International Working Group
on Data Protection
in Telecommunications

675.44.10

Arbeitspapier

Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes

– „Sopot Memorandum " –

- Übersetzung -

51. Sitzung, 23.-24. April 2012, Sopot (Polen)

Anwendungsbereich

In diesem Arbeitspapier wird insbesondere die Verarbeitung personenbezogener Daten beim Cloud Computing untersucht.

Nicht betrachtet werden Szenarien, in denen alle Endnutzer, der für die Verarbeitung Verantwortliche, der Auftragsdatenverarbeiter und alle Unterauftragnehmer denselben Datenschutzregeln unterliegen, physisch im selben Hoheitsgebiet angesiedelt sind und jegliche Datenverarbeitung und -speicherung in diesem Hoheitsgebiet erfolgt. Das Arbeitspapier ist ebenfalls weniger relevenat, wenn der Cloud-Dienst unter der vollständigen Kontrolle des Nutzers dieses Dienstes ist.

Schließlich befasst sich das Arbeitspapier nur mit der Nutzung von Cloud-Diensten durch Unternehmen und Behörden, die bestehende Verfahren „in die Cloud" verlagern, und nicht mit der Nutzung dieser Dienste durch Privatpersonen.

Allgemeiner Hintergrund

> *„Cloud Computing ist ein sich entwickelndes Paradigma."* [1]

Cloud Computing (CC) stößt auf wachsendes Interesse, da es eine höhere Wirtschaftlichkeit, geringere Umweltbelastung, einen einfacheren Betrieb, höhere Benutzerfreundlichkeit und eine Reihe weiterer Vorteile verspricht.

Im September 2011 erschien die Sonderveröffentlichung SP 800-145 des National Institute of Standards and Technology (NIST), in der Cloud Computing wie folgt definiert wird:

> *„Cloud Computing ist ein Modell zur Ermöglichung eines ubiquitären, komfortablen, auf Abruf verfügbaren Netzzugriffs auf einen gemeinsamen Pool aus konfigurierbaren Rechenressourcen (z. B. Netze, Server, Speicher, Anwendungen und Dienste), der schnell und mit geringfügigem Verwaltungsaufwand bzw. minimaler Interaktion mit dem Dienstanbieter bereitgestellt und öffentlich verfügbar gemacht werden kann. Das Cloud-Modell besteht aus fünf wesentlichen Charakteristika, drei Service- und vier Nutzungsmodellen."* [2]

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

Unter anderem soll die Definition

> *„als Ausgangspunkt für eine Diskussion darüber dienen, was Cloud Computing ist und wie es am besten genutzt werden kann.“* [3]

Die Definition trägt zu einem besseren Verständnis davon bei, was CC eigentlich ist. Dieses Verständnis entwickelt sich derzeit rasant. Die Definition des NIST ist ein hervorragender Ausgangspunkt für die weitere Untersuchung des CC und seiner Nutzung.

Allerdings gibt es auch immer noch Unklarheiten im Zusammenhang mit CC, insbesondere hinsichtlich des Datenschutzes und anderer rechtlicher Fragen. Die Empfehlungen in diesem Arbeitspapier sollen helfen, diese Unklarheiten zu verringern.

Im ersten Teil werden zunächst die Empfehlungen vorgestellt. Der zweite Teil enthält weitere Hintergrundinformationen über Cloud Computing und Begründungen für die Empfehlungen. Wer sich näher mit dem Thema auseinandersetzen möchte, sollte diesen Teil zuerst lesen.

Für die Zwecke dieses Arbeitspapiers ist der für die Verarbeitung Verantwortliche der Kunde und der Auftragsverarbeiter der Cloud-Anbieter.[4]

Die Entwicklung des CC har eine Reihe wichtiger Themen hervorgehoben, z. B.:

a. Es gibt noch keine internationale Einigung auf eine einheitliche Terminologie;
b. Die Technologie befindet sich noch in der Entwicklung;
c. Riesige Datenmengen werden zusammengetragen und gebündelt;
d. Die Technologie ist grenzenlos und grenzüberschreitend[5];
e. Daten werden weltweit verarbeitet;
f. Die Prozesse, Verfahren und Methoden der Cloud-Anbieter sind nicht ausreichend transparent, z. B. ob Cloud-Anbieter Unteraufträge für die Verarbeitung vergeben und wenn ja, welche Prozesse, Verfahren und Methoden diese verwenden;
g. Dieser Mangel an Transparenz erschwert eine angemessene Risikobewertung.
h. Aufgrund dieses Mangels an Transparenzist es auch schwerer, Datenschutzregeln durchzusetzen.
i. Die Cloud-Anbieter stehen unter einem großen Druck, möglichst schnell Kapital aus den hohen Investitionskosten zu schlagen.
j. Die Kunden stehen unter einem zunehmenden, teilweise der weltweiten Finanzkrise geschuldeten Druck, die Kosten auch für ihre Datenverarbeitung zu senken.
k. Um die Preise niedrig zu halten, sind Cloud-Anbieter eher bereit, allgemeine Geschäftsbedingungen anzubieten.

Daraus können sich folgende **Risiken** ergeben:

A. Verletzungen der Informationssicherheit, wie die Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von (personenbezogenen) Daten werden vom Verantwortlichen für die Verarbeitung nicht erkannt.
B. Daten werden in Hoheitsgebiete übertragen, die keinen angemessenen Datenschutz gewährleisten.
C. Verstöße gegen Gesetze und Grundsätze des Schutzes der Privatsphäre und des Datenschutzes.
D. Der für die Verarbeitung Verantwortliche akzeptiert allgemeine Geschäftsbedingungen, die dem Cloud-Anbieter zu viel Spielraum lassen, u. a. die Möglichkeit, Daten entgegen den Anweisungen des für die Verarbeitung Verantwortlichen zu verarbeiten.

E. Verwendung von Daten des für die Verarbeitung Verantwortlichen für eigene Zwecke ohne Wissen oder Erlaubnis des für die Verarbeitung Verantwortlichen durch Cloud-Anbieter oder ihre Unterauftragnehmer.
F. Die Rechenschaftspflicht und Verantwortung wird in einer Kette von Unterauftragnehmern scheinbar ausgehöhlt oder verschwindet.
G. Der für die Verarbeitung Verantwortliche verliert die Kontrolle über die Daten und die Datenverarbeitung.
H. Der für die Verarbeitung Verantwortliche oder ein vertrauenswürdiger Dritter (z. B. Prüfer) ist nicht in der Lage, den Cloud-Anbieter angemessen zu kontrollieren.
I. Datenschutzbehörden werden davon abgehalten, die Verarbeitung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen und den Cloud-Anbieter angemessen zu überwachen.
J. Der für die Verarbeitung Verantwortliche verlässt sich aufgrund mangelnder Informationen und Überwachung auf ungerechtfertigtes Vertrauen und verstößt dadurch möglicherweise gegen geltendes Datenschutzrecht im Niederlassungsland.

Die **folgenden Empfehlungen** sollen zur **Verringerung der Risiken bei der Nutzung von Cloud-Diensten beitragen und verantwortungsvolles Handeln fördern**[6], so dass die Vorteile der Verwendung von CC genutzt werden können, jedoch nicht auf Kosten der Rechte des Einzelnen.

Empfehlungen[7]

Allgemeine Empfehlungen

Die Arbeitsgruppe empfiehlt, dass:

- durch Cloud Computing Datenschutzstandards im Vergleich zur herkömmlichen Datenverarbeitung nicht abgesenkt werden dürfen;
- die für die Verarbeitung Verantwortlichen vor dem Einstieg in CC-Projekte eine Abschätzung der Folgen für den Datenschutz und eine Risikoabschätzung vornehmen (ggf. mithilfe vertrauenswürdiger Dritter).
- Anbieter von Cloud-Diensten ihre Verfahren weiterentwickeln, um mehr Transparenz, Sicherheit, Nachprüfbarkeit und Vertrauen in CC-Lösungen zu schaffen, insbesondere im Hinblick auf Informationen über mögliche Verstöße gegen den Datenschutz und ausgewogenere Vertragsbedingungen zur Förderung der Portabilität von Daten und der Kontrolle über die Datendurch die Cloud-Nutzer.
- Weitere Bemühungen in der Forschung, der Zertifizierung durch Dritte, der Standardisierung, von „Privacy by Design“-Technologien und anderen damit verbundenen Bereichen unternommen werden, um das gewünschte Vertrauen in CC zu erreichen.
- Gesetzgeber überprüfen, ob das bestehende Recht zur grenzüberschreitenden Datenübertragung weiterhin angemessen ist, und zusätzliche Datenschutzvorkehrungen im Bereich des CC in Erwägung ziehen[8].
- Datenschutzbehörden die für die Verarbeitung Verantwortlichen, Cloud-Anbieter und Gesetzgeber weiterhin über Fragen des Schutzes der Privatsphäre und des Datenschutzes informieren.

Weitere Hinweise zu bewährten Verfahren („best practices“)

1. CC sollte in sorgfältigen, maßvollen Schritten umgesetzt werden, beginnend mit nicht-sensiblen und nicht-vertraulichen Daten.

2. Die Verarbeitung sensitiver[9] Daten über CC stößt auf zusätzliche Bedenken. Unbeschadet nationaler Gesetze erfordert diese Art der Verarbeitung zusätzliche Schutzmaßnahmen.

3. Für die Verarbeitung Verantwortliche und Datenschutzbehörden sollten Zugang zu **standortbezogenen Audit Trails** haben. Der Audit Trail sollte automatisch aufgezeichnet werden und anzeigen, an welchen physischen Standorten personenbezogene Daten zu welchen Zeitpunkten gespeichert oder verarbeitet wurden[10].

4. Ein **automatisch aufgezeichneter Audit Trail über Kopier- und Löschvorgänge sollte** eingerichtet werden, anhand dessen eindeutig erkennbar ist, welche Kopien personenbezogener Daten der Auftragsverarbeiter oder seine Unterauftragnehmer angelegt und gelöscht haben.

5. Die Audit Trails zur Protokollierung des Standorts sowie der Kopier- und Löschvorgänge sollten auch die Datensicherung umfassen.

6. Wirksame technische Maßnahmen sollten entwickelt werden, um eine rechtswidrige Übertragung personenbezogener Daten in Hoheitsgebiete ohne ausreichenden Datenschutz zu verhindern.

7. Es sollte sichergestellt werden, dass personenbezogene Daten wirksam von Laufwerken und anderen Speichermedien **gelöscht** werden, z. B. durch **sofortiges Überschreiben mit Zufallsdaten[11]**.

8. Es sollte sichergestellt sein, dass ruhende Daten und die Datenübertragung[12] mithilfe anerkannter Standardalgorithmen und aktueller Schlüssellängen **verschlüsselt** werden. Die Schlüssel sollten von keinem anderen als dem für die Verarbeitung Verantwortlichen und den Cloud-Anbieter verwendet werden und nur diesen zugänglich sein. Die Schlüssel sollten nicht von anderen Kunden als denen des Cloud-Anbieters verwendet werden oder diesen zugänglich sein. Daten sollten nicht länger und in größerem Umfang in unverschlüsselter Form zugänglich sein als für die jeweilige Datenverarbeitung unbedingt nötig. Methoden, mit deren Hilfe Daten für CC-Anbieter zu jeder Zeit unlesbar gemacht werden können, sollten weiter untersucht werden[13]. Es könnte nützlich sein, Möglichkeiten zu erkunden, wie der für die Verarbeitung Verantwortliche die Entschlüsselung von Daten durch den Cloud-Anbieter und seine Unterauftragnehmer wirksam und schnell unterbinden kann (Notbremse).

9. Alle Verwendungen personenbezogener Daten durch Cloud-Anbieter und ihre Unterauftragnehmer sollten automatisch **protokolliert** werden. Das Protokoll sollte für den für die Verarbeitung Verantwortlichen leicht zugänglich sowie einfach und leicht verständlich gestaltet sein. Der Cloud-Anbieter und seine Unterauftragnehmer sollten die Integrität der Protokolle gewährleisten.

Verantwortliche für die Verarbeitung

10. Der für die Verarbeitung Verantwortliche sollte in die Vereinbarung mit dem Cloud-Anbieter eine vollständige Liste mit Informationen über alle physischen Standorte aufnehmen, an denen über die Laufzeit der Vereinbarung Daten durch den Cloud-Anbieter und/oder seine Unterauftragnehmer gespeichert oder verarbeitet werden, einschließlich zur Datensicherung (**Grundsatz der Standorttransparenz**).

11. Der für die Verarbeitung Verantwortliche sollte in der Vereinbarung sicherstellen, dass weder der Cloud-Anbieter noch seine Unterauftragnehmer, ungeachtet ihrer Gründe und ob die Da-

ten verschlüsselt werden, Daten an andere Standorte als die im Vertrag aufgelisteten übertragen. Dies sollte von technischen Maßnahmen begleitet werden, deren Vorhandensein und Zuverlässigkeit der für die Verarbeitung Verantwortliche tatsächlich prüfen kann.

12. Der für die Verarbeitung Verantwortliche sollte dafür sorgen, dass die Vereinbarung mit dem Cloud-Anbieter unmissverständlich ist und keine Auslegungen zulässt, die den Grundsatz untergräbt, dass der Cloud-Anbieter personenbezogene Daten nur entsprechend den Weisungen des für die Verarbeitung Verantwortlichen verarbeitet. Können Cloud-Anbieter die Vereinbarung einseitig ändern, sollte der für die Verarbeitung Verantwortliche das Recht haben, den Vertrag zu kündigen und die Daten an einen anderen Cloud-Anbieter zu übertragen.

13. Die Vereinbarung sollte ausdrücklich regeln, dass der Cloud-Anbieter die Daten des für die Verarbeitung Verantwortlichen nicht für seine eigenen Zwecke nutzen darf.

14. Der für die Verarbeitung Verantwortliche sollte die Möglichkeit haben, alle Standorte, an denen personenbezogene Daten ganz oder teilweise verarbeitet werden, in der Vergangenheit verarbeitet wurden oder gemäß der Vereinbarung in Zukunft verarbeitet werden, zu prüfen oder prüfen zu lassen. Die Vereinbarung sollte festlegen, dass der für die Verarbeitung Verantwortliche das Recht hat, vollständige Informationen über alle Aspekte des Cloud-Anbieters und seiner Unterauftragnehmer zu erhalten, die der für die Verarbeitung Verantwortliche als notwendig erachtet, um die Einhaltung der Vereinbarung zu gewährleisten, d. h. zu gewährleisten, dass die Verarbeitung personenbezogener Daten in Einklang mit den Weisungen und geltendem Recht sowie auf angemessen sichere Art und Weise erfolgt.

15. Der für die Verarbeitung Verantwortliche sollte sich in der Vereinbarung das Recht sichern, die Verarbeitung personenbezogener Daten durch den Cloud-Anbieter und ggf. seine Unterauftragnehmer durch einen vertrauenswürdigen Dritten (z. B. ein anerkanntes Prüfunternehmen)[14] vollständig oder teilweise überwachen zu lassen.

16. Vor dem Einsatz von CC sollte der für die Verarbeitung Verantwortliche auf der Grundlage seiner Informationen über die Bedingungen und Umstände, unter denen personenbezogene Daten vom Cloud-Anbieter und ggf. seinen Unterauftragnehmern verarbeitet werden, eine **Risikoabschätzung** vornehmen. Die Risikoabschätzung sollte alle Standorte umfassen, an denen personenbezogene Daten verarbeitet oder gespeichert werden. Setzt der Cloud-Anbieter für Teile der Verarbeitung Unterauftragnehmer ein, sollte die Risikoabschätzung auch alle Standorte der Unterauftragnehmer umfassen.

17. Der für die Verarbeitung Verantwortliche sollte die Risikoabschätzung regelmäßig überprüfen und aktualisieren, solange personenbezogene Daten vom Cloud-Anbieter verarbeitet werden.

18. Vor dem Einsatz von CC sollte der für die Verarbeitung Verantwortliche versuchen sicherzustellen, dass ein Ausstieg aus dem Cloud-Dienst tatsächlich möglich ist, wozu auch eine aktive Rolle des Cloud-Anbieters beim Transfer der Daten zählt, um nicht von einem Cloud-Anbieter abhängig zu werden (Lock-in-Effekt).

19. Der für die Verarbeitung Verantwortliche sollte prüfen, ob es notwendig ist, sich den Zugriff auf mindestens eine nutzbare Kopie der Daten außerhalb der Kontrolle, des Zugriffs oder des Einflusses des Cloud-Anbieters (und seiner Unterauftragnehmer) zu sichern. Falls ja, sollte die Kopie unabhängig von der Mitwirkung des Cloud-Anbieters und seiner Unterauftragnehmer für den Verantwortlichen für die Verarbeitung zugänglich und nutzbar sein.

20. Der für die Verarbeitung Verantwortliche sollte im Falle eines **Verletzung der Datensicherheit** seine Verpflichtungen gegenüber den Betroffenen und den Datenschutzbehörden voll-

ständig erfüllen und geeignete Maßnahmen ergreifen können. Von daher sollte der für die Verarbeitung Verantwortliche klare Vereinbarungen mit dem Cloud-Anbieter über die umgehende und umfassende Benachrichtigung des für die Verarbeitung Verantwortlichen und/oder der Datenschutzbehörde im Falle einer solchen Verletzung treffen.

21. Der für die Verarbeitung Verantwortliche sollte den Cloud-Anbieter vertraglich dazu verpflichten, wirksame und schnelle Verfahren umzusetzen, damit die Betroffenen ihr Recht auf Auskunft, Berichtigung, Löschung oder Sperrung von Daten wahrnehmen können.

Cloud-Anbieter

22. Der Cloud-Anbieter sollte gegenüber dem für die Verarbeitung Verantwortlichen vollständige Transparenz bezüglich der von ihm und ggf. seinen Unterauftragnehmern verwendeten Standorte für die Verarbeitung und Speicherung personenbezogener Daten gewährleisten.

23. Der Cloud-Anbieter sollte vollständige Transparenz bezüglich seiner Unterauftragnehmer und der von ihnen durchgeführten Verarbeitungsprozesse gewährleisten.

24. Der Cloud-Anbieter sollte Transparenz in Vertragsfragen gewährleisten und CC nicht mit allgemeinen Geschäftsbedingungen anbieten, die einseitige Vertragsänderungen ermöglichen.

25. Cloud-Anbieter und ggf. ihre Unterauftragnehmer werden ermutigt, sich nach bewährten Verfahren zu richten und es einem unparteiischen Dritten zu erlauben, sie zu vergleichen und zu bewerten (Benchmarking).

26. Allgemeine Geschäftsbedingungen für bestimmte Marktsegmente, z. B. kleine und mittelständische Unternehmen, sollten so gestaltet sein, dass die Achtung der Privatsphäre und angemessene Schutzmaßnahmen berücksichtigt werden.

Prüfungen

27. Da ein Cloud-Anbieter sehr große Mengen an personenbezogenen Daten ansammeln kann, sollte der Cloud-Anbieter im Interesse des für die Verarbeitung Verantwortlichen zusätzlich zu dessen Prüfungen auch von einer dritten Stelle überprüft werden. Der Prüfer sollte vollkommen unabhängig vom Cloud-Anbieter sein und der Sicherheit der Verarbeitung personenbezogener Daten besondere Aufmerksamkeit schenken. Der Prüfer sollte insbesondere prüfen, ob Maßnahmen in den folgenden Bereichen ergriffen wurden und ordnungsgemäß funktionieren: standortbezogener Audit Trail (vgl. Nr. 3), Audit Trails für das Kopieren und Löschen (vgl. Nr. 4), Löschung (vgl. Nr. 7) und Protokollierung (vgl. Nr. 9). Ferner sollte der Prüfer prüfen, ob folgende Maßnahmen ergriffen wurden und ordnungsgemäß funktionieren: Maßnahmen zur Verhütung der rechtswidrigen Datenübertragung in Hoheitsgebiete ohne ausreichenden Datenschutz (vgl. Nr. 6) und Maßnahmen zur Verhütung der Datenübertragung an andere Standorte als die ausdrücklich mit dem Kunden vereinbarten (vgl. Nr. 10 und 11). Schließlich sollte der Prüfer sicherstellen, dass es dem Cloud-Anbieter oder ggf. seinen Unterauftragnehmern nicht möglich ist, diese Maßnahmen unentdeckt zu umgehen.

Hintergrundinformationen zu den Empfehlungen

28. CC ist eine recht **neue Form** der Datenverarbeitung, die sich aus der mangels einer besseren Benennung **traditionelle Datenverarbeitung** genannten Form der Datenverarbeitung entwickelt hat. Es hat sich eine langjährige, solide Erfahrung mit der traditionellen Datenverarbeitung angesammelt, doch gibt es keine derartige solide Erfahrung mit CC.

29. Die Folge dieses **Paradigmenwechsels** ist, dass Grundannahmen, Erfahrungen, Ideen, Theorien und Modelle für die Datenverarbeitung nicht mehr mit der Praxis übereinstimmen und daher einer kritischen Prüfung, Neubewertung und ggf. Überarbeitung unterzogen werden müssen. Dies trifft auch auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten sowie die Art und Weise zu, wie **Risiken** analysiert, bewertet und beurteilt werden können. Die bewährten Verfahren von gestern sind nicht unbedingt die bewährten Verfahren von heute.

30. Die **neue Situation** muss untersucht und in **sorgfältig gewählten Schritten** umgesetzt werden, insbesondere hinsichtlich des Datenschutzes und des Schutzes der Rechte der Betroffenen im weiteren Sinne.

31. Die **technische Grundlage** des CC ist eine ausgereifte Netzwerktechnik und Server-Virtualisierung. Dies ermöglicht eine schnelle und dynamische Verlagerung von Daten und deren Verarbeitung lokal zwischen Servern im jeweiligen Rechenzentrum und global zwischen Servern in weltweiten Rechenzentren. Die Technologie ist hochgradig skalierbar, ohne einschränkende Engpässe zu erzeugen. Das Internet ermöglicht es dem Endnutzer, unabhängig vom Standort der Rechenzentren auf die Daten zuzugreifen.

32. Die **wirtschaftliche Antriebskraft** hinter CC sind **Skaleneffekte**. Die Zusammenfassung der Datenverarbeitung in großen Zentren verbessert die Nutzung teurer Ressourcen, wie z. B. menschlichem Wissen, Sachwerten (Hardware, Software, Gebäude), von Kommunikationsbandbreite und Energie. Aufgrund ihrer Größe und ihres Volumens haben Cloud-Anbieter zudem eine besonders starke Verhandlungsposition beim Erwerb von Ressourcen. Somit können Cloud-Anbieter Stückkosten reduzieren und den Kunden attraktive Preise anbieten. Um Skaleneffekte erzielen zu können, müssen möglichst viele Kunden den Dienst nutzen. Um ein ausreichendes **Volumen** zu erreichen, werden Cloud-Dienste weltweit über das Internet angeboten.

33. CC gilt als große Chance für kleine und mittelständische Unternehmen, Zugang zu bezahlbaren und skalierbaren Rechenressourcen zu erhalten. Aufgrund der großen Anzahl relativ kleiner Organisationen wird erwartet, dass Cloud-Anbieter allgemeine Geschäftsbedingungen für dieses Marktsegment entwickeln.

34. CC ist viel dynamischer als die traditionelle Datenverarbeitung. Der Standort, an dem Daten verarbeitet werden, kann sich stark verändern. Der aktuelle Standort von Daten und ihrer Verarbeitung kann von verschiedenen Faktoren abhängen, über die sich Endnutzer und für die Verarbeitung Verantwortliche bisher wenig Gedanken gemacht haben und über die sie unter Umständen wenig wissen und wenig Kontrolle haben. Beispielsweise siedeln Cloud-Anbieter ihre Datenzentren häufig in verschiedenen Ländern und auf mehreren Kontinenten an, u. a. aufgrund einer günstigen Stromversorgung, eines kühlen Klimas und unterschiedlicher Zeitzonen. Unvorhersehbare Umstände, z. B. Ausfälle in einem Rechenzentrum oder ein Kapazitätsmangel bei Spitzenlasten (Überlauf), können auch Einfluss auf den aktuellen Standort von Daten haben. Kopien von Daten können an andere Datenzentren übertragen werden, um die Online-Verfügbarkeit im Falle von Störungen in einem Datenzentrum zu gewährleisten oder Sicherungskopien zu erstellen (Redundanz).

35. CC beruht auf vielen Kunden, die dynamisch einen gemeinsamen Pool an Ressourcen des Cloud-Anbieters nutzen. Dies sollte jedoch nur geschehen, wenn eine **klare Trennung** der

verschiedenen Kundendaten und ihrer Verarbeitung aufrechterhalten werden kann. Die gemeinsame Nutzung von Ressourcen birgt ein höheres Risiko für umfangreiche Verluste oder die unbefugte Offenlegung von Daten.[15] Das Risiko erhöht sich auch dadurch, dass CC von der Kostenoptimierung durch ein großes Datenvolumen angetrieben wird (Skaleneffekt). Cloud-Kunden stellen ein Risiko für einander dar. Je mehr Kunden auf dieselben Ressourcen zugreifen, desto größer wird das Risiko für jeden einzelnen Kunden und somit für alle Cloud-Kunden zusammen.

36. Das Wissen über CC und Informationen über seine Risiken konzentrieren sich derzeit auf einige wenige große Cloud-Anbieter, die anscheinend aus wirtschaftlichen oder wettbewerblichen Gründen nur zögerlich Informationen über bestimmte Bedingungen und Umstände an die Öffentlichkeit weitergeben. Die ungleiche Verteilung von Wissen und Informationen zwischen Cloud-Anbietern und Kunden versetzt letztere in eine schwächere Position beim Abschluss von Vereinbarungen und erschwert es ihnen, die Risiken der beabsichtigten Nutzung von CC angemessen zu bewerten.

37. Eine gründliche **Risikoabschätzung** muss auf **dem Verständnis des** konkreten Aufbaus und der konkreten Umstände des Cloud-Dienstes an allen Standorten beruhen, an denen Daten verarbeitet werden.

38. Die CC-Technologie ist **grenzenlos** und **grenzüberschreitend**. Der weltweite Kundenstamm, gepaart mit der weltweiten Verteilung von Rechenzentren und dem dynamischen Strom von Daten (und von Datenverarbeitung) kann dazu führen, dass Daten nationale Grenzen überschreiten und Hoheitsgebiete mit einem damit einhergehenden Mangel an Transparenz wechseln. Personenbezogene Daten können in Datenzentren in Hoheitsgebieten ohne angemessenen Datenschutz gelangen oder kommerziell missbraucht werden, oder ausländische Mächte greifen ohne Berechtigung darauf zu[16].

39. Im Sinne des Datenschutzes muss zwischen den einander ausschließenden Rollen des für die Verarbeitung Verantwortlichen und des Auftragsdatenverarbeiters unterschieden werden. Der **für die Verarbeitung Verantwortliche** legt den Zweck und die Mittel für einen bestimmten Vorgang der Datenverarbeitung fest.

40. Allgemein anerkannt ist auch, dass ein für die Verarbeitung Verantwortlicher die Verarbeitung personenbezogener Daten durch einen **Auftragsdatenverarbeiter** erlauben kann, dies jedoch nur in Einklang mit den ausdrücklichen **Weisungen** des für die Verarbeitung Verantwortlichen.

41. Ein allgemein anerkannter Grundsatz des Datenschutzes ist, dass der Auftragsdatenverarbeiter personenbezogene Daten nicht in größerem Umfang verarbeiten darf, als sich aus den ausdrücklichen Weisungen des für die Verarbeitung Verantwortlichen ableiten lässt[17]. Für das CC bedeutet dies, dass ein Cloud-Anbieter keine einseitige Entscheidung treffen oder die mehr oder weniger automatische Übertragung personenbezogener Daten (und ihrer Verarbeitung) an unbekannte Rechenzentren veranlassen kann. Dies gilt unabhängig davon, ob der Cloud-Anbieter eine solche Übertragung mit der Verringerung der Betriebskosten, der Bewältigung von Spitzenlasten (Überlauf), der Lastenverteilung, der Erstellung von Sicherungskopien usw. begründet. Noch darf der Cloud-Anbieter personenbezogene Daten für seine eigenen Zwecke nutzen[18].

42. Ein weiterer allgemein anerkannter Grundsatz des Datenschutzes erfordert, dass der für die Verarbeitung Verantwortliche geeignete **technische und organisatorische Sicherheitsmaßnahmen** ergreift, um Daten vor versehentlicher oder rechtswidriger Zerstörung, Verlust oder Schädigung, sowie vor unbefugter Offenlegung, Missbrauch oder anderen Arten der

Verarbeitung, die gegen gesetzliche Bestimmungen verstoßen, zu schützen. Dasselbe gilt für Auftragsdatenverarbeiter.

43. Um seiner Verantwortung gerecht zu werden, muss der für die Verarbeitung Verantwortliche die Verarbeitung durch den Auftragsdatenverarbeiter **überwachen**, um sicherzustellen, dass sie entsprechend seiner Anweisungen erfolgt und dabei angemessene Sicherheitsmaßstäbe eingehalten werden.

44. Ohne seine Verantwortung abzutreten kann der für die Verarbeitung Verantwortliche ausdrückliche Anweisungen geben, dass die Überwachung der Verarbeitung durch den Auftragsverarbeiter teilweise von einem **vertrauenswürdigen Dritten** (z. B. einem Prüfer) übernommen wird. Bedingung ist, dass der Dritte über die notwendigen Qualifikationen verfügt, unabhängig vom Auftragsverarbeiter ist, vollen Zugang zu und vollständigen Einblick in die Bedingungen und Umstände der Verarbeitung durch den Auftragsverarbeiter hat und dem für die Verarbeitung Verantwortlichen zuverlässig über seine Beobachtungen, Bewertungen und Schlussfolgerungen berichten kann.

Die Arbeitsgruppe wird die Entwicklungen im Bereich des Cloud Computing weiter verfolgen und das vorliegende Arbeitspapier ggf. aktualisieren.

Anmerkungen

[1] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Seite 2.
[2] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Seite 3.
[3] National Institute of Standards and Technology (NIST), Special Publication 800-145, *The NIST Definition of Cloud Computing*, September 2011, Seite 2.
[4] Vgl. Nr. 39 und 40 unten. Die Unterauftragnehmer des Cloud-Anbieters gelten im Zusammenhang mit der Verarbeitung personenbezogener Daten ebenfalls als Auftragsverarbeiter.
[5] Vgl. Nr. 38
[6] Auf den Seiten 9 und 10 ihres Berichts *Cloud Computing – Benefits, risks and recommendations for information security* [Cloud Computing: Nutzen, Risiken und Empfehlungen zur Informationssicherheit] vom November 2009 nennt die ENISA die häufigsten Sicherheitsrisiken. Dazu zählen in zufälliger Reihenfolge: Kontrollverlust, Abhängigkeit von einem Anbieter (Lock-in-Effekt), fehlende Isolation, Datenschutz, unsichere oder unvollständige Löschung von Daten, interne Angreifer. Weitere Einzelheiten können dem Bericht entnommen werden. Hier wird der Kontrollverlust betont.
[7] Die Liste der Empfehlungen ist nicht abschließend.
[8] Vgl. Internationale Konferenz der Beauftragten für den Datenschutz und die Privatsphäre: Entschließung über Internationale Standards zum Schutz der Privatsphäre („Entschließung von Madrid“), 5. November 2009; http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf
[9] Der Begriff der sensitiven Daten ist in verschiedenen Rechtskulturen unterschiedlich besetzt: vgl. Art. 8 der Richtlinie 95/46/EG, Art. 9 des Entwurfs der Datenschutzverordnung sowie den FTC-Bericht „Protecting Comsumer Privacy in an Era of Rapid Change“ (2012).
[10] Der standortbezogene Audit Trail könnte beispielsweise eine klare Übersicht darüber geben, wann die einzelnen personenbezogenen Daten an bestimmten Standorten ein- und ausgetragen wurden und wann sie zu welchen Standort übertragen werden.
[11] Eine Löschung durch Dereferenzierung der Daten und späteres Überschreiben durch Wiederverwendung der Speicherbereiche reicht in der Regel nicht aus, da weiterhin die Möglichkeit besteht, dass Daten vor oder während der Wiederverwendung der Speicherbereiche durch erneute Referenzierung wieder zugänglich werden.
[12] Während der Datenübertragung sollte eine Ende-zu-Ende-Verschlüsselung erfolgen. Es muss sichergestellt sein, dass personenbezogene Daten während der Übertragung gegen aktive (z. B. Replays, Traffic Injection)

und passive Angriffe (z. B. Belauschen) geschützt sind. Ferner muss der Datenzugriff durch unbefugte Dritte mithilfe entsprechender technischer und organisatorischer Verfahren verhindert werden (z. B. Zugangskontrolle, Datenverschlüsselung).

[13] Ein Forschungsbeispiel in diesem Bereich ist die Sealed Cloud, welche im Preprint des Artikels von Hubert A. Jäger und Arnold Monitzer „Sealed Cloud - a novel approach to defend insider attacks“ beschrieben ist. Der Preprint kann unter der folgenden Adresse aufgerufen werden http://uniscon.de/pdf/Sealed_Cloud_Jaeger_Monitzer.pdf.

[14] Das Thema vertrauenswürdige Dritte ist in Nr. 44 näher beschrieben.

[15] Auf den Seiten 9 und 10 ihres Berichts *Cloud Computing – Benefits, risks and recommendations for information security* [Cloud Computing: Nutzen, Risiken und Empfehlungen zur Informationssicherheit] vom November 2009 nennt die ENISA die häufigsten Sicherheitsrisiken. Dazu zählen in zufälliger Reihenfolge: Kontrollverlust, Abhängigkeit von einem Anbieter (Lock-in-Effekt), fehlende Isolation, Datenschutz, unsichere oder unvollständige Löschung von Daten, interne Angreifer. Weitere Einzelheiten können dem Bericht entnommen werden. An dieser Stelle sei darauf hingewiesen, dass fehlende Isolation als eines der größten Risiken angesehen wird.

[16] Zwar können personenbezogene Daten in einem Hoheitsgebiet verarbeitet werden, doch kann der Cloud-Anbieter oder das Mutterunternehmen in einem anderen Hoheitsgebiet angesiedelt sein, was es ausländischen Strafverfolgungsbehörden ermöglichen würde, auf die Daten im Cloud-Dienst zuzugreifen, auch wenn die Daten physisch außerhalb der geografischen Grenzen dieses Landes gespeichert sind. Hierzu könnte der Abschluss eines internationalen Abkommens notwendig sein.

[17] Oder durch Gesetz.

[18] Verarbeiten Cloud-Anbieter Daten ohne Wissen des für die Verarbeitung Verantwortlichen, sollte der Cloud-Anbieter als Mitverantwortlicher für die Verarbeitung angesehen und als solcher für die unbefugte, unabhängige Datenverarbeitung zur Rechenschaft gezogen werden.