
# D1.1

# Datenschutzrechtliche Anforderungen an das SPLITCloud-Framework

**Autoren:**

SPLITCloud-Team des ULD

**Reviewer:**

Marit Hansen (ULD)

Rasmus Robrahn (ULD)

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

VDI|VDE|IT

# Inhaltsverzeichnis

# 1 Einleitung

## 1.1 Zum Dokument

Das Dokument enthält Ergebnisse des Forschungsprojekts SPLITCloud als Deliverable D1.1. Im Rahmen des Arbeitspakets 1 oblag es dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, datenschutzrechtliche Anforderungen an eine Cloud-Computing-Architektur zu formulieren. Dabei wurden nationale datenschutz- und telemedienrechtliche Anforderungen ebenso betrachtet wie die rechtlichen Rahmenbedingungen für den grenzüberschreitenden Datenaustausch.

Das Dokument bezieht sich dabei auf die Anforderungen an Software-as-a-Service-Plattformen, die die Einspeisung, Aufbereitung und Einsicht in Messwerte aus intelligenten digitalen Energieverbrauchszählern (Smart Meter) ermöglichen.

## 1.2 Zum Projekt

Das Projekt dient der Entwicklung der SPLITCloud-Architektur in der Software-as-a-Service (SaaS) datenschutzkonform angeboten werden soll.

Für den Begriff Cloud Computing besteht keine allgemeingültige Definition. Nach der verbreiteten Definition des US-amerikanischen National Institute of Standards and Technology (NIST) ist Cloud Computing ein Modell, „das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z.B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Service-Provider-Interaktion zur Verfügung gestellt werden können.“[1]

Cloud-Anwender ist jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken einen Cloud-Dienst in Anspruch nimmt.

Cloud-Diensteanbieter ist jede natürliche oder juristische Person, die eigene oder fremde Cloud-Dienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt oder die angebotenen Dienste wirksam kontrolliert. Bei Cloud-Diensten wird hauptsächlich zwischen vier Bereitstellungsmodellen unterschieden:[2]

1. Private Cloud mit Cloud-Infrastruktur für nur eine Institution mit verschiedenen Möglichkeiten, wer die Infrastruktur betreibt und wo sich diese Infrastruktur befindet;
2. Public Cloud mit Services eines Cloud-Diensteanbieters für die Allgemeinheit oder große Gruppen;

---

[1] Mell/Grance, NIST SP - 800-145, 2; verwendete Übersetzung nach https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html.

[2] Manche Modelle wie beispielsweise Virtual Private Cloud – also eine durch logische Unterteilung einer Public Cloud geschaffene Private Cloud – sind von dieser Einteilung nicht umfasst, https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html.

3. Community Cloud mit von mehreren Institutionen geteilter Cloud-Infrastruktur;
4. Hybrid Cloud bei der gemeinsamen Nutzung von mehreren eigenständigen Cloud-Infrastrukturen über Schnittstellen.

Davon unabhängig wird zwischen drei Service-Modellen unterschieden:

1. Infrastructure-as-a-Service (IaaS) besteht aus hardwaregebundenen IT-Ressourcen – also Rechenleistung, Datenspeicher oder Netzen. Der Cloud-Anwender baut auf diesem Dienst seine Betriebssysteme und Anwendungen auf.
2. Platform-as-a-Service (PaaS) beinhaltet über IaaS hinaus eine komplette Infrastruktur bestehend aus Hardware und Betriebssystem. Auf dieser kann der Cloud-Anwender mittels standardisierter Schnittstellen eigene Anwendungen laufen lassen.
3. Software-as-a-Service (SaaS) oder auch Application Service Providing (ASP) stellt dem Cloud-Anwender über Computernetzwerke Anwendungen und Programmfunktionalitäten des Cloud-Diensteanbieters bereit.

Im Gegensatz zu der vorherigen überwiegend vorherrschenden Strukturierung von IT-Outsourcing besteht für den Cloud-Anwender beim Cloud Computing keine statische Zuordnung bestimmter physikalischer Infrastrukturen.[3]

Die Vorteile des Cloud Computing bestehen in der Skalierbarkeit, also der schnellen Anpassung an den tatsächlichen Bedarf, verbunden mit einer Selbstzuweisung von Cloud-Diensten durch den Cloud-Anwender; in Kostenvorteilen erzeugt durch die Teilung der Infrastruktur und die Abrechnung nach Nutzung; in erhöhter Zuverlässigkeit und Ausfalltoleranz der IT-Infrastruktur sowie in der ständigen weltweiten Verfügbarkeit von Cloud-Diensten für den Cloud-Anwender.[4]

Die Nachteile des Cloud Computing bestehen in dem Kontrollverlust für den Cloud-Anwender in Folge der Verlagerung eigener Inhalte in die Cloud und der Abhängigkeit vom Cloud-Diensteanbieter. Der Cloud-Anwender muss dem Cloud-Diensteanbieter hinsichtlich der Integrität und Vertraulichkeit der an diesen übermittelten Daten vertrauen. Dabei sind die fehlenden physikalischen Hindernisse ein Nachteil, da auch unbefugte Dritte lediglich die Authentifizierungssysteme überwinden müssen um Zugriff zu erhalten.[5] Zudem sind die zusammenhängenden Themenbereiche Interoperabilität, Datenportabilität und Reversibilität zwischen Cloud-Umgebungen und aus Cloud-Umgebungen heraus noch nicht ausreichend gewährleistet.[6] Reversibilität bedeutet, dass Cloud-Anwender in der Lage sein sollen, vollständig autonom, zu jeder Zeit, in einem Standardformat, zu vorhersehbaren Kosten und in einem vorbestimmten Zeitraum alle ihre Daten zurückzuerhalten. Das beinhaltet die Möglichkeit,

[3] Grünwald/Döpkens, MMR 2011, 287.
[4] Nägele/Jacobs, ZUM 2010, 282; Grünwald/Döpkens, MMR 2011, 287.
[5] Jotzo, Der Schutz personenbezogener Daten in der Cloud, 2013, S. 81.
[6] Diesem Umstand versucht die Digitale Agenda für Europa abzuhelfen, http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy.

Applikationen und Daten von einer Cloud-Umgebung zu einer anderen Cloud-Umgebung oder aus der Cloud-Umgebung als solche heraus zu bewegen. Damit kann eine Abhängigkeit von einem Cloud-Diensteanbieter (Vendor-lock-in) verhindert werden.

Die SPLITCloud-Architektur soll in rechtskonformer Weise eine neue Art des Cloud Computing realisieren, die Datenschutzanforderungen umfassend berücksichtigt.

# 2 Nationale rechtliche Anforderungen

Zunächst gilt es zu untersuchen, welchen Anforderungen der Betrieb der SPLITCloud-Architektur nach deutschem Bundesrecht unterliegt.

## 2.1 Datenschutzrecht

Die zentrale rechtliche Vorgabe für den Aufbau und Betrieb der SPLITCloud-Architektur stellt das Datenschutzrecht dar. In Deutschland ist dieses im Wesentlichen im Bundesdatenschutzgesetz (BDSG) geregelt. Verfassungsrechtliche Grundlage für das BDSG ist das Grundrecht auf informationelle Selbstbestimmung. Dieses Rechtsinstitut hat das Bundesverfassungsgericht im Jahre 1983 in seinem Volkszählungsurteil,[7] aus dem allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 Grundgesetz in Verbindung mit Art. 1 Abs. 1 GG entwickelt. Darin wurde dem Einzelnen erstmals zugebilligt, selbst über die Preisgabe und Verwendung der ihn betreffenden Daten zu verfügen.[8] Eine weitere Konkretisierung des Grundrechts erfolgte beispielsweise durch das Urteil zur Online-Durchsuchung, in dem das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme als spezielle Ausprägung des Datenschutzes entwickelt wurde.[9]

Die Anforderungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts wurden im BDSG einfachgesetzlich verankert. Soweit nicht-öffentliche Stellen wie Unternehmen und Privatpersonen Cloud Computing nutzen oder betreiben, unterliegen sie den Verpflichtungen des BDSG.[10] Öffentliche Stellen unterliegen als Bundesbehörden dem BDSG und als Landesbehörden dem jeweiligen Landesdatenschutzgesetz.[11] Die Datenschutzgesetze der Länder orientieren sich inhaltlich stark am BDSG, auch wenn teilweise zusätzliche Spezialregelungen bestehen. Die nachfolgenden Ausführungen können großenteils entsprechend für Landesbehörden herangezogen werden und gelten somit für alle denkbaren Cloud-Anwender und Cloud-Diensteanbieter in Deutschland oder solche Cloud-Dienste aus dem EU-Ausland, die sich an deutsche Cloud-Anwender richten.

### 2.1.1 Schutz personenbezogener Daten

Unter dem Schutz des Rechts auf informationelle Selbstbestimmung stehen nicht sämtliche Informationen, die existieren. Nur personenbezogene Daten fallen unter die Schutzvorschrift des § 4 Abs. 1 BDSG. Personenbezogene Daten sind nach der Definition des § 3 Abs. 1 BDSG Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten und bestimmbaren Person.

---

[7] BVerfGE 65, 1.
[8] BVerfGE 65, 1 (43); 118, 168 (184); Epping, Grundrechte, Rn. 626; Hufen, Staatsrecht II, § 12 Rn. 4.
[9] BVerfGE 120, 274
[10] Weichert, DuD 2010, 679; allg. § 1 Abs. 2 Nr. 3 BDSG.
[11] Zum BDSG: § 1 Abs. 2 Nr. 1 BDSG; zum Landesrecht z.B. § 3 Abs. 1 LDSG SH.

#### 2.1.1.1 Allgemeines zum Personenbezug im BDSG

Die Begriffe persönliche Verhältnisse und sachliche Verhältnisse sind inhaltlich nicht scharf voneinander abgrenzbar, jedoch ist eine Unterscheidung in Ermangelung einer unterschiedlichen Rechtsfolge nicht erforderlich.[12]

Zu den persönlichen Verhältnissen gehören Angaben über den Betroffenen selbst und solche die ihn identifizieren oder charakterisieren, beispielsweise Name, Geburtsdatum, Anschrift, Beruf, Konfession, Aussehen, gesundheitliche Merkmale, Überzeugungen, Einstellungen sowie biometrische Daten und zugeordnete Standortdaten.[13] Auch Werturteile über den Betroffenen sind erfasst.[14]

Zu den sachlichen Verhältnissen zählen Angaben über einen Sachverhalt, der auf den Betroffenen direkt beziehbar ist, beispielsweise Eigentums- und Besitzverhältnisse, Vertragsverhältnisse, aber auch manche Geodaten.[15]

Um grundsätzlich unter rechtlichem Schutz zu stehen, müssen die personenbezogenen Daten nicht besonders qualifiziert sein, beispielsweise durch einen Bezug in die Intimsphäre. Auch relativ banale Informationen, die für sich genommen keine Persönlichkeitsrelevanz besitzen, sind rechtlich geschützte personenbezogene Daten.[16] Der Grund hierfür liegt in der Verkettbarkeit mit anderen Daten. Werden diverse Informationen über ein Individuum miteinander verknüpft, so besteht die Möglichkeit einer unkontrollierbaren Persönlichkeitserfassung.[17] Aus diesem Grund gibt es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr.[18]

Sensitive Daten sind gem. § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Für diese besondere Arten personenbezogener Daten enthalten die §§ 13 Abs. 2; 28 Abs. 6 bis 9; und 29 Abs. 5 BDSG Sonderregelungen betreffend Erhebung, Verarbeitung und Nutzung.

Personenbezug ist gegeben, wenn der Betroffene durch die Information bestimmt oder bestimmbar ist. Bestimmt ist die Person, wenn der Bezug sich unmittelbar herstellen lässt,[19] also klar ist, dass sich Angaben auf eine Person bezieht und nicht auf andere.[20] Dies betrifft vor allem Datensätze, die den Namen des Betroffenen enthalten. Kann der Betroffene ermittelt werden,

---

[12] Gola/Schomerus, BDSG, § 3 Rn. 5.
[13] Gola/Schomerus, BDSG, § 3 Rn. 6.
[14] Dammann, in: Simitis, BDSG, § 3 Rn. 12.
[15] Gola/Schomerus, BDSG, § 3 Rn. 7; Weichert, DuD 2009, 350 über den Personenbezug von Punktdaten.
[16] BVerfGE 65, 1 (45); 120, 274 (312); Horn, in: Stern/Becker, Grundrechte-Kommentar, Art. 2 Rn. 50.
[17] BVerfGE 65, 1 (43); Becker, in: Hill/Schliesky, E-Volution des Rechts- und Verwaltungssystems, 2010, S. 57 (62); Hansen/Meissner, Verkettung digitaler Identitäten.
[18] BVerfGE 65, 1 (45).
[19] Gola/Schomerus, BDSG, § 3 Rn. 10.
[20] Dammann, in: Simitis, BDSG, § 3 Rn. 22.

obwohl er nicht konkret benannt ist, so ist die Person bestimmbar.[21] Dies ist beispielsweise der Fall, wenn die Adresse des Betroffenen Teil der Information ist. In diesem Fall kann durch minimale Recherche nachvollzogen werden, wer an dem entsprechenden Ort wohnt. Auch die IP-Adresse einer Person besitzt einen bestimmbaren Personenbezug, wenn es möglich ist, nachzuvollziehen, welchem Anschluss diese Adresse wann zugeordnet war und wer der Anschlussinhaber ist. Die Bestimmbarkeit setzt also ein gewisses Maß an Zusatzwissen voraus, mit dem der Betroffene identifiziert werden muss. Dabei kommt es nach einer Ansicht nicht auf die Kenntnisse der speichernden Stelle an, sondern auf die objektive Möglichkeit zur Bestimmung der betroffenen Person.[22] Nach einer anderen Ansicht ist der Begriff des Personenbezugs relativ und somit für eine verantwortliche Stelle durch ihre Möglichkeit der Zuordnung bezüglich derselben Daten gegeben, für eine andere jedoch nicht.[23] Der Personenbezug ist in einem solchen Fall grundsätzlich herstellbar, nur nicht durch jedermann. Eine abschließende Klärung dieser Frage ist noch nicht abzusehen. Unter dem Gesichtspunkt eines vollumfänglichen Schutzes der informationellen Selbstbestimmung ist die erstgenannte Ansicht mit ihrem weitergehenden Schutz vorzugswürdig.

Da die speichernde verantwortliche Stelle jedoch weder einschätzen kann, wieviel Zusatzwissen bei anderen besteht, noch sicherstellen kann, dass die gespeicherten Daten niemals nach außen dringen, unterliegen gegebenenfalls auch solche Daten dem BDSG, die aus Sicht der verantwortlichen Stelle keinen Personenbezug aufweisen. Das BDSG kennt hinsichtlich dieser Unsicherheit kein „erlaubtes Risiko“ zugunsten der verantwortlichen Stelle.[24] Auch Informationen, die nach objektiven Maßstäben keinen Personenbezug aufweisen, können später zu personenbezogenen Daten werden, wenn neue Erkenntnisse eine entsprechende Verkettung mit personenbezogenen Daten zulassen.[25]

An sich personenbezogene Daten können durch wirksame Anonymisierung ihren Personenbezug verlieren. Das BDSG ist dann nicht mehr anwendbar. Die Verarbeitung in der Cloud kann jedoch zu einer nachträglichen Deanonymisierung führen, wenn die Daten dabei entweder mit anderen Informationen verknüpft werden oder wenn sie über die Cloud anderen Stellen zugänglich gemacht werden, die über entsprechendes Zusatzwissen verfügen.[26] Insofern erstreckt sich die Verantwortlichkeit nach dem BDSG auf alle potentiell personenbezogenen Daten.[27]

---

[21] Vgl. BGH, NJW 1991, 568; Caspar, DÖV 2009, 965 (967); Dammann, in: Simitis, BDSG, § 3 Rn. 22ff.
[22] Pahlen-Brandt, DuD 2008, 34 (37); Weichert, in: Däubler/Klebe/Wedde/ders., BDSG, § 3 Rn. 13; Wohlgemuth/Gerloff, Datenschutzrecht, Anm. 3.3.2.2..
[23] Gola/Schomerus, BDSG, § 3 Rn. 10.
[24] Vgl. Dammann, in: Simitis, BDSG, § 3 Rn. 38.
[25] Dammann, in: Simitis, BDSG, § 3 Rn. 32; Hornung, DuD 2004, 429 (430); Roßnagel/Scholz, MMR 2000, 722 (723); Tinnefeld, in: Roßnagel, Hdb Datenschutzrecht, Kap. 4.1 Rn. 22.
[26] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 5; Weichert, DuD 2010, 679 (681).
[27] Vgl. Art. 29-Datenschutzgruppe, WP 136, Abschnitt III 3, S. 23; Dammann, in: Simitis, BDSG, § 3 Rn. 36.

#### 2.1.1.2 Personenbezug in der Cloud und im Smart-Metering

Cloud-Speicher enthalten demnach oftmals personenbezogene Daten in verschiedenen Variationen. Werden dort etwa Kundendaten abgelegt, ist der Personenbezug unmittelbar aufgrund der Verwendung der Kundennamen gegeben. Dabei sind nicht nur die Namens- und Adressdaten rechtlich geschützt, sondern alle Informationen, die damit verknüpft sind. Darunter fallen beispielsweise Informationen über Einkäufe, Kaufinteressen, Zahlungsverhalten und Website-Besuche. Lediglich solche Daten, die nicht mit natürlichen Personen in Zusammenhang stehen, etwa die Warenbestellung eines Unternehmens, das die Cloud nutzt, sind nicht personenbezogen. Hier gilt es jedoch zu beachten, dass nicht nur Kunden, sondern auch eigene Mitarbeiter Betroffene im Sinne des BDSG sein können.[28] Wenn also beispielsweise Warenbestellungen des Unternehmens mit dem Namen oder der Kennung des entsprechenden Mitarbeiters versehen sind, dann handelt es sich bei dem kompletten Datensatz um personenbezogene Daten.

Auch Energie- und Ressourcenverbrauchsdaten geben Auskunft über die persönlichen Verhältnisse einer Person. Da in der heutigen Gesellschaft die Lebensweise mit Technik und Automatisierung verbunden ist, benötigen alltägliche Handlungen wie beispielsweise kochen, beheizen, duschen, radiohören und telefonieren Energie und Ressourcen durch Versorgungsunternehmen.[29] So kann aus Smart-Meter-Daten der Tagesablauf einer Person rekonstruiert werden.[30] Diese Möglichkeit zur Ausforschung wird insbesondere dann problematisch, wenn die Erfassung von Verbrauchsdaten kleinteilig erfolgt beispielsweise durch kurze Erfassungsintervalle oder Gerätebezug; beziehungsweise dann wenn spartenübergreifend Verbrauchsdaten von Wasser, Elektrizität, Wärme oder Gas erfasst werden.[31] Hinsichtlich des Potentials Lebensprofile von Menschen innerhalb des grundrechtlich gem. Art. 13 GG besonders geschützten Rückzugsbereichs Wohnung zu erstellen, ist der Einsatz von Smart-Metering daher mit einer umfassenden Ton und Videoüberwachung zu vergleichen.[32]

Zu beachten ist, dass der Smart-Meter-System-Betreiber abhängig von der Gesamtgestaltung auch Cloud-Anwender sein kann. Smart-Meter-System-Betreiber ist jede natürliche oder juristische Person, die eigene oder fremde Smart-Meter-Systeme zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt oder die angebotenen Dienste wirksam kontrolliert. Smart-Meter-Kunde ist jede natürliche oder juristische Person, die zu beruflichen oder sonstigen Zwecken ein Smart-Meter-System in Anspruch nimmt.

---

[28] Gaul/Koehler, BB 2011, 2229.
[29] Karg, DuD 2010, S 365 (366).
[30] ULD, Datenschutzrechtliche Bewertung des Einsatzes von „intelligenten“ Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter), S. 3, abrufbar unter https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.pdf.
[31] Karg, DuD 2010, S 365 (366).
[32] Ebd.

### 2.1.2 Rechtsgrundlagen der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig, wenn sie auf der Basis einer entsprechenden Rechtsgrundlage geschieht. Unter einer Verarbeitung ist nach der Definition des § 3 Abs. 4 S. 1 BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen zu verstehen. Damit ist der Anwendungsbereich des BDSG derart ausgedehnt, dass praktisch jede Verwendung personenbezogener Daten umfasst ist. Insbesondere die Übermittlung von Daten an einen Cloud-Anbieter zur Speicherung in der Cloud darf nur aufgrund einer Rechtsgrundlage erfolgen.[33] Bei der Regelung des § 4 Abs. 1 handelt es sich um ein sogenanntes Verbot mit Erlaubnisvorbehalt.[34] Das bedeutet, dass jegliche Verwendung personenbezogener Daten erst einmal verboten ist. Nur dann, wenn eine Rechtsgrundlage die Verwendung erlaubt, ist sie ausnahmsweise zulässig. Eine solche Rechtsgrundlage kann entweder eine Rechtsvorschrift oder eine Einwilligung des Betroffenen sein.[35]

#### 2.1.2.1 Rechtsvorschriften

##### 2.1.2.1.1 Bereichsspezifische Rechtsnorm

Eine datenschutzrechtliche Erlaubnisnorm kann auch aus dem Vorrang bereichsspezifischer Erlaubnisnormen folgen. Eine solche Norm findet sich für das Smart-Metering jedoch noch nicht. Zwar sollen zukünftig die datenschutzrechtlichen Fragen auch im Energierecht hinreichend geregelt sein, aber die die Ausgestaltung der Normen ist noch nicht sicher abzusehen. Fest steht bisher, dass die Regelungen betreffend Datenschutz und Datensicherheit in einer Messsystemverordnung und einer Datenkommunikationsverordnung normiert werden sollen. In der Messsystemverordnung sollen Schutzprofile und Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik festgeschrieben werden; in der Datenkommunikationsverordnung soll Transparenz beim Umgang mit Daten geschaffen werden. Es soll darin geregelt sein, wer welche Daten von wem wie oft zu welchem Zweck erhalten darf. Das Regelungssystem soll gegenüber neuen Bedrohungslagen flexibel gestaltet werden.[36]

##### 2.1.2.1.2 Auftragsdatenverarbeitung

Als Rechtsvorschrift, welche die Verwendung personenbezogener Daten erlaubt, ist § 11 BDSG für den Bereich der Auftragsdatenverarbeitung des Cloud Computing von zentraler Bedeutung.

Die Vorschrift dient der datenschutzrechtlichen Absicherung einer Auslagerung von Datenverarbeitung und -speicherung an externe Dienstleister und andere Stellen. Im Gegensatz zur Weitergabe an Dritte[37] erfasst die Erlaubnisnorm des § 11 BDSG die Datenweitergabe an

[33] Holtorf, MPR 2013, 196.
[34] Gola/Schomerus, BDSG, § 4 Rn. 3.
[35] § 4 Abs. 1 BDSG.
[36] BMWi, 7 Eckpunkte für das „Verordnungspaket Intelligente Netze“.
[37] Heidrich/Wegener, MMR 2010, 803 (805 f.).

den „verlängerten Arm“ des Auftraggebers, zur dortigen technischen Umsetzung der Datenverarbeitung. Der Auftragnehmer wird dabei in reiner Hilfsfunktion benötigt, die Erfüllung fremder Aufgaben umsetzend.[38]

Eine solche Auftragsdatenverarbeitung liegt dann vor, wenn der Auftragnehmer gegenüber dem Auftraggeber weisungsgebunden ist.[39] Der Auftraggeber muss die technische und rechtliche Herrschaft über die Daten behalten, damit die Erlaubnisnorm des § 11 BDSG greift.[40] Ob dies der Fall ist, hängt von der konkreten Vertragsgestaltung und von der Art des Cloud-Dienstes ab.[41]

##### 2.1.2.1.2.1 Die Cloud als reiner Speicherdienst

Die ursprüngliche Grundform des Cloud Computing ist die reine Datenspeicherung auf einem Internet-Server. Dabei werden die betreffenden Daten entweder aktiv vom Cloud-Anwender in den Onlinespeicher geladen oder es erfolgt eine automatisierte Synchronisierung bestimmter Datensätze, die der Cloud-Anwender auf seiner lokalen Festplatte ablegt. Diese Form des Cloud Computing ein klassischer Fall der Auftragsdatenverarbeitung.[42] Der Cloud-Anwender speichert Daten nicht auf seinem Rechner, sondern bedient sich der Hilfe eines Onlinespeicherplatzes. Das Ablegen neuer oder das Löschen vorhandener Dateien auf dem Onlinespeicher obliegt für gewöhnlich alleine dem Cloud-Anwender, der so seine Weisungsbefugnis gegenüber dem Cloud-Diensteanbieter ausübt. Der Cloud-Anwender bleibt damit die datenschutzrechtlich verantwortliche Stelle.[43] Diese Einschätzung kann allerdings nicht pauschal auf alle Varianten des Cloud Computing übertragen werden. Inwieweit der Cloud-Diensteanbieter weisungsgebunden ist, hängt schließlich von der konkreten Vertragsgestaltung und -umsetzung ab. Gerade die auf dem Markt tätigen Großkonzerne unterwerfen sich typischerweise nicht den Forderungen ihrer Kunden bei der Gestaltung ihrer Cloud-Dienste.[44] Insofern wird vielfach bezweifelt, dass ein Großteil der Cloud-Diensteanbieter tatsächlich Auftragsdatenverarbeitung im Sinne des § 11 BDSG anbietet.[45] Aufgrund des wirtschaftlich gebotenen Standardisierungs- und Automatisierungsgrades ist es für viele Anbieter auch nicht sachdienlich, sich umfangreichen Weisungen des einzelnen Cloud-Anwenders zu unterwerfen.[46] Für weltumspannende Dienste wie beispielsweise Google würde es schlichtweg zu immensen bürokratischen Aufwand führen, auf alle individuellen Wünsche jedes Cloud-Anwenders

[38] Engeler/Deibler/Hansen/Jensen/Obersteller, MonIKA, S. 28.
[39] Wedde, in: Däubler/Klebe/ders./Weichert, BDSG, § 11 Rn. 4 ff.
[40] Gola/Schomerus, BDSG, § 11 Rn. 3; Nägele/Jacobs, ZUM 2010, 281 (290).
[41] Vgl. AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 8.
[42] Holtorf, MPR 2013, 196; Rath/Rothe, K&R 2013, 623 (624 f.); Taeger/Gabel, BDSG, § 11 Rn. 18; Schulz, MMR 2010, 78; Weichert, DuD 2010, 679 (682 f.).
[43] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 8; Holtorf, MPR 2013, 196.
[44] Heidrich/Wegener, MMR 2010, 803 (806); Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 25.
[45] Engels, K&R 2011, 548; Heidrich/Wegener, MMR 2010, 803 (806); a.A. Hennrich, CR 2011, 546 (548); Thüsing/Pötters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 21.
[46] Engels, K&R 2011, 548.

einzugehen.[47] Es fehlt oftmals bereits an der notwendigen Transparenz, die der Cloud-Anwender benötigt, um die Hoheit über die von ihm abgespeicherten Dateien zu behalten.[48] Insbesondere die entscheidende Frage, welche Daten auf welchem Server liegen, wird dem Cloud-Anwender in der Praxis oftmals weder beantwortet noch kann er den Speicherort beeinflussen.[49] Freilich muss die Weisungsbefugnis des Cloud-Anwenders nicht die gesamte Geschäftstätigkeit des Cloud-Diensteanbieters erfassen. § 11 BDSG schreibt schließlich nicht den Grad der Weisungen vor.[50] Es genügt ein Mindestmaß an Einfluss auf die Verarbeitung der synchronisierten Daten des Cloud-Anwenders.[51] Zu diesem Mindestmaß gehört jedoch die Entscheidungshoheit über den Speicherort.[52] Zumindest muss der Cloud-Anwender Einfluss nehmen können auf die Frage, in welchem Land und damit nach welchem Rechtssystem die Speicherung erfolgt. Auch die Entscheidung über die Einschaltung von Subunternehmen, das Sicherheitsniveau der Datenverarbeitung und die Verfügbarkeit der Daten muss beim Cloud-Anwender verbleiben, wenn die Privilegierung des § 11 BDSG greifen soll.[53] Die vereinzelt im Schrifttum vertretene Annahme, dass der Cloud-Anwender bereits dadurch über die wesentlichen Aspekte der Datenverarbeitung entscheidet, indem er bewusst die Daten in eine von ihm nicht kontrollierbare Umgebung übermittelt,[54] greift zu kurz, da § 11 Abs. 3 S. 1 BDSG konkret an die Weisungsgebundenheit des Auftragnehmers anknüpft[55].

Es lässt sich somit nicht pauschal bestimmen, ob Datenübermittlungen an einen Onlinespeicher als Inanspruchnahme einer Auftragsdatenspeicherung anzusehen sind. Sind Cloud-Anwender und Cloud-Diensteanbieter bestrebt, den Cloud-Dienst so auszugestalten, dass er § 11 BDSG unterfällt, ist dies ohne weiteres möglich. Als „Dilemma des Cloud Computing“ wird hingegen der Umstand bezeichnet, dass das Machtgefälle zwischen Cloud-Diensteanbieter und Cloud-Anwender dem oftmals entgegensteht.[56]

#### 2.1.2.1.2.2 Software-as-a-Service

Moderne Cloud-Dienste bieten inzwischen Produkte an, die über bloßen Onlinespeicherplatz weit hinausgehen. So werden neben Daten auch Rechnerkapazität und andere Ressourcen vom Cloud-Anwender ausgelagert und aus der Cloud bezogen.[57] Auch der temporäre Bezug von Software über die Cloud hat sich inzwischen etabliert. Bei der als „Software-as-a-Service“ (SaaS) bezeichneten Cloud-Variante werden Anwendungen über das Internet bereitgestellt und können zumeist über den Webbrowser vom Cloud-Anwender bedient werden. Die so zur Verfügung gestellte Software ist lediglich auf der Infrastruktur des Cloud-Diensteanbieters

[47] Thalhofer, CCZ 2011, 222 (223).
[48] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 28.
[49] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 80; Schulz, MMR 2010, 75 (78).
[50] Holtorf, MPR 2013, 196 (197).
[51] Nägele/Jacobs, ZUM 2010, 281 (290); Schulz/Rosenkranz, ITRB 2009, 232 (235).
[52] Blume, CRi 2011, 76 (78); Weichert, DuD 2010, 679 (683).
[53] Holtorf, MPR 2013, 196.
[54] Jotzo, Der Schutz personenbezogener Daten in der Cloud, 2013, S. 81.
[55] Blume, CRi 2011, 76 (78).
[56] Schuster/Reichl, CR 2010, 38 (42).
[57] Grünwald/Döpkens, MMR 2011, 287; Nägele/Jacobs, ZUM 2010, 281.

installiert und wird beim Kunden nicht zwischengespeichert.[58] Das Modell bietet sich an, wenn Software nicht dauerhaft benötigt wird oder wenn die kollektive Bearbeitung von Dokumenten beabsichtigt ist.[59] Die Dateien, die mit derartigen Programmen erzeugt oder verarbeitet werden, werden ebenfalls auf dem Cloud-Server abgelegt.[60]

Auch SaaS-Dienste können Auftragsdatenverarbeitung sein.[61] Sie bieten jedoch oftmals nur geringfügige Anpassungsmöglichkeiten für die Cloud-Anwender,[62] sodass sie dann nicht als Verarbeitung im Auftrag eingestuft werden können. Davon abgesehen ist der Cloud-Anbieter, der eigene Dienstleistungen anbietet, oftmals selbst verantwortliche Stelle und nicht Datenverarbeiter im Auftrag.[63] Dies ist der Fall, wenn der Anbieter mit der Bereitstellung der Software auch für eigene Zwecke tätigt, um beispielsweise die Daten seiner Cloud-Anwender auszuwerten und daraus für das eigene Geschäft relevante Schlüsse zu ziehen.[64] Wie bereits dargelegt, hängt die Bewertung maßgeblich davon ab, ob der Cloud-Diensteanbieter eigene Aufgaben erfüllt oder fremde Aufgaben nach Weisung ausführt. Die Frage kann daher nicht pauschal für alle SaaS-Lösungen beantwortet werden.

#### 2.1.2.1.2.3 Überwachungspflicht des Auftraggebers

Sofern die oben genannten rechtlichen Hürden genommen sind und das Verhältnis zwischen Cloud-Anwender und Cloud-Diensteanbieter als Auftragsdatenverarbeitung klassifiziert werden kann, ist Übermittlung personenbezogener Daten in die Cloud zulässig. Verantwortliche Stelle ist dann noch immer der Cloud-Anwender, der die Daten lediglich an seinen verlängerten Arm weitergegeben hat. Daraus folgt, dass er auch nach der Weitergabe dafür zuständig ist, dass die Daten in der Cloud entsprechend der Regelungen des Datenschutzrechts behandelt werden. Etwaiges Fehlverhalten des Cloud-Diensteanbieters wird dem Cloud-Anwender dann zugerechnet.[65] Etwaige Schadenersatzansprüche Dritter richten sich dann gegen ihn. Er bleibt auch der Ansprechpartner für jegliche Ansprüche auf Löschung (§ 35 Abs. 2 BDSG), Berichtigung (§ 35 Abs. 1 BDSG), Sperrung (§ 35 Abs. 3 BDSG) und Auskünfte (§ 34 Abs. 1 BDSG).

##### 2.1.2.1.2.3.1 Regelmäßige Überprüfungen

Damit der Auftraggeber seiner Verantwortung nachkommen kann, ist er von Gesetzes wegen verpflichtet, den Auftragnehmer zu kontrollieren. § 11 Abs. 2 S. 4 BDSG verlangt von ihm, sich

---

[58] Grünwald/Döpkens, MMR 2011, 287.
[59] Schulz, MMR 2010, 75.
[60] Schulz, MMR 2010, 75 (78).
[61] Bergt, in: Taeger, Law as a Service (LaaS), S. 37/138; Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 6.
[62] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 7.
[63] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 8; Art. 29-Datenschutzgruppe, WP 179, S. 27.
[64] Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 22.
[65] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 84; s.a. Art. 29-Datenschutzgruppe, WP 196, S. 31.

regelmäßig von der Einhaltung der beim Arbeitnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Diese verpflichtende Kontrolltätigkeit erfordert wirkliche Recherchen. Es genügt nicht, sich auf Zusicherungen des Auftragnehmers zu verlassen.[66] Auch hier stellt sich das Problem, dass diese Überwachungsmaßnahmen bei weltumspannenden Großkonzernen faktisch nicht möglich sind.[67] Fehlt es an der erforderlichen Transparenz und Kooperation seitens des Cloud-Diensteanbieters, so kommt er als Auftragsdatenverarbeiter nicht in Frage.[68]

2.1.2.1.2.3.2 Zertifizierung

Eine Vor-Ort-Kontrolle hat der Gesetzgeber jedoch ausdrücklich nicht vorgeschrieben.[69] Sofern andere wirksame Möglichkeiten ergriffen werden als der persönliche Besuch im datenspeichernden Rechenzentrum, kann der Überwachungspflicht auch auf diese Weise begegnet werden. Zudem spricht von Gesetzes wegen zunächst nichts gegen eine Delegierung der Kontrolltätigkeiten. Ein Ausweg aus dem Dilemma der Unkontrollierbarkeit eines marktmächtigen Unternehmens kann deshalb die Zertifizierung seiner Dienstleistung durch eine unabhängige Stelle sein.[70] Den rechtlichen Anforderungen entspricht es beispielsweise, wenn sich der Auftraggeber der Datenverarbeitung einer vertrauenswürdigen Prüfinstanz bedient, die den Auftragnehmer überwacht. Der Prüfer kann auch die Tätigkeit für verschiedene Kunden bündeln, die denselben Cloud-Dienst nutzen.[71] Auf diese Weise können beispielsweise für einen Cloud-Dienst allgemeingültige Zertifizierungen beziehungsweise Gütesiegel vergeben werden, die jeder Auftraggeber des Dienstes als Bestandteil seiner Anbieterüberwachung heranziehen kann.

Solche Zertifizierungen werden von verschiedenen Institutionen angeboten. Selbstverständlich sollten Auftraggeber einer Auftragsdatenverarbeitung nur fachlich geeignete[72] und unabhängige[73] Stellen heranziehen. Bei kommerziellen Anbietern ist darauf zu achten, dass finanzielle Verflechtungen offengelegt sind und sich daraus keine Interessenskonflikte ableiten lassen.[74] Der Zertifizierung im staatlichen Rahmen wird nicht nur für gewöhnlich ein hohes Vertrauen entgegengebracht, sie bietet auch den Vorteil der wirtschaftlichen Unabhängigkeit.[75]

---

[66] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 9.
[67] Heidrich/Wegener, MMR 2010, 803 (806); Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 9.
[68] Vgl. Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 29.
[69] BT-Drs. 16/13657.
[70] Thalhofer, CCZ 2011, 222 (223); Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 26; Schuster/Reichl, CR 2010, 38 (42); Wedde, in: Däubler/Klebe/ders./Weichert, BDSG, § 11 Rn. 55; Weichert, DuD 2010, 679 (685).
[71] Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 12, 15.
[72] Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 13.
[73] Vgl. § 9a S. 1 BDSG.
[74] Weichert, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 13, Rn. 65.
[75] Bäumler, DuD 2004, 80 (82); CR 2001, 795.

So vergibt beispielsweise das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein das Datenschutz-Gütesiegel gemäß § 4 Abs. 2 LDSG SH an rechtskonforme Produkte.[76]

Neben der Wahl einer adäquaten Prüfinstanz ist darauf zu achten, dass die Zertifizierungskriterien ein angemessenes Niveau aufweisen.[77] Dabei gilt es, die Vielschichtigkeit von Cloud- und insbesondere SaaS-Architekturen im Blick zu behalten. Nicht nur der reine Vorgang der Datenspeicherung bedarf der Überprüfung durch den Auftraggeber einer Auftragsdatenverarbeitung. Komponenten des Cloud-Dienstes wie das Datenbankmanagement, die Datenverarbeitung über Applikationsserver und die Aufbereitung für den Cloud-Anwender (z.B. Webserver) werden unter Umständen von unterschiedlichen Akteuren an mehreren Orten betrieben und müssen jeweils kontrolliert werden. Gerade im Bereich des Cloud Computing bietet sich daher eine modulare Zertifizierung an, bei der jede Applikationsschicht einzeln betrachtet wird.[78] Auf diese Weise muss nicht jeder individuelle Service einzeln zertifiziert werden, wenn die jeweiligen Module, die den Gesamtservice bilden, jeweils bereits zertifiziert sind.[79]

Zu beachten ist, dass die Verwendung zertifizierter Cloud-Dienste den Auftraggeber bei seiner Überwachung zwar deutlich unterstützen kann. Es entbindet ihn jedoch nicht vollständig von seiner Verantwortlichkeit aus § 11 Abs. 2 S. 4 BDSG.[80] So muss er unter anderem sicherstellen, dass auch der Zertifizierer ordnungsgemäß arbeitet und den Anforderungen des Datenschutzrechts gerecht wird.[81] Zudem ist die Überprüfung durch einen Dritten stets nur eine Momentaufnahme,[82] die regelmäßig zu erneuern ist.[83]

2.1.2.1.2.3.3 Schriftliche Vereinbarung

Die Ausgestaltung der Überwachungspflicht muss in jedem Fall Gegenstand des Vertrages zwischen Auftraggeber und Auftragnehmer sein. Nach § 11 Abs. 2 S. 2 BDSG sind in die schriftlich zu schließende Vereinbarung zur Auftragsdatenverarbeitung eine Reihe von Angaben aufzunehmen. Dazu zählen:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

---

[76] Gegenstand der Beurteilung sind hingegen keine Verfahren, sodass kein kompletter Cloud-Dienst zertifiziert werden kann, sondern nur einzelne als Produkt abgrenzbare Komponenten.
[77] Meissner, DuD 2008, 525.
[78] Golland, Datenschutz-Berater 2014, 213.
[79] Dazu wesentlich die von Borges geleitete AG „Rechtsrahmen des Cloud Computing“, siehe Berthold/Borges/Cellarius/Dehmel/Doms, Trusted Cloud, Rechtsfragen des Cloud Computing Nr. 4, abrufbar unter http://www.trusted-cloud.de/369.php.
[80] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 9.
[81] Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 12 f.
[82] Weichert, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 13 Rn. 67.
[83] Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 14.

3. die zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die Überwachungspflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält sowie
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Unabhängig davon, wie viel Überwachung rechtlich geboten ist, sollte sie schon aus praktischen Gründen ernst genommen werden, um einer Haftung aus dem Wege zu gehen. Schließlich ist der Auftraggeber, wie sich aus § 11 Abs. 1 S. 1 BDSG ergibt, auch dann verantwortlich, wenn der Auftragnehmer sich vertrags- und rechtsbrüchig verhält und dadurch Dritte schädigt.[84]

#### 2.1.2.1.3 Weitere Rechtsvorschriften

Handelt es sich bei der Inanspruchnahme des Cloud-Dienstes nicht um eine Auftragsdatenverarbeitung, weil beispielsweise der Cloud-Diensteanbieter sich nicht den Weisungen des Cloud-Anwenders unterwirft, dann ist dieser Vorgang eine Funktionsübertragung.[85] Die datenschutzrechtlich verantwortliche Stelle ist dann der Cloud-Diensteanbieter. Jedoch benötigt der Cloud-Anwender für die Übermittlung personenbezogener Daten an den Cloud-Diensteanbieter auch hier eine Rechtsgrundlage. § 11 BDSG kommt dann nicht in Betracht.

Praktisch bedeutsame Vorschriften sind in den §§ 27 ff. BDSG zu finden. So erlaubt etwa § 27 Abs. 1 S. 2 BDSG pauschal die Datenverarbeitung, die ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Die Vorschrift gestattet Privatpersonen unter Umständen die Verarbeitung von Daten in einer Cloud. Hohe Relevanz weist ebenfalls § 32 Abs. 1 S. 1 BDSG auf. Die Vorschrift ermöglicht die Verarbeitung von Mitarbeiterdaten in einer Cloud, wenn dies zur Durchführung eines Beschäftigungsverhältnisses erforderlich ist. Dies kann der Fall sein, wenn etwa die Unternehmenskommunikation Cloud-basiert abläuft.[86]

---

[84] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 84; s.a. Art. 29-Datenschutzgruppe, WP 196, S. 31.
[85] Thalhofer, CCZ 2011, 222 (223).
[86] Zur Technik siehe Grünwald/Döpkens, MMR 2011, 287.

Beachtung finden sollte auch die Regelung des § 28 Abs. 1 S. 1 BDSG. Danach können personenbezogene Daten verarbeitet werden, wenn dies erforderlich für eine Vertragsdurchführung ist. Die Datenverarbeitung in einer Cloud erfolgt in der Praxis stets auf der Grundlage einer vertraglichen Beziehung zwischen dem Cloud-Anwender und dem Cloud-Diensteanbieter. Insofern dürfen personenbezogene Daten des Cloud-Anwenders durch den Cloud-Diensteanbieter verarbeitet werden. Festzuhalten ist jedoch, dass diese Erlaubnis ausschließlich auf das Verhältnis der beiden Vertragspartner beschränkt ist.[87] Personenbezogene Daten Dritter dürfen nicht auf dieser Grundlage in der Cloud abgelegt und dort verarbeitet werden.

Außerhalb von Konstellationen der Auftragsdatenverarbeitung ist damit keine Erlaubnis aus einer Rechtsvorschrift ersichtlich, welche die Einstellung personenbezogener Daten in eine Cloud rechtfertigt.

#### 2.1.2.1.4 Einwilligung

In Ermangelung einer gesetzlichen Grundlage als Rechtfertigung für Datenverarbeitungen in der Cloud kommt somit in vielen Fällen nur eine Einwilligung des Betroffenen in Betracht. § 4 Abs. 1 BDSG weist die Einwilligung als vollwertige Alternative zur Rechtsvorschrift aus.[88] Ist der Betroffene damit einverstanden, dass seine Daten in der Cloud gespeichert werden, kann er dies gegenüber dem Cloud-Diensteanbieter kundtun und so von seinem Recht auf informationelle Selbstbestimmung Gebrauch machen. Nicht erforderlich ist eine Einwilligung jedoch im Fall der Auftragsdatenverarbeitung.[89] Da in einer solchen Konstellation bereits mit § 11 BDSG eine Erlaubnisnorm besteht, besteht kein Bedarf für eine zusätzliche Einwilligung des Auftraggebers, die über die schriftliche Fixierung des Auftrags hinausgeht.

Die Einwilligung ist eine Einverständniserklärung, die der Betroffene vor Beginn der Datenerhebung oder –verarbeitung abgibt.[90] Eine nachträgliche (Genehmigung) oder zeitlich unbestimmte Zustimmung ersetzt nicht die vorweg abzugebende Einwilligung.[91] Ihre Anforderungen ergeben sich aus § 4a Abs. 1 BDSG. Danach muss die Einwilligung auf der freien Entscheidung des über die näheren Umstände informierten Betroffenen beruhen.

##### 2.1.2.1.4.1 Informierte Einwilligung

Den Betroffenen selbstbestimmt entscheiden zu lassen, wer welche seiner Daten verarbeitet, setzt voraus, dass er auch die dafür notwendigen Kenntnisse besitzt.[92] Eine Einwilligung ist nur dann gültig, wenn dabei klar ist, worin eingewilligt wird. Gerade bei technisierten Verfahren ist es alles andere als selbstverständlich, dass dem Cloud-Anwender klar ist, was eine Software mit seinen Daten unternimmt. Diese Unkenntnis geht nicht zu Lasten des Betroffenen. § 4a Abs. 1

[87] Thalhofer, CCZ 2011, 222 (223).
[88] Simitis, in: ders., BDSG, § 4 Rn. 6 ff.; 4a Rn. 1.
[89] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 112.
[90] Gola/Schomerus, BDSG, § 4 Rn. 15.
[91] Simitis, in: ders., BDSG § 4a Rn. 27, 29.
[92] Gola/Klug, Grundzüge des Datenschutzrechts, S. 49.

S. 2 BDSG weist demjenigen, der durch eine Einwilligung begünstigt wird, die Aufgabe zu, den Betroffenen über den Zweck der Datenverarbeitung zu informieren. Dazu gehört die gesamte beabsichtigte Verwendung.[93] Auch interner Datenverkehr ist offenzulegen.[94]

In der Praxis des Cloud Computing kann diese Information unter anderem in Form von Security-Service-Level-Agreements (SSLA) erfolgen.[95] Diese Vereinbarungen sind in der Regel als Allgemeine Geschäftsbedingungen an den §§ 305 ff. BGB. zu messen. Sie dürfen daher beispielsweise keine überraschenden Klauseln enthalten, mit denen der Cloud-Anwender nicht rechnen konnte. Bei teilweise verbreiteten Klauseln, nach denen sich Cloud-Diensteanbieter Zugriff oder gar Manipulation der Cloud-Anwenderdaten vorbehalten,[96] kann dies je nach Ausgestaltung der Klausel der Fall sein.

#### 2.1.2.1.4.2 Freiwillige Einwilligung

Wirksam sind gemäß § 4a Abs. 1 S. 1 BDSG zudem nur solche Einwilligungserklärungen, die auf der freien Entscheidung des Betroffenen beruhen. Diese Freiwilligkeit setzt zunächst die notwendige geistige Reife voraus, um die Tragweite einer datenschutzrechtlichen Einwilligung zu erfassen. Dies ist bei Kindern regelmäßig nicht der Fall. Eine feste Altersgrenze kann hier nicht festgemacht werden, sondern es bleibt bei der konkreten Einsichtsfähigkeit des jeweiligen Kindes.[97]

Freiwilligkeit setzt ferner voraus, dass die Entscheidung über die Einwilligung ohne direkten oder indirekten Zwang erfolgt.[98] Eine solche Zwangswirkung ist typischerweise bei Über- und Unterordnungsverhältnissen gegeben, wie sie beispielsweise in der Arbeitswelt existieren. Auch dann, wenn der Vorgesetzte keine verpflichtende Anweisung erteilt, sondern die Entscheidung über eine Einwilligung anheimstellt, steht der Arbeitnehmer oftmals unter einem zumindest psychischen Druck, der seiner Freiwilligkeit entgegensteht.[99] Die weiteren Bedingungen, unter denen die Freiwilligkeit gewahrt ist, sind umstritten.[100] Auch ausreichend hoher sozialer Druck im gesellschaftlichen oder privaten Umfeld kann somit beispielsweise der Wirksamkeit einer Einwilligung entgegenstehen.

Psychischer Druck kann zudem aus drohenden Kosten erwachsen. Willigt ein Betroffener in eine Datenverarbeitung nur deshalb ein, um damit finanzielle Nachteile abzuwenden, so tut er dies nicht freiwillig. Auch ausbleibende Gewinne können ein solcher Nachteil sein. Voraussetzung ist jedoch eine gewisse Erheblichkeit des Verlustes, damit von psychischem Druck gesprochen werden kann. Eng mit dieser Fallgruppe verwandt ist das sogenannte Koppelungsverbot aus

---

[93] Schaffland/Wiltfang, BDSG, § 4a Rn. 11; Simitis, in: ders., BDSG, § 4a Rn. 72.
[94] Gola/Schomerus, BDSG, § 4 Rn. 33; Klug, RDV 2001, 266; a.A. Schaffland/Wiltfang, BDSG, § 4 Rn. 14.
[95] Weichert, DuD 2010, 679 (680).
[96] Hansen, DuD 2012, 407 (411).
[97] Simitis, in: ders., BDSG, § 4a Rn. 20 f.
[98] Bizer, DuD 2007, 350 (351).
[99] Simitis, in: ders., BDSG, § 4a Rn. 62.
[100] Simitis, in: ders., BDSG, § 4a Rn. 62 m.w.N.

§ 28 Abs. 3b BDSG.[101] Danach darf der Abschluss eines Vertrages nicht an die Einwilligung in die Erhebung von Daten geknüpft werden, die für die Vertragsdurchführung nicht von Bedeutung sind.

#### 2.1.2.1.4.3 Widerrufliche Einwilligung

Die einmal erteilte Einwilligung muss nicht bis in alle Ewigkeit gelten, sondern kann jederzeit ohne Angabe von Gründen widerrufen werden. Die Datenverarbeitung ist dann einzustellen. Der Widerruf ist allerdings nur mit Wirkung für die Zukunft möglich.[102]

#### 2.1.2.1.4.4 Form der Einwilligung

Nach § 4a Abs. 1 S. 3 BDSG ist die Einwilligungserklärung schriftlich abzugeben. Von diesem Grundsatz bestehen jedoch zahlreiche Ausnahmen. Dies ist möglich, weil das Gesetz die Schriftform nur vorschreibt, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist." Wird beispielsweise in einem Gespräch eine eingriffsschwache, nicht sensible Datenverarbeitung thematisiert, so kann in dem Zusammenhang eine Einwilligung mündlich oder durch Kopfnicken erteilt werden. Ob diese Voraussetzungen gegeben sind, ist am konkreten Einzelfall zu beurteilen.

Auch im für das Cloud-Computing relevanten Bereich des elektronischen Geschäftsverkehrs sind solche besonderen Umstände anerkannt. Hier kann naheliegender Weise auch auf elektronischem Wege, also über das Internet, eine Einwilligung erteilt werden. Schließlich würde es der Praktikabilität des Onlinehandels entgegenstehen, wenn jeder Auftrag eine mit der Post zu versendende datenschutzrechtliche Einwilligungserklärung voraussetzen würde. Voraussetzung für eine wirksame Einwilligung ist zumindest ein aktives Handeln wie etwa das Setzen eines Häkchens.[103] Ein anderes Beispiel für aktives Handeln ist das bewusste Laden eigener Inhalte in einen Cloud-Speicher. Darin kann eine Einwilligung gesehen werden, dass die Daten dort auch gespeichert werden dürfen. Eine solche konkludente, nicht näher artikulierte Erklärung ist eng auszulegen. Das heißt, es darf nicht angenommen werden, dass die Einwilligung auch auf zweckwidrige Verarbeitungen wie beispielsweise für Werbung oder zur Weitergabe an Dritte von der Einwilligung umfasst sind.

Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, beispielsweise im Rahmen eines Vertragsabschlusses, so ist dies gesondert hervorzuheben, damit dem Unterzeichner klar wird, dass er mehrere Erklärungen abgibt. Dies folgt aus §§ 4a Abs. 1 S. 4, 28 Abs. 3a S. 2. Wird eine datenschutzrechtliche Einwilligungsklausel in das Kleingedruckte eines Vertrages eingefügt, ist sie nicht gültig.[104]

---

[101] Vgl. Däubler, in: ders./Klebe/Wedde/Weichert, BDSG, § 4a Rn. 24; Simitis, in: ders., BDSG, § 4a Rn. 63.
[102] Bizer, DuD 2007, 350 (351).
[103] Bizer, DuD 2007, 350 (351).
[104] Bizer, DuD 2007, 350 (351).

#### 2.1.2.1.5 Wartung von Cloud-Diensten

Besonderheiten gelten für die Wartung von Datenbanken oder Systemen, in denen personenbezogene Daten verarbeitet werden. Vielfach kann dabei nicht ausgeschlossen werden, dass der mit der Wartung betraute Administrator einzelne Datensätze zu Gesicht bekommt. Eine gesonderte Rechtsgrundlage ist jedoch nicht erforderlich, wenn es sich dabei um einen internen Vorgang der verantwortlichen Stelle handelt.[105] Die Maßnahme kann dann von der Vorschrift beziehungsweise der Einwilligung mit umfasst sein, nach der die eigentliche Datenspeicherung und -verarbeitung erlaubt ist.

Wird hingegen die Wartung von einer externen Stelle vorgenommen, ist darin eine Datenverarbeitung zu sehen, die einer Rechtsgrundlage bedarf. Eine solche ist in § 11 Abs. 5 BDSG zu finden. Danach ist die Wartung durch externe Dienstleister unter den Voraussetzungen der Auftragsdatenverarbeitung zulässig. Zwar handelt es sich bei der Wartung nicht um eine Auftragsdatenverarbeitung, weil in der Regel nur die technische Infrastruktur, nicht aber die einzelnen Datensätze betrachtet werden, die Wartung und die Auftragsdatenverarbeitung werden jedoch von Gesetzes wegen gleich behandelt.[106] Damit ist die Wartung durch Externe erlaubt, wenn sie auf Wartungsverträgen mit dem Inhalt nach § 11 Abs. 2 BDSG und der Auftraggeber unter anderem seiner Kontrollpflicht nachkommt.

### 2.1.3 Zweckbindung

Hat eine datenverarbeitende Stelle wie etwa ein Cloud-Diensteanbieter Daten auf rechtmäßige Weise, also aufgrund einer Rechtsvorschrift oder Einwilligung, erhoben, darf sie dennoch nicht frei darüber verfügen. Die datenverarbeitende Stelle darf die Daten nur zu dem Zweck verarbeiten, zu dem sie erhoben worden sind.[107] Dies ist der Zweck, auf den die Einwilligung oder die Rechtsvorschrift bezogen war. Wäre dies nicht so, wäre der Betroffene dem Risiko einer völligen Verwendungsfreiheit ausgeliefert, was dem Gedanken der informationellen Selbstbestimmung diametral entgegenstehen würde.[108] Das Zweckbindungsprinzip ist daher essentiell für ein effektives Datenschutzsystem.[109]

Möchte eine datenverarbeitende Stelle die ihr anvertrauten Daten zu einem anderen Zweck verwenden, gelten dieselben Regeln, die auch für die Erhebung galten. Sie benötigt dafür eine erneute Rechtsgrundlage in Form einer Rechtsvorschrift oder einer Einwilligung. Solche Rechtsvorschriften, die eine Zweckentfremdung ausnahmsweise erlauben, existieren beispielsweise zu Gunsten der wissenschaftlichen Forschung (§ 14 Abs. 2 Nr. 9 BDSG).

Eine wichtige Folge des Zweckbindungsprinzips ist die Verpflichtung der speichernden Stelle, die Daten nur solange aufzubewahren, wie dies zur Erfüllung des Zwecks erforderlich ist. Nicht

---

[105] Wedde, in: Däubler/Klebe/ders./Weichert, BDSG, § 11 R. 75.
[106] Gola/Schomerus, BDSG, § 11 Rn. 15.
[107] Gola/Klug, Grundzüge des Datenschutzrechts, S. 48.
[108] Engel, Reichweite und Umsetzung des Datenschutzrechts gemäß der Richtlinie 95/46/EG, S. 97; Simitis, in: ders., BDSG, § 4b Rn. 58.
[109] Schild, EuZW 1996, 549 (551).

mehr erforderlich sind Daten, wenn die Aufgabe, zu deren Erfüllung sie gespeichert waren, endgültig erledigt ist.[110] Kündigt beispielsweise ein Cloud-Anwender seinen Vertrag mit dem Cloud-Diensteanbieter, so verliert er typischerweise den Zugriff auf den Cloud-Speicher. Dann ist es nicht mehr erforderlich und deshalb auch nicht mehr zulässig, seine Daten weiterhin im Cloud-Speicher oder an anderer Stelle aufzubewahren. Sie sind dann zu löschen. Nicht nur Inhaltsdaten sind von dieser Verpflichtung betroffen. Werden beispielsweise die Zugriffe des Cloud-Anwenders auf Cloud-Dienste protokolliert, weil diese Informationen Relevanz für die Abrechnung haben, dann ist das Vorhalten der Protokolldaten nur erforderlich, solange die Abrechnung nicht erstellt wurde. Danach sind sie auch bei Fortbestehen des Vertrags zu löschen. Um die Einhaltung dieser Löschverpflichtungen zu gewährleisten, ist von der speichernden Stelle regelmäßig zu überprüfen, ob die weitere Speicherung noch erforderlich ist.

### 2.1.4 Datensparsamkeit und Anonymisierung

Aus dem Zweckbindungsprinzip ergibt sich, dass nur erforderliche Daten aufbewahrt werden dürfen. Die konsequente Fortführung dieses Gedankens führt zum Gebot der Datensparsamkeit.[111] Das in § 3a S. 1 BDSG festgeschriebene Rechtsinstitut verlangt, „so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen“. Dies bedeutet zum einen, dass nur die zur Aufgaben- beziehungsweise Vertragsdurchführung unbedingt erforderlichen Informationen erhoben werden dürfen. Zum anderen folgt daraus das sogenannte Need-to-know-Prinzip,[112] wonach nur diejenigen Mitarbeiter des datenverarbeitenden Unternehmens Zugriff auf die Cloud-Anwenderdaten haben dürfen, die ihn aufgrund ihrer Aufgabenstellung im Unternehmen benötigen.

Striktes datensparsames Verhalten hat zur Folge, dass nur dort mit personenbezogenen Daten gearbeitet werden muss, wo die Rückverfolgbarkeit der einzelnen Person von Bedeutung ist. Ist dies nicht der Fall, dürfen die entsprechenden Daten gar nicht erhoben werden. Bei bereits vorhandenen personenbezogenen Daten schreibt § 3a S. 2 BDSG für einen solchen Fall die Anonymisierung der Daten vor. Bei einer Anonymisierung wird der Personenbezug von Daten dauerhaft entfernt, sodass nicht mehr ermittelt werden kann, zu wem sie gehören. Sofern die Deanonymisierung tatsächlich niemandem mehr möglich ist, findet dann das BDSG auch keine Anwendung mehr.[113] Anonymisierte Informationen sind schließlich keine personenbezogenen Daten, sodass der Anwendungsbereich des Gesetzes nicht eröffnet ist.[114] Problematisch ist aber, dass mit dem technischen Fortschritt oder weiterer Verkettung möglicherweise ein Personenbezug herstellbar wird.[115] Für den klassischen Cloud-Speicher ist zudem die Anonymisierung keine Option. Damit ein Cloud-Anwender weiterhin Zugriff auf die ihm gehörigen Daten hat, müssen sie ihm zugeordnet bleiben. Dient eine Anwendung jedoch beispielsweise der Sammlung von Kundendaten, um diese zu Zwecken der Marktforschung

[110] Gola/Schomerus, BDSG, § 20 Rn. 11.
[111] Weichert, in: Kilian/Heussen, Computerrechts-Handbuch, Teil 13 Rn. 11.
[112] Parker, DuD 1991, 557; krit. Gilor, DuD 1991, 641.
[113] Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 128 ff.; Heidrich/Wegener, MMR 2010, 803 (806).
[114] Siehe oben S. 4.
[115] Roßnagel/Scholz, MMR 2000, 721 (726).

statistisch auszuwerten, so hat die Identität des Individuums keine Relevanz.[116] Ein solches System ist daher mit anonymen Daten zu betreiben.

Kann die Anonymisierung nicht erfolgen, weil die konkrete Aufgabe Daten mit Personenbezug erfordert, so kann für gewöhnlich eine Pseudonymisierung erfolgen. Ist sie möglich, ist sie aus Gründen der Datensparsamkeit auch geboten. Die Pseudonymisierung erfolgt, indem der Name des Betroffenen durch ein Kennzeichen ersetzt wird, um bei Bedarf die Identität offenzulegen.[117] Dies hat den Vorteil, dass ein Unbefugter Datensätze, an die er gelangt, niemandem zuordnen kann. Voraussetzung dafür ist natürlich, dass der Zuordnungsschlüssel an einem anderen Ort als die Inhaltsdaten gespeichert ist, also beispielsweise in einer anderen, physikalisch getrennten Cloud. Personenbezogene Daten sind es nach wie vor, da der Betroffene bestimmbar ist.[118] Die Regelungen des BDSG bleiben deshalb anwendbar. Optimaler Weise können die Daten so pseudonymisiert werden, dass nur der Betroffene zu einer Reidentifizierung in der Lage ist, indem selbstgenerierte Pseudonyme verwendet werden.[119] Zusätzliche Sicherheit verschaffen Einwegpseudonyme.[120]

### 2.1.5 Sensitive Daten

Wie eingangs dargestellt stehen alle personenbezogenen Daten unter dem Schutz des BDSG, unabhängig davon, ob sie besonders intimer Natur sind.[121] Einzelne Datenkategorien werden hingegen dennoch von Gesetzes wegen als besonders sensitiv angesehen. Diese „besonderen Arten personenbezogener Daten“ sind nach der Definition in § 3 Abs. 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Geraten derartige Informationen ohne den Willen des Betroffenen in die falschen Hände, so können daraus schwerwiegende Nachteile für ihn erwachsen. Solche Nachteile können im Einzelfall von der sozialen Ächtung bis hin zur politischen Verfolgung reichen.

Smart-Meter-Daten sind in der Regel nicht sensitiver Natur, können dies aber im Einzelfall sein. Es handelt sich um aktuelle Verbrauchsdaten einer Wohnung, beispielsweise für Strom, Wasser oder Erdgas, die in kurzen Zeitintervallen an den Versorger übermittelt werden.[122] Aus diesen lassen sich Informationen über den Tagesablauf der Bewohner der betreffenden Verbrauchsstelle ableiten.[123] Unter Umständen können diese Rückschlüsse auch die in § 3 Abs. 9 BDSG bezeichneten besonders schutzbedürftigen Kategorien betreffen. Verfügt ein Betroffener beispielsweise über verstärkten Harndrang, führt dies dazu, dass er zur Nachtzeit mehrfach das Licht in seiner Wohnung einschaltet und die Toilettenspülung betätigt. Dies kann anhand des Strom- und Wasserverbrauchs zur jeweiligen Uhrzeit nachvollzogen werden. In

[116] Dammann, in: Simitis, BDSG, § 3 Rn. 201 ff.; Wohlgemuth/Gerloff, Datenschutzrecht, Anm. 3.3.2.4.
[117] Wohlgemuth/Gerloff, Datenschutzrecht, Anm. 3.3.2.3.
[118] Weichert, in: Däubler/Klebe/Wedde/ders., BDSG, § 3 Rn. 14.
[119] AK Technik, Datenschutzfreundliche Technologien, S. 15.
[120] AK Technik, Datenschutzfreundliche Technologien, S. 15.
[121] Siehe oben S. 10 ff.
[122] Wiesemann, MMR 2011, 355 (356).
[123] Raabe/Lorenz/Pallas/Weis, Datenschutz im Smart Grid und der Elektromobilität, S. 7.

diesem Fall enthalten die Smart-Meter-Daten Angaben über die Gesundheit. In einem anderen Beispiel können möglicherweise Informationen über das Sexualleben einer alleine lebenden Person abgeleitet werden. Wenn die Verbrauchsdaten ergeben, dass sie – anders als sonst – spät heimgekehrt ist und am nächsten Morgen in der Wohnung zweimal geduscht wurde, ist dies ein Anhaltspunkt dafür, dass die Person die Nacht nicht alleine verbracht haben könnte.

Solche sensiblen Daten erfordern ein besonders hohes Schutzniveau. Dies folgt bereits aus dem Verhältnismäßigkeitsgrundsatz.[124] Auch das BDSG stellt für sensible Daten höhere Hürden auf. So gelten etwa besonders strenge Anforderungen an die Einwilligung zur Verarbeitung dieser Datenkategorien (§ 4a Abs. 3 BDSG). Bei der Datenverarbeitung ist dem Betroffenen ein besonderes Maß an Transparenz zuzugestehen.[125] Nicht zuletzt muss bei der Speicherung sensibler Daten anderer Personen mehr als sonst sichergestellt sein, dass unbefugter Zugriff ausgeschlossen ist.[126] Der erforderliche Grad dieser Gewährleistung kann beim Cloud Computing kaum erzielt werden.[127] Die Speicherung und Verarbeitung in der Cloud zeichnet sich dadurch aus, dass keine physische Trennung zwischen den Speicherbereichen einzelner Cloud-Anwender erfolgt, sondern die Trennung durch Virtualisierung erfolgt. Die hinreichende Sicherheit, dass die Vertraulichkeit und Integrität der sensiblen Daten gewährleistet ist, besteht dabei nach dem Stand der Technik nicht.[128]

Für Berufsgeheimnisträger wie Ärzte, Rechtsanwälte und Steuerberater gilt es zudem noch § 203 des Strafgesetzbuchs beachten. Danach machen sich die Mitglieder der Personengruppen strafbar, wenn sie die ihnen von ihren Patienten oder Mandanten anvertrauten Informationen an Dritte weitergeben. Dritte sind auch Cloud-Diensteanbieter, sodass die Auslagerung der Dateiverwaltung für diese Berufsgruppen erhebliche strafrechtliche Risiken birgt.[129] Selbst dann, wenn eine sichere, physikalische Trennung der Daten einzelner Mandanten gelingt, kann es rechtswidrig sein, dass die Daten die Praxis oder Kanzlei verlassen.

### 2.1.6 Vertraulichkeit und Integrität

Der für eine Datenverarbeitung Verantwortliche hat sicherzustellen, dass die Datensicherheit gewährleistet ist, also kein Unbefugter in das IT-System eindringen kann. Dies ist durch entsprechende technische und organisatorische Maßnahmen zu gewährleisten. Dazu zählt gemäß § 9 BDSG in Verbindung mit dessen Anlage unter anderem die Kontrolle von Zutritten, Zugängen, Zugriffen, Weitergaben, Eingaben, Aufträgen und Verfügbarkeiten.

Im Bereich des Cloud-Computing ergeben sich zahlreiche Bedrohungen, denen durch solche Maßnahmen zu begegnen ist. Als Gefährder kommen Außenstehende, Insider und Behörden in

[124] Siemen, Datenschutz als europäisches Grundrecht, S. 165 ff.
[125] Vgl. Simitis, in: ders., BDSG, § 4a Rn. 86 f.
[126] Schirmer, in: Roßnagel, Hdb Datenschutzrecht, Kap. 7.12 Rn. 81/84.
[127] Thalhofer, CCZ 2011, 222 (223).
[128] Leupold, in: ders., Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 27.
[129] Kroschwald, Wicker, CR 2012, 758.

Betracht.[130] Gefahren durch Außenstehende gehen vor allem von anderen Cloud-Anwendern aus. Da sich bei einer Virtualisierungslösung mehrere Kunden Speicherplatz und Rechnerleistung auf denselben Servern teilen,[131] sind ihre Daten untereinander besonders angreifbar.[132] Insider sind Mitarbeiter des Cloud-Diensteanbieters, Vertragspartner und andere mit generellem Zugang.[133] Hier sind insbesondere Administratoren der am Cloud-Dienst beteiligten Software- und Hardwareunternehmen zu nennen, die oft über großflächige Zugriffsberechtigungen verfügen. Der Zugang zu den gespeicherten Daten durch Behörden mittels hoheitlicher Verfügung aufgrund einer Eingriffsbefugnis zunächst rechtlich nicht problematisch.[134] Begehren staatlicher Stellen, die einer ausländischen Rechtsordnung angehören, kann jedoch nicht ohne weiteres gefolgt werden, sodass entsprechender Schutz gegen die zwangsweise Umsetzung bestehen muss.

#### 2.1.6.1 Anforderungen des Bundesverfassungsgerichts

Der Vertraulichkeit und Integrität informationstechnischer Systeme hat das Bundesverfassungsgericht im Jahr 2008 den Status als Grundrecht zuerkannt.[135] Als spezielle Ausprägung des Grundrechts auf informationelle Selbstbestimmung[136] schützt es denjenigen, der personenbezogene Daten auf einem informationstechnischen System ablegt davor, dass sich Dritte unbemerkt Zugriff darauf verschaffen. Die Besonderheit der wegweisenden Entscheidung besteht darin, dass nicht erst die mögliche Datenerhebung als Grundrechtseinschränkung angesehen wird. Das Gericht setzt bereits bei dem Eindringen in das IT-System an, das bereits in das Persönlichkeitsrecht des Betroffenen eingreift.[137] Bereits dann, wenn ein Unbefugter die Zugangssperren zu einem IT-System überwindet, ist dessen Vertraulichkeit nicht mehr gegeben.[138] Unabhängig davon, ob der Eindringling tatsächlich personenbezogene Informationen abgerufen hat, hindert nach der Rechtsprechung des Bundesverfassungsgerichts bereits die Möglichkeit hierzu den Betroffenen an seiner freien Persönlichkeitsentfaltung.[139] Der Integritätseingriff ist besonders gravierend, wenn er unbemerkt vom Betroffenen erfolgt.[140] Der Betroffene hat dann kaum eine Möglichkeit, ihn abzuwehren.[141] Zudem muss er, wenn er einzelne Eingriffe nicht bemerken kann, stets mit dem unsicheren Gefühl leben, dass seine Daten überwacht werden könnten. Dies ist bei Zugriffen auf

---

[130] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 30; Thalhofer, CCZ 2011, 222 (222, 225); vgl. Leupold, MMR 2014, 145.
[131] Grünwald/Döpkens, MMR 2011, 287; Nägele/Jacobs, ZUM 2010, 281.
[132] Heidrich/Wegener, MMR 2010, 803.
[133] Vgl. Chuvakin, Insider Attacks: The Doom of Information Security Methods to thwart insider attacks: products, techniques and policies, S. 2 f.
[134] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 32.
[135] BVerfGE 120, 274.
[136] Drallé, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2010, S. 42 f.
[137] Becker, in: Hill/Schliesky, E-Volution des Rechts- und Verwaltungssystems, 2010, S. 57 (64); Bäcker, in: Uerpmann-Wittzack, Das neue Computergrundrecht, 2009, 1 (9).
[138] Vgl. Leupold, in: ders., Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 28.
[139] BVerfGE 120, 247 (306 ff.).
[140] Hansen, DuD 2012, 407 (408).
[141] BVerfGE 120 274 (306).

informationstechnische Systeme in besonderem Maße problematisch, weil die Menge und Vielfalt der darauf gespeicherten Daten häufig eine umfassende Profilbildung infolge eines einzigen Erhebungsvorgangs ermöglicht.[142]

Ist die Vertraulichkeit eines IT-Systems nicht gesichert, kann auch die Unversehrtheit der darin verarbeiteten Daten nicht gewährleistet werden.[143] Dann muss damit gerechnet werden, dass der Eindringling gespeicherte Informationen unbefugt gelöscht, ergänzt oder verändert hat. Die Anwendbarkeit des Urteils auf die Datenspeicherung in der Cloud ist nicht unproblematisch. Dafür müsste es sich bei der Cloud um ein informationstechnisches System handeln. Das Bundesverfassungsgericht geht in seiner Entscheidung zunächst nur von eigener Hardware des Betroffenen aus, auf dessen Vertraulichkeit und Integrität er ein Recht hat. Das Gericht führt jedoch weiter aus, dass sich der grundrechtliche Schutz auch auf solche informationstechnischen Systeme erstreckt, die sich in der Verfügungsgewalt anderer befinden.[144] Voraussetzung dafür ist – nach Ansicht des Gerichts – dass es sich dabei um Systeme handelt, bei denen der Cloud-Anwender davon ausgehen kann, dass er alleine oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt.[145] Dies ist beim Computing für gewöhnlich nicht der Fall. Zum einen teilen sich verschiedene Cloud-Anwender Speicherplatz auf demselben Server, sodass es schon deshalb keinen einzelnen Cloud-Anwender gibt, der über das gesamte informationstechnische System verfügt. Zum anderen lassen sich internationale Großkonzerne, die Cloud Computing anbieten, selten ihre Kontrolle über die Datenverarbeitung nehmen.[146] Dieser enge Begriff des schutzwürdigen informationstechnischen Systems ist allerdings unter dem Einfluss moderner Technologien kaum noch haltbar. Das Bundesverfassungsgericht konnte bei der Urteilsfindung im Jahr 2008 noch nicht von der heute üblichen selbstverständlichen Nutzung von Clouds wie Festplatten ausgehen, bei der der Cloud-Anwender teilweise gar nicht merkt, dass seine Daten außerhalb seines Schutzbereichs gelangen.[147] Werden beispielsweise Daten des Mobiltelefons automatisch mit einem Cloud-Speicher synchronisiert, so entstünde eine massive Schutzlücke, wenn nur die auf dem Telefon abgelegten Daten schutzwürdig wären, nicht aber die in der Cloud befindlichen. Die Bestimmung der Reichweite eines im Grundgesetz nicht ausdrücklich verankerten Grundrechts hängt maßgeblich von der Bedrohungslage aus Sicht der betroffenen Bürger ab.[148] In der Cloud abgelegte Daten müssen daher ebenso unter Schutz stehen wie solche, die auf dem heimischen Rechner gespeichert sind.

---

[142] BVerfGE 120, 247 (323); Becker/Ambrock, JA 2011, 561 (566).
[143] Leupold, in: ders., Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 31.
[144] BVerfGE 120, 274 (315).
[145] BVerfGE 120, 274 (315).
[146] Siehe S. 7.
[147] Hansen, DuD 2012, 407 (408).
[148] Vgl. Eisenberg, Beweisrecht der StPO, Rn. 2541; Maunz/Dürig, GG, 71. EL 2014, Art. 11 Rn. 5; Pagenkopf, in Sachs, GG, Art. 11 Rn. 10/29.

#### 2.1.6.2 Technische und organisatorische Maßnahmen

Aus § 9 BDSG folgt die Notwendigkeit, technische und organisatorische Maßnahmen zu treffen, um die Vertraulichkeit und Integrität personenbezogener Daten in der Cloud zu gewährleisten. Die verfassungsrechtliche Verpflichtung aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme verstärkt diese Notwendigkeit zusätzlich.

Welche Maßnahmen genau zu treffen sind, um ein IT-System zu sichern, lässt sich nicht pauschal sagen. § 9 S. 2 BDSG erklärt dazu: „Erforderlich sind diese Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." Art und Umfang der Datensicherungsmaßnahmen sind demnach auf den konkreten Einzelfall zuzuschneiden.[149] Entscheidend ist, dass die Schutzwirkung der Maßnahme einen hinreichend großen Mehrwert aufweist, der den Aufwand rechtfertigt.[150] Ob dies der Fall ist, hängt zum einen vom der Wahrscheinlichkeit und der Intensität der Bedrohung ab. Zum anderen ist die konkrete Schutzbedürftigkeit der einzelnen gespeicherten Daten für die Beurteilung heranzuziehen.[151] Die Empfindlichkeit der Daten für den Betroffenen ist daher zentrales Kriterium für den Umfang der erforderlichen technischen und organisatorischen Maßnahmen.[152]

Smart-Meter-Daten enthalten im Wesentlichen die Verbrauchsdaten der jeweiligen Abnehmerstelle innerhalb der einzelnen Tarifzeiträume.[153] Isoliert betrachtet handelt es sich dabei um Daten mit sehr geringer Persönlichkeitsrelevanz. Problematisch ist jedoch, dass aufgrund der großen Datenmenge, die über eine Verbrauchsstelle zur Verfügung stehen, eine detaillierte Profilbildung der dort lebenden Menschen möglich ist.[154] An der Kombination aus Verbrauchsdaten und Zeitpunkt lassen sich verschiedenste Anhaltspunkte zu den Lebensgewohnheiten der Betroffenen ablesen.[155] So ist es beispielsweise möglich zu erkennen, wann eine Person morgens aufsteht, wann sie das Bett verlässt und wann sie ihren Tag beendet. Es ist auch möglich, präzise Rückschlüsse zu ziehen, wann und wie lange elektrische Geräte wie Fernseher, Computer und Herd genutzt werden. Neben dem Tagesablauf kann auch die Anzahl der im Haushalt lebenden Personen aus den Verbrauchsdaten abgelesen werden.[156] Smart-Meter-Daten ermöglichen damit einen sehr umfassenden und erstaunlich detaillierten Einblick in Wohnungen von Familien und damit in den Kernbereich der räumlichen Privatsphäre.[157]

---

[149] Gola/Schomerus, BDSG, § 9 Rn. 7; Kompetenzzentrum Trusted Cloud, Datenschutzrechtliche Lösungen für Cloud Computing, S. 12.
[150] Vgl. Nungesser, HessDSG, § 10 Rn. 8.
[151] Gola/Schomerus, BDSG, § 9 Rn. 9.
[152] Ambs, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 9 BDSG Rn. 2.
[153] Wiesemann, MMR 2011, 355 (356).
[154] Wiesemann, MMR 2011, 355 (356).
[155] Raabe/Lorenz/Pallas/Weis, Datenschutz im Smart Grid und der Elektromobilität, S. 7.
[156] Wiesemann, MMR 2011, 355 (356).
[157] Zur Bedeutung der Wohnung für die Privatsphäre s. Guttenberg, NJW 1993, 567; Papier, in: Maunz/Dürig, GG, Art. 13 Rn. 1; Zimniok, DÖV 1954, 392.

Die Brisanz der Erhebung von Smart-Meter-Daten liegt nicht nur in der möglichen Profilbildung. Sie ist auch deshalb so gravierend, weil Informationen unmittelbar aus der Wohnung der Betroffenen gewonnen werden. Die Wohnung eines Menschen ist nach Art. 13 Abs. 1 GG „unverletzlich". Dieses Grundrecht auf Schutz der räumlichen Privatsphäre[158] garantiert dem Einzelnen einen abgeschiedenen, elementaren Lebensraum zur freien Entfaltung der Persönlichkeit.[159] Unbeobachtet von Fremden soll jeder Mensch seine Wohnung als letzten Rückzugsraum empfinden dürfen, in dem er ganz er selbst sein kann. Diese besondere Privatsphäre ist auch ohne das physische Betreten verletzt, wenn durch technische Vorkehrungen eine Überwachung der Vorgänge in der Wohnung möglich wird.[160] Wenn intelligente Messgeräte Rückschlüsse auf den Tagesablauf der Bewohner einer Wohnung ermöglichen, müssen diese selbst an diesem geschützten Ort Beobachtung fürchten. Indem die Betroffenen dann gegebenenfalls ihr häusliches Verhalten anpassen, ist ihnen nicht einmal in der Wohnung mehr eine vollständig freie Persönlichkeitsentfaltung möglich.[161]

Unabhängig von der besonderen Sensibilität der Smart-Meter-Daten sind die intelligenten Messgeräte auch einer gesteigerten Missbrauchs- und Manipulationsgefahr durch Angriffe aus dem Netz ausgesetzt.[162] Diese können insbesondere auf die Fernabschaltungsfunktion der Geräte abzielen. § 14a EnWG sieht die Möglichkeit vor, über das Smart Meter die Stromzufuhr zur angeschlossenen Verbrauchsstelle werksseitig zu unterbrechen. Diese Maßnahme kann mit dem Kunden vertraglich vereinbart sein. So können sich etwa Tarife als wirtschaftlich erweisen, nach denen Elektrofahrzeuge automatisiert nur dann geladen werden, wenn der Energiepreis gerade niedrig ist. Zum anderen ist auch die Fernabschaltung bei Zahlungsverzug des Stromkunden denkbar, sodass in einem Prepaid-Modell erst wieder Energie geliefert wird, wenn ein entsprechendes Volumenpaket erworben wurde.[163] Die prinzipielle Möglichkeit, über das Smart Meter die Stromzufuhr zu einem Haushalt zu unterbrechen, kann auch durch Angreifer genutzt werden, sofern die Messgeräte vernetzt sind. Neben einem solchen gezielten Angriff ist auch das Abschneiden ganzer Stadtviertel oder Regionen von der Energieversorgung denkbar.[164] In diesem Szenario stünde nicht nur die regionale Wirtschaft vor massiven Einbrüchen, sondern auch Infrastrukturen wie die medizinische Versorgung könnten versagen.[165] Diese Gefahren, die von Terroristen, kriegsführenden Staaten oder einzelnen Internet-Kriminellen gleichermaßen ausgelöst werden könnten, erfordern eine besonders sichere Isolierung vernetzter Messgeräte.

Auch wenn für jede Cloud-Architektur für sich beurteilt werden muss, welche technischen und organisatorischen Maßnahmen im Einzelnen umgesetzt werden müssen, können allgemeine

---

[158] Papier, in: Maunz/Dürig, GG, Art. 13 Rn. 1.
[159] BVerfGE 51, 97 (110); 89, 1 (12); 103, 142 (150 f.).
[160] Fink, in: Epping/Hillgruber, GG, Art. 13 Rn. 8.
[161] Zum Anpassungsdruck infolge von Überwachung siehe BVerfGE 65, 1 (43); 69, 315 (349); BAG, MMR 2008, 777.
[162] Schaar, wiedergegeben in MMR-Aktuell 2011, 313869.
[163] Anderson/Fuloria, Who controls the offswitch?, S. 2 f.
[164] Vgl. Anderson/Fuloria, Who controls the offswitch?, S. 3.
[165] Anderson/Fuloria, Who controls the offswitch?, S. 1, 3.

Tendenzen aufgezeigt werden. Diese lassen sich anhand der jeweils durch sie geförderten Schutzziele kategorisieren, die die Art.-29-Gruppe der nationalen Datenschutzbeauftragten Europas für das Cloud Computing aufgestellt haben.[166] Neben den Schutzzielen der Vertraulichkeit und der Integrität des informationstechnischen Systems ist dabei an die Isolierung und die Revisionsfähigkeit zu denken.

#### 2.1.6.2.1 Vertraulichkeit

Mit dem Schutzziel der Vertraulichkeit wird die Anforderung beschrieben, dass nur Befugte Kenntnisse von personenbezogenen Daten erhalten dürfen.[167] Danach sind Angreifer von außen sowie Mitarbeiter eines Cloud-Dienstes oder einer vergleichbaren Einrichtung durch technische und durch organisatorische Maßnahmen von Zugriffen abzuhalten.[168] Auch ist dafür zu sorgen, dass kein Zugriff durch ausländische Behörden aus Staaten ohne angemessenes Datenschutzniveau erfolgt.[169]

Der anhand des jeweiligen Einzelfalls festzulegende erforderliche Grad an Vertraulichkeit kann unter anderem durch die Einhaltung der nachfolgenden Anforderungen erzielt werden.

Zunächst ist ein gewisses Maß an physischer Sicherung der Hardware vorzusehen, auf deren Speicher personenbezogene Daten gespeichert sind. Dazu zählt eine Überwachung des Gebäudes, in dem sie sich befindet. Regelungen zur Zugangsberechtigung sind nicht nur aufzustellen, sondern auch durch eine wirksame Zutrittskontrolle durchzusetzen, die automatisiert, mittels eines Schlüssels oder eines Pförtners geschehen kann.[170] In größeren Unternehmen ist das Ausstellen von Berechtigungsausweisen erforderlich.[171] Der Zutritt zu Speicherorten sensibler Daten sollte protokolliert werden.[172] Das Gebäude ist zusätzlich durch eine Alarmanlage zu überwachen.[173]

Parallel zur analogen Zutrittskontrolle sind auch die digitalen Zugriffe auf zu schützende Speicherorte zu beschränken und zu kontrollieren. Dies sollte mit Hilfe von Autorisierungsmechanismen und sicherer Authentifizierung erfolgen.[174]

Smart-Meter-Daten sind aufgrund ihrer hohen Persönlichkeitsrelevanz zu verschlüsseln.[175] Dies betrifft auf jeden Fall den Übertragungsvorgang,[176] jedoch empfiehlt sich auch die Kodierung

---

[166] Art. 29-Datenschutzgruppe, WP 136, Abschnitt III 3, Dok. F-EU 136, S. 17 ff.
[167] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 13.
[168] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 30.
[169] Art. 29-Datenschutzgruppe, WP 196, S. 7.
[170] Gola/Schomerus, BDSG, § 9 Rn. 22; Ernestus, in: Simitis, BDSG, § 9 Rn. 83.
[171] Gola/Schomerus, BDSG, § 9 Rn. 22.
[172] Ernestus, in: Simitis, BDSG, § 9 Rn. 83.
[173] Gola/Schomerus, BDSG, § 9 Rn. 22.
[174] Art. 29-Datenschutzgruppe, WP 136, S. 19.
[175] Wiesemann, MMR 2011, 355 (358).
[176] Bergt, in: Taeger, Law as a Service (LaaS), 2013, S. 37 (41).

ruhender Daten.[177] Zudem sollte die Kommunikation über einen sicheren Weg erfolgen.[178] Werden unverschlüsselte Daten etwa in einer Cloud gespeichert, senkt dies das Sicherheitsniveau erheblich ab, sodass an anderer Stelle besonders strenge technische und organisatorische Maßnahmen zu treffen sind. Optimalerweise erfolgt die Entschlüsselung erst auf dem Endgerät des Cloud-Anwenders[179] oder einer gesondert gesicherten Umgebung.[180] Ein sicherheitstechnisches Problem ergibt sich beim Cloud Computing daraus, dass der Cloud-Diensteanbieter teilweise auch die Daten bearbeiten muss, um beispielsweise ein Update einzuspielen.[181] Dazu benötigt er nach dem bisherigen Stand der Technik sehr häufig Zugriff auf unverschlüsselte Dateien. Die theoretisch denkbare Möglichkeit, verschlüsselte Daten zu bearbeiten,[182] ist technisch noch nicht ausgereift und kann daher noch nicht zum verpflichtenden Stand der Wissenschaft und Technik gezählt werden.

Das Vorhandensein einer Firewall im klassischen Sinne kann für den Betrieb eines Cloud-Systems nicht verlangt werden. Dies widerspräche dem Zweck des Cloud Computing, bei dem der Übergang zwischen internem und externem Netz verschwimmt.[183] Dennoch ist ein System zu etablieren, das Angriffe von Dritten über das Internet abwehrt. Der Betrieb einer Private Cloud, bei der jeder Cloud-Anwender über einen eigenen Server verfügt, ist hingegen über eine klassische Firewall zu sichern.[184] Da die Private Cloud wie ein normaler Online-Speicher zu bewerten ist, ergibt sich dies aus Gründen der Datensicherheit.

#### 2.1.6.2.2 Integrität

Mit dem Schutzziel der Integrität wird gefordert, dass die gespeicherten Datensätze authentisch, also vollständig und unverändert sind.[185] Dies betrifft freilich nicht die Bearbeitungen durch den Cloud-Anwender. Gefährdungen der Datenintegrität können hingegen zum einen von Softwarefehlern ausgehen. Zum anderen können unbefugte Dritte oder befugte Administratoren versehentlich oder absichtlich den Datenbestand manipulieren.[186] Fehlerhaft abgespeicherte Dateien sind eine unvermeidliche Begleiterscheinung der Datenverarbeitung. Aus der Unrichtigkeit der Daten ergibt sich ein Berichtigungsanspruch nach § 20 Abs. 1 S. 1 oder § 35 Abs. 1 S. 1 BDSG. Dies kann für die Betroffenen deshalb „existentiell wichtig“ sein, weil gespeicherte Informationen die Grundlage für eine Vielzahl von Entscheidungen darstellen.[187]Der wichtigste Schritt zur Wahrung der Datenintegrität ist die Sicherstellung ihrer

[177] Art. 29-Datenschutzgruppe, WP 136, S. 18.
[178] Art. 29-Datenschutzgruppe, WP 136, S. 19.
[179] Hansen, DuD 2012, 407 (409).
[180] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 26.
[181] Heidrich/Wegener, MMR 2010, 803 (804).
[182] Heidrich/Wegener, MMR 2010, 803 (806); Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 26
[183] Heidrich/Wegener, MMR 2010, 803 (804).
[184] Redeker, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Rn. 378.
[185] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 13.
[186] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 24.
[187] Gola/Schomerus, BDSG, § 20 Rn. 2.

Vertraulichkeit. Können keine unbefugten Dritten in ein IT-System eindringen, kann von ihnen keine Manipulationsgefahr ausgehen.[188] Deshalb sind zunächst alle oben genannten Maßnahmen zur Gewährleistung der Vertraulichkeit auch an dieser Stelle heranzuziehen. Zur Integritätswahrung sind zusätzliche Schritte zu unternehmen, um zu erkennen, ob und durch wen in der Vergangenheit Daten verändert wurden. Dazu zählt die Nutzung kryptographischer Authentifizierung, von Signaturen[189] und Prüfsummen.[190] Um nach einer nicht gewollten Datenveränderung die so gestörte Integrität wieder herzustellen, sind Datensicherungen durch den Cloud-Diensteanbieter erforderlich.[191] Regelmäßige Komplettsicherungen sind für datenverarbeitende Stellen verpflichtend.[192]

Ein weiteres, zur Wahrung der Unversehrtheit der Daten wichtiges Mittel ist die finale Umsetzung der durch den Cloud-Anwender gewollten Editierungen. Entscheidet sich beispielsweise ein Cloud-Anwender, eine bestimmte Datei zu löschen, so ist diese tatsächlich aus dem Speicher zu eliminieren. Möchte er seinen gesamten Account löschen, so sind alle seine Daten tatsächlich zu löschen. Es reicht nicht aus, dass der Cloud-Anwender lediglich den Zugriff auf die entsprechenden Daten verliert und er dazu verleitet wird, zu denken, die Daten seien gelöscht, weil er sie nicht mehr sieht. Weist er die Löschung an, so besteht von dem Moment an keine Einwilligung mehr für die weitere Aufbewahrung dieser Daten.[193] Diese Selbstverständlichkeit wird in der Praxis oftmals ignoriert. Insbesondere im Bereich der sozialen Netzwerke werden vom Cloud-Anwender vermeintlich gelöschte Daten und Konten häufig nicht endgültig gelöscht.[194]

#### 2.1.6.2.3 Isolierung

Das Schutzziel der Isolierung folgt aus der konsequenten Umsetzung des Zweckbegrenzungs-Erfordernisses.[195] Durch entsprechende technische und organisatorische Maßnahmen ist sicherzustellen, dass einzelne Akteure nur Zugang zu den Daten erhalten, die sie jeweils für die eigene Zweckerfüllung zwingend benötigen.[196] Das Schutzziel ist damit eng verwandt mit dem der Vertraulichkeit. Während es bei den Maßnahmen zur Wahrung der Vertraulichkeit primär darum geht, den Zugriff Unbefugter zu verhindern, steht an dieser Stelle das Bestreben im Focus, die Befugnis einzelner Akteure so eng wie möglich zu fassen. Dies betrifft erneut sowohl die Mitarbeiter des Cloud-Diensteanbieters als auch die verschiedenen Cloud-Anwender untereinander.

---

[188] Vgl. Leupold, in: Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 31.
[189] Art. 29-Datenschutzgruppe, WP 136, S. 18.
[190] Hansen, DuD 2012, 407 (409).
[191] Nägele/Jacobs, ZUM 2010, 281.
[192] Reiser, WM 1986, 1401 (1405).
[193] Weichert, SVR 2014, 241 (244).
[194] Schütze, ZD-Aktuell 2012, 03267.
[195] Siehe dazu oben S. 14.
[196] Art. 29-Datenschutzgruppe, WP 136, S. 19.

Das Erreichen des Ziels erfordert die Vergabe eng gefasster Rechte sowie die Etablierung einer regelmäßig zu überprüfenden Rechtekontrolle.[197] Umfassende Privilegien, etwa für einzelne Administratoren, die Zugriff auf alle in einer Cloud gespeicherten Daten haben, sind zu vermeiden.[198] Die Umsetzung einer strikten Rechtetrennung wird begünstigt durch die Etablierung getrennter Speicherbereiche und den Einsatz virtueller Maschinen. Vorteilhaft ist die Verteilung der Datensätze einer Person auf mehrere Clouds.[199] Dies kann beispielsweise durch die Verwendung sogenannter Hybrid Clouds erfolgen, bei der sensible Inhaltsdaten pseudonymisiert auf einem Cloud-Speicher abgelegt werden, während die zur Personenbestimmung notwendigen Daten in einer anderen Cloud abgelegt werden.[200] Akteure, die beispielsweise zur Wartungszwecken Zugriff auf die Daten jeweils einer Cloud haben, sehen dann jeweils nur wenig aussagekräftige personenbezogene Daten.

#### 2.1.6.2.4 Revisionsfähigkeit

Auch bei gewissenhafter Umsetzung der oben vorgeschlagenen Maßnahmen kann eine Verletzung der Vertraulichkeit und Integrität nicht vollständig ausgeschlossen werden. Wenn dies schon nicht möglich ist, soll zumindest erkennbar sein, ob ein Sicherheitsbruch stattgefunden hat.[201] Wenn zusätzlich noch ermittelt werden kann, von wem dieser ausging, geht davon eine abschreckende Wirkung aus, die das Sicherheitsniveau von IT-Systemen erhöht.[202] Das Wissen, jederzeit identifiziert werden zu können, führt regelmäßig zu einem rechtskonformeren Verhalten.[203] Aus diesem Grund wird das Schutzziel der Revisionsfähigkeit zur Förderung der Vertraulichkeit und Integrität herangezogen.[204] Darunter wird die Fähigkeit verstanden, im Nachhinein zu ermitteln, was eine Entität zu einem bestimmten Zeitpunkt gemacht hat.[205] Konkret soll nachvollziehbar sein, wer wann welche personenbezogenen Daten in welcher Weise verändert hat.[206] Neben dem Abschreckungseffekt dienen die entsprechenden Maßnahmen auch dem Nachweis, dass die erforderlichen Maßnahmen getroffen wurden, um datenschutzrechtliche Anforderungen umzusetzen.[207]

Revisionsfähigkeit wird im Wesentlichen erzielt durch die Protokollierung sicherheitsrelevanter Vorgänge.[208] Dazu zählen vor allem die Bearbeitung und Löschung von Dateien, Logins und

---

[197] Art. 29-Datenschutzgruppe, WP 136, S. 19.
[198] Art. 29-Datenschutzgruppe, WP 136, S. 19.
[199] Bedner/Ackermann, DuD 2010, 323; Hansen, DuD 2012, 407 (409).
[200] Heidrich/Wegener, MMR 2010, 803 (804).
[201] Federrath/Pfitzmann, DuD 2010, 704.
[202] Hansen, DuD 2012, 407 (409).
[203] Ernestus, in: Simitis, BDSG, § 9 Rn. 138.
[204] Art. 29-Datenschutzgruppe, WP 136, S. 20; AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 24.
[205] Art. 29-Datenschutzgruppe, WP 136, S. 20.
[206] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 13.
[207] Art. 29-Datenschutzgruppe, WP 173, Abs. 28, S. 10; dies., WP 136, S. 21.
[208] Hansen, DuD 2012, 407 (409).

Programmabrufe.[209] Die Protokollierung muss revisionssicher sein[210] und auch tatsächlich regelmäßig ausgewertet werden.[211] Dabei ist zu beachten, dass es sich auch bei den Protokolldaten um aussagekräftige personenbezogene Daten handelt, deren Erzeugung, Aufbewahrung und Auswertung im Einklang mit dem Datenschutzrecht erfolgen muss.[212]

Von der Protokollierung unabhängig wird die Revisionsfähigkeit gesteigert durch die Festlegung interner Verfahren zur effektiven Handhabung und Meldung von Sicherheitsverstößen[213] sowie die Bestellung eines Datenschutzbeauftragten und anderer für Datenschutz und Datensicherheit zuständiger Personen.[214]

#### 2.1.6.3 Trusted Virtual Domains (TVDs) als Vertraulichkeit und Integrität fördernde Komponente

Eine Möglichkeit Vertraulichkeit und Integrität der Datenverarbeitung zu fördern, ergibt sich durch die Implementierung von TVDs. Eine TVD ist eine Anordnung mehrerer virtueller Maschinen, die im Verkehr untereinander vertrauen und dabei gleiche Sicherheitsanforderungen auch auf physikalisch getrennten Plattformen ausführen. Dadurch wird es ermöglicht, mehrere voneinander getrennte Prozesse beispielsweise in verschiedenen Domänen mit unterschiedlichen Anforderungen an Sicherheitsebenen auf einer gemeinsamen physikalischen Plattform auszuführen.[215] Damit auf die Daten auf einer TVD trotz der gemeinsamen Nutzung von physikalischen Strukturen nur von Autorisierten zugegriffen werden kann, erfolgt auf logischer Ebene eine strikte, kryptographisch abgesicherte Trennung. Zudem werden Daten auf externen, beispielsweise mobilen, Datenträgern noch zusätzlich verschlüsselt und können nur innerhalb der zugeordneten TVD entschlüsselt werden. [216]

Die genannten Vorteile von TVDs unterstützen im Zusammenspiel mit anderen technischen und organisatorischen Maßnahmen mehrere Bereiche der in der Anlage zu § 9 BDSG geforderten Kontrollmaßnahmen.

Die Zugriffskontrolle in Nr. 3 der Anlage zu § 9 BDSG regelt die Gewährleistung, dass ein für die Datenverarbeitungsanlage Berechtigter ausschließlich innerhalb seiner Zugriffsberechtigung auf unterliegende Daten zugreifen kann und damit personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

---

[209] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 24.
[210] Hansen, DuD 2012, 407 (409).
[211] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 24
[212] Hansen, DuD 2012, 407 (409).
[213] Art. 29-Datenschutzgruppe, WP 173, Abs. 41.
[214] Art. 29-Datenschutzgruppe, WP 173, Abs. 41.
[215] Catuogno et al., DuD 2010, 289.
[216] Catuogno et al., DuD 2010, 290.

Die Weitergabekontrolle in Nr. 4 der Anlage zu § 9 BDSG regelt die Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. TVDs gewährleisten Nr. 3 und 4 der Anlage zu § 9 BDSG durch logische Trennung und kryptographische Absicherung.

Das Trennungsgebot in Nr. 8 der Anlage zu § 9 BDSG fordert die zweckbestimmte Verarbeitung auf technisch sichere Art. Dabei kann eine softwareseitige Trennung wie bei TVDs im Einzelfall ausreichend sein bzw. eine physikalische Trennung ist nicht immer erforderlich.[217]

Satz 3 der Anlage zu § 9 BDSG setzt als eine Maßnahme zur Zugriffskontrolle und Weitergabekontrolle insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren fest. Dabei sagt der Begriff „Stand der Technik entsprechenden Verschlüsselungsverfahren“ aus, „dass fortschrittliche Verfahren gemeint sind, die sich in der Praxis bewährt haben und einen hohen Sicherheitsstandard gewährleisten“.[218] Zwar bezieht sich der Wortsinn lediglich auf die Verschlüsselung als solche, jedoch lässt sich in der Gestaltung die gesetzgeberische Zielsetzung eines technisch vermittelten hohen Datensicherheits- und damit Datenschutzniveaus ablesen.

Zwar sind aus rechtlicher Sicht grundsätzlich nur die technischen und organisatorischen Maßnahmen zu treffen, die auch erforderlich sind, wobei Erforderlichkeit den Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck meint, § 9 BDSG. Jedoch kann die Verwendung einer sicherheitserhöhenden innovativen Technik auch als eine rechtlich ein Stück zukunftssicherere Lösung empfehlenswert sein. Denn der Stand der Technik ist ein zeitlich bezogener terminus technicus.[219] Ein Vorgreifen des zukünftig zu erwartenden Schutzniveaus erspart also im Einzelfall gegebenenfalls Nachbesserungen.

### 2.1.7 Transparenz

Um die benötigte Flexibilität einer Cloud-Computing-Lösung zu erzielen, werden die Daten eines Cloud-Anwenders für gewöhnlich auf mehrere Serverfarmen verteilt.[220] Es ist üblich, dass diese Rechenzentren über den Globus verteilt sind und sich die Speicherorte im Verlauf eines Tages mehrfach ändern. Da dies unter Beteiligung von Unterauftragnehmern geschieht, können in der Praxis sogar die Cloud-Diensteanbieter oftmals nicht nachvollziehen, wo die Daten eines Kunden aktuell gespeichert sind.[221] Für die Cloud-Anwender bedeutet diese Ungewissheit einen vollständigen Kontrollverlust über seine Daten, der mit dem Datenschutzrecht nicht vereinbar

[217] Gola/Schomerus, § 9, Rn. 29.
[218] BT-Drs. 16/13657, S. 23.
[219] Ernestus, in: Simitis, BDSG, § 9 Rn. 171.
[220] Nägele/Jacobs, ZUM 2010, 281.
[221] Nägele/Jacobs, ZUM 2010, 281 (289).

ist.[222] Das Recht verlangt, dass die Erhebung und Verarbeitung personenbezogener Daten gegenüber dem Betroffenen transparent erfolgen muss.[223] Dieser Grundsatz manifestiert sich unter anderem in den Benachrichtigungs- und Auskunftspflichten der §§ 33 f. BDSG.

Für die Cloud-Diensteanbieter bedeutet dies, dass sie in der Lage sein müssen, ihren Kunden zumindest auf Anfrage die konkreten Speicherorte und die involvierten Unterauftragnehmer und sonstigen Dienstleister mitzuteilen.[224] Dies erfordert im Vorfeld entsprechende Dokumentationen und Protokollierungen.[225] Zudem ist nach § 42 Abs. 1 BDSG jeder Betroffene über Sicherheitsbrüche beim Cloud-Diensteanbieter zu informieren, durch den seine personenbezogenen Daten Dritten unrechtmäßig zur Kenntnis gelangt sind. Das kann unter anderem in Fällen von Hacking, technischem Versagen oder Verlust von Hardware der Fall sein.[226]

Hilfreich bei der Herstellung von Transparenz ist die Zertifizierung durch eine dritte Stelle.[227] Erworbene Gütesigel können dem Betroffenen als Auskunftsquelle über die Verarbeitungsmethoden und -orte dienen, derer sich ein Cloud-Anbieter bedient.

### 2.1.8 Intervenierbarkeit

Stellt der Cloud-Anwender infolge der erfolgreichen Umsetzung des Transparenzerfordernisses fest, dass über ihn gespeicherte Daten in der Form nicht gespeichert werden dürfen, so benötigt er Mechanismen, um diesen Missstand zu beheben. Aus § 35 BDSG folgen die Betroffenenrechte auf Berichtigung, Löschung und Sperrung der personenbezogenen Daten. Das Recht auf Berichtigung betrifft Fälle, in denen Daten erfasst wurden, die inhaltlich falsch sind. Wurden Daten rechtswidrig erhoben oder besteht kein Anlass zur weiteren Aufbewahrung, weil beispielsweise der Erhebungszweck nicht mehr erreicht werden kann, wird das Recht auf Löschung relevant. Ist das Bestehen eines Löschungsanspruchs umstritten oder besteht eine Aufbewahrungspflicht für die betroffenen Daten,[228] so tritt an die Stelle der Löschung die Sperrung.

Für den Betreiber eines IT-Systems folgt aus diesen Betroffenenrechten die Pflicht, entsprechenden Ersuchen unverzüglich nachzukommen. Er darf keine Hürden durch Technik oder Verfahren aufstellen oder die Rechte vertraglich abbedingen.[229]

---

[222] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 28.
[223] Bizer, DuD 2007, 350 (353).
[224] Art. 29-Datenschutzgruppe, WP 196, S. 13; AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 9.
[225] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 23.
[226] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 29.
[227] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 23; Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 26.
[228] Dies kann u.a. steuerrechtliche Gründe haben.
[229] Art. 29-Datenschutzgruppe, WP 196, S. 20.

## 2.2 Telekommunikationsrecht

Neben dem im BDSG verankerten Datenschutzrecht kann der Betrieb von IT-Systemen noch weitere Rechtsbereiche berühren. Dazu zählen vor allem das Telekommunikations- und das Telemedienrecht. Handelt es sich bei der Cloud etwa um einen Telekommunikationsdienst, so hat der Cloud-Diensteanbieter zusätzlich die Vorschriften des Telekommunikationsgesetzes (TKG) zu befolgen.

### 2.2.1 Anwendbarkeit des Telekommunikationsrechts

Das TKG ist anwendbar, wenn die Cloud ein Telekommunikationsdienst im Sinne von § 3 Nr. 24 ist. Diese sind im Gesetz definiert als „Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen“. Die Flexibilität eines Cloud-Systems wird durch Datenübertragungen erzielt. Sowohl die Verbindung zwischen dem Cloud-Anwender und der Cloud als auch der Austausch zwischen mehreren genutzten Servern, die gemeinsam die Cloud bilden, erfolgt über leitungsgebundene Netze. Dennoch werden Cloud-Dienste nicht als Telekommunikationsdienste angesehen, weil die Datenübertragung nur als Nebenleistung angesehen wird.[230] Die zahlreichen Datentransfers, die im Hintergrund einer solchen Anwendung ablaufen, sind aus Cloud-Anwendersicht schließlich nicht entscheidend.[231] Für den Cloud-Anwender steht der Erwerb von Speicherkapazität im Vordergrund.[232] Je nach Ausgestaltung des Services kann es auch der Erwerb von Rechnerleistung oder Software sein. Wie der Cloud-Diensteanbieter es technisch umsetzt, diesen Dienst an den Cloud-Anwender zu übermitteln, ist für Letzteren von untergeordneter Bedeutung, solange er die Leistung zum vereinbarten Preis bekommt. Cloud-Systeme werden deshalb für gewöhnlich nicht als Telekommunikationsdienste angesehen, sodass das TKG nicht auf sie anwendbar ist.

In Ausnahmefällen kann eine Cloud allerdings so gestaltet sein, dass die Übertragung von Signalen aus der Cloud-Anwendersicht gegenüber den sonstigen Services überwiegt. Dies kann etwa in der Variante der Communication-as-a-Service (CaaS) der Fall sein, bei der eine Verwaltung der Unternehmenskommunikation per Email, Voice-over-IP oder auf ähnlichem Wege in die Cloud integriert ist.[233] In diesem speziellen Fall ist es die Kommunikation – also die Datenübertragung – die beim Cloud-Anwender im Fokus steht. Zudem greift das Telekommunikationsrecht dann, wenn der Cloud-Diensteanbieter zugleich der Internet-Provider des Cloud-Anwenders ist.[234]

### 2.2.2 Regelungen des Telekommunikationsrechts

Das Telekommunikationsrecht ist historisch gewachsen aus dem einstigen Monopol der Post im Telefonbereich.[235] Entsprechend liegt der inhaltliche Schwerpunkt des TKG auf der Telefonie,

---

[230] Heidrich/Wegener, MMR 2010, 803 (805); Schuster/Reichl, CR 2010, 38 (42).
[231] Grünwald/Döpkens, MMR 2011, 287 (288); Schuster/Reichl, CR 2010, 38 (43).
[232] Heidrich/Wegener, MMR 2010, 803 (805); Schuster/Reichl, CR 2010, 38 (42).
[233] Grünwald/Döpkens, MMR 2011, 287 (288).
[234] Grünwald/Döpkens, MMR 2011, 287 (288); Schuster/Reichl, CR 2010, 38 (42 f.).
[235] Scheurle, in: ders./Mayen, TKG, Einf. Rn. 12.

sodass Regelungen enthalten sind, die nur Telefonanbieter betreffen, etwa bezüglich Telefontarifen und Telefonnummern. Die meisten Regelungen sind jedoch technikneutral zu verstehen.[236] Die nachfolgend dargestellten Vorschriften betreffen deshalb auch Cloud-Diensteanbieter.

#### 2.2.2.1 Meldepflicht

Der Betrieb eines Telekommunikationsdienstes ist in Deutschland gemäß § 6 Abs. 1 TKG meldepflichtig. Wer einen solchen Dienst auf dem Markt anbieten möchte, muss der Regulierungsbehörde die Aufnahme des Services schriftlich mitteilen. Die Behörde nimmt den Anbieter daraufhin in ihr veröffentlichtes Verzeichnis auf (§ 6 Abs. 4 TKG).

#### 2.2.2.2 Fernmeldegeheimnis

Der Betreiber eines Telekommunikationsdienstes hat das in § 88 Abs. 1 S. 1 TKG verankerte Fernmeldegeheimnis zu wahren. Es betrifft nach der gesetzlichen Definition „den Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war“. Nicht nur Telefonanbieter unterliegen der Pflicht, das Fernmeldegeheimnis zu wahren. So sind auch die Inhalte eines Dateiaustauschs zwischen Computern umfasst,[237] unter anderem über Voice-over-IP-Technologie.[238] In der Folge darf der Cloud-Diensteanbieter, wenn er dem TKG unterliegt, die von den Cloud-Anwendern in der Cloud gespeicherten Daten nicht einsehen.[239] Diesem Grundsatz, der auch schon aus der im allgemeinen Datenschutzrecht verankerten Pflicht zur Datensparsamkeit folgt, ist bei Betreibern von Anlagen, die unter das TKG fallen, besonders strikte Beachtung beizumessen. So ist zwar der für die Sicherheit des Systems erforderliche Administratorzugriff nach wie vor möglich, um etwa die Cloud-Anwenderdaten auf Virenbefall zu überprüfen,[240] jedoch sind an die Beurteilung der Erforderlichkeit strenge Maßstäbe zu setzen.

#### 2.2.2.3 Verkehrsdatenspeicherung

§ 96 Abs. 1 TKG reglementiert den Umgang mit Verkehrsdaten. Darunter sind nach der gesetzlichen Definition unter anderem Angaben über die an einer Kommunikationsverbindung beteiligten Anschlüsse, Beginn und Ende sowie übermittelte Datenmengen zu verstehen, mithin die Informationen über die technischen Rahmenbedingungen. Diese dürfen durch den Anlagenbetreiber nur ausnahmsweise erhoben werden und sind nach Beendigung des Dienstes zu löschen. Das TKG sieht jedoch einzelne Ausnahmen vor, die eine zeitweise Aufbewahrung von Daten dieser Art ermöglichen. Sofern kein Flatrate-Tarif besteht, können nach § 97 TKG die für die Entgeltabrechnung erforderlichen Daten gespeichert werden. Ist ein Einzelverbindungsnachweis vom Cloud-Anwender gewünscht, versetzt § 99 TKG den Cloud-Diensteanbieter in die Lage, die entsprechenden Verbindungsdaten zu speichern, um diesen

---

[236] Schmitz, in: Stelkens/Bonk/Sachs, VwVfG, § 2 Rn. 146.
[237] Bock, in: Geppert/Schütz, TKG, § 88 Rn. 12; Wuermeling/Felixberger, CR 1997, 230 (233)
[238] BfDI, 20. Tätigkeitsbericht, S. 143.
[239] Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, Rn. 3.
[240] Schmidl, MMR 2005, 343 (344); Hoeren, NJW 2004, 3513 (3516).

erstellen zu können. § 100 TKG ermächtigt zudem den Cloud-Diensteanbieter zur Erhebung und kurzfristigen Speicherung der Verkehrsdaten, um Störungen und Missbrauch an der TK-Anlage zu begegnen. Auf dieser Grundlage dürfen nach überwiegender Ansicht etwa IP-Adressen maximal 7 Tage lang gespeichert werden.[241] Weitere Nutzungen der Verkehrsdaten wie etwa die Analyse zu Marktforschungszwecken sind nur nach entsprechender Einwilligung der betroffenen Cloud-Anwender möglich. Diese Nutzung des Telekommunikationsdienstes darf nach § 95 Abs. 5 TKG nicht an die Erteilung dieser Einwilligung gekoppelt werden.

## 2.3 Telemedienrecht

Während das Telekommunikationsrecht die technische Seite von Internet und Kommunikationsverbindungen regelt, finden sich im Telemedienrecht Vorschriften hinsichtlich der Inhalte, die über solche Technologien ausgetauscht werden.[242] Beim Telemedienrecht steht somit nicht die Transportleistung von Informationen im Vordergrund, sondern der transportierte Inhalt.[243] Das Rechtsgebiet ist im Telemediengesetz (TMG) geregelt.

### 2.3.1 Anwendbarkeit des Telemedienrechts

Nach der Definition in § 1 Abs. 1 S. 1 greift das TMG für alle elektronischen Informations- und Kommunikationsdienste, soweit diese keine Telekommunikations- oder Rundfunkdienste sind. Ob Cloud-Computing als Informations- und Kommunikationsdienst einzustufen ist, ist in der Rechtswissenschaft umstritten. Vielfach wird die Anwendung des TMG mit der Begründung abgelehnt,[244] dass es am dafür erforderlichen informativen beziehungsweise kommunikativen Element fehlt.[245] Diese Begriffe sind jedoch sehr weit zu verstehen.[246] Kommunikation ist zumindest dann gegeben, wenn ein Dateiaustausch stattfindet,[247] also wenn mehrere Personen oder Geräte auf einen Cloud-Speicher zugreifen.[248] Dient eine Plattform zudem nicht nur der reinen technischen Abwicklung beispielsweise der Speicherung, sondern bietet sie auch einen inhaltlichen Service, so handelt es sich zudem um einen Informationsdienst. Bei Software-as-a-Service-Lösungen kann grundsätzlich auch eine solche inhaltliche Leistung erbracht werden, sodass es sich dann um Telemedien handelt.[249] Im Vordergrund steht bei solchen Diensten nicht die Datenübermittlung, sondern die online bereitgestellte Software, die inhaltlichen Charakter hat. Für die meisten Cloud-Lösungen stellt das TMG deshalb ein zentrales Regelwerk dar.

---

[241] BGH NJW 2014, 2500 (2501 ff.); Graf, in: ders., BeckOK StPO, § 96 TKG, Rn. 3b; a.A. Breyer, MMR 2011, 573 (575); Karg, MMR 2011, 341 (346).
[242] Vgl. Sieber/Höfinger, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Rn. 32.
[243] Hoeren, NJW 2007, 801 (802).
[244] Nägele/Jacobs, ZUM 2010, 281 (290); Schuster/Reichl, CR 2010, 38 (42).
[245] Schuster/Reichl, CR 2010, 38 (42).
[246] Altenhain, in: Joecks/Schmitz, MüKo StGB, § 1 TMG Rn. 10; Müller-Broich, TMG, § 1 Rn. 6.
[247] Martiny, in: Säcker/Rixecker, MüKo BGB, § 3 TMG Rn. 8.
[248] Vgl. Heidrich/Wegener, MMR 2010, 803 (805).
[249] Bedner, Cloud Computing, S. 116; Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 51; Opfermann, ZEuS 2012, 121 (131).

## 2.3.2 Regelungen des Telemedienrechts

### 2.3.2.1 Zulassungs- und Anmeldefreiheit

Telemediendienste sind nach § 4 TMG zulassungs- und anmeldefrei. Anders als Telekommunikationsdienste oder Rundfunksender[250] können Sie von jedermann betrieben werden, ohne dass dies zuvor einer Behörde angezeigt werden muss.

### 2.3.2.2 Impressum

§ 5 TMG schreibt das Vorhandensein eines Impressums in Telemedien vor. Diese Pflicht betrifft nicht nur Websites und andere redaktionelle Plattformen, sondern auch beispielsweise Software, die dem TMG unterfällt, wie beispielsweise Apps für Mobiltelefone.[251] Damit ist auch eine SaaS-Lösung mit einem Impressum zu versehen. Zu beachten ist, dass das Impressum vom Benutzer jederzeit ohne wesentliche Zwischenschritte zu erreichen sein muss.[252] Ein längeres Suchen ist ihm nicht zuzumuten.[253] Bei Websites wird verlangt, dass das Impressum jederzeit durch maximal zwei Klicks auf Links erreichbar sein muss.[254] Dies lässt sich bei der graphischen Oberfläche einer Software nicht immer benutzerfreundlich umsetzen. Daher wird es als zulässig angesehen, einen Verweis auf das Impressum im Hauptmenü der Software zu integrieren.[255] Der Verweis hat eine eindeutige Bezeichnung wie „Impressum“ oder „Kontakt“ zu tragen.[256] Soweit sich in einzelnen Bereichen bestimmte Begrifflichkeiten eingebürgert haben, können diese in dem Bereich ebenfalls verwendet werden.[257] Beispielsweise hat sich bei Software der Begriff „Über“ als Link zu Versionsnummer und Herstellerangaben etabliert. Ob allerdings der oftmals verwendete Ort des Menüpunkts „Über“ als Unterpunkt der Kategorie „Hilfe“ für die Orientierung des Nutzers ausreicht, ist sehr fraglich.

### 2.3.2.3 Providerhaftung für Nutzerinhalte

Die §§ 7-10 TMG regeln, wer die Verantwortung dafür trägt, wenn Nutzer rechtswidrige Informationen in ein Telemedium einbringen. Die Gründe, warum die Veröffentlichung einer Information nicht gesetzeskonform ist, können vielfältig sein. So kann die Verfügbarmachung von Daten etwa gegen Urheberrechte, Ehrschutz oder behördliche Anordnungen verstoßen oder als öffentliche Anstiftung, Drohung oder Verunglimpfung gar strafrechtlich relevant sein. Verantwortlich ist in so einem Fall natürlich derjenige, der die Daten produziert und publik gemacht hat. Rechtlich problematischer ist die weitergehende Frage, ob auch den Betreiber der Plattform eine Verantwortlichkeit trifft, die der Nutzer zur Veröffentlichung genutzt hat. Neben Websites mit entsprechender Interaktionsmöglichkeit wie soziale Netzwerke kommen auch

---

[250] Müller-Broich, TMG, § 4 Rn. 1.
[251] Ewald, in: Baumgartner/Ewald, Apps und Recht, Rn. 168.
[252] OLG Hamburg, GRUR-RR 2003, 92.
[253] BT-Drucks. 14/6098, 2.
[254] Müller-Broich, TMG, § 5 Rn. 17.
[255] Hoffmann, MMR 2013, 631(633).
[256] BGH MMR 2007, 40 (41); OLG Hamburg, MMR 2003, 105.
[257] KG Berlin, GRUR-RR 2007, 326; Müller-Broich, TMG, § 5 Rn. 18.

Cloud-Plattformen in Betracht, auf denen mehrere Personen Daten ablegen und abrufen können.

§ 10 S. 1 TMG bestimmt hierzu, dass Plattformbetreiber keiner Haftung für fremde Informationen unterliegen, die sie für einen Nutzer speichern, solange sie keine Kenntnis von den rechtswidrigen Informationen haben beziehungsweise die betreffenden Daten nach Kenntniserlangung unverzüglich löschen oder sperren. Dies bedeutet, wie auch § 7 Abs. 2 S. 1 TMG klarstellt, dass die Betreiber nicht verpflichtet sind, die auf ihren Plattformen gespeicherten fremden Inhalte einer systematischen Kontrolle zu unterziehen. Dieses sogenannte Providerprivileg gilt jedoch nur für fremde Informationen der Nutzer. Dies ist der Fall, wenn die Speicherung vom Nutzer veranlasst wurde,[258] also nicht aus eigenem Antrieb des Providers.[259] Lädt also ein Nutzer Daten von seinem lokalen Rechner in einen Cloud-Speicher, so bleibt er auch der alleinige Verantwortliche für damit möglicherweise einhergehende Rechtsbrüche, solange dem Cloud-Diensteanbieter davon nichts bekannt ist. Ist der Nutzer hingegen Teilnehmer eines Cloud-basierten Mess- und Speichersystems für seinen Stromverbrauch, bei dem sein Stromzähler automatisch Messdaten in eine Cloud-Architektur sendet, so fehlt es an der Veranlassung des Nutzers. Diese Daten sind dann für den Betreiber des Systems keine fremden, sondern eigene Informationen. Er kann sich deshalb nicht auf das Providerprivileg des § 10 S. 1 TMG berufen.

Ausnahmsweise kann der Dienstanbieter auch für ihm fremde Nutzerdaten verantwortlich sein, wenn er sie sich zu eigen gemacht hat.[260] Dies ist der Fall, wenn er sich mit den Inhalten derart identifiziert, dass nach außen hin erkennbar ist, dass er Verantwortung für sie übernehmen möchte.[261] Dies kann etwa geschehen durch eine Kommentierung oder Bearbeitung des fremden Inhalts. Die Information wird dann als eigener Inhalt behandelt.[262]

#### 2.3.2.4 Datenschutz

Der Abschnitt 4 des TMG behandelt den Datenschutz im Verhältnis zwischen dem Anbieter und dem Nutzer von Telemedien. Die Grundsätze weichen nicht von denen des BDSG ab. Teilweise sind im TMG jedoch bereichsspezifische Konkretisierungen der allgemeinen Datenschutzregeln zu finden.

In § 12 finden sich zunächst die aus dem BDSG bekannten[263] Institute des Verbots mit Erlaubnisvorbehalt (Abs. 1) und der Zweckbindung (Abs. 2).

Da das TMG elektronische Medien behandelt, ermöglicht § 13 Abs. 2 sinnvollerweise die Erteilung einer Einwilligung in elektronischer Form anstatt wie das BDSG grundsätzlich die

[258] Altenhain, in: MüKo StGB, § 10 Rn. 4; Liebau, Jura 2006, 520 (525); Spindler, in: Spindler/Schmitz/Geis, TDG, § 11 Rn. 7.
[259] Heckmann, Internetrecht, Kap. 1.10 Rn 9.
[260] BT-Drs. 14/6098, S. 23; BGH GRUR 2004, 860; Müller-Broich, TMG, § 10 Rn. 2.
[261] Vgl. Müller-Broich, TMG, § 7 Rn. 2.
[262] Heckmann, Internetrecht, Kap. 1.7 Rn. 11 i.V.m. Kap. 1.10 Rn. 9.
[263] Siehe oben Kap. 2.1.2 und 2.1.3.

Schriftform zu verlangen.[264] Dabei bestimmt das Gesetz, dass eine solche Einwilligungserklärung bewusst abgegeben werden muss, protokolliert wird sowie jederzeit abrufbar und widerruflich ist.

Eine besondere Form der Nutzerinformation sieht § 13 Abs. 1 TMG vor. Danach ist dem Nutzer, dessen Daten erhoben werden, zu Beginn des Nutzungsvorgangs eine Datenschutzerklärung über Art, Umfang und Zwecke der Erhebung zur Verfügung zu stellen. Auch über Datenverarbeitungen außerhalb der Europäischen Union ist dabei zu informieren. Nach § 15a TMG ist der Nutzer schließlich im Nachhinein zu informieren, wenn ein Sicherheitsbruch zu unrechtmäßiger Kenntniserlangung der personenbezogenen Daten geführt hat.

§ 13 Abs. 4 TMG sieht schließlich einen bereichsspezifischen Katalog für technische und organisatorische Maßnahmen vor, die dem Datenschutz dienen. Danach ist sicherzustellen, dass der Nutzer jederzeit den Dienst beenden kann und seine Daten dann rückstandslos gelöscht werden. Zudem ist es dem Nutzer zu ermöglichen, das Telemedium gegen Kenntnisnahme Dritter geschützt in Anspruch zu nehmen und wenn möglich anonym zu bleiben oder ein Pseudonym zu verwenden. Eine Verkettung der Inhaltsdaten mit denen anderer hat ebenso zu unterbleiben wie eine Verknüpfung mit den Bestandsdaten, die die Identität des betreffenden Nutzers beinhalten.

#### 2.3.2.5 Sonstige Regelungen

Sofern Telemedien Werbung enthalten, ist diese so zu integrieren, dass sie als solche erkennbar ist (§ 6 TMG). Dies kann insbesondere durch die graphische Gestaltung oder eine entsprechende eindeutige Überschrift geschehen.

§ 14 TMG sieht die Bestandsdatenauskunft vor, die es Behörden im Einzelfall ermöglichen kann, die Identitäten anderer Nutzer zu erfahren. Teilweise sind auch Urheber berechtigt, eine Bestandsdatenauskunft zu erhalten, um ihre Rechte am geistigen Eigentum durchzusetzen.

[264] Siehe oben Kap. 2.1.2.1.4.4.

# 3 Internationale rechtliche Anforderungen

Ein wesentlicher Grund für den wirtschaftlichen Erfolg des Cloud Computing besteht darin, dass es nicht an geographische Grenzen gebunden ist.[265] Die Technologie ermöglicht die kostensparende Verteilung von Rechnerleistung auf Standorte in unterschiedlichen Ländern.[266] Auf diese Weise können Kapazitäten aus Rechenzentren bezogen werden, die in dem Moment schwach ausgelastet sind, weil an dem Ort beispielsweise Nacht- oder Ferienzeit herrscht.[267] Zudem kann primär auf Gebiete mit niedrigem Lohnniveau zurückgegriffen werden, was die Betriebs- und Wartungskosten senkt. Da die Kosten für den Datenaustausch im weltumspannenden Internet ebenso wie der durch die Übermittlung hervorgerufene Zeitverlust in der Regel nicht ins Gewicht fallen, ist es in technischer Hinsicht belanglos, in welchem Staat und auf wie viele Staatenverteilt die Daten gespeichert sind.[268]

In rechtlicher Hinsicht ist die Auslagerung von Rechenkapazität und Speicherplatz in das Ausland hingegen mit gravierenden Folgen verbunden. Der Betroffene sieht sich dann mit unterschiedlichen Rechtsregelungen konfrontiert, die ihm oftmals nur wenige Rechte einräumen, mit denen er seine informationelle Selbstbestimmung wahren kann.

## 3.1 Datenschutzrechtliche Anforderungen

Betroffenenrechte lassen sich zunächst aus dem Datenschutzrecht ableiten, das sowohl in Deutschland als auch in der Europäischen Union vom Territorialitätsprinzip geprägt ist.[269] Dies bedeutet, dass die datenschutzrechtliche Verantwortlichkeit sich nach dem Recht des Staates richtet, in dem die Daten verarbeitet werden.[270] Damit ist der Sitz des Cloud-Anbieters maßgeblich, an dem dessen Server stehen oder andere wesentliche Verarbeitungsschritte erfolgen.[271] Ist das Intervall, in dem die Daten an einen neuen Speicherort transferiert werden, sehr kurz, weil beispielsweise schon kurzfristige schwache Auslastungen einzelner Rechenzentren ausgenutzt werden, wechselt das anwendbare Recht ebenso zügig. In solch einem Fall ist es für den Betroffenen kaum möglich, stets nachzuvollziehen, wo seine Daten sich befinden, sodass im Zweifel gar kein anwendbares Recht ausgemacht werden kann.[272]

Um dem drohenden Kontrollverlust der Betroffenen zu begegnen, wurden in § 4b BDSG Regelungen aufgenommen, die Datenübermittlungen ins Ausland beschränken. Die

---

[265] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 9.
[266] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 118.
[267] Grünwald/Döpkens, MMR 2011, 287.
[268] Hansen, in: Borges/Schwenk, Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, S. 79 (79); Heidrich/Wegener, MMR 2010, 803 (806).
[269] Nägele/Jacobs, ZUM 2010, 281 (289).
[270] Nägele/Jacobs, ZUM 2010, 281 (289); Niemann/Paul, K&R 2009, 444 (448).
[271] Hansen, DuD 2012, 407 (410).
[272] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 27; Nägele/Jacobs, ZUM 2010, 281 (289 f.).

Voraussetzungen unterscheiden sich danach, ob es sich um Datenaustausch innerhalb der Europäischen Union handelt oder ob der Datenstrom den Binnenmarkt verlässt.

### 3.1.1 Übermittlungen innerhalb der Europäischen Union

#### 3.1.1.1 Zulässigkeit nach § 4b Abs. 1 BDSG

Das europäische Datenschutzrecht ist durch die EG-Datenschutzrichtlinie vollharmonisiert.[273] Dies bedeutet, dass den einzelnen Mitgliedstaaten nur ein geringer Umsetzungsspielraum bleibt. Die jeweiligen nationalen Rechtsakte zum Datenschutz entsprechen sich somit inhaltlich im Wesentlichen.[274] In sämtlichen Rechtsordnungen der EU ist beispielsweise der jeweils identisch definierte Personenbezug von Daten Grundvoraussetzungen für deren Schutz[275] und es existieren einheitliche Verantwortlichkeitsregelungen.[276] Zwar divergieren teilweise einzelne Detailregelungen, etwa zu Erhebungsbefugnissen oder dem Schutz sensibler Daten.[277] Die EG-Datenschutzrichtlinie gibt jedoch einen Mindeststandard vor, der nicht unterschritten werden darf und daher ein gemeinsames Schutzniveau liefert, das alle datenverarbeitenden Stellen in der EU einzuhalten haben.[278] Der Betroffene kann sich demnach auch darauf einstellen, europaweit relativ einheitliche Schutzrechte zur Wahrung seiner informationellen Selbstbestimmung vorzufinden. Deswegen werden Datenübermittlungen innerhalb des europäischen Wirtschaftsraums durch § 4b Abs. 1 BDSG mit reinen Inlands-Übermittlungen gleichgestellt.[279] Der Europäische Wirtschaftsraum umfasst alle Staaten der EU sowie Island, Liechtenstein und Norwegen.[280]

Für Clouds im innereuropäischen Raum ergeben sich daher keine rechtlichen Besonderheiten.[281] Der grenzüberschreitende Datenfluss ist grundsätzlich zulässig. Auch die Regelungen über die Auftragsdatenverarbeitung finden Anwendung.[282] Wichtig ist jedoch, dass nicht nur die beteiligten Server innerhalb des Europäischen Wirtschaftsraums belegen sind, sondern sämtliche Datenverarbeitungen auf diesem Gebiet stattfinden. Auf diese Weise können die Rechtsunsicherheiten vermieden werden, die regelmäßig zu erwarten sind, wenn eine Cloud teilweise in Drittstaaten betrieben wird.[283] Für den Anwender einer Cloud ist es empfehlenswert, den Cloud-Diensteanbieter vertraglich dazu zu verpflichten, ausschließlich europäische

---

[273] EuGH, verb. RS. C-468/10 und C-469/10, EuZW 2012, 37; Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 35.
[274] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 10.
[275] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 6.
[276] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 33.
[277] Vgl. Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 20.
[278] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 8.
[279] Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 4 Rn. 2; Gola/Schomerus, BDSG, § 4 Rn. 3.
[280] Brechmann, in: Calliess/Ruffert, EUV/AEUV, Art. 48 AEUV Rn. 5.
[281] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 10; Opfermann, ZEuS 2012, 121 (139); Thalhofer, CCZ 2011, 222 (223).
[282] Jotzo, Datenschutz in der Cloud, S. 147.
[283] Siehe unten S. 34 ff.

Ressourcen zu verwenden.[284] Dies gilt erst recht, wenn er als Auftraggeber einer Auftragsdatenverarbeitung für die Einhaltung der Betroffenenrechte vollständig verantwortlich ist.[285]

#### 3.1.1.2 Anwendbares Datenschutzrecht

Wie oben ausgeführt[286] richtet sich das anwendbare nationale Datenschutzrecht nach dem Territorialitätsprinzip,[287] folgt also aus dem Sitz der datenverarbeitenden Stelle.[288] Für rein europäische Sachverhalte wird das Territorialitätsprinzip allerdings durch das Niederlassungsprinzip modifiziert.[289] In Art. 4 Abs. 1 lit. a) S. 2 der EG-Datenschutzrichtlinie heißt es dazu: „Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält.“ Entscheidend ist danach weder der Unternehmenssitz noch der Ort der physischen Verarbeitung.[290] Vielmehr ist das Recht einzuhalten, das am Ort der Niederlassung oder gegebenenfalls der verschiedenen Niederlassungen gilt. Verarbeitet beispielsweise ein dänisches Unternehmen Daten deutscher Kunden, so kann es dies nach seinem heimischen dänischen Recht tun. Bestellt der deutsche Kunde hingegen bei einer in Deutschland gelegenen Filiale des dänischen Unternehmens, so sind auch die Standards nach deutschem Recht einzuhalten.[291] Die Folge des Niederlassungsprinzips ist also oftmals die parallele Anwendung verschiedener mitgliedstaatlicher Datenschutzgesetze.[292] Praktische Schwierigkeiten ergeben sich daraus aufgrund der harmonisierten Datenschutzstandards kaum.

Der Begriff der Niederlassung umfasst zwei Mindestkomponenten. Zunächst ist eine feste Einrichtung notwendig, das Unternehmen muss in dem Land also über Räumlichkeiten verfügen.[293] Hinzu kommt die tatsächliche Ausübung der unternehmerischen Tätigkeit in dem Land, sodass sogenannte Briefkastenfirmen keine Niederlassungen sind.[294] Reisen also deutsche Unternehmer ins europäische Ausland, um dort Kundendaten in ihren von Deutschland aus betriebenen Cloud-Speicher einzuspeisen, so fehlt es an einer festen Einrichtung im Ausland.[295] Andersherum reicht ein Serverstandort im Ausland auch noch nicht aus, um dort eine Niederlassung zu betreiben. Entscheidend ist gemäß der E-Commerce-

---

[284] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 10; Niemann/Hennrich, CR 2010, 686 (692).
[285] Zur Verantwortlichkeit in Auftragsdatenverarbeitungs-verhältnissen siehe oben S. 9 ff.
[286] Siehe oben S. 32.
[287] Nägele/Jacobs, ZUM 2010, 281 (289).
[288] Hansen, DuD 2012, 407 (410).
[289] Thüsing/Pötters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 14 f.
[290] Jotzo, Datenschutz in der Cloud, S. 124.
[291] Beispiel nach Jotzo, Datenschutz in der Cloud, S. 124.
[292] Thüsing/Pötters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 17.
[293] Fröhle, Web Advertising, Nutzerprofile und Teledienstedatenschutz, S. 146 f.
[294] Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 4 Rn. 3.
[295] Vgl. Jotzo, Datenschutz in der Cloud, S. 127.

Richtlinie der Ort, an dem der Verantwortliche seine wirtschaftliche Tätigkeit erbringt.[296] Darunter ist der Ort zu verstehen, an dem Menschen Tätigkeiten ausüben.[297] Dies folgt aus dem Zweck des Niederlassungsprinzips: Nur ein echtes Büro beziehungsweise eine tatsächliche Filiale schafft schutzwürdiges Vertrauen. Wird etwa ein deutscher Kunde von in Deutschland operierenden Mitarbeitern betreut, geht er zu Recht davon aus, dass ihnen anvertraute Kundendaten auch nach deutschen Standards verarbeitet werden.[298] Die Auslagerung einzelner Cloud-Server in das EU-Ausland führt daher nicht zwangsläufig zur Anwendung des ausländischen Datenschutzrechts.

### 3.1.2 Übermittlung in Drittstaaten

Besondere praktische Relevanz liegt im interkontinentalen Cloud Computing, da Cloud-Diensteanbieter aus Kostengründen oder zur Sicherung der ständigen Verfügbarkeit[299] oftmals Ressourcen im nicht-europäischen Ausland in ihre Architektur einbeziehen.[300] Außerhalb des Europäischen Wirtschaftsraums gespeicherte Daten unterliegen jedoch in der Regel nicht dem Schutz der EG-Datenschutzrichtlinie beziehungsweise ihrer Umsetzungsgesetze, sondern der Rechtsordnung des Empfängerstaates.[301] In Europa erhobene personenbezogene Informationen dürfen deshalb nicht ohne weiteres in außereuropäische Drittstaaten transferiert werden. Ansonsten könnte das in der EU garantierte Recht des Einzelnen auf Wahrung seiner informationellen Selbstbestimmung durch Auslagerung der Datenspeicherung in andere Regionen ausgehöhlt werden.[302]

Aus diesem Grund ist die Datenübermittlung in Drittstaaten an besondere Anforderungen geknüpft, die sich aus § 4b BDSG ergeben. Diese nachfolgend dargestellten Voraussetzungen sind zusätzlich zu den ohnehin geltenden Anforderungen des BDSG zu erfüllen. So erfordert jegliche Verarbeitung personenbezogener Daten etwa weiterhin eine Rechtsgrundlage und muss den üblichen Anforderungen an Zweckbindung, Datensparsamkeit usw. gerecht werden.[303] So ist beispielsweise die Auslandsübermittlung eine weitere Verarbeitung neben der Erhebung und der Benutzung. Dafür wird in der Regel eine Einwilligung des Betroffenen benötigt, weil die die Tatbestände des § 28 BDSG nicht greifen.[304]

#### 3.1.2.1 Gewährleistung eines angemessenen Schutzniveaus

Übermittlungen in Drittstaaten dürfen nach § 4b Abs. 2 S. 2 BDSG nur erfolgen, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist und der Betroffene auch darüber hinaus kein gegenläufiges schutzwürdiges Interesse hat. Das Erfordernis des

---

[296] Erwägungsgrund 19 der Richtlinie 2000/31/EG.
[297] Dammann, in: Simitis, BDSG, § 1 Rn. 203; Jotzo, MMR 2009, 232 (235).
[298] Jotzo, Datenschutz in der Cloud, S. 128.
[299] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten, S. 21.
[300] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 37.
[301] Stenzel, ZFAS 2010, 137 (139).
[302] Tamm, VuR 2010, 215 (217).
[303] Siehe oben S. 14 f.
[304] Nägele/Jacobs, ZUM 2010, 281 (290).

angemessenen Schutzniveaus stellt auch Art. 25 Abs. 1 der EG-Datenschutzrichtlinie auf, sodass es auch in den übrigen Mitgliedstaaten eine Grundvoraussetzung an Drittstaatenübermittlungen darstellt. Bei der Prüfung des angemessenen Schutzniveaus ist zweistufig vorzugehen:[305] Zunächst ist zu untersuchen, ob der rechtliche Schutz personenbezogener Daten in dem Empfängerstaat generell hinreichend ist. Sofern dies nicht der Fall ist, gilt es zu prüfen, ob im konkreten Fall anderweitige Maßnahmen getroffen wurden, um einen angemessenen Schutz der zu übermittelnden Daten im Ausland zu erzielen.

#### 3.1.2.1.1 Allgemeines Schutzniveau

Die Bewertung des im Empfängerstaat vorherrschenden Schutzniveaus setzt eine komplexe Analyse unter Berücksichtigung aller relevanten Umstände voraus.[306] Erforderlich ist nicht, dass dort mit dem EU-Datenschutzrecht identische Regelungen vorherrschen, sondern auch abweichende Konzepte zur Sicherung der Privatheit sind möglich.[307] Von entscheidender Bedeutung ist es dabei, dass wesentliche Kerngedanken des europäischen Datenschutzes vergleichbar geregelt sind, darunter etwa Zweckbestimmung, Verhältnismäßigkeit, Transparenz, Datensicherheit und Betroffenenrechte.[308]

Weder Cloud-Diensteanbieter noch Cloud-Anwender eines Cloud-Dienstes sind praktisch in der Lage, die erforderliche Analyse selbständig vorzunehmen. Abhilfe können zum Teil die förmlichen Beurteilungen der Europäischen Kommission schaffen, die zu einzelnen Staaten bereits gefasst wurden. Auf der Grundlage von Art. 25 Abs. 4 bzw. Abs. 6 der EG-Datenschutzrichtlinie kann das Unionsorgan verbindlich feststellen, ob ein untersuchter Staat ein angemessenes Schutzniveau aufweist. Die Entscheidung bindet sämtliche öffentlichen und nichtöffentlichen Stellen in allen Mitgliedstaaten.[309] Danach ist das Datenschutzrecht in Argentinien, Guernsey, der Isle of Man, Israel, Jersey, Kanada, Neuseeland, der Schweiz und in Ungarn hinreichend ausgeprägt.[310] Cloud-Infrastrukturen in diesen Ländern können ohne weitere Voraussetzungen genutzt werden. Es sind lediglich die Vorschriften einzuhalten, die für innerdeutsche oder unionsinterne Datentransfers gelten.

Staaten, die nicht in der Aufzählung enthalten sind und auch keine Mitglieder des Europäischen Wirtschaftsraums sind, müssen im Zweifel als unsichere Drittstaaten behandelt werden.[311] Cloud-Lösungen, die Datenübermittlungen in diese Länder beinhalten, sind dann nur unter besonderen Vorkehrungen möglich.

---

[305] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten, S. 109.
[306] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 37; Weniger, Grenzüberschreitende Datenübermittlungen, S. 403 f.
[307] Blume, Int. Journal of Law and Technology, Vol. 8/2000, 65 (78); Spindler, in: ders./Schuster, Recht der elektronischen Medien, § 4b BDSG Rn. 11.
[308] Art.-29-Datenschutzgruppe, WP 12, S. 6 f.
[309] Vgl. Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 39.
[310] Übersicht beim LfD Nds., Datenübermittlung ins Ausland, S. 2, abrufbar unter http://www.lfd.niedersachsen.de/download/32257/Datenuebermittlung_ins_Ausland.pdf.; s.a. Weniger, Grenzüberschreitende Datenübermittlungen, S. 408.
[311] Heidrich/Wegener, MMR 2010, 803 (807).

#### 3.1.2.1.2 Sonderfall: Schutzniveau in den USA

Eine besondere Situation ergibt sich, wenn Cloud-Server in den USA belegen sind. Das dort vorherrschende Datenschutzniveau ist verglichen mit europäischen Standards unzureichend.[312] Diese Einschätzung beruht im Wesentlichen darauf, dass es in den USA an umfassenden gesetzlichen Datenschutzregelungen fehlt.[313] Zwar wurden einzelfallbezogene Regelungen erlassen, eine allgemeingültige, flächendeckende Legislatur existiert hingegen nicht.[314] So betrifft der Privacy Act der USA beispielsweise nur Datenverarbeitungen des öffentlichen Sektors.[315] Zudem stellt der Privacy Act nur die Daten von Bürgern und Einwohnern der USA unter Schutz,[316] sodass die Daten europäischer Betroffener dort weitestgehend ungeschützt sind. Zur Wahrung des Datenschutzes in der Privatwirtschaft setzt die US-Politik vor allem auf Selbstregulierung und freiwillige Unterwerfung unter Privacy Polices.[317] Dieser Ansatz kann mangels verpflichtender Wirkung nicht an die europäischen Datenschutz-Maßstäbe heranreichen.

Wie zuvor dargelegt, ist die Übermittlung personenbezogener Daten in Länder ohne angemessenes Schutzniveau grundsätzlich unzulässig.[318] Demnach wäre es europäischen Stellen in der Regel verboten, Daten in eine Cloud zu laden, die auf US-amerikanischem Boden speichert. Auch die Kommunikation mit Einrichtungen in den USA wäre zumeist rechtswidrig, wenn persönliche Informationen wie Kundendaten davon umfasst sind. Ein solches Ergebnis ist jedoch von politischer Seite nicht gewollt. Schließlich wäre es mit gravierenden wirtschaftlichen Folgen verbunden, weil der transatlantische Handel Kommunikation erfordert.[319]

Um Datenübermittlungen in die USA allgemein zu ermöglichen, hat die EU-Kommission mit der US-Regierung die Safe-Harbor-Principles ausgehandelt. Es handelt sich dabei um Mindeststandards, nach denen US-Unternehmen die Daten europäischer Bürger behandeln sollen. Diese sind dann zwar in ein Land ohne angemessenes Schutzniveau übermittelt worden, werden aber bildlich gesprochen in einem sicheren Hafen verwahrt, innerhalb dessen ein hinreichender Datenschutz gilt. Sofern sich die empfangenden Unternehmen den Safe-Harbor-Principles unterworfen haben, ist nach den Festlegungen der Kommission ein hinreichendes Schutzniveau gewährleistet und der Datentransfer damit zulässig.[320] Dabei gilt es jedoch zu beachten, dass nur ein Bruchteil aller US-Unternehmen über eine Safe Harbor-Zertifizierung

---

[312] Art.-29-Datenschutzgruppe, WP 15; Heil, DuD 1999, 458 (458 ff.); Di Martino, Datenschutz im europäischen Recht, S. 68; Petri, DuD 2008, 729 (731); Röther/Seitz, (427); Spies, MMR 7/2007, V (VII).
[313] BT-Drs. 18/321; Arning/Haag, in: Heidrich/Forgó/Feldmann, Heise Online Recht, Kap. II Rn. 160.
[314] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten an die Terrorismusaufklärung der USA, S. 110; Assey/Eleftheriou, Commlaw Conspectus, S. 145 (150).
[315] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 39.
[316] Engel, Reichweite und Umsetzung des Datenschutzes gemäß der Richtlinie 95/46/EG für aus der Europäischen Union in Drittländer exportierte Daten am Beispiel der USA, S. 128.
[317] Heil, DuD 1999, 458 (458 ff.); Räther/Seitz, MMR 2002, 425 (427); s.a. Bäumler, CR 2011, 795 (796).
[318] Siehe oben S. 39.
[319] Blume, Int. Journal of Law and Technology, Vol. 8/2000, 65 (77); Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 37.
[320] ABl. L 215/7 v. 25.08.2000.

verfügt. Lediglich einige tausend Firmen haben sich den Principles unterworfen.[321] Die einflussreichen Cloud-Anbieter Amazon, IBM und Google haben sich jedoch in die Teilnehmerliste des US-Handelsministeriums eintragen lassen.[322]

Problematisch ist die Tatsache, dass es sich dabei um eine reine Selbstzertifizierung handelt.[323] Indem sie die Aufnahme in die Teilnehmerliste ersuchen, geben sie selbständig an, europäische Daten nur gemäß den Safe-Harbor-Principles zu verarbeiten. Das Handelsministerium überprüft in keiner Weise, ob diese Voraussetzung tatsächlich gegeben ist.[324] Auch nach erfolgter Eintragung finden Kontrollen nur in seltenen Einzelfällen statt.[325] Es ist deshalb nicht gewährleistet, dass die Safe-Harbor-zertifizierten Unternehmen tatsächlich die Grundsätze des Datenschutzes beachten. Im Gegenteil zeigt eine Studie des australischen Beratungsunternehmens Galexia aus dem Jahr 2008 auf, dass die selbstzertifizierten Unternehmen im Regelfall großflächig gegen die Safe-Harbor-Principles verstoßen.[326] Aus diesem Grund können europäische Datenexporteure nicht blind auf die Safe-Harbor-Zertifizierung vertrauen. Die Datenübermittlung setzt ferner voraus, dass sie weitere Mindestüberprüfungen vornehmen.[327] Nach den Anforderungen der deutschen Datenschutz-Aufsichtsbehörden erfordert die Auslagerung von Daten in eine Cloud in den USA drei Prüfungsschritte:[328]

1. Der Cloud-Anwender muss sich davon überzeugen, ob das Safe-Harbor-Zertifikat des Empfängers gültig ist und ob es die jeweils relevanten Datenkategorien enthält.
2. Der Cloud-Anwender muss nachweisen, dass der US-Anbieter seinen datenschutzrechtlichen Informationspflichten genügt.
3. Die Prüfungen des Cloud-Anwenders sind zu dokumentieren, sodass die zuständige Aufsichtsbehörde sie nachvollziehen kann.

---

[321] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 47; Schipper, Neue Instrumente des Datenschutzes, S. 116.
[322] http://safeharbor.export.gov/list.aspx.
[323] Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, S. 24; Erd, K&R 2010, 624 (626); Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 157.
[324] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 37.
[325] Heil, DuD 1999, 458 (458 ff.); Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 157; Rätzer/Seitz, MMR 2002, 425 (427); vgl. Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 49 ff.
[326] Connolly, The US Safe Harbor – Fact or Fiction, S. 8 f.
[327] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 40; Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 24.
[328] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 11; Düsseldorfer Kreis, Beschluss v. 28./29.04.2010, überarbeitete Fassung v. 23.08.2010; Holtorf, MPR 2013, 196 (197); a.A. Memo der ITA des US-Handelsministeriums, wiedergegeben bei Spies/Schröder, ZD-Aktuell 2013, 03566.

Seit den Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden im Sommer 2013[329] bestehen erhebliche Zweifel, ob diese Zusatzmaßnahmen noch ausreichend sind, um auf der Grundlage der Safe-Harbor-Principles Daten in die USA zu übermitteln. Der Grund ist die hohe Wahrscheinlichkeit, dass sich Geheimdienste Zugriff auf die Informationen verschaffen.[330] Dies kann auch ohne die Kooperation beziehungsweise ohne das Wissen der die Daten empfangenden Stelle erfolgen. Deshalb kann die vertrauliche Datennutzung auch dann nicht gewährleistet werden, wenn sich die Stelle den Safe-Harbor-Principles unterworfen hat und diese auch tatsächlich umsetzt. In der Folge hat nicht nur das Europäische Parlament die Aussetzung der Safe-Harbor-Entscheidung der Kommission gefordert.[331] Obwohl die Kommission dem Votum nicht gefolgt ist, kann momentan keine Datenübermittlung rechtssicher allein auf eine Safe-Harbor-Zertifizierung gestützt werden. Deutsche Aufsichtsbehörden haben bereits erste Anordnungen gegen solche Datentransfers in die USA erlassen.[332] Rechtssicherheit in dieser Frage kann künftig durch den Europäischen Gerichtshof hergestellt werden. Der irische High Court hat in einer Vorlageentscheidung beim EuGH die Klärung der Frage beantragt, ob die Safe-Harbor-Entscheidung der Kommission für die Aufsichtsbehörden verbindlich ist.[333] Die Kommission darf nach Art. 25 Abs. 6 der EG-Datenschutz-Richtlinie nur *feststellen*, ob das Schutzniveau in einem Drittstaat angemessen ist, dies aber nicht entgegen der Wirklichkeit bestimmen.[334] Deshalb ist zu erwarten, dass der EuGH keine Bindungswirkung der Safe-Harbor-Entscheidung annehmen wird. Die USA sind dann als Land mit unangemessenem Datenschutzniveau einzustufen, sodass die Übertragung personenbezogener Daten dort hin grundsätzlich unzulässig ist. Cloud Computing unter Einbeziehung der USA ist dann allenfalls möglich, wenn – wie nachfolgend erläutert – im Einzelfall für ein angemessenes Schutzniveau gesorgt ist.

#### 3.1.2.1.3 Schutzniveau im Einzelfall

Sowohl in die USA als auch in das übrige Ausland ohne angemessenes Datenschutzniveau dürfen nach den oben getroffenen Feststellungen grundsätzlich keine personenbezogenen Informationen übermittelt werden.[335] Damit ist es in der Regel nicht zulässig, rechtlich geschützte Daten in Cloud-Dienste einzuspeisen, deren Server außerhalb des Europäischen Wirtschaftsraums belegen sind.[336] Wird dies dennoch beabsichtigt, so hat der Versender

---

[329] Überblick bei Hansen, Präsentation auf der Sommerakademie 2014 des ULD, Folien abrufbar unter https://www.datenschutzzentrum.de/sommerakademie/2014/SAK14-Hansen-Sicherheitsdebatte-NSA-GCHQ-.pdf

[330] Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 24.07.2013, abrufbar unter http://www.bfdi.bund.de/DE/Home/homepage_Kurzmeldungen2013/PMDerDSK_SafeHarbor.html.

[331] Geiger, EuZW 2015, 161 (162).

[332] Dix, Safe Harbor am Ende?, S. 3; ders./Voßhoff, wiedergegeben bei Schröder, ZD-Aktuell 2015, 04531.

[333] Dazu Wybitul/Schuppert/v. Schweinitz, ZD-Aktuell 2014, 1.

[334] Simitis, in: Simitis, BDSG, § 4 b Rn. 77 f.; Thüsing/Forst, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 17 Rn. 60.

[335] Siehe oben S. 39 ff.

[336] Der Berliner Datenschutzbeauftragte, Jahresbericht 2008, S. 16.

sicherzustellen, dass die Datensätze unabhängig vom im Empfängerstaat gültigen Recht nach europäischen Maßstäben verarbeitet werden. Dies kann nur auf der Basis umfangreicher vertraglicher Vereinbarungen zwischen Übermittler und Empfänger gewährleistet werden.[337] Ferner ist ein auf diese Weise verpflichteter Cloud-Diensteanbieter zuvor sorgfältig auszuwählen, sodass gesichert ist, dass er tatsächlich europäische Schutzstandards umsetzen wird.[338]

Die Europäische Kommission hat Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern erlassen.[339] Der Mustertext enthält wesentliche Datenschutzpflichten, die aufgrund der EG-Datenschutzrichtlinie auch innerhalb der EU einzuhalten sind. Zudem sichert er die Einhaltung des Datenschutzstandards durch ein Zustimmungserfordernis des Datenexporteurs für jeden Unterauftragnehmer sowie die Verantwortlichkeit und Haftung des Datenimporteurs für Handlungen etwaiger Unterauftragnehmer ab. Diese Standardvertragsklauseln sind zwischen der übermittelnden Stelle und der empfangenden Stelle im Ausland ohne Änderungen zu vereinbaren. Hinsichtlich der tatsächlichen Umsetzung der darin enthaltenen Verpflichtungen im Ausland unterliegt der Datenexporteur einer Kontrollpflicht. Damit er in der Lage ist, entsprechende Kontrollen durchzuführen, sind die Einhaltung der Mindestanforderungen des § 11 Abs. 2 BDSG an Verträge über Auftragsdatenvereinbarungen ebenfalls zwischen den Parteien schriftlich zu vereinbaren.[340] Mit den Standardvertragsklauseln der EU-Kommission und den oben aufgelisteten[341] Klauseln nach § 11 Abs. 2 BGB sind also zwei Vertragsdokumente zwischen den Beteiligten zu unterzeichnen. Die Texte können auch als Anhang zu einem Hauptvertrag oder zum jeweils anderen Text vereinbart werden.

Eine alternative Form der Gewährleistung eines angemessenen Datenschutzniveaus nach der Datenübermittlung ins Ausland kann der Einsatz von Bindung Corporate Rules sein.[342] Dabei handelt es sich jedoch um eine konzerninterne Lösung,[343] die nur in Frage kommt, wenn der europäische Cloud-Anwender Daten in eine außereuropäische Cloud einspeist, die von demselben Konzern gehostet wird.

Besondere Vorsicht ist geboten, wenn sowohl der Auftraggeber als auch der Auftragnehmer einer Datenverarbeitung im Europäischen Wirtschaftsraum belegen sind, nicht aber ein vom Auftragnehmer herangezogener Unterauftragnehmer. Die Standardvertragsklauseln können

---

[337] Nägele/Jacobs, ZUM 2010, 281 (290).
[338] Vgl. Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 24.
[339] EU-Kommission, Beschluss Nr. 2010/87/EU v. 05.02.2010, Az. K(2010)593, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2010.039.01.0005.01.DEU.
[340] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 11; Weichert, DuD 2010, 679 (686); Weber/Voigt, ZD 2011, 74 (77 f.).
[341] Siehe oben S. 2.1.2.1.2.3 f.
[342] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 10; Weichert, DuD 2010, 679 (686).
[343] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 43; Holtorf, MPR 2013, 196 (197).

dann zwischen Auftraggeber und Auftragnehmer nicht verwendet werden, weil sie eine Drittstaatenübermittlung voraussetzen, die im Verhältnis zwischen diesen beiden Beteiligten nicht gegeben ist.[344] Ebenso wenig ist die Vereinbarung der Standardvertragsklauseln zwischen dem Auftragnehmer und dem Unterauftragnehmer zielführend, weil nicht der Auftragnehmer, sondern der Auftraggeber die verantwortliche Stelle ist.[345] Dieses Problem kann dadurch gelöst werden, dass alle Beteiligten untereinander Verträge schließen, die eine Datenverarbeitung nach europäischen Standards garantieren, also insbesondere der Auftraggeber mit dem im Drittstaat gelegenen Unterauftragnehmer.[346]

#### 3.1.2.2 Besonderheiten bei Auftragsdatenverarbeitung

Werden personenbezogene Daten in Drittstaaten ohne angemessenes Schutzniveau übermittelt, so finden die oben dargestellten rechtlichen Privilegien der Auftragsdatenverarbeitung keine Anwendung.[347] Es gelten dann die allgemeinen Regelungen für Datenübermittlungen mit der Folge, dass der Empfänger zur datenschutzrechtlich verantwortlichen Stelle wird und der Datenexporteur für die Übermittlung verantwortlich ist. Dies ergibt sich aus § 3 Abs. 8 S. 3 BDSG, wonach der außereuropäische Dienstleister Dritter im Sinne des BDSG ist, was die Einstufung als Auftragsdatenverarbeiter ausschließt.[348] Der Grund für diese rechtliche Ungleichbehandlung liegt in der Annahme, dass aufgrund des in Drittstaaten oftmals unzureichenden Datenschutzniveaus die erforderliche Kontrolle des Auftragnehmers nicht gewährleistet werden kann.[349]

Dennoch können die Rechtsfolgen der Auftragsdatenverarbeitung im Einzelfall auch erzielt werden, wenn die Standardvertragsklauseln[350] der EU-Kommission zwischen Datenexporteur und -importeur vereinbart wurden.[351] Als rechtliche Grundlage für diese Lösung wird § 18 Abs. 1 S. 1 Nr. 2 BDSG herangezogen, sodass die dort verankerte Rechtsgüterabwägung Voraussetzung für den Datentransfer ist.[352]

### 3.1.3 Spionage durch ausländische Geheimdienste

Gefahren für die Vertraulichkeit und die Integrität aller über das Internet versendeten Daten gehen nicht nur von Kriminellen oder marktmächtigen Unternehmen aus. Besonders in den

---

[344] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 42; Plath, in: ders., BDSG, § 11 Rn. 107.
[345] Hillenbrandt-Beck, RDV 2007, 231 (234).
[346] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 42; V. d. Bussche, in: Plath, BDSG, § 11 Rn. 107.
[347] Heidrich/Wegener, MMR 2010, 803 (806); Holtorf, MPR 2013, 196; Niemann/Hennrich, CR 2010, 686 (687); Niemann/Paul, K&R 2009, 444 (449); Thalhofer, CCZ 2011, 222 (223 f.); Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 20; Weichert, DuD 2010, 679 (682).
[348] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 148.
[349] Heidrich/Wegener, MMR 2010, 803 (806); Schulz, MMR 2010, 75 (79).
[350] Siehe oben, S. 35.
[351] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 150.
[352] AK Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe – Cloud Computing, S. 11; Weichert, DuD 2010, 679 (686).

öffentlichen Fokus gerückt sind in den letzten Jahren die Geheimdienste verschiedener Nationen, die in gesicherte IT-Systeme eindringen oder Cloud-Diensteanbieter zu einer Offenlegung der durch sie verwalteten Datensätze zwingen.

#### 3.1.3.1 Erhebungsbefugnisse ausländischer Geheimdienste

Verschiedene Staaten haben ihre Geheimdienste auf legislativem Wege mit weitreichenden Befugnissen ausgestattet, die ihnen breiten Zugriff auf in Clouds gespeicherte Informationen ermöglichen. Hierbei sind besonders die USA, Großbritannien und China zu nennen, da zum einen die dortigen Geheimdienste über besonders breite Erhebungsbefugnisse verfügen und diese Länder zum anderen zahlreiche international marktmächtige Cloud-Diensteanbieter beheimaten.

##### 3.1.3.1.1 USA

US-Amerikanischen Geheimdiensten gewährt der Patriot Act in Verbindung mit dem Foreign Intelligence Surveillance Act (FISA) seit dem Jahr 2001 erhebliche Eingriffsbefugnisse in den weltweiten Internet-Verkehr.[353] Einheimische Unternehmen sind danach dazu verpflichtet, Kommunikationsprotokolle ihrer Kunden weiterzugeben.[354] Zugriff auf durch Cloud-Dienste gespeicherte Inhaltsdaten erhalten die Geheimdienste durch den FISA, den Economic Communications Privacy Act (ECPA) sowie National Security Letters.[355] Der FISA Amendments Act (FAA) erweitert die Überwachungsbefugnisse der US-Behörden auf Ziele im Ausland. Die zunächst zur Auswertung der Auslandskommunikation geschaffene Rechtsgrundlage stellt inzwischen die zentrale Ermächtigung zum Ausspähen von Cloud-Speichern außerhalb der USA dar.[356]

Cloud-Dienste, die zumindest teilweise Infrastruktur auf dem Gebiet der Vereinigten Staaten nutzen, unterliegen damit in jedem Fall der ständigen Zugriffsmöglichkeit durch dortige Geheimdienste.[357] Auch außerhalb der USA gespeicherte Cloud-Daten sind an die US-Behörden auf Anforderung zu übermitteln. Diese Verpflichtung besteht für alle Unternehmen, deren Sitz in den USA liegt[358] oder die in ihrem Konzernverbund ein Unternehmen beinhalten, das dort seinen Sitz hat.[359] Ferner besteht die Herausgabeverpflichtung für alle weiteren Unternehmen, die kontinuierlich und systematisch in den USA Geschäfte betreiben.[360] Das letztgenannte Kriterium ist denkbar weit gefasst.[361] Selbst regelmäßige Geschäftspartner von

---

[353] Haag, in: Leupold/Glossner, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 44; Schröder/Haag, ZD-Aktuell 2012, 3132.
[354] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten, S. 31.
[355] Schröder/Haag, ZD-Aktuell 2012, 03132; Spies, ZD-Aktuell 2012, 03062; Voigt, MMR 2014, 158 (159).
[356] Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, S. 21 f.
[357] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 59.
[358] Hansen, DuD 2012, 407 (410); Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 147.
[359] Becker/Nikolaeva, CR 2012, 170 (170 ff.); Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 147; Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 59.
[360] Schuppert/v. Reden, ZD 2013, 210 (216 f.); Haag, in: Leupold, Münchener Anwaltshandbuch IT-Recht, Teil 4 Rn. 44; s.a. Schröder/Haag, ZD-Aktuell 2012, 03132; Schröder/Spies, ZD-Aktuell 2014, 03194.
[361] Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights, S. 19.

Unternehmen oder Kunden in den USA können darunter fallen. Aufgrund der bedeutenden Marktmacht der US-Computerindustrie trifft es auf eine Vielzahl der weltweiten Cloud-Diensteanbieter zu.[362]

Die angesprochenen Rechtsgrundlagen ermöglichen den US-Geheimdiensten damit weitreichenden Zugriff auf Cloud-Inhalte aus der gesamten Welt. Adäquate Garantien für den Datenschutz der Betroffenen lassen sich für Nicht-US-Bürger weder aus dem allgemeinen Recht der USA noch aus dem FISA ableiten.[363]

#### 3.1.3.1.2 Großbritannien

Auch das Vereinigte Königreich weist mit dem Regulation of Investigatory Powers Act (RIPA) eine Rechtsgrundlage zur geheimdienstlichen Überwachung des Internet-Verkehrs auf. Das Gesetz ist dem US-Patriot Act sehr ähnlich.[364] Sektion 8 Abs. 4-5 des RIPA gestattet die flächendeckende Überwachung von Auslandskommunikation. Davon umfasst ist unter anderem auch der rein innerdeutsche Informationsfluss.[365] Im Gegensatz zur Überwachung von Verbindungen innerhalb des Königreichs[366] ist die Auslandsüberwachung nicht auf Einzelfälle beschränkt.

#### 3.1.3.1.3 China

Die Volksrepublik China beheimatet ebenfalls zahlreiche aufstrebende Cloud-Diensteanbieter mit großer Marktmacht.[367] Auch dort existieren gesetzliche Erlaubnisnormen zur großflächigen Überwachung dieser Cloud-Dienste. Art. 4 des chinesischen Gesetzes über das Ministerium für Öffentliche Sicherheit ermächtigt den Staat zur Überwachung des chinesischen Internet-Verkehrs sowie der dort gelegenen Rechner. Von dieser Befugnis umfasst ist der Einsatz heimlicher Infiltrationstechniken wie etwa Trojaner-Programme.[368] Die Behörden dürfen auch Informationen aus geschlossenen SaaS-Diensten extrahieren, die eine persönliche Registrierung erfordern,[369] sodass Cloud-Infrastrukturen betroffen sind. Voraussetzung für solche Maßnahmen ist lediglich, dass die Behörde erwartet, Daten im Interesse des Landes zu finden.[370] Der Begriff der Interessen des Landes ist weit gefasst. So sind etwa chinesische Geheimdienste gesetzlich verpflichtet, einheimische Wirtschaftsunternehmen durch Informationsbeschaffung aktiv zu unterstützen[371] Die heimliche Informationsbeschaffung aus passwortgeschützten chinesischen Cloud-Speichern ist damit nach dortigem nationalen Recht einzelfallunabhängig zulässig, wenn sie der Wirtschaftsspionage dienlich ist.

---

[362] Voigt, MMR 2014, 158 (160).
[363] Bowden, The US surveillance programmes and their impact on EU citisens' fundamental rights, S. 23 f.
[364] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 59.
[365] Schlikker, NJOZ 2014, 1281.
[366] Sektion 8 Abs. 1-2 RIPA
[367] Ragland/McReynolds/Southerland/Mulvenon, Red Cloud Rising: Cloud Computing in China, S. 5 ff.
[368] Karden/v. Freiberg, Praxishandbuch Unternehmenssicherheit, S. 78 f.
[369] Mattis, Studies in Intelligence, Vol. 56, Nr. 3, S. 47 (50).
[370] Karden/v. Freiberg, Praxishandbuch Unternehmenssicherheit, S. 79.
[371] Karden/v. Freiberg, Praxishandbuch Unternehmenssicherheit, S. 15.

#### 3.1.3.2 Erhebungspraxis ausländischer Geheimdienste

Die Praxis zeigt, dass die oben aufgezeigten Eingriffsbefugnisse auch intensiv genutzt werden.

##### 3.1.3.2.1 USA

Seit den Enthüllungen des ehemaligen US-Geheimdienstmitarbeiters Edward Snowden[372] ist der Öffentlichkeit bekannt, dass die Geheimdienste der USA ein eine nahezu flächendeckende Überwachung des weltweiten Kommunikationsverkehrs im Internet betreiben.[373] Auf der Grundlage des FISA wurde das PRISM-Programm errichtet, das den Geheimdiensten direkten Zugriff auf die bei US-amerikanischen Unternehmen gespeicherten Daten verschafft.[374] Bei den Unternehmen sind gespeicherte Inhaltsdaten der Kunden ebenso umfasst, wie Kommunikationsinhalte, die in Echtzeit eingesehen werden können. Als weitere Datenquelle nutzen die US-Geheimdienste Knotenpunkte von bedeutsamen Verbindungskabeln des weltumspannenden Telefonnetzes.[375]

Im Rahmen des Upstream-Programms hat sie an diesen Kabeln Splitter angebracht, die den Datenfluss kopieren.[376] Auf diese Weise können auch Kommunikationsinhalte abgefangen werden, die keinen Bezug zu den USA aufweisen. Da die angezapften Telefonkabel insbesondere zum Datenaustausch im Internet verwendet werden, können auch Cloud-Inhalte abgefangen werden, während die Cloud-Anwender sie in die Cloud-Speicher laden oder von dort herunterladen. Werden die übermittelten Daten durch eine Transportverschlüsselung gesichert, erschwert dies den Zugriff der US-Geheimdienste signifikant. Dennoch sind sie im Einzelfall auch in der Lage, Verschlüsselungsmethoden zu überwinden.[377] Da die marktführenden Unternehmen im Bereich der Kryptographie in den USA ansässig sind, konnten sich die Geheimdienste im Rahmen des PRISM-Programms Generalschlüssel beschaffen sowie den gezielten Einbau von ihnen bekannten Schwachstellen und Hintertüren in die Verschlüsselungstechnologien erwirken.[378]

Die durch das PRISM- und das Upstream-Programm gewonnenen Daten werden durch die US-Geheimdienste für unbekannte Zeit gespeichert.[379] Die Auswertung erfolgt unter anderem durch das XKeyscore-Programm,[380] in dessen Rahmen Data Mining Anwendung findet.

##### 3.1.3.2.2 Großbritannien

Hinsichtlich der Geheimdienstaktivitäten Großbritanniens ist das TEMPORA-Programm bekannt. Es dient der Überwachung und Speicherung von Internet-Daten, die über das Hoheitsgebiet des

---

[372] Deiseroth, ZRP 2013, 194; Ewer/Thienel, NJW 2014, 30.
[373] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten an die Terrorismusaufklärung der USA, S. 18; Ewer/Thienel, NJW 2014, 30.
[374] Bowden, The US surveillance programmes and their impact on EU citisens' fundamental rights, S. 13.
[375] Bowden, The US surveillance programmes and their impact on EU citisens' fundamental rights, S. 13.
[376] Góralczyk, ZD-Aktuell 2015, 04568.
[377] Deiseroth, ZRP 2013, 194; Schaar, ZRP 2013, 214 (216).
[378] Geminn, MMR 2015, 98 (101); Ruhmann, DuD 2014, 40 (42).
[379] Schaar, ZRP 2013, 214.
[380] Bowden, The US surveillance programmes and their impact on EU citisens' fundamental rights, S. 13.

Vereinigten Königreichs versandt werden.[381] Die auf diese Weise abgefangenen Inhaltsdaten werden mindestens drei Tage lang gespeichert, die Metadaten darüber hinaus 30 Tage.[382] Es handelt sich um ein gemeinsames Programm mit den als Five Eyes bezeichneten Kooperationspartnern USA, Kanada, Australien und Neuseeland,[383] die ihre Erkenntnisse auch untereinander teilen. Aufgrund der geographischen Lage der britischen Insel an der europäischen Atlantikküste enden dort bedeutsame Seekabel, durch die ein Großteil der weltweiten Internet-Kommunikation übermittelt wird.

#### 3.1.3.2.3 China und andere Staaten

Auch der chinesische Geheimdienst ist in der Überwachung des Internet-Verkehrs sehr aktiv.[384] Ein besonderer Fokus liegt dabei auf der Durchführung von Industriespionage.[385] In die Entwicklung chinesischer Cloud-Technologien ist teilweise der Geheimdienst direkt involviert.[386] Es ist daher davon auszugehen, dass technische Schutzmaßnahmen wie Datenverschlüsselung keinen Schutz vor staatlicher Einsichtnahme bieten, wenn Daten in einer Cloud gespeichert werden, die Ressourcen auf chinesischem Boden oder Software aus chinesischer Herstellung nutzt.

Neben China betreiben auch zahlreiche Staaten Industriespionage durch Überwachung von Internet-Inhalten, darunter Russland, Rumänien, Polen und Bulgarien.[387]

### 3.1.3.3 Konsequenzen

Aus den oben beschriebenen Eingriffsszenarien folgt, dass die Vertraulichkeit und Integrität personenbezogener Daten oftmals nicht mehr gewährleistet werden kann, wenn sie in eine Cloud eingespeist werden, die über Komponenten im Ausland verfügt. Je nach Empfängerstaat besteht eine gesteigerte Gefahr, dass ausländische Geheimdienste die Informationen ohne das Wissen der Betroffenen abrufen, speichern, auswerten und weitergeben. Die Dienste kehren dabei das rechtsstaatliche Prinzip um, dass der Staat eine Rechtfertigung benötigt, um in die Privatsphäre des Einzelnen einzudringen.[388]

Obwohl einiges dafür spricht, dass das britische TEMPORA-Programm gegen höherrangiges Europarecht verstößt,[389] ändert dieser Umstand nichts an der grundsätzlichen Zulässigkeit, Daten deutscher Betroffener an einen Cloud-Diensteanbieter im Vereinigten Königreich zu übermitteln. § 4b Abs. 1 BDSG erlaubt nämlich ebenso wie Art. 25 der EG-Datenschutzrichtlinie die Datenübermittlung innerhalb der Europäischen Union. Diese Erlaubnis gilt jeweils unabhängig vom im Empfänger-Mitgliedstaat allgemein oder konkret herrschenden

[381] Ewer/Thienel, NJW 2014, 30; Gercke, ZUM 2013, 605 (612); Schlikker, NJOZ 2014, 1281.
[382] Schlikker, NJOZ 2014, 1281.
[383] Weichert, KJ 2014, 123.
[384] Leupold, MMR 2014, 145.
[385] Heide, GRURInt 2008, 12 (13).
[386] Ragland/McReynolds/Southerland/Mulvenon, Red Cloud Rising: Cloud Computing in China, S. 36 f.
[387] Többens, NStZ 2000, 505.
[388] Schellenberg, ZRP 2014, 24 (25).
[389] Schlikker, NJOZ 2014, 1281; a.A. Ewer/Thienel, NJW 2014, 30 (33).

Datenschutzniveau. Auch etwaige permanente Verletzungen der Unionsgrundrechte durch das TEMPORA-Programm stellen keinen Grund für ein Verbot von Datentransfers nach Großbritannien dar. Die Bestimmungen der EG-Datenschutzrichtlinie, die unionsinterne Übermittlungen vorbehaltlos erlauben, verfügen nach dem Willen des Grundrechtekonvents[390] als Konkretisierung von Art. 8 der Grundrechtecharta ebenfalls über Grundrechtsrang.[391]

Anders liegt der Sachverhalt bei US-amerikanischen Überwachungsmaßnahmen. Die grundsätzliche Zulässigkeit der Datenübermittlungen in dort gehostete Clouds im Rahmen der Safe-Harbor-Principles oder Standardvertragsklauseln beruht nicht direkt auf der EG-Datenschutzrichtlinie, sondern lediglich auf einer Entscheidung der EU-Kommission.[392] Die Kommission hat bei Erlass der Entscheidung betont, dass die nationalen Aufsichtsbehörden Datenübermittlungen in die USA aussetzen können, wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze aus der Safe-Harbor-Entscheidung großflächig verletzt werden.[393] Dieser Fall ist nun eingetreten. Infolge der Offenlegung der weitreichenden Aktivitäten US-amerikanischer Geheimdienste ist es sehr wahrscheinlich, dass exportierte Daten zweckfremd verarbeitet werden und dadurch die Safe-Harbor-Principles verletzt werden.[394] Weder eine Safe-Harbor-Zertifizierung noch Standardvertragsklauseln können demnach derzeit einen Datenexport in eine Cloud rechtfertigen, die zumindest teilweise Infrastrukturen auf dem Boden der USA beinhaltet.

Ähnliche Vorsicht ist bei Cloud-Diensteanbietern an den Tag zu legen, die ihre Daten innerhalb der EU speichern, aber einem US-amerikanischen Konzern angehören. Solche Unternehmen können verpflichtet werden, die Daten ihrer Kunden auf der Grundlage des FISA, des FAA und des ECPA an die US-Behörden zu übermitteln. Ausländische Rechtsakte sind keine Ermächtigungsgrundlagen im Sinne des deutschen und europäischen Datenschutzrechts.[395] Nach hiesigem Recht darf dem Auskunftsverlangen daher nicht entsprochen werden, solange es nicht auf einem entsprechenden Rechtshilfeverfahren beruht und damit einer nationalen Rechtsgrundlage unterfällt.[396] Die betroffenen Unternehmen sehen sich damit dem Spannungsverhältnis zweier sich in dem Punkt widersprechender Rechtssysteme ausgesetzt. Sie sind gezwungen, entweder das deutsche und europäische oder das US-Recht zu brechen. Beim Einspeisen von Daten in eine solche in Deutschland gehostete Cloud handelt es sich erneut um eine Datenübermittlung innerhalb der EU, gegen die bei Bestehen einer

---

[390] Erläuterungen des Präsidiums des europäischen Konvents v. 11.10.2000, CHARTE 4473/00, S. 11 CONVENT 49.
[391] Ambrock, Die Übermittlung von S.W.I.F.T.-Daten, S. 79 f.; Jarass, GRCh, Art. 6 Rn. 2-5; Siemen, Datenschutz als europäisches Grundrecht, S. 272 f., 281; Streinz, DuD 2011, 602 (604).
[392] Siehe oben, S. 43 ff.
[393] Hessischer Datenschutzbeauftragter, Pressemitteilung v. 24.07.2013, abrufbar unter https://www.datenschutz.hessen.de/presse_2013.htm.
[394] Thüsing/Potters, in: Thüsing, Beschäftigtendatenschutz und Compliance, § 15 Rn. 24; s.a. Hessischer Datenschutzbeauftragter, a.a.O. (Fn. 393).
[395] Scholz/Sokol, in: Simitis, BDSG, § 4 Rn. 9 Fn. 23; Taeger, in: ders./Gabel, BDSG, § 4 Rn. 33; Voigt, MMR 2014, 158 (160).
[396] A.A. Voigt, MMR 2014, 158 (160); ders./Klein, ZD 2013, 16 (17).

entsprechenden Einwilligung zunächst rechtlich nichts eingewendet werden kann.[397] Bestehen jedoch konkrete Anhaltspunkte dafür, dass ein nur in Deutschland agierender Cloud-Diensteanbieter mit US-amerikanischem Mutterkonzern den Auskunftsverlangen US-amerikanischer Geheimdienste nachgibt, widerspräche es der gebotenen Sorgfaltspflicht, ihm fremde personenbezogene Daten anzuvertrauen. Dasselbe gilt für Cloud-Dienste mit Servern ausschließlich in Europa, die von Unternehmen angeboten werden, die einem Mutterkonzern aus einem anderen Drittstaat wie etwa China angehören.

Nach alledem wird deutlich, dass die Standortauswahl des Cloud-Servers und -Diensteanbieters essentiell für die Vertraulichkeit und Integrität ist und die Legalität der Nutzung eines solchen Cloud-Dienstes beeinflusst. Aus diesem Grund gewinnen insbesondere seit den Enthüllungen Edward Snowdens sogenannte „Schengen-Clouds“ an Bedeutung, bei denen sichergestellt ist, dass nur Speicherorte im Europäischen Wirtschaftsraum beteiligt sind.[398] Auch wenn die Speicherung ausschließlich im EWR aus Datenschutzsicht sinnvoll ist, kann diese Maßnahme die Zugriffsmöglichkeiten ausländischer Geheimdienste nicht vollständig verhindern.[399] Etwa ein Viertel des vermeintlich innerdeutschen Internet-Verkehrs wird auch über Datenleitungen und Knotenpunkte abgewickelt, die im Ausland liegen.[400] Der genaue Weg, den die Daten auf dem Weg zu ihrem Bestimmungsort zurücklegen ist weder durch den Cloud-Anwender noch durch den Cloud-Diensteanbieter beeinflussbar. Nicht zuletzt deshalb sind technische und organisatorische Maßnahmen wie vor allem die Vornahme einer Transportverschlüsselung unverzichtbar.[401] Die Erkenntnisse aus der sogenannten NSA-Affäre zwingen die Anbieter eines Cloud-Dienstes deshalb zu gesteigerten Sicherheitsmaßnahmen, um die Vertraulichkeit und Integrität der Cloud-Anwenderdaten zu gewährleisten.[402]

### 3.1.4 Datenabruf durch Cloud-Anwender im Ausland

Ein vom Cloud-Diensteanbieter kaum kontrollierbarer Auslandsbezug kann entstehen, wenn Cloud-Anwender Daten aus dem Ausland heraus abrufen. Dies kann beispielsweise der Fall sein, wenn ein Stromkunde mit seinem Mobiltelefon von einer Urlaubsreise aus Informationen über seinen Energieverbrauch abfragt. Als weiteres Szenario kommen in diesem Zusammenhang Energieerzeuger oder Netzbetreiber (z.B. Stadtwerke) in Betracht, die einem im Ausland ansässigen Partnerunternehmen Zugriff auf die Cloud gewähren.

Handelt es sich bei dem genannten Stromkunden um den Betroffenen, ruft er also seine ausschließlich eigenen Verbrauchsdaten aus dem Ausland ab, so ist der Fall einfach zu beantworten. Die Weitergabe von Daten an den Betroffenen selbst stellt keine Übermittlung und damit auch keine Datenverarbeitung dar.[403] Es ist daher datenschutzrechtlich nicht zu

[397] Siehe oben, S. Konsequenzen51 f.
[398] Voigt, MMR 2014, 158; s.a. Marnau/Schlehahn, DuD 2011, 311 (316).
[399] Voigt, MMR 2014, 158 (161); vgl. Hartmann, wiedergegeben in: Pech, ZUM 2014, 22 (22 f.).
[400] Leupold, MMR 2014, 145 (146); s.a. Geminn, MMR 2015, 98.
[401] Leupold, MMR 2014, 145 (146).
[402] Schaar, ZRP 2013, 214 (216).
[403] Buchner, in: Taeger/Gabel, BDSG, § 3 Rn. 34.

beanstanden, wenn der Betroffene seine eigenen Daten abruft – unabhängig davon, in welchem Land er sich befindet.

Ruft hingegen ein Dritter Informationen über andere aus dem Ausland ab, so ist dieser Vorgang anders gelagert. Hält ein Cloud-Anwender Informationen zum Abruf durch Dritte bereit, handelt es sich dabei nach § 3 Abs. 4 Nr. 3 lit. b BDSG um eine datenschutzrechtlich relevante Übermittlung, für die er verantwortlich ist. Das Einstellen von Daten ins Internet fällt darunter,[404] folglich auch das Einspeisen in eine Cloud. Aus der Verantwortlichkeit des Uploaders für die Übermittlung folgt jedoch noch nicht, dass diesen auch die Verpflichtungen treffen, die § 4b BDSG für Auslandsübermittlungen[405] aufstellt. Der Begriff der Übermittlung wird im BDSG nämlich nicht einheitlich verwendet.[406] Nach der Lindqvist-Entscheidung des Europäischen Gerichtshofs ist das Angebot zum Abruf von Seiten aus dem Internet keine Auslandsübermittlung im Sinne des § 4b BDSG entsprechenden Art. 25 der EG-Datenschutzrichtlinie.[407] Eine solche Auslegung ist im Ergebnis auch geboten, weil ansonsten der Betrieb nahezu jeder Website unrechtmäßig wäre.[408] Er wäre dann nämlich automatisch mit einer Datenübermittlung in Drittstaaten mit zu niedrigem Schutzniveau verbunden, sobald der Aufruf der Website aus einem solchen Land technisch möglich ist. Die Gerichtsentscheidung ist zwar auf das World Wide Web bezogen, kann aber verallgemeinert werden für weitere Internet-Dienste, bei denen Cloud-Anwender aktiv Informationen abrufen, die andere Cloud-Anwender hierzu bereitgestellt haben.[409]

Für das Cloud Computing bedeutet dies, dass die Speicherung personenbezogener Daten auf einen europäischen Server unabhängig von der Frage erfolgen kann, ob später Cloud-Anwender aus dem Ausland auf diese Daten zugreifen werden, beziehungsweise könnten. Es handelt sich bei diesem Vorgang um keine Drittstaatenübermittlung im Sinne des § 4b BDSG. Unzulässig wäre hingegen eine bewusste Nutzung des Umwegs über die Cloud, um die gesetzlichen Regelungen zur Drittstaatenübermittlung zu umgehen. Kein Cloud-Anwender darf die Cloud bewusst missbrauchen, um personenbezogene Daten bewusst ins Ausland mit niedrigem Schutzniveau zu transferieren.[410] Gewähren also wie im oben genannten Beispiel Stadtwerke einem anderen, im Ausland gelegenen Unternehmen über die Cloud Zugriff auf die Verbrauchsdaten ihrer Kunden, so ist dies als Drittstaatenübermittlung einzustufen. Unabhängig von der ohnehin für jede Übermittlung notwendige Rechtsgrundlage[411] sind dann die Voraussetzungen des § 4b BDSG zusätzlich zu erfüllen.[412] Der Cloud-Anwender (in diesem Fall

---

[404] Dammann, RDV 2004, 19 (20 f); Schild, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.2 Rn. 69; Weichert, in: Däubler/Klebe/Wedde/ders., BDSG, § 3 Rn. 32.
[405] Siehe oben S. 41 ff.
[406] Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 154.
[407] EuGH, Urt. v. 06.11.2003, Rs. C-101/01 – Bodil Lindqvist/Schweden – Antwort zur 5. Vorlagefrage.
[408] Buchner, in: Taeger/Gabel, BDSG, § 3 Rn. 35; Roßnagel, MMR 2004, 99.
[409] Roßnagel, MMR 2004, 99.
[410] Vgl. Jotzo, Der Schutz personenbezogener Daten in der Cloud, S. 155; Kuner, European Data Protection Law, Rn. 4.08.
[411] Siehe oben S. 8 ff.
[412] Thalhofer, CCZ 2011, 222 (224).

die Stadtwerke) hat insofern ein angemessenes Datenschutzniveau beim Datenempfänger zu gewährleisten.[413]

## 3.2 Haftungsrechtliche Anforderungen

Der Begriff der Haftung ist an dieser Stelle rein zivilrechtlich zu verstehen.

Haftungsrecht ist im Wesentlichen nationales Recht. Eine vertiefte Analyse scheidet somit aus. Die allgemeinen Grundprinzipien der Haftung sind jedoch innerhalb der Unionsmitgliedstaaten oftmals ähnlich. Eine Pflicht zur Haftung ergibt sich in der Regel in Bezug auf die Elemente:

- Das Verhalten (Tun oder Unterlassen)
- Die Rechtswidrigkeit des Verhaltens
- Ein verursachter Schaden
- Die Kausalität zwischen dem Verhalten und dem Schaden
- Verschulden

Dieses Grundschema kann insbesondere durch vertragliche Regelungen modifiziert werden.

Dabei wirken zwischen den Vertragsparteien die vertraglichen Regelungen auch in die deliktische Haftung ein.

Eine vertragliche Haftungspflicht besteht jedoch nur zwischen den Vertragsparteien, deliktische Haftung besteht gegenüber jedem. Wegen der Haftungspflicht gegenüber jedem kennt das Deliktsrecht im Gegensatz zum Vertragsrecht keine Instrumente zur Begrenzung oder Erweiterung der Haftung. Die deliktische Haftung entsteht vielmehr nur aus den Tatsachen an die angeknüpft wird.

Haftungsfreistellungen aus Art. 12 -14 der E-Commerce-Richtlinie 2000/31/EG für Vermittler für die „reine Durchleitung“, „Caching“ oder „Hosting“ erscheinen fernliegend. Denn der Haftungsausschluss gilt nur beschränkt auf den technischen Prozess als rein technische, automatische, gleichsam passive Dienstleistung ohne Kenntnis oder Kontrolle über die Informationen.

Updates der Virtual Machine durch die Dienste-Admins oder die Tätigkeit der Cloud-Admins erfordern jedoch zumindest Kontrolle im Sinne einer Manipulierbarkeit von Informationen.

## 3.3 Steuer- und handelsrechtliche Anforderungen

Neben den datenschutzrechtlichen Vorschriften sind es auch Regelungen des deutschen Wirtschaftsverwaltungsrechts, die den Kreis der möglichen Anwendungsfelder für Cloud Computing beschränken. So verlangt § 146 Abs. 2 S. 1 der Abgabenordnung (AO), dass steuerlich relevante Aufzeichnungen im Inland aufzubewahren sind. Diese Verpflichtung trifft alle Unternehmen und Gewerbetreibende, die zu einer regelmäßigen Buchführung verpflichtet sind

[413] Siehe oben S. 41 ff.

(vgl. § 140 AO). Sinn der Regelung ist die Sicherung der kurzfristigen Zugriffsmöglichkeit des Finanzamtes im Fall einer steuerlichen Überprüfung.[414] Entsprechende Belege können nicht nur in Papierform existieren, sondern auch digitaler Natur sein. Es liegt gerade in größeren Unternehmen der Schluss nahe, solche elektronischen Belege in einer Cloud abzulegen, damit verschiedene Mitarbeiter an unterschiedlichen Orten darauf Zugriff haben. Aus § 146 AO folgt jedoch, dass dies nur zulässig ist, wenn die betreffenden Informationen auf Servern in Deutschland gespeichert werden.[415] Auch die datenschutzrechtlich relativ unproblematische Speicherung im europäischen Ausland wird vom Steuerrecht nicht gebilligt. Ausnahmen sind nach § 146 Abs. 2a AO im Rahmen der elektronischen Buchführung möglich, bedürfen jedoch der Zustimmung und Zugriffsmöglichkeit durch das zuständige Finanzamt.[416] Steuerrechtlich möglich ist es natürlich, die elektronischen Belege auf Sicherungsspeichern im Inland zu hinterlegen und Kopien zusätzlich auf ausländischen Cloud-Servern vorzuhalten.

Die handelsrechtlichen Dokumentationspflichten aus § 257 HGB verlangen keine zwingende Aufbewahrung von Handelsbüchern, Bilanzen, Buchungsbelegen und vergleichbaren Unterlagen im Inland.[417] Sie sind jedoch sechs bis zehn Jahre lang so vorzuhalten, dass ihre Verfügbarkeit und Lesbarkeit kurzfristig gewährleistet ist.[418] Dieses Erfordernis steht einer Cloud-Lösung nicht im Wege.[419] Es ist jedoch darauf zu achten, dass ein Service gewählt wird, bei dem jederzeit bekannt ist, an welchem Standort die Informationen aktuell gespeichert sind.[420] Die Nutzung ausländischer Infrastrukturen ist damit handelsrechtlich grundsätzlich möglich. Die entsprechenden Unterlagen haben jedoch in der Regel steuerliche Relevanz, sodass die oben dargestellten steuerrechtlichen Anforderungen zu erfüllen sind und somit nur inländische Speicherorte in Betracht kommen.

Vergleichbare Regelungen existieren auch in anderen Staaten und sind daher von multinationalen Unternehmen gegebenenfalls parallel zu beachten. Beispielsweise verlangt Art. 245 Abs. 1 des kanadischen Bank Act, dass Kreditinstitute aus Kanada ihre Datenverarbeitung ausschließlich im dortigen Inland betreiben dürfen.[421]

Privatpersonen unterliegen den oben dargestellten wirtschaftsrechtlichen Beschränkungen nicht. Die Vorschriften hindern Hauseigentümer daher in der Regel nicht daran, ihren Energieverbrauch über ein intelligentes Messgerät in eine Cloud-Architektur zu laden. Für an eine solche Cloud-Plattform angeschlossene Unternehmen wie beispielsweise Energieerzeuger können die Vorschriften relevant werden. Soll aus den Ablesedaten das Nutzungsentgelt einzelner Stromkunden ermittelt werden, so handelt es sich bei den Datensätzen um steuerlich

---

[414] BT-Drs. VI/1982, S. 126.
[415] Rätke, in: Klein, AO, § 146 Rn. 36; Sinewe/Frase, BB 2011, 2198.
[416] Thalhofer, CCZ 2011, 222 (224).
[417] Ballwieser, in: Schmidt, MüKo HGB, § 257 Rn. 20; Böcking/Gros, in: Ebenroth u.a., HGB, § 257 Rn. 20; a.A. Weichert, DuD 2010, 679, 680.
[418] Thalhofer, CCZ 2011, 222 (224 f.).
[419] Weichert, DuD 2010, 679 (680).
[420] Winkeljohann/Philipps, in: Förschle u.a., Beck'scher Bilanz-Kommentar, § 257 Rn. 18.
[421] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 59.

und handelsrechtlich relevante Belege. In diesem Fall ist sicherzustellen, dass diese Informationen vollständig auf deutschem Boden gespeichert werden und ihr Serverstandort jederzeit nachvollziehbar ist.

## 3.4 E-Commerce-Richtlinie

Die als Richtlinie über den elektronischen Rechtsverkehr – oder kurz: E-Commerce-Richtlinie – bezeichnete europäische Regelung[422] enthält Vorschriften für Internet-Auftritte, die genutzt werden, um Handel zu treiben.[423] Werden SaaS-Umgebungen zum Betrieb eines Webshops genutzt, handelt es sich dabei um eine E-Commerce-Plattform im Anwendungsbereich der Richtlinie. Dann sind die entsprechenden, sehr bereichsspezifischen Vorschriften über Vertragsabschlüsse im Internet und damit verbundene Informationspflichten zu beachten (Art. 5 f.; 9 ff. der Richtlinie). Wird mittels einer Cloud-Infrastruktur Werbung versendet, werden die Einschränkungen aus Art. 7 der Richtlinie relevant. Beide Anwendungsfälle stellen jedoch kein typisches Szenario des Cloud Computing dar, sondern überschneiden sich eher gelegentlich und peripher mit der Thematik.

Von hoher Bedeutung für das Cloud Computing ist hingegen Art. 14 der Richtlinie. Die mit der Überschrift „Hosting“ versehene Rechtsnorm behandelt den Fall eines „[…] Dienstes der Informationsgesellschaft, der in der Speicherung von durch den Cloud-Anwender eingegebenen Informationen besteht […]“. Die Gewährung von Speicherplatz zur Aufbewahrung von Cloud-Anwenderdaten stellt gerade das Geschäftsmodell vieler Cloud-Anbieter dar.[424] Sie bestimmt, dass der Anbieter des Dienstes für die Inhalte der Cloud-Anwender nur haftet, wenn er konkrete Kenntnis von den Daten und deren Rechtswidrigkeit hat. Eine Pflicht, die von Cloud-Anwendern gespeicherten Daten regelmäßig zu sichten und zu kontrollieren, besteht nicht (Art. 15 der Richtlinie) und ist daher wegen des Gebots der Datensparsamkeit[425] auch nicht zulässig. Jedoch sollte sich ein Cloud-Diensteanbieter auf Fälle vorbereiten, in denen er Kenntnis von unrechtmäßigen Datenspeicherungen erlangt. Diese können beispielsweise Urheberrechtsverletzungen[426] oder im Fall einer öffentlich einsehbaren Cloud ehrverletzende Beleidigungen[427] umfassen. Macht ein Dritter wie etwa das Opfer des rechtswidrigen Zustands den Cloud-Diensteanbieter darauf aufmerksam, kann letzterer in die Haftung genommen werden, wenn er nicht unverzüglich die betreffenden Daten löscht oder sperrt. Kann dies aufgrund des Umfangs der Cloud und damit auch der Rechtsverletzungen nicht stets individuell und manuell erfolgen, sollten entsprechende Prozesse beim Cloud-Diensteanbieter eingerichtet

---

[422] Kompletter Titel: Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABl. Nr. L 178, S. 1.
[423] Kuner, European Data Protection Law, Rn. 5.119.
[424] Siehe oben S. 9.
[425] Siehe oben S. 19.
[426] Überbl. Schnabel, MMR 2008, 281; Volkmann, K&R 2006, 245.
[427] BGH, MMR 2007, 518; Bortloff, GRUR Int 1997, 387 (388).

werden. Dies sollte bei der Etablierung technischer und organisatorischer Maßnahmen[428] Berücksichtigung finden.

Die Inhalte der Richtlinie hat jeder Mitgliedstaat der Europäischen Union in sein nationales Recht zu integrieren.[429] In Deutschland ist dies überwiegend durch Vorschriften des Telemediengesetzes geschehen.[430] Wegen der Umsetzungsverpflichtung gelten inhaltsgleiche Bestimmungen auch im sonstigen Unionsgebiet.

## 3.5 Datenschutzrichtlinie für elektronische Kommunikation

Die auch als E-Privacy-Richtlinie bezeichnete Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[431] ergänzt die EG-Datenschutzrichtlinie mit speziellen Regelungen zu einzelnen Technologien. So betreffen zahlreiche Vorschriften des Rechtstextes beispielsweise nur Telefongespräche, vielfach adressiert sie jedoch auch Internet-Technologien im Allgemeinen.[432]

### 3.5.1 Anwendbarkeit auf Cloud Computing

Die Anwendung der Richtlinie auf das Cloud Computing ist damit grundsätzlich nicht ausgeschlossen. Voraussetzung ist nach Art. 3 Abs. 1 der Richtlinie 2002/58/EG, dass es sich dabei um „elektronische Kommunikationsdienste in öffentlichen Verkehrsnetzen“ handelt, die „öffentlich zugänglich“ sind. Die öffentliche Zugänglichkeit ist in der Regel bei Cloud-Diensteanbietern unproblematisch, soweit sie ihre Dienstleistung auf dem Markt anbieten. Die Frage, ob Clouds „elektronische Kommunikationsdienste“ sind, ist anhand der Definition aus Art. 2 lit. c) der Rahmenrichtlinie 2002/21/EG zu beurteilen.[433] Der Begriff bezeichnet demnach „gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen“. Entscheidend ist, dass die Signalübermittlung bei dem Service im Vordergrund steht und nicht die Inhalte der Kommunikation, wie dies etwa bei Websites zumeist der Fall ist.

Der Anwendungsbereich der Richtlinie 2002/58/EG ist damit deckungsgleich mit dem des Telekommunikationsgesetzes. Es wird deshalb auf die oben gemachten Ausführungen zum TKG verwiesen.[434] Cloud-Dienste sind danach im Regelfall keine elektronischen Kommunikationsdienste, die der Richtlinie unterfallen, weil zumeist der Erwerb von

---

[428] Siehe oben S. 24 ff.
[429] Vgl. oben S. 39.
[430] Siehe oben S. 34 ff.
[431] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 201, S. 37.
[432] Kuner, European Data Protection Law, Rn. 1.49.
[433] Dies folgt aus dem Verweis in Art. 2 S. 1 der Richtlinie 2002/58/EG, der auf die Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, ABl. Nr. L 108, S. 33, Bezug nimmt.
[434] Siehe oben S. 32.

Speicherplatz oder Rechnerleistung,[435] nicht aber der Datenaustausch im Vordergrund steht. Dennoch betrifft die Richtlinie manche Konstellationen des Cloud Computing.[436] Dies kann beispielsweise der Fall sein, wenn eine Cloud für die Synchronisation der Daten auf unterschiedlichen Geräten konzipiert ist. Je nach konkretem Aufbau der Architektur kann dies gegebenenfalls die Speicherung von Smart-Meter-Daten aus verschiedenen Haushalten auf einer gemeinsamen Plattform betreffen, wenn der Hauptzweck darin besteht, die Informationen zentral erfassen zu können.

### 3.5.2 Inhalt der Richtlinie

Ein Großteil der Regelungen in der Richtlinie 2002/58/EG ist von ihrem Sinn und Zweck her nicht oder nur in seltenen Fällen auf das Cloud Computing anwendbar. Dazu zählen beispielsweise Anforderungen an die Rufnummernunterdrückung oder an Einzelverbindungsnachweise bei Telefongesprächen (Art. 7 ff.).

Wesentlich für den Cloud-Bereich sind hingegen die Regelungen zu technischen und organisatorischen Maßnahmen (Art. 4). So hat der Cloud-Diensteanbieter in der Richtlinie nicht näher bezeichnete Maßnahmen zur Gewährleistung der Netzsicherheit zu betreiben. Dabei hat er ein angemessenes Verhältnis zwischen den Kosten und dem vorherrschenden Risiko zu wahren (Art. 4 Abs. 1). Diese Verpflichtung greift weniger weit als die gleichartige Regelung in § 8 BDSG, weil nach der Richtlinie nur Maßnahmen zu Gunsten der Netzsicherheit notwendig sind, nach dem BDSG jedoch zusätzlich solche zur Wahrung des Datenschutzes. Wird das nationale deutsche Recht eingehalten, ist die Hürde des Art. 4 Abs. 1 der Richtlinie somit auch genommen. Über bestehende Risiken für die Netzsicherheit und über Abhilfemaßnahmen hat der Diensteanbieter die Teilnehmer nach Art. 4 Abs. 2 unaufgefordert zu informieren. Diese Verpflichtung deckt sich mit der nahezu wortgleichen Formulierung aus § 93 des Telekommunikationsgesetzes.

Von Relevanz für Cloud-Dienste ist zudem Art. 5 der Richtlinie, wonach die Vertraulichkeit in elektronischen Kommunikationsdiensten zu gewährleisten ist. Insbesondere dürfen Nachrichten darin ohne Zustimmung der Betroffenen weder abgefangen noch überwacht werden (Art. 5 Abs. 1). Das Setzen von sogenannten Cookies wird durch Art. 5 Abs. 3 beschränkt. Eine solche „Speicherung von Informationen, (…) die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind“ setzt demnach eine umfassende Information und die Möglichkeit der Verweigerung durch den Teilnehmer voraus. Nutzer i.S.d. Richtlinie 2002/587EG ist eine natürliche Person, die einen öffentlich zugänglichen elektronischen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst notwendigerweise abonniert zu haben. Teilnehmer i.S.d. Richtlinie 2002/587EG ist ein Nutzer der einen Dienst abonniert hat.

Aus der Formulierung der Regelung wird abgeleitet, dass der Nutzer (bzw. Teilnehmer) einwilligen muss bzw. er Gelegenheit zum Widerspruch erhalten muss, bevor der Cookie gesetzt

[435] Vgl. Hansen, DuD 2012, 407 (408 f.).
[436] Marnau/Schlehahn, TClouds, Cloud Computing: Legal Analysis, S. 14 f.

wird.[437] Es ist keine explizite Zustimmung erforderlich, sondern lediglich der informierte Verzicht auf einen Widerspruch, was zu einer Opt-out-Lösung führt.[438] Da jedoch der Cookie erst nach und nicht während der Information gespeichert werden darf, steht das Verfahren faktisch einer Opt-in-Lösung gleich. Der Cookie darf auf dem Gerät des Nutzers erst dann gesetzt werden, wenn der Nutzer seine Zustimmung dazu signalisiert hat.[439] Die Beibehaltung der Standardeinstellungen des Browsers kann jedenfalls nicht als Einwilligung gewertet werden.[440] Vielmehr könnte das Informationserfordernis durch eine Pop-up-Fenster-Lösung oder ein Do-not-track-Plugin im Browser gelöst werden.[441]

### 3.5.3 Umsetzung und Wirksamkeit der Richtlinie

Wie jede Richtlinie der EU sind die Gesetzgeber der einzelnen Mitgliedstaaten ihre Adressaten. Sie sind verpflichtet, den Inhalt der Richtlinie in ihre nationale Rechtsordnung zu integrieren. Die in Art. 17 Abs. 1 festgelegte Umsetzungsfrist ist abgelaufen. Deutschland, Slowenien und Rumänien haben die Richtlinie noch nicht umgesetzt.[442] Informelle Antworten auf Anfragen bei der Kommission und beim deutschen Bundesministerium für Wirtschaft und Energie zeigen, dass diese Stellen davon ausgehen, die europäischen Vorgaben seien bereits durch das Telemediengesetz umgesetzt.[443] Dann wäre der Erlass weiterer Gesetze nicht notwendig. Eine Auslegung, die Umsetzung sei bereits durch das TMG erfolgt, ist jedoch bereits deshalb abzulehnen, weil die Richtlinie und das TMG unterschiedliche Anwendungsbereiche haben.

Als Folge einer Nichtumsetzung kommt unter Umständen die unmittelbare Anwendbarkeit der Richtlinie in Betracht.[444] Daraus können sich jedoch keine rechtlichen Verpflichtungen für private Stellen ergeben.[445] Die überwiegenden Inhalte der Richtlinie, die etwa Cookies oder technische und organisatorische Maßnahmen betreffen, beschreiben jedoch gerade das Verhältnis zwischen den Privatrechtssubjekten Diensteanbieter und Dienstteilnehmer. Eine direkte Rechtswirkung geht von den Vorschriften deshalb nicht aus.

Mangels Umsetzung entfaltet die Richtlinie 2002/58/EG also in Deutschland zurzeit keine wirksamen Verpflichtungen. Es muss aufgrund des unionsrechtswidrigen Zustandes aber davon ausgegangen werden, dass die Umsetzung in Zukunft erfolgen wird, sodass der Regelungsgehalt bei der Konzeption von Cloud-Architekturen bereits Berücksichtigung finden

---

[437] Art.-29-Datenschutzgruppe, WP 187; WP 208, S. 3; Heckmann, in: ders., jurisPK Internetrecht, Kap. 9, Rn. 554.
[438] Kuner, European Data Protection Law, Rn. 5.150.
[439] Schütze, ZD-Aktuell 2014, 03873.
[440] Artikel-29-Datenschutzgruppe, WP 171, S. 17.
[441] Heckmann, in: ders., jurisPK Internetrecht, Kap. 9, Rn. 554.
[442] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung zur Verfolgung des Nutzerverhaltens im Internet, abrufbar unter https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9759.de.
[443] Vgl. den Internet-Auftritt des Bundesverbands digitale Wirtschaft: http://www.bvdw.org/medien/eu-kommission-bestaetigt-e-privacy-richtlinie-in-deutschland-durch-telemediengesetz-umgesetzt?media=5474.
[444] EuGH, Rs. 8/81, Slg. 1982, 53, Rn. 29 – Becker.
[445] Schroeder, in: Streinz, EUV/AEUV, Art. 288 AEUV Rn. 106,

sollte. Zudem ist die Richtlinie in nahezu allen übrigen Mitgliedstaaten umgesetzt worden. Um nicht gegen deren nationale Umsetzungsgesetze zu verstoßen, ist der umgesetzte Inhalt der Richtlinie deshalb zu achten, sobald ein Cloud-Dienst die Grenzen der Bundesrepublik überschreitet.

# 4 Literaturverzeichnis

*Ambrock*, Jens: Die Übermittlung von S.W.I.F.T.-Daten an die Terrorismusaufklärung der USA, Berlin 2013

*Anderson*, Ross/*Fuloria*, Shailendra: Who controls the offswitch?, Cambridge 2010, abrufbar unter http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

AK Technik der Datenschutzbeauftragten des Bundes und der Länder: Arbeitspapier „Datenschutzfreundliche Technologien“, 1997; Auszug veröffentlicht in DuD 1997, 12

*Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder*: Orientierungshilfe – Cloud Computing, Düsseldorf 2011

*Artikel-29-Datenschutzgruppe*: Arbeitsdokument v. 24.07.1998 zur Übermittlung personenbezogener Daten in Drittstaaten, WP 12

– Stellungnahme 1/99 zum Stand des Datenschutzes in den Vereinigten Staaten und zu den derzeitigen Verhandlungen zwischen der Europäischen Kommission und der amerikanischen Regierung, WP 15

– Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136

– Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171

– Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht, WP 173

– Stellungnahme 5/2012 zum Cloud Computing, WP 196

– Arbeitsunterlage 2/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies, WP 208

*Assey*, James/*Eleftheriou*, Demetrios: The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?, Commlaw Conspectus Vol. 9 (2001), 145, abrufbar unter http://scholarship.law.edu/cgi/viewcontent.cgi?article=1224&context=commlaw

*Baumgartner*, Ulrich/*Ewald*, Konstantin: Apps und Recht, München 2013

*Bäumler*, Helmut: Audits und Gütesiegel im Datenschutz, CR 2001, 795

– Ein Gütesiegel auf den Datenschutz, Made in Schleswig-Holstein, DuD 2004, 80

*Becker*, Florian/*Ambrock*, Jens: Datenschutz in den Polizeigesetzen, JA 2011, 561

*Becker*, Philipp/*Nikolaeva*, Julia: Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG, Zur Unmöglichkeit rechtskonformer Datenübermittlung für gleichzeitig in USA und Deutschland operierende Cloud-Anbieter, CR 2012, 170

*Bedner*, Mark: Schutzziele der IT-Sicherheit, DuD 2010, 323

– Cloud Computing, Technik, Sicherheit und rechtliche Gestaltung, Kassel 2013

*Bergmann*, Lutz/*Möhrle*, Roland/*Herb*, Armin: Datenschutzrecht, Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz, 47. EL Stuttgart 2014

*Berliner Datenschutzbeauftragte, der*: Jahresbericht 2008, Berlin 2008

*Berthold*, Oliver/*Borges*, Georg/*Cellarius*, Mathias/*Dehmel*, Susanne/*Doms*, Thomas: Kompetenzzentrum Trusted Cloud, Rechtsfragen des Cloud Computing Nr. 4, Arbeitspapier – Modulare Zertifizierung von Cloud-Diensten, Berlin 2014, abrufbar unter http://www.trusted-cloud.de/369.php.

*Bizer*, Johann: Sieben Goldene Regeln des Datenschutzes, DuD 2007, 350

*Blume*, Peter: Transborder Data Flow: Is There a Solution in Sight?, Int. Journal of Law and Information Technology, Volume 8/2000, S. 65

– Data Protection in the Cloud, CRi 2011, 76

*Borges*, Georg/*Schwenk*, Georg (Hrsg.): Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce, Berlin/Heidelberg 2012

*Bortloff*, Nils: Die Verantwortlichkeit von online-Diensten, Ein Überblick über den internationalen Diskussionsstand in den USA, Kanada, Australien, Großbritannien, Frankreich, der Schweiz und in Deutschland, GRUR Int 1997, 387

*Bowden*, Caspar: The US surveillance programmes and their impact on EU citisens' fundamental rights, Brüssel 2013, Briefingnote des Europäischen Parlaments, Plenardokument Nr. PE 474.405

*Breyer*, Patrick: (Un-)Zulässigkeit einer anlasslosen, siebentägigen Vorratsdatenspeicherung – Grenzen des Rechts auf Anonymität, MMR 2011, 573

*Bundesbeauftragte für den Datenschutz, der*: 20. Tätigkeitsbericht 2003-2004, Berlin 2005, auch BT-Drs. 15/5252

*Bundesministerium für Wirtschaft und Energie*, Bausteine für die Energiewende: 7 Eckpunkte für das „Verordnungspaket intelligente Netze", Februar 2015, abrufbar unter www.bmwi.de/BMWi/Redaktion/PDF/E/eckpunkte-fuer-das-verordnungspaket-intelligente-netze

*Calliess*, Christian/*Ruffert*, Matthias: EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 4. Auflage München 2011

*Caspar*, Johannes: Geoinformation und Datenschutz am Beispiel des Internetdienstes Google Street View, DÖV 2009, 965

*Catuogno, Luis/Löhr, Hans/Manulis, Mark/Sadeghi, Ahmed-Reza/Stüble, Christian/ Winandy, Marcel: Trusted Virtual Domains: Color Your Network, DuD 2010, 289*

*Chuvakin*, Anton: The Doom of Information Security Methods to thwart insider attacks: products, techniques and policies, 2002

*Connolly*, Chris: The US Safe Harbor – Fact or Fiction?, Pyrmont (Australien) 2008, abrufbar unter http://www.galexia.com/public/research/articles/research_articles-pa07.html

*Dammann*, Ulrich: Der EuGH im Internet – Ende des internationalen Datenschutzes?, RDV 2004, 19

*Dammann*, Ulrich/*Simitis*, Spiros: EG-Datenschutzrichtlinie, Baden-Baden 1997

*Däubler*, Wolfgang/*Klebe*, Thomas/*Wedde*, Peter/*Weichert*, Thilo: Bundesdatenschutzgesetz, 4. Auflage Frankfurt a.M. 2014

*Deiseroth*, Dieter: Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?, ZRP 2013, 194

*Dix*, Alexander: Safe Harbor am Ende? – Eine Betrachtung aus aufsichtsbehördlicher Sicht; Vortrag beim 9. Europäischen Datenschutztag am 28.01.2015 in Berlin, abrufbar unter http://www.datenschutz-berlin.de/attachments/1089/741_943_1.pdf?1424256331.

*Drallé*, Lutz: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Kiel 2010

*Ebenroth*, Carsten/*Boujong*, Karlheinz/*Joost*, Detlev/*Strohn*, Lutz: Handelsgesetzbuch, 3. Auflage München 2014

*Ehmann*, Eugen/*Helfrich*, Marcus: EG-Datenschutzrichtlinie, Köln 1999

*Eisenberg*, Ulrich: Beweisrecht der StPO, 8. Auflage München 2011

*Engel*, Alexandra: Reichweite und Umsetzung des Datenschutzrechts gemäß der Richtlinie 95/46/EG für aus der Europäischen Union in Drittländer exportierte Daten am Beispiel der USA, Berlin 2003

*Engeler*, Malte/*Deibler*, Daniel/*Hansen*, Marit/*Jensen*, Meiko/*Obersteller*, Hannah: MonIKA, Ausarbeitung aus Perspektive des Datenschutzes und der Datensicherheit zur Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internet-Infrastrukturen, Kiel 2014

*Engels*, Thomas: Datenschutz in der Cloud – Ist hierbei immer eine Auftragsdatenverarbeitung anzunehmen?, K&R 2011, 548

*Epping*, Volker: Grundrechte, 5. Auflage Heidelberg 2012

*ders./Hillgruber*, Christian (Hrsg.): Beck'scher Online-Kommentar Grundgesetz, 23. Edition München 2014

*Erbs*, Georg/*Kohlhaas*, Max (Hrsg.): Strafrechtliche Nebengesetze, 195. EL München 2013

*Erd*, Rainer: Zehn Jahre Safe Harbor Abkommen – kein Grund zum Feiern, K&R 2010, 624

*Ewer*, Wolfgang/*Thienel*, Tobias: Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 30

*Federrath*, Hannes/*Pfitzmann*, Andreas: Gliederung und Systematisierung von Schutzzielen in IT-Systemen, DuD 2000, 704

*Förschle*, Gerhart/*Grottel*, Bernd/*Schmidt*, Stefan/*Schubert*, Wolfgang/*Winkeljohann*, Norbert (Hrsg.): Beck'scher Bilanz-Kommentar, Handels- und Steuerbilanz, 9. Auflage München 2014

*Fröhle*, Jens: Web Advertising, Nutzerprofile und Teledienstedatenschutz, München 2003

*Gaul*, Björn/*Koehler*, Lisa-Marie: Mitarbeiterdaten in der Computer Cloud, Datenschutzrechtliche Grenzen des Outsourcing, BB 2011, 2229

*Geiger*, Andreas: Charlie versus Charly, EuZW 2015, 161

*Geminn*, Christian: Die Debatte um nationales Routing – eine Scheindebatte?, Eine kritische Analyse der Argumentationslinien, MMR 2015, 98

*Geppert*, Martin/*Schütz*, Raimund (Hrsg.): Beck'scher TKG-Kommentar, 4. Auflage München 2013

*Gercke*, Marco: Die Entwicklung des Internetstrafrechts 2012/2013, ZUM 2013, 605

*Glior*, Edward: Begriffserklärungen zur Sicherheit der Informationssysteme, DuD 1991, 641

*Gola*, Peter/*Klug*, Christoph: Grundzüge des Datenschutzrechts, München 2003

*Gola*, Peter/*Schomerus*, Rudolf (Hrsg.), Bundesdatenschutzgesetz, 10. Auflage München 2010

*Golland*, Alexander: Datenschutz durch modulare Zertifizierung: Trusted Cloud-Pilotprojekt bringt neuen Ansatz, Datenschutz-Berater 2014, 213

*Góralczyk*, Magdalena: USA: Jewel v. NSA – The Court Dismisses the Case Due to State Secrets Privilege, ZD-Aktuell 2015, 04568

*Graf*, Peter: Strafprozessordnung mit RiStBV und MiStra, 18. Edition München 2014

*Grünwald*, Andreas/*Döpkens*, Harm-Randolf: Cloud Control?, Regulierung von Cloud-Computing-Angeboten, MMR 2011, 287

*Guttenberg*, Ulrich: Die heimliche Überwachung von Wohnungen – Zur verfassungsrechtlichen Problematik des § 9 II, III BVerfSchG und verwandter Vorschriften, NJW 1993, 567

*Hansen*, Marit: Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter, DuD 2012, 407

*Hansen*, Marit*/Meissner*, Sebastian (Hrsg.): Verkettung digitaler Identitäten, Kiel 2007

*Heckmann*, Dirk (Hrsg.): Juris Praxiskommentar Internetrecht, 3. Auflage Saarbrücken 2011

*Heide*, Nils: Harmonisierungsaufgaben im internationalen Technologietransfer – Zum Schutz von Herstellungstechnologien in der Volksrepublik China, GRURInt 2008, 12

*Heidrich*, Joerg/*Forgó*, Nikolaus/*Feldmann*, Thorsten: Heise Online-Recht, Der Leitfaden für Praktiker und Juristen, 2. Ergänzungslieferung Hannover 2010

*Heidrich*, Joerg/*Wegener, Christoph*: Sichere Datenwolken, Cloud Computing und Datenschutz, MMR 2010, 803

*Heil*, Helmut: Europäische Herausforderung – Transatlantische Debatte, DuD 1999, 458

*Hennrich*, Thorsten: Compliance in Clouds, Datenschutz und Datensicherheit in Datenwolken, CR 2011, 546

*Hill*, Hermann/*Schliesky*, Utz (Hrsg.): Innovationen im und durch Recht, E-Volution des Rechts- und Verwaltungssystems II, Baden-Baden 2010

*Hillenbrand-Beck*, Renate: Aktuelle Fragestellungen des internationalen Datenverkehrs, RDV 2007, 231

*Hoeren*, Thomas: Virenscanning und Spamfilter – Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co., NJW 2004, 3513

*Hoeren*, Thomas*/Sieber*, Ulrich/*Holznagel*, Bernd: Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 39. Ergänzungslieferung München 2014

*Hoffmann*, Christian: Apps der öffentlichen Verwaltung – Rechtsfragen des Mobile Government, MMR 2013, 631

*Holtorf*, Marc: Cloud Computing – Ein Überblick (Teil 2), MPR 2013, 196

*Hömig*, Dieter: Grundgesetz, 8. Auflage Baden-Baden 2007

*Hornung*, Gerrit: Der Personenbezug biometrischer Daten, DuD 2004, 429

*Hufen*, Friedhelm: Staatsrecht II, Grundrechte, 4. Auflage München 2014

*Jarass*, Hans: Charta der Grundrechte der Europäischen Union, München 2010

*Joecks*, Wolfgang/*Schmitz*, Roland (Hrsg.): Münchener Kommentar zum Strafgesetzbuch, Band 6/1, Nebenstrafrecht II, München 2010

*Jotzo*, Florian: Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232

– Der Schutz personenbezogener Daten in der Cloud, Berlin 2013

*Karden*, Wilfried/*v. Freiberg*, Alexander: Praxishandbuch Unternehmenssicherheit, Sicherheit im Mittelstand, Norderstedt 2011

*Karg*, Moritz: Anmerkung zu BGH, Speicherung dynamischer IP-Adressen, MMR 2011, 341

*Karg*, Moritz: Datenschutzrechtliche Rahmenbedingungen beim Einsatz intelligenter Zähler, DuD 2010, 365

*Kilian*, Wolfgang/*Heussen*, Benno (Hrsg.): Computerrechts-Handbuch, Informationstechnik in der Rechts- und Wirtschaftspraxis, 30. Ergänzungslieferung München 2011

*Klein*, Franz (Hrsg.): Abgabenordnung einschließlich Steuerstrafrecht, 12. Auflage München 2014

*Klug*, Christoph: Beispiele richtlinienkonformer Auslegung des BDSG, RDV 2001, 266

*Kompetenzzentrum Trusted Cloud*: Thesenpapier – Datenschutzrechtliche Lösungen für Cloud Computing, Berlin 2014

*Koschwald*, Steffen/*Wicker*, Magda: Kanzleien und Praxen in der Cloud – Strafbarkeit nach § 203 StGB, CR 2012, 758

*Kuner*, Christopher: European Data Protection Law, Corporate and Regulation, 2. Auflage Oxford 2007

*Leupold*, Andreas: Münchener Anwaltshandbuch IT-Recht, 3. Auflage München 2013

– Geschäftsgeheimnisse gehören in die (Private) Cloud, MMR 2014, 145

*Liebau*, Tobias: Cyber-Crime – die strafrechtliche Verantwortlichkeit von Internetprovidern nach dem TDG/MDStV, Jura 2006, 520

*Maunz*, Theodor/*Dürig*, Günter (Hrsg.): Grundgesetz, 72. Ergänzungslieferung München 2014

*Marnau*, Ninja/*Schlehahn*, Eva: TClouds, Cloud Computing – Legal Analysis, Kiel 2011

– Cloud Computing und Safe Harbor, DuD 2011, 311.

*Martino*, Alessandra di: Datenschutz im europäischen Recht, Baden-Baden 2005

*Mattis*, Peter: The Analytic Challenge of Understanding Chinese Intelligence Services, Studies in Intelligence, Vol. 56 (2012), No. 3, S. 47

*Maunz*, Theodor/*Dürig*, Günter (Hrsg.): Grundgesetz, 71. Ergänzungslieferung München 2014

*Meissner*, Sebastian: Zertifizierungskriterien für das Datenschutzgütesiegel EuroPriSe, DuD 2008, 525

*Mell*, Peter/*Grance*, Timothy: The NIST Definition of Cloud Computing, NIST SP 800-145, 2011

*Müller-Broich*, Jan: Telemediengesetz, Baden-Baden 2012

*Nägele*, Thomas/*Jacobs*, Sven: Rechtsfragen des Cloud Computing, ZUM 2010, 281

*Niemann*, Fabian/*Hennrich*, Thorsten: Kontrolle in den Wolken?, Auftragsdatenverarbeitung in Zeiten des Cloud Computings, CR 2010, 686

*Niemann*, Fabian/*Paul*, Jörg-Alexander: Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings, K&R 2009, 444

*Nungesser*, Jochen: Hessisches Datenschutzgesetz, 2. Auflage Mainz 2001

*Opfermann*, Elisabeth: Datenschutzkonforme Vertragsgestaltung im „Cloud Computing“, ZEuS 2012, 121

*Pahlen-Brandt*, Ingrid: Datenschutz braucht scharfe Instrumente, Beitrag zur Diskussion um „personenbezogene Daten“, DuD 2008, 34

*Parker*, Donn: Neuformulierung der Grundlagen der Informationssicherheit, DuD 1991, 557

*Pech*, Sebastian: Lizenzmodelle in der Cloud, Diskussionsbericht zum gleichnamigen Symposion des Instituts für Urheber- und Medienrecht am 18. Oktober 2013, ZUM 2014, 22

*Petri*, Thomas: Unzulässige Vorratssammlungen nach dem Volkszählungsurteil? Die Speicherung von TK-Verkehrsdaten und Flugpassagierdaten, DuD 2008, 729

*Plath*, Kai-Uwe (Hrsg.): Bundesdatenschutzgesetz, Köln 2013

*Raabe*, Oliver/*Lorenz*, Mieke/*Pallas*, Frank/*Weis*, Eva: Datenschutz und Smart Grid in der Elektromobilität, Karlsruhe 2011, abrufbar unter http://compliance.zar.kit.edu/21_438.php

*Ragland*, Leigh/*McReynolds*, Joseph/*Southerland*, Matthew/*Mulvenon*, James: Red Cloud Rising, Cloud Computing in China, Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, 2. Auflage Washington D.C. 2014, abrufbar unter http://www.uscc.gov/sites/default/files/Research/DGI_Red Cloud Rising_2014.pdf

*Rath*, Michael/*Rothe*, Britta: Cloud Computing: Ein datenschutzrechtliches Update, K&R 2013, 623

*Räther*, Philipp/*Seitz*, Nicolai: Übermittlung personenbezogener Daten in Drittstaaten, Angemessenheitsklausel, Safe Harbor und die Einwilligung, MMR 2002, 425

*Reiser*, Christof: Rechtliche Aspekte der Zahlungsverkehrsnetze, WM 1986, 1401

*Roßnagel*, Alexander (Hrsg.): Handbuch Datenschutzrecht, die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003

– Anmerkung zu EuGH, Urteil vom 6.11.2003,Rs. C-101/01 Lindqvist/Schweden – Personenbezogene Daten im Internet, MMR 2004, 99

*Roßnagel*, Alexander/*Scholz*, Philip: Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721

*Ruhmann*, Ingo: NSA, IT-Sicherheit und die Folgen, DuD 2014, 40

*Sachs*, Michael: Grundgesetz, 6. Auflage München 2011

*Säcker*, Franz/*Rixecker*, Roland (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 10, 5. Auflage München 2010

*Schaar*, Peter: Lässt sich die globale Internetüberwachung noch bändigen?, ZRP 2013, 214

*Schaffland*, Hans-Jürgen/*Wiltfang*, Noeme (Hrsg.): Bundesdatenschutzgesetz, Ergänzungslieferung 3/14 Berlin 2014

*Schellenberg*, Ulrich: Wie die bürgerliche Freiheit im digitalen Fegefeuer verbrennen könnte, „Super-Grundrecht auf Sicherheit“ hebelt das System der Grundrechte nicht aus, ZRP 2014, 24

*Scheurle*, Klaus-Dieter/*Mayen*, Thomas (Hrsg.): Telekommunikationsgesetz, 2. Auflage München 2008

*Schild*, Hans-Hermann: Die EG-Datenschutz-Richtlinie, EuZW 1996, 549

*Schipper*, Martin: Neue Instrumente des Datenschutzes für das Verhältnis zwischen Privatpersonen und Unternehmen in der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika, Münster 2003

*Schlikker*, Michael: Anwendung des Europarechts auf das britische TEMPORA-Programm, NJOZ 2014, 1281

*Schmidl*, Martin: E-Mail-Filterung am Arbeitsplatz, MMR 2005, 343

*Schmidt*, Karsten: Münchener Kommentar zum Handelsgesetzbuch, 3. Auflage 2012

*Schnabel*, Christoph: Böse Zensur, guter Filter? – Urheberrechtliche Filterpflichten für Access-Provider, MMR 2008, 281

*Schröder*, Christian: (Un)Safe Harbor and Cloud Services in Germany under Scrutiny, ZD-Aktuell 2015, 04531

*Schröder*, Christian /*Haag*, Nils: Studie zu staatlichen Zugriffen beim Cloud Computing, ZD-Aktuell 2012, 03132

*Schröder*, Christian /*Spies*, Axel: USA: Vorlage von E-Mails an US-Behörden, die auf Servern in Irland gespeichert sind – Neue Gefahren für US-Clouds?, ZD-Aktuell 2014, 03194

*Schulz*, Carsten/*Rosenkranz*, Timo: Cloud Computing – Bedarfsorientierte Nutzung von IT-Ressourcen, ITRB 2009, 232

*Schulz*, Sönke: Cloud Computing in der öffentlichen Verwaltung, Chancen – Risiken – Modelle, MMR 2010, 75

*Schuppert*, Stefan/*von Reden*, Armgard: Einsatz internationaler Cloud-Anbieter: Entkräftung der Mythen, ZD 2013, 210

*Schuster*, Fabian/*Reichl*, Wolfgang: Cloud Computing & SaaS: Was sind die wirklich neuen Fragen?, CR 2010, 38

*Schütze*, Benjamin: Facebook: Irische Datenschutzbehörde veröffentlicht Abschlussbericht zum Re-Audit, ZD-Aktuell 2012, 03267

– Art. 29-Datenschutzgruppe: Stellungnahme zur Anwendung der sog. Cookie-RL, ZD-Aktuell 2014, 03873

*Siemen*, Birte: Datenschutz als europäisches Grundrecht, Berlin 2006

*Simitis*, Spiros (Hrsg.): Bundesdatenschutzgesetz, 8. Auflage Baden-Baden 2014

*Sinewe*, Patrick/*Frase*, Henning: Steuerrechtliche Aspekte des Cloud Computing, BB 2011, 2198

*Spies*, Axel: USA: Grenzüberschreitende elektronische Beweiserhebung (Discovery) vs. Datenschutz?, MMR 7/2007, V

– Europa: Wer hat Angst vor dem US-Patriot Act?, ZD-Aktuell 2012, 03062

*Spies*, Axel/*Schröder*, Christian: Cloud Computing und EU/US Safe Harbor Principles – US-Handelsministerium bezieht Stellung, ZD-Aktuell 2013, 03566

*Spindler*, Gerald/*Schmitz*, Peter/*Geis*, Ivo: Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz, München 2004

*Spindler*, Gerald/*Schuster*, Fabian (Hrsg.): Recht der elektronischen Medien, 2. Auflage München 2011

*Stelkens*, Paul/*Bonk*, Joachim/*Sachs*, Michael (Hrsg.): Verwaltungsverfahrensgesetz, 8. Auflage München 2014

*Stenzel*, Rainer: Datenschutz zwischen Utopie und Anpassung, Die politische Debatte um einen polizeilichen Datenaustausch mit den USA, ZFAS 2010, 137

*Stern*, Klaus/*Becker*, Florian (Hrsg.): Grundrechte-Kommentar, Die Grundrechte des Grundgesetzes mit ihren europäischen Bezügen, Köln 2009

*Streinz*, Rudolf: Die Rechtsprechung des EuGH zum Datenschutz, DuD 2011, 602

– Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Auflage München 2012

*Taeger*, Jürgen (Hrsg.): Law as a Service - Recht im Internet- und Cloud-Zeitalter, Oldenburg 2013

*Taeger*, Jürgen/*Gabel*, Detlev: Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage Frankfurt a.M. 2013

*Tamm*, Marina: Rückwirkungen des gescheiterten SWIFT-Abkommens auf das Abkommen über Fluggastdaten?, VuR 2010, 215

*Thalhofer*, Thomas: Grenzenlos: Compliance bei Cloud Computing, CCZ 2011, 222

*Thüsing*, Gregor (Hrsg.): Beschäftigtendatenschutz und Compliance, 2. Auflage München 2014

*Többens*, Hans: Wirtschaftsspionage und Konkurrenzausspähung in Deutschland, NStZ 2000, 505

*Uerpmann-Wittzack*, Robert (Hrsg.): Das neue Computergrundrecht, Münster 2009

*Voigt*, Paul: Weltweiter Datenzugriff durch US-Behörden, Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten, MMR 2014, 158

*ders./Klein*, David: Deutsches Datenschutzrecht als „blocking statute“?, Auftragsdatenverarbeitung unter dem USA PATRIOT Act, ZD 2013, 16

*Volkmann*, Christian: Aktuelle Entwicklungen in der Providerhaftung im Jahr 2005, K&R 2006, 245

*Weber*, Marc/*Voigt*, Paul: Internationale Auftragsdatenverarbeitung - Praxisempfehlungen für die Auslagerung von IT-Systemen in Drittstaaten mittels Standardvertragsklauseln, ZD 2011, 74

*Weichert*, Thilo: Datenschutz-Audit und -Gütesiegel im Medizinbereich, MedR 2003, 674

– Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, DuD 2009, 347

– Cloud Computing und Datenschutz, DuD 2010, 679

– Globaler Kampf um digitale Grundrechte, KJ 2014, 123

– Datenschutz im Auto – Teil 2, Das Kfz als großes Smartphone mit Rädern, SVR 2014, 241

*Weniger*, Robert: Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen, Nach Maßgabe der Europäischen Datenschutzrichtlinie 95/46/EG, Hamburg 2005

*Wiesemann*, Hans Peter: IT-rechtliche Rahmenbedingungen für „intelligente" Stromzähler und Netze, Smart Meter und Smart Grids, MMR 2011, 355

*Wohlgemuth*, Hans/*Gerloff*, Jürgen: Datenschutzrecht, eine Einführung mit praktischen Fällen, 3. Auflage Neuwied 2005

*Wuermeling*, Ulrich/*Felixberger*, Stefan: Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, 230

*Wybitul*, Tim/*Schuppert*, Stefan/*von Schweinitz*, Antoinette: Irish High Court Refers Questions to European Court of Justice: Can National DPAs Disregard Safe Harbor?, ZD-Aktuell 2014, 1

*Zimniock*, Klaus: Das Grundrecht der Unverletzlichkeit der Wohnung und die Enteignung, DÖV 1954, 392