Datenschutzkonforme Vertragsgestaltung im „Cloud Computing“

Elisabeth Opfermann*

Inhalt

* Der Beitrag beruht auf der gleichnamigen Master-Arbeit, die Elisabeth Opfermann LL.M. 2011 zum Abschluss Ihres Master-Studiums „Europäische Integration“ verfasst hatte. Im Februar 2012 wurde die Arbeit mit dem Europa-Preis der Villa Lessing ausgezeichnet. Ein besonderer Dank gilt Prof. Alfred Büllesbach, dem Betreuer der Master-Arbeit sowie Vilma Niclas, Rechtsanwältin in Berlin, für Inspiration und Kritik. Inzwischen arbeitet Elisabeth Opfermann bei der PwC AG in Frankfurt/Main.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

A. Einleitung

Cloud Computing, also IT-Service „aus der Steckdose" war in der Vergangenheit größeren Unternehmen vorbehalten. Doch in letzter Zeit werden zunehmend auch Verbraucher und Mittelständler auf das sogenannte „Rechnen in der Wolke" aufmerksam. Die Vorteile großer Serverkapazitäten und geringerer Kosten finden immer mehr Interessenten. Cloud Computing steht für Flexibilität je nach Bedarf. Immer häufiger werden Daten in die sogenannte „Wolke" hochgeladen, um sie später von

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

einem anderen Computer aus verwenden zu können. Das spart Zeit. Aktualisierungen von Softwareversionen entfallen ebenso wie die damit verbundenen Kompatibilitätsprobleme. Die Schattenseite: Niemand weiß genau, wo seine Daten liegen, wer darauf Zugriff hat und ob sie dort sicher sind.

Studien zufolge wird die Cloud bald in jedem größeren Unternehmen in Deutschland zur Anwendung kommen. Der deutsche Markt für Cloud-Dienstleistungen soll sich von 2011 bis 2015 verfünffachen.[1] Schon jetzt sind die Datenansammlungen im Internet unübersichtlich und unkontrollierbar geworden. Die Gefahr liegt in der zunehmenden und irreversiblen Transparenz von Daten aus allen Lebensbereichen.

Im Rahmen dieses Beitrags soll nach einer kurzen Definition des Cloud Computing erörtert werden, wo sich aus datenschutzrechtlicher Sicht Probleme befinden. Dazu gehören im Besonderen die Übertragung personenbezogener Daten an Dritte sowie die Auftragsdatenverarbeitung. Ein weiterer Schwerpunkt soll in der Beantwortung der Frage liegen, ob und wie Daten ins Ausland übermittelt werden können. Im Licht der europäischen Datenschutzreform soll jeweils kurz auf die besonders interessanten Änderungsvorschläge aus dem Entwurf der Datenschutz-Grundverordnung[2] eingegangen werden. Im Anschluss beschäftigt sich der Beitrag mit der Frage, wie Verträge im Cloud Computing so ausgestaltet werden können, dass der Schutz essenzieller Daten gewährleistet ist.

B. Cloud Computing – Definition

Viele chronisch Kranke bedürfen einer ständigen Überwachung. Eine kleine Arztpraxis stattet jeden dieser Patienten mit einem Netbook sowie den benötigten Messgeräten aus. Diese senden per Funk Daten an das Netbook, das seinerseits die Daten pseudonymisiert und über das Internet an eine zentrale Plattform schickt. Der Arzt kann auf diese Plattform zugreifen und die Befunde der Geräte auswerten sowie auf etwaige Verschlechterungen umgehend reagieren, ohne dass der Patient jeden Tag seine Praxis aufsuchen muss. Das erhöht die Lebensqualität des Patienten und steigert die Effektivität der Arztpraxis.[3]

Dieses Beispiel ist ein Anwendungsfall des Cloud Computing.

Zunächst soll eine Definition für diesen Begriff bestimmt und die technischen Aspekte durchleuchtet werden. Dieser Abschnitt wird keinesfalls abschließend und

1 BITKOM, Leitfaden Cloud Computing 2010, S. 23, Abb. 6.

2 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endg. v. 25.1.2012.

3 Das Beispiel wurde leicht abgewandelt aus BITKOM, Leitfaden Cloud Computing 2009, S. 58 ff. übernommen.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

umfassend alle technischen Möglichkeiten und Feinheiten des Cloud Computing erläutern. Vielmehr soll eine allgemeine Definition gefunden werden, die den rechtlichen Umgang mit der Thematik vereinfacht. Bisher hat sich weder in der technischen noch in der juristischen Literatur eine einheitliche Definition für Cloud Computing durchgesetzt.

I. Definition anhand von Delivery Models

Eine Möglichkeit, an die Thematik des Cloud Computing heranzugehen, ist die Betrachtung der verschiedenen Erscheinungsformen der Cloud-Dienste, den sogenannten *delivery models*.[4] Die Hauptform des Cloud Computing ist das sogenannte *Software as a Service* (SaaS). Hierbei wird dem Nutzer Software zur Verfügung gestellt, die nicht auf seinem eigenen Computer installiert wird, sondern sich nur auf den meist zahlreichen Servern des Cloud-Anbieters befindet. Dem Nutzer wird der Zugang meist durch einen Webbrowser ermöglicht. Beispiele dafür sind Web-Mail-Angebote oder auch Office-Anwendungen wie „Microsoft 365". Eine weitere Form von Cloud-Services ist *Platform as a Service* (PaaS). Sie stellt dem Nutzer eine Entwicklungsumgebung zur Verfügung, auf der dieser seine Ideen selbst umsetzen kann. Solche Dienste werden zum Beispiel durch die „App Engine" von Google erbracht. Die Bereitstellung von Infrastruktur wie beispielsweise reinem Datenspeicher heißt *Infrastructure as a Service* (IaaS). Dies beinhaltet die Ressourcen, die sowohl für PaaS als auch SaaS benötigt werden, wie Prozessorleistung oder Kommunikationsmöglichkeiten. Vorreiter im Feld des IaaS ist Amazon. Aufgrund der verschiedenen Service-Angebote könnte man Cloud Computing auch als *Anything as a Service* (XaaS) zusammenfassen. Gemeint ist damit, dass jede gewünschte Leistung innerhalb einer Cloud realisiert werden kann.

II. Definition anhand von Deployment Models

Cloud Computing kann neben den Services auch anhand seiner Bereitstellung, den sogenannten *deployment models*, typisiert werden.[5] Das einfachste Modell einer Cloud stellt eine sogenannte Private Cloud dar, auf die nur ein einziger Nutzer Zugriff hat. Es ist aber keinesfalls ausgeschlossen, dass auch ein fremder Server als Private Cloud

---

4 Siehe dazu *Heidrich/Wegener*, Sichere Datenwolken, Cloud Computing und Datenschutz, MMR 2010, S. 804; *Nägele/Jacobs*, Rechtsfragen des Cloud Computing, ZUM 2010, S. 282; *Niemann/Hennrich*, Kontrollen in den Wolken?, Auftragsdatenverarbeitung in Zeiten des Cloud Computings, CR 2010, S. 687; *Niemann/Paul*, Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings, K&R 2009, S. 445; *Schuster/Reichl*, Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?, Die eigentlichen Unterschiede zu Outsourcing, ASP & Co liegen im Datenschutz und der TK-Anbindung, CR 2010, S. 38 ff.; *Spies*, USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht, MMR 5/2009, S. XI.

5 Siehe dazu *Heidrich/Wegener*, (Fn. 4), S. 803 f.; *Niemann/Hennrich*, (Fn. 4), S. 687.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

fungieren kann, wenn der Anbieter die notwendige Sicherheit und Exklusivität bietet.[6] Merkmal einer Private Cloud ist, dass kein Fremder Zugriff auf dieselbe Cloud hat. Die Cloud unterliegt der vollen Kontrolle des jeweiligen Nutzers. Dieser Umstand macht eine Private Cloud jedoch teurer im Vergleich zu anderen Modellen, weil der Anbieter für einen einzelnen Kunden eine hohe Verfügbarkeit gewährleisten muss. Anderes ergibt sich im Fall einer sogenannten Public Cloud. Dort haben mehrere Nutzer Zugriff auf dieselben Serverkapazitäten. Dies gibt dem Anbieter eine größere Flexibilität als eine Private Cloud, weil er je nach Bedarf seine Ressourcen aufteilen kann. Diesen Vorteil kann der Anbieter an seine Kunden weitergeben, indem er geringere Preise fordert. Durch Abschirmung oder Vernetzung werden die einzelnen Softwarekomponenten auf dem Server nutzbar gemacht. So kann ein größeres Unternehmen mehrere Softwarestrukturen vernetzen und dadurch die Effektivität seiner Cloud-Nutzung erhöhen. Andererseits können von verschiedenen Parteien genutzte Strukturen voneinander abgeschirmt werden. Ein bekanntes Beispiel für eine Public Cloud ist „dropbox".[7] Hier wird jedem Nutzer eine gewisse Menge an Speicherplatz kostenlos zur Verfügung gestellt. Seine Inhalte kann der Nutzer mit anderen teilen und geteilte Inhalte beliebig verändern. Es steht außer Frage, dass die Gefahr eines unbefugten Zugriffs in einer Public Cloud größer ist, als wenn ausschließlich ein begrenzter Nutzerkreis auf eine Private Cloud zugreift. Wie der Name schon suggeriert, handelt es sich bei sogenannten Hybrid Clouds um Mischformen der oben beschriebenen Cloud-Modelle. So besteht für ein größeres Unternehmen die Möglichkeit, eigene Server zu nutzen (also eine Private Cloud) und im Falle eines Auftragshochs, externe Server dazu zu schalten (Public Cloud).[8]

III. Fazit

Allen Modellen und Services sind die Fortschritte in der Virtualisierung und die damit verbundene Trennung von Hard- und Software gemein.[9] Einem benutzerdefinierten System können je nach Bedarf Hardwareressourcen zugeordnet werden. Eine Hardwareplattform kann virtuell aufgeteilt oder mit anderen Plattformen zu einer einzigen virtuellen zusammengefasst werden.[10] Ressourcen werden verschiedenen Nutzern gleichzeitig zur Verfügung gestellt. Immer erfolgt die Datenverarbeitung zumindest teilweise auf externen Servern. Alle Dienste, ob nun Speicher, Kommunikation oder Entwicklerumgebung sind beliebig skalierbar und jederzeit verfügbar. Um dies zu garantieren, sind Server häufig über die ganze Welt verstreut, um nach dem „Follow the Sun"-Prinzip jeweils den Server mit der geringsten Auslastung

6 So auch *Niemann/Paul*, (Fn. 4), S. 445.

7 https://www.dropbox.com/ (12.6.2012).

8 *Niemann/Paul*, (Fn. 4), S. 445.

9 So auch *Nägele/Jacobs*, (Fn. 4), S. 281.

10 *Pohle/Ammann*, Über den Wolken... – Chancen und Risiken des Cloud Computing, CR 2009, S. 274.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

nutzen zu können.[11] Server in einer Zeitzone, in der Nacht ist, sind weniger ausgelastet und bieten sich daher für die Verarbeitung von Datenströmen einer Zeitzone an, in der gerade Tag ist. Der Zugang zu Cloud-Angeboten erfolgt meist über eine Breitbandverbindung. Diese wird in den meisten Fällen nicht vom Cloud-Anbieter bereitgestellt, weshalb der Cloud-Nutzer bei der Wahl des Cloud-Dienstes auch die Kapazitäten seiner Internet-Verbindung beachten muss.[12] Gleichzeitig steht die Hardware des Nutzers nicht mehr im Vordergrund, da keine Voraussetzungen für die Installation einer Software oder eine bestimmte Menge an Speicherplatz zur Verfügung stehen muss. Die Bezahlung stellt eine weitere Besonderheit des Cloud Computing dar. Der Nutzer bezahlt nach dem sogenannten „Pay per Use"-Prinzip, also nur den Service, den er nutzt, für den Zeitraum, in dem er ihn nutzt. Beim Cloud Computing werden also auf Anforderung eines Kunden Ressourcen und Services flexibel im benötigten Umfang über eine Breitbandverbindung zur Verfügung gestellt und nutzungsgenau abgerechnet.[13]

C. Datenschutzrechtliche Probleme

In der Praxis wird eine Cloud oft als Datenspeicher genutzt. Aber auch bei anderen Services, wie SaaS, werden sensible Daten verwendet und übertragen. In jedem Fall besteht die Frage, wie die Daten innerhalb der Cloud geschützt sind und wer darauf Zugriff nehmen kann. Schon im *Volkszählungsurteil*[14] hat das Bundesverfassungsgericht festgestellt, dass es im Zeitalter der elektronischen Datenverarbeitung keine belanglosen personenbezogenen Daten mehr gibt. Das Bundesverfassungsgericht hat in Folge dieser Feststellung das Grundrecht auf informationelle Selbstbestimmung entwickelt, das Teil des Allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ist. Durch die beinahe ungebremste Flut von personenbezogenen Daten im Zeitalter des Internet und rasanter Technologieentwicklungen läuft der Betroffene Gefahr, die Kontrolle über seine eigenen Daten zu verlieren. Das Grundrecht auf informationelle Selbstbestimmung soll genau davor schützen. Der Betroffene soll jederzeit Herr seiner Daten bleiben können und selbst bestimmen, was mit seinen Daten geschieht.

---

11 *Conrad/Hausen*, Datenschutzrechtliche Aspekte von Data Loss Prevention und Cloud Computing, in: Büchner/Briner (Hrsg.), DGRI-Jahrbuch 2009, Informationstechnik und Recht, 2010, S. 37 f.

12 So auch *Karger/Sarre*, Wird Cloud Computing zu neuen juristischen Herausforderungen führen?, in: Taeger/Wiebe (Hrsg.), Inside the Cloud – Neue Herausforderungen für das Informationsrecht, Tagungsband der DSRI Herbstakademie 2009, S. 429.

13 So auch *Fickert*, Entwicklungen des Cloud Computing im Überblick – aktuelle und künftige rechtliche Probleme, in: Taeger/Wiebe, (Fn. 12), S. 420.

14 BVerfGE 65, 1 (45) – *Volkszählung*.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Ein Datum kann im Zusammenhang mit anderen schon lang gespeicherten Daten bei der Erstellung eines Persönlichkeitsprofils den entscheidenden Baustein bilden. Unternehmen bezahlen dafür große Summen, um ihre Werbung und Produktentwicklung gezielter gestalten zu können. Auch in der Strafverfolgung ist die Speicherung von personenbezogenen Daten hilfreich. Die größte Gefahr liegt jedoch darin, dass immer mehr personenbezogene Daten zu unlauteren Zwecken bis hin zum Identitätsdiebstahl verwendet werden. Jede Verwendung fremder personenbezogener Daten greift in das Recht auf informationelle Selbstbestimmung des Einzelnen ein. Dieses Recht durchzusetzen ist Grund und Ziel des Datenschutzes. Durch die Zunahme von sozialen Netzwerken und nicht zuletzt Cloud Computing, geben immer mehr Personen unbedacht ihre Daten im Internet preis. Mit Blick auf diese Entwicklung stellt sich besonders im Rahmen des globalen Cloud Computing die Frage nach der ausreichenden Gewährleistung des Datenschutzes.

Die Unterscheidung nach Cloud-Modellen, wie Private oder Public Clouds, ist aus Sicht des Datenschutzes wichtig. Eine Private Cloud, die nur von dem Unternehmen genutzt wird, das die Cloud auch betreibt, stellt kein datenschutzrechtliches Problem dar, weil die Daten nicht an Außenstehende übermittelt werden. Anders ist dies schon bei internationalen Konzernen, bei denen die einzelnen Niederlassungen gemeinsam eine Private Cloud nutzen. Das deutsche Datenschutzrecht kennt durch § 3 Abs. 7 Bundesdatenschutzgesetz (BDSG) kein sogenanntes Konzernprivileg, sodass auch miteinander verbundene Unternehmen einander nicht ohne weiteres Daten übermitteln dürfen. Sie gelten alle selbst als eigene verantwortliche Stellen.

Public Clouds, die von mehreren voneinander unabhängigen Parteien genutzt werden und deren Server weltweit verteilt sind, stellen wohl das größte Problem in datenschutzrechtlicher Hinsicht dar. Dadurch, dass Daten über verschiedene Server und Systeme verteilt sind, werden die Kontrollierbarkeit von Datenflüssen und das Recht auf informationelle Selbstbestimmung eines Einzelnen gefährdet. Die Server sind nicht nur verschieden im Hinblick auf ihre Kapazität, Software und Organisation. Häufig befinden sie sich auch noch im Ausland. Dort herrscht möglicherweise ein anderes Verständnis von Datenschutz als in Deutschland und Europa. Cloud Computing funktioniert nur, wenn der Datenfluss intakt ist. Jedoch muss im Vorfeld geklärt werden, welche Art der Verwendung und Übertragung von Daten überhaupt erlaubt ist. Um die Flexibilität und Kostenattraktivität des Cloud Computing noch zu erhöhen, bieten Anbieter häufig Cloud-Dienste an, die auf den Angeboten anderer Anbieter aufbauen.[15] Diese sogenannten *Pools* erschweren den Datenschutz zusätzlich, weil schon bei Vertragsschluss geklärt werden muss, mit wie vielen Parteien ein Vertrag eingegangen wird und wie der Datenschutz geregelt werden muss.

15 *Conrad/Hausen*, (Fn. 11), S. 37.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

I. Anwendbares Recht

1. Territorialprinzip

Das europäische Datenschutzrecht funktioniert nach dem sogenannten Territorialprinzip. Das bedeutet, dass das Recht des Staates Anwendung findet, in dem die eigentliche Datenverarbeitung stattfindet. Das deutsche Datenschutzrecht beruht noch[16] auf der Europäischen Datenschutzrichtlinie (EU-DSRL).[17] Diese legt das Territorialprinzip in Art. 4 fest. § 1 Abs. 5 BDSG greift dies auf. Gleichzeitig enthält diese Bestimmung eine Ausnahme vom Territorialprinzip – das Sitzprinzip: Werden Daten auf deutschem Gebiet erhoben, der dafür Verantwortliche hat seinen Sitz aber in einem der Mitgliedstaaten der Europäischen Union bzw. des Europäischen Wirtschaftsraums, findet nicht das deutsche Recht Anwendung, sondern das des Sitzstaates. Dies soll die reibungslose Funktion des Europäischen Binnenmarktes garantieren.[18] Das BDSG ist also nicht anwendbar, wenn eine Stelle, die innerhalb der EU bzw. des EWR ihren Sitz hat, in Deutschland Daten erhebt. Es bleibt anwendbar, wenn ein ausländisches Unternehmen eine Niederlassung in Deutschland hat. Das BDSG ist auch dann immer anwendbar, wenn ein Unternehmen, das außerhalb der EU bzw. des EWR sitzt, Daten innerhalb Deutschlands erhebt, verarbeitet oder nutzt.[19] Nach dem Territorial- bzw. Sitzprinzip bestimmt sich, welche Stelle die für die Datenverarbeitung verantwortliche ist. Diese haftet im Falle von unzulässigen Datenübermittlungen gegenüber dem Betroffenen und muss sich durch die Datenschutzaufsichtsbehörden in die Verantwortung nehmen lassen.[20]

Dabei gehen sowohl das deutsche als auch das europäische Datenschutzrecht davon aus, dass jederzeit festgestellt werden kann, in welchem Staat und auf welchen Servern sich die Daten befinden. Dem ist aber in der Praxis des Cloud Computing nicht zwangsläufig so. Die Anbieter verschieben die Datensätze häufig, um stets eine optimale Auslastung ihrer Server zu gewährleisten. Es ist daher kaum feststellbar, wann sich welche Daten wo befinden und welches Recht gerade für die Datenverarbeitung gilt.[21] Und selbst wenn die eigentliche Feststellung, wo sich die Daten zum jeweiligen Zeitpunkt befinden, durchaus technisch möglich ist, erscheint es doch wenig praktikabel oder kundenfreundlich, wenn sich je nach Aufenthaltsort der Daten

16 Die Richtlinie soll durch die Datenschutz-Grundverordnung (derzeit im Entwurf) ersetzt werden (Art. 88 des Entwurfs der Datenschutz-Grundverordnung).

17 RL 95/46/EG des EP und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.1995, S. 31.

18 *Jotzo*, Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, S. 234 f.

19 *Erd*, Zehn Jahre Safe Harbor Abkommen – kein Grund zum Feiern, K&R 2010, S. 625.

20 *Bauer*, Herausforderung internationale Auftragsdatenverarbeitung, Datenschutz Praxis 5/2011, S. 14.

21 *Spies*, (Fn. 4), S. XI f.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

das anwendbare Recht ändern würde. *Nägele/Jacobs*[22] und *Jotzo*[23] schlagen daher vor, das Territorialprinzip aufzugeben und deutsches Datenschutzrecht nach dem sogenannten Adressatenprinzip dann anzuwenden, wenn sich Anbieter aus Drittstaaten mit ihren Leistungen an deutsche Nutzer richten. Das Adressatenprinzip greift auch der Entwurf der Datenschutz-Grundverordnung auf.[24] *Spies*[25] sieht in dieser Hinsicht ein Problem, weil sich die Anbieter häufig nicht an Nutzer, sondern an Unternehmen richten würden. Ebenso lehnt er die Anknüpfung des anwendbaren Rechts an den Niederlassungs- bzw. Serverstandort des Cloud-Anbieters ab. Er schlägt vor, die nationalen Datenschutzrechte eines Bürgers gelten zu lassen, ungeachtet des tatsächlichen Aufenthaltsortes seiner Daten. Damit laufe man jedoch wiederum Gefahr, dass verschiedene Datensätze auf ein und demselben Server unterschiedlich behandelt werden. Fest steht, dass das Territorialprinzip im Falle des Cloud Computing eher hinderlich ist und von daher eine Möglichkeit gefunden werden muss, um der ständig wechselnden Datenströme Herr zu werden.[26] Das Adressatenprinzip scheint hier eine praktikable Lösung zu sein.

Beim Cloud Computing taucht besonders oft die Frage nach der datenschutzgerechten Übermittlung von Daten an Dritte auf. Die Rechtfertigung dieser Übermittlung wird sich immer nach dem Datenschutzrecht des Staates, in dem der Übermittelnde sitzt, bestimmen. Für Datenübertragungen aus Deutschland findet daher das deutsche Datenschutzrecht Anwendung.[27] Im Folgenden wird daher vorrangig auf die deutschen Bestimmungen eingegangen.

2. Subsidiarität des Bundesdatenschutzgesetzes zu Telekommunikationsgesetz und Telemediengesetz

In Deutschland ist der Datenschutz in mehreren Gesetzen geregelt. Die speziellen Regelungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) gehen dabei gemäß § 1 Abs. 3 BDSG den allgemeinen Bestimmungen des BDSG und der EU-DSRL vor.[28] Daher muss zunächst die Anwendbarkeit des TKG und TMG geprüft werden.

---

22 *Nägele/Jacobs*, (Fn. 4), S. 290.

23 *Jotzo*, (Fn. 18), S. 237.

24 Erwägungsgründe 20-22 des Verordnungsentwurfs, (Fn. 2).

25 *Spies*, (Fn. 4), S. XII.

26 So auch *Niemann/Paul*, (Fn. 4), S. 449.

27 *Erd*, (Fn. 19), S. 625.

28 *Fetzer*, in: Arndt/Fetzer/Scherer (Hrsg.), TKG, 2008, Vorbemerkung §§ 91 ff. TKG, Rdnr. 10; *Holznagel/Ricke*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, § 11 TMG, Rdnr. 10 ff. (*e contrario*); *Jotzo*, (Fn. 18), S. 234; *Klesczewski*, in: Säcker (Hrsg.), Berliner Kommentar zum Telekommunikationsgesetz, 2009, § 91 TKG, Rdnr. 14; *Nägele/Jacobs*, (Fn. 4), S. 290.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Die datenschutzrechtlichen Vorschriften des TKG finden auf Dienste Anwendung, die ganz oder überwiegend der Übertragung von Signalen dienen.[29] Das Cloud Computing ist vordergründig kein Telekommunikationsdienst. Häufig wird der Zugriff über das Internet auf die Cloud-Dienste nicht einmal durch den Cloud-Anbieter gewährt. Vielmehr ist die Übertragung von Signalen – wenn überhaupt – nur eine Nebenleistung zu den Cloud-Services. Cloud Computing dient daher nicht ganz überwiegend der Signalübertragung, sondern bedient sich dieser nur, um die eigentlichen Dienste zu ermöglichen. Das TKG ist damit eindeutig nicht auf herkömmliche Cloud Computing-Dienste anwendbar.[30] Anders sieht der Fall aus, wenn der vordergründige Cloud-Dienst der Kommunikation an sich gilt. Übernimmt der Cloud-Anbieter dabei eine eigenständige Signalübertragung, ist das TKG anwendbar. Werden aber zum Beispiel nur interne Kommunikationsanlagen, also Software und Infrastruktur, für Büros aus der Cloud heraus angeboten, nicht jedoch die eigentliche Signalübertragung durchgeführt, ist das TKG nicht einschlägig.[31] Selbst im Falle einer Anwendbarkeit des TKG gelten die datenschutzrechtlichen Vorschriften des Gesetzes gemäß § 91 Abs. 1 Satz 1 TKG lediglich im Verhältnis zwischen Cloud-Anbieter und Cloud-Nutzer. Sobald personenbezogene Daten einer außenstehenden Person betroffen sind, wie zum Beispiel bei einer Auslagerung von Kundendatenbanken, ist das TKG ohnehin nicht mehr anwendbar.

Strittig ist die Anwendbarkeit des TMG auf Cloud-Services.[32] Das TMG findet gemäß der Legaldefinition aus § 1 Abs. 1 Satz 1 TMG auf alle Informations- und Kommunikationsdienste Anwendung. Fraglich ist daher, ob es sich bei Cloud-Services um solche Dienste handelt. Kommunikationsdienste im Sinne des TMG dienen überwiegend der Bereitstellung von Inhalten, nicht dem Zugang zu diesen wie bei der herkömmlichen Telekommunikation.[33] Sie stellen die erforderlichen Inhalte elektronisch zu Verfügung.[34] *Schuster/Reichl*[35] zufolge fehlt es dem Cloud Computing an einem kommunikativen Element. Damit wird die Anwendbarkeit des TMG abgelehnt. Im Vordergrund stehe beim Cloud Computing die Softwarenutzung als Leistung, nicht die Kommunikation. Diese Annahme ist richtig, sagt jedoch nichts über die Anwendbarkeit des TMG aus. Vielmehr werden Dienste, die ausdrücklich der Kommunikation dienen, sogar vom TMG ausgenommen, zum Beispiel *Voice over IP* (VoIP).[36] Sogenannte „reine" Kommunikationsdienste sind von der Anwendbarkeit des TMG ausgeschlossen, denn diese fallen ausschließlich unter

29 *Fetzer*, (Fn. 28), § 91 TKG, Rdnr. 3.

30 So auch *Heidrich/Wegener*, (Fn. 4), S. 805; *Grünwald/Döpkens*, Cloud Control?, Regulierung von Cloud Computing-Angeboten, MMR 2011, S. 288; *Schuster/Reichl*, (Fn. 4), S. 43.

31 *Grünwald/Döpkens*, (Fn. 30), S. 289.

32 So auch *Moos*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, 2010, Einführung TMG, Rdnr. 6.

33 *Munz*, in: Taeger/Gabel, (Fn. 32), Einführung TKG, Rdnr. 9.

34 *Holznagel/Ricke*, (Fn. 28), § 1 TMG, Rdnr. 4; *Moos*, (Fn. 32), Einführung TMG, Rdnr. 4.

35 *Schuster/Reichl*, (Fn. 4), S. 42; zustimmend *Nägele/Jacobs*, (Fn. 4), S. 290.

36 *Holznagel/Ricke*, (Fn. 28), § 1 TMG, Rdnr. 5.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

das TKG. Im Umkehrschluss fallen alle anderen Informations- und Kommunikationsdienste in den Anwendungsbereich des TMG,[37] solange sie online erbracht werden.[38] Insofern kann die Eigenheit des Cloud Computing, alle Abläufe virtuell über das Internet zu gestalten, auch als kommunikatives Element gewertet werden. Damit wäre die oben angesprochene Meinung widerlegt.

Das OLG Düsseldorf[39] erkannte kürzlich einem Hosting-Dienst die grundsätzliche Anwendbarkeit des § 10 TMG zu und bejahte damit indirekt die Anwendbarkeit des TMG auf Cloud-Anbieter. Der Fall beschäftigte sich mit einem klassischen Anwendungsfall des Cloud Computing,[40] nämlich, dass ein Anbieter Daten für einen Kunden speichert, und selbst keinen Einfluss darauf hat. In diesem Fall nehme § 10 TMG den Anbieter von der Haftung für die gespeicherten Inhalte aus, so das OLG Düsseldorf. Wichtig sei dabei, dass der Kunde selbst entscheidenden Einfluss auf die genutzten Kapazitäten ausüben kann. Die Anwendbarkeit des TMG auf Cloud-Dienste ist somit gegeben.[41] Insbesondere die Haftungserleichterungen aus §§ 7-10 TMG sollten auch Cloud-Anbietern zustehen.

Das TMG bezieht sich wie das TKG ausschließlich auf das Verhältnis zwischen Cloud-Anbieter und Kunden.[42] In den meisten Fällen des Cloud Computing werden aber auch fremde personenbezogene Daten in eine Cloud verlagert, zum Beispiel Personal- oder Kundendatenbanken. In diesem Fall scheidet eine Anwendbarkeit des TMG aus. Dann kommen die allgemeinen Bestimmungen des BDSG und der EU-DSRL zur Geltung.

Die vorherige Ausführung zeigt: Eine Anwendung des TKG entfällt in den allermeisten Fällen. Ansonsten ist es genauso wie das TMG nur in Fällen, die das direkte Verhältnis zwischen Cloud-Anbieter und Kunden betreffen, anwendbar. Meist finden das BDSG und die EU-DSRL Anwendung.

II. Personenbezogene Daten; Automatisierte Verarbeitung

In Deutschland schützt das BDSG in § 1 Abs. 2 den Umgang mit personenbezogenen Daten. Dies sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Artikel 2 lit. a EU-DSRL konkretisiert diese Aussage. Bestimmbar ist eine Person demnach, wenn

37 Bei Diensten die zu ca. 50 % inhaltliche Dienste erbringen und zu ca. 50 % der Signalübertragung dienen, finden sowohl TMG als auch TKG Anwendung, vgl. *Munz*, (Fn. 33), Einführung TKG, Rdnr. 9.

38 So auch *Holznagel/Ricke*, (Fn. 28), § 1 TMG, Rdnr. 11.

39 OLG Düsseldorf, Az. I-20 U 166-09, Urteil v. 27.4.2010, *Rapidshare*, MMR 2010, 484.

40 So auch *Schröder*, Anmerkung zu OLG Düsseldorf, U. v. 27.04.2010 – I-20 U 166/09 – (Rapidshare), MMR 2010, S. 486.

41 So auch *Heidrich/Wegener*, (Fn. 4), S. 805.

42 *Holznagel/Ricke*, (Fn. 28), § 11 TMG, Rdnr. 13.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

sie durch die Zuordnung spezifischer Daten direkt oder indirekt identifiziert werden kann. Entscheidend ist, dass die Daten ohne besonderen Aufwand einer Person zugeordnet werden können.[43] Im heutigen Internetzeitalter und der damit verbundenen Flut von Daten kann mit etwas größerem bzw. erheblichem Aufwand beinahe jedes Datum über kurz oder lang mit einer Person in Verbindung gebracht werden. Der Datenschutz soll jedoch die Diskriminierung aufgrund von preisgegebenen Schwächen und ähnlich verhindern. Daten, die nur mit erheblichem Aufwand einer einzelnen Person zugeordnet werden können, können wohl selten diskriminierend genutzt werden. So bestellen sehr viele Personen Bekleidung über das Internet. Rein theoretisch ist es möglich, herauszufinden, wer etwas Bestimmtes gekauft hat. Damit lassen sich zwar Werbeaktionen gezielter ausrichten oder Verkaufsstrukturen umstellen. Die Tatsache, dass jemand Sneaker statt Lederschuhen einkauft, hat aber wohl keine Bedeutung in Hinsicht auf eine Diskriminierung. Von daher ist eine Begrenzung der geschützten personenbezogenen Daten auf solche, die ohne großen Aufwand einer Person zugeordnet werden können, sinnvoll.[44] Sonst wäre beinahe jedes Datum als personenbezogen zu qualifizieren. Damit würde der Datenfluss ins Stocken geraten und der freie Datenverkehr innerhalb der EU gefährdet. Werden Daten anonymisiert bzw. verschlüsselt in die Cloud gegeben, entfällt trotzdem nicht die Anwendbarkeit des BDSG.[45]

Der Umgang mit Daten umfasst die Erhebung, Verarbeitung und Nutzung. Die Verarbeitung der personenbezogenen Daten muss zudem gemäß § 1 Abs. 2 Nr. 3 BDSG mithilfe von Datenverarbeitungsanlagen erfolgen. Da im Rahmen des Cloud Computing die Daten sowohl vor als auch nach der eigentlichen Übermittlung der Daten an den Cloud-Anbieter immer über technische Anlagen wie Server verarbeitet werden, ist dieses Kriterium für den Fall des Cloud Computing immer erfüllt. Es handelt sich demzufolge um eine automatisierte Datenverarbeitung im Sinne des BDSG.

III. Beteiligte

Im Rahmen des Cloud Computing sind häufig mehr Parteien als nur Cloud-Anbieter und Cloud-Nutzer beteiligt. So werden oft personenbezogene Daten Dritter übermittelt. Das BDSG nennt diese Personen in § 3 Abs. 1 die Betroffenen. Außerhalb des eigentlichen Übertragungsprozesses stehen die jeweiligen Aufsichtsbehörden des Landes, des Bundes oder der EU. Sie überwachen die Einhaltung des Datenschutzes und sind für Genehmigungen und Bußgeldverfahren zuständig.

Der Cloud-Nutzer wird in den meisten Fällen die für den Datenumgang verantwortliche Stelle sein. Das ist nach § 3 Abs. 7 BDSG diejenige, die eine datenschutz-

43 *Gola/Schomerus*, BDSG-Kommentar, 10. Aufl. 2010, § 3 BDSG, Rdnr. 3.

44 So auch *Härting*, Internetrecht, 4. Aufl. 2010, Rdnr. 39.

45 *Conrad/Hausen*, (Fn. 11), S. 40.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

rechtlich relevante Handlung selbst durchführt oder durch andere im Auftrag vornehmen lässt. Hervorzuheben ist, dass die Verantwortlichkeit gemäß Art. 2 lit. d Satz 1 EU-DSRL von der Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung herrührt. Es ist daher nicht notwendig, dass die Stelle die Datenverarbeitung tatsächlich selbst vornimmt. Entscheidend ist vielmehr, wer die Verfügungsmacht über die Daten besitzt.[46] Im Fall des Cloud Computing ist demnach der Cloud-Nutzer die verantwortliche Stelle, da er die Daten sowohl erhebt, als auch an den Cloud-Anbieter übermittelt sowie für eigene Zwecke nutzt.

IV. Übermittlung von personenbezogenen Daten an Dritte

Die Bekanntgabe personenbezogener Daten an Dritte, also eine Datenübermittlung, stellt eine Verarbeitung gemäß § 1 Abs. 4 Satz 2 Nr. 3 BDSG dar.[47] Eine Verarbeitung von personenbezogenen Daten ist jedoch durch § 4 Abs. 1 BDSG grundsätzlich verboten. Eine Ausnahme stellt die Verarbeitung personenbezogener Daten zu rein persönlichen oder familiären Zwecken dar. Werden also lediglich Familienfotos in die Cloud geladen, um sie anderen Verwandten zu zeigen, die als Einzige Zugriff darauf haben, greift das Verbot der Datenübertragung nach § 1 Abs. 2 Nr. 3 BDSG nicht. Da jedoch zu erwarten ist, dass die hauptsächliche Nutzung von Cloud-Diensten zu unternehmerischen Zwecken erfolgen wird, dürfte diese Ausnahme selten greifen.

1. Innerhalb Deutschlands

Grundsätzlich dürfen personenbezogene Daten nicht ohne weiteres an Dritte übermittelt werden. Dritter im Sinne des § 3 Abs. 8 Satz 2 BDSG ist jede Person oder Stelle außerhalb der Stelle, die personenbezogene Daten verwendet.[48] Dieses Verbot mit Erlaubnisvorbehalt bestimmt den Umgang mit personenbezogenen Daten. Eine Verarbeitung personenbezogener Daten und damit auch deren Übermittlung an einen Dritten darf nach § 4 Abs. 1 BDSG nur bei Vorliegen einer Rechtsvorschrift oder mit Einwilligung des Betroffenen, also desjenigen, auf den sich die Daten beziehen, erfolgen.

a) Informierte Einwilligung

Die erforderliche Einwilligung des Betroffenen trägt dessen Recht auf informationelle Selbstbestimmung Rechnung. Gemeint ist damit eine vorherige Einver-

46 *Jotzo*, (Fn. 18), S. 233.

47 So auch: *Busche*, Internationaler Datenverkehr und Bundesdatenschutzgesetz („BDSG"), in: Taeger/Wiebe, (Fn. 12), S. 63.

48 *Gola/Schomerus*, (Fn. 43), § 3 BDSG, Rdnr. 48 ff.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

ständniserklärung im Sinne des § 183 BGB.[49] Gemäß § 4a BDSG müssen dem Betroffenen der Zweck und der genaue Umfang der Datenübermittlung bekannt sein, bevor er seine Einwilligung gibt. Zudem muss die Einwilligung freiwillig erfolgen. So gibt ein Arbeitnehmer seine Einwilligung schon nicht mehr freiwillig ab, wenn er Konsequenzen für seine Arbeitsstelle zu befürchten hat, falls er die Einwilligung nicht erteilt.[50] Eine informierte Einwilligung setzt zudem Einsichtsfähigkeit des Betroffenen voraus. Damit ist nicht dessen Geschäftsfähigkeit gemeint, sondern seine Fähigkeit zu erkennen, welche Tragweite seine Entscheidung haben wird.[51] Die Einwilligung hat meist in Schriftform zu erfolgen und benötigt daher die persönliche Unterschrift des Betroffenen. Die Einwilligung erfolgt immer für die Zukunft. Eine nachträgliche Einwilligung ist nicht zulässig.[52] Zudem hat der Betroffene die Möglichkeit, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Dies gilt nicht, wenn die Einwilligung zur Erfüllung vertraglicher Pflichten notwendig ist oder an vertragliche Vereinbarungen geknüpft ist, die nicht einseitig widerrufen werden können.[53]

b) Auftragsdatenverarbeitung, § 11 BDSG

Die Auftragsdatenverarbeitung aus § 11 BDSG stellt eine Ausnahme vom generellen Verbot der Datenübermittlung an Dritte dar. Das BDSG bietet hier eine Erleichterung. Hat der Cloud-Anbieter keinen Einfluss auf die Daten, die ihm anvertraut werden, kann er sie also nicht zu eigenen Zwecken nutzen, verändern oder zusammenführen, dürfen die Daten an ihn auch ohne Einwilligung des Betroffenen übermittelt werden. Dafür muss der Cloud-Anbieter nicht nur seinen Sitz in Deutschland haben, sondern auch seine Server dort betreiben.[54] Das BDSG fingiert in diesem Fall Auftraggeber und Auftragnehmer zu einer juristischen Einheit, was dazu führt, dass der Auftragnehmer kein Dritter im Sinne des Gesetzes ist, § 3 Abs. 8 Satz 3 BDSG. Der Auftragnehmer wird aber auch nicht verantwortliche Stelle im Sinne des BDSG. Die Auftragsdatenverarbeitung stellt sich als Regelfall des Cloud Computing dar.[55] In der Praxis gestaltet sich die Auftragsdatenverarbeitung jedoch weitaus schwieriger.

Um auf das Privileg der Auftragsdatenverarbeitung zurückgreifen zu können, müssen sowohl Cloud-Nutzer als auch Cloud-Anbieter einige Anforderungen erfüllen. So

49 Ibid., § 4a BDSG, Rdnr. 2.

50 *Däubler*, in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 3. Aufl. 2010, § 4a BDSG, Rdnr. 20 f.

51 *Gola/Schomerus*, (Fn. 43), § 4a BDSG, Rdnr. 10.

52 Ibid., Rdnr. 15.

53 *Däubler*, (Fn. 50), § 4a BDSG, Rdnr. 38.

54 *Schuster/Reichl*, (Fn. 4), S. 41.

55 *Karger/Sarre*, (Fn. 12), S. 434; *Schulz/Rosenkranz*, Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen, ITRB 2009, S. 235.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

darf der Cloud-Anbieter nur Hilfsfunktionen für seinen Auftraggeber übernehmen und auch nur auf dessen Weisungen hin arbeiten.

Doch schon die Weisungen des Cloud-Nutzers können nur sehr beschränkt sein. Cloud Computing-Angebote beruhen auf standardisierten Verfahrensabläufen. Individuelle Wünsche des Cloud-Nutzers werden darin kaum berücksichtigt, höchstens im Gegenzug für erhöhte Entgelte. Der Cloud-Nutzer muss sich also schon in seinen Weisungen auf allgemeine Anforderungen beschränken, zum Beispiel auf technische Sicherheitsstandards. Der Umgang mit und die Löschung der Daten sollten ebenfalls von dieser Weisungsbefugnis erfasst sein.[56]

Grundsätzlich sind jedoch sämtliche zehn Voraussetzungen, die § 11 Abs. 2 BDSG katalogartig aufführt,[57] zu erfüllen. Das kann sich als schwierig erweisen.

§ 11 BDSG verlangt, dass der Cloud-Anbieter den Maßnahmen-Katalog der Anlage zu § 9 BDSG anwendet. Er muss dabei insbesondere Datenverlusten und unbefugten Zugriffen vorbeugen.[58] Die vorgesehenen Kontrollen durch den Cloud-Nutzer bedeuten jedoch, dass dieser genau über Art und Umfang, sowie Ort und Zeit der Datenverarbeitung Bescheid wissen sollte. Das ist im Cloud Computing oft gar nicht möglich, weil der Cloud-Anbieter seinen Service nur anbieten kann, wenn er die Daten frei von einem Server zum anderen verschieben kann.[59] Anderenfalls würde sich Cloud Computing für den Anbieter kaum rentieren.[60] Der Cloud-Nutzer als Auftraggeber wiederum müsste sicherstellen, dass alle beteiligten Rechenzentren Maßnahmen zur Zugangs- und Zugriffskontrolle durchführen. Das dürfte für den normalen Cloud-Nutzer fast unmöglich sein, da es den meisten Nutzern bereits an den Grundkenntnissen des Datenschutzes mangelt.[61] Eine Vor-Ort-Kontrolle der Rechenzentren bietet sich schon aus rein wirtschaftlichen Gründen selten an. Außerdem wäre eine Kontrolle jedes einzelnen Server-Standorts mit einem viel zu hohen Aufwand verbunden. *Niemann/Hennrich*[62] sowie der BITKOM[63] schlagen daher regelmäßige Prüfberichte des Cloud-Anbieters vor, um die Einhaltung der geforderten Maßnahmen zu protokollieren. Fragwürdig ist aber, ob eine schriftliche Stellungnahme des Cloud-Anbieters zu den getroffenen Maßnahmen ausreichend ist und als Kontrolle durch den Cloud-Nutzer angesehen werden kann. Vertrauenswürdiger

56 *Niemann/Hennrich*, (Fn. 4), S. 692.

57 Dazu im Einzelnen unter D.III.

58 Zur detaillierten vertraglichen Ausgestaltung der Auftragsdatenverarbeitung ISACA-Leitfaden, Auftragsdatenverarbeitung unter Berücksichtigung von Standards, 2011, S. 8-16.

59 *Pohle/Ammann*, (Fn. 10), S. 277.

60 So auch *Conrad/Hausen*, (Fn. 11), S. 38 f.

61 *Pohle/Ammann*, (Fn. 10), S. 278.

62 *Niemann/Hennrich*, (Fn. 4), S. 691.

63 BITKOM, Leitfaden Cloud Computing 2009, S. 52.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

erscheinen von daher regelmäßige Prüfberichte unabhängiger Instanzen.[64] Dies würde auch dem Cloud-Anbieter entgegenkommen. Sein Erfolg gründet größtenteils darauf, dass die genaue Funktionsweise seiner Infrastruktur und die exakten Datenverarbeitungsorte geheim bleiben. Könnte jeder seiner Kunden seine Rechenzentren inspizieren, wäre sein Geschäftsgeheimnis sehr bald öffentlich. Auch unter diesem Aspekt erscheinen externe Prüfer und Zertifikate als empfehlenswert.[65] Inwiefern sich dies in der Praxis entwickeln wird, bleibt abzuwarten.

Das BDSG verlangt außerdem eine Offenlegung aller beteiligten Sub-Unternehmer. Kurzfristige und flexible Absprachen zwischen Cloud-Anbietern und eventuellen Sub-Unternehmen sind damit nicht möglich. Doch die Flexibilität und Attraktivität des Cloud Computing beruht auch auf dem raschen Wechsel einzelner Sub-Unternehmer, je nach Bedarf des Kunden.[66] Weitere Sub-Unternehmer, also Sub-Sub-Unternehmer sieht das BDSG gar nicht vor.

Alle Anforderungen an Auftraggeber und -nehmer müssen bereits dann erfüllt werden, wenn der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Dies könnte mit technischen Hilfsmitteln wie Verschlüsselungsprogrammen gewährleistet werden.[67] Satz 3 der Anlage zu § 9 BDSG suggeriert ebenfalls die Nutzung von Verschlüsselungsverfahren, um den Zugang Unbefugter zu den Daten zu verhindern. Dabei ergeben sich jedoch häufig Schwierigkeiten bei der Übertragung oder der Verarbeitungsgeschwindigkeit. Verschlüsselte Dateien sind häufig größer als nicht verschlüsselte oder werden von Firewalls oder Virenprogrammen geblockt.

Der Auftrag selbst muss schriftlich erteilt werden und detaillierte Angaben zu Verarbeitungsprozessen, organisatorischen und technischen Maßnahmen sowie eventuellen Unterauftragsverhältnissen enthalten. Besonders in Public Clouds wird eine Auftragsdatenverarbeitung fast nicht möglich sein. In Public Clouds fehlt dem Cloud-Nutzer häufig die Möglichkeit, individuelle Regelungen durchzusetzen. Private Clouds dagegen können sehr gut im Rahmen der Auftragsdatenverarbeitung betrieben werden, weil der Cloud-Nutzer Mitspracherechte und bessere Gestaltungsmöglichkeiten hat.[68]

Die Anforderungen an die Auftragsdatenverarbeitung sind sehr umfangreich und kompliziert und stehen grundsätzlich der Idee des Cloud Computing, den Nutzer von den meisten Pflichten zu entlasten, entgegen. Zudem ist anzuzweifeln, ob der Cloud-Nutzer überhaupt „Herr seiner Daten" sein kann, wenn diese jederzeit über verschiedene Server verschoben und verteilt werden können und er nicht weiß, wo

64 So auch *Vander*, Auftragsdatenverarbeitung 2.0?, Neuregelungen der Datenschutznovelle II im Kontext von § 11 BDSG, K&R 2010, S. 295.

65 So auch *Niemann/Hennrich*, (Fn. 4), S. 690.

66 *Conrad/Hausen*, (Fn. 11), S. 37, 39.

67 *Schuster/Reichl*, (Fn. 4), S. 42.

68 *Niemann/Paul*, (Fn. 4), S. 449.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

sich seine Daten zum jeweiligen Zeitpunkt befinden. Um dieses Problem zu umgehen, schlägt *Reindl*[69] vor, dem Cloud-Nutzer in Form einer Online-Abfrage den jeweiligen Ort des Datenspeichers mitzuteilen. Diese Informationen müssten dem Cloud-Anbieter sowieso immer vorliegen.

So sehr sich eine Auftragsdatenverarbeitung auf den ersten Blick im Rahmen des Cloud Computing anbietet, so sehr stellt die konkrete Ausgestaltung des Auftragsverhältnisses die Vertragsparteien vor große Herausforderungen.

c) Funktionsübertragung, § 28 BDSG

Erhält der Cloud-Anbieter Zugriff auf die Daten bzw. kann er sie für eigene Zwecke nutzen, ist die Auftragsdatenverarbeitung nicht einschlägig. Man spricht dann von einer Funktionsübertragung.[70] Dabei werden dem Cloud-Anbieter die jeweiligen Daten vollumfänglich übermittelt. Er übernimmt damit auch die Zuständigkeit für die Daten und wird zur verantwortlichen Stelle im Sinne des BDSG. Folglich ist nach einer Funktionsübertragung der Empfänger der Daten zum Schutz der ihm übertragenen Daten verpflichtet.[71]

Wenn die vielschichtigen Anforderungen an die Auftragsdatenverarbeitung des § 11 BDSG nicht erfüllt werden und dennoch keine Funktionsübertragung vorliegt, handelt es sich um eine herkömmliche Übermittlung von Daten.[72] Sowohl dafür als auch für eine Funktionsübertragung muss eine datenschutzkonforme Übertragung personenbezogener Daten gewährleistet werden. Das heißt, ein gesetzlicher Rechtfertigungsgrund muss einschlägig sein. Dazu zählt die oben bereits besprochene Einwilligung.

In Betracht kommt aber auch die zulässige Datenübermittlung zu eigenen Zwecken nach §§ 28 ff. BDSG.[73] Nach § 27 BDSG ist § 28 BDSG auf jegliche automatisierte Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen anwendbar. Gemäß § 28 Abs. 1 Satz 1 BDSG kann eine Übermittlung personenbezogener Daten zu eigenen Geschäftszwecken zulässig sein, wenn dies zur Erfüllung eines Schuldverhältnisses zwischen der übermittelnden Stelle und dem Betroffenen erforderlich ist (Nr. 1); die berechtigten Interessen der übermittelnden Stelle gewahrt sind, ohne das schutzwürdige Interesse des Betroffenen zu verletzen (Nr. 2); oder die Daten ohnehin allgemein zugänglich sind und eine Übermittlung der Daten nicht dem schutzwürdigen Interesse des Betroffenen entgegensteht (Nr. 3). Die Übertragung von Datensätzen in die Cloud wird in den meisten Fällen als eigener Geschäftszweck

69 *Reindl*, Cloud Computing & Datenschutz, in: Taeger/Wiebe, (Fn. 12), S. 441.

70 *Gola/Schomerus*, (Fn. 43), § 11 BDSG, Rdnr. 9.

71 ISACA-Leitfaden, (Fn. 58), S. 4.

72 *Niemann/Hennrich*, (Fn. 4), S. 687.

73 So auch *Niemann/Paul*, (Fn. 4), S. 449.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

anzusehen sein. Gemeint ist damit, dass die Übertragung der Daten Mittel zum Zweck ist, also der Verfolgung wirtschaftlicher Interessen des Unternehmens dient. Dies wäre zum Beispiel dann erfüllt, wenn ein Unternehmen Datenbanken in die Cloud auslagert, um Kosten zu sparen. § 28 Abs. 1 BDSG wäre somit einschlägig. Selten wird die Übertragung von Daten in eine Cloud der Erfüllung von Schuldverhältnissen dienen, und ebenso wenig werden die zu übermittelnden Daten allgemein zugänglich sein. Als vorrangiger Rechtfertigungsgrund bleibt also das berechtigte Interesse der übermittelnden Stelle nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Dieses kann jedes von der Rechtsordnung gebilligte Interesse sein, also auch rein wirtschaftliche oder ideelle Ziele verfolgen.[74] Das Interesse des Cloud-Nutzers kann zum Beispiel in der Verringerung der Unternehmensausgaben, der erhöhten Flexibilität des Datenspeichers oder einer verbesserten Wettbewerbsfähigkeit liegen.[75] Die Datenübertragung muss aber auch erforderlich sein, um das jeweilige Ziel zu erreichen. Das heißt, dass die Übermittlung der jeweiligen Daten in dem Umfang erfolgen muss, der zum Erreichen des verfolgten Zweckes nötig ist. Führt ein milderes Mittel zum Ziel, ist eine Maßnahme nicht erforderlich. So fehlt die Erforderlichkeit zum Beispiel dann, wenn es auch ausreichen würde, anonymisierte oder pseudonymisierte Datensätze zu übermitteln.[76] Im Bereich des Cloud Computing wird aber wohl regelmäßig nur die Übertragung der vollständigen, personalisierten Daten zielführend sein. Das Kriterium der Erforderlichkeit ist daher meist gegeben. Dem berechtigten Interesse der verantwortlichen Stelle steht das schutzwürdige Interesse des Betroffenen am Schutz seiner Daten gegenüber. Hier muss eine Interessenabwägung stattfinden. Die Art und Weise, wie die Übermittlung der Daten den Betroffenen beeinflussen kann, muss nach den Regeln der Verhältnismäßigkeit gegen den Zweck der Datenübermittlung abgewogen werden.[77] Wird das schutzwürdige Interesse des Betroffenen durch die Datenübermittlung nicht beeinträchtigt, ist die Datenübermittlung nach § 28 Abs. 1 BDSG zulässig.[78] Dies wird im Cloud Computing regelmäßig dann der Fall sein, wenn der Cloud-Anbieter verlässlich auftritt, indem er zum Beispiel Zertifikate vorweist, und der Datenschutz vertraglich eindeutig geregelt wird. Diese Regelung muss dem Standard des in § 11 BDSG Verlangten entsprechen, um § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht zu einer Auffangnorm gescheiterter Auftragsdatenverarbeitungen zu machen und damit den Datenschutz zu gefährden.[79] Die zu übermittelnden Daten dürfen zudem nicht besonders sensibel sein. Als besondere Arten von personenbezogenen Daten definiert das BDSG in § 3 Abs. 9 Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder politische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit

74 *Gola/Schomerus*, (Fn. 43), § 28 BDSG, Rdnr. 24; *Niemann/Paul*, (Fn. 4), S. 449.

75 Ibid.

76 *Taeger*, in: Taeger/Gabel, (Fn. 32), § 28 BDSG, Rdnr. 59.

77 So auch *Härting*, (Fn. 44), Rdnr. 68.

78 *Taeger*, (Fn. 76), § 28 BDSG, Rdnr. 64.

79 *Conrad/Hausen*, (Fn. 11), S. 41; *Niemann/Hennrich*, (Fn. 4), S. 688.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

oder Sexualleben. Daneben wird davon ausgegangen, dass jedes personenbezogene Datum als sensibel eingestuft werden kann, wenn es sich aus dem Gesamtzusammenhang so ergibt.[80] Auch hier muss demnach eine Betrachtung des Einzelfalls erfolgen. Artikel 28 Abs. 1 Satz 2 BDSG verlangt zudem eine konkrete Zweckbindung. Die zu übermittelnden Daten dürfen zu keinem Zeitpunkt zu einem anderen Zweck übertragen werden, als zu dem im Vorfeld festgelegten.[81]

Es ist ratsam, zunächst alle gesetzlichen Rechtfertigungsgründe auf ihre Anwendbarkeit hin zu überprüfen, bevor man die Einwilligung des Betroffenen einholt. Dies hängt zum einen mit dem hohen Aufwand zusammen, den die Einholung einer Einwilligung bedeutet. Zum anderen ist eine Einwilligung widerruflich und eine Datenverarbeitung nach Widerruf der Einwilligung kann zu Vertrauensschäden zwischen dem Betroffenen und der verantwortlichen Stelle führen. Obwohl eine Datenverarbeitung ohne die Einwilligung trotzdem zulässig wäre, solange ein anderer gesetzlicher Rechtfertigungsgrund greift, wäre der ideelle Schaden doch beträchtlich.[82]

2. Innerhalb der EU bzw. des EWR

§ 4b Abs. 1 BDSG erlaubt die Übermittlung von personenbezogenen Daten in andere Mitgliedstaaten der EU sowie nach Norwegen, Island und Liechtenstein, den weiteren Mitgliedstaaten des EWR, zu denselben Voraussetzungen, die auch im deutschen Inland gelten.[83] Damit wird gemäß Art. 1 Abs. 2 EU-DSRL dem unbeschränkten Datenverkehr innerhalb der Union Rechnung getragen. Der freie Verkehr von Daten darf nicht aus Gründen des Datenschutzes beschränkt oder untersagt werden.[84] Auch die Fiktion der Auftragsdatenverarbeitung gilt EU- bzw. EWR-weit,[85] ist jedoch genau wie innerhalb Deutschlands nur selten wirklich für den Anwendungsfall des Cloud Computing geeignet.[86]

3. Außerhalb der EU bzw. des EWR

Die weltweite Verbreitung von Daten durch das Cloud Computing stellt den Datenschutz vor die größte Aufgabe. Häufig ist nicht bekannt, in welchem Land der Server des Cloud-Anbieters steht, auf dem die jeweiligen Daten gespeichert sind.[87] Die

80 *Gola/Schomerus*, (Fn. 43), § 3 BDSG, Rdnr. 56 f.

81 Ibid., § 28 BDSG, Rdnr. 35.

82 So auch *Taeger*, (Fn. 76), § 28 BDSG, Rdnr. 20.

83 Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Info 1, Bundesdatenschutzgesetz – Text und Erläuterung, 15. Aufl. 2011, S. 27.

84 So auch *Gola/Schomerus*, (Fn. 43), § 4b BDSG, Rdnr. 2.

85 *Busche*, (Fn. 47), S. 71, Fn. 33; *Reindl*, (Fn. 69), S. 444; *Schuster/Reichl*, (Fn. 4), S. 41.

86 So auch *Conrad/Hausen*, (Fn. 11), S. 40.

87 So auch *Pohle/Ammann*, (Fn. 10), S. 277.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

hohe Flexibilität der Angebote erfordert eine ständige Umverteilung der Daten auf weniger ausgelastete Server. Eine Übertragung von personenbezogenen Daten an Stellen im Ausland außerhalb der EU bzw. des EWR, also in Drittstaaten, ist jedoch nur gestattet, wenn kein besonderes schutzwürdiges Interesse des Betroffenen besteht. § 4b Abs. 2 Satz 2 BDSG unterstellt dieses Interesse am Schutz seiner personenbezogenen Daten und verbietet daher grundsätzlich deren Übermittlung außerhalb der EU bzw. des EWR.

Bezüglich der Auftragsdatenverarbeitung weicht das BDSG von der EU-DSRL ab, die in Art. 2 lit. f nicht zwischen Dritten im EU-Inland und -Ausland unterscheidet und damit auch eine Auftragsdatenverarbeitung im EU-Ausland zulässt.[88] Strittig ist, ob die deutsche Regelung des § 3 Abs. 8 Satz 2 BDSG damit gemeinschaftsrechtswidrig ist oder ob es sich dabei lediglich um eine rechtmäßige überschießende Richtlinienumsetzung handelt. Im ersten Fall müsste dann die Auftragsdatenverarbeitung auch auf Cloud-Anbieter in Drittstaaten Anwendung finden, ein angemessenes Datenschutzniveau vorausgesetzt.[89] Die Mehrheit der Literatur folgt jedoch dem deutschen Gesetzeswortlaut. Dem ist zuzustimmen. Ist eine Richtlinie nicht vollharmonisierend, haben die Mitgliedstaaten bei der Umsetzung also einen Spielraum, darf die Umsetzung vom Wortlaut der Richtlinie abweichen.[90] Dies gilt, solange bei der Umsetzung der wesentliche Regelungsgehalt und der von der Richtlinie verfolgte Harmonisierungsstandard trotzdem erreicht werden. Die EU-DSRL bietet den Mitgliedstaaten den erforderlichen Spielraum in Erwägungsgrund 9. Daraus ist zu schlussfolgern, dass die Richtlinie nicht vollharmonisierend wirken soll, sondern vielmehr der Grundgedanke des Schutzes personenbezogener Daten ohne Behinderung des innereuropäischen Datenverkehrs durchgesetzt werden soll. Der eingeschränkte Datenverkehr mit Drittstaaten behindert den innereuropäischen Datenverkehr nicht. Bei der deutschen Regelung handelt es sich daher um eine überschießende Richtlinienumsetzung, da der Mindeststandard der EU-DSRL eingehalten wird. Der Regelungsgehalt des BDSG verstärkt den Schutz der personenbezogenen Daten noch. Die Privilegierung der Auftragsdatenverarbeitung nach § 11 BDSG findet von daher keine Anwendung auf die Übermittlung von Daten aus Deutschland in Drittstaaten.[91] Erwägungsgrund 58 der EU-DSRL zählt zudem die möglichen Ausnahmen vom strikten Übermittlungsverbot aus Erwägungsgrund 57 auf. Die Auftragsdatenverarbeitung ist darin nicht zu finden. Folglich ist die untersagte Auftragsdatenverarbeitung des BDSG in Einklang mit der EU-DSRL. Die Diskrepanz zwischen dem Wortlaut des BDSG und der EU-DSRL wird durch sogenannte Standardver-

88 *Reindl*, (Fn. 69), S. 445.

89 *Giesen*, Datenverarbeitung im Auftrag in Drittstaaten – eine misslungene Gesetzgebung, Das deutsche Modell der Auftragsdatenverarbeitung im Konflikt mit den Vorgaben der EU-Datenschutzrichtlinie, CR 2007, S. 546.

90 So auch *Grunert*, Europarecht: Anforderungen an die Richtlinienumsetzung, 2008, S. 2.

91 *Gola/Schomerus*, (Fn. 43), § 4b BDSG, Rdnr. 5.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

tragsklauseln für Auftragsdatenverarbeiter[92] ausgeglichen, mit denen Auftragnehmer in Drittstaaten zu den Konditionen einer Auftragsdatenverarbeitung verpflichtet werden. Es herrscht Einigkeit, dass unter Verwendung der Standardvertragsklauseln für Auftragsdatenverarbeiter kein Anlass zur Annahme besteht, dass eine Übermittlung in Drittstaaten unzulässig wäre.[93] Streitfälle wie dieser würden mit der Datenschutz-Grundverordnung entfallen, da eine Verordnung gemäß Art. 288 AEUV anders als eine Richtlinie ohne Umsetzung in nationales Recht direkt in den Mitgliedsstaaten wirksam wird.

Fraglich ist, ob die datenschutzrechtlichen Regeln des TMG auch im internationalen Kontext zwischen Cloud-Anbieter und -Nutzer gelten. § 1 Abs. 5 TMG bestimmt, dass das Gesetz keine Anwendung auf das Internationale Privatrecht findet. Es entfaltet jedoch mittelbare Wirkung. Die Anwendbarkeit des BDSG im internationalen Kontext ergibt sich aus § 1 Abs. 5 Satz 2 BDSG. Die Datenschutzbestimmungen des TMG beruhen auf denselben Grundsätzen der EU-DSRL wie die des BDSG. Daraus ergibt sich die mittelbare internationale Anwendbarkeit des TMG.[94] Sie erfolgt nach den Regeln des § 1 Abs. 5 Satz 2 BDSG. Werden also Daten im Inland durch eine Stelle aus einem Drittstaat erhoben, so gilt das TMG im Verhältnis zwischen dem Anbieter und dem Nutzer. Meistens erhebt der Cloud-Anbieter die Daten jedoch nicht. Der Cloud-Nutzer hat die Daten bereits im Vorfeld erhoben und übermittelt die Daten an den Cloud-Anbieter. Das TMG ist daher zumeist nicht auf den Fall des Cloud Computing im internationalen Kontext anwendbar.

Die Datenübertragung in Drittstaaten muss genauso wie bei der Übermittlung innerhalb Deutschlands und der EU bzw. des EWR gerechtfertigt sein, zum Beispiel durch die Einwilligung des Betroffenen. Wie oben beschrieben, verlangt das BDSG eine informierte Einwilligung. Zu den zuvor bereits besprochenen Anforderungen an diese Einwilligung kommt die genaue Information des Betroffenen über das konkrete Risiko der Übermittlung seiner Daten in einen Drittstaat. Der Betroffene muss auch über den Empfänger und den Zielort der Daten informiert sein. Zudem können andere Rechtsvorschriften als Rechtfertigung für eine Datenübermittlung in Drittstaaten dienen. Hinzu kommt noch die Anforderung eines angemessenen Datenschutzniveaus im Drittstaat. Dieses kann auf verschiedene Arten gewährleistet werden.

a) Angemessenes Datenschutzniveau

Das schutzwürdige Interesse des Betroffenen bleibt dem § 4b Abs. 2 Satz 2 BDSG zufolge ausnahmsweise gewahrt, wenn bei der empfangenden Stelle ein ange-

92 Detaillierte Ausführungen zu den Standardvertragsklauseln finden sich unter C.IV.3.c).

93 *Gabel*, in: Taeger/Gabel, (Fn. 32), § 11 BDSG, Rdnr. 25 f.

94 *Jotzo*, (Fn. 18), S. 234.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

messenes Datenschutzniveau gewährleistet ist.[95] Hier weicht das BDSG erneut von der EU-DSRL ab, die ein angemessenes Datenschutzniveau im gesamten Drittstaat, nicht nur bei der jeweiligen Stelle, verlangt. Die Frage, ob dies in der Praxis wirklich zu Problemen führt, kann klar verneint werden. Während manche Teile der Literatur eine unzureichende Richtlinienumsetzung diskutieren, hat die Abweichung tatsächlich keinerlei Auswirkungen auf die Praxis. Zwar verlangt die EU-DSRL ein angemessenes Schutzniveau im Drittstaat. Gleichzeitig eröffnet sie aber auch die Möglichkeit, durch Standardvertragsklauseln[96] etc. eine einzelne Stelle auf das notwendige Datenschutzniveau zu heben. Insofern würde das EU-Recht sich selbst widersprechen, ließe es nur die Übermittlung in Drittstaaten mit angemessenem Schutzniveau zu. Die Abweichung des BDSG von der EU-DRSL ist in diesem Fall also zu vernachlässigen.

Ein angemessenes Datenschutzniveau muss nicht identisch mit dem deutschen sein. Vielmehr muss der Datenschutz im Drittland die Kernprinzipien der EU-DSRL beachten.[97] Ob dies der Fall ist, hat die übermittelnde Stelle zumeist eigenverantwortlich zu beurteilen. Diese Prüfung ist oft sehr umfangreich.[98] Dabei ist in den meisten Fällen eine Aufsichtsbehörde zu konsultieren. Bei der Beurteilung sind vor allem zwei Bedingungen genau zu beleuchten: Die Datenschutzvorschriften des Drittlandes und die Maßnahmen, mit denen diese wirksam durchgesetzt werden, z.B. Sanktionen.[99] § 4b Abs. 3 BDSG und Art. 25 Abs. 2 EU-DSRL stellen weitere Kriterien auf, nach denen sich die Angemessenheit des Datenschutzniveaus bestimmen lässt. Ausgegangen wird dabei von der möglichen Persönlichkeitsrechtsgefährdung. Je sensibler die übermittelten Daten sind; je umfangreicher der Zweck, für den sie gedacht sind, ist; je länger sie verarbeitet werden dürfen; je mehr Stellen die Daten durchlaufen, bis sie den Empfänger erreichen; und je weniger Durchsetzungsmaßnahmen das lokale Datenschutzrecht bietet – desto größer ist die Gefährdung der Interessen des Betroffenen. Dieser Katalog ist nicht abschließend. Vielmehr müssen alle Umstände der Datenübermittlung in die Abwägung einbezogen werden.[100]

In einigen Fällen hat die Europäische Kommission gemäß Art. 25 Abs. 6 EU-DSRL Stellungnahmen veröffentlicht, ob in dem jeweiligen Land aus europäischer Sicht ein angemessenes Datenschutzniveau vorliegt. Dazu gehören unter anderen Argentinien,

95 *Busche*, (Fn. 47), S. 64; *Gola/Schomerus*, (Fn. 43), § 4b BDSG, Rdnrn. 7 (*e contrario*) und 12.

96 Detaillierte Ausführungen zu den Standardvertragsklauseln finden sich unter C.IV.3.c).

97 *Gola/Schomerus*, (Fn. 43), § 4b BDSG, Rdnr. 12.

98 *Moos*, Die EU-Standardvertragsklauseln für Auftragsverarbeiter 2010 – Die wesentlichen Neuerungen und Kritikpunkte im Überblick, CR 2010, S. 281.

99 Artikel 29-Datenschutzgruppe, WP 12 v. 24.7.1998, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf (12.6.2012), S. 5.

100 *Erd*, (Fn. 19), S. 625; *Gola/Schomerus*, (Fn. 43), § 4b BDSG, Rdnr. 10 f.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Australien, Israel, Kanada und die Schweiz.[101] Im Falle der Übermittlung personenbezogener Daten in diese Länder, kann von einem angemessenen Datenschutzniveau ausgegangen werden. Eine eigene Beurteilung dieser Drittstaaten durch die verantwortliche Stelle ist sogar unzulässig.[102] In Hinblick auf die Auftragsdatenverarbeitung hat der deutsche Bundesrat im Rahmen des Gesetzgebungsverfahrens zum Beschäftigtendatenschutz erst kürzlich vorgeschlagen, die Privilegierung des § 11 BDSG auch auf solche Drittstaaten auszuweiten, denen die Kommission ein angemessenes Datenschutzniveau bescheinigt hat.[103] Diese Regelung wäre nur konsequent. Besteht in einem Drittstaat ein vergleichbares Datenschutzniveau, kann der grenzüberschreitende Datenverkehr in diesen Staat in allen Bereichen ausgeweitet werden.

b) Safe Harbor-Prinzipien

Die meisten großen Cloud-Anbieter sitzen in den USA.[104] Das Datenschutzniveau der Vereinigten Staaten ist jedoch nicht durch die Europäische Kommission anerkannt. Um den Handel zwischen der EU und den USA nicht einzuschränken, wurden die „Safe Harbor"-Prinzipien eingeführt. Unternehmen, die dieses Regelwerk anerkannt haben, sollen ein angemessenes Datenschutzniveau gewähren. An sie dürfen gemäß Art. 1 Abs. 1 der „Safe Harbor"-Entscheidung der Europäischen Kommission[105] auch personenbezogene Daten übermittelt werden. Dies gilt solange, bis das Unternehmen seine „Safe Harbor"-Erklärung zurückzieht. Das amerikanische Handelsministerium (*Department of Commerce*) verwaltet die Liste der „Safe Harbor"-Unternehmen. Die *Federal Trade Commission* übernimmt die Durchsetzung der „Safe Harbor"-Regeln. Auf eine Beschwerde hin kann die *Federal Trade Commission* Sanktionen gegen Unternehmen verhängen, die gegen die Datenschutzregeln verstoßen. Bei einem beständigen Verstoß kann ein Unternehmen auch vollständig ausgeschlossen werden. Der Verlust des „Safe Harbor"-Zertifikats würde für das Unternehmen auch den Verlust von gutem Ruf und Geschäftspartnern bedeuten. Die „Safe Harbor"-Prinzipien sind trotz allem nicht so umfassend wie das europäische Datenschutzrecht. Das Unternehmen darf zum Beispiel eigenständig entscheiden, welche Datensorten und Geschäftsbereiche es den „Safe Harbor"-Regeln unterziehen

---

101 Die vollständige Liste inklusive aller Entscheidungen der Europäischen Kommission, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm#countries (12.6.2011).

102 *Busche*, (Fn. 47), S. 64.

103 Bundesrat, Stellungnahme 535/10 (B) zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes v. 5.11.2010, S. 6.

104 So auch *Niemann/Hennrich*, (Fn. 4), S. 687.

105 Entscheidung 2000/520/EG der Kommission vom 26.7.2000 gemäß der RL 95/46/EG des EP und des Rates über die Angemessenheit des von den Grundsätzen des sicheren Hafens und der diesbezüglichen Häufig gestellten Fragen (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 v. 25.8.2000, S. 7; im Anhang dieser Entscheidung findet sich die gesamte „Safe Harbor"-Vereinbarung im deutschen Wortlaut.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

will.[106] Dies ist vor der Datenübertragung durch die übermittelnde Stelle genau zu prüfen.

Mit dem zehnjährigen Bestehen der „Safe Harbor"-Prinzipien häuft sich die Kritik an deren Durchsetzung des Datenschutzes. Der wohl wichtigste Kritikpunkt liegt in der Tatsache, dass sich die Unternehmen selbst zertifizieren. Sie veröffentlichen ihre Datenschutzbestimmungen, ohne dass eine unabhängige Agentur diese auf die Übereinstimmung mit den „Safe Harbor"-Regeln prüft. So kommt es, dass nur circa 350 der über 1.700 Unternehmen auf der Liste des *Department of Commerce* den „Safe Harbor"-Kriterien entsprechen. Noch viel weniger Unternehmen schützen alle personenbezogenen Daten.[107] Daraus lässt sich schließen, dass wohl die meisten der aus der EU in die USA übermittelten Daten dort rege verarbeitet und weitergegeben werden. Der Düsseldorfer Kreis, eine Versammlung der höchsten deutschen Datenschutzaufsichtsbehörden, empfiehlt in seinem Beschluss vom 29. April 2010, dass sich deutsche Unternehmen von der Einhaltung der Datenschutzregeln der „Safe Harbor"-Prinzipien überzeugen sollten, bevor sie Daten an Unternehmen in den USA übermitteln.[108] Zudem wird empfohlen, ein „Safe Harbor"-Zertifikat, das älter als sieben Jahre ist, nicht anzuerkennen.[109] Eine pauschale Diskriminierung von „Safe Harbor"-Unternehmen würde jedoch dem geltenden EU-Recht widersprechen. Ein Cloud-Anbieter aus einem Drittstaat muss prinzipiell genauso wie ein europäischer Anbieter behandelt werden, soweit die Einhaltung der „Safe Harbor"-Regeln nachgewiesen wurde.[110]

c) Vertragsklauseln und verbindliche Unternehmensregelungen, § 4c Abs. 2 BDSG

In Ländern ohne angemessenes Datenschutzniveau können Geschäftspartner nach § 4c Abs. 2 Satz 1 BDSG mithilfe von Vertragsklauseln, sogenannten *Data Transfer Agreements* zum Datenschutz verpflichtet werden. Dieses Vorgehen empfiehlt sich auch, wenn ein „Safe Harbor"-Unternehmen nicht die gewünschten Datenschutzregeln erfüllt.[111] Das Verfahren ist jedoch langwierig, weil die verwendeten Klauseln von den Datenschutzbehörden aller betroffenen Mitgliedstaaten gemäß § 4c Abs. 2 BDSG genehmigt werden müssen. Keine Behörde ist verpflichtet, die Genehmigung

106 *Busche*, (Fn. 47), S. 66.

107 Eine detaillierte Studie dazu liefert *Connolly*, The US Safe Harbor – Fact or Fiction?, 2008, S. 7.

108 Düsseldorfer Kreis, Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich v. 28./29.4.2010, S. 1.

109 *Erd*, (Fn. 19), S. 624.

110 *Niemann/Hennrich*, (Fn. 4), S. 688.

111 Düsseldorfer Kreis, (Fn. 108), S. 2.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

einer anderen anzuerkennen.[112] Zudem muss jede beteiligte Partei, zum Beispiel etwaige Sub-Unternehmer, in die Vertragsklauseln einbezogen werden.[113]

Um eine Erleichterung zu schaffen, hat die Europäische Kommission sogenannte Standardvertragsklauseln veröffentlicht. Ihr Einsatz schafft an sich noch kein angemessenes Datenschutzniveau beim Geschäftspartner im Drittland. Vielmehr werden ausreichende Garantien für den Schutz des Persönlichkeitsrechts im Sinne des § 4c Abs. 2 Satz 1 BDSG geschaffen. In diesem Fall muss dann kein angemessenes Datenschutzniveau gegeben sein. Die Standardvertragsklauseln sind zum wichtigsten Instrument der Vertragsgestaltung im internationalen Datenverkehr geworden.[114] Ihr Wortlaut darf weder abgeändert noch ergänzt werden. Der Geschäftspartner muss diesen Klauseln vollständig zustimmen, damit in diesem Verhältnis ein für die Daten gefahrloser Transfer gewährleistet ist. Eine Genehmigung durch die jeweiligen Datenschutzbehörden muss nicht erfolgen, es sei denn, die Klauseln wurden abgeändert.[115] Diese Standardvertragsklauseln gibt es bisher in drei Varianten: Die allgemeinen Standardvertragsklauseln[116] finden meist Anwendung, wenn der Empfänger der Daten diese in eigener Verantwortung weiterverwendet. Alternativ wurden die sogenannten ICC-Standardvertragsklauseln[117] durch die Internationale Handelskammer (*International Chamber of Commerce*, ICC) entwickelt. Diese sollen unternehmerfreundlicher sein, zum Beispiel durch erleichterte Haftungsregelungen. Sie sind jedoch nicht geeignet für die Übermittlung von Arbeitnehmerdaten.[118]

Zudem wurden 2001 erstmals spezielle Klauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter[119] in unsicheren Drittländern durch Auftraggeber innerhalb der EU bzw. des EWR verfasst. Sie bestimmen, dass die volle Verantwortung für die übertragenen Daten weiterhin beim Auftraggeber verbleibt. Diese Klauseln wurden 2010 abgeändert, um dem schnell zunehmenden Datenfluss

---

112 *Busche*, (Fn. 47), S. 69.

113 BITKOM, Leitfaden Cloud Computing 2009, S. 54.

114 *Moos*, (Fn. 98), S. 281; *Wybitul/Patzak*, Neue Anforderungen beim grenzüberschreitenden Datenverkehr, RDV 2011, S. 15.

115 *Gola/Schomerus*, (Fn. 43), § 4c BDSG, Rdnrn. 12 und 14.

116 Entscheidung 2001/497/EG der Kommission vom 15.6.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der RL 95/46/EG, ABl. L 181 v. 4.7.2011, S. 19.

117 Entscheidung 2004/915/EG der Kommission vom 27.12.2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer, ABl. L 385 v. 29.12.2004, S. 74.

118 So die Aufsichtsbehörden der AG „Internationaler Datenverkehr" im Positionspapier, www.datenschutz-berlin.de/attachments/459/PositionspapierApril2007.pdf?1208355040 (12.6.2012). S. 1.

119 Entscheidung 2002/16/EG der Kommission vom 27.1.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der RL 95/46/EG, ABl. L 6 v. 11.1.2001, S. 52.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

weltweit Rechnung zu tragen.[120] Seit Mai 2010 dürfen die alten Klauseln für Auftragsdatenverarbeiter nicht mehr verwendet werden.

Für internationale Konzerne bieten sich zur Gewährleistung des Datenschutzes, zum Beispiel in einer Private Cloud, innerhalb der Konzernstrukturen verbindliche Unternehmensregelungen, besser bekannt als sogenannte *Binding Corporate Rules* (BCR), an. Um die Übermittlung von personenbezogenen Daten an konzerninterne Stellen im Ausland ohne angemessenes Datenschutzniveau zu ermöglichen, kann sich der Konzern solche verbindlichen Unternehmensregeln auferlegen. Werden diese von den jeweiligen Aufsichtsbehörden gebilligt, gilt der Datenschutz als gewährleistet, auch wenn das Land, in dem die Konzernstelle sitzt, selbst kein angemessenes Datenschutzniveau bietet. Anders als bei den einfachen Vertragsklauseln, erkennen die meisten europäischen Datenschutzbehörden die Genehmigung von BCR einer anderen Behörde an. Jedoch existieren noch keine Muster-BCR. Die Unternehmen müssen ihre Regelungen immer noch selbst formulieren. Lediglich eine Checkliste der Artikel 29-Gruppe[121] gibt Anhaltspunkte. Diese Unsicherheiten sind ein Grund dafür, dass bisher nur wenige deutsche Konzerne BCR verwenden. Das Verfahren zur Genehmigung von BCR soll durch Art. 43 des Entwurfs der Datenschutz-Grundverordnung vereinfacht werden.

d) Weitere Ausnahmen nach § 4c Abs. 1 Satz 1 Nr. 2-6 BDSG, E-Discovery

Ist die Datenübermittlung zur Erfüllung vertraglicher Pflichten (Nr. 2 und 3), aus öffentlichem Interesse (Nr. 4) oder aufgrund lebenswichtiger Interessen des Betroffenen (Nr. 5) erforderlich, kann die Datenübermittlung in Drittstaaten trotz des Verbots erfolgen. Sind die Daten außerdem bereits öffentlich zugänglich (Nr. 6), ist kein besonderer Schutz mehr nötig. Diese Ausnahmen müssen sehr eng ausgelegt werden.

Besonders interessant ist der Ausnahmetatbestand aus § 4c Abs. 1 Nr. 4 BDSG, der unter anderen die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen als Rechtfertigungsgrund für eine Datenübermittlung in Drittsaaten nennt. Das Zivilprozessrecht der USA sieht vor, dass im Vorfeld der eigentlichen Gerichtsverhandlung mit Beweisaufnahme ein sogenanntes *pre-trial discovery* durchgeführt wird. Dabei können die Prozessparteien vom Gegner verlangen, eventuell relevante Beweisstücke vorzulegen. Handelt es sich dabei um E-Mails oder elektronische Dokumente, nennt man ein solches Verlangen *e-discovery request*.[122] Auch in

120 Beschluss 2010/87/EU der Kommission vom 5.2.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der RL 95/46/EG des EP und des Rates, ABl. L 39 v. 12.2.2010, S. 5.

121 Artikel 29-Datenschutzgruppe, Arbeitsdokument „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)", WP 154 v. 24.6.2008, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_de.pdf (12.6.2012).

122 *Busche*, (Fn. 47), S. 74.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Großbritannien wird dieses Verfahren angewandt, dort heißt es *disclosure*.[123] Wird ein deutsches Unternehmen mit einem solchen *e-discovery request* konfrontiert, kann es dieses häufig nur erfüllen, indem es fremde personenbezogene Daten – zum Beispiel von Kunden oder E-Mail-Adressaten – weitergibt. Das würde die Übermittlung personenbezogener Daten in einen Drittstaat ohne angemessenes Datenschutzniveau bedeuten, es sei denn, der Prozessgegner ist ein „Safe Harbor"-Unternehmen. Der Ausnahmetatbestand aus § 4c Abs. 1 Satz 1 Nr. 4 BDSG kann dahingehend ausgelegt werden, dass zu solchen Zwecken personenbezogene Daten immer übermittelt werden dürfen. Deutsche Datenschutzbehörden halten dem ein völkerrechtliches Übereinkommen entgegen. Aufgrund Art. 23 des Haager Übereinkommens über die Beweisaufnahme im Ausland in Zivil- und Handelssachen (HBÜ) erklärte Deutschland, dass es solche *pre-trial discoveries* nicht erfüllen wird. Die Art. 29-Datenschutzgruppe hat 2009 dies auch auf europäischer Ebene bestätigt. Sie hob hervor, dass die Interessen der von der Datenübermittlung betroffenen Personen beachtet werden müssten.[124] Radikal geht die US-amerikanische Rechtsprechung das Thema an. Ausländische Gesetze, die das US-Zivilprozessrecht hindern würden, seien schlichtweg nicht anwendbar. Es gelte dann immer das US-Recht.[125] Das Unternehmen, dem ein *e-discovery request* vorgelegt wird, steht damit vor einem Problem. Gibt es die geforderten Daten an den Prozessgegner weiter, läuft es Gefahr, eine Ordnungswidrigkeit nach § 43 BDSG zu begehen, weil es personenbezogene Daten in einen unsicheren Drittstaat übermittelt. Verweigert es die Übergabe der Daten, drohen Sanktionen seitens der US-Gerichte. Andere Ansichten gehen indes davon aus, dass *e-discovery* und deutscher Datenschutz sich nicht per se ausschließen. § 4c Abs. 1 Nr. 4 BDSG bietet eine Rechtfertigung der Datenübermittlung in unsichere Drittstaaten. Der Wortlaut des Artikels verlangt zwar nicht ausdrücklich nach einer Abwägung mit dem schutzwürdigen Interesse des Betroffenen. Jedoch muss die Übermittlung an sich erforderlich sein. Im Rahmen einer Erforderlichkeitsabwägung können neben Zweckbindung und Datensparsamkeit auch die Interessen des Betroffenen in Betracht kommen.[126] Unter diesen Gesichtspunkten ist eine Übermittlung personenbezogener Daten im Rahmen eines *e-discovery* auch ohne Sanktionsbedenken möglich.[127]

Interessant erscheint die Frage, wie personenbezogene Daten im Fall eines *e-discovery* behandelt werden, die sich physisch bereits auf Servern in den USA befinden. Dürfen die Dateien dann direkt von den Servern abgerufen werden? Eine Datenübermittlung in die USA hat ja bereits vorher stattgefunden. Wenn schon die Über-

123 *Brown/Rice*, Professional English in Use – Law, 2007, S. 16, 18.

124 Artikel 29-Datenschutzgruppe, (Fn. 121), S. 9 ff.

125 US District Court Utah, Urteil v. 21.10.2010, Case No. 2:08cv569, 2010 U.S. Dist. LEXIS 4566, MMR 2010, 276.

126 *Brisch/Laue*, E-Discovery und Datenschutz, RDV 2010, S. 7.

127 So auch *Spies/Schröder*, Anmerkung zu US District Court Utah, U. v. 21.01.2010 – 2:08cv569 – (Deutsches Datenschutzrecht blockiert nicht die US-Beweiserhebung (E-Discovery)), MMR 2010, S. 276.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

mittlung in die USA aufgrund eines *e-discovery* grundsätzlich möglich ist, sollten auch in dieser Hinsicht keine Probleme bestehen. Wichtig ist, dass der Cloud-Anbieter die Daten nicht von sich aus preisgibt, sondern den Nutzer im Vorfeld von dem *e-discovery request* unterrichtet und nur auf dessen Anweisung hin spezifische Daten weitergibt. Dies muss vertraglich abgesichert werden. Denn der Cloud-Nutzer sollte sich vor der Weitergabe der Daten von der Erforderlichkeit der Datenübermittlung überzeugen und nur die notwendigen Daten weitergeben lassen.

e) Patriot Act

Nach den Anschlägen auf das World Trade Center am 11. September 2001 wurde der *Patriot Act*[128] erlassen. Ihm zufolge dürfen US-Ermittlungsbehörden und -Geheimdienste auf die Datenbestände US-amerikanischer Unternehmen zugreifen, wenn ein Terrorverdacht besteht. Davon betroffen sind auch Server der Unternehmen, die gar nicht auf US-Territorium stehen. Die Tatsache, dass US-Behörden auf jeden Server eines US-Unternehmens, wie zum Beispiel auch Microsoft oder Google,[129] zugreifen können, hat viele deutsche Unternehmer skeptisch gegenüber Cloud-Diensten gemacht. Denn nicht nur sind US-Unternehmen verpflichtet, den Behörden die gewünschten Daten auszuhändigen. Sie können sogar dazu veranlasst werden, den Besitzern der Daten keinen Hinweis auf die Übermittlung zu geben (Section 215; 501 (d) des *Patriot Acts*).

Die US-Anbieter können den Zugriff durch die Behörden nicht unterbinden. Daraus ergeben sich für Cloud-Nutzer folgende Möglichkeiten: Sie können den möglichen Zugriff der Behörden akzeptieren und trotzdem Server von US-Anbietern nutzen. Genauso können sie US-Clouds ganz entsagen und ausschließlich europäische Anbieter nutzen. Oder sie können auf den Servern europäischer Anbieter die Services der US-Anbieter nutzen. In diesem Fall entfällt das Zugriffsrecht der US-Behörden, weil sich dieses nur auf die Server der Anbieter bezieht. Die letzte Möglichkeit setzt sich zunehmend durch, weil sie die ausgefeilten Dienste der US-Anbieter mit dem europäischen Datenschutz am besten verknüpft. Der *Patriot Act* ist also kein Grund, keine Cloud-Dienste zu nutzen. Einer Aussage von Microsoft zufolge fragen die US-Behörden bisher auch nur sehr wenige Daten ab.

Trotzdem hat die EU im Entwurf der Datenschutz-Grundverordnung in Art. 45 auf die Zugriffsansprüche der US-Behörden reagiert. Demzufolge soll ein Zugriff aus

128 H.R.3162 – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) v. 26.10.2001, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR: (12.6.2012).

129 So sowohl Microsoft am 28.6.2011, http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225 (12.6.2012); als auch Google am 11.8.2011, http://www.zdnet.com/blog/igeneration/google-admits-patriot-act-requests-handed-over-european-data-to-us-authorities/12191 (12.6.2012).

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Drittstaaten auf Daten europäischer Bürger nur noch mit Zustimmung der zuständigen Datenschutzbehörden zulässig sein.

f) Fazit

Die Datenübermittlung in Drittstaaten ist strenger reguliert, weil außerhalb der EU häufig ein anderes Verständnis von Datenschutz besteht. Um den Handel nicht massiv einzuschränken, wurden zahlreiche Lösungen gefunden, die die Gewährleistung des Datenschutzes sicherstellen sollen. Während das Vertrauen in die „Safe Harbor“-Prinzipien stark nachlässt, werden Standardvertragsklauseln im täglichen Geschäftsverkehr immer wichtiger. Die Diskussion um den *Patriot Act* unterstreicht die Notwendigkeit einer präzisen Vertragsgestaltung bereits vor der Nutzung von Cloud Computing.

Die Zunahme der Vertragsgestaltung im internationalen Datentransfer bedeutet für jeden, der zukünftig Cloud-Dienste nutzen will, dass er sich insbesondere über vertragliche Bestimmungen informieren muss, um den Schutz der betroffenen personenbezogenen Daten zu gewährleisten. Hier gilt schlicht: Vertrauen ist gut, Kontrolle ist besser.

D. Vertragliche Gewährleistung der Datensicherheit und des Datenschutzes

Die bisherige Darstellung hat gezeigt, dass eine sichere Nutzung von Cloud-Angeboten nicht nur von deren technischer Ausgestaltung abhängt. Vielmehr ist eine erfolgreiche Nutzung von Cloud-Diensten nur durch umfangreiche und detaillierte Vertragsgestaltung möglich.[130]

In diesem Beitrag soll allein auf Verträge zwischen Nutzern und Cloud-Anbietern eingegangen werden. Mögliche Vertragsgestaltungen unter Anbietern, zum Beispiel über Drittprodukte, sollen keine Rolle spielen. Es bietet sich an, Cloud-Services möglichst „aus einer Hand“ zu beziehen. Einheitliche Verträge mit nur einer Partei erleichtern die Vertragsgestaltung und die eventuelle Rechtsdurchsetzung bei Schlechtleistung. Kleine Cloud-Anbieter mieten oft Server größerer Anbieter an. In diesem Fall muss sich der Nutzer auch vertraglich gegenüber eventuellen Sub-Anbietern absichern.[131] Die Verteilung der Vertragsleistungen auf mehrere Anbieter verringert

130 So auch *Karger/Sarre*, (Fn. 12), S. 427; *Nägele/Jacobs*, (Fn. 4), S. 290, 284; *Schulz*, Rechtliche Aspekte des Cloud Computing im Überblick, in: Taeger/Wiebe, (Fn. 12), S. 403.

131 *Karger/Sarre*, (Fn. 12), S. 433.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

zwar einerseits die Abhängigkeit des Cloud-Nutzers vom Anbieter, erhöht jedoch gleichzeitig das Risiko mangelnder Kongruenz.[132]

Cloud-Verträge können ganz unterschiedliche Inhalte haben. Kostenlose, alltägliche Angebote wie zum Beispiel Webmail-Services erfordern einen anderen Regelungsgehalt als die Auslagerung zentraler Unternehmensprozesse. Je komplexer der in die Cloud ausgelagerte Prozess ist, desto umfangreicher muss auch die vertragliche Ausgestaltung der Interessen- und Risikoverteilung sein.

I. Anwendbares Recht

Da derzeit kein globales oder europäisches IT-Vertragsrecht existiert, wird selbst bei internationalen Cloud-Verträgen immer nationales bzw. europäisches allgemeines Vertragsrecht zur Anwendung kommen.[133] Nach Art. 3 Abs. 1 Satz 1 ROM I-Verordnung[134] dürfen die Vertragsparteien dabei im Zuge der Privatautonomie grundsätzlich das auf den Vertrag anwendbare Recht selbst bestimmen. Dies wird vor allem bei individuellen Verträgen der Fall sein. Je standardisierter die Verträge, desto mehr wird sich der Kunde nach den Bedingungen des Cloud-Anbieters richten müssen. Die freie Rechtswahl in Vertragswerken wird gemäß § 3 Abs. 3 Nr. 1 TMG auch nicht durch das Herkunftslandprinzip beeinträchtigt, wonach deutsche Diensteanbieter und ihre Telemedien immer deutschem Recht unterstehen, auch wenn sie ihre Dienste außerhalb der EU bzw. des EWR erbringen. Wenn kein anwendbares Recht von vornherein vereinbart wurde, gilt nach Art. 4 Abs. 1 ROM I-Verordnung das Recht, das den engsten Bezug zum Vertrag hat. Dies wird regelmäßig das Recht des Sitzstaates des Cloud-Anbieters sein, da dieser die Leistung erbringt, die den Vertrag definiert.[135] Viele Cloud-Anbieter treten nur virtuell auf. In diesem Fall wird es für die Bestimmung des anwendbaren Rechts entscheidend sein, festzustellen, in welchem Land die Datenverarbeitung stattfindet. Für Verbraucher gilt nach Art. 6 Abs. 1 und 2 ROM I-Verordnung grundsätzlich das Recht ihres gewöhnlichen Aufenthaltsstaates. Wurde ein abweichendes anwendbares Recht im Vertrag vereinbart, muss im Fall einer gerichtlichen Auseinandersetzung ein sogenannter Günstigkeitsvergleich zwischen dem vereinbarten Recht und dem Recht des Staates, in dem der Verbraucher seinen Aufenthalt hat durch das Gericht durchgeführt werden. Dem Verbraucher soll so der gewohnte Rechtsschutz seines Staates gewährleistet werden. Das im Vertrag vereinbarte Recht findet nur Anwendung, wenn es für den Verbraucher günstiger ist als das seines Aufenthaltsstaates. Fraglich ist jedoch, ob diese Regelung auch auf internationale Cloud-Verträge Anwendung findet. Artikel 6 Abs. 1 und 2 sind näm-

132 *Niemann/Paul*, (Fn. 4), S. 446.

133 So auch ibid.

134 VO (EG) Nr. 593/2008 des EP und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I), ABl. L 177 v. 4.7.2008, S. 6.

135 So auch *Martiny*, in: Rixecker/Säcker (Hrsg.), MüKo BGB, 5. Aufl. 2010, Art. 4 ROM I-VO, Rdnr. 232; *Niemann/Paul*, (Fn. 4), S. 446.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

lich nach Art. 6 Abs. 4 lit. a ROM I-Verordnung nicht anwendbar, wenn die geschuldeten Leistungen ausschließlich in einem anderen Land als dem des gewöhnlichen Aufenthalts des Verbrauchers erbracht werden. Jedoch gilt dies nicht für Internetleistungen. Diese berühren das Aufenthaltsland des Verbrauchers, weil dieser die Leistung regelmäßig dort abruft.[136] Folglich werden Cloud-Leistungen nicht ausschließlich außerhalb des Aufenthaltslandes des Verbrauchers erbracht und die Ausnahme aus Art. 6 Abs. 3 Nr. 1 ROM I-Verordnung greift nicht.

Im Falle einer deliktischen Schädigung, zum Beispiel einer Löschung oder Veränderung der Daten durch eingeschleuste Schadsoftware, kommen Ansprüche aus unerlaubter Handlung in Frage. Diese ergeben sich gemäß Art. 4 Abs. 1 ROM II-Verordnung[137] aus dem Recht des Staates, in dem der Schaden eingetreten ist. Dieses sogenannte Erfolgsortrecht wurde bisher im Fall des Internet so ausgelegt, dass der Erfolgsort der des Zielcomputers war. Durch einen Angriff auf die Daten innerhalb einer Cloud kommt jedoch nicht unbedingt der Server der Datenverarbeitung zu Schaden, sondern die Daten selbst. Es ist also nicht auf den Erfolgsort im allgemeinen Sinne abzustellen, sondern vielmehr auf den Lageort der Daten.[138] Im Falle des Cloud Computing erfolgt die Datenverarbeitung jedoch nicht unbedingt auf einem konkreten Server, sondern auf mehreren gleichzeitig. Die Datensätze werden je nach verfügbarem Speicherplatz aufgespalten, so dass die Daten eines einzelnen Cloud-Nutzers über mehrere Server verteilt sein können. Welche Server das genau sind und in welchem Staat sie sich befinden, ist für den Cloud-Nutzer selten feststellbar. Die Betrachtung des Lageorts führt in diesem Fall dazu, dass alle Rechtsordnungen der jeweils betroffenen Server-Standorte zur Anwendung kommen. Dies folgt aus der sogenannten Mosaikbetrachtung.[139] Dementsprechend müssten die eingetretenen Schäden einzeln mit Blick auf die jeweilige Rechtsordnung beurteilt werden. Das kann in der Praxis zu enormen Problemen führen. Der Cloud-Nutzer hat zu beweisen, wo sich seine Daten zum Zeitpunkt des Schadens befanden, was sich insbesondere dann als schwierig erweisen wird, wenn zwischen der Beschädigung der Daten und ihrer Entdeckung Zeit vergangen ist und die Daten eventuell schon auf einem neuen Server liegen. Technisch ist der Beweis des Lageorts der Daten zwar möglich, jedoch sehr aufwändig zu erbringen. Aus diesem Grund wird von *Nordmeier*[140] vorgeschlagen, anhand Art. 4 Abs. 3 ROM II-Verordnung auf den Vertrag

136 So auch *Martiny*, (Fn. 135), Art. 6 ROM I-VO, Rdnr. 18; *Niemann/Paul*, (Fn. 4), S. 446; *Nordmeier*, Cloud Computing und Internationales Privatrecht, Anwendbares Recht bei der Schädigung von in Datenwolken gespeicherten Daten, MMR 2010, S. 153.

137 VO (EG) Nr. 864/2007 des EP und des Rates vom 11.7.2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht (Rom II), ABl. L 199 v. 31.7.2007, S. 40.

138 *Nordmeier*, (Fn. 136), S. 154.

139 Vgl. *Junker*, in: MüKo BGB, (Fn. 135), Art. 4 ROM II-VO, Rdnr. 31; *Schulz/Rosenkranz*, (Fn. 55), S. 236.

140 *Nordmeier*, (Fn. 136), S. 156.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

zwischen Cloud-Nutzer und -Anbieter abzustellen. Damit wäre die Rechtsordnung, aus der das anwendbare Recht auf den Vertrag stammt, auch die, nach der sich die deliktische Haftung bestimmt. Die Rechtssicherheit und damit auch die Vorhersehbarkeit einer Gerichtsentscheidung würden so verbessert. Unternehmer untereinander können und sollten aufgrund der bisher bestehenden Unsicherheiten in Hinblick auf die deliktische Haftung nach Art. 14 Abs. 1 lit. b ROM II-Verordnung im Vertrag vorab eine Rechtswahl treffen, nach welchem Recht sich deliktische Ansprüche richten sollen. Sitzen beide Parteien im selben Staat, findet gemäß Art. 4 Abs. 2 ROM II-Verordnung immer dessen Recht Anwendung.

II. Vertragstypologie

Zunächst muss geklärt werden, welches Vertragsmodell einem Cloud Computing-Vertrag zugrunde liegen kann. Daraus ergibt sich die jeweilige Mängelgewährleistung. Außerdem können so eventuelle Lücken im Vertrag durch Auslegung gefüllt werden.[141] Im Fall von Massengeschäften spielt der Vertragstypus auch bei der Inhaltskontrolle von Allgemeinen Geschäftsbedingungen (AGB) eine Rolle. Auch dort wird meist ein Vertragsmodell zugrunde gelegt.[142]

Häufig handelt es sich bei Cloud Computing-Verträgen um typengemischte Verträge, je nachdem, welche und wie viele verschiedene Services vereinbart werden. Je nach Einzelfall kann sich die Gewichtung zum einen oder anderen Vertragstyp verschieben.[143]

Wird lediglich Software für eine bestimmte Zeit gegen Zahlung eines Preises zur Verfügung gestellt, handelt es sich nach Auffassung des Bundesgerichtshofs um ein Mietverhältnis nach §§ 535 ff. BGB.[144] Begründet wurde dies mit der körperlichen Verbundenheit der Software mit einem Datenträger, womit erfüllt wird, dass bei der Miete Zugang zu einer körperlichen Struktur verschafft wird. Gleiches gilt auch, wenn Hardwareressourcen gegen Entgelt zur Verfügung gestellt werden.[145] Eine physische Besitzverschaffung ist dabei nicht vonnöten. Es genügt die Verschaffung von Nutzungsmöglichkeiten. Mietvertragliche Strukturen sind damit der Regelfall im Cloud Computing.[146] Die allgemeine Pflege der Hard- bzw. Software fällt unter die mietvertraglichen Pflichten des Cloud-Anbieters.

Anders sieht es aus, wenn der Cloud-Anbieter darüber hinaus Aufgaben übernimmt, wie zum Beispiel besondere Softwareupdates oder individuelle Anpassungen für den

141 *Schulz*, (Fn. 130), S. 406.

142 *Schulz/Rosenkranz*, (Fn. 55), S. 233.

143 *Nägele/Jacobs*, (Fn. 4), S. 284.

144 BGH, Az. XII ZR 120/04, Urteil v. 15.11.2006, Rdnr. 11 ff.

145 *Pohle/Ammann*, (Fn. 10), S. 275.

146 Ibid., S. 274 f.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Nutzer. Dann kommen werkvertragliche Aspekte gemäß §§ 631 ff. BGB in Betracht.[147] Vereinbarungen zu Schulungen durch den Cloud-Anbieter für die Mitarbeiter des Kunden stellen beispielsweise klassische Dienstverträge nach §§ 611 ff. BGB dar. Da häufig neben der Soft- bzw. Hardwarebereitstellung weitere Dienstleistungen stattfinden, werden die meisten Cloud Computing-Verträge Mischformen aus Miet- und Werk- bzw. Dienstverträgen sein. Dies muss in jedem Einzelfall eingeschätzt werden.

Eine Auftragsdatenverarbeitung im Sinne des BDSG ist nicht zwangsläufig ein Auftrag nach dem BGB.[148] Nach §§ 662 ff. BGB ist der Auftragnehmer selbstständig für den Auftraggeber tätig. Ein Auftragsdatenverarbeiter hingegen nimmt seine Aufgaben unselbständig und ohne Gestaltungsbefugnisse wahr.

III. Auftragsdatenverarbeitung

Beabsichtigt der Cloud-Nutzer trotz der komplexen gesetzlichen Anforderungen eine Auftragsdatenverarbeitung zu nutzen, sind sämtliche zehn Voraussetzungen des § 11 Abs. 2 BDSG zu beachten.[149] Im Vertrag muss daher explizit geregelt sein, auf welche Daten sich der Auftrag erstreckt und für wie lange die Datenverarbeitung im Auftrag erfolgen soll (Nr. 1). Ebenso müssen der Umfang sowie die Art und Weise der Datenerhebung, -verarbeitung oder -nutzung und der Kreis der Betroffenen eingegrenzt werden (Nr. 2). Mithilfe der Anlage zu § 9 BDSG sind die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes zu definieren (Nr. 3). Diese Maßnahmen müssen die Vorgaben der Anlage gewährleisten: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und getrennte Verarbeitung. Insbesondere für die Zugangskontrolle, also die Hinderung Unbefugter an der Nutzung der Datenverarbeitungssysteme, bieten sich Verschlüsselungsverfahren an. Außerdem müssen Absprachen hinsichtlich der Berichtigung und Löschung der Daten (Nr. 4) sowie der Kontrollpflichten und -befugnisse des Auftraggebers (Nr. 5, 7) getroffen werden. Es ist festzulegen, ob und in welchem Umfang der Auftragnehmer seinerseits Unterauftragnehmer beauftragen darf (Nr. 6). Im Falle von Verstößen des Auftragnehmers gegen die Vereinbarungen, muss geregelt sein, dass diese dem Auftraggeber unverzüglich mitgeteilt werden (Nr. 8), sodass eventuelle Datenlecks geschlossen werden können. Vertraglich zu vereinbaren ist außerdem der

147 *Nägele/Jacobs*, (Fn. 4), S. 284.

148 *Abel*, Auftragsdatenverarbeitung in der Praxis, Datenschutz Praxis 4/2011, S. 14.

149 Zur detaillierten vertraglichen Gestaltung der Auftragsdatenverarbeitung ISACA-Leitfaden, (Fn. 58), S. 8-16.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Umfang der Weisungsbefugnis des Auftraggebers (Nr. 9) sowie der Umgang mit den Daten nach Beendigung des Auftragsverhältnisses (Nr. 10).[150]

Dieser Katalog ist nicht abschließend. Der Cloud-Nutzer sollte daher weitreichendere Vertragsabsprachen verlangen, um seine Interessen zu wahren.[151] Die folgenden Ausführungen gelten demnach auch für eine Auftragsdatenverarbeitung.

Bei Auftragsverhältnissen mit Cloud-Anbietern in unsicheren Drittstaaten sollten die Standardvertragsklauseln für Auftragsdatenverarbeiter der Europäischen Kommission genutzt werden.[152] Sie bieten die größtmögliche Rechtssicherheit für den Cloud-Nutzer. Individuelle Verträge sind durch eine Datenschutzbehörde zu genehmigen.

IV. Service Level Agreements

Da Cloud-Verträge meist ihren Schwerpunkt im Mietrecht haben, hat der Cloud-Anbieter grundsätzlich gemäß § 535 Abs. 1 Satz 2 BGB eine unterbrechungsfreie Verfügbarkeit des Mietgegenstands, also der Hard- bzw. Software, zu gewährleisten. Diese sogenannte Gewährleistungsverpflichtung besteht über die gesamte Dauer des Mietverhältnisses. Eine einhundertprozentige Verfügbarkeit ist für die Anbieter jedoch nicht möglich, ohne die Preise für die Nutzer in unangemessene Höhen zu treiben.[153] Normale Systemunterbrechungen sind häufig Folgen von Wartungsarbeiten, die unabdingbar für die Gewährleistung der Services sind.[154] Eine Internet-Verbindung, die der Nutzer benötigt, um den Cloud-Dienst zu erreichen, kann die Verfügbarkeit noch erschweren, weil auch der Internetzugang nicht immer zu 100 % gewährleistet werden kann. Der Nutzer kann in diesem Fall aber nicht immer feststellen, ob der Ausfall der Anwendung auf einem Fehler beim Internetzugangs- oder beim Cloud-Anbieter liegt.[155] Cloud-Anbieter sind deshalb darauf angewiesen, Verfügbarkeitsquoten mit ihren Nutzern zu vereinbaren, um Schadensersatzforderungen zu entgehen, weil keine einhundertprozentige Verfügbarkeit zu gewährleisten ist. Der Nutzer muss sich dann die höchstmögliche Verfügbarkeit zusichern lassen, denn obwohl der Cloud-Anbieter grundsätzlich zur Bereitstellung der Services verpflichtet ist, sind seine Pflichten hinsichtlich von Reaktionszeiten, Mängelbeseitigungszeiten und vor allem Verfügbarkeitswerten nicht festgelegt.[156]

---

150 Entwürfe für Musterverträge für die Auftragsdatenverarbeitung bieten u.a. BITKOM, http://www.bitkom.org/files/documents/Mustervertragsanlage_zur_Auftragsdatenverarbeitung_v_3_0.pdf (12.6.2012), und der GDD, https://www.gdd.de/nachrichten/news/neues-gdd-muster-zur-auftragsdatenverarbeitung-gemas-a7-11-bdsg (12.6.2012).

151 So auch *Vander*, (Fn. 64), S. 294.

152 Zu den Standardvertragsklauseln für Auftragsdatenverarbeiter siehe unter C.IV.3.c).

153 *Niemann/Paul*, (Fn. 4), S. 447.

154 *Pohle/Ammann*, (Fn. 10), S. 275.

155 *Karger/Sarre*, (Fn. 12), S. 431.

156 Ibid., S. 432.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Vereinbarungen dahingehend bieten die sogenannten *Service Level Agreements* (SLA). Die Definition vom Inhalt solcher Vereinbarungen ist uneinheitlich. Einige Ansichten sehen SLA als ganz allgemeine Leistungsbeschreibungen an, andere definieren damit die bestimmte Qualität der Leistung und wieder andere Meinungen nehmen SLA zur Ausgestaltung der Vertragsstrafen im Falle einer Schlechtleistung. Vor Abschluss von SLA sollten sich die Vertragsparteien von daher zuerst darüber einigen, welcher Ansicht sie folgen. In den meisten Fällen enthalten SLA Klauseln zur Ausgestaltung der speziellen Leistung des Cloud-Anbieters. Darunter fallen Wartungsarbeiten, Bezugsgrößen und eben die Verfügbarkeit des Service. Im Falle von Verfügbarkeitsvereinbarungen, meist 99,X % statt 100 %, handelt es sich um Konkretisierungen der geschuldeten Qualität.[157] Der Vorteil für den Cloud-Anbieter liegt dabei darin, dass SLA, obwohl sie durchaus AGB-Charakter haben können, nicht unter die Inhaltskontrolle der §§ 305 ff. BGB fallen.[158] Denn sie bestimmen das „wie" der Leistung des Anbieters und stellen keine Abweichung von den geltenden Rechtsvorschriften dar.[159] Werden in SLA jedoch Regelungen getroffen, die bestimmen, dass die Leistung nicht vollständig erbracht werden muss, werden sie von der Inhaltskontrolle erfasst und als unzulässige Haftungsbeschränkungen angesehen.[160]

Die Leistungsbeschreibung sollte so detailliert wie möglich ausfallen. Da dem Cloud-Nutzer eine Wartung und Pflege der Server selbst nur schwer möglich sein wird, müssen Vereinbarungen bezüglich dieser Leistungen in die SLA aufgenommen werden.[161] Selten wird eine schnelle Reaktionszeit zu gewährleisten sein, da dies mit erhöhten Kosten verbunden wäre. Kunden, die dennoch eine zeitnahe Fehlerbehebung fordern, sollten mit erhöhten Entgelten rechnen. Zudem lassen sich in SLA Sanktionsmechanismen aufnehmen, die Schadenersatz oder Minderungen herbeiführen, wird der Cloud-Anbieter den vereinbarten Leistungen nicht gerecht.[162] Die Vereinbarung von Vertragsstrafen wird häufig praktiziert, da sie dazu führt, dass beide Vertragsparteien ihre jeweiligen Pflichten mit erhöhter Sorgfalt erfüllen.[163]

Bezüglich investigativer Verfahren wie dem oben angesprochenen *pre-trial discovery* sollten ebenfalls Reaktionszeiten und Verfügbarkeitswerte mit dem Cloud-Anbieter vereinbart werden.[164] Andernfalls drohen dem betroffenen Unternehmen unter Umständen Sanktionen wegen Verzögerung des Verfahrens oder ähnlichem. Dass

157 *Helwig/Koglin*, Service Level Agreements für die Software-as-a-Service-Dienste, in: Büchner/Briner, (Fn. 11), S. 66.

158 BGH, Az.: XI ZR 274/00, Urteil v. 12.06.2001, NJW 2001, 2636.

159 So auch *Niemann/Paul*, (Fn. 4), S. 447.

160 BGH, Az. XI ZR 138/00, Urteil v. 12.12.2000, S. 6 ff.

161 *Helwig/Koglin*, (Fn. 157), S. 67.

162 *Schulz*, (Fn. 130), S. 408 f.

163 *Niemann/Paul*, (Fn. 4), S. 447.

164 Ibid., S. 450.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

die Daten aufgrund der Strukturen einer Cloud nicht rechtzeitig bereitgestellt werden konnten, wird kaum als Entschuldigungsgrund akzeptiert werden.

Die Gewährleistungspflichten aus dem Mietverhältnis umfassen nicht die Skalierbarkeit, also die Vergrößerung bzw. Verminderung des Umfangs des jeweiligen Cloud-Dienstes.[165] Ist absehbar, dass der Nutzer in Zukunft ein größeres Server-Volumen benötigen wird, sollte eine Option zur Erweiterung des Cloud-Angebots in den Vertrag aufgenommen werden.

V. Nichtpersonenbezogene Daten

Firmengeheimnisse, Know-How und Werbestrategien sind immanent wichtig für das Funktionieren eines Unternehmens. Häufig handelt es sich dabei aber nicht um personenbezogene Daten und damit unterfallen sie nicht dem Schutz des BDSG.[166] § 17 des Gesetzes gegen unlauteren Wettbewerb (UWG) schützt zwar Betriebs- und Geschäftsgeheimnisse vor der vorsätzlichen Preisgabe durch Personen, denen diese anvertraut wurden. Eine unabsichtliche Preisgabe dieser Daten wird davon jedoch nicht erfasst.[167] Um Firmengeheimnisse etc. gemeinsam mit personenbezogenen Daten zu schützen, sollten Klauseln zur Geheimhaltung und Vertraulichkeit in den Vertrag aufgenommen werden. Das Problem dabei ist, dass eine Überwachung der Einhaltung solcher Verpflichtungen beinahe unmöglich ist. Zusätzlich sollten daher Vertragsstrafen im Falle von verletzten Geheimhaltungspflichten vereinbart werden. Hilfreich kann außerdem ein Auditrecht des Cloud-Nutzers sein. Dieses erlaubt ihm, die Einhaltung der Vertraulichkeits- und Geheimhaltungsbestimmungen von Zeit zu Zeit zu überprüfen.[168] Geheimhaltungsklauseln gelten außerdem nicht für Zugriffe auf Daten durch die zuständigen Behörden im Ausland, zum Beispiel im Rahmen eines *pre-trial discovery* oder des *Patriot Acts* in den USA. Mit Hinblick darauf sollte zumindest vereinbart werden, dass der Cloud-Nutzer und damit die für die Daten verantwortliche Stelle informiert wird, bevor die Daten weitergegeben werden. In der Praxis erfolgt die Unterrichtung nämlich meist erst im Nachhinein. Damit wird eine eventuelle Verteidigung gegen die Herausgabeforderung unmöglich gemacht.

VI. Datensicherheit

Neben dem Datenschutz spielt die Gewährleistung der Sicherheit sowohl der personenbezogenen als auch der nichtpersonenbezogenen Daten eine wichtige Rolle. Sie müssen durch den Cloud-Anbieter und dessen technische Maßnahmen, wie zum

165 *Karger/Sarre*, (Fn. 12), S. 432 f.

166 *Härting*, (Fn. 44), Rdnr. 22; *Pohle/Ammann*, (Fn. 10), S. 278.

167 *Köhler*, in: Köhler/Bornkamm, Gesetz gegen den unlauteren Wettbewerb, 29. Aufl. 2011, § 17 UWG, Rdnr. 23.

168 *Karger/Sarre*, (Fn. 12), S. 435.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Beispiel Verschlüsselungstechniken, vor unbefugtem Zugriff Dritter und Verlust geschützt werden. Insbesondere sind Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Zurechenbarkeit der Cloud-Services zu gewährleisten.[169] Die Einhaltung der gesetzlichen Vorschriften zur Datensicherheit wird *Compliance* genannt. Ein Verstoß gegen Datensicherheitsvorschriften kann empfindliche Sanktionen nach sich ziehen. Daher gilt *Non-Compliance* mittlerweile als eigenständiges Unternehmensrisiko.[170]

Mit dem Urteil *Online-Durchsuchung*[171] hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – kurz IT-Grundrecht – etabliert. Genau wie das Recht auf informationelle Selbstbestimmung gehört es zum Umfang des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Im Rahmen des Cloud Computing ist das IT-Grundrecht insofern einschlägig, als dass es davor schützen soll, dass Dritte sich durch Zugriff auf die Systeme des Cloud-Anbieters unbefugt große Datenmengen beschaffen, die ohne weitere Datenverarbeitung sofort genutzt werden können.

Durch die Trennung von Hard- und Software und dem damit einhergehenden Kontrollverlust über die Daten, entfallen für den Cloud-Nutzer die bisherigen Möglichkeiten, den Zutritt und Zugang zu und Zugriff auf seine Daten durch physische Mittel zu kontrollieren. Die Pflichten eines jeden Unternehmers aus § 91 Abs. 2 des Aktiengesetzes (AktG), geeignete Maßnahmen zu ergreifen, um Gefahren für sein Unternehmen frühzeitig zu erkennen, werden in § 9 BDSG konkretisiert. Diese Pflichten müssen durch gezielte vertragliche Vereinbarungen dem Cloud-Anbieter übertragen werden. Andernfalls kommt der Cloud-Nutzer seiner Sorgfaltspflicht nicht nach.

Bei vertraglichen Regelungen zur Datensicherheit gilt es, einige allgemeine Grundsätze zu beachten. So kann es zum Beispiel, wie schon häufiger angesprochen, keine vollständige Sicherheit der Daten geben. Im Rahmen der Vertragsgestaltung ist folglich darauf zu achten, welches Risiko für den Cloud-Nutzer akzeptabel ist. Grundsätzlich werden kleinere Unternehmen ein geringeres Datensicherheitsniveau benötigen als große, global agierende Konzerne. Auch die Datensicherheit kann mittels SLA ausgestaltet werden. Da die Gestaltung der Datensicherheit abhängig von den technischen Fortschritten ist und sich demnach schnell verändern kann, müssen die vereinbarten Datensicherheitsmaßnahmen regelmäßig überwacht und auf dem neuesten Stand gehalten werden.[172] Diese Überprüfung kann mittels Audits erfolgen. § 9a BDSG erwähnt die Möglichkeit, zur Verbesserung des Datenschutzes und der

169 Ibid., S. 436; *Niemann/Paul*, (Fn. 4), S. 450.

170 *Kramer/Meints*, in: Hoeren/Sieber (Hrsg.), Handbuch Multimedia-Recht, 2010, Teil 16.5 Datensicherheit, Rdnr. 6.

171 BVerfG, Az. 1 BvR 370/07, Urteil v. 27.2.2008, *Online-Durchsuchung*, Leitsatz 1, Rdnr. 166.

172 Vgl. *Kramer/Meints*, (Fn. 170), Teil 16.5 Datensicherheit, Rdnr. 10.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

Datensicherheit, das Datenschutzkonzept und die technischen Einrichtungen Daten verarbeitender Stellen freiwillig durch unabhängige Gutachter prüfen zu lassen. Dazu soll ein eigenständiges Gesetz erlassen werden.

VII. Gewährleistung des Datenschutzes in unsicheren Drittstaaten

Das grundsätzliche Verbot der Datenübertragung in unsichere Drittstaaten hat dazu geführt, dass einige Anbieter ihre Dienste ausdrücklich nur in den Grenzen der EU anbieten, um datenschutzrechtlichen Problemen vorzubeugen. Außerdem erreichen sie auf diesem Weg Kunden, die den Zugriffsrechten von Behörden aus Drittstaaten – z.B. *Patriot Act* – skeptisch gegenüber stehen. Vertragsklauseln zur Absicherung des Datenschutzes in unsicheren Drittstaaten müssen von allen beteiligten Aufsichts behörden genehmigt werden. Aus Kosten- und Zeitgründen bietet sich dieses Verfahren nur für große Unternehmen an. Kleinere Unternehmen und auch Privatpersonen sollten bei der Vertragsgestaltung auf die Standardvertragsklauseln der EU zurückgreifen. Auch wenn der Vertragspartner ein US-amerikanisches „Safe Harbor"-Unternehmen ist, sollte er vertraglich noch einmal explizit auf die Einhaltung der „Safe Harbor"-Prinzipien verpflichtet werden. Insbesondere sollten Vertragstrafen im Falle eines Verstoßes gegen die Datenschutzvorschriften geregelt werden. Der Cloud-Nutzer sollte sich zudem Kontrollrechte einräumen lassen und regelmäßig Zertifizierungsberichte sowie Nachweise für die Einhaltung des Datenschutzes durch den Cloud-Anbieter verlangen.

VIII. Durchsetzung des Vertrags

Große Herausforderungen entstehen in der Rechtsdurchsetzung der jeweiligen Vertragsklauseln. Auch wenn theoretisch Möglichkeiten bestehen, im Falle von Lecks in der Geheimhaltung oder unzureichenden Datensicherungsmaßnahmen die vereinbarten Klauseln durchzusetzen, so wird in den meisten Fällen eine kurzfristige Durchsetzung aufgrund der langen Gerichtswege nicht möglich sein. Eine Abwendung von Schaden im Vorfeld ist daher kaum möglich. Lediglich Gewährleistungs- oder Haftungsansprüche nach eingetretenem Schaden erscheinen praktikabel. Das bedeutet im schlimmsten Fall auch, dass wichtige Daten verloren gegangen sind bzw. nicht mehr geheim gehalten werden können. Dem Cloud-Nutzer bleibt neben blindem Vertrauen nichts anderes übrig, als seine Daten an anderer Stelle in Form eines Back-ups zu sichern. Damit verbunden sind ein höherer Aufwand und steigende Kosten, auch im Hinblick auf eine immer notwendige Synchronisierung der Datensätze. Zudem widerspricht die Notwendigkeit von Back-ups dem Prinzip des Cloud Computing, eigene Server durch die Auslagerung von Daten in die Cloud zu entlasten.[173] Mit Blick auf den großen Aufwand, den die Durch-

[173] So auch *Karger/Sarre*, (Fn. 12), S. 436 f.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

setzung von Vertragsbestimmungen erfordert, sollte der Vertrag möglichst genau auf die Bedürfnisse beider Vertragsparteien eingehen, so dass die Einhaltung der Bestimmungen für beide Seiten lohnend ist.

IX. Beendigung des Vertrags

Das Ende des Vertragsverhältnisses ist aus datenschutzrechtlicher Sicht insofern interessant, als dass der Nutzer ein Interesse an der Herausgabe bzw. Löschung seiner Daten von den Servern des Cloud-Anbieters hat. Zur Löschung der Daten ist der Anbieter aber auch schon aufgrund des Zweckbindungsgrundsatzes des Datenschutzrechtes verpflichtet. Mit dem Ende des Vertragsverhältnisses fehlt der Datenverarbeitung die rechtliche Grundlage. Der Entwurf der Datenschutz-Grundverordnung enthält in Art. 17 das Recht auf Vergessenwerden. Das umfasst den auch bisher schon bestehenden Löschungsanspruch nach Wegfall des Zwecks der Datenerhebung. Eine Neuerung ist damit nicht verbunden. Sicherheitshalber sollte vereinbart werden, wie der Cloud-Anbieter mit den Daten zu verfahren hat, nachdem der Vertrag beendet ist. Hierbei ist das Format, in dem der Anbieter die Daten speichert besonders interessant. Aufgrund der verschiedenen Systeme, sind die Datenformate einzelner Anbieter oft nicht miteinander kompatibel. Um zu gewährleisten, dass ein Anbieterwechsel unkompliziert erfolgen kann, sollte vertraglich vereinbart werden, in welchem Format die Daten gespeichert werden.[174] Mögliche Kosten durch Kompatibilitätsprobleme oder Betriebsausfallrisiken sollten vertraglich abgesichert werden. Andererseits macht sich der Nutzer abhängig vom Cloud-Anbieter.[175] Der Entwurf der Datenschutz-Grundverordnung enthält in Art. 18 das interessante Recht auf Datenübertragbarkeit. Demnach steht jedem Betroffenen das Recht zu, von der datenverarbeitenden Stelle jederzeit eine elektronische Kopie aller seiner Daten anzufordern. Diese muss auch in einem gängigen Format vorliegen, um die Weiterverarbeitung der Daten zu gewährleisten. Damit wäre die Gefahr eines sogenannten *Lock-Ins*, also der dauerhaften Bindung an einen Anbieter, unterbunden. Darüber hinaus sollten Regelungen zur Vertragsabwicklung getroffen werden, zum Beispiel wie eine Kündigung zu erfolgen hat, und was im Nachhinein mit den Daten geschieht.

174 So auch *Fickert*, (Fn. 13), S. 422; *Pohle/Ammann*, (Fn. 10), S. 277.

175 So auch *Schulz*, (Fn. 130), S. 410.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -

E. Fazit und Ausblick

Die Betrachtung der derzeitigen datenschutzrechtlichen und vertragsgestalterischen Herausforderungen im Cloud Computing hat gezeigt, dass eine umfangreiche Vorbereitung auf die Nutzung von Cloud-Services unerlässlich ist. Dabei ist noch einmal hervorzuheben, dass Cloud Computing zwar auf den ersten Blick eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG darstellen könnte, die strengen Anforderungen an diese sowie an jede Datenübermittlung jedoch sehr hoch und für den Cloud-Nutzer nur schwer zu erfüllen sind. Festgestellt wird, dass die datenschutzrechtlichen Regularien dem Cloud Computing teilweise seinen Reiz und seine Vorteile nehmen. Die gewünschte Flexibilität und Erleichterung der Datenverarbeitung werden durch die zu beachtenden Vorschriften konterkariert. Eine genaue Vorbereitung empfiehlt sich daher. Der Cloud-Nutzer muss sich im Vorfeld darüber bewusst sein, welche Arten von Daten er in welcher Form in die Cloud geben will. Außerdem muss er sich über den Cloud-Anbieter informieren und gegebenenfalls mit diesem in Vertragsverhandlungen eintreten, um seine Interessen bestmöglich durchzusetzen. Zur Gewährleistung des Datenschutzes eignen sich eher Private Clouds, wegen der besseren Möglichkeiten, individuelle Vereinbarungen zu treffen. Public Clouds sind die kostengünstigere Variante, bei der sich der Cloud-Nutzer mit den standardisierten Verfahren des Cloud-Anbieters arrangieren muss.

Die Zukunft gehört dem Cloud Computing. Sei es die Mail-Applikation auf dem Smartphone oder das Dokument, das über GoogleDocs zwischen den Kollegen ausgetauscht wird. Derzeit ist die Entwicklung in Deutschland und Europa durch Sicherheits- und Datenschutzbedenken noch gehemmt, wozu auch die unzureichende Gesetzgebung beiträgt. Es wäre wünschenswert, dass der Datenschutz so schnell wie möglich den technischen Möglichkeiten der Praxis angepasst wird, sodass die Nutzung der umfangreichen Technik nicht durch veraltete Vorschriften beeinträchtigt wird. Ein einheitlicher europäischer Standard würde außerdem zur verbesserten Rechtssicherheit und Transparenz im Datenschutz führen. Der Entwurf der europäischen Datenschutz-Grundverordnung setzt ein deutliches Zeichen in diese Richtung. Es bleibt abzuwarten, wie viele der Innovationen des Verordnungsentwurfs nach dem legislativen Verfahren übrig bleiben. Zweifellos wird es Zeit, dass nicht nur das Web auf den Stand 2.0 kommt, sondern ebenso der Datenschutz.

https://doi.org/10.5771/1435-439X-2012-2-121 - am 30.01.2026, 22:06:29. https://www.inlibra.com/de/agb - Open Access -