KAPITEL 6

Auftragsverarbeitung

Wir kommen nun zu einer im Cloud Computing besonders praxisrelevanten Rechtsgrundlage: der *Auftragsverarbeitung*. Die meisten Leserinnen und Leser werden schon einmal mit einem sogenannten *AV-Vertrag* in Berührung gekommen sein, da nahezu jedes Unternehmen heutzutage mit zahlreichen Lieferanten und Dienstleistern zusammenarbeitet.

Ob Cloud-Anbieter (wie AWS, Google, Microsoft oder ein weiterer Provider), IT-Systemhaus, IT-Security-Spezialist oder externe Lohn- und Gehaltsabrechnung – die Einschaltung spezialisierter Dienstleister im Wege des IT-Outsourcings bietet sich bei allen Leistungen an, die nicht zu den Kerntätigkeiten eines Unternehmens gehören. Neben der Erfahrung und dem Know-how eines Dienstleisters ist im Cloud Computing vor allem die flexible Nutzung externer Ressourcen attraktiv: Es werden nur diejenigen Kapazitäten bezahlt, die auch genutzt werden (*Pay per Use*).

Sind personenbezogene Daten Gegenstand einer Auslagerung, ist die Einschaltung eines externen Dienstleisters im Wege der Auftragsverarbeitung eine langjährige und beliebte IT-Outsourcing-Praxis. Ihr kommt daher gerade auch im Cloud Computing eine besondere Bedeutung zu. Aus diesem Grund haben Sie die Auftragsverarbeitung im Rahmen der »wichtigen Begriffe« auf Seite 76 bereits kurz kennengelernt. Im Folgenden wollen wir nun einen genaueren Blick auf dieses im Cloud Computing besonders praxisrelevante Rechtsinstrument des Datenschutzes werfen.

6.1 Hohe Praxisrelevanz im Cloud Computing

Die hohe Praxisrelevanz der Auftragsverarbeitung im Cloud Computing ist vor allem darauf zurückzuführen, dass die meisten Cloud-Computing-Szenarien IT-Outsourcing im klassischen Sinn sind. Sie entsprechen im Anbieter-Nutzer-Verhältnis also derjenigen Konstellation, die typischerweise auch der Auftragsverarbeitung zugrunde liegt. So besteht vor allem bei hochstandardisierten Cloud-Leistungen (wie Public Clouds) meist kein weiteres Ausführungsermessen des Anbieters. Der

Anbieter entscheidet also nicht über Zwecke und Mittel der Datenverarbeitung, sondern wird allein als »verlängerter Arm« bzw. »verlängerte Werkbank« des verantwortlichen Nutzers tätig. Das gilt im Grundsatz unabhängig davon, ob die Cloud eines großen Hyperscalers wie AWS, Google oder Microsoft genutzt wird oder ob auf die Cloud-Services eines anderen spezialisierten Anbieters zurückgegriffen wird, sofern die Voraussetzungen einer Auftragsverarbeitung vorliegen.

Die Auslagerung von Datenverarbeitungstätigkeiten an spezialisierte Dienstleister kann im Cloud Computing sämtliche IT-Outsourcing-Konstellationen betreffen. Sie kann also von der Auslagerung einzelner Ressourcen, Applikationen und Fachanwendungen (z. B. Office-Anwendungen wie bei Microsoft 365, Software für Buchführung oder Lohn- und Gehaltsabrechnung) bis hin zu einem vollständigen Übergang von Prozessen und Betriebsmitteln reichen.

Die Weitergabe personenbezogener Daten an einen Cloud-Anbieter auf Basis einer Auftragsverarbeitung ist vor allem deswegen beliebt, da personenbezogene Daten hiernach ohne Einwilligung des Betroffenen und ohne Vorliegen der Voraussetzungen eines sonstigen Erlaubnistatbestands in der Cloud eines externen Anbieters verarbeitet werden können. Neben der Rechtsgrundlage, auf die der Verantwortliche seine Verarbeitungstätigkeiten selbst stützt, bildet die Auftragsverarbeitung somit die Rechtsgrundlage, damit der Verantwortliche Daten an einen Cloud-Anbieter als Auftragsverarbeiter weitergeben kann. Diese sogenannte *Privilegierung* werden wir uns in Abschnitt 6.2 noch etwas genauer anschauen.

Hinweis: Hohe Relevanz der Auftragsverarbeitung als Rechtsgrundlage für die Datenweitergabe an einen Cloud-Anbieter

Die Auftragsverarbeitung bildet die Rechtsgrundlage für die Weitergabe personenbezogener Daten an einen externen Cloud-Anbieter. Dieser fungiert als Auftragsverarbeiter. Die Auftragsverarbeitung ist daher von hoher Praxisrelevanz im Cloud Computing. Neben der Rechtsgrundlage, auf die der Verantwortliche selbst seine Verarbeitungstätigkeiten stützt, bedarf die Datenweitergabe auf Grundlage einer Auftragsverarbeitung keiner weiteren Rechtsgrundlage.

Die *Auftragsverarbeitung* existierte in Gestalt der *Auftragsdatenverarbeitung* (oft vereinfacht als ADV bezeichnet) grundsätzlich auch schon vor der Datenschutzreform. Deren Voraussetzungen waren im alten Recht in § 11 BDSG a. F. und in der Anlage zu § 9 BDSG a. F. wiederzufinden. Da die Abkürzungen ADV und AVV von Personen, die sich nicht tagtäglich mit Datenschutzthemen beschäftigen, noch immer gern verwechselt werden, sind in nachstehender Box die Begriffe und Abkürzungen vor und nach der Datenschutzreform noch einmal zusammengefasst:

Hinweis: Früher ADV, heute AVV

Bezeichnung vor der Datenschutzreform (Bundesdatenschutzgesetz a. F.):
ADV = **A**uftrags**d**aten**v**erarbeitung

Der Vertrag wurde auch als *ADV-Vertrag* oder schlicht ADV bezeichnet.

Aktuelle Bezeichnung nach der Datenschutzreform (DSGVO):
AV = **A**uftrags**v**erarbeitung

Der Vertrag wird umgangssprachlich als *AV-Vertrag* oder schlicht AVV bezeichnet.

6.2 Definition der Auftragsverarbeitung und kennzeichnendes Privileg

Eine *Auftragsverarbeitung* liegt vor, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen *Auftragsverarbeiter* (z.B. Cloud-Anbieter) im Auftrag des *Verantwortlichen* (z.B. Cloud-Nutzer) auf Grundlage eines Vertrags erfolgt. Der Auftragsverarbeiter wird *im Auftrag* tätig und ist weisungsgebunden. Der Verantwortliche verbleibt im Rahmen einer Auftragsverarbeitung als »Herr über die Daten« weiterhin verantwortlich. Der weisungsgebundene Auftragsverarbeiter nimmt dagegen lediglich eine Hilfsfunktion ein. Er fungiert quasi als »verlängerter« Arm bzw. als »verlängerte Werkbank« des Verantwortlichen und verarbeitet die personenbezogenen Daten ausschließlich in seinem Auftrag.

Schauen wir uns noch einmal die Grundkonstellation im Schaubild an, wie Sie sie bereits im Rahmen der wichtigen Begriffe kennengelernt haben:

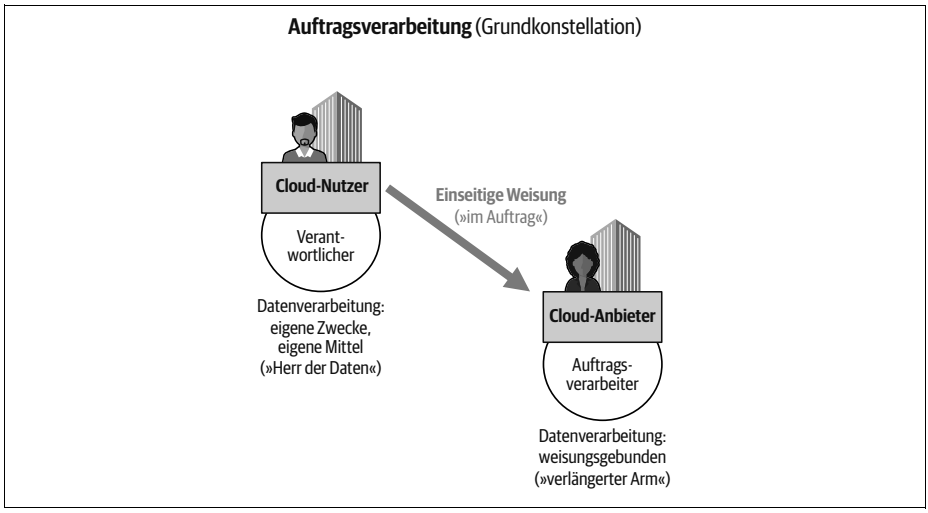

Abbildung 6-1: Grundkonstellation der Auftragsverarbeitung

Der Auftragsverarbeiter führt die Verarbeitung für den Verantwortlichen nicht als *Dritter* durch. Zwischen dem Verantwortlichen, der den Auftrag erteilt, und dem Auftragsverarbeiter besteht eine Art *Innenverhältnis*. Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet.

Die *Zwecke und Mittel* der Datenverarbeitung werden bei einer Auftragsverarbeitung vom Verantwortlichen festgelegt. Der weisungsgebundene Auftragsverarbeiter verarbeitet die Daten lediglich im Auftrag des Verantwortlichen und entscheidet damit weder ganz noch teilweise über die Zwecke und Mittel der Verarbeitung. Allerdings – und hierbei handelt es sich um eine oftmals nicht einfach zu beantwortende Rechtsfrage im Datenschutz – kann auch der Auftragsverarbeiter bestimmte Mittel der Verarbeitung selbst festlegen, soweit sie vertraglich an ihn delegiert wurden. Im Cloud Computing betrifft dies vor allem betriebliche, technische und organisatorische Maßnahmen sowie Details »im Hintergrund« der Datenverarbeitung, die der Cloud-Anbieter als Auftragsverarbeiter in seinem Verantwortungsbereich (vor allem Rechenzentrum, Serverbetrieb, eingesetzte Serverbetriebssysteme, Virtualisierungslösungen etc.) festlegt und bestimmt.

Zur Wiederholung: Auftragsverarbeitung

Als *Auftragsverarbeitung* wird jede Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen Auftragsverarbeiter im Auftrag des Verantwortlichen auf Grundlage eines Vertrags bezeichnet. Der Verantwortliche verbleibt als »Herr über die Daten«. Der weisungsgebundene Auftragsverarbeiter nimmt dagegen lediglich eine Hilfsfunktion ein und fungiert quasi als »verlängerter Arm« bzw. als »verlängerte Werkbank« des Verantwortlichen. Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet. Die meisten Cloud-Computing-Szenarien entsprechen im Anbieter-Nutzer-Verhältnis derjenigen Konstellation, die auch einer Auftragsverarbeitung zugrunde liegt.

Kennzeichnendes Element der Weitergabe von Daten an einen Auftragsverarbeiter im Wege der Auftragsverarbeitung ist ihre sogenannte *Privilegierung* gegenüber anderen Konstellationen der Datenweitergabe. Während deren Zulässigkeit ganz allgemein an den Voraussetzungen eines Erlaubnistatbestands als *Rechtsgrundlage* (etwa Einwilligung des Betroffenen, Datenverarbeitung zur Erfüllung eines Vertrags oder zur Wahrung berechtigter Interessen) zu messen ist, ist die Übermittlung von personenbezogenen Daten an den Auftragsverarbeiter sowie die weitere Verarbeitung durch diesen bereits auf Basis eines AV-Vertrags zulässig.

Anders ausgedrückt: Liegen die rechtlichen Voraussetzungen einer Auftragsverarbeitung vor (wie sie in Art. 28 DSGVO enthalten sind, also Abschluss eines entsprechenden AV-Vertrags), bilden sie die Rechtsgrundlage für die Datenweitergabe an den Auftragsverarbeiter. Die Datenweitergabe bedarf darüber hinaus keiner weiteren Rechtsgrundlage als derjenigen, auf die der Verantwortliche selbst seine

Verarbeitungstätigkeiten stützt. Die Datenweitergabe an den Auftragsverarbeiter auf Grundlage eines AV-Vertrags gilt insoweit als privilegiert.

Das Privileg hat einen besonderen Grund. Denn im Unterschied zu den anderen Konstellationen der Datenweitergabe verbleibt der Verantwortliche im Rahmen einer Auftragsverarbeitung weiterhin der »Herr der Daten«, und der weisungsgebundene Auftragsverarbeiter nimmt lediglich eine Hilfsfunktion ein (»verlängerter Arm« bzw. »verlängerte Werkbank« des Verantwortlichen). Die Auftragsverarbeitung stellt insoweit eine besondere Rechtsgrundlage für die Datenweitergabe an einen entsprechend weisungsgebundenen Auftragsverarbeiter dar.

Kurz erklärt: Privilegierung der Auftragsverarbeitung

Die Auftragsverarbeitung ist gegenüber anderen Konstellationen der Datenweitergabe insoweit privilegiert, als dass neben der Übermittlung von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch diesen auf Grundlage eines AV-Vertrags keine weitere Rechtsgrundlage als diejenige erforderlich ist, auf die der Verantwortliche selbst seine Verarbeitungstätigkeiten stützt.

Auch wenn der Auftragsverarbeiter nur eine Hilfsfunktion einnimmt, ist er dennoch ein *Empfänger* von Daten. Der Verantwortliche hat daher darauf zu achten, dass er den Auftragsverarbeiter in seinen Datenschutzerklärungen als *Empfänger* benennt (Art. 13 Abs. 1 lit. e i. V. m. Art. 4 Nr. 9 DSGVO), in Datenschutzauskünften der betroffenen Person mitteilt (Art. 15 Abs. 1 lit. c DSGVO) und auch im Verarbeitungsverzeichnis angibt (Art. 30 Abs. 1 lit. d DSGVO).

Für die Datenweitergabe eines Verantwortlichen an einen Auftragsverarbeiter werden im internationalen Kontext oftmals die Begriffe aus der englischen Sprachfassung der DSGVO verwendet: hier die Datenweitergabe *Controller to Processor* (C2P).

Werden Rechenzentren im Ausland genutzt (wie bei AWS, Google und Microsoft durch die Wahl der Datenverarbeitungsstandorte bzw. Verfügbarkeitszonen möglich), ist zusätzlich noch ein *angemessenes Datenschutzniveau* aufseiten des Empfängers außerhalb der EU erforderlich (sogenannte *2. Stufe* zu internationalen Datentransfers, siehe Kapitel 12).

6.3 Verarbeitung »im Auftrag« – Beispiele und Erscheinungsformen der Auftragsverarbeitung in der Praxis

Die Auftragsverarbeitung hat in der IT-Outsourcing-Praxis viele ganz unterschiedliche Gesichter. Ob auf Basis moderner und flexibler Abrechnungs- und Nutzungs-

modelle oder auf Grundlage klassischer Verträge mit langfristigen Laufzeiten: Externe Dienstleister werden heutzutage in ganz unterschiedlichen Szenarien mit der Verarbeitung von Daten beauftragt.

Ob hierbei im Anbieter-Nutzer-Verhältnis eine Verarbeitung *im Auftrag* vorliegt, hängt davon ab, wer über die Verarbeitungszwecke entscheidet. Als »Herr über die Daten« muss der Verantwortliche die Entscheidungsgewalt in den eigenen Händen haben und darüber bestimmen können, ob ein Auftrag überhaupt erteilt wird und zu welchem Ziel und Zweck die Daten verarbeitet werden. Auch wenn die Datenverarbeitung an sich auf den Auftragsverarbeiter übertragen wird, darf die Entscheidungsgewalt über die Daten gerade nicht mit übertragen werden.

Im Cloud Computing wird vor allem bei einem hohen Standardisierungsgrad der Leistung (wie vor allem in Public Clouds) meist kein weiteres Ausführungsermessen aufseiten des Cloud-Anbieters anzunehmen sein. Dieser entscheidet also nicht über Zwecke und Mittel der Datenverarbeitung. Es liegt daher keine eigenverantwortliche Datenverarbeitung vor, die über eine bloße Hilfs- und Unterstützungsfunktion hinausgeht.

Auch ist keine eigenverantwortliche Datenverarbeitung darin zu sehen, dass die Entscheidung über die technische und organisatorische Ausführung und Ausgestaltung der Verarbeitung (das »Wie« der Verarbeitung) an den Auftragsverarbeiter delegiert wird. Im Cloud Computing betrifft dies vor allem das technische und organisatorische Maßnahmenkonzept an einem Rechenzentrumsstandort.

Doch welche Verarbeitungsszenarien gelten als typische Beispiele für eine Auftragsverarbeitung im Sinne der DSGVO? Auch wenn es hierbei im Detail immer auf die Umstände des konkreten Einzelfalls ankommt, wollen wir zu einer besseren Veranschaulichung im Folgenden einen Blick auf typische Beispiele werfen, die im Anbieter-Nutzer-Verhältnis derjenigen Konstellation entsprechen, die einer Auftragsverarbeitung zugrunde liegt. Danach schauen wir uns Beispiele an, die keine Auftragsverarbeitung sind.

6.3.1 Typische Beispiele für eine Auftragsverarbeitung

Datenverarbeitungskonstellationen, in denen personenbezogene Daten durch einen *Auftragsverarbeiter* im *Auftrag des Verantwortlichen* verarbeitet werden, sind regelmäßig:

- IT-Outsourcing von IT-Infrastruktur und Anwendungen an spezialisierte Dienstleister (z. B. IaaS-/PaaS-/SaaS-/Hosting-Anbieter, E-Mail-Provider, Speicherplatzanbieter, Office-Anwendungen),
- Beauftragung externer Dienstleister mit Fernzugriff auf Daten (z. B. externe IT-Administratoren, die ihre Tätigkeiten remote erbringen),
- Betreuung von Webseiten bzw. Webshops durch Webagenturen (insbesondere Betreuung der Kontaktformulare und Kundenprofile),

- Beauftragung externer Dienstleister für die Einrichtung/Anpassung von Datenbanken zur Verwaltung von Kunden- oder Marketingkontakten,
- Auslagerung der Speicherung von Backups und externe Datenarchivierung,
- Scan von Dokumenten durch externe Dienstleister,
- Vernichtung oder Entmagnetisierung (*Degaussing*) von Festplatten und sonstigen Datenträgern durch einen externen Dienstleister,
- Einschaltung einer externen Marketingagentur für Kundenumfragen oder den Versand von Newslettern,
- Einschaltung externer Agenturen für die Auswertung von Webseitenanalysedaten,
- externe Dienstleister für Druckaufträge,
- externe Lohn- und Gehaltsabrechnung,
- externe Finanzbuchhaltung sowie
- Verarbeitung von Kundendaten durch externes Callcenter zwecks Kundenbetreuung (Support) ohne wesentliche eigene Entscheidungsspielräume in Bezug auf den Datenumgang.

Erfahrungsgemäß wird in der Praxis sehr schnell dazu tendiert, quasi jeden Dritten pauschal und undifferenziert als Auftragsverarbeiter anzusehen, der auch nur irgendwie mit personenbezogenen Daten in Berührung kommt. Dann möge noch schnell ein AV-Vertrag abgeschlossen werden, und das Thema »Datenschutz« könne damit abgehakt werden – so oftmals die landläufige Meinung in einigen Abteilungen.

Der Abschluss eines AV-Vertrags ist aber gerade nicht die allumfängliche Lösung des Themas Datenschutz. Im Gegenteil, ob und in welchen Fällen überhaupt eine Auftragsverarbeitung vorliegt, lässt sich mitunter gar nicht so leicht beantworten. Bereits kleine Details können einen Unterschied ausmachen. Besonders hilfreich sind hierbei auch Hinweise und Handreichungen von Datenschutzbehörden (wie z. B. Auslegungshilfen des *Bayerischen Landesamts für Datenschutzaufsicht*) oder von Branchenverbänden (wie z. B. Bitkom), die verschiedene Verarbeitungskonstellationen unter die Lupe genommen und datenschutzrechtlich bewertet haben. Sie sind auf den jeweiligen Webseiten veröffentlicht.

Praxistipp: Hinweise und Handreichungen der Aufsichtsbehörden für den Datenschutz

Die auf den Webseiten der Aufsichtsbehörden veröffentlichten Hinweise und Handreichungen von Datenschutzbehörden oder von Branchenverbänden können bei der datenschutzrechtlichen Einordnung einer speziellen Datenverarbeitungskonstellation unterstützen. Auch hier finden sich oft Praxistipps und Beispiele.

6.3.2 Keine Auftragsverarbeitung

Zum besseren Verständnis schauen wir uns im Folgenden aber auch einmal Verarbeitungsszenarien an, die keine Auftragsverarbeitung sind.

Keine Auftragsverarbeitung Dieser Fall liegt vor, wenn der Datenempfänger nicht im Auftrag tätig wird, sondern *eigenständig* mit den Daten umgeht. Er verarbeitet die Daten dann nicht als Auftragsverarbeiter, sondern als eigener Verantwortlicher. Insoweit hatte sich schon vor der Datenschutzreform zur Abgrenzung gegenüber einer Datenverarbeitung im Auftrag der Begriff der *Funktionsübertragung* etabliert. Keine Auftragsverarbeitung – sondern ein Handeln als eigener Verantwortlicher – liegt daher zum Beispiel vor, wenn ein Cloud-Anbieter personenbezogene Daten selbst erhebt (z. B. bei der AWS-Account-Registrierung die E-Mail-Adresse und Bestandsdaten des AWS-Kunden) und die Zwecke und Mittel der Verarbeitung festlegt. Auch von Berufsgeheimnisträgern (wie Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern) werden Daten in eigener Verantwortlichkeit verarbeitet. Sie liegt aber beispielsweise auch dann vor, wenn personenbezogene Daten an eine Bank weitergegeben werden, damit diese Überweisungsaufträge ausführen kann.

Des Weiteren liegt keine Auftragsverarbeitung vor, wenn eine Datenverarbeitung nicht Bestandteil der vertraglichen Leistung ist. Dies ist im Cloud- und Hosting-Umfeld vor allem bei solchen Dienstleistern der Fall, die mit personenbezogenen Daten gar nicht erst in Berührung kommen. Ein typisches Beispiel ist der Einsatz von allgemeinem Sicherheitspersonal, das allein zur Absicherung von Gebäude und Gelände eines Rechenzentrums zum Einsatz gelangt und keinen Zugang und Zugriff auf personenbezogene Daten hat.

Aber auch beim Einsatz von Reinigungspersonal in Büroräumen liegt grundsätzlich keine Auftragsverarbeitung vor, da das Reinigungsunternehmen mit Reinigungstätigkeiten und nicht mit der Verarbeitung personenbezogener Daten beauftragt ist. Hier sollte darauf geachtet werden, dass der Vertrag mit dem Reinigungsunternehmen eine Klausel enthält, die das eingesetzte Reinigungspersonal bei zufälliger Kenntniserlangung von personenbezogenen Daten zur Verschwiegenheit verpflichtet. Parallel hierzu sollten jedoch auch die eigenen Mitarbeiter angewiesen werden, ihren Arbeitsplatz so zu hinterlassen, dass personenbezogene Daten gar nicht erst von Reinigungspersonal oder sonstigen Dienstleistern zur Kenntnis genommen werden können.

Datenverarbeitungskonstellationen, in denen *keine Auftragsverarbeitung anzunehmen ist*, sind daher regelmäßig:

- Sicherheitsdienste und mit der Bewachung von Objekten (wie Rechenzentren) beauftragte Dienstleister,
- Datenverarbeitungstätigkeiten der Berufsgeheimnisträger (Rechtsanwälte, Steuerberater, Notare etc., etwa im Rahmen einer anwaltlichen oder steuerrechtlichen Beratung) und Insolvenzverwalter; diese Tätigkeiten in Ausübung des Berufs sind nicht zu verwechseln mit den besonderen berufsspezifischen An-

forderungen an Berufsgeheimnisträger, wenn diese Verarbeitungstätigkeiten wiederum selbst an Cloud-Anbieter outsourcen und hierfür Daten in eine Cloud hochladen und dort verarbeiten (siehe hierzu Kapitel 19),

- Reinigungsdienstleister,
- Handwerker,
- Zahlungsdienstleister und Bankinstitute mit Blick auf elektronische Zahlungen und den Geldtransfer sowie
- Versicherungsmakler.

6.3.3 Colocation als besondere Fallgestaltung im Rechenzentrumsumfeld

Colocation Ebenfalls keine Auftragsverarbeitung liegt bei der klassischen Reinform von *Colocation* (bzw. *Serverhousing*) vor. Dies sind Leistungen zur Unterbringung von IT-Systemen (Server, Switches, Router und sonstige IT-Infrastrukturkomponenten) im Rechenzentrum eines Colocation-Anbieters. Dieser stellt dem Kunden zum Betrieb seiner IT-Systeme geeignete Flächen und Serverschränke (*Racks*) in der Sicherheitsumgebung des jeweiligen Rechenzentrums zur Verfügung. Die am Markt verfügbaren Leistungen reichen von der Bereitstellung einzelner Racks auf einem für mehrere Kunden allgemein zugänglichen *Data Floor* bis hin zu der Bereitstellung von Racks in separaten Räumen, Brandschutzbereichen oder in physikalisch abgetrennten und hierdurch nochmals besonders gesicherten *Cages*. Der Anbieter sorgt regelmäßig auch für eine (mehrfach) redundante Stromversorgung sowie für die Anbindung der IT-Systeme an Datennetze (*Connectivity*), etwa durch Betrieb eines Backbone-Netzwerks, das an Carrier-Netzwerke und Netzknotenpunkte (z. B. DE-CIX, AMS-IX) angeschlossen ist und eine Datenkommunikation ermöglicht.

Bei Colocation befinden sich die IT-Systeme meist vollständig im Eigentum des Kunden und werden von ihm selbst in das Rechenzentrum eingebracht. Insoweit besteht ein Unterschied zum klassischen Hosting und Cloud Computing, wo sich die IT-Systeme im Eigentum des Anbieters befinden und einem Kunden zur Nutzung auf Zeit überlassen werden.

Unternehmen, die ihre Server und IT-Systeme im Wege von Colocation in einem Rechenzentrum unterbringen, profitieren von der sicheren Betriebsumgebung. Zugleich behalten sie die größtmögliche Kontrolle, da Betrieb und Administration der kundeneigenen IT-Systeme im Regelfall ausschließlich durch Personal des Kunden oder von ihm beauftragte Subunternehmer erfolgen. Daher ist auch vertraglich sicherzustellen, dass diese Personen Zugang zum Rechenzentrum haben und sich verpflichten, die Verhaltensregeln (z. B. *Acceptable Use Policies*) im Rechenzentrumsgebäude einzuhalten. Die IT-Systeme können aber auch in Hybrid- oder Multi-Cloud-Szenarien eingebunden werden, etwa als Private Cloud.

Bei dieser *Reinform* von Colocation erbringt der Colocation-Anbieter über die Bereitstellung von Rechenzentrumsfläche hinaus grundsätzlich keine weiteren Services mit Zugriffsmöglichkeiten auf personenbezogene Daten (z. B. *Remote Hands*, *Managed Services*). Seine Tätigkeiten beschränken sich allein auf die Bereitstellung der Sicherheitsumgebung sowie auf deren technische Wartung (z. B. Arbeiten an Stromzufuhr, Kühlung, Wärmeableitung etc.). Zugriffsmöglichkeiten auf personenbezogene Daten des Kunden bestehen keine. In einem solchen Fall ist daher kein Abschluss eines Auftragsverarbeitungsvertrags mit dem Colocation-Anbieter erforderlich. Allein der Umstand, dass sich die IT-Systeme des Kunden in den Räumlichkeiten des Colocation-Anbieters befinden, reicht für sich im Normalfall nicht aus, um eine Auftragsverarbeitung anzunehmen.

Dennoch werden in der Colocation-Praxis oftmals (rein vorsorglich) Auftragsverarbeitungsverträge abgeschlossen, da Colocation-Anbieter ihre Colocation-Leistungen häufig zusammen mit weiteren Services (z. B. *Remote Hands*, *Managed Services*) anbieten. Hierbei bestehen regelmäßig Zugriffsmöglichkeiten auf personenbezogene Daten durch Mitarbeiter des Colocation-Anbieters (z. B. Administrationstätigkeiten direkt im Rechenzentrum vor Ort auf dem IT-System des Kunden und auf dessen Weisung, etwa mithilfe eines Monitorwagens). In solchen Fällen ist wiederum ein AV-Vertrag zu schließen. Im Unterschied zu Standard-AV-Verträgen kann sich eine klarstellende Vorbemerkung (als Präambel oder Ähnliches) empfehlen, wonach auf die besondere Verarbeitungssituation bei Colocation hingewiesen wird. In seiner Reinform (Bereitstellung von Rechenzentrumsfläche) liegt grundsätzlich keine Auftragsverarbeitung vor, sodass die Parteien hieraus keine datenschutzrechtlichen Pflichten treffen. Sofern Gegenstand des Colocation-Vertrags aber auch Leistungen sind (bzw. im Bedarfsfall kurzfristig sein können, etwa beim Ausfall eines IT-Systems), in deren Rahmen ein Zugriff auf personenbezogene Daten besteht, liegt in den meisten Fällen eine Auftragsverarbeitung vor.

Praxistipp: Auftragsverarbeitungsvertrag bei Colocation

In der Praxis empfiehlt sich bei Colocation der Abschluss eines AV-Vertrags, sofern Colocation-Leistungen zusammen mit weiteren Services (z. B. *Remote Hands*, *Managed Services*) erbracht werden und hierbei Zugriffsmöglichkeiten auf personenbezogene Daten bestehen (z. B. unterstützende Administrationstätigkeiten auf den IT-Systemen des Kunden).

6.4 Beteiligte der Auftragsverarbeitung

Kommen wir nun zu den Beteiligten der Auftragsverarbeitung. In der Regel sind dies:

- der *Verantwortliche* (Cloud-Nutzer bzw. Kunde),
- der *Auftragsverarbeiter* (Cloud-Anbieter) sowie
- gegebenenfalls weitere in der Kette eingeschaltete *Subunternehmer* (bzw. *Unterauftragsverarbeiter*).

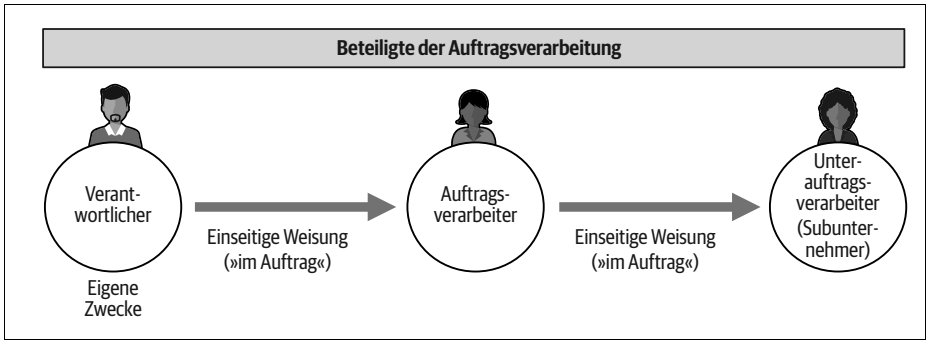

Abbildung 6-2: Verantwortlicher

Verantwortlicher (bzw. *Controller*) ist – wie Sie im Rahmen der wichtigen Begriffe unter Seite 73. gelernt haben – jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet und mit den personenbezogenen Daten von anderen natürlichen Personen im eigenen Interesse umgeht. Im Cloud Computing ist in aller Regel der *Cloud-Nutzer* datenschutzrechtlich verantwortlich, der als Kunde die Services eines Cloud-Anbieters zur Verarbeitung von personenbezogenen Daten nutzt.

Zur Wiederholung: Verantwortlicher (bzw. Controller)

Verantwortlicher ist jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche geht also – vereinfacht ausgedrückt – mit den personenbezogenen Daten von anderen natürlichen Personen im eigenen Interesse um. Im Cloud Computing ist dies in aller Regel der Cloud-Nutzer, der als Kunde die Services eines als Auftragsverarbeiter fungierenden Cloud-Anbieters nutzt. Im internationalen Umfeld ist es üblich, den Verantwortlichen als *Controller* zu bezeichnen (korrespondierender Begriff aus der englischen DSGVO-Sprachfassung).

Auftragsverarbeiter bzw. Processor *Auftragsverarbeiter* (bzw. *Processor*) sind alle natürlichen und juristischen Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Liegen die Voraussetzungen einer Auftragsverarbeitung vor, ist im Anbieter-Nutzer-Verhältnis der Cloud-Anbieter der Auftragsverarbeiter und wird als »verlängerte Werkbank« für den Verantwortlichen (Cloud-Nutzer bzw. Kunde) tätig.

Zur Wiederholung: Auftragsverarbeiter

Auftragsverarbeiter ist eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. In den typischen Cloud-Computing-Konstellationen ist der Cloud-Anbieter regelmäßig der Auftragsverarbeiter und wird als »verlängerte Werkbank« für seinen Kunden als Verantwortlichen tätig.

Subunternehmer bzw. Unterauftragsverarbeiter *Subunternehmer* bzw. *Unterauftragsverarbeiter* (*Sub-Processor*) sind alle Stellen, die als *weitere Auftragsverarbeiter* personenbezogene Daten im Auftrag des Auftragsverarbeiters in der weiteren Kette verarbeiten. Sie werden ebenfalls als »verlängerte Werkbank« weisungsgebunden tätig.

Kurz erklärt: Subunternehmer bzw. Unterauftragsverarbeiter

Subunternehmer bzw. *Unterauftragsverarbeiter* (*Sub-Processor*) sind alle Stellen, die als *weitere Auftragsverarbeiter* personenbezogene Daten im Auftrag des Auftragsverarbeiters in der weiteren Kette verarbeiten.

6.5 Voraussetzungen der Auftragsverarbeitung

Kommen wir nun zum Kern der Auftragsverarbeitung: ihren Voraussetzungen. Eine Auftragsverarbeitung setzt voraus, dass der Auftragsverarbeiter einerseits sorgfältig ausgewählt wurde und zum anderen zwischen den Parteien ein *Auftragsverarbeitungsvertrag* (ein sogenannter *AV-Vertrag* nach Art. 28 DSGVO, in der Praxis oft schlicht als AVV bezeichnet) abgeschlossen wurde. Der AV-Vertrag bildet die *Rechtsgrundlage* für die Weitergabe personenbezogener Daten an den Auftragsverarbeiter für die vertraglich festgelegten Verarbeitungszwecke.

6.5.1 Sorgfältige Auswahl

Jede Auftragsverarbeitung beginnt mit der *sorgfältigen Auswahl* des Auftragsverarbeiters. Vor Auftragsvergabe ist also zunächst zu prüfen, ob ein Anbieter überhaupt fachlich dazu geeignet ist, personenbezogene Daten gemäß den in der DSGVO enthaltenen Anforderungen zu Datenschutz und Datensicherheit als Auftragsverarbeiter zu verarbeiten. Der Verantwortliche darf nur solche Auftragsverarbeiter engagieren, die *hinreichende Garantien* dafür bieten, dass *geeignete technische und organisatorische Maßnahmen* für eine DSGVO-konforme Verarbeitung implementiert sind (vgl. Art. 28 Abs. 1 DSGVO). Der Verantwortliche hat den Auftragsverarbeiter dabei insbesondere im Hinblick auf dessen Fachwissen, Zuverlässigkeit und Ressourcen auszuwählen (vgl. Erwägungsgrund 81 DSGVO).

Hinweis: Auswahl des Auftragsverarbeiters

Die *sorgfältige Auswahl* des Cloud-Anbieters als Auftragsverarbeiter bezieht sich auf dessen fachliche Eignung. Es ist sicherzustellen, dass hinreichende Garantien dafür bestehen, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Kriterien für eine fachliche Eignung sind insbesondere Fachwissen, Zuverlässigkeit und Ressourcen des Cloud-Anbieters.

Die von einem Anbieter in technisch-organisatorischer Hinsicht konkret getroffenen und implementierten *hinreichenden Garantien* sind meist in einer *Liste der technischen und organisatorischen Maßnahmen* (TOMs) wiederzufinden, die sich an den Vorgaben des Art. 32 DSGVO orientiert. Bei zahlreichen Anbietern ist diese Liste – neben einer Auflistung der eingeschalteten Subunternehmer – der AV-Vertragsvorlage als Anhang beigefügt. Die *Liste der TOMs* oder andere diesbezügliche Informationen finden sich oftmals auch in den DSGVO-spezifischen Sektionen der Webseite oder in den Kundenportalen der Anbieter wieder. Ist dies nicht der Fall, sollte der Anbieter diesbezüglich kontaktiert werden. Zum Beleg von Garantien können auch genehmigte Verhaltensregeln oder bestehende Zertifizierungen des Auftragsverarbeiters herangezogen werden.

Es sollte darauf geachtet werden, dass sich die TOMs an den Anforderungen und Begriffen des Art. 32 DSGVO orientieren (und begrifflich nicht noch aus Zeiten des »alten« BDSG und dessen Anlage zu § 9 BDSG a. F. entstammen, wie sich vereinzelt noch beobachten lässt). Der Verantwortliche sollte zudem eine Plausibilitätskontrolle der vom Auftragsverarbeiter benannten technischen und organisatorischen Maßnahmen durchführen, da das Datenschutzniveau durch die Auslagerung der Verarbeitung nicht abgesenkt werden darf. Denn andernfalls wäre die Auswahl des Auftragsverarbeiters nicht sorgfältig und eine darauf gestützte Verarbeitung von Daten im Auftrag rechtswidrig.

Hinweis: Sorgfältige Auswahl anhand der anbieterseitig implementierten technischen und organisatorischen Maßnahmen

In der Praxis sind die *hinreichenden Garantien* eines Anbieters meist in der *Liste der technischen und organisatorischen Maßnahmen* (TOMs) wiederzufinden. Diese sind einem AV-Vertrag regelmäßig als Anhang beigefügt. Aber auch bestehende Zertifizierungen können zum Beleg hinreichender Garantien herangezogen werden.

6.5.2 Abschluss eines AV-Vertrags

Eine Auftragsverarbeitung erfordert im nächsten Schritt sodann einen Vertrag zwischen dem auslagernden Unternehmen als Verantwortlichem und dem Cloud-Anbieter als Auftragsverarbeiter. In diesem schriftlich oder in einem elektronischen Format abzufassenden *Auftragsverarbeitungsvertrag* bzw. *AV-Vertrag* (englisch *Data Processing Agreement* bzw. DPA) sind vor allem Gegenstand, Art und Zweck der Verarbeitung sowie die Weisungs- und Kontrollrechte des Auftraggebers festzuschreiben. Es sind aber auch Regelungen darüber zu treffen, was mit den Daten nach Abschluss der Auftragsverarbeitung geschehen soll.

Hinweis: AV-Vertrag (AVV) = Data Processing Agreement (DPA)

Der deutschen Bezeichnung *AV-Vertrag* (bzw. kurz AVV) entspricht der englische Begriff *Data Processing Agreement* (bzw. kurz DPA). Englische Bezeichnungen sind vor allem bei US-Cloud-Anbietern wiederzufinden. So heißt bei AWS der AV-Vertrag *AWS GDPR Data Processing Addendum* und ist ein Anhang zu dem *AWS Customer Agreement*. Bei Google heißt das korrespondierende Dokument für die Google Cloud Platform *Data Processing and Security Terms*. Bei Microsoft ist das Dokument auch in deutscher Sprache verfügbar und heißt *Nachtrag zum Datenschutz für Microsoft-Produkte und -Services*. Diese Dokumente lernen Sie in Kapitel 21 noch näher kennen.

Die inhaltlichen Mindestanforderungen an einen AV-Vertrag sind in Art. 28 Abs. 3 DSGVO enthalten. Ein AV-Vertrag hat hiernach vor allem zu den folgenden Punkten Festlegungen zu enthalten:

- zu den *Vertragsparteien* des AV-Vertrags, Cloud-Nutzer (Verantwortlicher) und Cloud-Anbieter (Auftragsverarbeiter) sind namentlich zu benennen
- zu *Gegenstand* und *Dauer* der Verarbeitung
- zu *Art* und *Zweck* der Verarbeitung

Hinweis: Gegenstand und Dauer sowie Art und Zweck der Verarbeitung

Der *Gegenstand* der Verarbeitung ist regelmäßig die Verarbeitung von Kundendaten. Die *Dauer* sowie *Art* und *Zweck* der Verarbeitung durch den Cloud-Anbieter als Auftragsverarbeiter ergeben sich grundsätzlich aus dem jeweiligen *Hauptvertrag* über die Bereitstellung von IT-Ressourcen und Anwendungen. Es ist daher darauf zu achten, dass der AV-Vertrag auf den Hauptvertrag Bezug nimmt und entsprechende Festlegungen enthält. Die AV-Verträge der verschiedenen Anbieter unterscheiden sich sehr in der Detailtiefe. Während einige kleinere Anbieter hier über

Freitextfelder oder Ankreuzmöglichkeiten umfassende Anpassungsmöglichkeiten vorsehen, arbeiten gerade die großen Hyperscaler mit nicht individualisierbaren Standardverträgen mit hohem Abstraktionsgrad und recht allgemein gehaltenen Formulierungen.

- zu *Art* der personenbezogenen Daten

Hinweis: Art der personenbezogenen Daten

Unter *Art* der personenbezogenen Daten sind die von der Auftragstätigkeit betroffenen Datenkategorien von Kunden, Lieferanten, Geschäftspartnern und Beschäftigten des Verantwortlichen (Cloud-Kunden) anzugeben. Beispiele hierfür sind: Stammdaten, Adressdaten, Mitarbeiter-/Personaldaten, Kontaktdaten, Bankverbindungsdaten, Daten von Videoaufzeichnungen von Überwachungskameras. Auch besondere Kategorien personenbezogener Daten (etwa Gesundheitsdaten) sind hier anzugeben.

- zu *Kategorien* betroffener Personen

Hinweis: Kategorien betroffener Personen

Der Punkt *Kategorien betroffener Personen* bezieht sich auf den Kreis der Personen, die durch die Datenverarbeitung durch den Cloud-Anbieter betroffen sind. Beispiele hierfür sind: Mitarbeiter, Kunden, Lieferanten, Interessenten, Bewerber, Auszubildende, Praktikanten, Berater.

- zu *Rechten* und *Pflichten* des Verantwortlichen

Hinweis: Rechte und Pflichten des Verantwortlichen

Der AV-Vertrag sollte Bestimmungen zur Verantwortlichkeit des Verantwortlichen und seiner Weisungsbefugnisse (einschließlich der Benennung weisungsbefugter Personen) enthalten.

- zu *Pflichten* des Auftragsverarbeiters:
  - Verarbeitung nur auf *dokumentierte Weisung* des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland,
  - Gewährleistung der Vertraulichkeit und Verschwiegenheit der Mitarbeiter,
  - Ergreifung aller erforderlichen technischen und organisatorischen Datensicherheitsmaßnahmen nach Art. 32 DSGVO (TOMs),

Hinweis: Unterstützung des Auftragsverarbeiters bei der Einhaltung von Datensicherheitspflichten

Der Auftragsverarbeiter hat den Verantwortlichen bei der Einhaltung der Pflichten nach Art. 32 DSGVO (siehe hierzu Abschnitt 9.5) zu unterstützen, da der Verantwortliche nach Art. 24 DSGVO selbst zur Umsetzung von geeigneten technischen und organisatorischen Maßnahmen verpflichtet ist, um eine DSGVO-konforme Verarbeitung sicherzustellen.

- rechtmäßige *Einschaltung von Subunternehmern/Unterauftragnehmern* (mehr ausführlich in Abschnitt 6.6)
- Unterstützung des Verantwortlichen, wenn *Betroffenenrechte* geltend gemacht werden (zu den Rechten der Betroffenen siehe Kapitel 14)
- Unterstützung des Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO (zur Datensicherheit Abschnitt 9.5 und zur Datenschutz-Folgenabschätzung siehe Kapitel 11)
- Löschung oder Rückgabe der personenbezogenen Daten nach Abschluss der Verarbeitungsleistungen
- Zurverfügungstellung von Informationen und Ermöglichung von *Überprüfungen/Kontrollen* durch den Verantwortlichen oder einen von diesem beauftragten Prüfer/Auditor

Praxistipp: Kontrollrechte

Der Verantwortliche sollte sich möglichst weitgehende Kontrollrechte einräumen lassen. Bei fehlendem Know-how aufseiten des Verantwortlichen empfiehlt es sich, die Kontrollen durch Sachverständige bzw. Auditoren durchführen zu lassen. Zahlreiche Anbieter verweisen in Bezug auf das Vorhandensein eines technischen und organisatorischen Maßnahmenkonzepts auch auf vorhandene Zertifizierungen, Audits und Prüfberichte (etwa ISO 27001 oder BSI C5).

Die vertraglichen Festlegungen zu den vorstehend genannten Punkten werden im Regelfall direkt im AV-Vertrag vorgenommen. In komplexen Datenverarbeitungskonstellationen kann es sich aus Platzgründen sowie für eine bessere Übersicht eventuell anbieten, bestimmte Angaben in einer Anlage zum AV-Vertrag festzuhalten.

Auch die Liste der von einem Anbieter implementierten technischen und organisatorischen Maßnahmen wird üblicherweise als Anlage dem AV-Vertrag beigefügt. Gleiches gilt für die vom Auftragsverarbeiter eingeschalteten Subunternehmer, die in einer *Subunternehmerliste* dem AV-Vertrag beigefügt werden oder durch einen im Vertrag enthaltenen eindeutigen Link in Bezug genommen werden.

6.5.3 Praxisprobleme bei Standardverträgen

Bei Cloud-Anbietern, die – wie die Hyperscaler – ihre Leistungen auf Basis von Standardverträgen mit hohem Abstraktionsgrad bereitstellen, besteht für individuelle vertragliche Festlegungen meist kein Spielraum. Dies ist darauf zurückzuführen, dass Anbieter nicht nur die zugrunde liegenden Prozesse und organisatorischen Abläufe, sondern auch die Verträge größtmöglich standardisiert bereitstellen wollen.

Soweit derartige Standardverträge einen solch hohen Abstraktionsgrad aufweisen, wie vonseiten der Aufsichtsbehörden unter anderem in Bezug auf die *Microsoft Office 365* zugrunde liegenden Kundenverträge und Datenschutznachträge kritisch vorgebracht wird, besteht oftmals nur die Möglichkeit der Wahl zwischen verschiedenen Anbietern und deren Standardverträgen. Kleinere Cloud-Anbieter sind hier erfahrungsgemäß eher bereit, nicht nur die Kundenverträge, sondern auch die AV-Verträge an die konkrete Datenverarbeitungssituation und an bestimmte Anforderungen eines Kunden anzupassen.

6.6 Einsatz von Unterauftragsverarbeitern (den sogenannten Subunternehmern)

Auch Cloud-Anbieter erbringen nicht alle Leistungen selbst. In den meisten Fällen ist sogar ein ganzes Netzwerk an weiteren Dienstleistern eingeschaltet. Dies können weitere Konzernunternehmen, aber auch Dritte sein. In der anbieterspezifischen Betrachtung in Kapitel 21 sind Links auf die von den Hyperscalern AWS, Google und Microsoft eingeschalteten Subunternehmer zu finden. Wer sich mit diesem Thema näher befassen und ein Gefühl dafür bekommen möchte, wie umfangreich diese weitere Leistungserbringung »in der Kette« weltweit sein kann, der sollte einmal diesen Links zu den Subunternehmerlisten der Hyperscaler folgen oder sie über Google suchen.

In der DSGVO heißen diese weiteren zur Verarbeitung personenbezogener Daten eingeschalteten Dienstleister *weitere Auftragsverarbeiter*. In AV-Verträgen finden sich aber häufig auch die Begriffe *Unterauftragnehmer*, *Unterauftragsverarbeiter* und *Subunternehmer*. Diese Begriffe sind grundsätzlich gleichbedeutend. Da sich nach dem subjektiven Empfinden des Autors vor allem die Bezeichnung als *Subunternehmer* einer hohen Beliebtheit bei Entscheiderinnen und Entscheidern in der IT-Branche erfreut, werden im Folgenden sämtliche *weiteren Auftragsverarbeiter* im Sinne der DSGVO zum Zwecke der Vereinfachung möglichst einheitlich als *Subunternehmer* bezeichnet. Ausnahmen werden dort gemacht, wo ein Cloud-Anbieter einen anderen Begriff verwendet (wie z. B. Microsoft in dem in Abschnitt 21.3 verlinkten *Nachtrag zum Datenschutz für Microsoft-Produkte und -Services*, wo die Bezeichnung *Unterauftragsverarbeiter* verwendet wird).

Cloud-Anbieter können auch bei der Auswahl und Beauftragung von Subunternehmern nicht nach Belieben verfahren. Als Auftragsverarbeiter haben sie bei der Vergabe von Unteraufträgen die diesbezüglichen Anforderungen der DSGVO zu beachten. Denn das Datenschutzniveau, das der AV-Vertrag im Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter sicherstellt, soll nicht durch die Einschaltung von Subunternehmern unterlaufen werden. Daher hat der Auftragsverarbeiter mit jedem Subunternehmer, der für die Verarbeitung personenbezogener Daten eingesetzt werden soll, ebenfalls einen AV-Vertrag zu schließen, der den Datenschutzpflichten und -anforderungen entspricht, die im AV-Vertrag mit dem Verantwortlichen festgelegt sind. Die Datenschutzpflichten werden auf diesem Weg an den jeweiligen Subunternehmer weitergereicht.

Subunternehmer »in der Kette« Weitere Subunternehmer können dabei nicht nur nebeneinander, sondern auch hintereinander »in der Kette« eingeschaltet sein. In diesem Fall hat der Auftragsverarbeiter sicherzustellen, dass die im AV-Vertrag zwischen Auftragsverarbeiter und Verantwortlichem festgelegten Datenschutzpflichten und -anforderungen auch in der weiteren Kette an jeden eingeschalteten Subunternehmer weitergegeben werden.

Regelungen in der DSGVO Die Regelungen für die Einschaltung von Subunternehmern sind in der DSGVO in Art. 28 Abs. 2 und Abs. 4 wiederzufinden. Zu unterscheiden ist hierbei zwischen:

- der *Genehmigung* der Subunternehmer durch den Verantwortlichen (Art. 28 Abs. 2 DSGVO) und
- der *Weiterreichung* der Datenschutzpflichten durch den Auftragsverarbeiter durch entsprechende vertragliche Vereinbarungen mit dem Subunternehmer (Art. 28 Abs. 4 DSGVO).

6.6.1 Genehmigung der Subunternehmer durch den Verantwortlichen

Nach der DSGVO bedarf jede Einschaltung von Subunternehmern der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen. Diese kann entweder im Wege einer *Einzelgenehmigung* oder einer *allgemeinen Genehmigung* erfolgen und ist – im Unterschied zu den Regelungen des Bürgerlichen Gesetzbuchs (BGB) – grundsätzlich im Sinne einer vorherigen Zustimmung (*Einwilligung*) zu verstehen. Da sich Genehmigungserfordernisse in den hochstandardisierten Prozessen der Cloud-Anbieter nicht so ohne Weiteres abbilden lassen, sind Fragestellungen im Zusammenhang mit der Genehmigung von Subunternehmern durch den Verantwortlichen ein häufig wiederkehrendes Thema und ein »Klassiker« in AV-Vertragsverhandlungen, sofern diese möglich sind und nicht abstrakte Standardverträge zum Einsatz kommen.

Einzelgenehmigung Zustimmungserfordernisse im Wege einer *Einzelgenehmigung* lassen sich in hochstandardisierten Bereitstellungsszenarien (gerade in Public Clouds mit einer hohen Zahl an Nutzern) nicht praxisgerecht umsetzen, etwa wenn einige Kunden nicht zustimmen oder sich gar nicht erst zurückmelden. Da der kurzfristige Einsatz eines Subunternehmers durch den Cloud-Anbieter in bestimmten Fällen aber betrieblich dringend erforderlich sein kann (z. B. kurzfristige Beauftragung von Wartungstechnikern oder Dienstleistern), könnte bereits ein einzelner Kunde den sicheren Betrieb einer Cloud-Plattform behindern.

Allgemeine Genehmigung Aus Gründen der Standardisierung und Praktikabilität werden Subunternehmer daher meist auf Grundlage einer *allgemeinen Genehmigung* eingeschaltet, gerade wenn Cloud-Anbieter ihre Leistungen gegenüber mehreren Kunden erbringen. Cloud-Anbieter müssen somit nicht bei jedem einzelnen Kunden die vorherige Zustimmung (*Einzelgenehmigung*) einholen, sondern können auf Grundlage einer allgemeinen Berechtigung Subunternehmer einschalten. Eine allgemeine Genehmigung ist in der DSGVO dabei nicht zivilrechtlich, sondern eher im Sinne einer *allgemeinen Berechtigung* zu verstehen. Im AV-Vertrag ist festzulegen, ob diese generell oder nur für bestimmte Gruppen von Subunternehmern gelten soll. Im Fall einer allgemeinen schriftlichen Genehmigung hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung zu informieren. Dies gilt sowohl in Bezug auf die Hinzuziehung als auch die Ersetzung von Subunternehmern. Im Gegenzug ist dem datenschutzrechtlich verantwortlichen Kunden aber die Möglichkeit einzuräumen, gegen Subunternehmer Einspruch zu erheben, mit denen er sich nicht einverstanden erklärt.

Subunternehmer Vor Abschluss eines AV-Vertrags sollten in Bezug auf die Subunternehmer zwei Konstellationen im Auge behalten werden:

- die zum Zeitpunkt des Vertragsschlusses bereits eingeschalteten Subunternehmer und
- die Subunternehmer, die künftig durch Hinzuziehung oder Ersetzung eines bestehenden Subunternehmers eingeschaltet werden.

Mit Blick auf die zum Zeitpunkt des Vertragsschlusses bereits eingeschalteten Subunternehmer sollte vor Abschluss eines AV-Vertrags darauf geachtet werden, dass der Cloud-Anbieter eine aktuelle Liste der eingesetzten Unterauftragnehmer zur Verfügung stellt (*Subunternehmerliste* als Anlage zum AV-Vertrag, auf Webseiten, in Kundenportalen etc.).

Praxistipp: Subunternehmerliste

Es sollte vor Abschluss eines AV-Vertrags darauf geachtet werden, dass der Cloud-Anbieter eine aktuelle Liste der eingesetzten Unterauftragnehmer zur Verfügung stellt.

Gerade AWS, Google und Microsoft haben in ihrem weltweiten Netz an Rechenzentren zahlreiche Subunternehmer eingeschaltet, die aus verschiedenen Konzerngesellschaften und externen Dritten bestehen (siehe Kapitel 21). Hier ist es anhand der auf den Webseiten verfügbaren Informationen in vielen Fällen jedoch nicht transparent, welcher Subunternehmer für welchen Service eingeschaltet ist. In vielen Fällen muss ein Cloud-Nutzer mit diesen Unklarheiten leben – ein Umstand, der gerade vonseiten der Aufsichtsbehörden immer wieder kritisiert wird, verbunden mit der Forderung nach weiterer Transparenz. Aber auch bei kleineren Anbietern fehlt es oftmals an Transparenz in Bezug auf die weiteren in der Kette eingeschalteten Subunternehmer, was dazu führen kann, dass ein Nutzer die tatsächliche Subunternehmerkette nicht mehr überblicken kann.

Informationspflicht des Kunden über künftige Subunternehmer Mit Blick auf *künftige* Subunternehmer, die durch Hinzuziehung oder Ersetzung eines bestehenden Subunternehmers zu einem späteren Zeitpunkt eingeschaltet werden, hat der Anbieter den Verantwortlichen über jede beabsichtigte Änderung zu informieren. Die *Information* über jede beabsichtigte Änderung kann etwa dahin gehend erfolgen, dass der Cloud-Anbieter dem Kunden proaktiv die Information über die Hinzuziehung oder Ersetzung von Subunternehmern so früh wie möglich mitteilt und ihm eine jeweils aktuelle Subunternehmerliste zur Verfügung stellt (z. B. per E-Mail, im Kundenportal zum Download oder auf einer Webseite).

Die Vertragsparteien können sowohl die Informationspflicht wie auch ein Einspruchsrecht vertraglich weiter spezifizieren, um beides an die konkreten Begebenheiten und Prozesse bei einem Anbieter anzupassen. So wird bei vielen Cloud-Anbietern die Informationspflicht im AV-Vertrag vor allem dahin gehend präzisiert, dass eine Liste im Kundenportal oder auf einer Webseite und eine Information des Kunden bei Änderungen ausreichend sein sollen. Derart anbieterfreundliche und praktikable Handhabungen der Informationspflicht werden von den Aufsichtsbehörden aber nicht immer befürwortet. Aktuelle aufsichtsbehördliche Entwicklungen sollten daher auch hier (z. B. durch das Abonnement fachspezifischer Newsletter) im Auge behalten werden.

Einspruchsrecht und Voraussetzungen des Einspruchs Da die DSGVO im Fall einer allgemeinen Genehmigung dem Kunden die Möglichkeit gibt, gegen Subunternehmer Einspruch zu erheben, sollte der AV-Vertrag Regelungen zu den Voraussetzungen und Rechtsfolgen eines Einspruchs enthalten. In der Praxis wird das Einspruchsrecht meist auf diejenigen Fälle beschränkt, in denen die Einschaltung eines weiteren Subunternehmers für den Kunden aus *wichtigem Grund* nicht zumutbar wäre. Der Einsatz eines Subunternehmers muss konkret die dem IT-Servicevertrag des Kunden zugrunde liegenden Leistungen betreffen. Das wäre etwa dann nicht der Fall, wenn der Subunternehmer an einem Rechenzentrumsstandort zum Einsatz gelangen soll, an dem sich gar keine vom Kunden genutzten IT-Systeme befinden. Es sind also Gründe erforderlich, die sich besonders nachteilig auf die weitere Ver-

tragsdurchführung auswirken und sich vom Cloud-Anbieter nicht durch angemessene Maßnahmen ausschließen lassen. Ein wichtiger Grund kann daher etwa vorliegen, wenn ernsthafte Zweifel bestehen, dass der Subunternehmer als zuverlässig anzusehen ist und keinen ausreichenden Schutz der zu verarbeitenden Daten gewährleisten kann. Aber auch der Einsatz eines Wettbewerbers des Cloud-Kunden als Subunternehmer kann für diesen einen wichtigen Grund darstellen.

Rechtsfolgen des Einspruchs Als Rechtsfolge des Einspruchs können sich Regelungen anbieten, wonach sich Cloud-Anbieter und Kunde zunächst zur Herbeiführung einer gütlichen Einigung verpflichten (z.B. Vorschlag des Anbieters, wie der Zugriff des Subunternehmers auf vom Kunden genutzte IT-Systeme ausgeschlossen werden kann). Für den Fall, dass keine gütliche Einigung möglich und die Einschaltung des Subunternehmers weiterhin unzumutbar ist, kann etwa ein Sonderkündigungsrecht vereinbart werden.

Praxistipp: Regelungen zu den Folgen eines Einspruchs

Bei einer allgemeinen Genehmigung zur Einschaltung von Subunternehmern durch den Cloud-Anbieter sollte ein AV-Vertrag Regelungen zu den Voraussetzungen, zum Umfang und zu den Folgen eines solchen Einspruchs enthalten.

Standardverträge Anbieter mit einer besonders hohen Anzahl an Kunden haben dagegen meist auch den Einsatz von Subunternehmern größtmöglich standardisiert und bieten oft keine Widerspruchsmöglichkeiten. Bei Standardverträgen verweisen Anbieter lediglich auf die Möglichkeit des Kunden, den Vertrag zu kündigen, wenn er mit einem Subunternehmer nicht einverstanden ist. Es bleibt einem Kunden damit letztendlich nur die Wahl, den Service so zu nutzen, wie er angeboten wird (einschließlich aller Subunternehmer), oder zu kündigen und zu einem anderen Anbieter zu wechseln. Die insoweit in der Praxis wiederzufindenden Prozesse und Möglichkeiten entsprechen mal einer strengeren, mal einer weniger strengen Umsetzung der DSGVO. Einige Umsetzungsvarianten von Anbietern lassen sich sogar nur sehr schwer mit der DSGVO in Einklang bringen, was für den Kunden als Auftraggeber letztendlich ein Risiko darstellt, da eine »DSGVO Compliance« oft nicht mehr gegeben ist.

6.6.2 Weiterreichung der Datenschutzpflichten an den Subunternehmer

Im Fall der Einschaltung eines Subunternehmers hat der Cloud-Anbieter die datenschutzrechtlichen Pflichten in der Kette weiterzureichen und mit dem Subunternehmer hinreichende Garantien über geeignete technische und organisatorische

Maßnahmen festzulegen. Eine oftmals gestellte Frage ist, ob sich der Verantwortliche im Vertrag mit dem Cloud-Anbieter ein direktes Kontrollrecht beim Subunternehmer (etwa im Wege eines Audits) einräumen lassen soll oder ob es stattdessen nicht ausreicht, dass der Cloud-Anbieter als Auftragsverarbeiter diese Kontrollen wahrnimmt. Letzteres erscheint etwas leichter und praxisgerechter in der Handhabung. Der Kunde kann als Verantwortlicher beim Audit des Cloud-Anbieters wiederum überprüfen, ob dieser auch seine Subunternehmer regelmäßig kontrolliert. Vor allem bei Standardverträgen und den Clouds der großen Hyperscaler sind Vor-Ort-Kontrollen quasi nicht möglich. Zum Nachweis technischer und organisatorischer Maßnahmen wird hier in der Praxis meist auf Zertifizierungen, Audits und Prüfberichte zurückgegriffen.

6.7 Auftragsverarbeitung im Ausland

Bei einer Auftragsvergabe an Auftragsverarbeiter im Ausland ist zu unterscheiden zwischen:

- *EU-/EWR-Ausland* (Auftragsverarbeiter, die auf EU-/EWR-Territorium personenbezogene Daten verarbeiten) und
- *Drittländern außerhalb von EU und EWR* (wie USA, Indien, China oder Russland).

Da die DSGVO für Datenverarbeitungen in *Drittländern* besondere Anforderungen enthält (hierzu mehr später in Kapitel 12), ist immer zu schauen, an welchen Standorten sich die Cloud-Infrastruktur eines Anbieters befindet, in der die Daten verarbeitet werden. Es ist hierbei auf den *Standort der Datenverarbeitung* und nicht auf die Nationalität oder den Sitz eines Cloud-Anbieters als datenverarbeitendes Unternehmen abzustellen. Liegen der Datenverarbeitung mehrere Standorte zugrunde, sind alle Standorte zu berücksichtigen. Dies kann sich dann als Herausforderung erweisen, wenn die Feststellung der konkreten Datenverarbeitungsstandorte aufgrund fehlender Transparenz oder bestimmter Sicherheitsinteressen (z.B. Standortgeheimnis) eines Cloud-Anbieters nicht eindeutig möglich ist. Bei Datenverarbeitungsszenarien, die über mehrere Standorte verteilt sind, reicht es aber aus, wenn anhand der Anbieterinformationen Bezugnahmen auf ein bestimmtes Territorium oder Regionen (z.B. Deutschland, Irland, Niederlande bzw. Frankfurt, München) möglich sind.

Der Unterscheidung zwischen EU-/EWR-Ausland und Drittländern kommt speziell bei der Nutzung der Hyperscaler-Clouds Bedeutung zu. Denn dort lassen sich quasi mit wenigen Mausklicks auch außereuropäische Datenverarbeitungsstandorte auswählen. Gerade bei AWS, Google und Microsoft stehen neben Standorten in der EU auch zahlreiche Regionen und Verfügbarkeitszonen außerhalb von EU und EWR zur Verfügung (wie Sie im Grundlagenkapitel in Abschnitt 2.7 gesehen haben).

6.7.1 Auftragsverarbeitung innerhalb von EU und EWR

Die Übermittlung von Daten an Auftragsverarbeiter mit Datenverarbeitungsstandorten innerhalb von EU und EWR unterliegt deshalb keinen zusätzlichen Anforderungen (wie z. B. der Abschluss von Standardvertragsklauseln bei Datenempfängern in Drittländern), da die DSGVO einen freien Datenverkehr innerhalb des EU-Binnenmarkts bezweckt und dies durch ein EU-weites, einheitliches Datenschutzniveau sicherstellt. Verarbeitet daher ein Verantwortlicher (z. B. ein Unternehmen mit Sitz in Deutschland) personenbezogene Daten durch einen Auftragsverarbeiter in Rechenzentren in der EU (z. B. in Österreich, Frankreich, Spanien, Irland oder den Niederlanden), liegt zwar eine Datenverarbeitung im europäischen Ausland vor, da sich die Daten jedoch weiterhin in der EU und mithin im Geltungsbereich der DSGVO befinden, kann diese Verarbeitung auf Grundlage der Auftragsverarbeitung erfolgen.

Beispiel: Datenverarbeitung in der EU (etwa in Österreich, Frankreich, Spanien, Irland oder den Niederlanden)

Verarbeitet ein Unternehmen aus Deutschland personenbezogene Daten in einem Rechenzentrum in der EU, kann dies im Wege einer Auftragsverarbeitung erfolgen. Insoweit bestehen bei der Nutzung von Datenverarbeitungsstandorten innerhalb der EU keine zusätzlichen Anforderungen.

6.7.2 Internationale Auftragsverarbeitung in Drittländern außerhalb von EU und EWR

Anders stellt sich die Situation bei der Übermittlung personenbezogener Daten an Auftragsverarbeiter mit Datenverarbeitungsstandorten außerhalb von EU und EWR dar (das betrifft z. B. eine außereuropäische *Region* oder *Availability Zone* von AWS, aber auch etwa eine Nutzung der Cloud-Ressourcen von Alibaba in China). Hier sind die besonderen Anforderungen an internationale Datentransfers zu beachten, die im 5. Kapitel der DSGVO enthalten sind. Denn die von der DSGVO sichergestellten Datenverarbeitungsstandards sollen nicht dadurch wieder unterlaufen werden, dass personenbezogene Daten außerhalb von EU und EWR in Ländern mit geringerem Datenschutzniveau verarbeitet werden. Ein Verantwortlicher hat daher auf einer 2. *Prüfungsstufe* das Vorhandensein eines *angemessenen Datenschutzniveaus* aufseiten des Datenempfängers zu prüfen, das in der Praxis vor allem durch den Einsatz von *Standardvertragsklauseln* bewerkstelligt werden kann, sofern es sich nicht wiederum um ein *sicheres Drittland* handelt, für das die EU-Kommission ein angemessenes Datenschutzniveau festgestellt hat (hierzu mehr in Kapitel 12).

6.8 Besonderheiten in regulierten Märkten

Besonderheiten im Bereich der Auftragsverarbeitung bestehen in regulierten Märkten, wie wir in Kapitel 19 noch sehen werden.

6.9 FAQs

Die folgenden *Frequently Asked Questions* (FAQs) zum Thema Auftragsverarbeitung sollen beim Einstieg in das Thema weiter unterstützen. Die Antworten verfolgen einen möglichst praxistauglichen Lösungsansatz. Es ist daher nicht auszuschließen, dass einige Aufsichtsbehörden für den Datenschutz im Detail eine (leicht) andere Ansicht vertreten bzw. in künftigen Stellungnahmen eine neue Position einnehmen werden. Insofern sind aktuelle Entwicklungen immer zu beachten.

Was ist eine Auftragsverarbeitung?

Die Auftragsverarbeitung ist eine besondere Form der Übertragung von Datenverarbeitungstätigkeiten auf externe Dienstleister. Sie liegt vor, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen Auftragsverarbeiter auf Grundlage eines AV-Vertrags im Auftrag des Verantwortlichen erfolgt. Der Verantwortliche verbleibt der »Herr der Daten« gegenüber dem weisungsgebundenen Auftragsverarbeiter, der lediglich eine Hilfsfunktion einnimmt und quasi als »verlängerter Arm« bzw. als »verlängerte Werkbank« des Verantwortlichen für ihn die Daten verarbeitet.

Ist neben dem AV-Vertrag noch eine weitere Rechtsgrundlage erforderlich, damit ich Daten an den Auftragsverarbeiter weitergeben kann?

Mit Abschluss eines AV-Vertrags bedarf es keiner weiteren Rechtsgrundlage, um die Daten an den Auftragsverarbeiter weitergeben zu können. Neben der Rechtsgrundlage, auf die der Verantwortliche selbst die von ihm durchgeführte Datenverarbeitung stützt, bildet der AV-Vertrag die Rechtsgrundlage für die Datenweitergabe an den Auftragsverarbeiter. Dies ist das sogenannte *Privileg* der Auftragsverarbeitung gegenüber anderen Rechtsgrundlagen für eine Datenweitergabe.

Ich bin mir nicht sicher, ob eine Datenweitergabe die Voraussetzungen einer Auftragsverarbeitung erfüllt. Was soll ich machen?

Überprüfen Sie die fragliche Datenweitergabe anhand der Beispiele in diesem Buch. Besprechen Sie den Sachverhalt zudem mit ihrem Datenschutzbeauftragten. Holen Sie, falls erforderlich, weiteren datenschutzrechtlichen Rat durch einen Anwalt ein. Liegt die Konstellation einer Auftragsverarbeitung vor, ist ein AV-Vertrag abzuschließen.

Kann ich auf einen Muster-AV-Vertrag aus dem Internet zurückgreifen?

Das ist grundsätzlich möglich. Allerdings sollte der Einsatz von Musterverträgen aus dem Internet mit Vorsicht geschehen. Denn einige der online wiederzufindenden Verträge sind teilweise veraltet und entstammen in Einzelfällen sogar noch den Zeiten vor der Datenschutzreform. Es sollte daher bevorzugt auf Vorlagen zurückgegriffen werden, die auf den Webseiten von einschlägigen Branchenverbänden oder Datenschutzbehörden veröffentlicht sind. Meist sind sie aber noch auf die konkreten Umstände der Datenverarbeitung anzupassen. Die meisten Cloud-Anbieter arbeiten auf Grundlage eigener standardisierter AV-Vertragsvorlagen, die auf die Begebenheiten bei diesem Anbieter zugeschnitten sind. Die jeweiligen AV-Verträge können auf der Webseite heruntergeladen und teilweise auch online abgeschlossen werden bzw. werden auf Anfrage bereitgestellt.

Ein Dokument mit der Bezeichnung »AV-Vertrag« finde ich bei meinem Anbieter nicht. Gibt es auch noch andere Bezeichnungen?

Ja, es kommt nicht auf die Überschrift des Vertrags an, sondern auf den Inhalt. Üblich sind Bezeichnungen wie *Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO* oder ähnlich. Bei englischsprachigen Verträgen finden Sie Bezeichnungen wie *Data Processing Agreement*. So heißt der Vertrag bei AWS beispielsweise *AWS GDPR Data Processing Addendum*, bei Google *Data Processing and Security Terms* und bei Microsoft *Datenschutznachtrag zu den Produkten und Services von Microsoft* (mehr hierzu in Kapitel 21).

Ich habe von meinem Cloud-Anbieter einen AV-Vertrag erhalten. Was sind die nächsten Schritte?

Prüfen Sie den AV-Vertrag. Die Checklisten und Ausführungen in diesem Buch können Ihnen hierbei bereits eine Hilfe sein. Sofern individuelle Anpassungsmöglichkeiten vorgesehen sind, ergänzen Sie den AV-Vertrag um die konkreten Details Ihrer Verarbeitung (vor allem um Angaben zu Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen). Halten Sie sich überdies an die bestehenden Prozesse in Ihrem Unternehmen. In den meisten Unternehmen ist der AV-Vertrag dem Datenschutzbeauftragten oder der Rechtsabteilung zur Bewertung vorzulegen. In komplizierten Fällen kann es sich empfehlen, zusätzliche Unterstützung durch einen spezialisierten externen Anwalt einzuholen.

Bedarf der AV-Vertrag einer bestimmten Form? Kann ich z. B. auch mit DocuSign unterschreiben?

Nach Art. 28 Abs. 9 DSGVO ist der Vertrag oder das andere Rechtsinstrument schriftlich abzufassen, was jedoch auch in einem elektronischen Format erfolgen kann. Was genau unter einem elektronischen Format zu verstehen ist, dazu gibt es verschiedene Auffassungen. Wichtig ist, dass der elektronische Vertragsschluss mit Beweiskraft hinreichend dokumentiert werden kann. Hierfür ist eine qualifizierte elektronische Signatur nicht zwingend erforderlich. Auch einfache Signaturen oder

andere elektronische Möglichkeiten können ausreichen. Da zum Beispiel die elektronischen Signaturlösungen von DocuSign (und anderen Anbietern vergleichbarer Lösungen) die technischen Anforderungen an eine einfache Signatur, an eine fortgeschrittene elektronische Signatur sowie an eine qualifizierte elektronische Signatur im Sinne der *eIDAS-VO* (Verordnung VO 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) erfüllen können (je nach gewähltem Produkt und abhängig von der Signaturlösung), bestehen hier verschiedene Möglichkeiten mit unterschiedlicher Beweiskraft.

Ich habe mit meinem Cloud-Anbieter noch einen alten Auftragsdatenverarbeitungsvertrag aus BDSG-Zeiten. Kann ich diesen auch weiterhin nutzen? Gibt es hierfür eine »Übergangsfrist«?

Es gibt keinen Bestandsschutz für »alte« ADV-Verträge. Seit dem 25. Mai 2018 hat die Verarbeitung personenbezogener Daten im Einklang mit den Anforderungen der DSGVO zu stehen. Verträge, die vor diesem Datum abgeschlossen wurden, sind daher an die Anforderungen der DSGVO anzupassen, nicht zuletzt mit Blick auf den hohen Bußgeldrahmen bei einer Verletzung der in der DSGVO enthaltenen Vorgaben (siehe hierzu Kapitel 18).

Inwieweit können AWS, Google, Microsoft & Co. als Auftragsverarbeiter angesehen werden? Und für welche Daten sind sie selbst Verantwortlicher?

AWS, Google, Microsoft und andere Anbieter werden grundsätzlich immer dann als Auftragsverarbeiter tätig, wenn Kunden personenbezogene Daten in die jeweiligen Clouds hochladen und dort verarbeiten. Ist der Kunde des Cloud-Anbieters als Auftragsverarbeiter seines Endkunden tätig, so ist der Cloud-Anbieter Unterauftragsverarbeiter. Für den Abschluss eines AV-Vertrags bieten diese Anbieter meist Standardverträge an, bei AWS zum Beispiel das *AWS GDPR Data Processing Addendum* als Ergänzung zum *AWS-Kundenvertrag* (siehe hierzu Kapitel 21).

Keine Auftragsverarbeitung liegt dagegen vor, wenn ein Cloud-Anbieter personenbezogene Daten eigenständig verarbeitet und die Zwecke und Mittel selbst festlegt (z. B. Erhebung von E-Mail-Adressen und Kontaktinformationen bei der Kontoregistrierung, Protokollierung der Service- und Supportnutzung). In diesen Fällen handelt der Cloud-Anbieter vielmehr selbst als Verantwortlicher.

Ich plane ein Multi-Cloud-Szenario. Was habe ich aus Sicht des Datenschutzes zu berücksichtigen, und was muss ich dabei bei dem Einsatz von Resellern berücksichtigen?

Eine Multi Cloud ist eine Cloud-Umgebung, in der die Leistungen verschiedener Cloud-Anbieter miteinander verbunden sind (Abschnitt 2.5.4 im Grundlagenkapitel). Es ist daher mit jedem Cloud-Anbieter, der im Rahmen des Multi-Cloud-Szenarios personenbezogene Daten im Auftrag verarbeitet, ein AV-Vertrag zu schließen.

Werden Leistungen dabei ganz oder teilweise über Reseller (etwa IT-Systemhäuser) bezogen, ist die Situation etwas komplizierter. Soweit Leistungen von einem Reseller bezogen werden, wird der AV-Vertrag im Regelfall direkt mit diesem abgeschlossen. Der Reseller wiederum hat »in der Kette« mit dem Cloud-Anbieter einen eigenen AV-Vertrag abzuschließen. Von diesem Grundsatz abweichende Konstellationen mit direktem Vertragsschluss mit dem Cloud-Anbieter finden sich in der Praxis aber auch wieder. Das hängt davon ab, wie der Hauptvertrag bzw. das Channel-Partner-Programm ausgestaltet ist.

Kann ich einen AV-Vertrag abschließen, wenn der Datenempfänger die Daten (teilweise) auch zu eigenen Zwecken verwenden soll?

In diesem Fall liegt keine Auftragsverarbeitung mehr vor. Der Datenempfänger ist nicht als Auftragsverarbeiter anzusehen, sondern wird selbst als Verantwortlicher tätig. Die Datenweitergabe bedarf daher einer eigenen Rechtsgrundlage. Im Fall einer *gemeinsamen Verantwortlichkeit* ist eine *Vereinbarung zwischen den gemeinsam Verantwortlichen* (siehe Abschnitt 7.1) abzuschließen.

Was habe ich innerhalb eines Konzerns oder einer Unternehmensgruppe zu beachten? Muss ich einen AV-Vertrag abschließen, wenn ein Konzernunternehmen für ein anderes Konzernunternehmen Datenverarbeitungstätigkeiten durchführt?

Es gibt in der DSGVO grundsätzlich kein *Konzernprivileg*. Einzige Ausnahme ist die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe für interne Verwaltungszwecke oder zum Zwecke der Videoüberwachung (das *kleine Konzernprivileg*), die als *berechtigtes Interesse* einer Übermittlung nach Art. 6 Abs. 1 lit. f DSGVO anerkannt sind (Abschnitt 5.6 weiter oben). Konzernunternehmen sind daher datenschutzrechtlich betrachtet eigene Stellen. Es kommt folglich darauf an, welche Tätigkeiten das datenverarbeitende Konzernunternehmen durchführen soll. Eine Auftragsverarbeitung ist möglich, wenn das Konzernunternehmen die Daten weisungsgebunden verarbeiten soll. Es ist dann ein AV-Vertrag zu schließen, der unter anderem die Weisungsgebundenheit und die diesbezüglichen Kontrollrechte regelt. Dagegen scheidet eine Auftragsverarbeitung aus, wenn das Konzernunternehmen mit den Daten selbst als Verantwortlicher umgehen soll. In diesem Fall bedarf die Datenweitergabe einer Rechtsgrundlage, gegebenenfalls kann sich auch hier der Abschluss einer Vereinbarung im Rahmen einer *gemeinsamen Verantwortlichkeit* (siehe Kapitel 7) anbieten.

Muss ich mit dem Reinigungsunternehmen für meine Büroräume auch einen AV-Vertrag abschließen?

Nein, ein Abschluss eines AV-Vertrags ist grundsätzlich nicht erforderlich. Es liegt keine Auftragsverarbeitung vor, da ein Reinigungsunternehmen nicht mit der Verarbeitung personenbezogener Daten beauftragt ist, sondern allein mit der Reinigung der Büroräume. Es empfiehlt sich aber, in den Vertrag mit dem Reinigungsunternehmen eine Klausel aufzunehmen, wonach die Mitarbeiter des Reinigungsunternehmens bei einer zufälligen Kenntniserlangung von personenbezogenen Daten zur Verschwiegenheit verpflichtet sind. Eigene Mitarbeiter sollten angewiesen werden,

ihren Arbeitsplatz so zu hinterlassen, dass Reinigungspersonal erst gar keine Möglichkeit hat, personenbezogene Daten zur Kenntnis zu nehmen.

Wie ist es mit einer Datenweitergabe an Steuerberater und Rechtsanwälte? Ist dies auf Grundlage eines AV-Vertrags möglich?

Steuerberater und Rechtsanwälte können in der Regel nicht auf Grundlage eines AV-Vertrags als Auftragsverarbeiter tätig werden. Eine weisungsgebundene AV-Tätigkeit ist grundsätzlich nicht mit den berufsrechtlichen Vorgaben vereinbar, wonach Steuerberater und Rechtsanwälte ihren Beruf weisungsfrei, eigenverantwortlich und unabhängig auszuüben haben. Die Datenweitergabe bedarf in diesem Fall einer anderen Rechtsgrundlage (in der Regel kommt Art. 6 Abs. 1 lit. b DSGVO in Betracht, »Erfüllung eines Vertrags«).

Kann ein Auftragsverarbeiter auch außerhalb von EU und EWR seinen Sitz haben?

Ja, das ist möglich. Anders als im »alten« Bundesdatenschutzgesetz ist die Auftragsverarbeitung seit der Datenschutzreform nicht nur innerhalb von EU und EWR privilegiert. Nach der DSGVO ist sie auch dann möglich, wenn der Auftragsverarbeiter in einem Drittland personenbezogene Daten verarbeitet. Allerdings sind hierfür die besonderen Zulässigkeitsanforderungen für internationale Datentransfers (*2. Stufe*, siehe Kapitel 12) zu berücksichtigen, insbesondere ein *angemessenes Datenschutzniveau* etwa durch den Einsatz von *Standardvertragsklauseln* (SCC): *Verantwortlicher an Auftragsverarbeiter (Modul 2)*.

Die Fristen, die einige Anbieter für ein Kontrollrecht (Audit) in einem AV-Vertrag gewähren, erscheinen unverhältnismäßig lang (z.B. drei Wochen Vorlauf). Ist das in Ordnung?

Die DSGVO verfolgt das Ziel, dass Kontrollen bzw. Audits gerade im Cloud-Umfeld bevorzugt anhand von Zertifikaten und zentralen Prüfdokumenten erfolgen sollen (vgl. Art. 28 Abs. 5 DSGVO). Dahinter verbirgt sich der Gedanke, dass eine inhaltlich tiefgreifende Prüfung durch entsprechend qualifizierte und erfahrene Prüfer bzw. Auditoren und ein Nachweis anhand eines anerkannten Zertifikats oder Testats meist sehr aussagekräftig sind – und damit für beide Seiten effizient. Die Übertragung der Prüfung auf spezialisierte Fachleute ist meist auch effektiver als Prüfungen jedes einzelnen Kunden. Dennoch hat ein Cloud-Kunde als Verantwortlicher grundsätzlich das Recht, sich auch vor Ort vom implementierten technisch-organisatorischen Maßnahmenkonzept und dem hierdurch gewährleisteten Datensicherheitsniveau zu überzeugen. Ein solches Recht soll durch längere Vorlauffristen grundsätzlich nicht beschnitten werden. Aus Anbietersicht kann eine solche Frist (gerade bei einer Vielzahl an Kunden) organisatorisch erforderlich sein, um einen geordneten Ablauf eines Audits mit Begleitung durch fachkundiges Personal zu ermöglichen. Durch entsprechende Formulierungen im AV-Vertrag sollte aber sichergestellt werden, dass in dringenden Fällen auch eine kurzfristige Überprüfung bzw. Inaugenscheinnahme möglich ist. Bei den großen Hyperscalern sind derartige individuelle Festlegungen erfahrungsgemäß für die allermeisten Kunden aber nicht möglich.

Kann ein Cloud-Anbieter eine Kostenerstattung für Audits verlangen?

Aus Sicht eines Anbieters erscheint eine Regelung über eine angemessene Kostenerstattung aufgrund der mit einem Audit regelmäßig verbundenen organisatorischen Aufwände durchaus als eine vertretbare Regelung. Allerdings vertreten hier vor allem die Aufsichtsbehörden andere Ansichten, da die DSGVO dem Verantwortlichen gerade das Recht einräumt, sich vor Ort ein Bild zu verschaffen. In der Praxis gibt es vereinzelte Lösungsansätze, wonach Kontrollen in angemessenem Umfang grundsätzlich kostenfrei sind, bei besonders hohen Aufwänden der Anbieter jedoch in angemessenem Umfang eine Kostenerstattung verlangen kann. Aufgrund der aufsichtsbehördlichen Sichtweise ist hier jedoch Vorsicht und Zurückhaltung geboten.

Was hat ein Cloud-Anbieter bei einer Auftragsverarbeitung besonders zu beachten?

Neben den Pflichten aus dem AV-Vertrag und diesbezüglichen Unterstützungs- und Mitwirkungspflichten hat ein Cloud-Anbieter beispielsweise ein *Verarbeitungsverzeichnis* für Verarbeitungen im Auftrag zu führen.

6.10 Checkliste: Auftragsverarbeitung/AV-Vertrag

Folgende Checkliste soll den Cloud-Nutzer beim Abschluss eines AV-Vertrags unterstützen:

- ☑ Wurde der Cloud-Anbieter als Auftragsverarbeiter sorgfältig ausgewählt?
- ☑ Wurde ein Auftragsverarbeitungsvertrag (AV-Vertrag) schriftlich oder in einem elektronischen Format mit dem Cloud-Anbieter geschlossen?
- ☑ Enthält der AV-Vertrag konkrete Bestimmungen zu:
  - Gegenstand und Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - Art der personenbezogenen Daten,
  - Kategorien der betroffenen Personen sowie
  - Pflichten und Rechte des Verantwortlichen?
- ☑ Ist in dem AV-Vertrag die Weisungsgebundenheit des Auftragsverarbeiters festgeschrieben?
- ☑ Ist beim Auftragsverarbeiter ein Datenschutzbeauftragter bestellt?
- ☑ Sind die Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis verpflichtet?
- ☑ Enthält der AV-Vertrag Bezugnahmen auf geeignete technische und organisatorische Maßnahmen (z.B. Verweis auf eine »TOM-Liste«)? Hat der Cloud-Anbieter ein technisch-organisatorisches Maßnahmenkonzept zur Gewährleistung der angemessenen Sicherheit der Verarbeitung implementiert, das

den Anforderungen des Art. 32 DSGVO entspricht? Sind hierbei insbesondere die folgenden Aspekte berücksichtigt?
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten,
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen sowie
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
- ☑ Enthält der Vertrag Regelungen in Bezug auf die Datenverarbeitung in einem Drittland? Falls diese ausgeschlossen werden soll, ist das entsprechend geregelt?
- ☑ Sind Kontroll-/Audit-Rechte des Verantwortlichen festgelegt?
- ☑ Enthält der Vertrag Regelungen zur Unterauftragsvergabe? Ist hierbei sichergestellt, dass die Beauftragung von Subunternehmern zumindest von einer allgemeinen Genehmigung abhängt und Widerspruchsmöglichkeiten vereinbart sind?
- ☑ Ist sichergestellt, dass ein Unterauftragnehmer den gleichen datenschutzrechtlichen Anforderungen unterliegt, wie sie gegenüber dem Auftragsverarbeiter vereinbart sind?
- ☑ Enthält der AV-Vertrag Regelungen zu Unterstützungsleistungen durch den Auftragsverarbeiter, damit der Verantwortliche den Betroffenenrechten nachkommen kann?
- ☑ Enthält der AV-Vertrag Regelungen zur Löschung bzw. Rückgabe der Daten nach Auftragsbeendigung?