Kontrolle des SLA auf Tauglichkeit;
    - Prüfung, ob SLC vorhanden und angemessen sind;
    - Überprüfung Durchgriffs- und Widerspruchsrechte bei Subunternehmen.
- Prüfung effektiver Audit- oder Kontrollrechte
    - Möglichkeit der Kontrolle während der Laufzeit für den Kunden und zuständige Behörden?
    - Wie kann Kunde Compliance überprüfen?
- Kritische Prüfung Lizenzmodell
    - Kostenminimierendes Modell für die Anlaufzeit sicherstellen;
    - Fixierung von Volumsrabatten und bad weather Konditionen für den worst case;
    - Vermeidung zu hoher Kosten und/oder brach liegender Lizenzen;
    - Sicherstellung der notwendigen Nutzungsrechte im Konzern und für Dritte wie Kunden, Lieferanten oder Berater;

    - Abklärung von Zusatzkosten für erforderliche zusätzliche Leistungen und Funktionalitäten.
- Kritische Prüfung bei US-Datentransfer
    - Werden SCC vereinbart und sind diese im Lichte der Schrems II Entscheidung angepasst?
    - Sind Abfederungsmaßnahmen für potentielle Datenherausgaben an US-Behörden vorgesehen?
    - Sind Maßnahmen zur Wahrung von Betriebs- und Geschäftsgeheimnissen getroffen?
- Kündigungsregelungen
    - Passt das Konstrukt der Vertragslaufzeit zum Projekt?
    - Für welche Fälle gibt es Kündigungsmöglichkeiten? Wie sind die Fristen – angemessen, um Umstieg auf Drittprovider zu ermöglichen, gleichzeitig aber nicht zu lange, um ausufernde Kosten zu vermeiden;
    - Sind ausreichende Unterstützungsleistungen vereinbart, damit der Umstieg auch tatsächlich umgesetzt werden kann?
    - Ist ein zeitlich ausreichender und faktisch (technisch) umsetzbarer Datenzugang für den Kunden nach der Beendigung sichergestellt?

Autoren:

Dr Axel Anderl, LLM (IT-Law) ist Managing Partner bei DORDA Rechtsanwälte GmbH und leitet dort das IT/IP und Datenschutzteam sowie die Digital Industries Group (axel.anderl@dorda.at).

Mag Nino Tlapak, LLM (IT-Law) ist Rechtsanwalt im Team von Axel Anderl bei DORDA Rechtsanwälte GmbH und auf Datenschutzrecht, Cybersecurity und Cloudsourcing spezialisiert (nino.tlapak@dorda.at).