Orientierungshilfe – Cloud Computing

der Arbeitskreise Technik und Medien
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises

Version 2.0
Stand 09.10.2014

In der Arbeitsgruppe haben mitgewirkt:

Jens Budszus (Die Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht Brandenburg)
Oliver Berthold (Berliner Beauftragter für Datenschutz und Informationsfreiheit)
Alexander Filip (Bayerisches Landesamt für Datenschutzaufsicht)
Dr. Sven Polenz (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
Dr. Thomas Probst (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)
Maren Thiermann (Der Hessische Datenschutzbeauftragte)

Inhaltsübersicht

0 Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder beschäftigen sich bereits seit längerer Zeit mit der Thematik des Cloud Computing. Da das Thema weiter an Aktualität gewonnen hat, wurde von den Arbeitskreisen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises die vorliegende Orientierungshilfe erarbeitet. Die Orientierungshilfe richtet sich an Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche und soll den datenschutzgerechten Einsatz dieser Technologie fördern.

Der Schwerpunkt liegt dabei auf Hinweisen bei der Nutzung von Cloud-Computing-Diensten durch datenverarbeitende Stellen.

Anbieter von Cloud-Computing-Dienstleistungen können aus dieser Orientierungshilfe diejenigen Anforderungen entnehmen, die ihre Kunden aus datenschutzrechtlicher Sicht stellen.

1 Einführung

Nutzen

„Cloud Computing“ steht für „Datenverarbeitung in der Wolke“ und beschreibt eine über Netze angeschlossene Rechnerlandschaft, in welche die eigene Datenverarbeitung ausgelagert wird.[1] Teilweise wird von Cloud Computing auch dann gesprochen, wenn eine oder mehrere IT-Dienstleistungen (Infrastruktur, Plattformen, Anwendungssoftware) aufeinander abgestimmt, schnell und dem tatsächlichen Bedarf angepasst sowie nach tatsächlicher Anwendung abrechenbar über ein Netz bereitgestellt werden.[2] Cloud Computing kann auch als eine Form der bedarfsgerechten und flexiblen Anwendung von IT-Dienstleistungen verstanden werden, indem diese in Echtzeit als Service über das Internet bereitgestellt werden und danach eine Abrechnung erfolgt. Damit ermöglicht Cloud Computing eine Umverteilung von Investitions- und Betriebsaufwand. Die IT-Dienstleistungen können sich wiederum auf Anwendungen, Plattformen für Anwendungsentwicklungen und -betrieb sowie auf die Basisinfrastruktur beziehen. Dabei hat sich eine Einteilung in die drei Cloud-Services bzw. Organisationsformen „Software as a Service“, „Platform as a Service“ und „Infrastructure as a Service“ weitgehend durchgesetzt. Weiterhin wird zwischen „Public-, Private-, Hybrid- und Community-Clouds“ differenziert.[3]

Die Entstehung jener Form der Datenverarbeitung ist eng verbunden mit der enormen Steigerung der Rechenleistung, der flächendeckenden Verfügbarkeit höherer Bandbreiten für die Datenübertragung und der einfachen Einsetzbarkeit von Virtualisierungstechnologien. Als Synthese von IT- und Telekommunikations-Leistungen führt Cloud Computing dazu, dass – einfach dargestellt – jegliche Leistung als Ser-vice erhältlich wird. Cloud Computing repräsentiert somit den Gedanken von „Services aus dem Netz“, vergleichbar mit „Strom aus der Steckdose“. Cloud Computing lässt sich damit auch als eine dynamisch allokierbare Infrastruktur verstehen, in der Kapazitäten und Services nach Bedarf bezogen werden können und die Grundlage dieser Struktur in der Virtualisierung von Hardware, des Speichers, des Netzwerks und der Software besteht.[4]

Datenschutzrechtliche Schwerpunkte

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen von Cloud-Services sind alle datenschutzrechtlichen Bestimmungen einzuhalten. Cloud Computing darf nicht zu einer Absenkung der Datenschutzstandards im Vergleich zur herkömmlichen Datenverarbeitung führen[5]. Personenbezogen sind nur Da-

---

[1] Weichert, Cloud Computing und Datenschutz, DuD 2010, 679. Vgl. auch Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, Meinungsspiegel: Was ist Cloud-Computing?, S. 147 ff.

[2] Alex D. Essoh (BSI): Cloud Computing und Sicherheit – Geht denn das?, 2009, www.bsi.bund.de/cln_174/ContentBSI/Aktuelles/Veranstaltungen/gstag/gstag_091119.html.

[3] Vgl. BITKOM-Leitfaden: Cloud Computing – Evolution in der Technik, Revolution im Business, 2009, www.bitkom.org/de/themen/36129_61111.aspx.

[4] So Ulrich Roderer: Cloud Computing, SaaS, PaaS und IaaS verändert die Geschäftsmodelle der Dienstleister, 2010, www.searchdatacenter.de/themenbereiche/cloud/infrastruktur/articles/258317/.

[5] So auch die Empfehlung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation („Berlin Group“) im Sopot-Memorandum zu Cloud Computing – Fragen des Schutzes der Pri-

ten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Ein verfassungsrechtlicher Schutz personenbezogener Daten besteht zudem durch das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[6] Die folgenden Erörterungen beziehen sich nur auf das für die nichtöffentlichen Stellen und die Bundesverwaltung geltende BDSG. Soweit die Anwendung von Cloud-Services auch für öffentliche Stellen an Bedeutung gewinnt, müssen diese die entsprechenden Regelungen in den Landesdatenschutzgesetzen einhalten. Teilweise entsprechen die Vorschriften der Landesdatenschutzgesetze den Vorschriften des BDSG, teilweise können aber auch erhebliche Unterschiede bestehen. Es ist daher eine sorgfältige Prüfung geboten.[7] Ebenso müssen spezielle Vorschriften beachtet werden, wie beispielsweise § 80 SGB X, der für die Auftragsdatenverarbeitung im Sozialbereich gilt. Für das Cloud Computing ergeben sich dabei sowohl aus Sicht des Datenschutzes als auch der IT-Sicherheit folgende Besonderheiten:

Vermeintlich als anonymisiert angesehene Daten (vgl. § 3 Abs. 6 BDSG) können durch ihre Verarbeitung in der Cloud reidentifizierbar werden, weil verschiedene Beteiligte über Zusatzwissen verfügen, mit dem eine Reidentifizierung möglich ist.[8] Für die verantwortliche Stelle (§ 3 Abs. 7 BDSG) muss daher deutlich werden, in welchem Rahmen Datenschutzbestimmungen einzuhalten sind.

Bei der Anwendung von Cloud-Services und der Bereitstellung von IT-Dienstleistungen werden regelmäßig mehrere Beteiligte tätig. Hier ist von Bedeutung, wie deren Beziehungen zueinander datenschutzrechtlich zu bewerten sind und wie vor allem die verantwortliche Stelle ihren Verpflichtungen nachkommt.

Die verantwortliche Stelle hat die Rechtmäßigkeit der gesamten Datenverarbeitung zu gewährleisten, insbesondere muss sie ihren Löschpflichten nachkommen (§ 35 Abs. 2 BDSG), unrichtige Daten berichtigen (§ 35 Abs. 1 BDSG), für eine Sperrung von Daten sorgen (§ 35 Abs. 3 BDSG) und dem Betroffenen (§ 3 Abs. 1 BDSG) u. a. Auskünfte über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, erteilen (§ 34 Abs. 1 BDSG). Zur Erfüllung der entsprechenden gesetzlichen Bestimmungen muss die verantwortliche Stelle besondere Vorkehrungen treffen.

Zu untersuchen ist die Zulässigkeit grenzüberschreitender Datenverarbeitungen. Bei Clouds, die international verteilt sind und sich auch über Staaten außerhalb des EWR erstrecken, ist eine Rechtsgrundlage für die Übermittlung personenbezogener Daten in Drittstaaten erforderlich.

Aus technisch-organisatorischer Sicht müssen vor allem besondere Vorkehrungen für die ordnungsgemäße Löschung und Trennung von Daten sowie für die Sicherstellung von Transparenz, Integrität und Revisionsfähigkeit der Datenverarbeitung getroffen werden.

---

vatsphäre und des Datenschutzes v. 24.4.2012, in: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Dokumente zu Datenschutz und Informationsfreiheit 2012, 171, 174.

[6] BVerfG, Urteil v. 27.02.2008, 1 BvR 370/07.

[7] Siehe hierzu auch Fußnote 38.

[8] Weichert, Cloud Computing und Datenschutz, DuD 2010, 679, 681.

Bei Nichteinhaltung der Datenschutzbestimmungen drohen der verantwortlichen Stelle haftungsrechtliche Konsequenzen, indem diese gegenüber den Betroffenen zum Schadensersatz verpflichtet ist, Bußgelder verhängt oder Anordnungen (§ 38 Abs. 5 BDSG) verfügt werden können. Weiterhin entstehen bei unrechtmäßiger Kenntniserlangung von Daten gegenüber der zuständigen Aufsichtsbehörde und den Betroffenen Informationspflichten (§ 42a BDSG).

2 Begriffe

In der Praxis besteht keine einheitliche Terminologie der Begriffe. Die Definitionen haben sich an den Ausführungen des BSI und des Fraunhoferinstitutes für Offene Kommunikationssysteme orientiert und werden der Bewertung zugrunde gelegt.

Cloud-Anwender

Cloud-Anwender ist jede natürliche oder juristische Person, die von Betroffenen personenbezogene Daten erhebt, verarbeitet oder nutzt und hierfür von anderen Stellen IT-Dienstleistungen für Cloud-Services in Anspruch nimmt.

Cloud-Anbieter

Cloud-Anbieter ist jede natürliche oder juristische Person, die einem Cloud-Anwender IT-Dienstleistungen für Cloud-Services bereitstellt. Fehlen dem Cloud-Anbieter hierfür die Ressourcen, so kann dieser zur Erfüllung seiner Verpflichtungen gegenüber dem Cloud-Anwender u. U. weitere Unter-Anbieter einbeziehen.

Public Cloud

IT-Dienstleistungen für Public Clouds werden am freien Markt und nicht innerhalb einer Institution oder im internen Unternehmensbereich einer verantwortlichen Stelle angeboten. Sie können folglich von einer beliebigen Zahl von Cloud-Anwendern in Anspruch genommen werden.[9]

Private Cloud

IT-Dienstleistungen werden hierbei innerhalb einer Institution oder im internen Unternehmensbereich einer verantwortlichen Stelle angeboten,[10] sodass der Cloud-Anwender und der Cloud-Anbieter (oder mehrere Cloud-Anbieter) dem Bereich dieser verantwortlichen Stelle zuzuordnen sind.[11]

Community Cloud

In einer Community Cloud schließen sich zwei oder mehrere Cloud-Anbieter aus Private Clouds zusammen, um für einen definierten Kundenkreis IT-Dienstleistungen für Cloud-Services zu erbringen.[12]

---

[9] Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, S. 22.
[10] Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, S. 20.
[11] Eine andere gängige Definition der Private Cloud ist die Bereitstellung von Cloud-Infrastruktur für nur einen einzigen Kunden durch einen externen Anbieter. Dies hat andere rechtliche und vertragliche Implikationen als die hier definierte Private Cloud.
[12] Fraunhofer Institut für Offene Kommunikationssysteme, ISPRAT-Studie, Cloud-Computing für die öffentliche Verwaltung, 11/2010, S. 21.

Hybrid Cloud

Bei Hybrid Clouds werden Public-, Private- und/oder Community Clouds miteinander kombiniert. Dieses Modell kann im Rahmen der Erhöhung der Verfügbarkeit oder zur effizienten Lastverteilung zum Einsatz kommen.

Infrastructure as a Service (IaaS)

Cloud-Anwender erhalten Zugriff auf üblicherweise virtualisierte Komponenten zur Datenverarbeitung, zum Datentransport und zur Datenspeicherung. Sie können nahezu beliebige Anwendungsprogramme und Betriebssysteme einsetzen

Platform as a Service (PaaS)

Platform as a Service ermöglicht dem Cloud-Anwender, auf der vom Cloud-Anbieter angebotenen Infrastruktur eigene Programme zu entwickeln und auszuführen. Der Cloud-Anbieter macht hierbei Vorgaben zu den zu verwendenden Programmiersprachen und Schnittstellen zu Datenspeichern, Netzwerken und Datenverarbeitungssystemen. Wie bei der Dienstleistung Software as a Service auch, hat der Cloud-Anwender keine Möglichkeit, auf die zur Bereitstellung des Dienstes genutzte Infrastruktur administrativ oder kontrollierend zuzugreifen. Die Kontrollmöglichkeiten beschränken sich auf die selbst eingebrachten Programme und Daten.

Software as a Service (SaaS)

Der Zugriff des Cloud-Anwenders auf die vom Cloud-Anbieter bereit gestellten Anwendungen erfolgt üblicherweise über einen Web-Browser, kann aber auch mit speziellen Programmen erfolgen, die hauptsächlich über Anzeigefunktionen verfügen („Thin-Clients“). Software as a Service wird aufbauend auf Plattform- oder Infrastruktur-orientierten Cloud-Angeboten betrieben. Die bereitgestellten Anwendungen können allenfalls in geringem Umfang auf spezielle Anforderungen der Cloud-Anwender angepasst werden. Auf die für das Bereitstellen der Anwendung genutzten Dienste und Systeme haben die Cloud-Anwender regelmäßig keinen direkten administrativen, operativen oder kontrollierenden Zugriff.

3 Datenschutzrechtliche Aspekte

Verantwortlichkeit des Cloud-Anwenders

Das europäische und deutsche Datenschutzrecht knüpft die rechtliche Verantwortlichkeit für die Datenverarbeitung personenbezogener Daten an die inhaltliche Verantwortlichkeit über die Entscheidung des Umgangs mit den Daten. Danach ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt und allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, § 3 Abs. 7 BDSG, Art. 2 Buchst. d) 4 Richtlinie 95/46/EG. Der Cloud-Anwender ist verantwortliche Stelle in diesem Sinne. Ein Cloud-Anbieter kann jedoch dann ausnahmsweise verantwortliche Stelle sein, wenn er selbst Dienstleistungen anbietet.[13]

Nimmt der Cloud-Anwender von einem Cloud-Anbieter IT-Dienstleistungen für Cloud-Services in Anspruch, so wird Letzterer als Auftragnehmer nach § 11 Abs. 2 BDSG tätig. Der Cloud-Anwender bleibt hingegen nach § 11 Abs. 1 BDSG für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich. Weiterhin muss der Cloud-Anwender einen schriftlichen Auftrag an den Cloud-Anbieter erteilen und dabei die inhaltlichen Anforderungen nach § 11 Abs. 2 BDSG erfüllen. Hilfreich kann hierfür beispielsweise die Mustervereinbarung zur Auftragsdatenverarbeitung des Hessischen Datenschutzbeauftragten in der Fassung des vom Regierungspräsidiums Darmstadt entwickelten Musters sein.[14]

Vertraglich festzulegen sind etwa die Berichtigung, Löschung und Sperrung von Daten. Die praktische Umsetzung dieser Verpflichtung kann durch technische Maßnahmen erfolgen (Kapitel 4.). Weiterhin ist z. B. nach § 11 Abs. 2 Nr. 6 BDSG zu regeln, ob eine Berechtigung zur Begründung von Unterauftragsverhältnissen besteht. Cloud-Anbieter werden zur Erbringung der IT-Dienstleistungen oft Unter-Anbieter einbeziehen, wobei auch für dieses Verhältnis die Regeln der Auftragsdatenverarbeitung zu erfüllen sind. Die Einbeziehung von Unter-Anbietern kann für den Cloud-Anwender intransparent sein, da deren Inanspruchnahme auch nur für einen kurzzeitig gestiegenen Bedarf an Rechenleistung in Betracht kommt und nicht deutlich wird, wessen Kapazitäten genutzt wurden. Der Cloud-Anbieter muss daher vertraglich verpflichtet werden, sämtliche Unter-Anbieter - auch solche, die zu Beginn noch nicht bekannt waren - und auch sämtliche Standorte der Datenzentren, an denen die personenbezogenen Daten verarbeitet werden können[15], abschließend gegenüber dem Cloud-Anwender zu benennen. Will der Cloud-Anbieter ggf. zu einem späteren Zeitpunkt neue Unter-Anbieter einschalten - d.h. solche, die anfangs noch nicht vorgesehen und somit dem Cloud-Anwender noch nicht genannt worden waren - so muss er den Cloud-Anwender somit über die Identität auch jedes der neuen vorgesehenen Unter-Anbieter und die vorgesehenen Standorte der Datenverarbeitung informieren, und zwar bevor die personenbezogenen Daten an den jeweiligen neuen Unter-Anbieter fließen. Dem Cloud-Anwender muss dabei eine ausreichend bemessene Frist zum Widerspruch gegen die

[13] vgl. Art.-29-Datenschutzgruppe, WP 179, S. 27.
[14] http://www.datenschutz.hessen.de/mustervereinbarung_auftrag.htm
[15] Working Paper 196 „Cloud Computing“ der Art.-29-Datenschutzgruppe, Nr. 3.4.1.2, Nr. 3.4.2 Ziffer 9 und Nr. 4.1 (vierter Spiegelstrich)

Einschaltung des neuen Unter-Anbieters oder zur Vertragsbeendigung zur Verfügung stehen. Der Cloud-Anwender muss sich dies vertraglich vorbehalten.[16]

Zudem sind dem Cloud-Anwender die für § 11 Abs. 2 BDSG relevanten Inhalte der Unteraufträge[17] offen zu legen.

Der Unter-Anbieter ist ferner zu verpflichten, die Weisungen des Auftragnehmers zu beachten. Zudem ist zu fordern, dass alle Verpflichtungen, denen der Cloud-Anbieter - d.h. der Auftragnehmer - unterliegt, auch für die Unter-Anbieter gelten (Näheres zur Kontrolle von Unter-Anbietern vgl. Nr. 3.2).Weiterhin besteht das Risiko eines auftragswidrigen Umgangs mit personenbezogenen Daten durch den Cloud-Anbieter, indem dieser z. B. Weisungen des Cloud-Anwenders missachtet und eine Verarbeitung und Nutzung für eigene Geschäftszwecke vornimmt. Dem kann durch die Aufnahme einer Vertragsstrafenregelung entgegengewirkt werden. Weitere organisatorische sowie technische Gegenmaßnahmen werden unter 4. beschrieben.

Kontrolle der Cloud-Anbieter

Der Cloud-Anwender hat sich als Auftraggeber nach § 11 Abs. 2 Satz 4 BDSG vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Cloud-Anbieter als Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Dem Cloud-Anwender wird es dabei nicht immer möglich sein, eine Vor-Ort-Prüfung durchzuführen. Allerdings darf er sich nicht auf bloße Zusicherungen des Cloud-Anbieters verlassen, sondern er muss eigene Recherchen betreiben, um sich Gewissheit darüber zu verschaffen, dass gesetzlich normierte oder vertraglich vereinbarte IT-Sicherheitsstandards eingehalten werden.[18] Die Lösung kann darin bestehen, dass der Cloud-Anbieter sich einem Zertifizierungs- bzw. Gütesiegelverfahren zu Fragen des Datenschutzes und der IT-Sicherheit bei einer unabhängigen und kompetenten Prüfstelle unterwirft.[19] Das Vorliegen von Zertifikaten entbindet den Cloud-Anwender aber nicht von seinen Kontrollpflichten nach § 11 Abs. 2 Satz 4 BDSG, da die bloße Berufung auf eine Zertifizierung z. B. nach ISO 27001 für den Bereich Datenschutz nicht aussagekräftig wäre. Vielmehr muss sich der Cloud-Anwender anhand der in den Zertifizierungs- bzw. Gütesiegelverfahren erarbeiteten Gutachten, Berichte und Analyseergebnisse darüber Klarheit verschaffen, ob und in welchem Umfang sich der Untersuchungsgegenstand auf cloudspezifische Datenschutz- und IT-Sicherheitsrisiken bezieht und dabei die vom Cloud-Anbieter zur Verfügung gestellten Dienste (IaaS, PaaS oder SaaS) geprüft wurden. Es reicht z. B. nicht aus, wenn für den Cloud-Anbieter mit dem Gütesiegel oder der Zertifizierung bescheinigt wurde, dass für einen beliebigen Geschäftsprozess ein Sicherheitskonzept vorliegt. Das Sicherheitskonzept muss sich auf den jeweiligen Cloud-Dienst beziehen,

---

[16] vgl. WP 196 „Cloud Computing“ der Art.-29-Datenschutzgruppe, Nr. 3.3.2 und Nr. 3.4.2 Ziffer 7.
[17] Offenzulegen sind auch Vereinbarungen zwischen dem Auftragnehmer und Unterauftragnehmern, vgl. Klausel 5j des Controller-Processor-Standardvertrages, http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm#h2-5.
[18] Wedde, in: Däubler/Klebe/Wedde/Weichert, Kommentar zum BDSG, 3. Aufl. 2010, § 11 Rndr. 55.
[19] Vgl. z. B. Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), https://www.datenschutzzentrum.de/guetesiegel/index.htm; Europäisches Datenschutz-Gütesiegel beim ULD, https://www.datenschutzzentrum.de/europrise/; Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/cln_174/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html;jsessionid=19D1C64BFD37C3547FF0724D1D973F5A.

was schon im Rahmen einer Strukturanalyse zur Festlegung der Schutzbedarfe von Bedeutung ist. Das Maß an Schutzbedürftigkeit der Anwendungen in den Geschäftsprozessen muss dann auch für die eingesetzten IT-Systeme eingehalten werden, welche die Anwendungen unterstützen.[20]

Eine Zertifizierung z. B. nach ISO 27001 kann hier als wichtiger Baustein für einen Prüfnachweis dienen, indem das erforderliche Sicherheitsniveau aus Unternehmensperspektive untersucht wurde. Ergänzend muss der Cloud-Anwender vom Cloud-Anbieter aber auch den Nachweis einer unabhängigen Stelle erbringen, dass mit diesem Sicherheitsniveau auch die Datenschutzrisiken für die Betroffenen wirksam und im erforderlichen Maß und Umfang begrenzt werden, was mit einer Zertifizierung nach ISO 27001 gerade nicht bescheinigt wird. Es geht etwa um die Frage, ob die Betroffenenrechte wie die Rechte auf Auskunft, Löschung, Berichtigung und Sperrung mittels der eingesetzten Hard- und Software auf dem jeweiligen Sicherheitsniveau umgesetzt wurden. Nur vor diesem Hintergrund kann auf Seiten des Cloud-Anwenders bezüglich der beim Cloud-Anbieter getroffenen technisch-organisatorischen Maßnahmen eine Überzeugungsbildung nach § 11 Abs. 2 Satz 4 BDSG stattfinden. Die Untersuchungsgegenstände sind im Übrigen von den unabhängigen Prüfstellen zu veröffentlichen oder zumindest dem Cloud-Anwender zur Verfügung zu stellen[21]. Im Übrigen dürfen eigene Kontrollrechte des Cloud-Anwenders vertraglich nicht ausgeschlossen werden, selbst wenn gewollt ist, dass die Auftragskontrolle in der Praxis in aller Regel durch die Vorlage geeigneter Zertifikate ausgeführt werden soll. Der Auftraggeber muss sich daneben zumindest die rechtliche Möglichkeit vorbehalten, Kontrollen auch selbst (oder durch einen von ihm ausgewählten sachkundigen Dritten) durchzuführen. Mit anderen Worten darf aus den zwischen Cloud-Anbieter und Cloud-Anwender geschlossenen vertraglichen Vereinbarungen nicht hervorgehen, dass die Vorlage von Zertifikaten die einzige Möglichkeit zur Ausübung der Auftragskontrolle sein soll. Darauf ist bei der Vertragsgestaltung besonders zu achten, insbesondere dann, wenn der Cloud-Anwender eigene vorformulierte Vertragsbedingungen vorlegt.

Besteht eine Erlaubnis zur Beauftragung von Unter-Anbietern, so müssen im Rahmen der Unterbeauftragung die Vorgaben des Vertrags zwischen Cloud-Anwender und Cloud-Anbieter berücksichtigt werden. Der Cloud-Anbieter muss in diesem Fall vor Beginn der Datenverarbeitung im Rahmen der Unterbeauftragung eine Kontrolle nach § 11 Abs. 2 Satz 4 BDSG vornehmen. Hierfür muss dann derselbe Kontrollmaßstab gelten wie im Verhältnis zwischen Cloud-Anwender und Cloud-Anbieter. Dabei ist zu fordern, dass der Cloud-Anwender die Begründung von Unteraufträgen davon abhängig macht, dass der Cloud-Anbieter entsprechende Vereinbarungen mit dem Unter-Anbieter trifft. Allgemein gilt daher: Zwischen dem Cloud-Anbieter und dem Unterauftragnehmer ist ein Vertrag zu schließen, der die zwischen Cloud-Anwender und Cloud-Anbieter geltenden Vertragsbedingungen widerspiegelt (vgl. WP 196, Nr. 3.3.2, letzter Absatz). Unter anderem müssen daher im Unterauftrag auch Kontrollrechte des Auftraggebers selbst gegenüber dem Unterauftragnehmer vorbehalten werden. Selbst wenn gewollt ist, dass die Kontrolle des Unterauftragnehmers in der Regel durch den Cloud-Anbieter (d. h. den Haupt-Auftragnehmer) durchgeführt werden soll, dürfen eigene Kontrollrechte des Auftraggebers gegenüber Unterauftragnehmern nicht ausge-

[20] Vgl. etwa BSI-Standard 100-1, Managementsysteme für Informationssicherheit, S. 36.
[21] Vgl. z. B. www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Zertifikate/iso27001zertifikate_node.html und www.datenschutzzentrum.de/guetesiegel/index.htm.

schlossen werden; ein solcher Ausschluss wäre mit der sich aus § 11 Abs. 1 Satz 1 BDSG ergebenden datenschutzrechtlichen Verantwortlichkeit des Cloud-Anwenders als Auftraggeber nicht vereinbar. Hierauf ist bei der Vertragspraxis zur Vergabe von Unteraufträgen besonderes Augenmerk zu legen, insbesondere wenn vorformulierte Vertragsbedingungen großer Cloud-Anbieter Verwendung finden sollen. Weiterhin sollte der Cloud-Anbieter gegenüber dem Cloud-Anwender vertraglich verpflichtet sein, auf Verlangen vorhandene Nachweise zu Zertifizierungen bzw. Datenschutz-Gütesiegeln der Unter-Anbieter vorzulegen.

Unrechtmäßige Kenntniserlangung von Daten

Stellt der Cloud-Anwender in seiner Funktion als Auftraggeber fest, dass z. B. personenbezogene Daten, die einem Berufsgeheimnis unterliegen, oder personenbezogene Daten zu Bank- und Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, so muss er dies unter Einhaltung der Anforderungen nach § 42a Satz 2 bis 5 BDSG unverzüglich der zuständigen Datenschutzaufsichtsbehörde sowie den Betroffenen mitteilen. Die entsprechende Benachrichtigung darf dann in einem Straf- oder Ordnungswidrigkeitenverfahren gegen den Benachrichtigungspflichtigen oder gegen seine Angehörigen im Sinne von § 52 Abs. 1 StPO nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden. Die unterbliebene, nicht richtige, nicht vollständige oder nicht rechtzeitige Benachrichtigung ist für den Cloud-Anwender nach § 43 Abs. 2 Nr. 7 BDSG bußgeldbewehrt. Da gemäß § 11 Abs. 4 BDSG mangels Verweis auf § 42a BDSG die Benachrichtigungspflicht nicht für den Cloud-Anbieter in seiner Funktion als Auftragnehmer gilt, die Verantwortung jedoch nach § 11 Abs. 1 BDSG beim Cloud-Anwender verbleibt, muss im Vertrag zur Auftragsdatenverarbeitung eine präzise Formulierung nach § 11 Abs. 2 Nr. 8 BDSG zur Steuerung des Meldeprozesses gewählt werden.[22]

Verarbeitung verschlüsselter Daten

Bei der Verarbeitung personenbezogener Daten in der Cloud gerät zunehmend der Umgang mit verschlüsselten Daten in den Fokus. Verstärkt wird die Frage aufgeworfen, ob verschlüsselte Daten einen Personenbezug aufweisen und sie damit in den Regelungsbereich des BDSG fallen. Die Verschlüsselung betrifft eine nach § 9 BDSG i.V.m. Satz 3 der Anlage zum BDSG geforderte technisch-organisatorische Maßnahme zur Gewährleistung der IT-Sicherheit. Der Personenbezug von Daten entfällt jedoch regelmäßig nicht durch die Verschlüsselung. Auch pseudonymisierte Daten i.S.v. § 3 Abs. 6a BDSG weisen einen Personenbezug auf, indem die Betroffenen über eine Zuordnungsregel identifizierbar sind. Nach dem Erwägungsgrund 26 der Richtlinie 95/46/EG sollten bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die „vernünftigerweise entweder von den Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen." Berücksichtigt werden muss vor allem, ob eine Verschlüsselung nach dem Stand der Technik verwandt wurde bzw. ob der eingesetzte Algorithmus durch Zeitablauf keinen angemessenen Schutz mehr bietet und inwieweit ein

[22] Berliner Beauftragter für Datenschutz und Informationsfreiheit, FAQ zur Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten nach § 42a BDSG v. 21.12.2010, S. 2 f.

starker oder schwacher Kryptoalgorithmus[23] zum Einsatz kommt. Ferner ist anhand einer Risikoabschätzung zu prüfen, wie groß die Wahrscheinlichkeit ist, den Personenbezug herzustellen. Diese Analyse muss regelmäßig durchgeführt werden. Im Rahmen eines Kryptokonzepts[24] sollten die technischen und organisatorischen Maßnahmen zur Vergabe und zum Entzug von Schlüsseln sowie zur Schlüsselhinterlegung dokumentiert werden.

Betroffenenrechte

Der Cloud-Anwender bleibt als Auftraggeber nach § 11 Abs. 1 BDSG zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet, wobei ihm auch die Verpflichtung obliegt, personenbezogene Daten nach den §§ 34, 35 BDSG zu berichtigen, zu löschen, zu sperren und auf Verlangen des Betroffenen Auskünfte vor allem zu den zu seiner Person gespeicherten Daten und zur Herkunft der Daten zu erteilen. Da der Cloud-Anwender nur einen sehr eingeschränkten administrativen, operativen und kontrollierenden Zugriff auf die Infrastruktur des Cloud Computing hat, sollte er gegenüber dem Cloud-Anbieter vertragsstrafenbewehrte Weisungsrechte festlegen, die eine Erfüllung der Betroffenenrechte gewährleisten und diesem zusätzlich die Verpflichtung auferlegen, gegenüber Unter-Anbietern dieselben Rechte einzuräumen. Weiterhin können zur Durchsetzung der Betroffenenrechte technische Maßnahmen ergriffen werden (Kapitel 4).

Grenzüberschreitender Datenverkehr

Da die Cloud nicht an geographische Grenzen gebunden und darin stattfindende Datenverarbeitung gerade nicht ortsgebunden ist, muss für eine datenschutzrechtliche Betrachtung insbesondere deutlich werden, wo die Cloud-Anbieter und Unter-Anbieter tätig werden. Der Cloud-Anwender wird aber oft nicht wissen, an welchem "Ort" im jeweiligen Augenblick die Verarbeitung erfolgt. Deshalb ist es wichtig, dass er über sämtliche möglichen Verarbeitungsorte vorab informiert wird (vgl. Verantwortlichkeit des Cloud-Anwenders). EU-Recht ist in diesem Zusammenhang bereits dann anwendbar, wenn der Cloud-Anwender als im Regelfall für die Verarbeitung verantwortliche Stelle im Rahmen der Tätigkeiten einer in der EU gelegenen Niederlassung personenbezogene Daten verarbeitet oder wenn die für die Verarbeitung verwendeten Mittel im Hoheitsgebiet der EU gelegen sind. [25]

Im Folgenden werden zunächst die grundsätzlichen Anforderungen an die Zulässigkeit eines grenzüberschreitenden Datenverkehrs dargestellt (vgl. 3.1.1 und 3.1.2). Im Anschluss erfolgt eine Neubewertung, die aufgrund der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste, insbesondere der US-amerikanischen National Security Agency (NSA), erforderlich wurde (vgl. 3.1.3).

---

[23] Vgl. Algorithmenkataloge der Bundesnetzagentur, http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html und TR 02102 des Bundesamts für Sicherheit in der Informationstechnik (BSI) https://www.bsi.bund.de/cln_183/ContentBSI/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[24] Vgl. Baustein 1.7 („Kryptokonzept") der Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI), https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b01/b01007.html

[25] vgl. Art.- 29-Datenschutzgruppe, WP 179, S. 27

3.1.1 Innereuropäischer Raum

Aufgrund des innerhalb des EWR weitgehend harmonisierten Datenschutzniveaus gelten für alle Cloud-Anwender, -Anbieter und Unter-Anbieter dieselben datenschutzrechtlichen Anforderungen nach der Richtlinie 95/46/EG. Durch vertragliche Vereinbarungen zwischen dem Cloud-Anwender und dem Cloud-Anbieter müssen der Ort bzw. die Orte der technischen Verarbeitung personenbezogener Daten eindeutig festgelegt werden (vgl. Verantwortlichkeit des Cloud-Anwenders). Cloud-Anbieter sowie Unter-Anbieter können so verpflichtet werden, nur technische Infrastrukturen zu verwenden, die sich physikalisch auf dem Gebiet des EWR befinden.[26] Es ist daher nicht hinnehmbar, dass der Cloud-Anbieter eine Auskunft zu den Standorten der Datenverarbeitung verweigert. Keinesfalls dürfte bei einer Verweigerung pauschal von einer Cloud im innereuropäischen Raum ausgegangen werden.

3.1.2 Außereuropäischer Raum

Erfolgen die Datenverarbeitungen allerdings außerhalb der EU und des EWR, indem die Cloud-Anbieter und/oder Unter-Anbieter eine Datenverarbeitung in Drittstaaten vornehmen, so gelten die besonderen Anforderungen der §§ 4b, 4c BDSG für den Drittstaatentransfer. Falls in dem Drittstaat kein angemessenes Datenschutzniveau besteht[27], müssen daher durch den Cloud-Anwender als verantwortliche Stelle ausreichende Garantien zum Schutz des allgemeinen Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorgewiesen werden. Die Garantien können sich aus Standardvertragsklauseln oder u. U. aus Binding Corporate Rules (BCR; insbesondere BCR für Auftragsverarbeiter, sog. Processor Binding Corporate Rules[28]) ergeben[29]. In jedem Fall ist ein besonderes Augenmerk auf die Festlegung eines technischen und organisatorischen Datenschutzes zu legen (Kapitel 4).

Im Rahmen des Datentransfers mit Drittstaaten erlangen die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG vom 05.02.2010[30] Bedeutung. Demnach agiert der Cloud-Anwender als verantwortliche Stelle und Datenexporteur, der Cloud-Anbieter oder Unter-Anbieter hingegen als Datenimporteur, sofern er in einem Drittstaat ansässig ist.[31]

Gibt der im Drittstaat ansässige Cloud-Anbieter Daten an einen Unter-Anbieter, der ebenfalls seinen Sitz im außereuropäischen Raum hat, so wird Ersterer als Übermittler mitverantwortlich für die Rechtmäßigkeit der Datenübermittlung und -verarbeitung. Gleichwohl verbleibt eine Verantwortlichkeit des Cloud-Anwenders. Der Cloud-

---

[26] Über eine Regionalgarantie hinaus ist auch eine Bindung an EU-Recht zwingend.
[27] Siehe hierzu die Entscheidungen der EU-Kommission:
http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.
[28] Diese Möglichkeit steht seit dem 01.01.2013 zur Verfügung; vgl. dazu die WP 195, 195a und 204 der Art.-29-Datenschutzgruppe
[29] Es sollte immer auch die Option eines individuellen Vertrages erwogen werden.
[30] Entscheidung der EU-Kommission: siehe Fußnote 27; zur Auslegung und Umsetzung dieser Entscheidung siehe die FAQs in WP 176 der Artikel 29-Gruppe:
http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm
[31] Näheres siehe WP 176 der Artikel 29 Gruppe (Fußnote 30). Hier ist u. a. die Frage behandelt, inwieweit der Standardvertrag angewendet werden kann, wenn sich nur der Unterauftragnehmer (hier: Unter-Anbieter) im Drittstaat befindet, der Auftragnehmer (hier:Cloud-Anbieter) aber noch innerhalb der EU/des EWR

Anwender bleibt in jedem Fall haftungsrechtlich für sämtliche Schäden verantwortlich, die der Cloud-Anbieter oder Unter-Anbieter den Betroffenen zufügen.

Sofern der Cloud-Anbieter seinen Sitz nicht in einem Drittstaat ohne angemessenes Datenschutzniveau hat, sondern vielmehr in der EU bzw. im EWR oder in einem Drittstaat mit angemessenem Datenschutzniveau, sind die Standardvertragsklauseln gemäß Kommissionsbeschluss 2010/87/EU für Auftragsverarbeitung vom 05.02.2010 allerdings nicht anwendbar, jedenfalls nicht „als solche", d.h. nicht im Sinne eines Standardvertrags, der genehmigungsfreie Exporte personenbezogener Daten in einen Drittstaat ermöglichen würde.[32] Die Vergabe von Unteraufträgen stellt die beteiligten Stellen in dieser Konstellation vor besondere Herausforderungen. Denn anders als es Klausel 11 Abs. 1 der Standardvertragsklauseln ermöglicht, ist in dieser Konstellation die Vergabe von Unteraufträgen nicht durch den Haupt-Auftragsdatenverarbeiter (d.h. den Cloud-Anbieter) im eigenen Namen möglich, jedenfalls nicht im Wege einer genehmigungsfreien Lösung. Die Artikel-29-Gruppe der Datenschutzbehörden der EU-Mitgliedstaaten hat für diese Fallgestaltung folgende Möglichkeiten für die Einschaltung von Unter-Anbietern aufgezeigt:[33]

- a. Abschluss der Standardvertragsklauseln gemäß Kommissionsbeschluss 2010/87/EU im Direktverhältnis zwischen Cloud-Anwender als Datenexporteur und Unter-Anbieter als Datenimporteur („Direktvertrag").

- b. Der Cloud-Anbieter schließt mit entsprechender Vollmacht im Auftrag des Cloud-Anwenders den Standardvertrag im Namen des Cloud-Anwenders mit dem Unter-Anbieter ab; rechtlich werden somit auch bei diesem Vorgehen nur der Cloud-Anwender und der Unter-Anbieter Parteien des Standardvertrags.

- c. Abschluss eines Ad-hoc-Vertrags, d.h. eines Vertrags, der nicht den Standardvertragsklauseln entspricht; die Datenübermittlung an den Untern-Anbieter bedarf in diesem Fall allerdings gemäß § 4c Abs. 2 Satz 1 BDSG der Genehmigung der zuständigen Aufsichtsbehörde.

Das Erfordernis, in dieser Konstellation - d.h. wenn nur der Unter-Anbieter in einem Drittstaat ohne angemessenes Datenschutzniveau ansässig ist, nicht jedoch auch der Haupt-Auftragsverarbeiter (hier: der Cloud-Anbieter) - die Standardvertragsklauseln direkt zwischen der verantwortlichen Stelle (d.h. dem Cloud-Anwender) und dem Unter-Anbieter abzuschließen, wird zwar bisweilen kritisiert. Jedoch ist auf der Basis des geltenden europäischen Datenschutzrechts keine andere Möglichkeit zur Einschaltung eines Unter-Anbieters erkennbar, bei der in dieser Konstellation die Übermittlung personenbezogener Daten ohne das Erfordernis einer aufsichtsbehördlichen Genehmigung zulässig wäre.[34] Eine Vergabe von Unteraufträgen durch den Cloud-Anbieter

---

[32] WP 176, Nr. I.1 und I.2 unter Verweis auf den Erwägungsgrund 23 des Kommissionsbeschlusses 2010/87/EU.
[33] WP 176, Nr. I.3.
[34] Vgl. dazu bereits den Beschluss des Düsseldorfer Kreises vom 19./29.04.2007 „Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung", dort Fallgruppe B,
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/HandreichungApril2007.html?nn=409242.

selbst im eigenen Namen ist bei dieser Fallgestaltung nicht möglich, jedenfalls nicht im Wege einer genehmigungsfreien Lösung.

Im Rahmen der durch eine Entscheidung der EU-Kommission erlassenen Standardvertragsklauseln, die vom Cloud-Anwender und Cloud-Anbieter unverändert übernommen werden müssen[35], wurden allerdings die spezifischen Regelungen der Auftragsdatenverarbeitung nicht vollständig abgebildet, obwohl die vertraglichen und faktischen Beziehungen zwischen Datenexporteur und Datenimporteur einer solchen Verarbeitung ähnlich sind. Aus diesem Grunde muss der Cloud-Anwender über die Vereinbarung von Standardvertragsklauseln hinaus die Anforderungen nach § 11 Abs. 2 BDSG erfüllen und entsprechend vertraglich abbilden. Dies kann durch Regelungen in den Anlagen zum Standardvertrag und/oder ergänzende geschäftsbezogene Klauseln oder durch separate vertragliche Regelungen erfolgen, die nicht inhaltlich von den Standardvertragsklauseln abweichen.[36]

Solche Regelungen dienen der Wahrung der schutzwürdigen Belange der Betroffenen und können dazu führen, dass die Übermittlung durch den Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt ist.

Da aufgrund der Begriffsbestimmung in § 3 Abs. 4 Nr. 3 in Verbindung mit § 3 Abs. 8 BDSG die privilegierende Wirkung der Auftragsdatenverarbeitung nicht greift, wenn der Datenverarbeitungsdienstleister seinen Sitz außerhalb der EU und des EWR hat, und die Datenweitergabe an einen „Datenverarbeiter“ in einem Drittstaat also eine Übermittlung darstellt[37], bedarf sie als solche einer Rechtsgrundlage. § 28 Abs. 1 Satz 1 Nr. 2 BDSG kann als Rechtsgrundlage in Betracht kommen. Im Rahmen der danach vorzunehmenden Interessenabwägung ist zu berücksichtigen, welche Rolle dem Datenempfänger im Drittstaat zukommt und welche Regelung der Datenexporteur mit diesem geschlossen hat. Wenn der Datenexporteur mit dem Datenimporteur einen Vertrag mit Festlegungen entsprechend § 11 Abs. 2 BDSG geschlossen hat, kann dies dazu führen, dass die Datenübermittlung aufgrund der Interessenabwägung gerechtfertigt ist.

Dies gilt freilich nur, soweit der Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG überhaupt einschlägig sein kann.[38] Soweit besondere Arten personenbezoge-

---

[35] Werden die EU-Standardvertragsklauseln geändert und wird dadurch ein individueller Vertrag geschaffen, so darf der Drittstaatentransfer nur erfolgen, wenn die zuständige Datenschutzaufsichtsbehörde die dann erforderliche Genehmigung gemäß § 4c Abs. 2 BDSG erteilt hat.
Geringfügige Ergänzungen, die ausschließlich der Erfüllung der Voraussetzungen des § 11 Abs. 2 BDSG dienen, lösen noch keine Genehmigungspflicht aus. Näheres hierzu: Tätigkeitsbericht der Hessischen Landesregierung für die Datenschutzaufsicht im nicht öffentlichen Bereich für das Jahr 2009, Nr. 11.1, sowie Synopse der Datenschutzaufsichtsbehörden zu § 11- EU-Standardverträge (https://www.datenschutz.hessen.de/download.php?download_ID=238&download_now=1)

[36] Näheres siehe Synopse, Fußnote 35

[37] Dies ist eine Besonderheit des BDSG. Nach der Richtlinie 95/46/EG und den Datenschutzgesetzen anderer europäischer Länder gelten auch Datenverarbeitungsdienstleister in Drittstaaten als Auftragsdatenverarbeiter.

[38] Soweit öffentliche Stellen Cloud Services in Drittstaaten anwenden, ist hier eine besonders sorgfältige Prüfung geboten, denn ein dem § 28 Abs. 1 Satz 1 Nr. 2 BDSG entsprechender Erlaubnistatbestand dürfte es in den Landesdatenschutzgesetzen nicht geben, soweit ersichtlich. Die Verfasser dieser Orientierungshilfe haben allerdings keine Prüfung aller Landesdatenschutzgesetze vorgenommen.

ner Daten betroffen sind, scheidet das Cloud Computing daher regelmäßig aus, denn § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist grundsätzlich nicht anwendbar und die Voraussetzungen der speziellen Erlaubnistatbestände nach § 28 Abs. 6 bis 9 BDSG dürften grundsätzlich nicht erfüllt sein.[39]

Erfolgt eine Verarbeitung personenbezogener Daten durch einen Cloud-Anbieter oder Unter-Anbieter mit Sitz in den USA, so können die EU-Standardvertragsklauseln ebenso wie Binding Corporate Rules entbehrlich sein, wenn sich der Cloud-Anbieter zur Einhaltung der Safe-Habor-Grundsätze verpflichtet hat. Cloud-Anbieter oder Unter-Anbieter mit Sitz in den USA können sich dabei auf freiwilliger Basis gegenüber dem US-Handelsministerium selbst zertifizieren, indem sie eine Beitrittserklärung unterzeichnet und eine Datenschutzerklärung veröffentlicht haben. Solange jedoch eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe-Harbor-Liste geführtes US-Unternehmen übermitteln.[40] Daher ist zu fordern, dass sich der Cloud-Anwender mindestens davon überzeugt, ob das Zertifikat des Cloud-Anbieters noch gültig ist und sich auf die betreffenden Daten bezieht.[41] Soweit EU-Personaldaten verarbeitet werden sollen, muss der Cloud-Anwender ferner prüfen, ob der Cloud-Anbieter sich gemäß FAQ 9 Frage 4 des Safe-Harbor-Abkommens zur Zusammenarbeit mit den EU-Datenschutzaufsichtsbehörden verpflichtet hat.[42] Ferner muss der Cloud-Anwender prüfen und mit dem Cloud-Anbieter im Innenverhältnis sicherstellen, dass er (der Cloud-Anwender) bei einer Anfrage durch einen Betroffenen auch die nötigen Informationen erhält, um die Anfrage beantworten zu können.

Bestehen für den Cloud-Anwender Zweifel an der Einhaltung der Safe-Harbor-Grundsätze durch den Cloud-Anbieter, so sollte auf Standardvertragsklauseln oder Anbieter mit Binding Corporate Rules zurückgegriffen werden.[43]

Zu beachten ist, dass auch eine gültige Safe-Harbor-Zertifizierung des Cloud-Anbieters (und ggf. des Unter-Anbieters) den Cloud-Anwender nicht von dem Erfordernis befreit, schriftliche Vereinbarungen entsprechend § 11 Abs. 2 BDSG zu treffen. Auch in der Antwort zu FAQ 10 zu den Safe-Harbor-Grundsätzen wird klargestellt, dass vertragliche Regelungen entsprechend dem nationalen Datenschutzrecht des Datenexporteurs durch die Safe-Harbor-Zertifizierung nicht entbehrlich werden.

---

[39] § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist auch nicht einschlägig, soweit es sich um Daten handelt, die dem TMG unterfallen. Bei Personaldaten ist streitig, ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG einschlägig sein kann. Hier sind letztlich die Regelungen in der geplanten BDSG-Novelle maßgeblich.

[40] Siehe dazu Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover (überarbeitete Fassung vom 23.8.2010).

[41] Diese Prüfung kann anhand der Eintragungen in der Safe-Harbor-Liste erfolgen: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list
(Siehe auch Tätigkeitsbericht der Hessischen Landesregierung für die Datenschutzsicht im nicht öffentlichen Bereich für das Jahr 2007 Nr. 10, abrufbar unter: http://www.datenschutz.hessen.de)

[42] Auch dies kann anhand der Eintragungen in der Safe-Harbor-Liste geprüft werden.

[43] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 28./29.04.2010 in Hannover; Prüfung der Selbstzertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen.

Die weiteren obigen Ausführungen zum Erfordernis einer Rechtsgrundlage für die Übermittlung (insbesondere die Problematik, falls § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht einschlägig sein kann) sind ebenfalls zu beachten.

Ebenso wenig entbindet die bloße Safe-Harbor-Zertifizierung den Cloud-Anwender von seiner Kontrollpflicht analog § 11 Abs. 2 Satz 3 BDSG. Die bloße Prüfung der Safe Harbor Zertifizierung genügt regelmäßig nicht den oben (vgl. Kontrolle des Cloud-Anbieters) dargestellten Anforderungen.

Beim Drittstaatentransfer können bei konzernangehörigen Auftragnehmern die erforderlichen ausreichenden Garantien zum Schutz der Persönlichkeitsrechte – wie bereits oben erwähnt – durch Binding Corporate Rules geschaffen werden. Wenn Cloud-Anwender und Cloud-Anbieter derselben Unternehmensgruppe angehören, sind Binding Corporate Rules selbstverständlich ohne weiteres möglich. Auch hier wäre zu beachten, dass Binding Corporate Rules den Cloud-Anwender nicht von dem Erfordernis befreien, schriftliche Vereinbarungen entsprechend § 11 Abs. 2 BDSG zu treffen.[44] Es besteht ebenfalls das Erfordernis einer Rechtsgrundlage für die Übermittlung.

Seit 01.01.2013 besteht mit den sog. Processor Binding Corporate Rules (BCR für Auftragsdatenverarbeiter; im folgenden: PBCR) eine weitere, gerade auch für Cloud Computing interessante Möglichkeit zur Erbringung ausreichender Datenschutzgarantien für den Drittstaatstransfer personenbezogener Daten.[45] Das Instrument der PBCR ist auf Konzerne und Unternehmensgruppen zugeschnitten, zu deren Geschäftsgegenständen die Auftragsverarbeitung personenbezogener Daten (ggf. für unterschiedliche Auftraggeber) zählt. PBCR sind wie schon die bislang bekannten, „herkömmlichen“ BCR den Datenschutzaufsichtsbehörden aller betroffenen[46] EU-/EWR-Staaten zur Überprüfung vorzulegen, die hierzu eine koordiniertes Abstimmungsverfahren eingerichtet haben.[47] Bestätigen die Aufsichtsbehörden, dass die PBCR alle Anforderungen an ausreichende Datenschutzgarantien für den Drittstaatstransfer erfüllen, so eröffnet sich für eine solche „Auftragsverarbeitungs-Unternehmensgruppe“ jedenfalls grundsätzlich die Möglichkeit, im Zuge der Auftragsverarbeitungstätigkeit personenbezogene Daten von gruppenangehörigen Unternehmen im EWR an gruppenangehörige Unternehmen außerhalb des EWR zu transferieren.[48] Damit können PBCR gerade auch für Unternehmensgruppen geeignet sein, die Cloud-Computing-Dienste anbieten und zu diesem Zwecke personenbezogene Daten auch an gruppenangehörige Unternehmen außerhalb des EWR transferieren wollen. Verantwortlich für die Drittstaatsübermittlungen bleibt dabei aber stets der jeweilige Auftraggeber. Auftraggeber, die sich einer „Auftragsdatenverarbeitungs-Unternehmensgruppe“ bedienen, deren PBCR von den Datenschutzbehörden der betroffenen EWR-Staaten als ausreichende Da-

---

[44] Siehe auch WP 153 Nr. 6.1und WP 154 Nr. 11 und 12 der Artikel 29-Gruppe: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2008_en.htm

[45] zu PBCR vgl. die WP 195, 195a und 204 der Artikel-29-Datenschutzgruppe

[46] Bei PBCR wären dies alle Aufsichtsbehörden, aus deren Zuständigkeitsbereich möglicherweise personenbezogene Daten auf der Grundlage der PBCR exportiert werden könnten. Will sich der Auftragsverarbeiter-Konzern somit vorbehalten, seine Dienste Auftraggebern in allen EWR-Staaten anzubieten, so sind somit die Aufsichtsbehörden aller Mitgliedstaaten betroffen.

[47] vgl. WP 107 der Artikel-29-Datenschutzgruppe

[48] Die weiteren Anforderungen an die Zulässigkeit der einzelnen konkreten Übermittlungen - insb. das Erfordernis einer Rechtsgrundlage - müssen jedoch stets zusätzlich erfüllt werden, s. dazu im folgenden.

tenschutzgarantien anerkannt worden sind, erfüllen damit jedenfalls die für den Drittstaatstransfer geltenden Anforderungen der §§ 4b, 4c BDSG. Daneben muss jedoch der Auftraggeber auch hier - wie bei jeder anderen Übermittlung personenbezogener Daten - stets noch sorgfältig prüfen, ob die einzelnen Übermittlungen auf eine Rechtsgrundlage (z.B. § 28 Abs. 1 Satz 1 Nr. 2 BDSG, s. oben) gestützt werden können.[49] Zudem muss der Auftraggeber mit einem Mitglied der Auftragsverarbeitungs-Unternehmensgruppe einen Vertrag mit Festlegungen entsprechend § 11 Abs. 2 BDSG abschließen[50]. Aufgrund der PBCR entfällt jedoch das ansonsten für den Auftraggeber bestehende Erfordernis, mit jedem einzelnen Mitglied der Auftragsverarbeitungs-Unternehmensgruppe einen gesonderten derartigen Vertrag abzuschließen.[51] Gerade aufgrund dieses Umstands können PBCR - in den dazu geeigneten Fällen - zu einer erheblichen praktischen Vereinfachung bei der Auftragsverarbeitung personenbezogener Daten durch eine Mehrzahl von Einzelgesellschaften führen, die derselben Unternehmensgruppe angehören.

3.1.3 Neuere Entwicklungen und deren Bewertung

US-Behörden, wie etwa das Federal Bureau of Investigation (FBI), die National Security Agency (NSA) oder die Central Intelligence Agency (CIA) sind auf der Grundlage von US-amerikanischem Recht ermächtigt, auf personenbezogene Daten in Europa zuzugreifen, was bezüglich einer Datenverarbeitung in der Cloud eine besondere Relevanz aufweist. Als Rechtsgrundlagen werden hierfür z.B. der Patriot Act, der Foreign Intelligence Surveillance Act, der Electronic Privacy Act, der Stored Communications Act, die Rechtsprechung von US-Gerichten über „Bank of Nova Scotia Subpoena“ und Einwilligungsanordnungen (Compelled Consent Order) aufgeführt. In einer Studie des Instituts für Informationsrecht der Universität Amsterdam[52] wird dargelegt, dass es für die Zugriffsbefugnisse der US-Behörden nicht maßgebend sein soll, ob sich die Cloud innerhalb oder außerhalb der USA befindet. Es wird nach US-Recht als ausreichend angesehen, wenn der Cloud-Anbieter zumindest auch in den USA geschäftlich tätig ist. Vor allem Title 50 USC, Sec. 1881a FISA erlaube einen nahezu uneingeschränkten staatlichen Zugriff auf Daten und Kommunikationsprotokolle. Für die weitere Verarbeitung erhobener Daten existiere keine Zweckbindung.

Ferner wird es als möglich angesehen, dass sich eine US-Behörde auf Basis der genannten Rechtsgrundlagen direkt an ein Unternehmen mit Sitz in der EU wendet und einen Datenzugriff einfordert, wenn dieses Unternehmen z.B. ein Büro in den USA betreibt, so dass auch personenbezogene Daten in einer innereuropäischen Cloud betroffen sein können.[53] Ausgehend von dem im US-Recht geltenden Grundsatz der

---

[49] In einer Reihe der EU-/EWR-Staaten sowie in einigen deutschen Bundesländern bedarf der Datenexporteur - im vorliegenden Fall somit der Auftraggeber - für den Drittstaatstransfer auf der Grundlage von BCR (oder PBCR) noch der Genehmigung der Aufsichtsbehörde (nach deutschem Recht gemäß § 4c Abs. 2 Satz 1 BDSG). Inwieweit dieses Erfordernis besteht, sollte frühzeitig mit der für den Datenexporteur zuständigen Datenschutzbehörde geklärt werden.

[50] Aus Sicht der EU-Datenschutzrichtlinie handelt es sich hierbei um einen Vertrag zur Auftragsdatenverarbeitung gemäß Art. 17 RL 95/46/EU, vgl. WP 204 der Artikel-29-Datenschutzgruppe, Nr. 2.1.

[51] WP 204 der Artikel-29-Gruppe, Nr. 2.1, vierter Absatz („one global commitment instead of multiple contracts“) und Nr. 2.2.1, dritter Absatz, jeweils in der englischen Sprachfassung.

[52] Schröder/Haag, Studie zu staatlichen Zugriffen beim Cloud Computing, ZD-Aktuell 2012, 03132 – beck online; Vgl. Van Hoboken/Arnbak/Va Eijk, Studie des Instituts für Informationstechnik der Universität Amsterdam, „Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act“, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534.

[53] Vgl. Spies, ZD-Aktuell 2012, 03062 – beck online, „Europa: Wer hat Angst vor dem Patriot Act?“.

Personal Jurisdiction, wonach die internationale Zuständigkeit eines US-Gerichts über eine bestimmte Person und ihre Rechtsbeziehungen begründet werden kann, wäre es für eine Anordnung der US-Behörden nicht von Bedeutung, an welchem Ort sich die Daten befinden.[54]

Entsprechende Datenübermittlungen durch Unternehmen mit Sitz in Europa bzw. Deutschland würden mit Art. 26 der Richtlinie 95/46/EG bzw. § 4c BDSG nicht im Einklang stehen. Unabhängig davon, ob die Aufforderung zur Datenübermittlung an einen Cloud-Anbieter mit Sitz in oder außerhalb der Vereinigten Staaten erfolgt, würde der Cloud-Anwender durch die Beibehaltung seiner datenschutzrechtlichen Verantwortlichkeit mit der Übersendung der personenbezogenen Daten durch den Cloud-Anbieter gegen europäisches und deutsches Datenschutzrecht verstoßen. Die Datenübermittlung könnte auch nicht auf die ausschließlich für die Privatwirtschaft entwickelten Grundsätze zu Safe Harbor gestützt werden. Derzeit fehlen internationale Übereinkommen, die eine solche Datenverarbeitung regeln.

Vergleichbares gilt auch für Datenzugriffe durch andere Staaten außerhalb der Europäischen Union, für welche kein angemessenes Schutzniveau nach Maßgabe von Art. 25 der Richtlinie 95/46/EG festgestellt wurde. Die Zulässigkeit einer Datenübermittlung durch die Cloud-Anbieter an dort ansässige staatliche Stellen darf nicht auf in diesen Staaten geltendes Recht gestützt werden, sondern muss in Ermangelung internationaler Abkommen zur Datenverarbeitung den strengen Vorgaben nach Art. 26 der Richtlinie 95/46/EG, § 4c BDSG genügen. Diese Anforderungen dürften jedoch regelmäßig nicht erfüllt sein, sodass eine Datenübermittlung unzulässig wäre.

Darüber hinaus wurde auch bekannt dass, wonach staatliche Behörden in EU-Mitgliedstaaten, wie das Government Communications Headquarters (GCHQ – britischer Nachrichten- und Sicherheitsdienst) und die Direction Generale de la Securite Exterieure (DGSE – französischer Nachrichtendienst) umfassend und ohne Rechtsgrundlage auf personenbezogene Daten von EU-Bürgern, d.h. Verbindungs- wie Inhaltsdaten (Telefon- und Internetverbindungsdaten sowie E-Mails, SMS, Chats), zugreifen würden.[55] Entsprechende Maßnahmen verstießen gegen europäisches Datenschutzrecht.

Vor dem Hintergrund der aktuellen Entwicklungen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sich Ende Juli 2013 an die Bundesregierung gewandt und große Besorgnis über die Gefährdung des Datenverkehrs zwischen Deutschland und außereuropäischen Staaten geäußert.[56] Demnach hat die Europäische Kommission in der Vergangenheit betont, dass die nationalen Aufsichtsbehörden

---

[54] Bettinger, GRUR Int. 1998, 660, „Der lange Arm amerikanischer Gerichte: Personal Jurisdiction im Cyberspace – Bericht über die neuere Rechtsprechung amerikanischer Gerichte zur interlokalen und internationalen Zuständigkeit bei Kennzeichenkonflikten im Internet“; Spies, ZD-Aktuell 2012, 03062 – beck online, „Europa: Wer hat Angst vor dem Patriot Act?“; allerdings hat Microsoft gegen ein entsprechendes Urteil eines US-Gerichts aufgrund des Stored Communications Act Berufung eingelegt, über die noch nicht entschieden ist, http://www.heise.de/newsticker/meldung/Microsoft-verweigert-US-Behoerden-Zugriff-auf-europaeische-E-Mails-2305158.html.

[55] Lehnartz, Meldung vom 05.07.2013, „Franzosen spionieren auch mit“, http://www.welt.de/print/die_welt/politik/article117740966/Franzosen-spionieren-auch-mit.html; Stöcker/Horchert, Meldung vom 03.07.2013, „Alles was man über Prism, Tempora und Co. wissen muss“, http://www.spiegel.de/netzwelt/netzpolitik/prism-und-tempora-fakten-und-konsequenzen-a-909084.html.

[56] Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.07.2013, http://www.datenschutz-bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de.

Datenübermittlungen in Drittstaaten aussetzen können, wenn eine „hohe Wahrscheinlichkeit“ besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind. Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist dieser Fall jetzt eingetreten, weil die NSA und andere ausländische Geheimdienste nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden. Bevor nicht der unbeschränkte Zugriff ausländischer Nachrichtendienste auf personenbezogene Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt wird, behalten sich die Aufsichtsbehörden für den Datenschutz vor, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten zur Nutzung von Cloud-Diensten zu erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind.

Weiterhin hat die EU-Justizkommissarin angekündigt, dass die EU-Kommission aufgrund der grundsätzlichen Kritikpunkte an Safe-Harbor-Zertifizierungen eine Überprüfung des gleichnamigen Abkommens durchführen wird.[57] Diese Überprüfung dauert gegenwärtig noch an.

Schließlich hat die Art. 29-Gruppe betont, dass keines der juristischen Instrumente zur Herstellung eines angemessenen Datenschutzniveaus in Drittstaaten (Grundsätze des „sicheren Hafens“, Standardvertragsklauseln oder bindende Unternehmensregelungen) die Übermittlung personenbezogener Daten an eine Drittstaatsbehörde zum Zweck massiver und willkürlicher Überwachung rechtfertigen kann[58].

Bei der Prüfung der Aufsichtsbehörden, ob ein Datentransfer in die USA den datensicherheitsrechtlichen Anforderungen entspricht, ist etwa von Bedeutung, ob der Cloud-Anbieter sowie die Unteranbieter dem Cloud-Anwender zu Prüfzwecken einen Zugriff auf die Protokolldaten ermöglichen. Dem Cloud-Anwender muss eine auswertbare Protokollierung zur Verfügung gestellt und die Berechtigung zur Einsichtnahme in die Protokolldaten sollte explizit an den Cloud-Anwender vergeben werden können. Das Durchführen einer Auswertung muss dann wiederum zu einem Protokolleintrag führen. Die Aufbewahrungszeit der Protokolldaten muss durch den Cloud-Anwender konfigurierbar sein. Die Anforderungen der „Orientierungshilfe Protokollierung“[59] und der „Orientierungshilfe Mandantenfähigkeit“[60] müssen umgesetzt werden. Durch eine auswertbare Protokollierung ist es dem Cloud-Anwender zumindest möglich, neben eigenen Zugriffen auch die Zugriffe des Cloud-Anbieters und der Unteranbieter auf die Daten nachzuvollziehen.

---

[57] http://www.heise.de/newsticker/meldung/EU-Justizkommissarin-Reding-stellt-Datenabkommen-mit-den-USA-auf-den-Pruefstand-1920796.html; http://europa.eu/rapid/press-release_MEMO-13-710_en.htm.

[58] Art. 29-Gruppe, Stellungnahme 04/2014 zur Überwachung der elektronischen Kommunikation zu nachrichtendienstlichen und nationalen Sicherheitszwecken v. 10.4.2014 (WP 215)

[59] http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OH Protokollierung.html?nn=409206.

[60] http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OrientierungshilfeMandantenfaehigkeit.html?nn=409206.

Auch eine weitgehende Verschlüsselung wie eine Transport – und Inhaltsverschlüsselung bildet bei den vorgestellten Servicetypen (IaaS, PaaS und SaaS) nur einen Teilaspekt und kann nicht eine vollständige Datensicherheit gewährleisten, da der Cloud-Anwender im Rahmen der Verarbeitung der Daten eine Entschlüsselung vornehmen muss und der Cloud-Anbieter sowie die Unteranbieter dann auf die entschlüsselten Daten Zugriff nehmen könnten. Eine Inhaltsverschlüsselung unter Verwendung eigener Schlüssel (d.h. auf die der Cloud-Anbieter keinen Zugriff hat und sich auch nicht verschaffen kann) ist aber dann besonders zu empfehlen, wenn es sich um bloße Storage-Dienste handelt, bei denen über die Datenspeicherung in der Cloud hinaus keine weitere Verarbeitung erfolgt. Durch geeignete Wahl von Algorithmen und Schlüssellängen kann man hier einen langwährenden Schutz erreichen.

4 Technische und organisatorische Aspekte

Cloud-Computing-Systeme der Cloud-Anbieter unterliegen bestimmten infrastrukturellen Rahmenbedingungen, deren Schutz bezüglich der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Intervenierbarkeit und Nicht-Verkettbarkeit (nähere Definitionen siehe Kapitel 4.1.1) gewährleistet werden muss.

Dieser Schutz orientiert sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten. Die Umsetzung der Schutzziele ist durch technische und organisatorische Maßnahmen abzusichern. Die wirksame Umsetzung der technischen und organisatorischen Maßnahmen ist schriftlich nachzuweisen.

Kapitel 4.1.2 beschreibt die klassischen Risiken, und in Kapitel 4.1.3 werden die grundsätzlichen cloudspezifischen Risiken, die ein Erreichen der Schutzziele erschweren, näher erläutert.

In dem Kapitel 4.2 werden anhand der beschriebenen Schutzziele für die verschiedenen Betriebsmodelle IaaS, PaaS, SaaS die Risiken spezifiziert und die möglichen technischen und organisatorischen Maßnahmen benannt.

Kapitel 4.3 beschäftigt sich mit der Thematik Zertifizierung und Gütesiegeln aus technischer Sicht.

4.1 Ziele und Risiken

Im Bereich der IT-Sicherheit hat sich bei der Erstellung einer Risikoanalyse die Orientierung an Schutzzielen bewährt. Eine datenschutzgetriebene Risikoanalyse bezieht die klassischen Schutzziele ein und nimmt zusätzlich originäre Datenschutz-Ziele mit auf, die dem Schutz der Betroffenen dienen[61].

4.1.1 Schutzziele

Die klassischen Schutzziele der IT-Sicherheit für personenbezogene Daten sind wie folgt definiert

Verfügbarkeit: Personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß von autorisierten Benutzern verarbeitet werden.

Vertraulichkeit*:* Nur Befugte können personenbezogene Daten zur Kenntnis nehmen.

Integrität: Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell. Der spezifische Aspekt der Authentizität stellt darauf ab, dass der Ursprung von personenbezogenen Daten festgestellt werden kann.

---

[61] Siehe auch: Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Ein modernes Datenschutzrecht für das 21. Jahrhundert - Eckpunkte -, Kapitel 3, http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf

Die Schutzziele des Datenschutzes fokussieren auf Verfahren und Verfahrensabläufen:

Datensparsamkeit: Datensparsamkeit konkretisiert den Grundsatz der Erforderlichkeit, der vom Verarbeitungsprozess insgesamt wie auch von jedem seiner Schritte verlangt, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks erforderlich ist. Dies schließt auch das Löschen von Daten ein.

Transparenz: Die Verarbeitung personenbezogener Daten kann mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden. Dabei stellt der Aspekt der Revisionsfähigkeit spezifisch darauf ab, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Intervenierbarkeit: Verfahren sind so gestaltet, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte wirksam ermöglichen und entsprechende Funktionalitäten für die Daten verarbeitende Stelle zur Verfügung stehen.

Nicht-Verkettbarkeit: Verfahren sind so zu gestalten, dass personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können.

Eine Risikoanalyse muss im Hinblick auf diese unterschiedlichen Schutzziele mögliche Risiken für die Verarbeitung personenbezogener Daten identifizieren und angemessene und wirksame technische und organisatorische Maßnahmen finden, die die verbleibenden Restrisiken aus Sicht der Betroffenen und der Leitung der verantwortlichen Stelle auf ein akzeptables Maß reduzieren.

Die Angemessenheit der Schutzmaßnahmen lässt sich erst beurteilen, nachdem der Schutzbedarf der Daten und des Verfahrens, für das die Cloud genutzt werden soll, festgestellt wurde. Der Schutzbedarf lässt sich anhand einer aus der IT-Sicherheit übernommenen Typologie in „normal“, „hoch“ und „sehr hoch“ festlegen.

Wichtig dabei ist, dass der Schutzbedarf der Betroffenen, deren Daten verarbeitet werden, im Fokus steht und definiert wird. Des Weiteren sind bei einem Verfahren grundsätzlich die Komponenten Daten, IT-System und Prozess zu unterscheiden, um dann in diesen drei Bereichen jeweils bereichsspezifische Maßnahmen zu treffen, die den Schutzbedarf im jeweiligen Schutzziel umsetzen.

Es wird im Folgenden davon ausgegangen, dass in der Cloud Daten von Verfahren verarbeitet werden, die dem Schutzbedarf „normal“ unterliegen. Wenn die Cloud für Verfahren mit höherem Schutzbedarf genutzt werden soll, müssen im Einzelfall die möglichen Nutzungsformen von Clouds (siehe Kapitel 2) und entsprechende den Schutz verbessernde Maßnahmen festgelegt werden.

Im Rahmen der Dokumentation der Restrisiken sind ggf. Betroffenen über die für sie relevanten Restrisiken zu informieren.

Zusicherungen bezüglich der Schutzziele und der entsprechend getroffenen Schutzmaßnahmen müssen gemäß § 11 Abs. 2 Nr. 3 BDSG Vertragsbestandteile mit einem Cloud-Anbieter sein.

Risikoanalyse, Risikobehandlung und der Umgang mit Restrisiken sollten bereits bestehende und bewährte Vorgehensweisen übernehmen und sich auf die cloudspezifischen Risiken konzentrieren, die im folgenden Abschnitt beschrieben werden.

4.1.2 Klassische Risiken

Cloud-Computing-Systeme unterliegen ebenso wie klassische Computing-Systeme bestimmten Rahmenbedingungen, deren Schutz bezüglich der Grundwerte Verfügbarkeit, Vertraulichkeit, Integrität, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit gewährleistet werden muss.

Die Umsetzung dieser Schutzziele kann auch in der Cloud gefährdet werden durch z.B.

– versehentliches oder vorsätzliches Handeln von Mitarbeitern und Unter-Anbietern des Cloud-Computing-Providers, z. B. durch unberechtigtes Kopieren oder Klonen von Systemen, unberechtigte Manipulation oder Herunterfahren von Virtuellen Maschinen, Herunterfahren von Hosts, unberechtigte Manipulation von Konfigurationsdateien;

– unzureichendes Patchmanagement beim Provider und bei Kundensystemen;

– vorsätzliche Nutzung von Sicherheitslücken beim Provider durch andere Kunden, z. B. zur Übernahme der Kontrolle über andere Virtuelle Maschinen, durch Zugriff auf das Dateisystem des Host, zu Denial-of-Service-Angriffe auf den Hypervisor, zum Abhören der Datenkommunikation zwischen Virtuellen Maschinen, durch unberechtigte Speicherzugriffe;

– vorsätzliche Nutzung von Sicherheitslücken durch Angriffe Dritter;

– Missbrauch der Plattform des Providers, z. B. für Brute-Force-Angriffe auf Passwörter, den Aufbau von Botnetzen, die Einschleusung von Schadsoftware, das Versenden von SPAM;

– Nutzung von Sicherheitslücken auf den Übertragungswegen via Internet zwischen Kunden und Providern;

– unbeabsichtigte oder vorsätzliche Nutzung von Sicherheitslücken in den vom Provider zur Nutzung durch die Kunden bereit gestellten Software-Schnittstellen und APIs;

– Angriffe durch Schadsoftware auf die Dienste in der Cloud;

– Risiken jeglicher Form von Computerkriminalität durch schlecht kontrollierte Registrierungsmodalitäten zur Nutzung von Cloud-Diensten;

– Cloud-unabhängige Sicherheitsmängel der technischen Infrastruktur – bedingt durch fehlende oder unzureichende Sicherheitskonzepte, wie z. B. eine unsichere Stromversorgung, eine mangelhafte Klimatisierung der Infrastrukturräume oder die Zutrittskontrolle zu Gebäuden und Räumen.

4.1.3 Cloudspezifische Risiken

Eine zentrale Eigenschaft des Cloud Computing ist, dass Computerressourcen von den Cloud-Anwendern genutzt werden, auf die sie selbst keinen konkreten Zugriff haben.

Daher ist es in der Regel nicht nachvollziehbar, wo und auf welchen Systemen Anwendungen und Daten gespeichert sind, ausgeführt oder verarbeitet werden. Das Problem verstärkt sich, wenn Cloud-Anbieter ihre Dienstleistungen bei anderen Anbietern einkaufen. Dies geschieht meist nicht transparent für den Cloud-Anwender.

Im Folgenden werden die meisten der cloudspezifischen Risiken, die sich aus der Gesamtproblematik ergeben, im Einzelnen dargestellt:

Löschung von Daten

Das Löschen im Sinne des endgültigen Unkenntlichmachens von Daten kann bei Anwendungen des Cloud Computing nicht ohne Weiteres realisiert und überprüft werden. So besteht für den Cloud-Anwender die Unsicherheit, ob

– eine vollständige Löschung seiner Daten erfolgt, wenn er ein entsprechendes Kommando absetzt;

– die Daten am vorherigen Ort zuverlässig und sicher gelöscht werden oder vor dem Zugriff späterer Anwender sicher geschützt sind, wenn der Cloud-Anbieter den Ort der Erbringung der Dienstleistungen aus eigenen Erwägungen verlagert;

– für den Fall, dass in der Cloud – u. U. auch an unterschiedlichen Verarbeitungsorten - Datensicherungen vorgenommen werden, die im Echtsystem bereits gelöschten Daten nicht noch im Backup-System vorhanden sind;

– für den Fall, dass der Cloud-Betreiber defekte Speichermedien für Echt- und Backup-Systeme austauschen muss, die Daten immer noch auf diesen (defekten) Datenträgern vorhanden und damit nicht irreversibel gelöscht sind.

Nachvollziehbarkeit durch Protokollierung und Dokumentation

– Die meisten Protokolle und Dokumentationen zur Datenverarbeitung in der Cloud befinden sich beim Cloud-Anbieter, so dass die darauf aufbauende Kontrolle nicht durch den verantwortlichen Cloud-Anwender, sondern nur durch den Cloud-Anbieter erfolgen kann. Während der Cloud-Anwender kaum über regelmäßige Reports, Informationen über Schwierigkeiten und wichtige Vorfälle sowie über System- und Nutzungsprotokolle verfügt, kontrolliert sich der Cloud-Anbieter allenfalls selbst.

Vervielfältigung und Verteilung der Daten

– Anwender von Cloud Computing haben in der Regel keine Gewissheit, wo auf der Welt ihre Anwendungen laufen bzw. ihre Daten verarbeitet werden. Die Verarbeitung und Speicherung kann auch fragmentiert und damit verteilt geschehen, insbesondere dann, wenn der Cloud-Anbieter Teile seines Portfolios bei anderen Anbietern bezieht.

– Anbieter von Cloud-Services sind gemeinhin an Standorten angesiedelt, die über extrem breitbandige Internet-Anbindungen verfügen. Diese leistungsfähigen Anbindungen sind notwendig, um überhaupt Cloud-Services anbieten zu können; sie ermöglichen es aber auch, in kürzester Zeit auch große Datenmengen an andere Standorte zu verschieben oder zu kopieren.

Datentrennung

Die unter Umständen schwierige Kontrolle des Zugriffs auf Daten und Anwendungen bei der Nutzung von Cloud-Services kann dazu führen, dass

– Cloud-Anwender sogenannter virtueller Maschinen (VM) die Ressourcennutzung anderer auf dem Rechner befindlicher VM ausspionieren und darüber weitere Aktivitäten zum unbefugten Zugriff auf die in den anderen VM gespeicherten und verarbeiteten Daten entwickeln können;

– wegen der Teilung der verfügbaren Ressourcen zwischen vielen Cloud-Anwendern Risiken bestehen, da die Daten verschiedener Kunden nicht hinreichend getrennt verarbeitet werden. Dies ist insbesondere dann der Fall, wenn die gleiche Datenbankinstanz aus Kostengründen für verschiedene Cloud-Anwender eingesetzt wird und damit auf Datenseparierung verzichtet wird. Auf diese Weise können u. U. kundenindividuelle Sicherheitsanforderungen (etwa Backupzeiträume, Protokollierungsparameter, Kennwortrichtlinien) nicht mehr individuell umgesetzt werden.

Transparenz der Datenverarbeitung in der Cloud

Die Transparenz der Datenverarbeitung in der Cloud ist für die aus der Ferne arbeitenden Cloud-Anwender ohne besondere Maßnahmen des Cloud-Anbieters kaum gegeben. Dies führt u. U. dazu, dass

– die Cloud-Anwender die Kontrolle über den Zugriff auf die eigenen Daten aufgeben, wenn das Personal des Cloud-Anbieters zu allen Daten Zugang hat, die in der Cloud verarbeitet werden;

– bei der Nutzung einer (Public) Cloud – insbesondere in Drittländern – der Zugriff auf Daten des Cloud-Anwenders durch staatliche und private Stellen möglich und nicht kontrollierbar ist;

– Cloud-Anwender nicht über den Ort der Verarbeitung oder die Wege ihrer Daten durch die Cloud und die näheren Umstände der Verarbeitung beim Cloud-Anbieter informiert werden;

– Cloud-Anwender nicht kontrollieren können, ob die Umstände der Datenverarbeitung und die Maßnahmen zum organisatorischen Datenschutz beim Cloud Computing Anbieter den Verträgen zur Auftragsdatenverarbeitung (§ 11 BDSG) gerecht werden;

– Cloud-Anwender keine Kontrolle über die Datenspuren haben, die sie bei der Nutzung der Cloud hinterlassen;

– Cloud-Anwender keine Kontrolle über Unter-Anbieter der Cloud-Anbieter haben, denen der Zugriff auf die Rechner ermöglicht wird.

Weiterhin besteht aus Sicht des Cloud-Anwenders die Gefahr, dass organisationsintern neue Verfahren zur Verarbeitung personenbezogener Daten ohne die erforderliche Sorgfalt eingerichtet werden:

Cloud-Services können oft innerhalb sehr kurzer Zeiträume bereitgestellt werden. Sie sind in der Regel vorkonfiguriert und können schnell in Betrieb genommen werden. Dies kann dazu verleiten, neue Verfahren ohne die erforderliche Sorgfalt einzurichten, indem insbesondere nicht oder nur oberflächlich geprüft wird, ob bzw. unter welchen Bedingungen die vorgesehene Verarbeitung rechtlich zulässig ist, oder Systeme nicht schrittweise mit sorgfältig ausgewählten Testdaten, sondern mit Echtdaten getestet werden.

Verfügbarkeit in der Cloud

Die Verfügbarkeit der über die Cloud angebotenen Dienstleistung kann gefährdet werden durch

– Leistungsverweigerung durch betrügerisches Handeln des Cloud-Anbieters;

– Ausfall der Hardware des Providers (spontan, etwa durch Softwarefehler in den komplexen Plattformen, durch Fehler oder vorsätzliches Handeln von Mitarbeitern des Providers, durch Angriffe von außen, z. B. bei DDoS-Angriffen durch Botnetze, Beschädigung von Speichermedien bei fehlendem Backup);

– Ausfall der Dienste und Anwendungen oder Löschung von Daten durch versehentliches oder vorsätzliches Handeln von Mitarbeitern und von Unter-Anbietern des Cloud-Anbieters, z. B. durch unberechtigtes Herunterfahren einer Virtuellen Maschine oder eines Hosts;

– die spontane, versehentlich oder absichtlich bewirkte Unterbrechung von Verbindungen zwischen Netzelementen, z. B. in der Verbindung zwischen Kunden und Provider, auch bewirkt durch die bei Cloud Computing erhöhte Komplexität der Netze;

– Mängel des Qualitätsmanagements bei Vorbereitung und Betrieb der Cloud-Anwendungen, die zu Ausfällen der Provisionierung (Bereitstellung), fehlerhaften Betriebsmittel-Reservierungen, Konfigurationsfehlern sowie Fehlern beim System-Upgrade führen können;

– technische Störungen der Kommunikationskanäle eines Cloud-Anwenders, die nicht nur die Kommunikation, sondern auch die Geschäfts- und Produktionsprozesse beeinträchtigen;

– die erschwerte Erstellung von Backups sowie die Intransparenz des Backup und die Abhängigkeit vom Anbieter dabei;

– Angriffe durch Schadsoftware auf die Dienste in der Cloud.

4.2 Cloudbetriebsmodelle

In den Abschnitten 4.2.1 – 4.2.3 werden anhand der beschriebenen Schutzziele für die verschiedenen Betriebsmodelle die Risiken spezifiziert und die möglichen technischen und organisatorischen Maßnahmen benannt.

Die Umsetzung von IT-Sicherheitsmaßnahmen in Cloud-Umgebungen wird in verschiedenen Publikationen behandelt, u.a, in den Bausteinen B 5.23 Cloud-Management und B 5.25 Cloud-Nutzung der IT-Grundschutzkataloge62 des BSI, der Norm ISO 27018 und dem Dokument „Cloud-Services der Datenzentralen - Eine Richtlinienempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud“.

4.2.1 Infrastructure as a Service (IaaS)

Cloud-Anbieter, deren Dienste IaaS-Angebote beinhalten, stellen essentielle IT-Ressourcen zur Verfügung. Diese beinhalten im Wesentlichen Speicherressourcen, Rechenleistung und Kommunikationsverbindungen, die meist virtualisiert in einem Cloud-Computing-System von einem oder mehreren Anbietern bedarfsgerecht zur Verfügung gestellt werden. Ein direkter Zugriff auf die zum Anbieten des Dienstes genutzten Systemkomponenten ist nicht möglich. Alle Kernkomponenten liegen ausschließlich im Einflussbereich des Anbieters. Dennoch muss sich der Cloud-Anwender als Auftraggeber für die Datenverarbeitung über den Stand der Informationssicherheit selbst überzeugen können. Dazu sollte der Anwender die Möglichkeit erhalten, die Seriosität der Cloud-Anbieter verifizieren zu können, indem unabhängige Stellen Zertifikate für datenschutzkonforme Anbieter erteilen dürfen.

Alle Maßnahmen auf der Ebene des IaaS, die zum Erreichen der einzelnen Schutzziele dienen, liegen in der Verantwortung des Cloud-Anbieters und sollten sich an dem Schutzbedarf der zu verarbeitenden personenbezogenen Daten orientieren. In diesem Zusammenhang sind Kumulationseffekte auf Grund der systemimmanenten offenen Struktur, die an einer Vielzahl von Anwendern ausgerichtet ist, zu beachten.

---

[62] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/ Download/ download_node.html

Wie können auf der Ebene des IaaS die grundsätzlichen datenschutzrechtlichen Anforderungen technisch umgesetzt werden?

Infrastrukturelle Gegebenheiten (z.B. physikalische Sicherheit)

Der Schutz der infrastrukturellen Gegebenheiten umfasst alle technischen und organisatorischen Maßnahmen, die auf den Schutz der Liegenschaft, insbesondere der Gebäude und Räume, in denen die zu betrachtenden IT-Komponenten aufgestellt sind, gerichtet sind. Dazu zählt z. B. eine sichere Stromversorgung, Aspekte des Brandschutzes und der Klimatisierung, Zugangs-, Zutritts- und Zugriffssicherungssysteme sowie Redundanzen essentieller Komponenten.

Vertraulichkeit, Verfügbarkeit

Eine typische Gefährdung für die Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und deren personenbezogener Daten basiert auf dem Diebstahl und Ausfall von nicht redundanter Hardware (z. B. Speichermodule oder Rechner), die sich im Einflussbereich des Cloud-Anbieters (Ressourcen-Anbieter) befinden.

IT-Systeme (z. B. Host, Speicher)

Die Prozesse in der Cloud und deren Berechnungen werden auf den IT-Systemen (Hardware) des Ressourcen-Anbieters ausgeführt und müssen ebenfalls angemessen abgesichert werden. Dazu zählen z. B. Zugangsbeschränkungen, Patchmanagement, sichere Grundkonfiguration, Sicherheitsrichtlinien, Integritätsprüfung, revisionssichere Protokollierung, Datensicherung, Intrusion-Detection-Systeme (IDS), Firewalls und Virenschutz.

Vertraulichkeit, Integrität, Verfügbarkeit

Der Cloud-Anwender wird mittels der Virtualisierungstechnologie daran gehindert, direkt auf die Hardware-Ebene durchzugreifen. Diese Isolation kann die Etablierung einer sicheren Umgebung begünstigen.

Als besonders schützenswert ist der Cloud-Operator (Cloud Control) zu betrachten, da dieser die zur Verfügung gestellten Ressourcen koordiniert und dem Nutzer bedarfsgerecht zur Verfügung stellt.

Die wesentliche Maßnahme der Zusicherung von Verfügbarkeit besteht in Redundanz. Das bedeutet bei Daten typischerweise das Vorhalten von Backups und bei IT-Systemen das Vorhalten von Ersatzsystemen beim Cloud-Anbieter. Redundanz kann unter Umständen auch bedeuten, dass die Cloud eines Vertragspartners für eine gewisse Zeit, für den Anwender normalerweise nicht erkennbar, ersatzweise „einspringt“.

Datensparsamkeit

Zur Umsetzung dieses Schutzzieles ist es erforderlich, dass Löschungen, die im Wesentlichen durch Anwendungen gesteuert werden, auch auf IT-System-Ebene durchgesetzt werden (z.B. Löschung in Backups, Datenschutzgerechte Vernichtung von Datenträgern).

Netze (z. B. Kommunikationsverbindungen)

Die Kommunikationsverbindungen zwischen den Cloud-Ressourcen sowie den Cloud-Anwendern stellen zentrale Komponenten dar, die bezüglich der Schutzziele, insbesondere der Vertraulichkeit und Verfügbarkeit, abgesichert werden müssen.

Vertraulichkeit, Integrität

Die Vertraulichkeit personenbezogener Daten ist zu wahren, indem zu deren Schutz kryptographische Verfahren (gegenseitige Authentifizierung und Ende-zu-Ende-Verschlüsselung zwischen den Kommunikationspartnern) eingesetzt werden. Dies betrifft auch die für die Administration eingerichteten Fernwartungszugänge.
Netzbasierte Angriffe können mittels Intrusion-Detection-Systemen (IDS) und Intrusion-Prevention-Systemen (IPS) ermittelt bzw. verhindert werden, um mit speziell abgestimmten Maßnahmen reagieren zu können.

Verfügbarkeit

Da die Verfügbarkeit ein wesentlicher Aspekt netzbasierter Maßnahmen darstellt, sollten die Kommunikationsverbindungen zwischen den Rechenzentren sowie deren Anbindung an das Netz redundant ausgelegt sein.

Virtualisierung

Cloud-Systeme zeichnen sich durch die Verwendung der Virtualisierung aus, hierbei werden dem Cloud-Anwender virtualisierte Ressourcen (z. B. virtueller Speicher, virtuelle Maschinen) zur Verfügung gestellt. Die physischen Ressourcen werden dabei mittels einer Virtualisierungssoftware (Virtual Machine Monitor - VMM oder Hypervisor) abstrahiert. Die damit einhergehende Steigerung der Komplexität (jede virtuelle Maschine benötigt ein Server-, Storage- und Netzwerkkonzept) erhöht auch die Komplexität der Sicherheitsanforderungen und bedarf zusätzlicher, der Technologie geschuldeter Sicherheitsuntersuchungen (z. B. Verschiebung (VMotion) und Snapshots virtueller Maschinen). Des Weiteren unterliegen Virtualisierungen besonderen Bedingungen bei den Bereitstellungsmechanismen von CPU und RAM sowie der Storage- und Netzwerk-Anbindung, die einer gesonderten Risikoanalyse bedürfen.

Transparenz

Der Cloud-Anwender sollte auf die Veröffentlichung von Benutzerrichtlinien zur Absicherung der virtuellen Systemlandschaft des Cloud-Anbieters achten. Der Einsatz zertifizierter Virtualisierungssoftware erhöht neben der Sicherheit auch die Transparenz des verwendeten Systems und schafft Vertrauen bei den Anwendern.

Integrität / Vertraulichkeit

Eine besondere Bedeutung kommt dem sensitiven administrativen Zugang zu diesen Maschinen zu, da dieser in der Regel über öffentliche Netze läuft und dementsprechend abgesichert werden muss. Ferner sollte ein durchdachtes Rechte- und Rollenkonzept für diese Zugänge geschaffen werden.

4.2.2 Platform as a Service (PaaS)

Bietet ein Cloud-Anbieter PaaS-Dienste an, so bietet er Infrastrukturen zur Entwicklung von Cloud-Anwendungen an. In diesen Entwicklungsumgebungen, die auch als technische Frameworks oder Laufzeitumgebungen bezeichnet werden, können Cloud-Anwender eigene Anwendungen entwickeln.
Die Entwicklungsumgebung bietet technische Funktionen, wie Datenbanken und Werkzeuge, die es den Anwendern ermöglicht, gleichzeitig an Programmen, Dokumenten und Daten zu arbeiten.

Grundlegende Einstellungen an diesen Infrastrukturen können in der Regel vom Cloud-Anwender nicht oder nur in sehr begrenztem Umfang durchgeführt werden. Diese administrative Hoheit liegt daher beim Cloud-Anbieter. Da die Anwender die Anwendungen selbst entwickeln, haben sie direkten Einfluss auf diese und somit auf die Art und Weise, wie Daten innerhalb der Anwendungen und der Laufzeitumgebungen verarbeitet werden. Die datenschutzrechtliche Verantwortung für diese Daten liegt bei den Cloud-Anwendern.

Bei der Entwicklung der Anwendungen ist der Grundsatz der Datensparsamkeit zu beachten (§ 3a BDSG). Dies gilt sowohl für die innerhalb der Anwendung zu verarbeitenden Daten als auch für eventuelle Protokoll-Daten, die von den selbst ent-wickelten Anwendungen oder den dabei eingesetzten Funktionalitäten der PaaS-Umgebung erzeugt werden.

Wie bei allen Cloud-Services gilt es, genaue vertragliche Regelungen (Verträge nach § 11 BDSG bzw. in Standardverträgen und ggf. in separaten Verträgen, im Folgenden vereinfachend insgesamt auch als Service Level Agreements bezeichnet, SLA) zwischen Cloud-Anbieter und Anwender festzulegen, um weitestgehende Kontrolle des Anwenders über die Datenverarbeitung in der Cloud zu realisieren. Ändert der Cloud-Anbieter Bestandteile seiner PaaS-Umgebungen, so darf das nur mit voriger Information – in Einzelfällen auch nur mit Zustimmung – des Cloud-Anwenders passieren.

Die Kontroll- und Regelungsmöglichkeiten sind von immenser Wichtigkeit, um die gesetzlichen Anforderungen bezüglich des Datenschutzes an den Auftraggeber (hier Cloud-Anwender) erfüllen zu können. Die Anforderungen können nur bei ausreichender Transparenz, das heißt durch einen wohl informierten Kunden, wahrgenommen werden. Wohl informiert bedeutet in diesem Fall, dass der Cloud-Anwender Hilfsmittel an die Hand bekommt, mit denen er sich von der datenschutzkonformen und vertragsgemäßen Verarbeitung personenbezogener Daten überzeugen kann. Diese Hilfsmittel können sowohl technischer als auch organisatorischer Natur sein.

Transparenz

Wenn der Cloud-Anbieter Richtlinien zur Erstellung von sicheren, datenschutzkonformen Anwendungen an die Cloud-Anwender herausgibt, kann dies zur Umsetzung des Schutzziels „Transparenz“ beitragen.

Verfügbarkeit

Jeder Cloud-Anbieter muss – wie jedes herkömmliche Rechenzentrum – zwingend über eine funktionierende Sicherheitsarchitektur und das zugehörige Management verfügen. Idealerweise nutzt jeder Cloud-Anbieter nur entsprechend zertifizierte, eigene Rechenzentren oder Rechenzentren von Unter-Anbietern.

Besonderes Augenmerk bei der Auswahl des Cloud-Anbieters muss der Cloud-Anwender grundsätzlich auch auf die Portabilität richten: Alle Inhalte der PaaS-Umgebung sollten ohne Probleme zu einem anderen Anbieter portierbar sein. Leider ist der Datenexport häufig nicht ohne größeren Aufwand möglich, da die Anwendungen in einem bestimmten Kontext entwickelt wurden. Portierbarkeit ist eine Vorsichtsmaßnahme, die besonders bei einer Insolvenz des Cloud-Anbieters zum Tragen kommt, wenn der PaaS-Dienst nicht aufrechterhalten werden kann. In diesem Zusammenhang kommt auch der Zugriffsmöglichkeit durch den Cloud-Anwender eine besondere Bedeutung zu: Der Anwender muss die Möglichkeit haben, auch im Rahmen einer Insolvenz des Anbieters auf seine Daten zuzugreifen und diese aus den Systemen des Anbieters beispielsweise auf die Systeme eines anderen Anbieters zu transferieren.

Eine (möglichst) geographisch verteilte, redundante Datenhaltung und -Verarbeitung ist in Hinblick auf die Verfügbarkeit in der Cloud von Vorteil, für die Transparenz von Nachteil. Eine leicht zu realisierende, geografisch vom jeweils aktuell genutzten Verarbeitungsstandort getrennte Datensicherung ist hinsichtlich der Verfügbarkeit notwendig. Wie immer im Zusammenhang mit Datensicherungen gilt: Werden Daten im Echtsystem ordnungsgemäß gelöscht, müssen diese auch aus den vorhandenen Datensicherungen irreversibel entfernt werden.

Datensparsamkeit

Bei der Entwicklung der Anwendungen ist der Grundsatz der Datensparsamkeit zu beachten (§ 3a BDSG). Dies gilt sowohl für die innerhalb der Anwendung zu verarbeitenden Daten als auch für eventuelle Protokoll-Daten, die von den selbst ent-wickelten Anwendungen oder den dabei eingesetzten Funktionalitäten der PaaS-Umgebung erzeugt werden. Löschanweisungen von Anwendungen müssen auch auf Ebene der Plattform (z. B. Datenbankmanagementsystem) durchgesetzt werden.

Transparenz und Revisionsfähigkeit

Im Hinblick auf die Transparenz ist für den Cloud-Anwender bei der Nutzung von PaaS eine revisionssichere Protokollierung erforderlich. Das betrifft in erster Linie die Protokoll-Systeme des Cloud-Anbieters. Die Anwender müssen in die Lage versetzt werden, Einsicht in eine lückenlose, unverfälschte Protokollierung zu erhalten, um etwaige unberechtigte Zugriffe auf personenbezogene Daten festzustellen und beson-

ders auch um die Tätigkeiten des Anbieters in Bezug auf die SLA überprüfen zu können.

Weiterhin ist ein Konfigurationsmanagement seitens des Anbieters geboten, um sich selbst und auch den Anwender jederzeit in die Lage versetzen zu können, die jeweils aktuellen oder in der Vergangenheit in Betrieb befindlichen Cloud-Konfigurationen nachvollziehen zu können.

Nicht-Verkettbarkeit

Bedrohungen für das Schutzziele Nicht-Verkettbarkeit bestehen in einer PaaS-Umgebung durch eine unkontrollierte verfahrensübergreifende Zusammenführung von Daten oder Funktionalitäten aufgrund einer leichteren technischen Machbarkeit: Liegen beispielsweise Adressendatenbestände eines Verfahrens in einer Datenbank „ohnehin“ vor, so liegt der Gedanke nahe, diese Adressdaten in anderen Verfahren mittels einer Schnittstelle zu nutzen und auf diese Weise (unbeabsichtigt) ein gemeinsames Verfahren zu schaffen.

Eine geeignete Maßnahme zur Sicherstellung ist eine sorgfältige Analyse im Vorfeld, welche Plattformbestandteile und welche Datenbestände sich unter welchen Voraussetzungen (mit-)nutzen lassen.

Intervenierbarkeit

Relevant ist hier, ein IT-Sicherheits- und Datenschutzmanagement auf Seiten des Cloud-Anbieters sicherzustellen (z. B. im Rahmen vertraglicher Vereinbarungen) und Schnittstellen zum eigenen IT-Sicherheits- und Datenschutzmanagement zu schaffen.

Es ist wichtig, Vorgehensweisen für die Bearbeitung von IT-Sicherheits- und Datenschutzvorfällen zu etablieren (etwa Verlust von Daten, unberechtigte Zugriffe auf Plattformebene, Bearbeitung von Auskunftsersuchen).

4.2.3 Software as a Service (SaaS)

Bei der Nutzung eines SaaS-Angebots nutzt der Cloud-Anwender die Infrastruktur, die Plattformen und Anwendungssoftware des Cloud-Anbieters. Die „Schnittstelle“ zwischen Anwender und Anbieter ist dabei weiter in die Sphäre des Anwenders und seiner konkreten Anwendungsbedürfnisse vorgerückt. Daher gelten die technischen und organisatorischen Anforderungen, die für die Betriebsformen Infrastructure as a Service (IaaS) und Platform as a Service (PaaS) formuliert worden sind, für SaaS gleichermaßen. Zu den IT-Sicherheitsanforderungen, die der Anbieter mit seiner Infrastruktur und seinen Plattformen zu erfüllen hat, kommen zusätzliche verfahrensspezifische Anforderungen an eine sichere und ordnungsgemäß funktionierende Anwendung hinzu. Zwar wird der Anwender von seiner datenschutzrechtlichen Verantwortung für seine IT-Anwendungen nicht entbunden, seine Einflussmöglichkeiten im laufenden Betrieb sind jedoch auch für die Anwendungsprogramme minimal, weil er alles – sozusagen von der Stange – einkauft.

Da die Spielräume für das Customizing bei Cloud-Anwendungen meist gering sind, muss der Anwender je nach Bedeutung und Tiefe der Anwendung[63] mehr oder weniger einschneidende Anpassungen seiner Strukturen und Geschäftsprozesse in Kauf nehmen. Weil er sich im laufenden Betrieb in großer Abhängigkeit vom Anbieter befindet, muss der Anwender seiner Verantwortung für die Anwendung vor Beginn der Cloud-Nutzung nachkommen und über die wichtigsten Anwendungsaspekte die Kontrolle behalten. Das wichtigste Schutzziel, dessen Erreichung der Anwender vom Anbieter verlangen muss, ist daher die Transparenz. Sie muss den Anwendern ermöglichen, mit den Anbietern anspruchsvolle Service Level Agreements (SLAs) zu vereinbaren, die es den Anwendern ermöglichen, ihre Verantwortung wahrzunehmen, schon um den hohen Compliance-Anforderungen nachzukommen.

Cloud-Dienste werden gewöhnlich mittels Web-basierten Technologien (z. B. Webinterfaces für Anwender und zur Administration, client-seitige Application Frameworks) zur Verfügung gestellt. Diese beinhalten Risiken für die in der Cloud zu verarbeitenden Daten, sofern die Prinzipien einer sicheren Software-Entwicklung auf Seiten des Cloud-Anbieters nicht eingehalten werden und der Cloud-Anwender sein Webinterface im Rahmen eines Sicherheitskonzepts, dem Schutzbedarf der Daten angemessen, nicht schützt.

Datensparsamkeit

Bei der Auswahl und der Konfiguration der Anwendungen ist der Grundsatz der Datensparsamkeit zu beachten (§ 3a BDSG). Dies gilt sowohl für die innerhalb der Anwendung zu verarbeitenden Daten als auch für eventuelle Protokoll-Daten, die von den Anwendungen oder den dabei eingesetzten Funktionalitäten der SaaS-Umgebung erzeugt werden. Anwendungen müssen Löschanweisungen erlauben und diese auch auf Ebene der Plattform (z. B. Datenbankmanagementsystem) durchgesetzen.

Transparenz und Intervenierbarkeit

Der Anwender ist verpflichtet zu prüfen, ob der Anbieter neben anderem auch hinreichende Garantien für die Sicherheit und Ordnungsmäßigkeit aller in der Cloud bereitgestellten Ressourcen gibt und ob das Anwendungsverfahren hinsichtlich der Nutzung personenbezogener Daten den für den Anwender geltenden gesetzlichen Bestimmungen genügt. Dazu gehören sowohl die datenschutzrechtliche Zulässigkeit als auch die Beachtung des Gebots der Datensparsamkeit und die Umsetzbarkeit der Betroffenenrechte, die ggf. spezielle Funktionalitäten zur Auskunftserteilung, Sperrung oder Beachtung von Widersprüchen erfordern. Der Anwender muss dies durch bereit gestellte Dokumentationen und Protokolle nachvollziehen und ggf. nachweisen können. Dabei würde ihm helfen, wenn der Anbieter auch Zertifikate unabhängiger Stellen vorlegen kann, die die Konformität der Anwendungssoftware mit den datenschutzrechtlichen Bestimmungen versichern, die für den Anwender gelten.

Der spezielle Aspekt der Revisionsfähigkeit wird durch die nachträgliche regelmäßige oder anlassbezogene Prüfung sicherheitsrelevanter Vorgänge bei der Datenverarbei-

[63] So wird zum Beispiel eine SaaS-Nutzung von Office-Anwendungen wie etwa bei Google Apps weniger Anpassungsbedarf benötigen als Personalinformationssysteme oder Kundenbindungssysteme (CRM)

tung erreicht. Diese Prüfung setzt voraus, dass die wichtigsten Angaben zu den sicherheitsrelevanten Vorgängen wie z. B. Veränderungen an der Infrastruktur, an den Plattformen und der Anwendungssoftware, wie bestimmte Systemverwaltereingriffe, Änderung und Löschung von Anwendungsdaten, Logins und Programmaufrufe von Anwendern einer Protokollierung unterliegen. Entsprechende Anforderungen an Auditing- und Reportfunktionen sind in den SLAs festzulegen.

Protokolle bezüglich der Infrastruktursicherheit sind vom Anbieter zu führen und zu kontrollieren. Der Anwender sollte sich vertraglich vorbehalten, dass ihm Sicherheitsvorfälle, die seine Anwendungen betreffen können, rechtzeitig bekannt gemacht werden, damit er nötigenfalls eigene Konsequenzen ziehen kann. Seitens der Anwender sind die Aktivitäten an der Cloud-Schnittstelle einer Protokollierung zu unterwerfen, um fehlerhafte bzw. missbräuchliche Nutzungen des Cloud-Zugangs kontrollieren zu können.

Ein weiterer Aspekt der Intervenierbarkeit, aber auch der Verfügbarkeit im Hinblick auf das ganze Verfahren ist die Möglichkeit des Datenexports und Migration zu einem anderen Cloud-Anbieter, damit der Wechsel zu einem anderen Auftragnehmer ein realistisches Szenario ist.

Vertraulichkeit

Die Vertraulichkeit der Anwendungsdaten wird durch die Verhinderung des unbefugten Zugangs an Netz-, Speicher- und Verarbeitungskomponenten der Infrastruktur und des unbefugten Zugriffs auf die Daten sowie durch die Nutzung kryptografischer Verfahren bei der Übertragung und Speicherung der Daten gewährleistet (gemäß Nr. 2 der Anlage zu § 9 Satz 1 BDSG). Die Sicherung des Zugangs zur Infrastruktur gehört ebenso zum Angebot des Anbieters wie auch die Bereitstellung kryptografischer Verfahren für die sichere Übertragung und Speicherung der Anwendungsdaten. Soweit der Anbieter die Verschlüsselung der Daten nicht obligatorisch vorsieht, ob er es also dem Anwender überlässt, bei der Übertragung der Daten zwischen Anwender und Anbieter und/oder bei der Speicherung in der Infrastruktur des Anbieters für eine Verschlüsselung der Daten zu sorgen, kann der Anwender insoweit selbst in Abhängigkeit vom Schutzbedarf seiner Daten für die angemessene Nutzung der Verschlüsselungsoptionen sorgen.

Ebenfalls liegen die Sicherheitsmaßnahmen an der Anwender-Anbieter-Schnittstelle in der Verantwortung des Anwenders. Dies gilt sowohl für die Nutzung der Systeme des Anwenders, von denen aus die Cloud-Anwendung betrieben wird, als auch für den Aufruf der Cloud-Anwendung über diese Systeme, bei dem allerdings das von der Anwendungssoftware des Anbieters bereitgestellte Authentisierungsverfahren Verwendung findet.

Der Umgang mit den Authentisierungsmitteln, also mit Kennungen, Passwörtern, PINs, TANs, maschinenlesbaren Ausweisen und Token, ggf. auch biometrischen Merkmalen liegt in der Verantwortung des Anwenders.

Verfügbarkeit

Maßnahmen zu Absicherung der Verfügbarkeit einer SaaS-Anwendung liegen fast ausschließlich in der Hand des Anbieters. Der Schutz vor Angriffen auf die Verfügbar-

keit der Infrastruktur (z. B. DDoS-Angriffe), der Plattformen und der Anwendungssoftware ist Teil der Dienstleistung, die in Verträgen verabredet wird.

Die Anwender sind für die Verfügbarkeit ihrer Seite der Anwender-Anbieter-Schnittstelle verantwortlich, also in der Regel für den PC, die Internetverbindung und den Webbrowser für den Zugang an die Cloud. Sofern die Datensicherung nicht Teil der Cloud-Dienstleistung ist, muss sie ferner vom Anwender über die Schnittstelle zur Cloud realisiert werden können.

Integrität

Die Integrität der Anwendungsdaten wird durch fehlerhafte bzw. nicht ordnungsgemäß gestaltete Verarbeitungsverfahren und durch unbefugte oder unbeabsichtigte Datenveränderungen gefährdet. Da bei SaaS die Verarbeitungsverfahren in der Verantwortung des Anbieters liegen, hat dieser Verfahrensmängel zu vermeiden bzw. zu beseitigen. Unbefugte Datenveränderungen können durch Angriffe auf die Infrastruktur und die Plattformen, z. B. durch unzuverlässige Mitarbeiter des Anbieters bewirkt werden und müssen durch Maßnahmen des Anbieters wirksam verhindert werden.

Aber auch seitens der Anwender kann der nachlässige oder vorsätzlich schädigende Umgang mit den eigenen Anwendungsdaten über die Cloud-Schnittstelle zu Integritätseinbußen führen. Hier liegt es nun wieder in der Verantwortung der Anwender, angemessene Maßnahmen zu ergreifen, damit dies nicht geschieht bzw. großer Schaden verhindert wird. Dabei wäre den Anwendern geholfen, wenn die vom Anbieter bereitgestellten Anwendungen geeignete Plausibilitätsprüfungen ermöglichen würden.

Nichtverkettbarkeit

Ähnlich wie bei der Betriebsform PaaS kann eine Bereitstellung von Verkettungsmöglichkeiten durch Softwarefunktionen bei der Betriebsform SaaS das Schutzziel Nichtverkettbarkeit gefährden. Hier liegt die Gefährdung in einer ungeregelten Nutzung solcher Funktionalitäten der Software,

Eine Gegenmaßnahme ist eine sorgfältige Auswahl und Analyse der Software im Vorfeld, die Festlegung der zu nutzenden Funktionalitäten und deren Umsetzung im Rahmen der Konfiguration.

4.3 Zertifizierungen

Cloud-Anwendern ist es in der Regel nicht oder nur selten möglich, sich direkt bei den Cloud-Anbietern von der vertragsgemäßen Verarbeitung der Daten zu überzeugen. Die Daten und Anwendungen können zeitgleich über eine Vielzahl von geografisch getrennten Standorten verteilt sein. Eine Vor-Ort-Kontrolle wird dadurch unmöglich. Es ist daher zwingend notwendig und vertraglich zu regeln, dass der Cloud-Anbieter alle möglichen Unter-Anbieter sowie alle Standorte bekannt gibt, an denen die Verarbeitung stattfindet bzw. im Rahmen des Vertragsverhältnisses stattfinden könnte. Dazu gehören insbesondere auch die Standorte der Unter-Anbieter. In diesem Zusammenhang ist darauf hinzuweisen, dass der Cloud-Anbieter für die Datenverarbeitung der Unter-Anbieter haftet, aber mit zunehmender Anzahl von eingebundenen Unter-Anbietern selbst das Problem hat, die Kontrolle über die Daten zu verlieren.

Dem Problem schwieriger Überprüfbarkeit der vertragsgemäßen Verarbeitung der Daten kann unter Umständen dadurch begegnet werden, dass lediglich Angebote von Cloud-Anbietern genutzt werden, die regelmäßig von unabhängigen Stellen auditiert und zertifiziert werden. Unabhängige Stellen können die Korrektheit der entsprechenden Verfahren zu einem Prüfzeitpunkt bestätigen. Zusätzlich ist es für die Transparenz gegenüber dem Anwender von Vorteil, wenn der Anbieter von Cloud-Diensten regelmäßig Berichte über das Sicherheitsumfeld zu den Diensten veröffentlicht. Bei akuten Vorfällen ist eine unverzügliche und aussagekräftige direkte Information der Cloud-Anwender erforderlich.

Ein den deutschen Datenschutzanforderungen gleichwertiges Datenschutzniveau ist lediglich dann gewährleistet, wenn die Verarbeitung personenbezogener Daten ausschließlich innerhalb der EU oder EWR-Vertragsstaaten stattfindet und die personenbezogenen Daten bei Unternehmen gespeichert und verarbeitet werden, die keinen EU/EWR- fremden staatlichen Kontrollen unterstehen.

5 Fazit

Cloud Computing steht für vielfältige Möglichkeiten, Dienstleistungen zur Datenverarbeitung unter Verwendung des Internet oder anderer Wide Area Networks wie Konzernnetze oder die Landesnetze der Verwaltungen in Anspruch zu nehmen. Ob Public, Private, Community oder Hybrid Clouds, ob SaaS, PaaS oder IaaS: Allen Varianten gemein ist, dass die Anwender Leistungen von Anbietern in Anspruch nehmen, die über das jeweilige Netz erreicht werden können, die wegen ihrer Skalierbarkeit flexibel an den jeweils aktuellen Bedarf angepasst werden können und nach Verbrauch bezahlt werden. Bei allen Varianten unterschiedlich sind jedoch der Umfang und die Art der Dienstleistung, die Bestimmt- oder Unbestimmtheit der Verarbeitungsorte, die Einflussmöglichkeiten der Anwender auf die örtlichen, infrastrukturellen und qualitativen Rahmenbedingungen der Verarbeitung. Unterschiedlich sind auch die datenschutzrechtlichen und informationssicherheitstechnischen Anforderungen.

Die wirtschaftlichen Vorteile des Cloud Computing für die Anwender sind nicht zu übersehen. Die starke Reduktion der selbst noch vorzuhaltenden Infrastruktur, die Verringerung des Bedarfs an eigenem IT-Fachpersonal, die Vermeidung von Risiken der Über- und Unterkapazitäten und die bessere Übersichtlichkeit der Kosten der Datenverarbeitung sind für Unternehmen und Behörden gute Gründe, die Beauftragung von Cloud-Computing-Anbietern in Erwägung zu ziehen.

Problematisch ist es jedoch, die Compliance-Anforderungen an die Datenverarbeitung der Unternehmen und Behörden, zu denen Datenschutz und Informationssicherheit, aber auch die Kontrollierbarkeit, Transparenz und Beeinflussbarkeit gehören, unter den Rahmenbedingungen des Cloud Computing, insbesondere in der Public Cloud, zu erfüllen. Es muss verhindert werden, dass die Fähigkeit der Organisationen, allen voran ihrer Leitungen, die Verantwortung für die eigene Datenverarbeitung noch tragen zu können, durch das Cloud Computing untergraben wird.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Anwender klare Entscheidungskriterien bei der Wahl zwischen den Anbietern haben, aber auch, ob Cloud Computing überhaupt in Frage kommt;

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z. B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen“ kann;

- die Umsetzung von abgestimmten Sicherheitsmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender;

- die Vorlage aktueller Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird, zur Gewährleistung der Informationssicherheit und der o. g. Portabilität und Interoperabilität durch anerkannte und unabhängige Prüfungsorganisationen.

Zur Gewährleistung einer rechtmäßigen Weitergabe personenbezogener Daten an einen Cloud-Anbieter, der außerhalb der EU/des EWR seinen Sitz hat, bedarf es in erster Linie der Verwendung von Standardvertragsklauseln oder BCR`s, wobei der Beschreibung und Umsetzung technisch-organisatorischer Sicherheitsmaßnahmen eine besondere Bedeutung zukommt. Rechtsgrundlage für die Datenweitergabe an einen Cloud-Anbieter kann in diesem Zusammenhang § 28 Abs. 1 Satz 1 Nr. 2 BDSG sein. Eine Rechtsgrundlage für die Weitergabe besonderer personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG wird dabei regelmäßig nicht bestehen, da die Anforderungen nach § 28 Abs. 6 bis 9 BDSG nicht erfüllt sind.

Soweit öffentliche Stellen Cloud Services in Drittstaaten anwenden, ist eine besonders sorgfältige Prüfung der Rechtsgrundlage geboten, denn ein dem § 28 Abs.1 Satz 1 Nr. 2 BDSG entsprechender Erlaubnistatbestand dürfte es in den Landesdatenschutzgesetzen nicht geben, soweit ersichtlich.

Da insbesondere außereuropäische Behörden nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt werden, muss eine Neubewertung vorgenommen werden. Bevor nicht der unbeschränkte Zugriff

ausländischer Nachrichtendienste auf personenbezogene Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt wird, behalten sich die Aufsichtsbehörden für den Datenschutz vor, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten zur Nutzung von Cloud-Diensten zu erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind.