Trusted Cloud

Kompetenzzentrum Trusted Cloud

Leitfaden – Datenschutz und Cloud Computing

Nr. 11

Arbeitsgruppe „Rechtsrahmen des Cloud Computing“

Cloud Computing kann in Deutschland nur wirtschaftlich erfolgreich sein, wenn die rechtlichen Rahmenbedingungen eine effiziente Nutzung von Cloud-Diensten ermöglichen. Ein innovationsfreundlicher Rechtsrahmen ist daher von besonderer Bedeutung. Für die rechtlichen Aspekte von Cloud Computing hat das Bundesministerium für Wirtschaft und Energie (BMWi) daher innerhalb des Kompetenzzentrums Trusted Cloud eine eigene Arbeitsgruppe einrichten lassen.

In der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ erarbeiten Experten aus Wirtschaft, Anwaltschaft und Wissenschaft sowie Vertreter aus Datenschutzbehörden gemeinsam mit Projektbeteiligten aus dem Trusted-Cloud-Programm Lösungsvorschläge für rechtliche Herausforderungen. Sie wird geleitet von Prof. Dr. Georg Borges. Themenschwerpunkte sind u. a. Datenschutz, Vertragsgestaltung, Urheberrecht sowie Haftungsfragen und Strafbarkeitsrisiken. Darüber hinaus wird ein Pilotprojekt zur datenschutzrechtlichen Zertifizierung von Cloud-Diensten durchgeführt, das Impulse für die rechtssichere Nutzung von Cloud Computing und die Gewährleistung eines hohen Datenschutzniveaus setzen soll.

Inhaltsverzeichnis

Vorwort **6**

1 Einführung **7**

2 Allgemeine Aspekte der Nutzung von Cloud-Diensten **8**
2.1 Anwendungsbereich des Datenschutzrechts 8
2.2 Telemedien-, Telekommunikationsgesetz und andere Gesetze 10
2.3 Der Cloud-Nutzer als datenschutzrechtlich Verantwortlicher 10
2.4 Grundsätze des Datenschutzrechts und Beauftragung eines Cloud-Anbieters 11
2.5 Weitere rechtliche Anforderungen 14

3 Die Nutzung von Cloud-Diensten in der Auftragsdatenverarbeitung **15**
3.1 Allgemeine Anforderungen an die Auftragsdatenverarbeitung 15
3.2 Die Auswahl des Cloud-Anbieters 16
3.3 Prüfung der technischen und organisatorischen Maßnahmen 19
3.4 Anforderungen an den Vertrag zwischen Cloud-Anbieter und Cloud-Nutzer 22

4 Cloud-Anbieter und Subunternehmer aus Drittstaaten **26**
4.1 Anwendbarkeit des deutschen Datenschutzrechts 26
4.2 Wann ist die grenzüberschreitende Datenübermittlung zulässig? 27

5 Die Überwachung des Cloud-Anbieters durch den Cloud-Nutzer **32**

6 Security Breach Notification (§ 42a BDSG, § 83a SGB X; §§ 93 Abs. 3, 109a TKG; § 15a TMG) **34**

7 Die Beendigung des Auftragsverhältnisses **35**

8 Checkliste **36**

Autoren **42**

Vorwort

Cloud Computing bietet wesentliche Vorteile für die Datenverarbeitung, nicht zuletzt in kleinen und mittelgroßen Unternehmen. Daher überrascht es nicht, dass sich weltweit ein Trend zur Nutzung von Cloud-Diensten entwickelt hat, der auch die technisch-organisatorische Grundlage neuer Entwicklungen wie „Industrie 4.0“ darstellt.

Der Einsatz von Cloud-Diensten birgt Herausforderungen für den Datenschutz. Noch vor wenigen Jahren wurden die datenschutzrechtlichen Anforderungen als kaum überwindbare Hürde für Cloud Computing angesehen. In der Zwischenzeit wurden jedoch praxistaugliche Lösungen entwickelt, mit deren Hilfe Cloud-Dienste datenschutzkonform genutzt werden können. Auch wenn in einigen Aspekten noch Rechtsunsicherheit besteht und in einzelnen Fragen, insbesondere bei der Nutzung von Cloud-Diensten aus Drittstaaten, noch keine Einigkeit erzielt ist, sind die Grundlagen für datenschutzfreundliches Cloud Computing gelegt.

Cloud Computing stellt gleichwohl durchaus erhebliche datenschutzrechtliche Anforderungen an Anbieter wie an Nutzer von Cloud-Diensten. Der vorliegende Leitfaden soll eine Orientierungshilfe für die datenschutzkonforme Nutzung von Cloud-Diensten bieten. Er richtet sich insbesondere an Entscheider in Unternehmen sowie Mitglieder von Rechtsabteilungen in Unternehmen, die Cloud Computing nutzen möchten.

Der Leitfaden befindet sich auf dem Stand März 2015 und wurde im Rahmen der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Kompetenzzentrum „Trusted Cloud“ erarbeitet. Die von Prof. Dr. Georg Borges geleitete Arbeitsgruppe ist Bestandteil des Technologieprogramms Trusted Cloud des Bundesministeriums für Wirtschaft und Energie (BMWi). Weitere Informationen finden Sie unter www.trusted-cloud.de.

Der Leitfaden zielt darauf ab, eine schnelle Orientierung zu ermöglichen und eine Unterstützung bei der Nutzung von Cloud-Diensten zu bieten.

Dr. Jens Eckhardt

Leiter der Task Force „Datenschutz“
der AG „Rechtsrahmen des Cloud Computing“

Prof. Dr. Georg Borges

Leiter der AG „Rechtsrahmen
des Cloud Computing“

1 Einführung

Cloud Computing ist aus der Sicht des Nutzers von Cloud-Diensten mit der Auslagerung von IT-Diensten an einen Dritten, den Cloud-Anbieter, verbunden. Bei einer solchen Einbeziehung Dritter in die Datenverarbeitung sind, soweit der Nutzer personenbezogene Daten verarbeitet, besondere datenschutzrechtliche Anforderungen zu erfüllen. Das deutsche Datenschutzrecht bietet als datenschutzrechtliche Grundlage für die Auslagerung von IT-Diensten die Auftragsdatenverarbeitung, die beim Cloud Computing regelmäßig genutzt wird.

Der Leitfaden soll vor allem dem Nutzer von Cloud-Diensten Hilfestellung geben, die datenschutzrechtlichen Anforderungen zu erkennen und die Instrumente zum Einsatz von Cloud-Diensten, die das deutsche Datenschutzrecht zur Verfügung stellt, zu nutzen. Entsprechend dieser Zielsetzung ist der Leitfaden so aufgebaut, dass er dem Cloud-Nutzer die datenschutzrechtlichen Aspekte beim Einsatz von Cloud-Diensten entsprechend der zeitlichen Abfolge („Lifecycle“) darstellt. Im ersten Abschnitt (Ziffer 2, S. 8 ff.) werden wesentliche Grundlagen erläutert, etwa der Anwendungsbereich des Datenschutzrechts („Wann liegen personenbezogene Daten vor?“) und die Grundbegriffe des Datenschutzes („Wer ist die ‚verantwortliche Stelle‘ im Sinne des Datenschutzrechts? Welche datenschutzrechtlichen Grundlagen sind beim Cloud Computing anwendbar?“). Darauf aufbauend werden – ausgehend von der datenschutzrechtlichen Auftragsdatenverarbeitung, die in der Praxis zum Einsatz von Cloud Computing regelmäßig vorliegen wird – die wesentlichen Etappen des Einsatzes von Cloud-Diensten dargestellt: Die Auswahl des Cloud-Anbieters („Was muss der Cloud-Nutzer tun, um sich von der Zuverlässigkeit des Cloud-Anbieters zu überzeugen? – Ziffer 3.2, S. 16 ff.), die Möglichkeit der Nutzung von Cloud-Anbietern aus Drittstaaten („Kann ein Cloud-Dienst eines US-amerikanischen Anbieters genutzt werden? – Ziffer 4, S. 26 ff.), die Überwachung des Cloud-Anbieters durch den Cloud-Nutzer (Ziffer 5, S. 32 ff.), Meldepflichten bei Datenschutzverstößen (Ziffer 6, S. 34 f.) und, ebenfalls sehr wichtig, die Beendigung des Auftragsverhältnisses (Ziffer 7, S. 35 f.).

Der Leitfaden ist, obwohl er in vielem nur einen Einstieg bieten kann, recht umfangreich geworden. Daher bietet eine umfangreiche Checkliste (Ziffer 8, S. 36 ff.) dem eiligen Leser einen Einstieg in die jeweilige Sachfrage. Zugleich kann die Checkliste helfen, die Beachtung der wesentlichen datenschutzrechtlichen Aspekte beim Einsatz von Cloud Computing zu sichern.

Der Leitfaden geht von der Geltung des deutschen Datenschutzrechts aus. Dieses ist für Nutzer von Cloud-Diensten jedenfalls maßgeblich, soweit diese in Deutschland ansässig sind und innerhalb Deutschlands Datenverarbeitung betreiben.

2 Allgemeine Aspekte der Nutzung von Cloud-Diensten

Dieses Kapitel beschreibt die Grundlagen des deutschen Datenschutzrechts im Kontext der Nutzung des Cloud Computing.

2.1 Anwendungsbereich des Datenschutzrechts

Der nachfolgenden Darstellung liegt – wie bereits in der Einleitung angesprochen – die Anwendung deutschen Datenschutzrechts zugrunde.

Eine grundlegende Frage bei der Festlegung der Anforderungen an die Nutzung eines Cloud-Dienstes ist: Sind die Anforderungen und Beschränkungen des Datenschutzrechts zu beachten?

2.1.1 Anwendungsbereich

Der Anwendungsbereich des deutschen Datenschutzrechts wird grundlegend durch § 1 Abs. 2 Bundesdatenschutzgesetz (BDSG) beschrieben. Danach ist das Datenschutzrecht bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu beachten.

> **Hinweis**
> Das Datenschutzrecht greift bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten.

Diese Definition besteht aus zwei Bestandteilen: „Erhebung, Verarbeitung und Nutzung“ und „personenbezogener Daten“.

Erhebung, Verarbeitung und Nutzung sind in § 3 BDSG gesetzlich definiert. Vereinfacht gesagt ergibt sich aus den Definitionen in § 3 BDSG, dass praktisch jeder Umgang mit personenbezogenen Daten in den Anwendungsbereich des Datenschutzrechts fällt. Oder anders formuliert: Die Anwendung des Datenschutzrechts kann typischerweise nicht aufgrund der Art des Umgangs mit den personenbezogenen Daten verneint werden.

Damit ist für die Anwendung des Datenschutzrechts von zentraler Bedeutung, was unter „personenbezogenen Daten“ zu verstehen ist.

2.1.2 Personenbezogene Daten als zentrales Element der Anwendung des Datenschutzrechts

Das Bundesdatenschutzgesetz definiert in § 3 Abs. 1 BDSG personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Diese Person wird im Datenschutzrecht als Betroffener bezeichnet (§ 3 Abs. 1 BDSG).

Eine natürliche Person – ein Mensch – ist in diesem Sinn bestimmt, wenn eine Information direkt mit ihr verbunden ist.

Schwieriger zu beantworten – und derzeit in der datenschutzrechtlichen Fachwelt im Detail heftig umstritten – ist allerdings die Frage, wann von einer Bestimmbarkeit auszugehen ist. Vereinfacht lässt sich sagen, dass hiervon auszugehen ist, wenn die Information nicht direkt einem Menschen zugeordnet ist, aber durch weitere Informationen der Zusammenhang hergestellt werden kann.

Hinweis
Das Datenschutzrecht ist zu beachten, wenn Einzelangaben einem bestimmten oder bestimmbaren Menschen zugeordnet werden können.

Der Anwendungsbereich des Datenschutzrechts endet, wenn die Daten anonymisiert sind. Anonymisieren ist nach der Definition in § 3 Abs. 6 BDSG das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Ein sogenanntes Pseudonymisieren hingegen ändert nichts an der Geltung des Datenschutzrechts. Hierauf ist hinzuweisen, da in der Praxis häufig von Anonymisieren gesprochen wird, obgleich tatsächlich nur eine Pseudonymisierung gegeben ist. Pseudonymisieren ist nach der Definition in § 3 Abs. 6a BDSG das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Hinweis
Das Datenschutzrecht gilt nicht und seine Anwendung endet, wenn die Daten anonymisiert sind. Bei einer bloßen Pseudonymisierung bleibt es hingegen bei der Anwendung des Datenschutzrechts.

Die deutschen Datenschutzaufsichtsbehörden vertreten den Standpunkt, dass das Datenschutzrecht auch dann zu beachten ist, wenn die Daten, welche in die Cloud „ausgelagert“ werden, derart verschlüsselt sind, dass der Cloud-Anbieter sie nicht der jeweiligen Person zuordnen kann.[1] Dieser Ansatz ist aufgrund seiner Begründung jedoch umstritten. Eine Klärung dieses Streitpunkts wird sich in absehbarer Zeit dadurch ergeben, dass der Bundesgerichtshof (BGH) in einer Entscheidung im Oktober 2014 die Frage zur Reichweite des Personenbezugs dem Europäischen Gerichtshof (EuGH) zur Entscheidung vorgelegt hat.[2]

Hinweis
Selbst die Übertragung verschlüsselter Daten in die Cloud wird – nach derzeitigem Stand der Diskussion – regelmäßig die Anwendung des Datenschutzrechts nicht entfallen lassen.

1 Siehe Orientierungshilfe Cloud Computing des Arbeitskreises Technik und Medien der Konferenz des Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Version 2.0 vom 9.10.2014 (fortan „Orientierungshilfe Cloud Computing“), Seite 12/13.
2 BGH, Beschl. v. 28.10.2014 - VI ZR 135/13.

2.2 Telemedien-, Telekommunikationsgesetz und andere Gesetze

Das deutsche Recht kennt verschiedene gesetzliche Regelungen zum Datenschutz. Insbesondere enthalten neben dem Bundesdatenschutzgesetz das Sozialgesetzbuch Zehntes Buch (SGB X), das Telemediengesetz und das Telekommunikationsgesetz Datenschutzbestimmungen, die dem Bundesdatenschutzgesetz vorgehen. Dies bedeutet, dass das Bundesdatenschutzgesetz nicht angewendet wird, soweit diese spezielleren Gesetze eine Datenschutzregelungen enthalten.

Für die Bewertung der Anwendungsbereiche ist nicht auf das Verhältnis zwischen Cloud-Nutzer und Cloud-Anbieter abzustellen, sondern auf das Verhältnis zwischen Cloud-Nutzer und Betroffenem – demjenigen, dessen Daten in der Cloud verarbeitet werden sollen. Das Telekommunikationsgesetz kommt also deshalb nicht auf jeden Cloud-Dienst zur Anwendung, obwohl der Nutzung eines Cloud-Dienstes Telekommunikation zugrunde liegt.

Die Abgrenzung zwischen Bundesdatenschutz-, Telemedien- und Telekommunikations-gesetz ist im Detail umstritten. Bei einer Auslagerung in die Cloud auf der Grundlage einer Auftragsdatenverarbeitung wirkt sich diese Unterscheidung in der Praxis nicht aus. Denn es gilt gleichermaßen § 11 BDSG (vgl. Ziffer 3). Auch das eingangs angesprochene SGB X enthält eine Regelung über die Auftragsdatenverarbeitung, die mit § 11 BDSG vergleichbar ist.

Mit anderen Worten: Die Unterscheidung spielt nur dann eine Rolle, wenn dem Cloud-Dienst keine Auftragsdatenverarbeitung zugrunde liegt (vgl. Ziffer 2.4.2.2).

2.3 Der Cloud-Nutzer als datenschutzrechtlich Verantwortlicher

Die Einhaltung des Datenschutzrechts hat die sogenannte verantwortliche Stelle sicher-zustellen. Verantwortliche Stelle ist nach der Definition in § 3 Abs. 7 BDSG „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“.

Für das Cloud Computing bedeutet das: Zunächst und in erster Linie ist der Cloud-Nutzer die verantwortliche Stelle und bleibt es auch bei der Nutzung von Cloud-Diensten. Denn er wird die personenbezogenen Daten der Betroffenen in der Cloud verarbeiten lassen.

Der Cloud-Nutzer ist damit beim Cloud Computing insbesondere für drei Aspekte verantwortlich:

- Dass der Umgang mit den personenbezogenen Daten in der Cloud datenschutz-konform ist.

  Mit anderen Worten: Der Cloud-Nutzer ist für die Erhebung und Verwendung der personenbezogenen Daten mittels des Cloud-Dienstes ebenso verantwortlich, wie wenn er dies selbst auf eigenen Systemen täte.

- Für die Auslagerung der personenbezogenen Daten in die Cloud.

  Mit anderen Worten: Der Cloud-Nutzer ist für die datenschutzkonforme Einbeziehung des Cloud-Anbieters einschließlich dessen eventueller Subunternehmer verantwortlich.

- Dass grenzüberschreitendes Cloud Computing datenschutzkonform ausgestaltet ist (vgl. Ziffer 4).

Hinweis
Die Nutzung von Cloud Computing bedeutet für den Cloud-Nutzer keine Aufhebung der datenschutzrechtlichen Verantwortlichkeit und keine Delegation der datenschutzrechtlichen Verantwortlichkeit auf den Cloud-Anbieter. Der Cloud-Nutzer bleibt datenschutzrechtlich in der Verantwortung – insbesondere auch für die datenschutzrechtliche Zulässigkeit der Nutzung eines Cloud-Dienstes.

2.4 Grundsätze des Datenschutzrechts und Beauftragung eines Cloud-Anbieters

Für das Verständnis datenschutzrechtlicher Grundsätze zur Beauftragung eines Cloud-Anbieters ist das sogenannte Verbot mit Erlaubnisvorbehalt von elementarer Bedeutung.

2.4.1 Verbot mit Erlaubnisvorbehalt

Das sogenannte Verbot mit Erlaubnisvorbehalt ist in § 4 Abs. 1 BDSG verankert: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."

Hinweis
Jede Erhebung oder Verwendung personenbezogener Daten ist unzulässig, es sei denn, die Erhebung und/oder Verwendung ist im konkreten Einzelfall durch Gesetz oder Einwilligung des Betroffenen gestattet.

Die Beweislast für die konkrete Zulässigkeit in jedem Einzelfall trägt der Cloud-Nutzer als sogenannte verantwortliche Stelle (vgl. Ziffer 2.4).

2.4.2 Beauftragung eines Cloud-Anbieters

Das Verbot mit Erlaubnisvorbehalt gilt auch für die Beauftragung eines Cloud-Anbieters. Denn eine Übertragung personenbezogener Daten an ein anderes Unternehmen fasst das Bundesdatenschutzgesetz unter die Definition des Verwendens von personenbezogenen Daten (siehe § 3 Abs. 4 S. 2 Nr. 3 BDSG).

2.4.2.1 Beauftragung im Wege der Auftragsdatenverarbeitung

Das Datenschutzrecht sieht gerade für die Beauftragung von Dienstleistern eine Art „Spezialgestaltung“ vor: Die sogenannte Auftragsdatenverarbeitung. Deren Besonderheit besteht darin, dass ein anderes Unternehmen, das als sogenannter Auftragsdatenverarbeiter beauftragt wird, nicht als sogenannter Dritter gilt, sodass das Verbot mit Erlaubnisvorbehalt nicht greift (§ 3 Abs. 8 S. 2 BDSG). Diese Besonderheit wird auch als „Privilegierungswirkung der Auftragsdatenverarbeitung“ bezeichnet.

> **Hinweis**
> Die Auftragsdatenverarbeitung ist – vereinfacht gesagt – eine datenschutzrechtliche Grundlage für die Übertragung von Daten in den durch den Cloud-Anbieter bereitgestellten Cloud-Service.

Der Cloud-Nutzer kann sich damit neben der gesetzlichen Zulässigkeit und der Einwilligung selbst eine Art dritten Weg schaffen, indem er den Cloud-Anbieter als sogenannten Auftragsdatenverarbeiter beauftragt. Bildlich gesprochen ist der Preis, den er hierfür zahlt, die strikte Einhaltung und Umsetzung der Vorgaben über die Auftragsdatenverarbeitung, wie sie in § 11 BDSG geregelt sind (vgl. Ziffer 3).

Sind die Anforderungen des § 11 BDSG nicht eingehalten, stellt die Übertragung der Daten eine Übermittlung dar und es greift das Verbot mit Erlaubnisvorbehalt. Es besteht dann die Gefahr einer unzulässigen und damit bußgeldbewehrten Übermittlung von Daten.

> **Hinweis**
> Die Auftragsdatenverarbeitung greift – vereinfacht gesagt – als Rechtsgrundlage nur, wenn die Vorgaben des § 11 BDSG strikt eingehalten sind.

Die Auftragsdatenverarbeitung hat nach deutschem Recht allerdings geografische Grenzen. § 3 Abs. 8 S. 2 BDSG regelt nämlich: „Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.“ Dies gilt nicht nur für den Cloud-Anbieter, sondern auch für seine eventuellen Subunternehmer.

Die oben angesprochene Privilegierungswirkung der Auftragsdatenverarbeitung ist damit auf die Europäische Union (EU) und den Europäischen Wirtschaftsraum (EWR) beschränkt. Diese Begrenzung wird heftig als europarechtswidrig kritisiert, weil die maßgebliche EU-Richtlinie 95/46/EG[3] (im Folgenden: „EU-Datenschutzrichtlinie“) keine solche Begrenzung auf die EU oder den EWR vorsieht. Die Praxis der deutschen Aufsichtsbehörden hält unter Bezugnahme auf den Wortlaut des Gesetzes gleichwohl an der Beschränkung fest.

3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Hinweis
Die Privilegierungswirkung einer vertraglichen Auftragsdatenverarbeitung greift nur für Cloud-Anbieter in der EU oder im EWR.

Die Nutzung eines Cloud-Dienstes außerhalb der EU oder des EWR ist damit datenschutzrechtlich zwar nicht ausgeschlossen. Allerdings greift dann wiederum die Grundregel, dass eine gesetzliche Zulässigkeitsregelung oder eine Einwilligung des Betroffenen die Nutzung des Cloud-Dienstes tragen muss. Einwilligungen derjenigen, deren Daten in der Cloud verarbeitet werden sollen, sind allerdings typischerweise nicht praktisch zu erlangen.

2.4.2.2 Gesetzliche Zulässigkeitsregelung statt Auftragsdatenverarbeitung

Im Anwendungsbereich des Bundesdatenschutzgesetzes kommt als gesetzliche Zulässigkeitsregelung insbesondere § 28 Abs. 2 BDSG in Betracht (Näheres unter Ziffer 4). Auf diese Regelung ist insbesondere dann zurückzugreifen, wenn eine Auftragsdatenverarbeitung nicht in Betracht kommt (vgl. Ziffer 2.4.2.1).

Auch in diesem Fall sind zum Eigenschutz des Cloud-Nutzers vertragliche Regelungen zum Umgang mit den personenbezogenen Daten geboten. Hierfür bietet sich eine Anlehnung an den Inhalt einer Vereinbarung über die Auftragsdatenverarbeitung an.

Nach Ansicht der Datenschutzaufsichtsbehörden wird die Zulässigkeitsprüfung nach Maßgabe gesetzlicher Regelungen positiv beeinflusst, wenn eine Vereinbarung über die Auftragsdatenverarbeitung geschlossen wird. Dies hat seinen Grund darin, dass die gesetzlichen Zulässigkeitsregelungen des Bundesdatenschutzgesetzes im Kern auf einer Interessenabwägung beruhen.

Hinweis
Eine Nutzung von Cloud-Diensten außerhalb der EU und dem EWR bedarf regelmäßig einer gesetzlichen Zulässigkeitsregelung. Gleichwohl ist es sinnvoll, eine Vereinbarung in Anlehnung an die Vorgaben für die Auftragsdatenverarbeitung zu schließen.

2.4.2.3 Zwang zum Vertrag entsprechend § 11 BDSG bei Cloud-Diensten außerhalb der EU und des EWR

§ 11 Abs. 5 BDSG sieht vor, dass § 11 Absätze 1 bis 4 BDSG entsprechend gelten, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Mit anderen Worten: Wenn die Möglichkeit des Cloud-Anbieters zum Zugriff auf die durch dessen Cloud-Dienst verarbeiteten Daten nicht mit Sicherheit ausgeschlossen werden kann, weil er die Hard- und/oder Software wartet und pflegt, gelten – vereinfacht gesagt – die Regelungen über die Auftragsdatenverarbeitung gleichwohl.

Hinweis
Es ist typischerweise ratsam, bei jedem Cloud-Dienst eine Vereinbarung über die Auftragsdatenverarbeitung zu schließen. Denn jedenfalls dann, wenn ein Zugriff des Cloud-Anbieters oder eines Subunternehmers auf die personenbezogenen Daten nicht tatsächlich mit Sicherheit ausgeschlossen werden kann, besteht die gesetzliche Pflicht zu einer solchen Vereinbarung.

2.5 Weitere rechtliche Anforderungen

Der vorliegende Leitfaden befasst sich mit den datenschutzrechtlichen Rahmenbedingungen des Cloud Computing. Gleichwohl soll zur Abrundung auf weitere gesetzliche Anforderungen hingewiesen werden.

Aus § 203 Strafgesetzbuch (StGB) ergibt sich eine Geheimhaltungspflicht für Berufsgeheimnisträger. Diese gilt neben den Datenschutzbestimmungen und kann auch nicht durch eine Auftragsdatenverarbeitung „durchbrochen“ werden.[4]

Das Telekommunikations- und Briefgeheimnis ist strafrechtlich durch § 206 StGB geschützt. Diese Vorschrift ist ebenfalls zu beachten. Typischerweise ist jedoch davon auszugehen, dass für Reichweite und Umfang des Schutzes die spezialgesetzlichen Datenschutzbestimmungen des Telekommunikations- und des Postgesetzes gelten, sodass jedenfalls durch eine Auftragsdatenverarbeitung nach § 11 BDSG ein Verstoß gegen § 206 StGB vermieden werden kann.

Das Bankgeheimnis ist in Deutschland kein gesetzlich geschütztes Geheimnis, sondern – vereinfacht gesagt – eine vertragliche Geheimhaltungspflicht, welche die Bank gegenüber den Kunden eingeht. Für diese Geheimhaltungspflicht gilt, wie auch für andere Geheimhaltungsvereinbarungen –, dass der Inhalt der vertraglichen Vereinbarung darüber entscheidet, ob diese Vereinbarung der Nutzung von Cloud Computing entgegensteht.

Es ist darauf hinzuweisen, dass in vielen Verträgen Geheimhaltungspflichten vereinbart sind oder sich diese als nebenvertragliche Pflicht ergeben können. Es ist daher stets zu prüfen, ob Geheimhaltungspflichten der Nutzung von Cloud Computing im Einzelfall entgegenstehen.

Darüber hinaus bestehen steuerrechtliche Beschränkungen bei der – vereinfacht gesagt – Auslagerung der Buchhaltung in eine Cloud außerhalb Deutschlands (vgl. z. B. §§ 146, 147 Abgabenordnung (AO)). Es empfiehlt sich, dazu einen steuerrechtlichen Sachverstand in Anspruch zu nehmen, um die jeweilige Besonderheit des konkret zuständigen Finanzamtes in Erfahrung zu bringen.

4 Näheres im Thesenpapier 7 der AG Rechtsrahmen des Kompetenzzentrums Cloud Computing „Schweigepflicht bei der Auslagerung von IT-Leistungen“.

3 Die Nutzung von Cloud-Diensten in der Auftragsdatenverarbeitung

Die Anforderungen an die Auftragsdatenverarbeitung sind im Kern in § 11 BDSG geregelt. § 11 BDSG setzt Vorgaben des EU-Rechts um. Art. 17 der EU-Datenschutzrichtlinie regelt: Die wesentlichen Elemente sind die Weisungsgebundenheit des Auftragnehmers, die Vereinbarung von technischen und organisatorischen Maßnahmen und das Erfordernis der Dokumentation.

Die Umsetzung dieser Vorgaben in § 11 BDSG erfolgte allerdings mit einigen Besonderheiten.

3.1 Allgemeine Anforderungen an die Auftragsdatenverarbeitung

Wesentliches Merkmal der Auftragsdatenverarbeitung ist die weisungsabhängige Datenverarbeitung durch den Cloud-Anbieter (insoweit in der Rolle des Auftragnehmers).

Abzugrenzen davon ist die Einbeziehung eines Dienstleisters, der im Rahmen der Auslagerung auch eigene Entscheidungen zu treffen hat (sog. Funktionsübertragung), wie beispielsweise ein Steuerberater oder eine Inkassogesellschaft. Dies wird bei Cloud Computing aber seltener der Fall sein, sodass diese Thematik hier nicht weiter vertieft werden muss. Denn typischerweise wird die Aufgabe des Cloud-Anbieters darin bestehen, gerade keine personenbezogenen Daten zu erheben oder eigene Entscheidungen zu treffen.

Hinweis
Eine Funktionsübertragung, im Rahmen derer eine Zulässigkeitsvoraussetzung erfüllt sein muss, wird im Cloud-Umfeld eher die Ausnahme sein.

Bei der Auftragsdatenverarbeitung bleibt wie oben (vgl. Ziffer 2.4) ausgeführt der Cloud-Nutzer (Auftraggeber) auch bei der Beauftragung eines Cloud-Anbieters (hier in der Rolle des Auftragnehmers) in der Verantwortung für die Zulässigkeit der Datenverarbeitung und die Angemessenheit der Datensicherheitsmaßnahmen. Um dieser Verantwortung gerecht werden zu können, sieht die Gestaltung der Auftragsdatenverarbeitung einige Regelungen vor, die den Cloud-Nutzer in die Lage versetzen, weiterhin die „Herrschaft“ über diese Datenverarbeitung zu haben.

Hinweis
Der Cloud-Nutzer bleibt die „verantwortliche Stelle“ für die Verarbeitung personenbezogener Daten. Dies bringt einige Privilegien mit sich, stellt den Cloud-Nutzer aber auch vor die Herausforderung, dieser Verantwortung gerecht zu werden.

Die Weisungsgebundenheit bedeutet aber nicht, dass der Cloud-Nutzer beliebig über die Leistungserbringung bestimmen können muss. Diese Weisungsbefugnis des Cloud-Nutzers ist nur innerhalb der vereinbarten Leistung auszuüben und bezieht sich ausschließlich auf den Umgang mit den personenbezogenen Daten und nicht generell auf die Leistungserbringung. Insbesondere begründet die Weisungsbefugnis des Datenschutzes kein einseitiges Leistungsänderungsrecht des Cloud-Nutzers gegenüber dem Cloud-Anbieter.

Vor diesem Hintergrund und der Tatsache, dass die Cloud-Dienste zumeist im Massenmarkt angeboten werden und individuelle Vereinbarungen in der Regel nicht vorgesehen sind, kommt der Auswahl des Cloud-Anbieters besondere Bedeutung zu.

Hinweis
Bereits bei der Auswahl des Cloud-Anbieters ist zu beachten, welche Einflussmöglichkeiten dem Cloud-Nutzer hinsichtlich der Datenlöschung und anderen Weisungen konkret möglich sind.

3.2 Die Auswahl des Cloud-Anbieters

Zunächst sollte derjenige, der künftig einen Cloud-Dienst nutzen möchte (hier „potenzieller Cloud-Nutzer“ genannt) sicherstellen, dass er die Datenverarbeitung überhaupt auslagern darf und keine für bestimmte Berufsgruppen geltenden Geheimhaltungsverpflichtungen (vgl. Ziffer 2.5) dagegen sprechen.

Das Bundesdatenschutzgesetz sieht für einen potenziellen Cloud-Nutzer bereits vor der Auftragserteilung Prüfpflichten, die die Auswahl eines Cloud-Anbieters betreffen, vor. Gemäß § 11 Abs. 2 Satz 1 BDSG hat ein potenzieller Cloud-Nutzer den Cloud-Anbieter „sorgfältig auszuwählen“. Die Sorgfalt ist jedenfalls dann gegeben, wenn die Auswahl auf ein angemessenes Datenschutzniveau bei dem Cloud-Anbieter gerichtet ist. Erforderlich ist dabei mindestens dasjenige Niveau, das der potenzielle Cloud-Nutzer selbst einhalten müsste, wenn er die Daten (weiterhin) selbst verarbeiten würde.

3.2.1 Grundsätzliche Auswahlfreiheit

Sofern insbesondere die Weisungsbefugnis des Cloud-Nutzers (vgl. Ziffer 3.1) sichergestellt ist, besteht grundsätzliche Wahlfreiheit. Somit kann jeder Cloud-Anbieter ausgewählt werden, der bestimmte Anforderungen erfüllt.

Im Falle der Auswahl eines konzernangehörigen Unternehmens sollte besonderes Augenmerk auf die Einhaltung des Trennungsgebots gelegt werden. Denn – zumindest ein Auftragsdatenverarbeiter – darf die Daten verschiedener Auftraggeber nicht zusammen verarbeiten.

3.2.2 Erster Schritt: Erstellung eines Anforderungsprofils

In einem ersten Schritt sollte der potenzielle Cloud-Nutzer ein Anforderungskonzept erstellen und dem Cloud-Anbieter zukommen lassen. Um ein ausreichendes Maß an Sicherheit für das eigene Bedürfnis gewährleisten zu können, muss sich der potenzielle Cloud-Nutzer dabei über die Art der zu verarbeitenden Daten gewahr werden und eventuell einzuhaltende Sondervorschriften kennen (vgl. Ziffern 2.2 und 2.5).

3.2.3 Zweiter Schritt: Eigentliche Eignungsprüfung

Anhand eines solchen Konzepts erfolgt in einem zweiten Prüfungsschritt die eigentliche Eignungsprüfung des Cloud-Anbieters. Darin muss der potenzielle Cloud-Nutzer untersuchen, ob der Cloud-Anbieter fähig und bereit ist, beispielsweise die im Rahmen eines Sicherheitskonzepts entwickelten Anforderungen an die technische und organisatorische Datensicherheit und Datensicherung zu erfüllen.

Gegenstand der Prüfung ist im Besonderen die Eignung der vom Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen.

> **Hinweis**
> Der Cloud-Nutzer ist auch für die technisch-organisatorischen Schutzmaßnahmen beim Cloud-Anbieter verantwortlich. Daher sollten bei der Auswahlentscheidung nicht nur Preis und Leistungsinhalt des Cloud-Dienstes, sondern auch die Schutzmaßnahmen des Cloud-Anbieters entscheidungserheblich sein.

Für die Auswahlentscheidung können Angaben des potenziellen Cloud-Anbieters, vertragliche Leistungsbeschreibungen oder Selbstauskünfte genügen. Dabei ist zu beachten, dass die Auswahlentscheidung (§ 11 Abs. 1 S. 2 BDSG) von der Überzeugungsbildung in Bezug auf die technisch-organisatorischen Maßnahmen (§ 11 Abs. 2 S. 4 BDSG; vgl. Ziffer 3.3) zu unterscheiden ist. Im Einzelfall können diese jedoch inhaltlich oder zeitlich zusammenfallen (vgl. 3.3).

3.2.3.1 Schutzziele der IT-Sicherheit

Ein entsprechender – allerdings nicht abschließender – Katalog erforderlicher technischer und organisatorischer Maßnahmen findet sich in der Anlage zu § 9 BDSG. Dabei geht es inhaltlich um die Schutzziele der IT-Sicherheit Vertraulichkeit, Verfügbarkeit und Integrität.

Maßnahmen zur Sicherung der **Vertraulichkeit** können etwa Zugangsbeschränkungen, Patchmanagement, sichere Grundkonfigurationen, Sicherheitsrichtlinien, Integritätsprüfungen, revisionssichere Protokollierung, Datensicherung, Intrusion-Detection-Systeme (IDS), Firewalls und Virenschutz sein. Interne und externe Kommunikation ist nach dem Stand der Technik zu verschlüsseln (z. B. Ende-zu-Ende-Verschlüsselung), sichere Authentifizierungen sind zu verwenden.

Verfügbarkeit kann etwa durch Redundanzen der Kommunikationsverbindungen, der Datenspeicherung und der Systeme (z. B. Backups und Ersatz-IT-Systeme) sichergestellt werden. Die großzügige örtliche Trennung von Rechenzentren und damit die Schaffung von Ausweichkapazitäten im Falle von Naturkatastrophen ist eine weitere Möglichkeit zur Verfügbarkeitsförderung.

Die **Integrität** der Anwendungsdaten und Systeme wird durch fehlerhaft gestaltete Verarbeitungsverfahren und durch unbefugte oder unbeabsichtigte Datenveränderungen und Systemzugriffe gefährdet. Unbefugte Datenveränderungen können durch Angriffe auf Infrastruktur und Plattform, beispielsweise durch unzuverlässige Mitarbeiter des Anbieters, bewirkt werden. Eine sorgfältige Auswahl des Personals des Cloud-Anbieters und entsprechende Weiterbildungen können dem entgegenwirken.

Grundsätzlich gilt es aber zu bedenken, dass auch der Cloud-Nutzer eine große Verantwortung zur IT-Sicherheit trägt: Der Umgang mit den Authentisierungsmitteln (Kennungen, Passwörtern, PINs, TANs, maschinenlesbaren Ausweisen und Token, ggf. auch biometrischen Merkmalen) liegt in der Verantwortung des Cloud-Nutzers und dessen Mitarbeitern.

Hinweis
Die Einschaltung eines Dienstleisters entbindet den Cloud-Nutzer nicht davon, die Risiken in seiner eigenen Sphäre ebenso kritisch zu hinterfragen und zu minimieren.

3.2.3.2 Technische und organisatorische Maßnahmen im Einzelnen

Die Anlage zu § 9 BDSG setzt eine Vorgabe aus der EU-Datenschutzrichtlinie in deutsches Recht um. Da die nationale Umsetzung in jedem EU-Mitgliedsstaat anders lauten kann, sieht Art. 17 Abs. 3 2. Spiegelstrich der EU-Datenschutzrichtlinie vor, dass die technischen und organisatorischen Maßnahmen des Sitzes des Auftragsdatenverarbeiters anzuwenden sind. Ein europäischer Cloud-Anbieter mit Kunden in allen EU-Mitgliedsstaaten muss in diesem Zusammenhang folglich nicht 28 verschiedene nationale Vorgaben umsetzen, sondern nur diejenigen seines Sitzlandes, in dem die Verarbeitung dann tatsächlich erfolgt. Folglich wird ein deutscher Nutzer eines europäischen Cloud-Dienstes die konkreten Vorgaben des Bundesdatenschutzgesetzes zur Anlage zu § 9 BDSG möglicherweise nicht auf den ersten Blick in den Schutzmaßnahmen des Cloud-Anbieters wiederfinden. Darauf kommt es aber auch gar nicht an. Vielmehr muss der Cloud-Anbieter lediglich Maßnahmen vorweisen können, mithilfe derer die soeben (Ziffer 3.2.3.1) dargestellten Schutzziele der IT-Sicherheit erreicht werden können. Unmittelbar können die Maßnahmen aus der Anlage zu § 9 BDSG nur gegenüber deutschen Cloud-Anbietern eingefordert werden. Gegenüber Cloud-Anbietern außerhalb der EU oder des EWR können die Vorgaben der Anlage zu § 9 BDSG dem Cloud-Nutzer indes lediglich als Orientierung dienen.

Folglich muss der Anbieter von Cloud-Diensten innerhalb der EU oder des EWR (aber außerhalb Deutschlands) die Darstellung seiner Schutzmaßnahmen zwar nicht exakt an der Anlage zu § 9 BDSG ausrichten, jedoch hat er im Ergebnis vergleichbare Maßnahmen umzusetzen. Darstellungsstruktur und Begrifflichkeiten sind dabei unerheblich.

Hinweis
Der Cloud-Anbieter ist bei der Beschreibung der technischen und organisatorischen Maßnahmen nicht verpflichtet, Struktur und Begrifflichkeiten der Anlage zu § 9 BDSG zu verwenden, soweit die Schutzmaßnahmen inhaltlich erkennbar sind.

Nachfolgend werden die Maßnahmen aus der Anlage zu § 9 BDSG aufgezählt. Dabei erfolgt eine Wiedergabe des wesentlichen Gesetzestextes. Es sind Maßnahmen zu treffen, die je nach Art der personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle);
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle);

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle);
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weisungskontrolle);
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle);
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle);
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle);
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Hinweis
Angesichts der mit einer Verbreitung betriebsinterner Informationen einhergehenden Risikoerhöhung ist keine allzu detaillierte Darstellung der Schutzmaßnahmen seitens des Cloud-Anbieters zu erwarten. Die Darstellung der Schutzmaßnahmen muss die Kompetenz des Cloud-Anbieters erkennen lassen.

3.3 Prüfung der technischen und organisatorischen Maßnahmen

Hat sich der potenzielle Cloud-Nutzer nach sorgfältiger Auswahl (vgl. Ziffer 3.2) für einen Cloud-Anbieter entschieden, ist damit seine Prüfpflicht allerdings nicht erschöpft.

Vielmehr verpflichtet ihn § 11 Abs. 2 Satz 4 BDSG, „sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen“. Der (potenzielle) Cloud-Nutzer muss demzufolge bereits vor und sodann in regelmäßigen Abständen während der Auftragsdatenverarbeitung den Cloud-Anbieter auf die Einhaltung der Anforderungen und seiner Weisungen kontrollieren.

Danach kann der potenzielle Nutzer zwar den Vertragsschluss abwarten und die Kontrolle vor der tatsächlichen Datenverarbeitung vornehmen, da diese Prüfung nicht – wie die Auswahlentscheidung (§ 11 Abs. 1 Satz 2 BDSG) – vor Vertragsschluss erfolgen muss. Allerdings dürfte dieses Vorgehen beim Cloud Computing insbesondere aus den folgenden zwei Gründen eher unpraktisch sein:

- Wenn die Überzeugungsbildung zeigt, dass die Angaben des Cloud-Anbieters, welche der Auswahl zugrunde lagen, nicht zutreffen, dann muss rechtlich geprüft werden, wie es mit dem Vertrag weitergeht. Das kann durch eine vorgezogene Prüfung vermieden werden.
- Die Zeitspanne zwischen Vertragsschluss und tatsächlicher Nutzung wird bei der Nutzung von Cloud-Diensten häufig nicht für ein zweistufiges Vorgehen (1. sorgfältige Auswahl und dann zusätzlich 2. Überzeugungsbildung) ausreichen.

Die dafür erforderlichen Einblicke des Cloud-Nutzers in Informationen, an deren Geheimhaltung der Cloud-Anbieter ein gesteigertes Interesse haben kann, werden möglicherweise die Unterzeichnung von Verschwiegenheitsvereinbarungen voraussetzen. Dies kann selbst für den Fall gelten, dass Selbstauskünfte des Cloud-Anbieters wie schlüssige Datenschutzkonzepte oder aber Zertifikate, Testate oder Gütesiegel durch sachverständige Dritte (vgl. Ziffer 3.3.3) anstelle einer persönlichen Vor-Ort-Kontrolle ausreichen sollten.

Hinweis
Während das Gesetz lediglich davon spricht, dass die Überzeugung vor der Verarbeitung von personenbezogenen Daten zu erfolgen hat, ist es ratsam und nicht unüblich, diese Einschätzung bereits zum Gegenstand der Auswahlentscheidung zu machen und damit bereits vor Vertragsschluss zu vollziehen. Die dafür erforderlichen Einblicke des Cloud-Nutzers in Informationen, an deren Geheimhaltung der Cloud-Anbieter abhängig von der Detailtiefe ein gesteigertes Interesse haben wird, setzen die Unterzeichnung von Verschwiegenheitsvereinbarungen voraus.

3.3.1 Prüfungsturnus

Die erste Überprüfung der Einhaltung der technischen und organisatorischen Maßnahmen hat ausdrücklich vor der Verarbeitung personenbezogener Daten zu erfolgen. Hinsichtlich der Folgeprüfungen hat der Gesetzgeber indes bewusst von der Regelung starrer Fristen abgesehen. Vielmehr richtet sich die Häufigkeit der Prüfungen nach dem Einzelfall, wobei etwa die Sensitivität der Daten und die Auftragsdauer zu berücksichtigen sind. Es ist von einem Richtwert von etwa einem Jahr bis zu drei Jahren auszugehen.[5] Jede Abweichung davon ist besonders zu begründen. Geboten ist ferner eine anlassbezogene Kontrolle, wenn beispielsweise der Cloud-Nutzer von tatsächlichen, technischen oder rechtlichen Veränderungen Kenntnis erlangt.

3.3.2 Das „Wie“ der Überzeugungsbildung

Keine der genannten Vorschriften liefert konkrete Anhaltspunkte dazu, wie die Überzeugung von der Einhaltung von Schutzmaßnahmen praktisch zu erfolgen hat. Flexibilität und Volatilität der Daten sind wesentliche Eigenschaften des Cloud Computing. Dem (potenziellen) Cloud-Nutzer wird es in den meisten Fällen praktisch unmöglich oder zumindest nur verbunden mit einem unverhältnismäßig hohen Aufwand möglich sein, den Cloud-Anbieter persönlich an dessen Niederlassung oder an den Standorten der Datenverarbeitung aufzusuchen und zu kontrollieren. Die geforderte „Überzeugungsbildung“ kann auch – je nach Einzelfall – auf andere Weise erfolgen. Das Gesetz ordnet –

5 BayLDA, Auftragsdatenverarbeitung nach § 11 BDSG Gesetzestext mit Erläuterungen, Stand Januar 2014, Seite 8.

ausweislich des Gesetzgebungsverfahrens – jedenfalls keine persönliche Vor-Ort-Kontrolle an. Es ist nicht einmal von einer Kontrolle im Sinne einer Inspektion, sondern lediglich von „Überzeugungsbildung“ die Rede.

Die Varianten zum „Wie“ der Überzeugungsbildung reichen von Selbstauskünften des Cloud-Anbieters und Berichten eigener Prüfung des Cloud-Anbieters[6] über eigene Kontrollen des Cloud-Nutzers vor Ort zu Prüfungen durch sachkompetente und unabhängige Dritte. Bei der Wahl des Vorgehens sind das Schutzbedürfnis der Daten und die Besonderheiten des Cloud Computing zu berücksichtigen. Die Orientierungshilfe Cloud Computing, Version 2.0, fordert eine eigene Kontrolle oder eine Prüfung durch Dritte. Der Gesetzeswortlaut des § 11 Abs. 2 S. 4 BDSG[7] und die Regelung in der EU-Datenschutzrichtlinie machen diese Auslegung nicht zwingend.[8] Zukünftig wird, mit entsprechender Verbreitung von Datenschutz-Zertifizierungen für Cloud-Dienste, die Zertifizierung ein angemessener Weg für die Überprüfung von Cloud-Diensten sein.[9]

3.3.3 Anforderungen an ein Testat

Das Testat, Zertifikat oder Gütesiegel (die jeweilige Bezeichnung ist im vorliegenden Kontext im Unterschied zum Prüfungsinhalt unerheblich[10]) muss den gesetzlichen Anforderungen an Datenschutz und IT-Sicherheit entsprechen. Zudem muss die Stelle, die das Konformitätsbewertungsverfahren durchführt und das Testat ausstellt sowohl den erforderlichen Sachverstand als auch die notwendige Unabhängigkeit und Neutralität aufweisen. Auch hat der Prüfungsinhalt den gesetzlichen Anforderungen, zumindest des Bundesdatenschutzgesetzes, zu genügen. Dabei können sich aus Spezialgesetzen weitergehende Anforderungen ergeben (vgl. Ziffer 2.5). So kann eine Zertifizierung nach ISO 27001 zwar hinsichtlich der Datensicherheit als Nachweis herangezogen werden. Sie trifft aber keine Aussage über zu erfüllende Datenschutzanforderungen. Entscheidend ist, dass sich die Zertifizierung auf den jeweiligen Cloud-Dienst bezieht, an dem der (potenzielle) Cloud-Nutzer Interesse hat oder den er bereits nutzt. Auf eine allgemein gehaltene Bestätigung der Datenschutzkonformität eines beliebigen anderen Dienstes kann sich der (potenzielle) Cloud-Nutzer nicht stützen. Neben den Diensten müssen die IT-Systeme den genannten Anforderungen entsprechen. Damit sich der Cloud-Kunde von all dem selbst ein Bild machen kann, ist ihm der (technische) Prüfbericht offenzulegen, soweit nicht ohnehin eine Veröffentlichung des Berichts erfolgt ist. Mit diesen belastbaren technischen und gegebenenfalls zusätzlichen erforderlichen Unterlagen muss sich der (potenzielle) Cloud-Kunde sorgfältig, das heißt eingehend, auseinandersetzen, bevor er eine positive Auswahlentscheidung treffen kann. Eine reine Kenntnisnahme ohne eigene Meinungsbildung dürfte den Anforderungen an ein „Überzeugen“ wie im Gesetz gefordert nicht gerecht werden. Da die individuelle Prüfung durch einen Cloud-Nutzer häufig für den Cloud-Anbieter mit erheblichem Ressourcenaufwand verbunden ist, empfiehlt sich eine vertragliche Regelung zur Kostentragung.

Auch ein vom Dienstleister vorgelegtes schlüssiges Datensicherheitskonzept kann gegebenenfalls in Verbindung mit weiteren Dokumenten für die Überzeugungsbildung des Cloud-Nutzers herangezogen werden.

6 Vgl. BayLDA, a.a.O.: „ … sondern es können im Einzelfall auch ein vom Dienstleister vorgelegtes schlüssiges Datensicherheitskonzept (…) ausreichen“.

7 Entwurfsbegründung zu § 11 Abs. 2 BDSG, BT Drs. 16/13657, Seite 18 „(…) Dies wäre regelmäßig nicht angemessen und mit einem Verlust an Flexibilität verbunden, z. B. wenn der Auftraggeber ein Testat eines Sachverständigen einholen möchte oder wenn eine schriftliche Auskunft des Auftragnehmers ausreicht.“

8 Art. 17 Abs. 2 2. Halbsatz EU-Datenschutzrichtlinie: „(…) der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen.“

9 Hierzu Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier „Datenschutzrechtliche Lösungen für Cloud-Computing“, 2012.

10 Hierzu Kompetenzzentrum Trusted Cloud, Arbeitsgruppe „Rechtsrahmen des Cloud Computing“, Thesenpapier „Datenschutz-Zertifizierung durch private Stellen“, Seite 6.

3.4 Anforderungen an den Vertrag zwischen Cloud-Anbieter und Cloud-Nutzer

Die Regelungen zur Auftragsdatenverarbeitung in § 11 BDSG geben sehr „engmaschige“ Vorgaben bei der Beauftragung von Dienstleistern vor, die auch im Verhältnis des Cloud-Nutzers zum Cloud-Anbieter Anwendung finden.

Wenn mehrere Cloud-Dienste des Cloud-Anbieters durch den Cloud-Nutzer genutzt werden, kommt eine Rahmenvereinbarung über die Auftragsdatenverarbeitung in Betracht, welche dann mehrere Cloud-Dienste umfasst.

Das Risiko (und somit das Interesse) hinsichtlich einer korrekten Umsetzung der Vorgaben der Auftragsdatenverarbeitung liegt dabei eindeutig beim Cloud-Nutzer. Denn allein der Cloud-Nutzer ist Adressat der Bußgelddrohung im Fall einer unzureichenden Ausgestaltung der Auftragsdatenverarbeitung (Bußgeld bis zu 50.000 Euro, § 43 Abs. 1 Nr. 2b, Abs. 3 BDSG).

Danach muss der Cloud-Nutzer darauf achten, dass die vertragliche Konstruktion mit dem Cloud-Anbieter zu den zehn Punkten des § 11 Abs. 2 S. 2 BDSG eine Aussage trifft (vgl. Ziffer 3.3.2).

3.4.1 Schriftform der Vereinbarung über die Auftragsdatenverarbeitung

Nach „deutscher Lesart“ bedarf die Vereinbarung über die Auftragsdatenverarbeitung der Schriftform. Dies erfordert eine händische oder qualifiziert signierte Unterschrift.

Diese Anforderung des § 11 Abs. 2 Satz 2 BDSG geht weit über die Anforderungen der EU-Datenschutzrichtlinie hinaus. Diese deutsche Verschärfung gegenüber den Anforderungen der EU-Datenschutzrichtlinie im Vergleich zu den anderen europäischen Marktteilnehmern wird nachhaltig kritisiert, hat aber bislang kaum Resonanz im „gelebten“ Datenschutzrecht gefunden.

Es empfiehlt sich daher vorsichtshalber darauf zu achten, dass eine schriftliche Vereinbarung über die Auftragsvereinbarung mit dem Cloud-Anbieter vorliegt, welche die Anforderungen an die Schriftlichkeit nach § 126 BGB erfüllt.

> **Hinweis**
> Der Cloud-Nutzer sollte darauf achten, eine händisch unterzeichnete oder qualifiziert elektronisch signierte Vereinbarung zur Auftragsdatenvereinbarung vorweisen zu können. Dies gilt, obwohl Zweifel an der Europarechtskonformität einer strengen Schriftformklausel bestehen.

3.4.2 Zehn Mindestinhalte der Vereinbarung über die Auftragsdatenverarbeitung

Da in der Praxis Cloud-Dienste als Massengeschäft angeboten werden, ist davon auszugehen, dass keine individuellen Regelungen im Verhandlungswege zwischen Cloud-Anbieter und Cloud-Nutzer getroffen werden, sondern der Cloud-Nutzer das Vertragskonstrukt des Cloud-Anbieters auf Konformität mit den Vorgaben des § 11 BDSG prüfen muss. Die Vorgaben des § 11 BDSG müssen nicht in der gesetzlich normierten Reihenfolge oder alle in ein und demselben Vertragsdokument geregelt sein. Es ist durchaus denkbar, dass

sich die Kündigungsregelungen aus den allgemeinen Geschäftsbedingungen und andere Regelungsvorgaben aus der Leistungsbeschreibung ergeben.

Nachfolgend werden die Anforderungen nach § 11 Abs. 2 BDSG über die zehn Punkte der inhaltlichen Gestaltung der Vereinbarung über eine Auftragsdatenverarbeitung aufgeführt und kurz erläutert:

- **„Gegenstand und Dauer des Auftrags" (so § 11 Abs. 2 S. 2 Nr. 1 BDSG)**
  Diese Anforderung ergibt sich zumeist aus der Leistungsbeschreibung und der Regelung zur Vertragsdauer. Es kann aber auch eine Mindestlaufzeit mit automatischer Verlängerung und beidseitiger Kündigungsmöglichkeit vereinbart werden. Ein bei Beginn festgelegtes Enddatum ist nicht erforderlich.

- **„Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen" (so § 11 Abs. 2 S. 2 Nr. 2 BDSG)**
  Im Rahmen dieser Anforderungen sind die Informationen zu hinterlegen, die der verantwortlichen Stelle bewusst machen sollen, welche Daten im Rahmen der Auftragsdatenverarbeitung durch den Dienstleister zu verarbeiten sind. Zu beachten ist dabei, dass Verarbeiten nach § 3 Abs. 4 BDSG auch Speichern, Verändern, Übermitteln und Löschen umfasst. Abhängig von dem vereinbarten Cloud-Dienst kann auch der Anbieter diese Angaben bereits in seinem Vertrag berücksichtigen. So können zum Beispiel beim Angebot eines Kundenverwaltungsprogramms als Cloud-Dienst Art der Daten und Kreis der Betroffenen bereits aus Sicht des Cloud-Anbieters im Vertrag definiert werden. Bei einem reinen Speicherdienst weiß letzterer aber überhaupt nicht, welche Daten bei ihm eingestellt werden sollen, um welche Art von Daten es sich handelt und wie der Kreis der Betroffenen aussehen wird.
  Nach der herrschenden Meinung können für die Angabe zum Kreis der Betroffenen Oberbegriffe wie etwa Beschäftigtendaten, Kundendaten, Lieferantendaten, Besucherdaten etc. herangezogen werden. Eine Einzelauflistung nach den einzelnen Datenfeldern ist nicht erforderlich.

- **„die nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen" (so § 11 Abs. 2 S. 2 Nr. 3 BDSG),**
  In der Anlage zu § 9 BDSG werden die Kontrollmaßnahmen aufgeführt, die im Ergebnis Vertraulichkeit, Verfügbarkeit und Integrität der personenbezogenen Daten sichern sollen. In der Summe müssen diese Schutzmaßnahmen ein dem Schutzbedarf der personenbezogenen Daten angemessenes Niveau gewährleisten. Es ist zu beachten, dass bei einer vertraglichen Regelung, die zu sehr ins Detail ginge, jede Änderung der Sicherheitsmaßnahmen durch den Cloud-Anbieter zu einer vertraglichen Anpassung mit jedem einzelnen seiner Kunden führen müsste. Es empfiehlt sich daher, dem Cloud-Anbieter Änderungen an den technischen und organisatorischen Maßnahmen zuzugestehen, sofern in der Summe das Sicherheitsniveau dadurch nicht reduziert wird.

- **„die Berichtigung, Löschung und Sperrung von Daten" (so § 11 Abs. 2 S. 2 Nr. 4 BDSG),**
  Diese Regelung darf nicht darüber hinwegtäuschen, dass sich die Rechte des Betroffenen nach §§ 34, 35 BDSG gegen den Cloud-Nutzer richten (§ 11 Abs. 1 S. 2 i.V. m. § 6 BDSG) und der Cloud-Anbieter in den seltensten Fällen in der Lage sein dürfte, hierüber kompetent und eigenverantwortlich zu entscheiden. Diese Regelung ist daher der Hinweis des Gesetzes an den Cloud-Nutzer als verantwortlicher Stelle im Verhältnis zum Betroffenen, dass er dieser Pflicht auch bei Nutzung eines Cloud-Dienstes nachkommen können muss und sich notfalls gegenüber dem Cloud-Anbieter entsprechende Möglichkeiten vertraglich sichern muss. Kurzum: Der Cloud-Nutzer wird von seinen

Pflichten gegenüber dem Betroffenen nicht durch die Nutzung eines Cloud-Dienstes befreit. Dieser muss die Möglichkeit haben, die Berichtigung, Sperrung und Löschung personenbezogener Daten selbst vorzunehmen oder durch den Cloud-Anbieter vornehmen zu lassen. Dies ist bei der Auswahl der eingesetzten Anwendung, die in der Cloud betrieben wird, im Rahmen der Prüfung der Funktionalitäten zu beachten.

- **„die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen" (so § 11 Abs. 2 S. 2 Nr. 5 BDSG),**
  Der Cloud-Anbieter muss eine Organisationsstruktur aufweisen, die sicherstellt, dass er auch eigene, interne Kontrollen durchführt. So muss ein Cloud-Anbieter darlegen, dass er einen betrieblichen Datenschutzbeauftragten nach § 4f und § 4g BDSG hat und der Kontrolle einer Datenschutzaufsichtsbehörde nach § 38 BDSG unterliegt, sofern jeweils die Voraussetzungen dafür vorliegen. Das Gesetz verlangt nicht, dass der Name des betrieblichen Datenschutzbeauftragten vereinbart wird – eine Vertragsänderung bei einem Wechsel in der Personalie des Datenschutzbeauftragten wäre ein zu großer administrativer Aufwand.

- **„die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen" (so § 11 Abs. 2 S. 2 Nr. 6 BDSG),**
  Gerade dieser Passus ist vertraglich genau zu fassen: Das Gesetz verlangt nicht, was genau geregelt sein muss oder die namentliche Benennung eines Unterauftragnehmers, sondern nur, dass eine Regelung zur Berechtigung von Unterauftragsverhältnissen getroffen werden muss. Die Anforderung der Aufsichtsbehörden alle Unterauftragnehmer vertraglich zu vereinbaren, geht über diese gesetzliche Anforderung hinaus.[11] Zudem empfiehlt es sich, zu definieren, wann ein Unterauftragsverhältnis vorliegt. Ein solches dürfte in der Regel dann vorliegen, wenn der Cloud-Anbieter für die Erbringung der gegenüber dem Cloud-Nutzer vereinbarten Leistung ein weiteres Unternehmen einbindet, wobei sicherzustellen ist, dass die Weisungen des Cloud-Nutzers auch für dieses weitere Unternehmen gelten.
  Abzugrenzen sind dabei die Leistungen eines dritten Unternehmens, die der Cloud-Anbieter nutzt, um seine eingesetzte Hard- und Software und Abläufe „am Laufen" zu halten wie z. B. Wartungspartner, Reinigungskräfte, Transportpartner, aber auch Telekommunikationsdienstanbieter etc.
  Wird der Einsatz von Unterauftragnehmern gestattet, ist darauf zu achten, in welchem Land die Unterauftragnehmertätigkeiten erbracht werden und es empfiehlt sich, dies vertraglich zu dokumentieren. Bei Unterauftragnehmertätigkeiten außerhalb der EU und des EWR vergleiche Ziffer 4.2.2.

- **„die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers" (so § 11 Abs. 2 S. 2 Nr. 7 BDSG),**
  Da sich der Cloud-Nutzer nach § 11 Abs. 4 Satz 2 BDSG vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen überzeugen muss, empfiehlt es sich auch für das laufende Vertragsverhältnis im Vertrag zu regeln, welche Rechte dem Cloud-Nutzer dafür zustehen. Aufgrund des erhöhten Sicherheitsrisikos, das jeglicher Zutritt unternehmensfremder Personen zu den Sicherheits- und Produktionsbereichen des Cloud-Anbieters bedeutet, liegt es im Interesse des Cloud-Anbieters, diese Art der Zutritte möglichst zu begrenzen

11 Siehe Orientierungshilfe Cloud Computing (Fn. 1), Seite 9.

und den Cloud-Kunden stattdessen eine andere Möglichkeit, wie beispielsweise ein Zertifikat, anzubieten, das die Einhaltung von IT-Sicherheitsvorgaben bestätigt.

Hinweis
Nach Ansicht der deutschen Aufsichtsbehörden berechtigt auch ein Zertifikat den Cloud-Nutzer nicht, auf sein Recht auf Kontrolle der Einhaltung der technischen und organisatorischen Maßnahmen vor Ort vertraglich zu verzichten.

- **„mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen“ (so § 11 Abs. 2 S. 2 Nr. 8 BDSG),**
  Die Verantwortlichkeit des Cloud-Nutzers bei der Datenverarbeitung durch einen Dienstleister wie einem Cloud-Anbieter bedingt, dass geregelt wird, inwieweit der Cloud-Nutzer auch über Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder den Regelungen des Auftrages durch den Cloud-Anbieter oder bei diesem beschäftigten Personen zu informieren ist. Nur so kann er selbst denkbaren Informationspflichten gegenüber Aufsichtsbehörden oder den betroffenen Personen (vgl. Ziffer 6) nachkommen.
- **„der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält“ (so § 11 Abs. 2 S. 2 Nr. 9 BDSG),**
  Die Weisungen umfassen die Festlegung der Datenverarbeitung durch den Cloud-Anbieter. Diese kann durch eine Vereinbarung über die Funktionalitäten des Cloud-Dienstes geschehen. Diese Vereinbarung kann im Cloud-Vertrag, etwa durch Verweis auf die Dokumentation der Funktionalitäten, getroffen werden. Dem Cloud-Nutzer muss darüber hinaus das Recht zur Einzelweisung vorbehalten werden. Das Weisungsrecht ist kein Instrument, mit der die vereinbarte Leistungsbeschreibung durch den Cloud-Nutzer geändert werden kann.
- **„die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags“ (so § 11 Abs. 2 S. 2 Nr. 10 BDSG).**
  Wie bei allen Schuldverhältnissen sollte auch die Beendigung des Auftragsverhältnisses so geregelt sein, dass die Rückabwicklung und die datenschutzkonforme Behandlung der personenbezogenen Daten vorgesehen ist. Bei einer Vereinbarung über die Löschung nicht mehr benötigter Daten auf Datenträgern, empfiehlt es sich, die DIN 66399 zu berücksichtigen (vgl. auch Ziffer 7).

Vorstehendes ist der gesetzliche Mindestinhalt des Vertrages. Es ist zulässig, weitere Regelungen aufzunehmen (vgl. Ziffer 6 zu Datenschutzpannen), sofern solche Regelungen nicht vorstehende Vorgaben aushöhlen oder unterlaufen.

4 Cloud-Anbieter und Subunternehmer aus Drittstaaten

Dieses Kapitel beschreibt die rechtlichen Voraussetzungen einer Datenverarbeitung durch Cloud-Anbieter und deren Subunternehmer mit Sitz in Staaten außerhalb der EU und/oder des EWR (sog. Drittstaaten).

Cloud Computing ermöglicht durch die Virtualisierung sowie die Zugriffsmöglichkeiten über das Internet eine flexible Datenverarbeitung, d.h. eine Datenverarbeitung, die gegebenenfalls auf verschiedene Standorte und Anbieter aufgeteilt ist. Insbesondere die Standorte können einem schnellen Wandel unterliegen. Dabei kommt es häufig zu einem grenzüberschreitenden Datentransfer, der strengen datenschutzrechtlichen Voraussetzungen unterliegt. Für die datenschutzkonforme Ausgestaltung des grenzüberschreitenden Cloud Computing hat in erster Linie der Cloud-Nutzer als verantwortliche Stelle zu sorgen (vgl. Ziffer 2.3).

4.1 Anwendbarkeit des deutschen Datenschutzrechts

Die Anwendbarkeit des materiellen deutschen Datenschutzrechts richtet sich grundsätzlich nach dem Sitz des Cloud-Nutzers und seinem Verhältnis zu demjenigen, dessen Daten in der Cloud verarbeitet werden sollen. Unerheblich für die Anwendbarkeit des Bundesdatenschutzgesetzes ist hingegen, wo der Cloud-Anbieter und seine Subunternehmer ihren Sitz haben.

Ist der Cloud-Nutzer in der Bundesrepublik Deutschland ansässig und verwendet er Daten von Personen, die ebenfalls in Deutschland ansässig sind, ist das Bundesdatenschutzgesetz ohne Weiteres anwendbar.

Verarbeitet der Cloud-Nutzer hingegen Daten von Betroffenen, die außerhalb Deutschlands ansässig sind, dann ist zu unterscheiden: Sind die Betroffenen in der EU oder dem EWR ansässig, dann kommt deutsches Recht zur Anwendung. Sind die Betroffenen hingegen außerhalb der EU oder des EWR ansässig, lässt sich nicht nach deutschem Recht beurteilen, welches Datenschutzrecht zur Anwendung kommt. Häufig wird dann das Datenschutzrecht des Heimatlandes der Betroffenen zur Anwendung kommen. Dies muss in jedem Einzelfall bewertet werden.

Der Vollständigkeit halber sei erwähnt, dass deutsches Datenschutzrecht durchaus nicht nur auf deutsche Cloud-Nutzer anwendbar ist. Ist der Cloud-Nutzer im Ausland ansässig, ist danach zu unterschieden, ob es sich bei dem Sitzland um ein Land innerhalb oder außerhalb der EU oder des EWR handelt. Auf die entsprechenden Konstellationen kann an dieser Stelle jedoch nicht näher eingegangen werden. Dieser Leitfaden geht – wie in der Einleitung angesprochen – von der Anwendung deutschen Datenschutzrechts aus.

Hinweis
Sitzt der Cloud-Nutzer als verantwortliche Stelle in Deutschland und erhebt er Daten von Personen in Deutschland, in der EU oder im EWR, so ist stets das Bundesdatenschutzgesetz anwendbar. Keine Rolle spielt, ob Cloud-Anbieter und/oder Subunternehmer in Drittstaaten sitzen und ob die eigentliche Datenverarbeitung im In- oder Ausland stattfindet.

4.2 Wann ist die grenzüberschreitende Datenübermittlung zulässig?

Die Beurteilung der Zulässigkeit einer Übermittlung personenbezogener Daten an ausländische Cloud-Anbieter hängt entscheidend von der Frage ab, ob diese innerhalb der EU oder des EWR oder in einem Drittstaat ansässig sind. Anknüpfungskriterium ist also in erster Linie das Sitzland des Cloud-Anbieters.

4.2.1 Datenübermittlung an Stellen mit EU- oder EWR-Sitz

Da in der EU und dem EWR aufgrund der EU-Datenschutzrichtlinie ein weitgehend harmonisiertes Datenschutzniveau besteht, steht die Datenübermittlung durch den Cloud-Nutzer an den Cloud-Anbieter und/oder dessen Subunternehmer mit EU- oder EWR-Sitz der Übermittlung an Stellen in Deutschland gleich (§ 4b Abs. 1 BDSG). D. h. die Privilegierung der Auftragsdatenverarbeitung gem. § 11 BDSG ist einschlägig (zu den Voraussetzungen vgl. Ziffern 2.4.2.1 und 3.1). Daher sollte der Cloud-Nutzer stets darauf bedacht sein, die Orte der technischen Verarbeitung genauestens vertraglich festzulegen und insoweit Transparenz von dem Cloud-Anbieter zu verlangen. Dies gilt auch und insbesondere für den Einsatz von Subunternehmern und deren Sitz. Dem Cloud-Nutzer ist es andernfalls unmöglich, die datenschutzrechtlichen Voraussetzungen an die Beauftragung und Datenübermittlung festzustellen geschweige denn durchzusetzen.

Hinweis
Die Datenübermittlung an Cloud-Anbieter und Subunternehmer mit Sitz in der EU oder im EWR unterliegt den gleichen Anforderungen wie eine Übermittlung an einen inländischen Anbieter.

4.2.2 Datenübermittlung an Stellen mit Drittstaatensitz

Etwas anderes gilt, wenn der Cloud-Anbieter und/oder Subunternehmer in einem Drittstaat, also in einem Land außerhalb des EWR, ansässig sind. In diesem Fall greift die Privilegierung der Auftragsdatenverarbeitung gemäß § 11 BDSG nicht (zu den Voraussetzungen vgl. Ziffern 2.4.2.1 und 3.1), mit der Folge, dass eine zweistufige Zulässigkeitsprüfung vorzunehmen ist.

4.2.2.1 Die erste Stufe der Zulässigkeitsprüfung

Auf der ersten Stufe ist nach dem in § 4 Abs. 1 BDSG verankerten Verbot mit Erlaubnisvorbehalt (vgl. Ziffer 2.4.1) zu prüfen, ob eine Rechtsgrundlage für die Datenübermittlung in Betracht kommt. Als Rechtsgrundlage kann entweder die Einwilligung der Betroffenen (diese einzuholen wird jedoch in der Regel nicht praktikabel sein) oder ein gesetzlicher Erlaubnistatbestand dienen. Als gesetzlicher Erlaubnistatbestand kommt insbesondere § 28 Abs. 2 BDSG in Betracht. Allerdings ist zu beachten, dass für Beschäftigtendaten vorrangig § 32 BDSG gilt und ein Rückgriff auf § 28 Abs. 2 BDSG für die Verarbeitung von Beschäftigtendaten in der Cloud nicht unumstritten ist. Für sogenannte besondere personenbezogene Daten nach § 3 Abs. 9 BDSG gelten als Spezialregelung die Absätze 6 bis 9 des § 28 BDSG. Danach scheidet eine Verarbeitung solcher Daten in der Cloud außerhalb einer Auftragsdatenverarbeitung und des Vorliegens einer Einwilligung typischerweise aus. Im Anwendungsbereich der Datenschutzbestimmungen des Telekommunikations- und des Telemediengesetzes kommt typischerweise ebenfalls kein Rückgriff auf § 28 Abs. 2 BDSG in Betracht.

Die Zulässigkeit nach § 28 Abs. 2 BDSG basiert – vereinfacht gesagt – auf einer Abwägung der berechtigten Interessen des Cloud-Nutzers an der Nutzung des konkreten Cloud-Dienstes einerseits und den entgegenstehenden schutzwürdigen Interessen der Betroffenen, deren Daten in der Cloud verarbeitet werden sollen. Im Rahmen dieser Interessenabwägung kann es sich positiv zugunsten der Zulässigkeit auswirken, wenn zwischen dem Cloud-Nutzer und dem Cloud-Anbieter eine Vereinbarung nach Maßgabe der Auftragsdatenverarbeitung geschlossen wird. Diese wird dann zwar nicht die Rechtsgrundlage, beeinflusst aber die Interessenabwägung positiv.

Hinweis
Eine Nutzung von Cloud-Diensten außerhalb der EU oder dem EWR muss auf der Grundlage einer gesetzlichen Zulässigkeitsregelung erfolgen.

4.2.2.2 Die zweite Stufe der Zulässigkeitsprüfung

Auf der zweiten Stufe ist die Zulässigkeit der Übermittlung gerade an eine Drittlandstelle zu prüfen. D. h. die Übermittlung ist nur zulässig, wenn bei dem Cloud-Anbieter als datenempfangende Stelle ein angemessenes Datenschutzniveau herrscht. Die Angemessenheit des Schutzniveaus ist unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung von Bedeutung sind. Insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden (§ 4b Abs. 3 BDSG).

Zur Sicherstellung des angemessenen Datenschutzniveaus kommen verschiedene Möglichkeiten in Betracht.

4.2.2.2.1 Cloud-Anbieter in einem sogenannten sicheren Drittland

Die Europäische Kommission hat die nachfolgend genannten Länder als sogenannte sichere Drittländer anerkannt. Damit ist festgestellt, dass in diesen Länder ein für eine Übermittlung ausreichendes Datenschutzniveau besteht.

- Andorra
- Argentinien
- Australien
- Färöer Inseln
- Guernsey
- Isle of Man
- Israel
- Jersey
- Kanada
- Neuseeland
- Schweiz
- Uruguay

4.2.2.2.2 US-amerikanische Cloud-Anbieter und Safe-Harbor

Die Vereinigten Staaten von Amerika (USA) gehören grundsätzlich nicht zu dem Kreis der sicheren Drittländer. Für US-amerikanische Datenverarbeiter besteht jedoch mit dem sogenannten Safe-Harbor-Abkommen zwischen der EU und den USA eine Besonderheit. Vereinfacht gesagt gelten, dass US-amerikanische Datenverarbeiter, welche sich den Anforderungen des Safe-Harbor-Abkommens (sog. Safe Harbor Principles) unterworfen haben, als Unternehmen mit einem ausreichenden Datenschutzniveau gelten.

Die Aufsichtsbehörden haben klargestellt, dass sich Cloud-Nutzer nicht allein auf die Behauptung einer Safe-Habor-Zertifizierung des Cloud-Anbieters verlassen können, sondern haben Anforderungen an eine Mindestprüfung durch den Cloud-Nutzer aufgestellt.[12]

Cloud-Nutzer sollten sich bewusst sein, dass das Safe-Harbor Abkommen in der Kritik der deutschen Datenschutzaufsichtsbehörden steht. Die Kritik bezieht sich auf die praktische Tauglichkeit der Selbstzertifizierung und der Kontrolle durch die US-Aufsichtsinstanz. Vor dem Hintergrund der jüngsten Entwicklungen im Zusammenhang mit der NSA-Affäre ist das Safe-Harbor-Abkommen stark in die Kritik geraten ist.

4.2.2.2.3 Der Abschluss der EU-Standardvertragsklauseln

In der Praxis ist vor allem der Abschluss der EU-Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern (EU-Standardvertragsklauseln) relevant. Die Europäische Kommission hat im Februar 2010 ein überarbeitetes Standardvertragswerk speziell für den Fall der Auftragsdatenverarbeitung mit einem im Drittland ansässigen Auftragnehmer beschlossen. Soll die Zulässigkeit der Übermittlung an Drittstaatenstellen durch die EU-Standard-vertragsklauseln erreicht werden, kommt es für die Vertragskonstruktion entscheidend auf zwei Fragen an. Erstens, hat der Cloud-Anbieter Subunternehmer beauftragt? Zweitens, wo befindet sich der Sitz der Beteiligten?

Werden keine Subunternehmer eingebunden (was in der Praxis jedoch eher die Ausnahme sein dürfte), ist der Abschluss des EU-Standardvertrages unproblematisch. Es handelt sich dann um die Grundkonstellation der Klauseln; der Cloud-Nutzer als verantwortliche Stelle mit Sitz innerhalb des EWR ist der Datenexporteur und kontrahiert mit dem Cloud-Anbieter mit Sitz außerhalb des EWR. Dieser ist der Datenimporteur.

Komplizierter sind Konstellationen, in denen die Datenverarbeitung zumindest teilweise durch Subunternehmer erfolgt.[13] Nach Ansicht der Aufsichtsbehörden muss die verantwort-liche Stelle (hier also der Cloud-Nutzer) immer Partei des EU-Standardvertrages werden. Ein direkter Abschluss zwischen Cloud-Anbieter und Subunternehmer ist grundsätzlich nicht möglich, da für diese Konstellation zumindest derzeit kein Standardvertrag vorge-sehen ist.[14] Dies führt zu der nicht sehr praxisfreundlichen Konstellation, dass der Cloud-Nutzer in Abweichung des zivilrechtlichen Vertrages über den Cloud-Dienst grundsätzlich direkt mit einem oder mehreren Subunternehmern des Cloud-Anbieters kontrahieren

12 Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe-Harbor-Abkommen durch das Daten exportierende Unternehmen, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 28./29. April 2010 in Hannover, überarbeitetet durch die Fassung vom 23.8.2010.

13 Für eine Übersicht über die verschiedenen Konstellationen siehe Anhang.

14 Siehe aber Entwurf der Art. 29 Datenschutzgruppe über Standardklauseln für die Übermittlung von Daten durch Auftragsdatenverarbeiter an Unterauftragnehmer im Arbeitspapier 214.

muss.[15] Der neue EU-Standardvertrag von 2010 bietet jedoch eine Vereinfachung für den Fall, dass sowohl Cloud-Anbieter als auch Subunternehmer in einem Drittstaat ansässig sind. Über Ziffer 11 des EU-Standardvertrages von 2010 ist eine Unterbeauftragung von dem Cloud-Anbieter an den Subunternehmer im eigenen Namen unmittelbar anerkannt, sofern zwischen diesen vergleichbare Verträge zum Hauptauftrag abgeschlossen werden.[16] Für alle anderen Fälle bleibt es bei dem Erfordernis des Direktvertrages. Zusammenfassend sind folgende Konstellationen zu unterscheiden:

- **Cloud-Anbieter und Subunternehmer sitzen in Drittstaaten**
  Der Cloud-Anbieter kann auf Grund von Ziffer 11 des EU-Standardvertrages von 2010 den oder die Subunternehmer im eigenen Namen unterbeauftragen. Voraussetzung ist, dass zwischen diesen dem Standardvertrag vergleichbare Verträge abgeschlossen werden.
- **Cloud-Anbieter sitzt in EU oder EWR, Subunternehmer sitzt in Drittstaat**
  Der Cloud-Nutzer muss mit dem Subunternehmer einen EU-Standardvertrag abschließen. Ein Standardvertrag mit dem Cloud-Anbieter ist nicht erforderlich, da dieser nicht in einem Drittland ansässig ist.[17] Da u. U. wegen der möglichen Vielzahl von Subunternehmern entsprechend viele Standardverträge abgeschlossen werden müssen, ist es, sofern der Cloud-Nutzer dies wünscht, auch praktikabel und akzeptabel, dass der Cloud-Anbieter in Vertretung des Cloud-Nutzers den Standardvertrag mit den Subunternehmern abschließt. Andernfalls kann es u. U. sinnvoll sein, dass der Cloud-Anbieter dem Vertrag zwischen Cloud-Nutzer und Drittstaaten-Subunternehmer beitritt.[18]
- **Cloud-Anbieter sitzt in Drittstaat, Subunternehmer sitzt in EU oder EWR**
  Nur zwischen Cloud-Nutzer und Cloud-Anbieter muss ein EU-Standardvertrag geschlossen werden, da nur dieser einen Drittlandsitz hat. Ein Vertragsbeitritt des EU- oder EWR-Subunternehmers ist jedenfalls sinnvoll.[19]

Übersicht: Cloud-Anbieter in EU/EWR mit Subunternehmern in Drittstaaten

	Kein Subunternehmer	Subunternehmer in EU/EWR	Subunternehmer in Drittstaat
Cloud-Anbieter in EU/EWR	Kein EU-Standardvertrag erforderlich.	Kein EU-Standardvertrag erforderlich.	EU-Standardvertrag nur zwischen Cloud-Nutzer und Subunternehmer erforderlich. Cloud-Anbieter kann dem Vertrag beitreten. Cloud-Anbieter kann auch in Vertretung des Cloud-Nutzers kontrahieren.
Cloud-Anbieter in Drittstaat	Grundkonstellation. EU-Standardvertrag zwischen Cloud-Nutzer und Cloud-Anbieter erforderlich.	EU-Standardvertrag nur zwischen Cloud-Nutzer und Cloud-Anbieter erforderlich. Subunternehmer kann diesem Vertrag beitreten.	EU-Standardvertrag zwischen Cloud-Nutzer und Cloud-Anbieter erforderlich. Nach dem EU-Standardvertrag von 2010 kann der Cloud-Anbieter den/die Subunternehmer im eigenen Namen unterbeauftragen. Das Schutzniveau dieser Verträge darf nicht hinter den EU-Standardvertragsklauseln zurückbleiben.

15 Siehe Fallgruppen zur internationalen Auftragsdatenverarbeitung, Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung, 28.03.2007, Seite 3.
16 Orientierungshilfe Cloud Computing (Fn. 1), Seite 14 f.
17 Siehe Arbeitspapier 176 der Art. 29-Datenschutzgruppe „Häufig gestellte Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG".
18 Fallgruppen zur internationalen Auftragsdatenverarbeitung, Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung, 28.03.2007, Seiten 4, 5.
19 A.a.O., Seiten 6 – 10.

4.2.2.2.4 Processor Binding Corporate Rules

Für international agierende Cloud-Anbieter besteht mit dem sogenannten Processor Binding Corporate Rules (PBCR) die Möglichkeit zur grenzüberschreitenden Datenverarbeitung auch in Drittstaaten. Das Instrument ist jedoch nur auf den Fall zugeschnitten, in dem die Verarbeitung der Daten im Konzern des Cloud-Anbieters verbleibt.

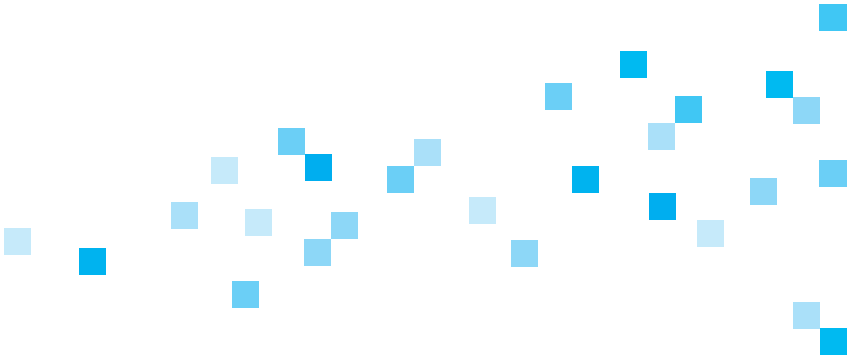
4.2.2.2.5 Gesetzliche Ausnahmen

Die genannten Maßnahmen zur Herstellung eines angemessenen Datenschutzniveaus beim Cloud-Anbieter sind entbehrlich, wenn eine der gesetzlichen Ausnahmen nach § 4c Abs. 1 BDSG vorliegt. Für das Cloud Computing sind in erster Linie die Ausnahmetatbestände in § 4c Abs. 1 Nr. 1 und Nr. 2 BDSG relevant. Diese Fälle kommen in der Praxis jedoch eher selten vor, weshalb auf diese an dieser Stelle nicht näher eingegangen wird.

4.2.2.2.6 Ergänzungen nach § 11 Abs. 2 BDSG

Nach Ansicht der Aufsichtsbehörden befreien weder der Abschluss eines EU-Standardvertrages noch eine Safe-Harbor-Zertifizierung oder PBCR des Cloud-Anbieters den Cloud-Nutzer davon, zusätzlich eine den Anforderungen des § 11 BDSG entsprechende Vereinbarung zu treffen.[20] Dies gilt unabhängig davon, dass die Privilegierungswirkung des § 11 BDSG nicht greift. Begründet wird dies vor allem damit, dass die EU-Standardvertragsklauseln den spezifischen Pflichtenkatalog nach § 11 BDSG nicht vollständig abbilden und das Schutzniveau bei der Beauftragung eines Anbieters aus einem Drittstaat nicht hinter dem Schutzniveau einer rein europäischen Verarbeitung zurückbleiben darf. Die Vereinbarung des Pflichtenkatalogs kann durch ergänzende Anlagen zum EU-Standardvertrag oder zum zivilrechtlichen Dienstvertrag und durch separate vertragliche Regelungen erfolgen.

Diese Ansicht der Aufsichtsbehörden ist jedoch umstritten. Allerdings spricht für die Ansicht der Aufsichtsbehörden rechtlich die Regelung in § 11 Abs. 5 BDSG (vgl. Ziffer 2.4.2.3) und faktisch, dass der Abschluss einer solchen Vereinbarung die Interessenabwägung im Rahmen der Zulässigkeitsprüfung positiv beeinflusst (vgl. Ziffer 4.2.2.1).



20 Siehe Orientierungshilfe Cloud Computing (Fn. 1), Seite 9.

5 Die Überwachung des Cloud-Anbieters durch den Cloud-Nutzer

Um seiner Verantwortlichkeit gerecht zu werden, obliegen dem Cloud-Nutzer bestimmte Pflichten, die sich aus § 11 BDSG ergeben. Nach § 11 Abs. 2 Satz 4 BDSG muss er sich hinsichtlich des Cloud-Anbieters (des Auftragnehmers) vor Beginn der Verarbeitung und sodann regelmäßig von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen überzeugen. Wie er sich überzeugen kann/muss, hat der Gesetzgeber nicht vorgeschrieben. Aus den Gesetzesbegründungen ergibt sich, dass eigene Vor-Ort-Kontrollen des jeweiligen Auftraggebers (Cloud-Nutzers) nicht erforderlich sind. Die Datenschutzaufsichtsbehörden empfehlen die Überzeugung durch ein Testat eines fachkundigen Sachverständigen; der Gesetzgeber hat aber auch nicht ausgeschlossen, dass in Einzelfällen auch andere Unterlagen, wie ein schlüssiges Datensicherheitskonzept, je nach Fallgestaltung für die Überzeugung herangezogen werden. Details hierzu werden oben unter Ziffern 3.3.2 und 3.3.3 dargestellt.

Auf dem Markt werden hierzu einige Testate, Zertifikate und Gütesiegel angeboten, die letztendlich auch verhindern, dass in dem Massengeschäft Cloud-Dienste ein Rechenzentrumstourismus entsteht, der den Sicherheitsinteressen der Cloud-Anbieter und der Cloud-Nutzer zuwiderläuft.

Aus den derzeit erhältlichen Angeboten seien im Folgenden drei aufgeführt:

Das **Datenschutzsiegel der DSZ Datenschutz Zertifizierungsgesellschaft GmbH,** welches als Audit nach § 11 BDSG durch die Datenschutzverbände Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. und die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) entwickelt wurde und durch den Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen befürwortet wird. Allerdings ist dort aktuell noch kein Modul speziell für Cloud-Dienste eingeführt.

Die ISO (International Organization for Standardization) versucht mit der Norm **„ISO/IEC 27018:2014-08 Informationstechnik – Sicherheitsverfahren – Anwendungsregel für den Schutz von personenbezogenen Daten in Public Clouds“** im August 2014 einen weltweiten Standard für Cloud-Dienste vorzugeben. Sie baut dabei auf die bereits existierenden Sicherheitsstandards ISO 27001 und ISO 27002 auf. Die neuen Standards fordern zusätzlich zu den Sicherheitsinformationen die Einhaltung bestimmter datenschutzrechtlicher Aspekte. Erfahrungswerte zu dieser neuen Norm sind bisher nicht bekannt.

Im Pilotprojekt „Datenschutz-Zertifizierung für Cloud-Dienste“ des Kompetenzzentrums Trusted Cloud wurde ein datenschutzrechtlicher Prüfstandard, das **Trusted Cloud-Datenschutzprofil für Cloud Dienste (TCDP)**[21] entwickelt, das auf dem Standard ISO/IEC 27018 beruht und die gesetzlichen Anforderungen des BDSG für Cloud-Dienste konkretisiert. Eine Zertifizierung nach dem TCDP kann vom Cloud-Nutzer zur Erfüllung seiner Überzeugungspflicht herangezogen werden.

21 Kompetenzzentrum Trusted Cloud, Trusted Cloud-Datenschutzprofil für Cloud-Dienste .v.09, 2014, abrufbar unter www.trusted-cloud.de.

Gleich für welches Angebot eines externen Testats sich der Cloud-Nutzer und der Cloud-Anbieter entscheiden, damit der Cloud-Nutzer seiner Überzeugungspflicht nach § 11 Abs. 2 Satz 4 BDSG nachkommen kann, sollten die Anforderungen berücksichtigt werden, die der Düsseldorfer Kreis im Februar 2014 definierte, welche er an eine Zertifizierung stellt (Beschluss vom 26.02.2014: „Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden“). Bei der Auswahl eines Zertifizierungsverfahrens, sollten diese Anforderungen als Entscheidungshilfe herangezogen werden. Danach ist u. a. zu berücksichtigen, dass

- im Zertifizierungsverfahren unterschiedliche Ebenen eingebunden sind (Prüfung, Zertifizierung, Akkreditierung),
- die zugrundeliegenden Prüfungsstandards öffentlich zugänglich sind,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten getroffen sind,
- die Anforderungen an die Eignung als Prüferin und Prüfer festgelegt wurden,
- dem Zertifikat die Prüfaussage ohne Weiteres entnommen werden kann, die Regelungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten bestimmt sind und
- die Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte veröffentlicht werden.

6 Security Breach Notification (§ 42a BDSG, § 83a SGB X; §§ 93 Abs. 3, 109a TKG; § 15a TMG)

Das Datenschutzrecht sieht für den Fall von „Datenschutzpannen“ Meldepflichten vor. Diese sind insbesondere in § 42a BDSG, § 83a SGB X, §§ 93 Abs. 3, 109a TKG, § 15a TMG geregelt.

Die Meldepflicht trifft den Cloud-Nutzer (als verantwortliche Stelle) und nicht den Cloud-Anbieter.

Eine Datenschutzpanne liegt – vereinfacht gesagt – vor, wenn bestimmte personenbezogene Daten „unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind“. Hiervon sind Hacking-Fälle oder andere „Sicherheitslücken“ erfasst. Um eine Meldepflicht auszulösen, müssen zwar weitere Voraussetzungen hinzukommen, aber in jedem Fall muss der Cloud-Nutzer von einem solchen Vorfall Kenntnis erlangen, um die weiteren Voraussetzungen einer Meldepflicht prüfen zu können.

Der Cloud-Anbieter muss den Cloud-Nutzer dazu hierüber informieren. Dies muss in dem Vertrag mit dem Cloud-Nutzer geregelt sein. Denn ein Cloud-Anbieter wird nicht gern eine solche Panne bei ihm mitteilen wollen.

Vereinfacht gesagt müssen die zuständige Datenschutzaufsichtsbehörde und jeder Betroffene – alternativ zur Information der Betroffenen: die Öffentlichkeit – unverzüglich über den Vorfall informiert werden.

Die Datenschutzaufsichtsbehörden scheinen – jedenfalls teilweise – die Frist bereits mit der Kenntnis des Cloud-Anbieters und nicht erst mit der Kenntnis des Cloud-Nutzers beginnen zu lassen.[22] Es mag bezweifelt werden, dass dies rechtlich belastbar ist, macht aber gleichwohl einen in der Praxis relevanten Standpunkt deutlich.

Zusammenfassend zeigt sich, dass dieser Aspekt und insbesondere die Unterstützungshandlungen des Cloud-Anbieters vertraglich explizit geregelt sein sollten.

22 Vgl. Berliner Beauftragter für den Datenschutz und die Informationsfreiheit, FAQ zu § 42a BDSG, Stand: Mai 2014, Seite 2.

7 Die Beendigung des Auftragsverhältnisses

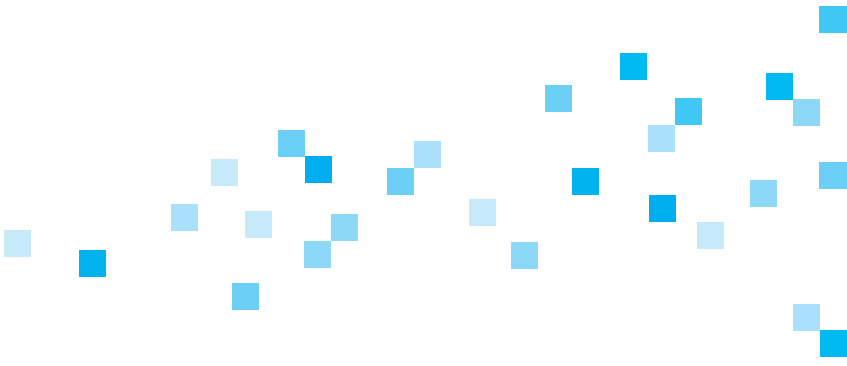
Die Beendigung ist unter zwei Aspekten zu regeln:

- Die Auftragsdatenverarbeitung darf nicht enden, bevor alle Daten beim Cloud-Anbieter gelöscht und gegebenenfalls zusätzlich auf den Cloud-Nutzer rückübertragen sind.
- Die Auftragsdatenverarbeitung muss entweder die Löschung oder die Rückübertragung und die anschließende Löschung eindeutig regeln.

Anderenfalls besteht die Gefahr, dass die durch die Auftragsdatenverarbeitung zu sichernde Herrschaft des Cloud-Nutzers über die Daten verloren geht.

Es ist auch ratsam explizit zu regeln, dass eines der genannten Szenarien ohne zusätzliche Vergütung geleistet werden muss. Denn gerade bei Beendigung des Vertrags sind solche Aspekte schwieriger zu besprechen als zu Beginn einer Vertragsbeziehung.

Entscheidend ist, dass auch zum Ende der Vertragsbeziehung hin nicht die „Herrschaft über die Daten“ verloren geht.



8 Checkliste

Hinweis
Dieser Katalog ist nicht abschließend. Die tatsächlichen, bereichsspezifischen Anforderungen richten sich unter anderem nach der Art der zu verarbeitenden Daten.

Anwendung des Datenschutzrechts (Ziffer 2.1)

Sollen Daten, welche Menschen zugeordnet werden können, mit dem Cloud-Dienst verarbeitet werden?

- Falls nein: Das Datenschutzrecht muss nicht beachtet werden.
- Falls ja: Die nachfolgende Checkliste ist zu beachten.

Abschluss einer Vereinbarung über die Auftragsdatenverarbeitung (Ziffer 2.4.2)

Soll eine Vereinbarung über die Auftragsdatenverarbeitung geschlossen werden, sollen die Einwilligungen der Betroffenen eingeholt werden oder wird die Nutzung des Cloud-Dienstes mit einer gesetzlichen Regelung gerechtfertigt?

- Die Datenschutzaufsichtsbehörden tendieren zur Ausgestaltung als Auftragsdatenverarbeitung.

  Ist der Zugriff des Cloud-Anbieters auf personenbezogene Daten im Rahmen der Wartung und Pflege der Hard- und Software tatsächlich sicher ausgeschlossen?

  Typischerweise wird ein solcher Zugriff bei Cloud-Services nicht tatsächlich sicher ausgeschlossen sein.
- Falls nein: Es besteht die gesetzliche Pflicht zum Abschluss eine Vereinbarung über die Auftragsdatenverarbeitung.

Auswahl des Cloud-Anbieters (Ziffer 3.2)

Bei der Auswahlentscheidung sollte sich der potenzielle Cloud-Nutzer unter anderem die folgenden Fragen stellen und die folgenden Aspekte berücksichtigen:

Anforderungsprofil (Ziffer 3.2.2)

- Welche Verarbeitungsprozesse sollen in „die Cloud“ verlagert werden?
- Welche Arten von personenbezogenen Daten sollen verarbeitet werden?
- Greifen bereichsspezifische Vorschriften in diesem Zusammenhang?

Auswahlkontrolle (Ziffer 3.3)

Anhand welcher Dokumente kann eine Überzeugungsbildung stattfinden?

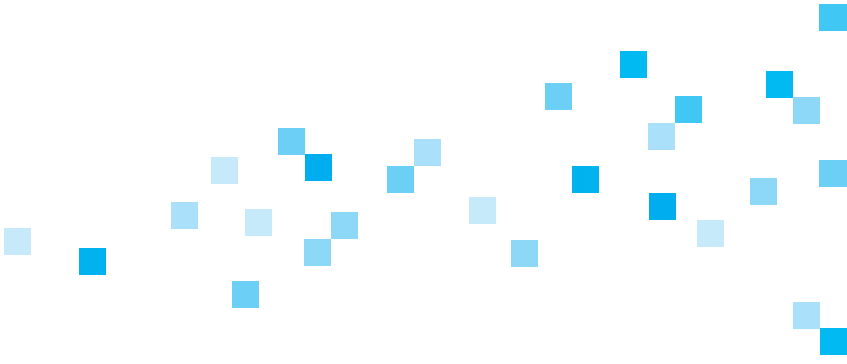
- Verfügt der Cloud-Anbieter über ein Testat, das eine sachverständige, unabhängige dritte Stelle ausgegeben hat?
- Ist das Testat aktuell? Hat der Cloud-Anbieter seine Gültigkeit bestätigt?
- Ist ein aufschlussreicher Prüfbericht einsehbar? Ist das Prüfergebnis nachvollziehbar? Was genau bestätigt das Testat?

  Bestätigen diese Dokumente die Erfüllung der (ggf. speziellen) Anforderungen an Datenschutz und IT-Sicherheit?
- Entsprechen die Sicherheitsmaßnahmen für die jeweiligen Bereiche der Anlage zu § 9 BDSG dem jeweiligen Stand der Technik?

  Werden gegebenenfalls weitere Nachweise benötigt und zur Verfügung gestellt?

Weitere Auswahlkriterien

- Sind die Vertragsbedingungen des Cloud-Anbieters transparent gestaltet? Finden sich darin beispielsweise Regelungen zu den verwendeten Rechenzentren, zu einzuschaltenden Unterauftragnehmern und zur Löschung von Daten nach Vertragsschluss? (Ziffer 3.4.2 sowie Ziffern 6 und 7)
- Stellt der Cloud-Anbieter eine (Muster-)Leistungsbeschreibung (Service-Level-Agreement) zur Verfügung, die konkrete Rechtsfolgen bei Nichterfüllung der zugesagten Verfügbarkeit oder Performanz vorsieht? (Ziffer 3.2)
- Räumt der Cloud-Anbieter dem Cloud-Nutzer die Möglichkeit ein, auf Aspekte, wie Speicherort, Einschaltung und Auswahl von Unterauftragnehmern usw. Einfluss zu nehmen? (Ziffern 3.2 und 3.4.2)
- Gewährt der Cloud-Anbieter dem Cloud-Nutzer auch die Ausübung seines Kontrollrechts vor Ort (gegebenenfalls mit Regelungen zur Kostentragung)? (Ziffern 3.3 und 3.4.2)
- Ist bei einem späteren Anbieterwechsel auch die Übertragbarkeit der Daten und Ergebnisse sichergestellt?



Anforderungen an die vertragliche Gestaltung (Ziffer 3.4)

Finden sich in den Vertragswerken zwischen Cloud-Anbieter und Cloud-Nutzer Regelungen zu den folgenden Punkten (Ziffer 3.4.2):

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Art der Daten und Kreis der Betroffenen,
- nach § 9 zu treffende technische und organisatorische Maßnahmen,
- Berichtigung, Löschung und Sperrung von Daten,
- nach Absatz 4 bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
  - wenn ja, Klärung und Dokumentation: Wo werden diese Leistungen erbracht?
- Innerhalb oder außerhalb der EU/des EWR?
- Kontrollrechte des Auftraggebers und entsprechende Duldungs- und Mitwirkungspflichten des Auftragnehmers,
  - Die Möglichkeit einer Vor-Ort-Kontrolle darf nicht vertraglich ausgeschlossen sein.
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
  - Ist geregelt, dass der Cloud-Anbieter Datenschutzpannen sofort an den Cloud-Nutzer zu melden hat?
  - Ist geregelt, dass und wie der Cloud-Anbieter den Cloud-Nutzer mit den erforderlichen Informationen unverzüglich versorgt, damit der Cloud-Nutzer seinen gesetzlichen Pflichten nachkommen kann?
- Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- Rückgabe überlassener Datenträger und die Löschung gespeicherter Daten nach Beendigung des Auftrags beim Auftragnehmer (vgl. zusätzlich Ziffer 7).
  - Ist geregelt, ob und wie der Cloud-Nutzer die Daten zurückerhält und/oder der Cloud-Anbieter die Daten löscht?
  - Ist geregelt, dass jedenfalls eine der vorgenannten Tätigkeiten bereits mit der normalen Vergütung abgegolten ist?
- Erfüllt die Vereinbarung über die Auftragsdatenverarbeitung die Anforderungen an die Schriftform? (Ziffer 3.4.1)

Überzeugung über die Einhaltung der vereinbarten Maßnahmen (Ziffer 3.3.2)

Habe ich Möglichkeiten, mich durch Vor-Ort-Kontrolle, ein Zertifikat eines Dritten oder andere Unterlagen von der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen zu überzeugen?

Cloud-Anbieter und Subunternehmer aus Drittstaaten (Ziffer 4)

Ist der Cloud-Nutzer in Deutschland ansässig und werden Daten von Betroffenen, die in Deutschland oder einem Land innerhalb der EU/des EWR ansässig sind, verarbeitet? Dann ist deutsches Datenschutzrecht anwendbar (Ziffer 4.1).

Die Datenübermittlung an Cloud-Anbieter und Subunternehmer mit Sitz in der EU oder im EWR unterliegt den gleichen Anforderungen wie eine Übermittlung an einen inländischen Anbieter. (Ziffer 4.2.1)

Die Zulässigkeit der Datenübermittlung an Cloud-Anbieter und Subunternehmer mit Sitz in einem Land außerhalb der EU oder des EWR ist im Rahmen einer zweistufigen Prüfung zu beurteilen (Ziffer 4.2.2).

Die erste Stufe der Zulässigkeitsprüfung: Kommt eine Rechtsgrundlage (Einwilligung der Betroffenen oder gesetzlicher Erlaubnistatbestand) für die Datenübermittlung in Betracht? (Ziffer 4.2.2.1)

Die zweite Stufe der Zulässigkeitsprüfung: Gewährleistet der Cloud-Anbieter ein angemessenes Datenschutzniveau? (Ziffer 4.2.2.2)

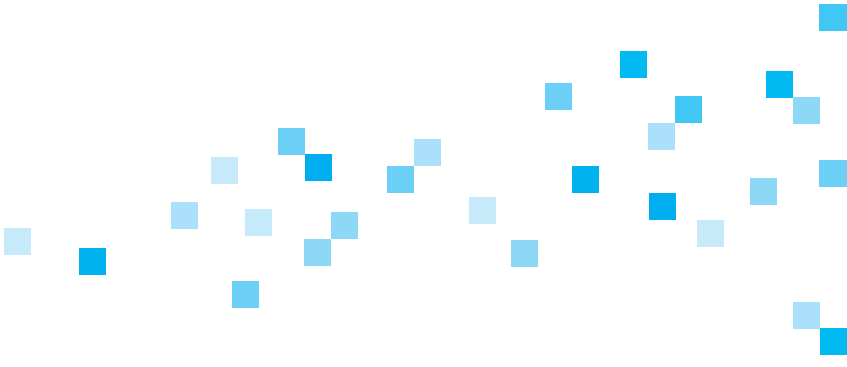
Möglichkeiten zur Sicherstellung des angemessenen Datenschutzniveaus (Ziffer 4.2.2.2):

- Das Sitzland des Cloud-Anbieters ist ein sicheres Drittland (Ziffer 4.2.2.2.1).
- Der US-amerikanische Cloud-Anbieter ist Safe-Harbor zertifiziert (Ziffer 4.2.2.2.2).
- Der Abschluss der EU-Standardvertragsklauseln (Ziffer 4.2.2.2.2).
- Der Cloud-Anbieter hat Processor Binding Corporate Rules implementiert (Ziffer 4.2.2.2.4).
- Es liegt eine gesetzliche Ausnahme im Sinne von § 4c Abs. 1 BDSG vor (Ziffer 4.2.2.2.5).
- Konstellationen im Zusammenhang mit dem Abschluss der EU-Standardvertragsklauseln (Ziffer 4.2.2.2.5.).

Die Beendigung des Auftragsverhältnisses (Ziffer 7)

Ist sichergestellt, dass die Auftragsdatenverarbeitung nicht endet, bevor alle Daten beim Cloud-Anbieter gelöscht und gegebenenfalls zusätzlich auf den Cloud-Nutzer rückübertragen sind?

Ist entweder die Löschung oder die Rückübertragung und die anschließende Löschung in der Vereinbarung über die Auftragsdatenverarbeitung eindeutig geregelt?



Autoren

Prof. Dr. Georg Borges, Kompetenzzentrum Trusted Cloud, Universität des Saarlandes
Mathias Cellarius, SAP SE
Dr. Jens Eckhardt, JUCONOMY Rechtsanwälte
Alexander Glaus, Deutsche Bank AG
Dr. Marc Hilber, Oppenhoff & Partner
Dr. Hubert Jäger, Uniscon universal identity control GmbH
Britta Hinzpeter, DLA Piper UK LLP
Johanna Hofmann, Universität Kassel
Rudi Kramer, DATEV eG
Thomas Kranig, Bayerisches Landesamt für Datenschutzaufsicht
Gunther Schiefer, Karlsruher Institut für Technologie (KIT)
Dr. Claus Dieter Ulmer, Deutsche Telekom AG

Impressum

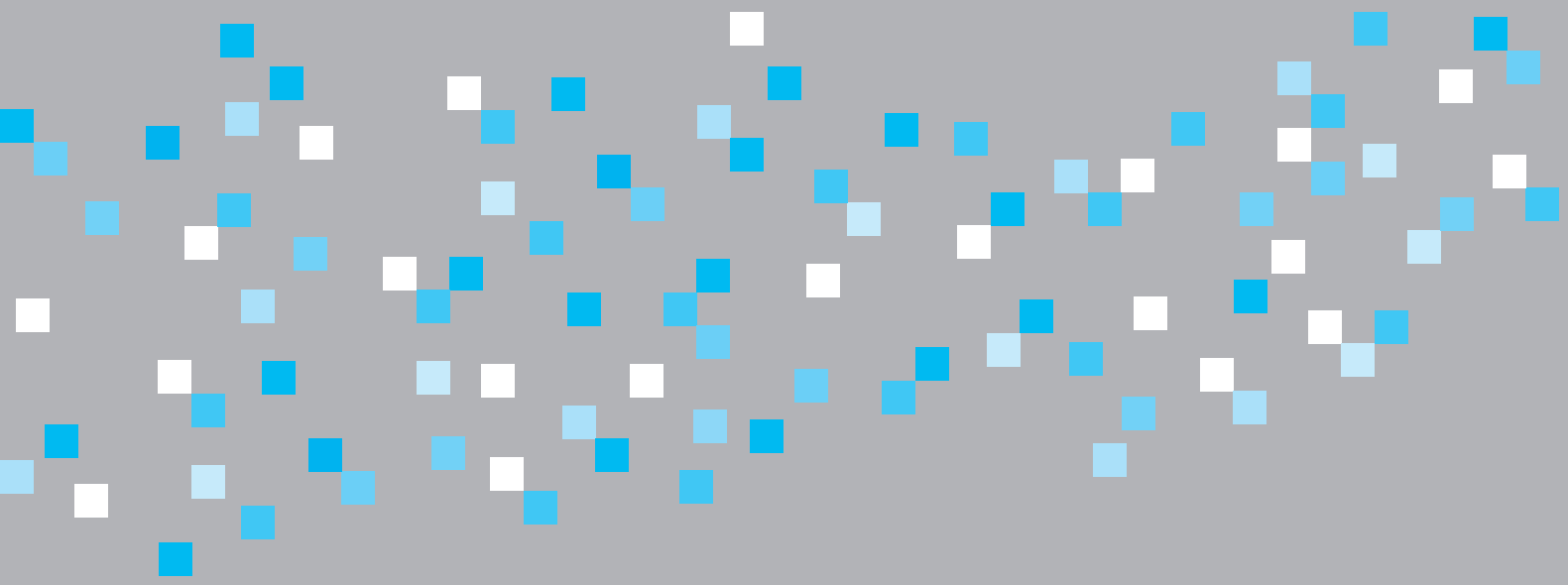
Herausgeber
Kompetenzzentrum Trusted Cloud
Arbeitsgruppe „Rechtsrahmen des Cloud Computing“
E-Mail: kompetenzzentrum@trusted-cloud.de
www.trusted-cloud.de

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi)

Gestaltung
A&B One Kommunikationsagentur, Berlin

Druck
DCM Druck Center Meckenheim

Stand: April 2015



www.trusted-cloud.de