01037/12/DE
WP 196

Stellungnahme 05/2012 zum Cloud Computing

Angenommen am 1. Juli 2012

Zusammenfassung

In dieser Stellungnahme analysiert die Artikel-29-Datenschutzgruppe alle relevanten Fragen, die im Europäischen Wirtschaftsraum (EWR) tätige Cloud Computing-Diensteanbieter und ihre Kunden betreffen. Dabei werden alle einschlägigen anzuwendenden Grundsätze aus der EU-Datenschutzrichtlinie (95/46/EG) und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung) aufgeführt.

Trotz der anerkannten wirtschaftlichen und gesellschaftlichen Vorteile des Cloud Computing zeigt die vorliegende Stellungnahme, wie die weit verbreitete Nutzung von Diensten des Cloud Computing zu einer Reihe von Datenschutzrisiken führen kann. Hier geht es in erster Linie um die fehlende Kontrolle über personenbezogene Daten und über unzureichende Informationen darüber, wie, wo und durch wen die Daten verarbeitet bzw. im Unterauftrag verarbeitet werden. Diese Risiken müssen von öffentlichen Einrichtungen und Privatunternehmen sorgfältig bewertet werden, wenn sie in Betracht ziehen, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen. Die vorliegende Stellungnahme untersucht Fragen, die mit der gemeinsamen Nutzung von Ressourcen mit anderen Parteien verbunden sind; die fehlende Transparenz in einer Outsourcing-Kette, die aus zahlreichen Auftragsverarbeitern und Unterauftragnehmern besteht; das Fehlen eines gemeinsamen, weltweiten Rahmens für die Datenportabilität und die Ungewissheit bezüglich der Zulässigkeit der Übermittlung personenbezogener Daten an Cloud-Anbieter, die außerhalb des EWR niedergelassen sind. Ähnlich wird in der Stellungnahme hervorgehoben, dass der Mangel an Transparenz in Bezug auf die Informationen, die ein für die Verarbeitung Verantwortlicher der betroffenen Person über die Art der Verarbeitung ihrer personenbezogenen Daten geben kann, Anlass zu ernster Besorgnis ist. Die betroffenen Personen müssen[1] darüber informiert werden, wer ihre Daten für welche Zwecke verarbeitet, damit sie ihre diesbezüglichen Rechte ausüben können.

Eine wichtige Schlussfolgerung dieser Stellungnahme ist, dass Unternehmen und Verwaltungen, die Cloud Computing nutzen wollen, als ersten Schritt eine umfassende und gründliche Risikoanalyse durchführen sollten. Alle Cloud-Anbieter, die Dienste im EWR anbieten, sollten dem Cloud-Anwender alle Informationen geben, die dieser benötigt, um die Vor- und Nachteile der Inanspruchnahme eines solchen Dienstes gründlich gegeneinander abwägen zu können. Beim Anbieten von Diensten des Cloud Computing sollten Sicherheit, Transparenz und Rechtssicherheit für die Anwender die wichtigsten Aspekte sein.

In den Empfehlungen dieser Stellungnahme wird die Verantwortung eines Cloud-Anwenders als für die Verarbeitung Verantwortlicher hervorgehoben, und es wird folglich empfohlen, dass der Anwender einen Cloud-Anbieter auswählt, der die Einhaltung der EU-Datenschutzbestimmungen gewährleistet. In der Stellungnahme werden geeignete vertragliche Absicherungsklauseln angesprochen. Dabei wird gefordert, dass jeder Vertrag zwischen dem Cloud-Anwender und dem Cloud-Anbieter ausreichende Garantien in

[1] Die im nachstehenden Teil dieses Dokuments verwendeten Schlüsselbegriffe "MUSS" bzw. "MÜSSEN", "DARF NICHT" bzw. "DÜRFEN NICHT", "ERFORDERLICH", "SOLLTE(N)", "SOLLTE(N) NICHT", "EMPFOHLEN", "KANN" bzw. "KÖNNEN" und "OPTIONAL" sind wie in RFC 2119 beschrieben auszulegen. Das Dokument ist verfügbar unter http://www.ietf.org/rfc/rfc2119.txt. Aus Gründen der Lesbarkeit werden diese Wörter in dem Dokument jedoch nicht alle in Großbuchstaben gedruckt.

Bezug auf technische und organisatorische Maßnahmen enthält. Die Empfehlung, dass der Cloud-Anwender überprüfen sollte, ob der Cloud-Anbieter die Rechtmäßigkeit jeder grenzüberschreitenden Datenübermittlung garantieren kann, ist ebenfalls von Bedeutung.

Wie bei jedem Entwicklungsprozess stellt auch der Aufstieg des Cloud Computing zu einem weltweiten technologischen Paradigma eine Herausforderung dar. Für sich betrachtet, kann diese Stellungnahme als wichtiger Schritt zur Festlegung der Aufgaben angesehen werden, die von der Datenschutzgemeinde in den folgenden Jahren übernommen werden müssen.

Inhalt

Zusammenfassung ... 2
1. Einleitung ... 5
2. Datenschutzrisiken des Cloud Computing ... 6
3. Rechtsrahmen ... 8
3.1 Datenschutzrahmen ... 8
3.2 Anwendbares Recht ... 8
3.3 Pflichten und Verantwortlichkeiten der verschiedenen Beteiligten ... 9
3.3.1 Cloud-Anwender und Cloud-Anbieter ... 9
3.3.2 Unterauftragnehmer ... 11
3.4 Datenschutzanforderungen in dem Verhältnis Anwender-Anbieter ... 13
3.4.1 Einhaltung der Grundprinzipien ... 13
3.4.1.1 Transparenz ... 13
3.4.1.2 Zweckbestimmung und -begrenzung ... 14
3.4.2 Vertragliche Absicherungsklauseln der Beziehung(en) „für die Verarbeitung Verantwortlicher“ - „Auftragsverarbeiter“ ... 15
3.4.3 Technische und organisatorische Maßnahmen des Datenschutzes und der Datensicherheit ... 17
3.4.3.1 Verfügbarkeit ... 18
3.4.3.2 Integrität ... 18
3.4.3.3 Vertraulichkeit ... 18
3.4.3.4 Transparenz ... 19
3.4.3.5 Isolierung (Zweckbegrenzung) ... 19
3.4.3.5 Intervenierbarkeit ... 20
3.4.3.6 Portabilität ... 20
3.4.4.7 Rechenschaftspflicht ... 20
3.5 Internationale Übermittlungen ... 21
3.5.1 Safe Harbor und angemessene Länder ... 21
3.5.2 Ausnahmen ... 22
3.5.3 Standardvertragsklauseln ... 23
3.5.4 Verbindliche unternehmensinterne Vorschriften: in Richtung eines globalen Ansatzes ... 23
4. Schlussfolgerungen und Empfehlungen ... 24
4.1 Leitlinien für Anwender und Anbieter von Cloud Computing-Diensten ... 24
4.2 Datenschutz-Zertifizierung durch Dritte ... 27
4.3 Empfehlungen: zukünftige Entwicklungen ... 28
ANHANG ... 30
a) Rollout-Modelle ... 30
b) Servicemodelle ... 31

1. Einleitung

Für Manche stellt das Cloud Computing eine der größten technologischen Revolutionen der letzten Jahre dar. Andere sehen es lediglich als natürliche Weiterentwicklung einer Reihe von Technologien, die dem Wahrwerden des langersehnten Traums des Utility Computing dienen. Auf jeden Fall haben zahlreiche Stakeholder dem Cloud Computing bei der Entwicklung ihrer technologischen Strategien Priorität eingeräumt.

Das Cloud Computing besteht aus einer Reihe von Technologien und Service-Modellen, die sich auf eine internetbasierte Nutzung und Lieferung von IT-Anwendungen, auf die Verarbeitungsfähigkeit, die Aufbewahrung und den Speicherplatz konzentrieren. Das Cloud Computing kann wichtige Wirtschaftsvorteile schaffen, da nach Bedarf bereitgestellte Ressourcen im Internet ziemlich einfach konfiguriert, erweitert und genutzt werden können. Außerdem kann das Cloud Computing Sicherheitsvorteile bieten. Insbesondere kleine bis mittlere Unternehmen können zu geringen Kosten erstklassige Technologien erwerben, die ansonsten außerhalb ihrer finanziellen Möglichkeiten lägen.

Es gibt eine große Bandbreite an Leistungen, die Cloud-Anbieter anbieten. Diese reichen von virtuellen Verarbeitungssystemen (die unter der direkten Kontrolle des für die Verarbeitung Verantwortlichen konventionelle Server ersetzen und/oder parallel zu ihnen arbeiten) über Dienste, die die Anwendungsentwicklung und erweitertes Hosting unterstützen, bis zu webbasierten Softwarelösungen, die Anwendungen ersetzen können, die auf herkömmliche Weise auf den Computern der Endnutzer installiert sind. Dazu gehören Textverarbeitungsanwendungen, Agenden und Kalender, Ablagesysteme für Online-Dokumente, die Speicherung und ausgelagerte E-Mail-Lösungen. Einige der am häufigsten verwendeten Definitionen für diese unterschiedlichen Arten von Diensten sind im Anhang zu dieser Stellungnahme enthalten.

In dieser Stellungnahme analysiert die Artikel-29-Datenschutzgruppe (nachfolgend WP 29) das anzuwendende Recht und die Verpflichtungen der für die Verarbeitung Verantwortlichen, die im Europäischen Wirtschaftsraum (nachfolgend EWR) tätig sind, und der Anbieter von Cloud-Diensten im EWR. Die vorliegende Stellungnahme konzentriert sich auf die Situation, in der angenommen wird, dass eine Beziehung des Typs „für die Verarbeitung Verantwortlicher – Auftragsverarbeiter“ vorliegt, wobei der Anwender als für die Verarbeitung Verantwortlicher und der Cloud-Anbieter als Auftragsverarbeiter klassifiziert wird. In den Fällen, in denen der Cloud-Anbieter auch als für die Verarbeitung Verantwortlicher handelt, muss er zusätzliche Anforderungen erfüllen. Vor der Nutzung von Cloud Computing ist eine durch den für die Verarbeitung Verantwortlichen durchgeführte, angemessene Risikobewertung folglich Voraussetzung. Dabei sind auch die Standorte der Server zu berücksichtigen, auf denen die Daten verarbeitet werden. Außerdem sollte anhand der nachfolgend dargelegten Kriterien eine Abwägung der Vor- und Nachteile aus Sicht des Datenschutzes durchgeführt werden.

Die Stellungnahme bestimmt sowohl für die für die Verarbeitung Verantwortlichen als auch für die Auftragsverarbeiter die im Sinne der allgemeinen Datenschutzrichtlinie (95/46/EG) anzuwendenden Grundsätze wie Zweckbestimmung und Zweckbegrenzung, die Löschung von Daten sowie technische und organisatorische Maßnahmen. Die Stellungnahme bietet Anleitung in Bezug auf die Sicherheitsanforderungen, sowohl als strukturelle als auch als verfahrensrechtliche Garantie. Besondere Betonung wird auf die vertraglichen Vereinbarungen gelegt, die die Beziehung zwischen dem für die Verarbeitung

Verantwortlichen und dem Auftragsverarbeiter in diesem Zusammenhang regeln sollten. Die klassischen Ziele der Datensicherheit sind Verfügbarkeit, Integrität und Vertraulichkeit. Datenschutz ist jedoch nicht auf Datensicherheit beschränkt, und deshalb werden diese Ziele um die spezifischen Datenschutzziele Transparenz, Isolierung, Intervenierbarkeit und Portabilität ergänzt, um das in Artikel 8 der Charta der Grundrechte der Europäischen Union niedergelegte Recht des Einzelnen auf Datenschutz zu stärken.

In Bezug auf die Übermittlung personenbezogener Daten aus dem EWR werden Instrumente wie die von der Europäischen Kommission angenommenen Standardvertragsklauseln, die Bescheinigung eines angemessenen Schutzniveaus und mögliche zukünftige verbindliche unternehmerische Vorschriften sowie die Datenschutzrisiken, die sich aus Ersuchen internationaler Strafverfolgungsbehörden ergeben, analysiert.

Die vorliegende Stellungnahme schließt mit Empfehlungen für Cloud-Anwender als für die Verarbeitung Verantwortliche, für Cloud-Anbieter als Auftragsverarbeiter und für die Europäische Kommission in Bezug auf zukünftige Änderungen im Europäischen Datenschutzrahmen.

Die Berliner Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat im April 2012 das *Sopot Memorandum*[2] angenommen. In diesem Memorandum werden Fragen der Privatsphäre und des Datenschutzes beim Cloud Computing untersucht. Es wird betont, dass Cloud Computing nicht zu niedrigeren Datenschutzstandards als bei der konventionellen Datenverarbeitung führen darf.

2. Datenschutzrisiken des Cloud Computing

Da sich diese Stellungnahme auf die Verarbeitung personenbezogener Daten unter Verwendung des Cloud Computing konzentriert, werden nur die spezifischen Risiken betrachtet, die in diesem Zusammenhang auftreten.[3] Die Mehrheit dieser Risiken fällt in zwei große Kategorien, nämlich die fehlende Kontrolle über die Daten und unzureichende Informationen über die Verarbeitung selbst (fehlende Transparenz). Spezifische, in dieser Stellungnahme berücksichtigte Risiken des Cloud Computing umfassen:

fehlende Kontrolle

Wenn personenbezogene Daten Systemen überlassen werden, die von einem Cloud-Anbieter verwaltet werden, haben Cloud-Anwender möglicherweise nicht mehr länger die ausschließliche Kontrolle über diese Daten und können die technischen und organisatorischen Maßnahmen nicht ergreifen, die zur Sicherstellung der Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Isolierung[4], Intervenierbarkeit und Portabilität der Daten erforderlich sind. Diese fehlende Kontrolle kann sich folgendermaßen manifestieren:

- fehlende Verfügbarkeit aufgrund fehlender Interoperabilität (Vendor Lock-in): Wenn der Cloud-Anbieter eine eigene Technologie verwendet, kann es für den Cloud-

[2] http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

[3] Zusätzlich zu den ausdrücklich in dieser Stellungnahme genannten Risiken, die sich aus der Verarbeitung personenbezogener Daten „in der Wolke“ ergeben, müssen auch alle Risiken berücksichtigt werden, die mit der Auslagerung der Verarbeitung personenbezogener Daten in Verbindung stehen.

[4] In Deutschland wurde das breitere Konzept der „Unverkettbarkeit“ eingeführt. Vgl. die nachfolgende Fußnote 24.

Anwender schwierig sein, Daten und Dokumente zwischen verschiedenen cloudbasierten Systemen zu verschieben (Datenportabilität) oder Informationen mit Stellen auszutauschen, die von anderen Anbietern verwaltete Cloud-Dienste nutzen (Interoperabilität).

- fehlende Integrität durch die gemeinsame Nutzung von Ressourcen: Eine Cloud setzt sich aus gemeinsam genutzten Systemen und Infrastrukturen zusammen. Cloud-Anbieter verarbeiten personenbezogene Daten, die im Hinblick auf die betroffenen Personen und Organisationen aus einer Vielzahl von Quellen stammen. Dabei kann es zu Interessenkollisionen und/oder unterschiedlichen Zielen kommen.
- fehlende Vertraulichkeit in Bezug auf Ersuchen von Strafverfolgungsbehörden, die direkt an den Cloud-Anbieter gerichtet werden: Personenbezogene Daten, die in der Cloud verarbeitet werden, können Gegenstand von Ersuchen von Strafverfolgungsbehörden aus den EU-Mitgliedstaaten und aus Drittländern sein. Es besteht das Risiko, dass personenbezogene Daten einer (fremden) Strafverfolgungsbehörde offengelegt werden, ohne dass hierfür eine geltende Rechtsgrundlage nach dem EU-Recht vorliegt. Dann würde eine Verletzung des EU-Datenschutzrechts vorliegen.
- fehlende Intervenierbarkeit aufgrund der Komplexität und der Dynamik in der Outsourcing-Kette: Der Cloud-Dienst eines Anbieters kann sich aus einer Kombination von Diensten einer Reihe anderer Anbieter zusammensetzen, die im Laufe der Dauer des Vertrags mit dem Kunden dynamisch hinzugefügt oder entfernt werden.
- fehlende Intervenierbarkeit (Rechte der betroffenen Person): Ein Cloud-Anbieter kann möglicherweise nicht die erforderlichen Maßnahmen und Werkzeuge bereitstellen, die den für die Verarbeitung Verantwortlichen bei der Verwaltung der Daten beispielsweise im Hinblick auf den Zugang zu, die Löschung von oder die Berichtigung von Daten unterstützen.
- fehlende Isolierung: Ein Cloud-Anbieter könnte seine physische Kontrolle über die Daten von verschiedenen Anwendern zur Verknüpfung personenbezogener Daten nutzen. Wenn die Administratoren mit ausreichend privilegierten Zugangsrechten (mit hohen Risiken behaftete Funktionen) ausgestattet sind, könnten sie Informationen verschiedener Anwender miteinander verbinden.

fehlende Informationen zur Verarbeitung (Transparenz)

Unzureichende Informationen über die Verarbeitungsprozesse eines Cloud-Dienstes stellen ein Risiko sowohl für den für die Verarbeitung Verantwortlichen als auch für die betroffenen Personen dar, da ihnen möglicherweise die potenziellen Gefahren und Risiken gar nicht bewusst sind und sie folglich auch keine ihnen angemessen erscheinenden Maßnahmen ergreifen können.

Es können sich potenzielle Bedrohungen ergeben, wenn der für die Verarbeitung Verantwortliche nicht weiß, dass

- eine Kettenverarbeitung stattfindet, die zahlreiche Auftragsverarbeiter und Unterauftragnehmer umfasst.
- personenbezogene Daten an verschiedenen geografischen Standorten im EWR verarbeitet werden. Dies wirkt sich direkt auf das Recht aus, das bei Datenschutzstreitigkeiten anzuwenden ist, die sich möglicherweise zwischen dem Anwender und dem Anbieter ergeben.

- personenbezogene Daten in Drittländer außerhalb des EWR übermittelt werden. Drittländer sind möglicherweise nicht dazu in der Lage, ein angemessenes Datenschutzniveau zu bieten und Übermittlungen werden vielleicht nicht durch geeignete Maßnahmen geschützt (z. B. Standardvertragsklauseln oder verbindliche unternehmensinterne Vorschriften), so dass sie illegal sein könnten.

Betroffene Personen, deren personenbezogene Daten in der Cloud verarbeitet werden, müssen über die Identität des für die Verarbeitung Verantwortlichen und den Zweck der Verarbeitung informiert werden (in der Datenschutzrichtlinie 95/46/EG niedergelegte Anforderung für alle für die Verarbeitung Verantwortlichen). Damit gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben gewährleistet wird (Artikel 10 Richtlinie 95/46/EG) und angesichts der potenziellen Komplexität von Verarbeitungsketten in der Cloud Computing-Umgebung sollten für die Verarbeitung Verantwortliche - auch im Sinne einer angemessenen Vorgehensweise - weitere Informationen bezüglich der (Unter-)Auftragsverarbeiter erteilen, die die Cloud-Dienste bereitstellen.

3. Rechtsrahmen

3.1 Datenschutzrahmen

Die Datenschutzrichtlinie 95/46/EG ist der einschlägige Rechtsrahmen. Diese Richtlinie findet in jedem Fall Anwendung, in dem personenbezogene Daten aufgrund einer Nutzung von Cloud Computing-Diensten verarbeitet werden. Die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung) findet auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich verfügbarer elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzwerken Anwendung (Telekom-Betreiber) und ist folglich die einschlägige Richtlinie, wenn solche Dienste mittels einer Cloud-Lösung angeboten werden[5].

3.2 Anwendbares Recht

Die Kriterien zur Festlegung des anwendbaren Rechts sind in Artikel 4 der Richtlinie 95/46/EG niedergelegt, der sich auf das Recht bezieht, das auf die für die Verarbeitung Verantwortlichen anwendbar ist[6], die eine oder mehr Niederlassungen im EWR besitzen oder die außerhalb des EWR niedergelassen sind, aber für die Verarbeitung personenbezogener Daten Ausrüstung verwenden, die sich innerhalb des EWR befindet. Die Artikel-29-Datenschutzgruppe hat dies in ihrer Stellungnahme 8/2010 zum anwendbaren Recht[7] analysiert.

---

5 Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung): Die Richtlinie 2002/58/EG zur Privatsphäre in der Telekommunikation findet auf die Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste Anwendung und verlangt, dass sie die Einhaltung der Verpflichtungen in Bezug auf die Geheimhaltung von Mitteilungen und auf den Schutz personenbezogener Daten sowie der Rechte und Pflichten in Bezug auf elektronische Kommunikationsnetzwerke und -dienste sicherstellen. In Fällen, in denen der Anbieter des Cloud Computing als Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste auftritt, unterliegt er dieser Richtlinie.

6 Der Begriff des für die Verarbeitung Verantwortlichen wird in Artikel 2 Buchstabe h der Richtlinie genannt und wurde von der Artikel-29-Datenschutzgruppe in ihre Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ analysiert.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf

Im ersten Fall wird gemäß Artikel 4 Absatz 1 Buchstabe a der Richtlinie die Anwendung des EU-Rechts auf den für die Verarbeitung Verantwortlichen durch den Standort seiner Niederlassung und durch den Ort der Durchführung seiner Tätigkeit festgelegt, ohne dass hierfür die Art des Cloud-Dienst-Modells von Bedeutung wäre. Es ist das Recht des Landes anwendbar, in dem der für die Verarbeitung Verantwortliche seine Niederlassung hat, der den Vertrag über die Cloud Computing-Dienste geschlossen hat und nicht der Ort, an dem der Anbieter des Cloud Computing seinen Sitz hat.

Sollte der für die Verarbeitung Verantwortliche Niederlassungen in mehreren Mitgliedstaaten haben und die Daten als Teil seiner Tätigkeit in diesen Ländern verarbeiten, ist jeweils das Recht jedes Mitgliedstaats anzuwenden, in dem die Verarbeitung stattfindet.

Artikel 4 Absatz 1 Buchstabe c[8] bezieht sich darauf, wie die Datenschutzbestimmungen auf für die Verarbeitung Verantwortliche anzuwenden sind, die nicht im EWR niedergelassen sind, aber automatisierte oder nicht automatisierte Mittel einsetzen, die sich im Hoheitsgebiet des Mitgliedstaates befinden, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr genutzt werden. Das heißt, dass wenn ein Cloud-Anwender, der außerhalb des EWR niedergelassen ist, aber einen innerhalb des EWR niedergelassenen Cloud-Anbieter beauftragt, dieser Anbieter die Datenschutzbestimmungen zum Anwender exportiert.

3.3 Pflichten und Verantwortlichkeiten der verschiedenen Beteiligten

Wie bereits gesagt, betrifft Cloud Computing eine Reihe verschiedener Beteiligter. Es ist wichtig, die Rolle jedes dieser Beteiligten zu bewerten und zu klären, um so ihre spezifischen Verpflichtungen in Bezug auf die aktuellen Datenschutzbestimmungen festzulegen.

Es sollte daran erinnert werden, dass die WP 29 in ihrer Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ darauf hingewiesen hat, dass *„der Begriff „für die Verarbeitung Verantwortlicher“ in erster Linie dazu dient, zu bestimmen, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und wie die betroffenen Personen ihre Rechte in der Praxis ausüben können. Anders ausgedrückt: Er dient dazu, Verantwortung zuzuweisen.“* Die von der vorliegenden Analyse betroffenen Personen sollten diese beiden allgemeinen Kriterien für die Einhaltung und die Zuweisung von Verantwortung im Hinterkopf behalten.

3.3.1 Cloud-Anwender und Cloud-Anbieter

Der Cloud-Anwender legt den letztendlichen Zweck der Verarbeitung fest und entscheidet über die Auslagerung dieser Verarbeitung und die Delegierung von allen oder Teilen der Verarbeitungstätigkeiten an eine externe Organisation. Folglich fungiert der Cloud-Anwender als für die Datenverarbeitung Verantwortlicher. Die Richtlinie legt fest, dass der für die Verarbeitung Verantwortliche als *„natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, […] allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“* Der Cloud-Anwender als für

[8] Artikel 4 Absatz 1 Buchstabe c legt fest, dass das Recht eines Mitgliedstaats anwendbar ist, wenn der „für die Verarbeitung Verantwortliche [...] nicht im Gebiet der Gemeinschaft niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.“

die Verarbeitung Verantwortlicher muss die Verantwortung für die Einhaltung der Datenschutzbestimmungen übernehmen. Er ist verantwortlich und unterliegt allen rechtlichen Verpflichtungen, die in der Richtlinie 95/46/EG angesprochen werden. Der Cloud-Anwender kann den Cloud-Anbieter damit beauftragen, die Methoden und die technischen oder organisatorischen Maßnahmen für das Erreichen der Zwecke des für die Verarbeitung Verantwortlichen auszuwählen.

Der Cloud-Anbieter ist die juristische Person, die die Cloud Computing-Dienste in den verschiedenen, vorstehend diskutierten Formen bereitstellt. Wenn der Cloud-Anbieter die Mittel und die Plattform bereitstellt und dabei im Auftrag des Cloud-Anwenders handelt, wird er als Auftragsverarbeiter angesehen, das heißt er ist nach der Richtlinie 95/46/EG *„die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet“*.[9] [10]

Wie in der Stellungnahme 1/2010 festgestellt wurde, können manche Kriterien[11] genutzt werden, um zu bewerten, wer für die Verarbeitung verantwortlich ist. Tatsächlich kann es Situationen geben, in denen ein Anbieter von Cloud-Diensten je nach den jeweiligen Umständen entweder als gemeinsamer oder als eigenständiger für die Verarbeitung Verantwortlicher betrachtet werden kann. Das könnte beispielsweise der Fall sein, wenn der Anbieter Daten für seine eigenen Zwecke verarbeitet.

Es sollte betont werden, dass auch in komplexen Datenverarbeitungsumgebungen, in denen verschiedene für die Verarbeitung Verantwortliche bei der Verarbeitung personenbezogener Daten eine Rolle spielen, die Datenschutzbestimmungen eingehalten werden müssen. Auch die Verantwortung für eine mögliche Verletzung dieser Bestimmungen muss klar zugewiesen sein, um zu vermeiden, dass der Schutz personenbezogener Daten reduziert wird oder dass „negative Zuständigkeitskonflikte“ und Lücken auftreten und dadurch einige Verpflichtungen und Rechte aus der Richtlinie durch eine der Parteien nicht gewährleistet werden.

Im aktuellen Cloud Computing-Szenario haben die Anwender von Cloud Computing-Diensten vielleicht nicht die Möglichkeit, die Vertragsbedingungen für die Nutzung der Cloud-Dienste auszuhandeln, da diese häufig Gegenstand standardisierter Angebote sind. Dennoch ist es letztendlich der Anwender, der für bestimmte Zwecke über die Zuweisung eines Teils oder aller Verarbeitungsschritte an Cloud-Dienste entscheidet. Die Rolle des Anbieters gegenüber dem Anwender ist die eines Auftragnehmers. In diesem Fall ist das der entscheidende Punkt. Wie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 1/2010[12] zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ festgestellt hat *„darf das Ungleichgewicht in der Vertragsposition zwischen einem kleinen für die Verarbeitung Verantwortlichen und großen Dienstleistern nicht als Rechtfertigung dafür gelten, dass der für die Verarbeitung Verantwortliche Vertragsklauseln und -bedingungen akzeptiert, die gegen das Datenschutzrecht verstoßen.“* Aus diesem Grund muss der für die

---

9 Diese Stellungnahme konzentriert sich lediglich auf die normale Beziehung „für die Verarbeitung Verantwortlicher – Auftragsverarbeiter“.

10 Die Cloud Computing-Umgebung kann auch von natürlichen Personen (Nutzern) verwendet werden, um ausschließlich persönliche oder heimische Tätigkeiten durchzuführen. In dem Fall muss gründlich analysiert werden, ob die sogenannte Ausnahmeklausel für Privathaushalte Anwendung findet, nach der Nutzer keine für die Verarbeitung Verantwortlichen sein können. Diese Frage geht jedoch über den Zweck dieser Stellungnahme hinaus.

11 Z.B. Weisungsebene, Überwachung durch den Cloud-Anwender, Kenntnisse der Parteien.

12 Stellungnahme 01/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

Verarbeitung Verantwortliche einen Cloud-Anbieter auswählen, der die Einhaltung der Datenschutzbestimmungen garantiert. Besondere Betonung muss auf die Bestandteile der anzuwendenden Verträge gerichtet werden. Diese haben einen Satz standardisierter Datenschutzgarantien zu enthalten, die die Garantien umfassen müssen, welche die Datenschutzgruppe in Abschnitt 3.4.3 (Technische und organisatorische Maßnahmen) und in Abschnitt 3.5 (Grenzüberschreitende Datenflüsse) dargelegt hat - sowie etwaige zusätzliche Mechanismen, die sich als eine Vereinfachung in Bezug auf die gebührende Sorgfalt und Rechenschaftspflicht herausstellen können (wie unabhängige Prüfungen durch Dritte und Zertifizierungen der Leistungen des Anbieters - siehe Abschnitt 4.2).

Cloud-Anbieter sind (als Auftragsverarbeiter) zur Sicherstellung der Vertraulichkeit verpflichtet. Richtlinie 95/46 EC stellt Folgendes fest: *„Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind und Zugang zu personenbezogenen Daten haben, sowie der Auftragsverarbeiter selbst dürfen personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten, es sei denn, es bestehen gesetzliche Verpflichtungen.“* Der Zugang des Cloud-Anbieters zu den Daten während der Dienstebereitstellung ist ebenfalls im Wesentlichen durch die Anforderung geregelt, die Bestimmungen von Artikel 17 der Richtlinie einzuhalten - siehe Abschnitt 3.4.2.

Auftragsverarbeiter müssen die Art der betreffenden Cloud berücksichtigen (Public, Private, Community oder Hybrid / IaaS, SaaS oder PaaS [siehe Anhang a) Rollout-Modelle - b) Modelle der Diensteerbringung]) und die Art Dienst, für den der Anwender einen Vertrag abgeschlossen hat. Die Auftragsverarbeiter sind dafür verantwortlich, Sicherheitsmaßnahmen zu ergreifen, die den EU-Bestimmungen entsprechen, in deren Anwendungsbereich der für die Verarbeitung Verantwortliche und Auftragsverarbeiter fallen. Auftragsverarbeiter müssen den für die Verarbeitung Verantwortlichen auch bei der Einhaltung der (ausgeübten) Rechte der betroffenen Personen unterstützen.

3.3.2 Unterauftragnehmer

Cloud Computing-Dienste können die Beteiligung einer Reihe von Vertragsparteien mit sich bringen, die als Auftragsverarbeiter fungieren. Auftragsverarbeiter schließen häufig Unterverträge mit zusätzlichen Unterauftragsverarbeitern, die dann Zugang zu personenbezogenen Daten erhalten. Wenn ein Auftragsverarbeiter Dienste an Unterauftragsverarbeiter weitervergibt, muss der Anwender darüber informiert werden. Dabei müssen die Art des weitervergebenen Dienstes und die Kenndaten aktueller oder potenzieller Unterauftragnehmer angegeben werden. Außerdem muss garantiert werden, dass diese dem Anbieter der Cloud Computing-Dienste anbieten, die Richtlinie 95/46/EG einzuhalten.

Alle einschlägigen Verpflichtungen müssen folglich durch Verträge zwischen dem Cloud-Anbieter und dem Unterauftragnehmer auch für Unterauftragsverarbeiter gelten. Diese Verträge sollten die vertraglichen Vereinbarungen zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegeln. In ihrer Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ hat die Artikel-29-Datenschutzgruppe auf die Vielzahl von Auftragsverarbeitern hingewiesen, die in einer direkten Beziehung zu dem für die Verarbeitung Verantwortlichen stehen können oder die Unterauftragnehmer sein können, an die die Auftragsverarbeiter einen Teil der ihnen anvertrauten Verarbeitungstätigkeiten ausgelagert haben. *„In der Richtlinie spricht nichts dagegen, dass durch Aufteilung der betreffenden Aufgaben aufgrund organisatorischer Anforderungen mehrere Organisationen zu Auftragsverarbeitern oder (Unter-)*

Auftragsverarbeitern bestimmt werden. Bei der Durchführung der Verarbeitung müssen jedoch alle diese Auftragsverarbeiter die Weisungen des für die Verarbeitung Verantwortlichen befolgen.“[13]

Bei solchen Szenarien sollten die sich aus den Datenschutzbestimmungen ergebenden Verpflichtungen und Verantwortlichkeiten klar zugewiesen sein und nicht entlang der Kette von Auslagerungen oder der Vergabe von Unterverträgen gestreut werden, damit eine wirksame Kontrolle sichergestellt und eine klare Verantwortung für die Verarbeitungstätigkeiten zugewiesen wird.

Ein mögliches Muster der Zusicherungen, das zur Klärung der Pflichten und Verpflichtungen von Auftragsverarbeitern genutzt werden kann, wenn sie die Datenverarbeitung weitervergeben, wurde zuerst im Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern[14] eingeführt. Nach diesem Muster ist eine Vergabe von Unteraufträgen nur mit der vorherigen schriftlichen Einwilligung des für die Verarbeitung Verantwortlichen und mit einer schriftlichen Vereinbarung möglich, welche dem Unterauftragsverarbeiter dieselben Verpflichtungen auferlegt, die der Auftragsverarbeiter hat. Erfüllt der Unterauftragsverarbeiter seine Datenschutzverpflichtungen aus einer solchen schriftlichen Vereinbarung nicht, bleibt der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für die Erfüllung der Verpflichtungen des Unterauftragsverarbeiters aus einer solchen Vereinbarung uneingeschränkt haftbar. Eine Bestimmung dieser Art könnte in jeder Vertragsklausel zwischen einem für die Verarbeitung Verantwortlichen und einem Cloud-Diensteanbieter verwendet werden, wenn der letztgenannte die Dienste durch die Vergabe von Unteraufträgen bereitstellen möchte. So können die erforderlichen Garantien für die Vergabe von Unteraufträgen sichergestellt werden.

Eine ähnliche Lösung bezüglich der Zusicherungen im Lauf einer Vergabe von Unteraufträgen wurde kürzlich von der Kommission in dem Vorschlag für eine Datenschutz-Grundverordnung[15] gemacht. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem unter anderem insbesondere vorgesehen ist, dass der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters nur mit vorheriger Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch nehmen darf (Artikel 26 Absatz 2 des Vorschlags).

Nach Ansicht der WP29 kann der Auftragsverarbeiter seine Tätigkeiten nur auf der Grundlage der Einwilligung des für die Verarbeitung Verantwortlichen weitervergeben. Diese Einwilligung kann bei Beginn der Bereitstellung der Dienste generell erteilt werden[16]. Der Auftragsverarbeiter ist eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über beabsichtigte Änderungen in Bezug auf weitere Unterauftragnehmer oder den Ersatz von Unterauftragnehmern zu informieren. Der für die Verarbeitung Verantwortliche hat jederzeit die Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, alle beauftragten Unterauftragnehmer

---

[13] Vgl. WP169, S. 29, Stellungnahme 01/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

[14] Siehe FAQ II.5 in WP176.

[15] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 25.1.2012.

[16] Siehe FAQ II.1 in WP176, angenommen am 12. Juli 2010.

zu nennen. Darüber hinaus sollte zwischen dem Cloud-Anbieter und dem Unterauftragnehmer ein Vertrag geschlossen werden, der die Vertragsbedingungen zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegelt. Der für die Verarbeitung Verantwortliche sollte im Fall von Vertragsverletzungen durch die Unterauftragsverarbeiter vertragliche Rückgriffsmöglichkeiten in Anspruch nehmen können. Hierzu könnte sichergestellt werden, dass der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für alle Vertragsverletzungen direkt haftbar ist, die von einem von ihm beauftragten Unterauftragsverarbeiter begangen werden. Eine weitere Möglichkeit wäre die Schaffung des Rechts als Drittbegünstigter zugunsten des für die Verarbeitung Verantwortlichen in allen Verträgen, die zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter unterzeichnet werden. Eine weitere Möglichkeit stellt auch die Tatsache dar, dass diese Aufträge im Auftrag des für die Datenverarbeitung Verantwortlichen unterzeichnet werden, so dass dieser Vertragspartei wird.

3.4 Datenschutzanforderungen in dem Verhältnis Anwender-Anbieter

3.4.1 Einhaltung der Grundprinzipien

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in der Cloud hängt von der Einhaltung der Grundprinzipien der Datenschutzbestimmungen der EU ab: Gegenüber der betroffenen Person muss Transparenz garantiert sein, der Grundsatz der Zweckbestimmung und Zweckbegrenzung muss eingehalten werden und personenbezogene Daten sind zu löschen, sobald ihre Aufbewahrung nicht mehr länger erforderlich ist. Darüber hinaus müssen geeignete technische und organisatorische Maßnahmen umgesetzt werden, um ein angemessenen Niveau des Datenschutzes und der Datensicherheit zu gewährleisten.

3.4.1.1 Transparenz

Transparenz ist eine grundlegende Voraussetzung dafür, dass personenbezogene Daten nach Treu und Glauben und rechtmäßig verarbeitet werden. Richtlinie 95/46/EG verpflichtet den Cloud-Anwender dazu, der betroffenen Person, bei der die sie betreffenden Daten erhoben werden, seine Identität und die Zweckbestimmung der Verarbeitung mitzuteilen. Der Cloud-Anwender sollte auch weitere Informationen beispielsweise betreffend die Empfänger oder Kategorien der Empfänger der Daten erteilen, die auch Auftragsverarbeiter und Unterauftragsverarbeiter umfassen können, sofern diese Informationen notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten (vgl. Artikel 10 der Richtlinie)[17].

Transparenz muss auch in der (den) Beziehung(en) zwischen dem Cloud-Anwender, dem Cloud-Anbieter und den Unterauftragnehmern (sofern vorhanden) sichergestellt werden. Der Cloud-Anwender kann die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in der Cloud nur dann prüfen, wenn ihn der Anbieter über alle einschlägigen Fragen informiert. Ein für die Verarbeitung Verantwortlicher, der in Erwägung zieht, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen, sollte die Geschäftsbedingungen des Cloud-Anbieters sorgfältig prüfen und sie von einem datenschutzrechtlichen Standpunkt aus bewerten.

Transparenz in der Cloud bedeutet, dass es erforderlich ist, den Cloud-Anwender über alle Unterauftragnehmer zu informieren, die zur Bereitstellung der entsprechenden Cloud-Dienste

[17] Eine ähnliche Informationspflicht gegenüber der betroffenen Person besteht, wenn Daten, die nicht bei der betroffenen Person erhoben wurden, sondern aus einer anderen Quelle stammen, aufgezeichnet oder an Dritte weitergegeben werden (vgl. Artikel 11).

beitragen sowie über alle Standorte der Datenzentren, an denen personenbezogene Daten verarbeitet werden können.[18]

Erfordert die Bereitstellung der Dienste die Installation von Software auf dem System des Cloud-Anwenders (z.B. Browser Plug-ins), sollte der Cloud-Anbieter den Kunden im Rahmen einer angemessenen Vorgehensweise über diesen Umstand informieren und insbesondere über die Konsequenzen aus der Sicht des Datenschutzes und der Datensicherheit. Entsprechend sollte der Cloud-Anwender dieses Thema vorab ansprechen, wenn es von dem Cloud-Anbieter nicht in ausreichendem Maß behandelt wird.

3.4.1.2 Zweckbestimmung und -begrenzung

Der Grundsatz der Zweckbestimmung und -begrenzung sieht vor, dass personenbezogene Daten für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden (vgl. Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG). Der Cloud-Anwender muss den (die) Zweck(e) der Verarbeitung festlegen, bevor er personenbezogene Daten von der betroffenen Person erhebt und diese darüber informieren. Er darf personenbezogene Daten nicht für andere Zwecke verarbeiten, die nicht mit den ursprünglichen Zwecken vereinbar sind.

Außerdem muss sichergestellt werden, dass personenbezogene Daten nicht (gesetzeswidrig) für weitere Zwecke von dem Cloud-Anbieter oder von einem seiner Unterauftragnehmer verarbeitet werden. Da ein typisches Cloud-Szenario leicht eine größere Anzahl an Unterauftragnehmern umfassen kann, muss das Risiko einer Verarbeitung personenbezogener Daten für weitere, nicht vereinbarte Zwecke als recht hoch angesehen werden. Zur Minimierung dieses Risikos sollte der Vertrag zwischen dem Cloud-Anbieter und dem Cloud-Anwender technische und organisatorische Maßnahmen zur Eindämmung dieses Risikos umfassen und Sicherungen für das Protokollieren und die Kontrolle der einschlägigen Verarbeitungen personenbezogener Daten enthalten, die von Angestellten des Cloud-Anbieters oder der Unterauftragnehmer durchgeführt werden.[19] Der Vertrag sollte bei einer Verletzung der Datenschutzbestimmungen Vertragsstrafen gegen den Anbieter oder den Unterauftragnehmer vorsehen.

3.4.1.3 Löschung von Daten

Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG sieht vor, dass personenbezogene Daten nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht. Personenbezogene Daten, die nicht länger benötigt werden, müssen gelöscht oder wirklich anonymisiert werden. Wenn solche Daten aufgrund gesetzlicher Aufbewahrungsbestimmungen (z.B. Steuerbestimmungen) nicht gelöscht werden können, sollte der Zugang zu diesen personenbezogenen Daten gesperrt werden. Es obliegt der Verantwortung des Cloud-Anwenders, sicherzustellen, dass

---

[18] Nur dann kann er beurteilen, ob personenbezogene Daten an ein sogenanntes Drittland außerhalb des Europäischen Wirtschaftsraums (EWR) übermittelt werden können, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG sicherstellt. Vgl. auch den nachstehenden Abschnitt 3.4.6.

[19] Vgl. den nachstehenden Abschnitt 3.4.3.

personenbezogene Daten gelöscht werden, sobald sie nicht mehr in dem vorgenannten Sinn erforderlich sind[20].

Der Grundsatz der Löschung der Daten gilt für personenbezogene Daten unabhängig davon, ob sie auf der Festplatte oder auf einem anderen Speichermedium (z.B. Backup-Bänder) gespeichert sind. Da personenbezogene Daten möglicherweise zusätzlich auf verschiedenen Servern an unterschiedlichen Orten gespeichert sind, muss sichergestellt werden, dass alle gespeicherten Daten unwiderruflich gelöscht werden (d. h. es müssen auch vorherige Versionen, temporäre Dateien und selbst Dateifragmente gelöscht werden).

Es muss Cloud-Anwendern bewusst sein, dass Logdaten[21], die die Überprüfbarkeit beispielsweise der Speicherung, einer Änderung oder Löschung von Daten vereinfachen, auch als personenbezogene Daten der Person gelten können, die die entsprechende Verarbeitung eingeleitet hat.[22]

Eine sichere Löschung personenbezogener Daten erfordert, dass das Speichermedium entweder zerstört oder entmagnetisiert wird oder dass die personenbezogenen Daten durch Überschreiben wirkungsvoll gelöscht werden. Für das Überschreiben personenbezogener Daten sollte eine spezielle Software verwendet werden, die Daten entsprechend einem anerkannten Verfahren vielfach überschreibt.

Der Cloud-Anwender sollte sicherstellen, dass der Cloud-Anbieter eine sichere Löschung im vorgenannten Sinne garantiert und dass der Vertrag zwischen dem Anbieter und dem Anwender eindeutige Bestimmungen zur Löschung personenbezogener Daten enthält[23]. Das gilt auch für Verträge zwischen Cloud-Anbietern und Unterauftragnehmern.

3.4.2 Vertragliche Absicherungsklauseln der Beziehung(en) „für die Verarbeitung Verantwortlicher“ - „Auftragsverarbeiter“

Der für die Verarbeitung Verantwortliche hat im Fall einer Verarbeitung in seinem Auftrag einen Auftragsverarbeiter auszuwählen, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet; der für die Verarbeitung Verantwortliche überzeugt sich von der Einhaltung dieser Maßnahmen (Artikel 17 Absatz 2 der Richtlinie 95/46/EG). Artikel 17 Absatz 3 der Richtlinie 95/46/EG legt außerdem fest, dass sie rechtlich dazu verpflichtet sind, einen förmlichen Vertrag mit dem Cloud-Anbieter zu unterzeichnen. Dieser Artikel legt die Anforderung fest, dass ein Vertrag oder Rechtsakt die Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter regelt. Zum Zwecke der Beweissicherung sind die datenschutzrelevanten Elemente des Vertrags oder Rechtsakts und die Anforderungen in Bezug auf technische Maßnahmen und organisatorische Vorkehrungen schriftlich oder in einer anderen Form zu dokumentieren.

In dem Vertrag muss insbesondere mindestens festgelegt werden, dass der Auftragsverarbeiter auf Weisung des für die Verarbeitung Verantwortlichen handeln muss und dass er technische und organisatorische Maßnahmen für einen angemessenen Schutz der personenbezogenen Daten zu ergreifen hat.

---

[20] Die Löschung von Daten spielt sowohl während der Laufzeit des Cloud Computing-Vertrags, als auch nach Beendigung des Vertrags eine Rolle. Sie ist auch im Fall des Austauschs oder der Streichung eines Unterauftragnehmers von Bedeutung.

[21] Anmerkungen zu den Anforderungen an das Protokollieren folgen unter 4.3.4.2.

[22] Das heißt, dass angemessene Aufbewahrungsfirsten für Logdateien festgelegt werden müssen und dass Prozesse vorhanden sein müssen, welche die rechtzeitige Löschung oder Anonymisierung dieser Daten sicherstellen.

[23] Vgl. den nachstehenden Abschnitt 3.4.3.

Zur Sicherstellung der Rechtssicherheit sollte der Vertrag Folgendes enthalten:

1. detaillierte Angaben zu den Anweisungen des Anwenders (Ausmaß und Modalitäten), die dem Anbieter zu übermitteln sind, insbesondere bezüglich der anzuwendenden Dienstgütevereinbarungen (die objektiv und messbar sein sollten) und der entsprechenden Strafen (finanzieller oder sonstiger Natur, einschließlich der Möglichkeit, den Anbieter im Fall der Nichteinhaltung verklagen zu können).
2. Darlegung der Sicherheitsmaßnahmen, die der Cloud-Anbieter abhängig von den Risiken einhalten muss, die durch die Verarbeitung und die Natur der zu schützenden Daten bestimmt werden. Es ist sehr wichtig, dass konkrete technische und organisatorische Maßnahmen spezifiziert werden, beispielsweise wie die im nachfolgenden Abschnitt 3.4.3 aufgeführten. Dies gilt unbeschadet der Anwendung möglicherweise strengerer Maßnahmen, die nach dem innerstaatlichen Recht des Anwenders vorgesehen sind.
3. Gegenstand und Zeitrahmen des durch den Cloud-Anbieter zu erbringenden Cloud-Dienstes, Umfang, Art und Zweck der Verarbeitung der personenbezogenen Daten durch den Cloud-Anbieter sowie die Arten der personenbezogenen Daten, die verarbeitet werden.
4. Spezifizierung der Bedingungen für die Rückgabe der (personenbezogenen) Daten oder für die Zerstörung der Daten bei Beendigung der Diensteerbringung. Darüber hinaus muss sichergestellt werden, dass die personenbezogenen Daten auf Antrag des Cloud-Anwenders zuverlässig gelöscht werden.
5. Einschluss einer Vertraulichkeitsklausel, die sowohl für den Cloud-Anbieter als auch für alle seine Angestellten verbindlich ist, die Zugang zu den Daten haben. Ausschließlich autorisierte Personen dürfen Zugang zu den Daten haben.
6. Verpflichtung von Seiten des Anbieters, den Anwender zu unterstützen, so dass die betroffenen Personen ihre Rechte auf Zugang, Berichtigung und Löschung ihrer Daten leichter ausüben können.
7. In dem Vertrag sollte ausdrücklich festgelegt werden, dass der Cloud-Anbieter die Daten keinem Dritten mitteilen darf - auch nicht zu Zwecken der Aufbewahrung - sofern die Hinzuziehung von Unterauftragnehmern nicht vertraglich geregelt ist. Der Vertrag sollte festlegen, dass Unterauftragsverarbeiter ausschließlich auf der Grundlage einer Einwilligung beauftragt werden dürfen, die der für die Verarbeitung Verantwortliche generell erteilen kann. Der Auftragsverarbeiter ist eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über beabsichtigte diesbezügliche Änderungen zu informieren. Der für die Verarbeitung Verantwortliche hat dabei jederzeit die Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, alle beauftragten Unterauftragnehmer zu nennen (z. B. in einem öffentlichen digitalen Register). Es muss sichergestellt werden, dass Verträge zwischen dem Cloud-Anbieter und dem Unterauftragnehmer die Bestimmungen des Vertrags zwischen dem Cloud-Anwender und dem Cloud-Anbieter widerspiegeln (d. h., dass Unterauftragsverarbeiter denselben vertraglichen Verpflichtungen unterliegen wie der Cloud-Anbieter). Es muss insbesondere garantiert werden, dass sowohl der Cloud-Anbieter als auch alle Unterauftragnehmer ausschließlich auf Weisung des Cloud-Anwenders handeln. Wie in dem Abschnitt über die Vergabe von Unteraufträgen erklärt wurde, sollte die Haftungskette in dem Vertrag klar festgelegt werden. Der Vertrag sollte den Auftragsverarbeiter verpflichten, internationalen Übermittlungen einen Rahmen zu geben, beispielsweise durch die Unterzeichnung von Verträgen mit

den Unterauftragsverarbeitern, die auf den Standardvertragsklauseln aus 2010/87/EU basieren.

8. Klarstellung der Verantwortung des Cloud-Anbieters auf Benachrichtigung des Cloud-Anwenders im Falle einer Datenschutzverletzung, welche die Daten des Cloud-Anwenders betrifft.
9. Verpflichtung des Cloud-Anbieters, eine Liste der Standorte bereitzustellen, an denen die Daten möglicherweise verarbeitet werden.
10. Das Recht des für die Verarbeitung Verantwortlichen auf Überwachung und die entsprechende Pflicht des Cloud-Anbieters zur Zusammenarbeit.
11. Es sollte vertraglich festgelegt werden, dass der Cloud-Anbieter dazu verpflichtet ist, den Anwender über einschlägige Änderungen bei den jeweiligen Cloud-Diensten zu informieren, wie beispielsweise über die Implementierung zusätzlicher Funktionen.
12. Der Vertrag sollte die Protokollierung und Prüfung der relevanten Verarbeitungstätigkeiten an personenbezogenen Daten festlegen, die durch den Cloud-Anbieter oder die Unterauftragnehmer durchgeführt werden.
13. Benachrichtigung des Cloud-Anwenders über alle rechtlich verbindlichen Ersuchen einer Strafverfolgungsbehörde auf Weitergabe der personenbezogenen Daten, es sei denn, dies wäre anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen.
14. eine generelle Verpflichtung des Anbieters zur Zusicherung, dass seine interne Organisation und seine Maßnahmen zur Datenverarbeitung (und die seiner Unterauftragsverarbeiter, sofern vorhanden) die anzuwendenden nationalen und internationalen rechtlichen Anforderungen und Standards einhalten.

Im Falle einer Verletzung durch den für die Verarbeitung Verantwortlichen hat jede Person, die aufgrund der unrechtmäßigen Verletzung einen Schaden erlitten hat, das Recht auf Begleichung der verursachten Schäden durch den für die Verarbeitung Verantwortlichen. Sollte der Auftragsverarbeiter die Daten für einen anderen Zweck nutzen oder sie verbreiten oder auf eine vertragsverletzende Weise nutzen, wird er auch als für die Verarbeitung Verantwortlicher angesehen und ist für die Vertragsverletzungen haftbar, in die er persönlich verwickelt war.

Es sollte angemerkt werden, dass Anbieter von Cloud-Diensten in vielen Fällen Standarddienste und von den für die Verarbeitung Verantwortlichen zu unterzeichnende Standardverträge anbieten, die ein Standardformat für die Verarbeitung personenbezogener Daten festlegen. Das Ungleichgewicht in der Vertragsposition zwischen einem kleinen für die Verarbeitung Verantwortlichen und großen Dienstleistern darf nicht als Rechtfertigung dafür gelten, dass für die Verarbeitung Verantwortliche Vertragsklauseln und -bedingungen akzeptieren, die gegen das Datenschutzrecht verstoßen.

3.4.3 Technische und organisatorische Maßnahmen des Datenschutzes und der Datensicherheit

Artikel 17 Absatz 2 der Richtlinie 95/46/EG macht den Cloud-Anwender (der als für die Datenverarbeitung Verantwortlicher handelt) allein verantwortlich für die Wahl von Cloud-Anbietern, die hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bieten und Rechenschaft ablegen können.

Zusätzlich zu den wichtigsten Sicherheitszielen der Verfügbarkeit, Vertraulichkeit und Integrität muss die Aufmerksamkeit auch auf die zusätzlichen Datenschutzziele der Transparenz (siehe vorstehenden Punkt 3.4.1.1) Isolierung[24], Intervenierbarkeit, Rechenschaft und Portabilität gerichtet werden. Dieser Abschnitt richtet das Augenmerk unbeschadet zusätzlicher sicherheitsorientierter Risikoanalysen[25] auf diese zentralen Datenschutzziele.

3.4.3.1 Verfügbarkeit

Die Bereitstellung von Verfügbarkeit bedeutet, den zeitnahen und zuverlässigen Zugang zu personenbezogenen Daten sicherzustellen.

Eine große Gefahr für die Verfügbarkeit in der Cloud ist der versehentliche Verlust der Netzwerkverbindung zwischen dem Kunden und dem Anbieter der Serverleistung durch böswillige Handlungen wie (Distributed) Denial of Service (DoS) [26] -Angriffe. Zu den weiteren Verfügbarkeitsrisiken zählen versehentliche Hardware-Ausfälle sowohl im Netzwerk als auch in den Verarbeitungs- und Speichersystemen der Cloud, Stromausfälle und sonstige Infrastrukturprobleme.

Für die Datenverarbeitung Verantwortliche sollten prüfen, ob der Cloud-Anbieter angemessene Maßnahmen ergriffen hat, um dem Risiko der Störungen zu begegnen. Zu diesen Maßnahmen zählen unter anderem Backup-Internet-Netzwerkverbindungen, redundante Speicherung und wirksame Mechanismen zum Daten-Backup.

3.4.3.2 Integrität

Integrität kann definiert werden als Eigenschaft, dass die Daten authentisch sind und nicht böswillig oder versehentlich während der Verarbeitung, Aufbewahrung oder Übermittlung geändert wurden. Der Begriff der Integrität kann auf IT-Systeme ausgeweitet werden und erfordert, dass die Verarbeitung personenbezogener Daten auf diesen Systemen unverändert bleibt.

Änderungen an personenbezogenen Daten können durch Mechanismen der kryptografischen Authentifizierung wie Message Authentication Codes oder Signaturen entdeckt werden.

Störungen der Integrität von IT-Systemen in der Cloud können mit Hilfe von Intrusion Detection und Intrusion Prevention Systemen (IDS / IPS) entdeckt bzw. verhindert werden. Das ist besonders bei der Art offener Netzwerkumgebung erforderlich, in der Clouds normalerweise betrieben werden.

3.4.3.3 Vertraulichkeit

Korrekt ausgeführt kann die Verschlüsselung in der Cloud-Umgebung maßgeblich zur Vertraulichkeit personenbezogener Daten beitragen, auch wenn sie personenbezogene Daten nicht unwiderruflich anonymisiert[27]. Personenbezogene Daten sollten während des „Transits“

---

[24] In Deutschland wurde der breitere Begriff der „Unverkettbarkeit“ in das Recht eingeführt und wird von der Konferenz der Datenschutzbeauftragten unterstützt.

[25] Vgl. z. B. ENISA unter http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] Ein DoS-Angriff ist ein koordinierter Versuch, die Verfügbarkeit eines Computers oder einer Netzwerkressource für die autorisierten Nutzer entweder vorübergehend oder dauerhaft zu unterbinden (z. B. mittels einer großen Anzahl von angreifenden Systemen, die ihr Ziel mit einer Vielzahl von externen Kommunikationsanforderungen blockieren).

[27] Richtlinie 95/46/EG - Erwägungsgrund 26: „(...) Die Schutzprinzipien finden keine Anwendung auf Daten, die derart anonymisiert sind, dass die betroffene Person nicht mehr identifizierbar ist. (...)“ Gleichermaßen führen die technischen Datenfragmentierungsprozesse, die im Rahmen der Bestimmungen von Cloud

immer verschlüsselt sein und „ruhende Daten“ sofern möglich.[28] In einigen Fällen (z. B. in einem IaaS Speicherdienst) kann sich ein Cloud-Anwender möglicherweise nicht auf die Verschlüsselungslösung verlassen, die der Cloud-Anbieter anbietet, sondern wird sich eventuell entscheiden, personenbezogene Daten zu verschlüsseln, bevor er sie in die Cloud sendet. Werden ruhende Daten verschlüsselt, muss besondere Aufmerksamkeit auf die Verwaltung der kryptografischen Schlüssel gerichtet werden, da die Datensicherheit dann letztendlich von der Vertraulichkeit der Schlüssel für die Verschlüsselung abhängt.

Mitteilungen zwischen dem Cloud-Anbieter und dem Anwender sowie zwischen den Datenzentren sollten verschlüsselt werden. Die Fernverwaltung der Cloud-Plattform sollte nur über sichere Kommunikationskanäle erfolgen. Wenn ein Anwender nicht nur die Aufbewahrung, sondern auch die weitere Verarbeitung personenbezogener Daten in der Cloud plant (z. B. Suchdatenbanken für Datensätze), muss er daran denken, dass die Verschlüsselung während der Verarbeitung der Daten nicht aufrecht erhalten werden kann (mit Ausnahme sehr spezieller Berechnungsmethoden).

Weitere technische Maßnahmen zur Sicherstellung der Vertraulichkeit umfassen Autorisierungsmechanismen und die sichere Authentifizierung (z. B. Zwei-Faktor-Authentifizierung). Die Vertragsklauseln sollten auch den Angestellten von Cloud-Anwendern, Cloud-Anbietern und Unterauftragnehmern die Verpflichtung zur Vertraulichkeit auferlegen.

3.4.3.4 Transparenz

Die technischen und organisatorischen Maßnahmen müssen die Transparenz unterstützen, so dass eine Überprüfung möglich ist. Vgl. 3.4.1.1.

3.4.3.5 Isolierung (Zweckbegrenzung)

In Cloud-Infrastrukturen teilen sich viele Mieter Ressourcen wie Aufbewahrung, Speicher und Netzwerke. Das schafft neue Risiken in Bezug auf die Offenlegung oder Weiterverarbeitung der Daten für illegale Zwecke. Das Schutzziel „Isolierung“ soll dieses Problem angehen und dazu beitragen, dass Daten nicht über ihren ursprünglichen Zweck hinaus verwendet werden (Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG) und dass die Vertraulichkeit und Integrität gewahrt bleiben.[29]

Damit eine Isolierung erreicht werden kann, ist zuerst eine adäquate Kontrolle der Rechte und Rollen für den Zugang zu den personenbezogenen Daten erforderlich. Es ist eine regelmäßige Überprüfung durchzuführen. Die Einführung von Funktionen mit sehr großen Privilegien sollte vermieden werden (so sollte kein Anwender oder Administrator für die gesamte Cloud zugangsberechtigt sein). Allgemeiner gesagt: Administratoren und Anwender dürfen nur Zugang zu den Informationen haben, die sie für die rechtmäßige Zweckerfüllung benötigen (Least Privilege Prinzip).

Zweitens hängt die Isolierung auch von technischen Maßnahmen wie dem Verstärken der Hypervisoren und einer richtigen Verwaltung gemeinsam genutzter Ressourcen ab, wenn

---

Computing-Diensten genutzt werden können, nicht zu einer unwiderbringlichen Anonymisierung der Daten und implizieren folglich nicht, dass die Datenschutzvorschriften keine Anwendung finden.

[28] Das gilt insbesondere für die Datenverarbeitung Verantwortliche, die eine Übermittlung sensibler Daten im Sinne von Artikel 8 der Richtlinie 95/46/EG (z. B. Gesundheitsdaten) oder von dem Berufsgeheimnis unterliegenden Daten in die Cloud planen.

[29] Vgl. 3.4.1.2.

virtuelle Maschinen genutzt werden, um physische Ressourcen gemeinsam mit verschiedenen Cloud-Anwendern zu nutzen.

3.4.3.5 Intervenierbarkeit

Richtlinie 95/46/EG gibt der betroffenen Person das Recht auf Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch (vgl. Artikel 12 und 14). Der Cloud-Anwender muss überprüfen, dass der Cloud-Anbieter diesen Anforderungen keine technischen und organisatorischen Hürden auferlegt. Dies gilt auch für die Fälle, in denen die Daten von Unterauftragnehmern weiterverarbeitet werden.

Der Vertrag zwischen dem Anwender und dem Anbieter sollte festlegen, dass der Cloud-Anbieter dazu verpflichtet ist, den Anwender dahingehend zu unterstützen, dass die Ausübung der Rechte der betroffenen Person vereinfacht wird. So muss auch sichergestellt werden, dass dies auch für seine Beziehung zu jedem Unterauftragnehmer gilt.[30]

3.4.3.6 Portabilität

Derzeit nutzen die wenigsten Cloud-Anbieter Standard-Datenformate und Service-Schnittstellen, die die Interoperabilität und Portabilität zwischen verschiedenen Cloud-Anbietern vereinfachen. Wenn ein Cloud-Anwender entscheidet, von einem Cloud-Anbieter zu einem anderen zu migrieren, kann dieser Mangel an Interoperabilität dazu führen, dass der Transfer der (personenbezogenen) Daten des Anwenders zu einem neuen Cloud-Anbieter unmöglich oder zumindest schwierig ist (sogenanntes Vendor Lock-in). Das gilt auch für Dienste, die der Anwender auf einer Plattform entwickelt hat, die von dem ursprünglichen Cloud-Anbieter angeboten wurden (PaaS). Der Cloud-Anwender sollte vor Buchen eines Cloud-Dienstes prüfen, ob und wie der Anbieter die Portabilität der Daten und Leistungen garantiert.[31]

3.4.4.7 Rechenschaftspflicht

Im IT-Bereich kann Rechenschaft als die Fähigkeit definiert werden, festzustellen, was eine Entität zu einem bestimmten Zeitpunkt in der Vergangenheit gemacht hat und wie sie es getan hat. Im Bereich des Datenschutzes ist die Bedeutung meist weiter gefasst und beschreibt die Fähigkeit der Parteien, nachzuweisen, dass sie angemessene Schritte zur Umsetzung der Datenschutzgrundsätze unternommen haben.

Rechenschaft in der Informationstechnik ist besonders wichtig für die Ermittlung von Datenschutzverletzungen im Bereich personenbezogener Daten, wo der Cloud-Anwender, der Anbieter und der Unterauftragsverarbeiter je einen Teil der operativen Verantwortung tragen können. Diesbezüglich ist die Fähigkeit der Cloud-Plattform, eine verlässliche Überwachung und verständliche Protokollierungs-Mechanismen zu bieten, von größter Bedeutung.

Darüber hinaus sollten die Cloud-Anbieter durch die Vorlage von entsprechenden Schriftstücken nachweisen, dass sie die in den vorstehenden Abschnitten aufgeführten Datenschutzgrundsätze mittels angemessener und effektiver Maßnahmen umgesetzt haben. Beispiele für solche Maßnahmen sind Verfahren zur Sicherstellung der Identifizierung aller Datenverarbeitungsschritte, die Beantwortung von Auskunftsersuchen, die Zuweisung von Ressourcen einschließlich der Ernennung von Datenschutzbeauftragten, die für die

---

[30] Vgl. den vorstehenden Abschnitt 3.4.2 Nr. 6. Der Anbieter kann sogar dazu instruiert werden, Anfragen im Namen des Anwenders zu beantworten.

[31] Der Anbieter sollte vorzugsweise standardisierte oder offene Datenformate und Schnittstellen nutzen. Es sollten auf jeden Fall Vertragsklauseln vereinbart werden, die gesicherte Formate, die Erhaltung logischer Beziehungen und die Kosten der Migration zu einem anderen Cloud-Anbieter festlegen.

Organisation der Einhaltung der Datenschutzbestimmungen zuständig sind oder unabhängige Zertifizierungsverfahren. Darüber hinaus sollten die für die Datenverarbeitung Verantwortlichen sicherstellen, dass sie gegenüber der zuständigen Überwachungsbehörde jederzeit auf Anfrage die notwendigen Maßnahmen nachweisen können.[32]

3.5 Internationale Übermittlungen

Artikel 25 und 26 der Richtlinie 95/46/EG sehen den freien Verkehr personenbezogener Daten in Länder außerhalb des EWR nur dann vor, wenn das Land oder der Empfänger ein angemessenes Datenschutzniveau bietet. Andernfalls sind von dem für die Verarbeitung Verantwortlichen und seinen für die Verarbeitung Mitverantwortlichen und/oder den Auftragsverarbeitern besondere Garantien einzurichten. Cloud Computing basiert jedoch meistens auf dem vollständigen Fehlen eines festen Standorts, an dem sich die Daten innerhalb des Netzwerks des Cloud-Anbieters befinden. Die Daten können um 14.00 Uhr in dem einen Datenzentrum sein und um 16.00 Uhr in einem anderen Datenzentrum am anderen Ende der Welt. Der Cloud-Anwender kann deshalb nur selten in Echtzeit wissen, wo sich die Daten befinden, wo sie gespeichert oder übermittelt werden. In diesem Zusammenhang sind die traditionellen Rechtsinstrumente zur Bereitstellung eines Rahmens zur Regulierung der Datenübermittlungen in Drittländer außerhalb der EU, die keinen angemessenen Schutz bieten, eingeschränkt.

3.5.1 Safe Harbor und angemessene Länder

Die Angemessenheit des Schutzniveaus, einschließlich Safe Harbor sind in Bezug auf den geografischen Anwendungsbereich eingeschränkt und decken folglich nicht alle Übermittlungen in der Cloud ab.
Übermittlungen an US-amerikanische Organisationen, die sich an die Grundsätze halten, können rechtmäßig unter EU-Recht stattfinden, da davon ausgegangen wird, dass die Empfängerorganisationen ein angemessenes Schutzniveau für die übermittelten Daten bieten.

Die Arbeitsgruppe vertritt jedoch die Ansicht, dass allein die Selbstzertifizierung nach dem Safe Harbor Abkommen bei einem gleichzeitigen Fehlen der tatsächlichen Durchsetzung der Datenschutzgrundsätze in der Cloud-Umgebung nicht als ausreichend angesehen werden kann. Darüber hinaus verlangt Artikel 17 der EU-Richtlinie, dass zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter für die Verarbeitungszwecke ein Vertrag unterzeichnet wird. Dies wird in FAQ 10 der EU-US Safe Harbor Rahmendokumente bestätigt. Dieser Vertrag unterliegt nicht der vorherigen Genehmigung durch die europäischen Datenschutzbehörden. Ein solcher Vertrag spezifiziert die durchzuführende Verarbeitung und alle Maßnahmen, die erforderlich sind, damit die sichere Aufbewahrung der Daten sichergestellt ist. Einige nationale Bestimmungen und Datenschutzbehörden können zusätzliche Anforderungen stellen.

Die Arbeitsgruppe ist der Ansicht, das sich Daten exportierende Unternehmen nicht nur auf die Erklärung des Datenimporteurs verlassen sollten, dass er eine Safe-Harbor-Zertifizierung hat. Stattdessen sollte das Daten exportierende Unternehmen einen Nachweis erhalten, dass die Safe Harbor Selbstzertifizierung vorliegt und einen Nachweis fordern, dass die

[32] Die Arbeitsgruppe hat in ihrer Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht detaillierte Ausführungen zur Rechenschaftspflicht vorgelegt http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_de.pdf.

Grundsätze wirklich befolgt werden. Das ist besonders wichtig in Bezug auf die Informationen, die den von der Datenverarbeitung betroffenen Personen erteilt werden[3334].

Die Arbeitsgruppe ist auch der Ansicht, dass der Cloud-Anwender überprüfen muss, ob die von Cloud-Anbietern aufgesetzten Standardverträge den nationalen Anforderungen im Hinblick auf die vertragliche Datenverarbeitung entsprechen. Die nationalen Anforderungen können möglicherweise verlangen, dass die Vergabe von Unteraufträgen im Vertrag definiert wird. Dazu gehören die Standorte und andere Daten zu den Unterauftragsverarbeitern sowie die Nachverfolgbarkeit der Daten. Normalerweise bieten die Cloud-Anbieter den Anwendern diese Informationen nicht - ihre Verpflichtung zu den Safe-Harbor-Grundsätzen kann das Fehlen der vorgenannten Garantien nicht ersetzen, wenn diese in den nationalen Rechtsvorschriften gefordert werden. In solchen Fällen wird der Exporteur dazu aufgefordert, andere verfügbare Rechtsinstrumente zu nutzen, wie beispielsweise Standardsvertragsklauseln oder verbindliche unternehmensinterne Vorschriften.

Schließlich vertritt die Arbeitsgruppe die Ansicht, dass die Safe-Harbor-Grundsätze an sich dem Daten-Exporteur nicht die erforderlichen Mittel garantieren, um sicherstellen zu können, dass von dem Cloud-Anbieter in den USA angemessene Sicherheitsmaßnahmen angewendet wurden, wie es möglicherweise von den nationalen Rechtsvorschriften basierend auf Richtlinie 95/46/EC [35] gefordert wird. Im Hinblick auf die Datensicherheit führt Cloud Computing zu einigen Cloud-spezifischen Sicherheitsrisiken, wie den Verlust der Kontrolle, ein unsicheres oder unvollständiges Löschen der Daten, unzureichende Prüfpfade oder Fehler bei der Isolierung[36], die durch die bestehenden Safe Harbor Grundsätze zum Datenschutz nicht ausreichend behandelt werden [37] . Es können also zusätzliche Garantien zur Datensicherheit eingesetzt werden, wie durch die Einbindung des Fachwissens und der Ressourcen von Dritten, die dazu befähigt sind, die Angemessenheit des Cloud-Anbieters durch verschiedene Prüfungs-, Standardisierungs- und Zertifizierungssysteme zu bewerten[38]. Aus diesen Gründen könnte es empfehlenswert sein, die Verpflichtung des Datenimporteurs zu den Safe Harbor Grundsätzen mit zusätzlichen Garantien zu vervollständigen, die die besondere Natur der Cloud berücksichtigen.

3.5.2 Ausnahmen

Die Ausnahmen gemäß Artikel 26 der Richtlinie 95/46/EG ermöglichen Datenexporteuren die Übermittlung von Daten aus der EU ohne dass sie zusätzliche Garantien bereitstellen. Die WP29 hat jedoch eine Stellungnahme angenommen, in welcher sie die Ansicht vertritt, dass Ausnahmen nur dann anwendbar sein sollten, wenn die Übermittlungen weder wiederkehrend noch in großem Umfang oder strukturell sind. [39]

---

33 Siehe die deutsche Datenschutzbehörde. http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

34 Für die Anforderungen in Bezug auf Verträge mit Unterauftragsverarbeitern siehe 3.3.2.

35 Siehe die Stellungnahme der dänischen Datenschutzbehörde. http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Detailliert in dem ENISA-Papier zum Cloud Computing beschrieben: Vorteile, Risiken und Empfehlungen der Informationssicherheit unter: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 „Organisationen müssen angemessene Vorkehrungen treffen, um personenbezogene Informationen vor Verlust, Missbrauch und unautorisiertem Zugriff, vor Offenlegung, Änderung und Zerstörung zu schützen."

38 Siehe nachfolgenden Abschnitt 4.2.

39 Arbeitsunterlage 12/1998: Übermittlungen personenbezogener Daten an Drittländer : Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU. Von der Arbeitsgruppe am 24. Juli 1998 angenommen (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_de.pdf).

Basierend auf solchen Auslegungen ist es fast unmöglich, sich im Zusammenhang mit Cloud Computing auf Ausnahmen zu verlassen.

3.5.3 Standardvertragsklauseln

Standardvertragsklauseln wie die von der EU-Kommission angenommenen, mit denen internationalen Datenübermittlungen zwischen zwei für die Verarbeitung Verantwortlichen oder einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter ein Rahmen gegeben werden soll, basieren auf einem bilateralen Ansatz. Wenn der Cloud-Anbieter als Auftragsverarbeiter angesehen wird, sind Standardklauseln nach dem Kommissionsbeschluss 2010/87/EG ein Instrument, das zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen als eine Grundlage in der Cloud Computing-Umgebung herangezogen werden kann, um angemessene Garantien im Zusammenhang mit internationalen Übermittlungen zu bieten.

Die Arbeitsgruppe vertritt die Ansicht, dass der Cloud-Anbieter den Kunden zusätzlich zu den Standardvertragsklauseln Bestimmungen anbieten könnte, die auf ihren pragmatischen Erfahrungen basieren, solange diese nicht direkt oder indirekt den von der Kommission bewilligten Standardvertragsklauseln widersprechen oder Grundrechte oder -freiheiten der betroffenen Personen beeinträchtigen [40] . Dennoch können Unternehmen die Standardvertragsklauseln nicht ergänzen oder ändern, ohne dass dies bedeutet, dass die Bestimmungen nicht mehr länger „Standard“[41] sind.

Wenn der als Auftragsverarbeiter agierende Cloud-Anbieter in der EU niedergelassen ist, könnte die Situation noch komplexer sein, da die Musterklauseln im Allgemeinen nur auf Datenübermittlungen von einem für die Verarbeitung Verantwortlichen in der EU an einen Auftragsverarbeiter außerhalb der EU Anwendung finden (siehe Erwägungsgrund 23 des Kommissionsbeschlusses 2010/87/EU über Standardvertragsklauseln und WP 176).

Bezüglich der vertraglichen Beziehungen zwischen einem nicht in der EU ansässigen Auftragsverarbeiter und den Unterauftragsverarbeitern sollte eine schriftliche Vereinbarung getroffen werden, die dem Unterauftragsverarbeiter dieselben Verpflichtungen auferlegt, die dem Auftragsverarbeiter auferlegt würden, fänden die Musterklauseln Anwendung.

3.5.4 Verbindliche unternehmensinterne Vorschriften: in Richtung eines globalen Ansatzes

Verbindliche unternehmensinterne Vorschriften sind ein Verhaltenskodex für Unternehmen, die Daten innerhalb ihrer Gruppe übermitteln. Ist der Anbieter ein Auftragsverarbeiter, werden solche Lösungen auch im Kontext des Cloud Computing bereitgestellt. Derzeit arbeitet die WP29 an verbindlichen unternehmensinternen Vorschriften für Auftragsverarbeiter, die die Übermittlung innerhalb der Gruppe zugunsten der für die Verarbeitung Verantwortlichen ermöglichen, ohne dass für jeden Anwender ein Vertrag zwischen dem Auftragsverarbeiter und dem Unterauftragsverarbeiter unterzeichnet werden muss.[42]

---

[40] Siehe FAQ IV B1.9 9, Can companies include the standard contractual clauses in a wider contract and add specific clauses? veröffentlicht von der EG unter http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[41] Siehe FAQ IV B1.10, Can Companies amend and change the standard contractual clauses approved by the Commission?

[42] Siehe Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, angenommen am 6. Juni 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

Solche verbindlichen unternehmensinternen Vorschriften für Auftragsverarbeiter würden es dem Kunden des Anbieters ermöglichen, dem Auftragsverarbeiter seine personenbezogenen Daten anzuvertrauen und dabei sicher zu sein, dass für die innerhalb des Geschäftsbereichs des Anbieters übermittelten Daten ein angemessenes Schutzniveau besteht.

4. Schlussfolgerungen und Empfehlungen

Unternehmen und Verwaltungen, die Cloud Computing nutzen wollen, sollten als ersten Schritt eine umfassende und gründliche Risikoanalyse durchführen. Diese Analyse muss unter Berücksichtigung der Art der in der Cloud verarbeiteten Daten die Risiken untersuchen, die mit der Verarbeitung der Daten in der Cloud einhergehen (fehlende Kontrolle und unzureichende Informationen - siehe Abschnitt 2 oben). [43] Es sollte besondere Aufmerksamkeit auf die Bewertung der rechtlichen Risiken in Bezug auf den Datenschutz gelegt werden, die in erster Linie Sicherheitsvorschriften und internationale Übermittlungen betreffen. Die Verarbeitung sensibler Daten mittels Cloud Computing weckt zusätzliche Bedenken. Unbeschadet nationaler Rechtsvorschriften erfordern solche Verarbeitungen folglich zusätzliche Garantien. [44] Die nachstehenden Schlussfolgerungen sollen eine Checkliste für die Einhaltung des Datenschutzes durch Cloud-Anwender und Cloud-Anbieter bieten. Sie basieren auf dem aktuellen Rechtsrahmen. Einige Empfehlungen werden auch angesichts zukünftiger Entwicklungen in den Rechtsvorschriften auf EU-Ebene und darüber hinaus erteilt.

4.1 Leitlinien für Anwender und Anbieter von Cloud Computing-Diensten

- Beziehung „für die Verarbeitung Verantwortlicher – Auftragsverarbeiter“: Diese Stellungnahme konzentriert sich auf die Anwender-Anbieter-Beziehung als Beziehung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter (siehe Abschnitt 3.3.1). Basierend auf konkreten Umständen kann es jedoch Situationen geben, in denen der Cloud-Anbieter auch als für die Verarbeitung Verantwortlicher fungiert, beispielsweise, wenn der Anbieter einige personenbezogene Daten für seine eigenen Zwecke erneut verarbeitet. In einem solchen Fall trägt der Cloud-Anbieter die vollständige (gemeinsame) Verantwortung für die Verarbeitung und muss alle rechtlichen Verpflichtungen erfüllen, die in den Richtlinien 95/46/EG und 2002/58/EG niedergelegt sind (sofern anwendbar).
- Die Verantwortung des Cloud-Anwenders als für die Verarbeitung Verantwortlicher: Der Kunde als der für die Verarbeitung Verantwortliche muss die Verantwortung für die Einhaltung der Datenschutzvorschriften übernehmen und unterliegt allen rechtlichen Verpflichtungen, die in den Richtlinien 95/46/EG und 2002/58/EG niedergelegt sind (sofern anwendbar). Dies gilt insbesondere gegenüber den betroffenen Personen (siehe 3.3.1). Der Anwender sollte sich für einen Cloud-Anbieter entscheiden, der die Einhaltung der EU-Datenschutzvorschriften garantiert, wie sie in den nachfolgend zusammengefassten vertraglichen Garantien wiedergegeben werden.

[43] Die ENISA stellt eine Liste der Risiken bereit, die berücksichtigt werden müssen http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[44] Siehe Sopot-Memorandum, vgl. Fußnote 2 oben.

- Garantien bei der Untervergabe: In jedem Vertrag zwischen dem Cloud-Anbieter und dem Cloud-Anwender sollten Bestimmungen für Unterauftragnehmer enthalten sein. Der Vertrag sollte festlegen, dass Unterauftragsverarbeiter ausschließlich auf der Grundlage einer Einwilligung beauftragt werden dürfen, die der für die Verarbeitung Verantwortliche generell erteilen kann. Gleichzeitig ist der Auftragsverarbeiter eindeutig dazu verpflichtet, den für die Verarbeitung Verantwortlichen über diesbezügliche beabsichtigte Änderungen zu informieren. Der für die Verarbeitung Verantwortliche hat jederzeit die Möglichkeit, solchen Änderungen zu widersprechen oder den Vertrag zu beenden. Der Cloud-Anbieter sollte eindeutig dazu verpflichtet sein, alle beauftragten Unterauftragnehmer zu nennen. Der Cloud-Anbieter sollte mit jedem Unterauftragnehmer einen Vertrag unterzeichnen, der die Vereinbarungen mit dem Cloud-Anwender wiedergibt. Der Anwender sollte sicherstellen, dass er im Fall von Vertragsverletzungen durch die Unterauftragnehmer des Anbieters Regress nehmen kann (siehe 3.3.2).
- Einhaltung der grundlegenden Datenschutzgrundsätze:
    - Transparenz (siehe 3.4.1.1): Cloud-Anbieter sollten die Cloud-Anwender während der Vertragsverhandlungen über alle (datenschutzrechtlich) relevanten Aspekte ihrer Dienste informieren. Die Anwender sollten insbesondere über alle Unterauftragnehmer informiert sein, die zur Bereitstellung des jeweiligen Cloud-Dienstes beitragen und über alle Orte, an denen Daten vom Cloud-Anbieter und/oder seinen Unterauftragnehmern aufbewahrt oder verarbeitet werden können (insbesondere, wenn sich einige oder alle der Orte außerhalb des Europäischen Wirtschaftsraums (EWR) befinden). Der Anwender sollte aussagekräftige Informationen über technische und organisatorische Maßnahmen erhalten, die von dem Anbieter umgesetzt wurden. Der Anwender sollte die betroffenen Personen im Sinne einer angemessenen Vorgehensweise über den Cloud-Anbieter und alle Unterauftragnehmer (sofern vorhanden) informieren sowie über die Orte, an denen die Daten von dem Cloud-Anbieter und/oder seinen Unterauftragnehmern möglicherweise aufbewahrt oder verarbeitet werden.
    - Zweckbestimmung und -begrenzung (3.4.1.2): Der Anwender sollte die Einhaltung der Grundsätze der Zweckbestimmung und -begrenzung sicherstellen und garantieren, dass keine Daten von dem Anbieter oder von Unterauftragnehmern für weitere Zwecke verarbeitet werden. Entsprechende Verpflichtungen sollten in angemessenen vertraglichen Maßnahmen (einschließlich technischer und organisatorischer Garantien) festgehalten werden.
    - Datenspeicherung (3.4.1.3): Der Anwender muss sicherstellen, dass personenbezogene Daten (durch den Anbieter und jeden Unterauftragnehmer) von jedem Speicherort gelöscht werden, sobald sie nicht mehr für den bestimmten Zweck benötigt werden. Sichere Mechanismen zur Löschung (Zerstörung, Entmagnetisierung, Überschreiben) sollten vertraglich festgelegt werden.
- Vertragliche Garantien (siehe 3.4.2, 3.4.3 und 3.4.5):
    - Generell sollten der Vertrag mit dem Anbieter (und die Verträge, die zwischen dem Anbieter und den Unterauftragnehmern geschlossen werden) ausreichende Garantien in Bezug auf die technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen (gemäß Artikel 17 Absatz 2 der Richtlinie) enthalten und schriftlich oder in einer anderen angemessenen Form

vorliegen. Der Vertrag sollte die Anweisungen des Anwenders an den Anbieter genau beschreiben, einschließlich des Gegenstands und Zeitrahmens des Dienstes, des Ziels und der messbaren Servicelevel und der entsprechenden Strafen (finanzieller oder sonstiger Natur). Er sollte die Sicherheitsmaßnahmen aufführen, die abhängig von den Risiken der Verarbeitung und der Natur der Daten und gemäß den nachfolgenden Anforderungen und vorbehaltlich strengerer Maßnahmen durchzuführen sind, die im nationalen Recht des Kunden vorgesehen sind. Wenn Cloud-Anbieter Standardvertragsklauseln nutzen wollen, sollten sie sicherstellen, dass die Bestimmungen die Datenschutzvorschriften einhalten (siehe 3.4.2). In den entsprechenden Vertragsbedingungen sollten insbesondere die technischen und organisatorischen Maßnahmen genau dargelegt werden, die vom Anbieter umgesetzt wurden.

- Zugang zu den Daten: Nur autorisierte Personen sollten Zugang zu den Daten haben. Der Vertrag sollte in Bezug auf den Anbieter und seine Angestellten eine Vertraulichkeitsvereinbarung enthalten.
- Offenlegung der Daten gegenüber Dritten: Dies sollte vertraglich geregelt sein. Der Anbieter sollte in dem Vertrag dazu verpflichtet werden, alle seine Unterauftragnehmer zu nennen - beispielsweise in einem öffentlichen digitalen Register - und sicherzustellen, dass der Anwender jederzeit Zugang zu den die Änderungen betreffenden Informationen hat, so dass er diesen Änderungen widersprechen oder den Vertrag beenden kann. Der Vertrag sollte den Anbieter auch dazu verpflichten, jede rechtlich verbindliche Anfrage auf Offenlegung personenbezogener Daten durch eine Strafverfolgungsbehörde zu melden, sofern eine solche Offenlegung nicht anderweitig verboten ist. Der Anwender sollte gewährleisten, dass der Anbieter jede Anfrage auf Offenlegung ablehnt, die nicht rechtlich verbindlich ist.
- Verpflichtung zur Kooperation: Der Anwender sollte sicherstellen, dass der Anbieter zur Kooperation in den folgenden Bereichen verpflichtet ist: Recht des Anwenders auf Überwachung der Verarbeitung, Vereinfachung der Ausübung des Rechts der betroffenen Personen auf Zugang/Berichtigung/Löschung ihrer Daten und (sofern anwendbar) Benachrichtigung des Cloud-Anwender über alle Datenschutzverletzungen, die die Daten des Anwenders betreffen.
- Grenzüberschreitende Datenübermittlungen: Der Cloud-Anwender sollte überprüfen, ob der Cloud-Anbieter die Rechtmäßigkeit grenzüberschreitender Datenübermittlungen garantieren und die Übermittlungen, wenn möglich, auf Länder beschränken kann, die der Anwender ausgewählt hat. Übermittlungen in nicht angemessene Drittländer erfordern spezielle Garantien durch die Anwendung von Safe Harbor Vereinbarungen, Standardvertragsklauseln oder verbindlicher unternehmensinterner Vorschriften - je nach Fall. Die Anwendung von Standardvertragsklauseln für Anbieter (gemäß Beschluss der Kommission 2010/87/EG) erfordert gewisse Anpassungen an die Cloud-Umgebung (um zu verhindern, dass für die jeweiligen Anwender getrennte Verträge zwischen einem Anbieter und seinen Unterauftragsverarbeitern bestehen), die möglicherweise vorher durch die zuständige Datenschutzbehörde genehmigt werden müssen. Es sollte eine Liste der Orte zur Verfügung gestellt werden, in welchen die Dienste möglicherweise bereitgestellt werden.

- Protokollieren und Überprüfung der Verarbeitung: Der Anwender sollte verlangen, dass die Verarbeitungsschritte durch den Anbieter und seine Unterauftragnehmer protokolliert werden. Der Anwender sollte dazu befugt sein, diese Verarbeitungsschritte zu überprüfen. Eine Kontrolle und die Zertifizierung durch Dritte, die der für die Verarbeitung Verantwortliche ausgewählt hat, sollten jedoch auch möglich sein, sofern eine vollständige Transparenz garantiert wird (beispielsweise durch Erhalt einer Kopie der Prüfbescheinigung oder des Prüfberichts zur Überprüfung der Zertifizierung).
- Technische und organisatorische Maßnahmen: Diese sollten zur Beseitigung der Risiken dienen, die der in der Cloud-Computing-Umgebung sehr weit verbreitete Mangel an Kontrolle und Informationen nach sich zieht. Die Erstgenannten umfassen Maßnahmen, mit denen die Verfügbarkeit, Integrität, Vertraulichkeit, Isolierung, Intervenierbarkeit und Portabilität in den in der Stellungnahme niedergelegten Definitionen sichergestellt werden sollen während sich die Letztgenannten auf die Transparenz konzentrieren (siehe 3.4.3 für alle Einzelheiten).

4.2 Datenschutz-Zertifizierung durch Dritte

- Eine unabhängige Überprüfung oder Zertifizierung durch einen anerkannten Dritten kann für Cloud-Anbieter ein glaubwürdiges Mittel sein, um ihre Einhaltung der in dieser Stellungnahme niedergelegten Verpflichtungen nachzuweisen. Eine solche Zertifizierung würde mindestens angeben, dass eine anerkannte dritte Organisation anhand anerkannter Standards die Überwachung des Datenschutzes überprüft hat und dass die in dieser Stellungnahme niedergelegten Anforderungen erfüllt werden.[45] Im Bereich des Cloud Computing sollten potenzielle Kunden prüfen, ob die Anbieter der Cloud-Dienste eine Kopie dieser Prüfbescheinigung durch eine dritte Partei oder des Prüfberichts, der die Zertifizierung in Bezug auf die in dieser Stellungnahme niedergelegten Anforderungen überprüft, vorlegen kann.
- Individuelle Prüfungen von Daten, die in einer virtualisierten Serverumgebung mit vielen Parteien gehostet sind, könnten sich als technisch unpraktisch herausstellen und unter bestimmten Umständen die Risiken für die bereits stattfindenden physischen und logischen Netzwerk-Sicherheitskontrollen erhöhen. In solchen Fällen könnte eine entsprechende Prüfung durch einen von dem für die Verarbeitung Verantwortlichen ausgewählten Dritten anstelle des Rechts auf Prüfung durch einen individuellen für die Verarbeitung Verantwortlichen ausreichen.
- Die Annahme von privatsphärenspezifischen Standards und Zertifizierungen ist für den Aufbau eines Vertrauensverhältnisses zwischen Cloud-Anbietern, für die Verarbeitung Verantwortlichen und betroffenen Personen von großer Bedeutung.
- Diese Standards und Zertifizierungen sollten technische Maßnahmen betreffen (wie die Lokalisierung oder Verschlüsselung von Daten) sowie die Prozesse innerhalb der Organisation des Anbieters, die den Datenschutz sicherstellen (wie Vorgehensweisen zur Zugangskontrolle, die Zugangskontrolle oder Backups).

[45] Zu diesen Standards würden unter anderem die der Internationalen Normenorganisationen, des International Auditing and Assurance Standards Board und des Auditing Standards Board of the American Institute of Certified Public Accountants zählen, insoweit diese Organisationen Standards bereitstellen, die die in dieser Stellungnahme niedergelegten Anforderungen erfüllen.

4.3 Empfehlungen: zukünftige Entwicklungen

Der Arbeitsgruppe ist es vollkommen bewusst, dass die in dieser Stellungnahme dargelegten Garantien und Lösungen keine allumfassende Lösung für die Komplexität des Cloud Computing sind. Sie stellen jedoch eine tragfähige Grundlage dar, um die Verarbeitung personenbezogener Daten abzusichern, die im EWR niedergelassene Anwender an Cloud-Anbieter übergeben. Dieser Abschnitt konzentriert sich auf einige Fragen, die kurz- oder mittelfristig angegangen werden müssen, um die bestehenden Garantien zu stärken, die Cloud-Industrie bezüglich der dargelegten Fragen zu unterstützen und gleichzeitig die Achtung der Grundrechte auf Privatsphäre und Datenschutz sicherzustellen.

- Mehr Ausgewogenheit zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter in Bezug auf die Verantwortung: Die Arbeitsgruppe begrüßt die Bestimmungen in Artikel 26 des Vorschlags der Kommission (Entwurf einer EU-Datenschutz-Grundverordnung), mit denen die Rechenschaftspflicht des Auftragsverarbeiters gegenüber dem für die Verarbeitung Verantwortlichen hervorgehoben wird, indem er diesem helfen muss, die Einhaltung insbesondere der Sicherheits- und ähnlicher Verpflichtungen sicherzustellen. Artikel 30 dieses Vorschlags führt die Pflicht für den Auftragsverarbeiter ein, geeignete technische und organisatorische Maßnahmen einzuführen. Der Vorschlagsentwurf stellt klar, dass ein Auftragsverarbeiter, der die Anweisungen des für die Verarbeitung Verantwortlichen nicht befolgt, als für die Verarbeitung Verantwortlicher gilt und spezifischen Bestimmungen unterworfen ist, da er für die Verarbeitung mitverantwortlich ist. Die Artikel-29-Arbeitsgruppe ist der Ansicht, dass dieser Vorschlag in die richtige Richtung geht, um das Ungleichgewicht auszugleichen, das häufig in der Cloud Computing-Umgebung besteht, in welcher der Anwender (insbesondere wenn es sich um ein KMU handelt) Schwierigkeiten haben könnte, die in den Datenschutzvorschriften geforderte Kontrolle darüber auszuüben, wie der Anbieter die geforderten Dienste ausführt. Darüber hinaus wird angesichts der asymmetrischen Rechtsposition von betroffenen Personen und kleinen Unternehmen gegenüber großen Cloud Computing-Anbietern eine proaktivere Rolle für Verbraucher- und Unternehmensschutzorganisationen empfohlen, um ausgewogenere allgemeine Geschäftsbedingungen solcher Anbieter auszuhandeln.

- Zugang zu personenbezogenen Daten für nationale Sicherheits- und Strafverfolgungszwecke: Es ist von größter Bedeutung, der zukünftigen Verordnung hinzuzufügen, dass es den in der EU tätigen für die Verarbeitung Verantwortlichen untersagt sein muss, personenbezogene Daten an Drittländer offenzulegen, wenn dies von einer Gerichts- oder Verwaltungsbehörde eines Drittlandes gefordert wird, es sei denn, dies wird ausdrücklich in einer internationalen Vereinbarung oder einem Rechtshilfeabkommen gestattet oder von einer Überwachungsbehörde genehmigt. Die Verordnung (EG) Nr. 2271/96 des Rates ist ein angemessenes Beispiel einer Rechtsgrundlage hierfür.[46] Die Arbeitsgruppe ist besorgt über diese Lücke in dem Vorschlag der Kommission, da dies einen beträchtlichen Verlust an Rechtssicherheit für die betroffenen Personen bedeutet, deren personenbezogenen Daten in Datenzentren in der ganzen Welt gespeichert werden. Aus diesem Grund möchte die Arbeitsgruppe betonen[47], dass es wichtig ist, in der Verordnung festzuhalten, dass im Fall von Offenlegungen, die nicht durch das Recht der Union oder der Mitgliedstaaten berechtigt sind, Rechtshilfeabkommen zu nutzen sind.

---

[46] Verordnung (EG) Nr. 2271/96 des Rates vom 22. November 1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen, Amtsblatt L 309, 29.11.1996 S. 0001 - 0006, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:DE:HTML

[47] Vgl. WP 191 - Stellungnahme 01/2012 zu den Reformvorschlägen im Bereich des Datenschutzes, S. 23.

- Besondere Vorkehrungen durch den öffentlichen Sektor: Ein besonderer Vorbehalt ist in Bezug auf die Notwendigkeit hinzuzufügen, dass eine öffentliche Behörde erst prüfen muss, ob die Kommunikation, Verarbeitung und Speicherung der Daten außerhalb des innerstaatlichen Hoheitsgebiets die Sicherheit und Privatsphäre der Bürger sowie die nationale Sicherheit und Wirtschaft unannehmbaren Risiken aussetzen würde. Dies gilt insbesondere, wenn sensible Datenbanken (z.B. Zensusdaten) und Leistungen (z.B. Gesundheitsfürsorge) betroffen sind.[48] Dies sollte unbedingt jedes Mal in Erwägung gezogen werden, wenn sensible Daten in der Cloud-Umgebung verarbeitet werden. Ausgehend davon könnten nationale Regierungen und Organe der Europäischen Union über eine weitere Prüfung des Konzepts einer Europäischen Regierungs-Cloud als einen supranationalen virtuellen Raum nachdenken, in dem einheitliche und harmonisierte Vorschriften angewendet werden könnten.

- Europäische Cloud-Partnerschaft: Die Arbeitsgruppe unterstützt die Strategie für eine Europäische Cloud-Partnerschaft (ECP), die Frau Kroes, Vizepräsidentin der Europäischen Kommission, im Januar 2012 in Davos vorgestellt hat.[49] Diese Strategie umfasst die öffentliche IT-Beschaffung zur Anregung eines Europäischen Cloud-Marktes. Die Übermittlung personenbezogener Daten an einen europäischen Cloud-Anbieter, der sich an europäische Datenschutzvorschriften zu halten hat, könnte für die Kunden mit großen datenschutzrechtlichen Vorteilen verbunden sein, insbesondere durch die Förderung der Annahme allgemeiner Standards (vor allem in Bezug auf die Interoperabilität und die Datenportabilität) und könnte ihnen Rechtssicherheit geben.

---

[48] Diesbezüglich macht die ENISA in ihrem Papier zur Sicherheit und Belastbarkeit von Regierungs-Clouds folgende Empfehlung (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): „In Bezug auf den Aufbau scheinen Private und Community Clouds derzeit die beste Lösung für den Bedarf von staatlichen Verwaltungsbehörden in Bezug auf sensible Anwendungen zu sein, da sie das höchste Maß an Governance, Kontrolle und Sichtbarkeit bieten, auch wenn beim Planen einer Private oder Community Cloud besonderes Augenmerk auf die Größe der Infrastruktur gerichtet werden sollte."

[49] Neelie Kroes, Vizepräsidentin der Europäischen Kommission, verantwortlich für die Digitale Agenda, Setting up the European Cloud Partnership World Economic Forum Davos, Schweiz, 26. Januar 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANHANG

a) Rollout-Modelle

Private Cloud[50] beschreibt eine IT-Infrastruktur, die einer einzigen Organisation gewidmet ist. Sie befindet sich entweder in den Geschäftsräumen der Organisation oder ihre Verwaltung ist an einen Dritten ausgelagert (üblicherweise über Server-Hosting), der der strikten Anweisungsbefugnis des für die Verarbeitung Verantwortlichen unterliegt. Eine Private Cloud kann mit einem herkömmlichen Datenzentrum verglichen werden. Der Unterschied liegt darin, dass technische Maßnahmen umgesetzt werden, um die verfügbaren Ressourcen zu optimieren und diese Ressourcen über kleine Investitionen zu stärken, die schrittweise im Laufe der Zeit gemacht werden.

Die **Public Cloud** dagegen ist eine Infrastruktur, die sich im Eigentum eines Anbieters befindet, der sich auf die Bereitstellung von Diensten spezialisiert hat und der seine Systeme Nutzern, Unternehmen und/oder öffentlichen Verwaltungsbehörden zur Verfügung stellt und folglich unter ihnen teilt. Auf die Dienste kann über das Internet Zugriff genommen werden, was die Datenverarbeitung und/oder Übermittlung der Daten an die Systeme des Diensteanbieters nach sich zieht. Deshalb hat der Diensteanbieter eine Schlüsselrolle in Bezug auf den wirksamen Schutz der an sein System übergebenen Daten. Zusammen mit den Daten gibt der Nutzer einen großen Teil seiner Kontrolle über diese Daten ab.

Neben „Public" und „Private" Clouds gibt es noch sogenannte „intermediäre" oder „hybride" Clouds, bei denen die Dienste sowohl von privaten Infrastrukturen bereitgestellt werden, als auch von Public Clouds gekauft werden. Es sollte auch auf die „Community Cloud" hingewiesen werden, bei der sich verschiedene Organisationen die IT-Infrastruktur zum Nutzen einer bestimmten Nutzergemeinschaft teilen.

Flexibilität und Einfachheit bei der Konfigurierung von Cloud-Systemen ermöglichen ihre „elastischen" Dimensionen, d. h. diese Systeme können gemäß einem nutzerbasierten Ansatz an die besonderen Ansprüche angepasst werden. Die Nutzer müssen nicht selbst IT-Systeme verwalten, auf die auf der Grundlage von Auslagerungs-Vereinbarungen Zugriff genommen wird und die deshalb vollständig von dem Dritten verwaltet werden, in dessen Cloud die Daten aufbewahrt werden. Häufig kommen große Anbieter mit komplexen Infrastrukturen ins Spiel. Deshalb kann sich die Cloud über mehrere Standorte erstrecken. Die Anwender wissen nicht unbedingt genau, wo ihre Daten aufbewahrt werden.

---

[50] Das NIST (National Institute of Standards and Technology) in den USA, das seit einiger Zeit an der Standardisierung cloudbasierter Technologien arbeitet und auf dessen Definitionen auch in dem ENISA-Papier hingewiesen wird.
Private Cloud.
Die Cloud-Infrastruktur wird nur für eine Organisation betrieben. Sie kann von der Organisation selbst oder von einem Dritten verwaltet werden und muss sich nicht unbedingt in den Geschäftsräumen befinden. Es sollte darauf hingewiesen werden, dass sich eine „Private Cloud" zumindest auf manche Technologien stützt, die auch für „Public Clouds" üblich sind - einschließlich insbesondere der Virtualisierungs-Technologien, die – wie oben erklärt - eine Re-Organisation (oder Überarbeitung) der Datenverarbeitungsorganisation fördern.
Public Cloud.
Die Cloud-Infrastruktur wird der Allgemeinheit oder einer großen Industriegruppe zur Verfügung gestellt. Sie ist das Eigentum einer Organisation, die Cloud-Dienste verkauft.

b) Servicemodelle

Abhängig von den Anforderungen des Nutzers gibt es verschiedene Cloud Computing-Lösungen auf dem Markt, die in drei Hauptkategorien oder „Servicemodelle“ zusammengefasst werden können. Diese Modelle finden normalerweise sowohl auf Private als auch auf Public Clouds Anwendung:

- **IaaS (Cloud Infrastructure as a Service):** Ein Anbieter vermietet eine technische Infrastruktur, d. h. virtuelle Remote-Server, auf die sich der End-Nutzer gemäß den Mechanismen und Vereinbarungen stützen kann. Dadurch wird es einfach, wirksam und vorteilhaft, die IT-Systeme des Unternehmens in den Geschäftsräumen des Unternehmens zu ersetzen und/oder die gemietete Infrastruktur zusammen mit dem unternehmensinternen System zu nutzen. Solche Anbieter sind normalerweise spezialisierte Marktteilnehmer, die sich auf eine physische, komplexe Infrastruktur stützen können, die sich häufig über mehrere geografische Gebiete erstreckt.
- **SaaS (Cloud Software as a Service):** Ein Anbieter liefert verschiedene Anwendungsdienste über das Web und macht sie für den End-Nutzer verfügbar. Mit diesen Diensten sollen häufig konventionelle Anwendungen ersetzt werden, die von den Nutzern auf ihren lokalen Systemen installiert werden müssen. Entsprechend wird von den Nutzern letztendlich erwartet, dass sie ihre Daten an den individuellen Anbieter auslagern. Das ist beispielsweise bei den typischen webbasierten Office-Anwendungen wie Tabellen, Textverarbeitungstools, computergestützten Verzeichnissen und Agenden, gemeinsam genutzten Kalendern usw. der Fall. Die betreffenden Dienste umfassen jedoch auch cloudbasierte E-Mail-Anwendungen.
- **PaaS (Cloud Platform as a Service):** Ein Anbieter bietet Lösungen für die fortgeschrittene Entwicklung und das Hosting von Anwendungen. Diese Dienste werden üblicherweise an Marktteilnehmer gerichtet, die sie nutzen, um eigene, anwendungsbasierte Lösungen zu entwickeln und zu hosten, mit denen betriebsinterne Anforderungen erfüllt und/oder Leistungen an Dritte erbracht werden sollen. Auch hier machen es die von einem PaaS-Anbieter bereitgestellten Dienste unnötig, dass der Anwender sich auf zusätzliche und/oder spezifische Hardware oder Software auf interner Ebene stützt.

Der vollständige Übergang zu einem vollkommen öffentlichen Cloud-System scheint kurzfristig aus verschiedenen Gründen nicht durchführbar zu sein; insbesondere in Bezug auf große Institutionen wie wichtige Unternehmen oder Organisationen, die bestimmte Verpflichtungen zu erfüllen haben wie z. B. große Banken, Regierungsbehörden, große Stadtverwaltungen usw. Das kann hauptsächlich anhand von zwei Gründen erklärt werden: Erstens gibt es einen Faktor mit Eigendynamik, der mit den Investitionen zusammenhängt, die für einen solchen Übergang erforderlich wären, und zweitens müssen die besonders wertvollen und/oder sensiblen Informationen berücksichtigt werden, die in diesen spezifischen Fällen zu verarbeiten sind.

Ein weiterer Faktor, der für die Verwendung von Private Clouds spricht (zumindest in den vorgenannten Fällen), hängt damit zusammen, dass häufig kein öffentlicher Cloud-Anbieter eine Qualität des Dienstes (basierend auf einer Dienstgütevereinbarung) sicherstellen kann, die mit der kritischen Natur des von dem für die Verarbeitung Verantwortlichen bereitzustellenden Dienstes Schritt halten kann - möglicherweise weil die Bandbreite und Verlässlichkeit des Netzes in einem bestimmten Gebiet nicht ausreicht oder nicht angemessen ist oder in Bezug auf spezifische Nutzer-Anbieter-Verbindungen. Andererseits kann man davon ausgehen, dass in einigen der vorgenannten Fällen Private Clouds geleast oder gemietet werden können (da sich dies als kostenwirksamer herausstellen könnte) oder dass hybride Cloud-Modelle (die sowohl Komponenten der Public als auch der Private Cloud umfassen)

genutzt werden können. Die entsprechenden Auswirkungen müssten in allen Fällen sorgfältig abgewogen werden.

Wenn international vereinbarte Standards fehlen, besteht die Gefahr von „do-it-yourself"-Cloud-Lösungen oder zusammengeschlossenen Cloud-Lösungen, die erhöhte Gefahren des Lock-in mit sich brächten (und sogenannter „Privatsphären-Monokulturen") [51] . Eine vollständige Kontrolle über die Daten würde verhindert, ohne dass die Interoperabilität sichergestellt wäre. Tatsächlich sind sowohl die Interoperabilität als auch die Datenportabilität Schlüsselfaktoren für die Entwicklung cloudbasierter Technologien und für die Sicherstellung einer vollständigen Ausübung der Datenschutzrechte, die den betroffenen Personen übertragen wurden (wie das Recht auf Zugang und Berichtigung).

Unter diesem Aspekt gibt die aktuelle Debatte über Cloud-Technologien ein signifikantes Beispiel der Spannung, die zwischen dem kostenorientierten und dem rechteorientierten Ansatz besteht, die kurz im vorstehenden Abschnitt 2 dargelegt wurden. Während es unter Berücksichtigung der spezifischen Umstände der Verarbeitung datenschutzrechtlich gesehen machbar und tatsächlich empfehlenswert sein könnte, sich auf Private Clouds zu stützen, ist dies auf lange Sicht einfach aus Kostengründen für Organisationen vermutlich nicht möglich. Eine sorgfältige Abwägung der auf dem Spiel stehenden Interessen ist erforderlich, da in diesem Bereich derzeit keine Lösung vorgelegt werden kann, die auf alle Situationen passt.

[51] Siehe die Studie des Europäischen Parlaments „Nützlich oder hinderlich? Die Förderung von Innovationen im Internet und das Recht der Bürger auf Schutz der Privatsphäre", veröffentlicht im Dezember 2011.