Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE -

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1],

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 41[2],

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG

I.1. Ziel der Stellungnahme

1. In Anbetracht der Bedeutung des Cloud Computing in der sich entwickelnden Informationsgesellschaft sowie der bereits stattfindenden politischen Debatte innerhalb der EU über das Cloud Computing hat der EDSB beschlossen, die vorliegende Stellungnahme auf eigene Initiative herauszugeben.

2. Diese Stellungnahme ist als Reaktion auf die Mitteilung der Kommission „Freisetzung des Cloud-Computing-Potenzials in Europa“ vom 27. September 2012 (nachstehend „die Mitteilung“)[3], zu verstehen, in der Schlüsselaktionen und politische Schritte dargelegt werden, mit denen sich die Nutzung von Cloud-Computing-Diensten in Europa beschleunigen lässt. Der EDSB wurde vor der Annahme der Mitteilung informell konsultiert und gab informelle Kommentare ab. Er begrüßt, dass einige seiner Kommentare in die Mitteilung eingeflossen sind.

[1] ABl. L 281 vom 23.11.1995, S. 31.
[2] ABl. L 8 vom 12.1.2001, S. 1.
[3] COM(2012) 529 final.

3. In Anbetracht des Umfangs und der Bedeutung der derzeitigen Debatte über die Beziehung zwischen Cloud Computing und Datenschutzrechtsrahmen beschränkt sich die vorliegende Stellungnahme allerdings nicht auf die in der Mitteilung behandelten Themen.

4. Im Mittelpunkt der Stellungnahme stehen die Herausforderungen, die das Cloud Computing für den Datenschutz bedeutet, sowie die Art und Weise, in der die vorgeschlagene Datenschutzverordnung („vorgeschlagene Verordnung“)[4] damit umgeht. Des Weiteren äußert sie sich zu den Bereichen, in denen laut Mitteilung ein weiteres Tätigwerden erforderlich ist.

I.2. Hintergrund

5. Vor dem Hintergrund der allgemeinen politischen Debatte in der EU über Cloud Computing kommt folgenden Tätigkeiten und Dokumenten besondere Bedeutung zu:

- Im Anschluss an ihre Mitteilung von 2010 über die digitale Agenda für Europa[5] führte die Kommission vom 16. Mai bis 31. August 2011 eine öffentliche Konsultation über Cloud Computing durch, deren Ergebnisse am 5. Dezember 2011 veröffentlicht wurden[6];

- am 1. Juli 2012 nahm die Artikel-29-Datenschutzgruppe[7] eine Stellungnahme zum Cloud Computing an („Stellungnahme der Artikel 29-Datenschutzgruppe“)[8], in der die Anwendung der derzeitigen Datenschutzvorschriften in der Richtlinie 95/46/EG auf im Europäischen Wirtschaftsraum (EWR) tätige Anbieter von Cloud-Computing-Diensten und ihre Kunden analysiert werden[9];

- am 26. Oktober 2012 verabschiedeten die Datenschutzbeauftragten auf ihrer 34. Internationalen Konferenz eine Entschließung zum Thema Cloud Computing[10].

---

[4] COM(2012) 11 final.
[5] KOM(2010) 245 endgültig.
[6] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf
[7] Die Artikel-29-Datenschutzgruppe ist ein gemäß Artikel 29 der Richtlinie 95/46/EG eingerichtetes beratendes Gremium. Sie besteht aus Vertretern der nationalen Aufsichtsbehörden und des EDSB sowie einem Vertreter der Kommission.
[8] Artikel-29-Datenschutzgruppe, Stellungnahme 05/2012 zum Cloud Computing, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf.
[9] Außerdem haben nationale Datenschutzbehörden in mehreren Mitgliedstaaten eigene Leitfäden zum Thema Cloud Computing herausgegeben; dazu gehören Italien, Schweden, Dänemark, Deutschland, Frankreich und das Vereinigte Königreich.
[10] Entschließung zum Thema Cloud Computing, angenommen auf der 34. Internationalen Konferenz der Datenschutzbeauftragten, Uruguay, 26. Oktober 2012.

I.3. Mitteilung über Cloud Computing

6. Der EDSB begrüßt die Mitteilung. Sie nennt drei konkrete Schlüsselaktionen, die auf EU-Ebene erforderlich sind, um die Nutzung des Cloud Computing in Europa zu begleiten und zu fördern, und zwar
   - Schlüsselaktion 1: Lichten des Normendschungels
   - Schlüsselaktion 2: Sichere und faire Vertragsbedingungen
   - Schlüsselaktion 3: Aufbau einer Europäischen Cloud-Partnerschaft zur Förderung der Innovation und des Wachstums durch den öffentlichen Sektor.

7. Darüber hinaus sind weitere politische Maßnahmen vorgesehen, so z. B. die Förderung der Nutzung des Cloud Computing durch Unterstützung von Forschung und Entwicklung oder Sensibilisierung sowie die erforderliche Behandlung zentraler Fragen im Zusammenhang mit Cloud-Diensten – dazu gehören Datenschutz, Zugang für Strafverfolgungsbehörden, Sicherheit, Verantwortlichkeit der Vermittler (Dienstleister) – in einem intensiveren internationalen Dialog.

8. Der Datenschutz wird in der Mitteilung als wesentliches Element erwähnt, das den Erfolg der Einführung des Cloud Computing in Europa gewährleistet. In der Mitteilung heißt es[11], dass der Verordnungsvorschlag viele Bedenken aufgreift, die von Anbietern von Cloud-Diensten und von Cloud-Anwendern[12] geäußert worden sind.

1.4. Schwerpunkt und Struktur der Stellungnahme

9. Die vorliegende Stellungnahme verfolgt drei Ziele.

10. Erstens möchte sie die Relevanz des Schutzes der Privatsphäre und des Datenschutzes in den aktuellen Diskussionen über Cloud Computing unterstreichen. So weist sie insbesondere darauf hin, dass das Datenschutzniveau in einer Cloud-Computing-Umgebung nicht niedriger sein darf als in jedem anderen Datenverarbeitungsumfeld. Cloud Computing kann nur weiterentwickelt und rechtmäßig angewandt werden, wenn es gewährleistet, dass dieses Datenschutzniveau gewahrt wird (siehe Kapitel III.3). Die Stellungnahme berücksichtigt hier die Orientierungshilfen in der Stellungnahme der Artikel-29-Datenschutzgruppe.

11. Zweitens sollen die größten Herausforderungen näher analysiert werden, die das Cloud Computing vor dem Hintergrund der vorgeschlagenen Datenschutzverordnung mit sich bringt, insbesondere die Schwierigkeit, eindeutig die Verantwortlichkeiten der einzelnen Beteiligten und die Begriffe des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters festzulegen. Die Stellungnahme untersucht (im Wesentlichen in Kapitel IV), wie der Verordnungsvorschlag in seiner jetzigen Fassung[13], dazu beitragen könnte, bei

---

[11] Siehe S. 8 der Mitteilung, Abschnitt „Vertrauensbildung im digitalen Umfeld".

[12] Der Begriff „Cloud-Anwender" wird in dieser Stellungnahme im Allgemeinen als Bezeichnung für Kunden verwendet, die in ihrer Eigenschaft als Unternehmen handeln, und für Verbraucher, die in ihrer Eigenschaft als individuelle Endbenutzer handeln.

[13] Es sollte berücksichtigt werden, dass der Verordnungsentwurf derzeit im ordentlichen Gesetzgebungsverfahren im Rat und im Europäischen Parlament erörtert wird.

Cloud-Computing-Diensten ein hohes Datenschutzniveau zu gewährleisten. Sie stützt sich daher auf die Ansichten, die der EDSB in seiner Stellungnahme zum Datenschutzreformpaket dargelegt hat (nachstehend „Stellungnahme des EDSB zum Datenschutzreformpaket“)[14] , und ergänzt diese durch besonderes Eingehen auf die Cloud-Computing-Umgebung. Der EDSB weist nachdrücklich darauf hin, dass seine Stellungnahme zum Datenschutzreformpaket in vollem Umfang auch auf Cloud-Computing-Dienste Anwendung findet und als Grundlage der vorliegenden Stellungnahme zu betrachten ist. Einige der dort behandelten Fragen – wie die neuen Bestimmungen über die Rechte betroffener Personen[15] – sind außerdem hinreichend klar und werden daher in dieser Stellungnahme nicht weiter erörtert.

12. Drittens sollen die Bereiche ermittelt werden, in denen aus der Sicht des Schutzes der Privatsphäre und des Datenschutzes mit Blick auf die von der Kommission in der Mitteilung dargelegte Cloud-Strategie ein weiteres Tätigwerden auf EU-Ebene erforderlich ist. Dazu gehören unter anderem weitere Orientierungshilfen, Normungsbemühungen, die Durchführung weiterer Risikobewertungen für bestimmte Sektoren (wie den öffentlichen Sektor), die Ausarbeitung von Standardvertragsklauseln, die Aufnahme eines internationalen Dialogs über Fragen im Zusammenhang mit dem Cloud Computing und die Gewährleistung wirksamer Mittel der internationalen Zusammenarbeit (dargestellt in Kapitel V).

13. Die Stellungnahme ist folgendermaßen aufgebaut: Kapitel II bietet einen Überblick über die Hauptmerkmale des Cloud Computing und die damit zusammenhängenden Datenschutzprobleme. Kapitel III enthält eine Übersicht über die relevantesten Elemente des EU-Rechtsrahmens und des Verordnungsvorschlags. In Kapitel IV wird der Frage nachgegangen, wie die vorgeschlagene Verordnung bei der Bewältigung der Herausforderungen helfen kann, die die Nutzung von Cloud-Computing-Diensten mit sich bringt. Kapitel V analysiert die Vorschläge der Kommission für weitere politische Entwicklungen und benennt die Bereiche, in denen weitere Arbeiten erforderlich sein könnten. Kapitel VI enthält die Schlussfolgerungen.

14. Zwar gelten viele der in dieser Stellungnahme angestellten Überlegungen für alle Umgebungen, in denen Cloud Computing zum Einsatz kommt, doch befasst sich diese Stellungnahme nicht mit der Nutzung von Cloud-Computing-Diensten durch Organe und Einrichtungen der EU, die gemäß der Verordnung (EG) Nr. 45/2001 der Aufsicht durch den EDSB unterliegen. Für diese Organe und Einrichtungen wird der EDSB zu diesem Thema eigene Leitlinien herausgeben.

II. DIE CLOUD-COMPUTING-UMGEBUNG

II.1. Begriffsbestimmungen

15. Cloud Computing ist ein sich ständig weiterentwickelndes Phänomen, das eine breite Spanne von technologischen Lösungen und Geschäftsabläufen umfasst. Der Begriff wird in unterschiedlichen Zusammenhängen mit unterschiedlichen Bedeutungen verwendet. Die wohl gebräuchlichste Definition ist die des US

[14] Die Stellungnahme kann abgerufen werden unter www.edps.europa.eu.
[15] Siehe Stellungnahme des EDSB, insbesondere Punkte 140 bis 158.

National Institute of Standards and Technology (NIST)[16], die folgendermaßen lautet: „*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*“ („*Cloud Computing ist ein Modell für einen einfachen, auf Abruf verfügbaren Netzzugriff auf einen gemeinsam genutzten Pool aus konfigurierbaren Rechenressourcen (z. B. Netzwerke, Server, Speicher, Anwendungen und Dienste), der schnell bereitgestellt und mit geringem Aufwand bzw. minimalen Eingriffen durch den Diensteanbieter freigegeben werden kann*“). Im NIST-Dokument werden drei Servicemodelle (SaaS: Software as a Service, PaaS: Platform as a Service und IaaS: Infrastructure as a Service) sowie vier Rollout-Modelle (öffentliche, private, Gemeinschafts- und Hybrid-Cloud-Umgebungen) definiert. In der vorliegenden Stellungnahme sind die Begriffe und Abkürzungen im Sinne der NIST-Definition zu verstehen.

II.2. Auswirkungen des Cloud Computing auf Unternehmen und Verbraucher

16. Vom Cloud Computing erwartet man sich unter anderem eine Senkung der IT-Kosten, hauptsächlich aufgrund von Skaleneffekten und einer effizienteren Nutzung von Informations- und Kommunikationsinfrastrukturen. Eine dynamische Zuweisung und Wiederverwendung von Ressourcen in größeren Pools ermöglicht eine Senkung der Kapitalausgaben für IT-Infrastruktur und einen wirtschaftlicheren Betrieb.

17. Kosteneinspareffekte werden von allen Cloud-Einführungsmodellen erwartet, doch können öffentliche (und in geringerem Umfang auch Gemeinschafts-) Cloud-Dienste die Kosten für Cloud-Anwender noch weiter senken, wenn ihnen nur die Dienste (wie Rechenzeit, Speicherplatz und andere Ressourcen) in Rechnung gestellt würden, die sie tatsächlich nutzen; damit würden praktisch alle Fixkosten für IT-Dienste wegfallen. Mit diesem Modell der nutzungsabhängigen Bezahlung könnten Unternehmen Dienste dynamisch dann erwerben, wenn sie sie tatsächlich benötigen. Darüber hinaus könnten auch kleine Organisationen wie KMU Zugang zu hochwertigen Diensten bekommen, die sie sich nach traditionellen Modellen nicht leisten können, weil dort hohe Eintrittskosten für Infrastruktur, Lizenzen und Einrichtungskosten entstehen und es an Skalierbarkeit fehlt[17]. Diese neuen Möglichkeiten dürften innovativen Start-up-Unternehmen den Weg ebnen, damit sie eine breite Palette neuer Dienste anbieten können.

18. Drittanwendungen bei sozialen Netzwerken können als ein Beispiel für solche neuen Möglichkeiten in einem SaaS-Umfeld gelten. Jede Person mit ausreichendem technischen Wissen, einer Computergrundausstattung und Internetanschluss kann Anwendungen entwickeln und anbieten, die in dem von dem sozialen Netzwerkdienst bereitgestellten Umfeld laufen. Cloud Computing bietet vielen Nutzern die Möglichkeit zum Mitmachen und ist daher das ideale Modell für neue Formen des Social Computing.

---

[16] US NIST SP 800-145, The NIST Definition of Cloud Computing, Sept. 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[17] Web-Shops sind ein Beispiel, das das Potenzial dynamischerer und skalierbarer Modelle zeigt.

19. Mobile Computing und Cloud Computing ergänzen und verstärken einander und bilden zusammen die Grundlage für Umgebungsintelligenz[18] und das Internet der Dinge. Mobile Geräte bieten überall Zugang zu Cloud-Diensten, und Cloud-Dienste ermöglichen den Zugang zu äußerst anspruchsvollen Diensten und riesigen Datensammlungen, die über die physischen Grenzen mobiler Geräte hinausgehen. Der Zugang zur Cloud eröffnet neue Möglichkeiten auch für Smartphones und Tablets, da Browser und Apps als Schnittstelle zu Cloud-Diensten genutzt werden können.

II.3. Künftige Konsolidierung des Marktes für Cloud Computing

20. Zwar ist der Markt für Cloud-Computing-Dienste noch von starkem Wachstum gekennzeichnet, doch ist hier, genau wie in anderen Sektoren, mit einer Konsolidierung zu rechnen, an deren Ende einige wenige Anbieter übrigbleiben dürften, die einer großen Anzahl von Kunden Dienste anbieten.

21. Mit einer solchen Konzentration könnte sich das bereits bestehende Ungleichgewicht auf dem Markt für Cloud-Dienste zwischen den Diensteanbietern und den meisten Nutzern ihrer Dienste weiter verstärken. Während es Regierungen und großen Unternehmen unter Umständen offensteht, nach ihren eigenen Anforderungen private Clouds einzurichten oder von gleich zu gleich mit Cloud-Anbietern Leistungsvereinbarungen auszuhandeln, müssten kleine und mittlere Organisationen des öffentlichen und des privaten Sektors sowie Verbraucher die von den Anbietern öffentlicher Cloud-Dienste vorgegebenen Bedingungen akzeptieren. Diese Asymmetrie könnte von Diensteanbietern dahingehend ausgenutzt werden, dass sie für ihre Dienste für die Anwender nachteilige Bedingungen festlegen, in denen die Pflichten und die Haftung des Anbieters begrenzt und die Rechte des Anwenders eingeschränkt werden, in denen den Anbietern weit reichende Vorrechte und Befugnisse eingeräumt oder sogar die Bedingungen für die Leistungserbringung zu Lasten des Cloud-Anwenders einseitig geändert werden.

II.4. Relevanz des Datenschutzes in einer Cloud-Computing-Umgebung

22. Cloud Computing erleichtert die Verarbeitung großer Datensammlungen[19] und die Schaffung neuer Dienste und Anwendungen, mit denen diese Daten zu Geld gemacht werden, wie Social-Media-Anwendungen oder Cloud-Dienste für mobile

---

[18] Ambient Intelligence and Ubiquitous Computing refer to a vision where humans will be surrounded by intelligent interfaces everywhere, sometimes embedded in everyday objects, connected everywhere and always on, enabling people and devices to interact with each other and with the environment (Umgebungsintelligenz und Ubiquitäres Computing bezeichnen ein Konzept, dem zufolge die Menschen überall von intelligenten Schnittstellen umgeben sein werden, die teilweise in Gegenstände des Alltags eingebettet sind, überall verbunden und immer eingeschaltet sind und damit Menschen und Geräten die Möglichkeit geben, miteinander und mit der Umgebung zu interagieren) (A social and technological view of Ambient Intelligence in Everyday Life, EC IPTS, 2003).

[19] Der Begriff „Big Data“ (große Datenmengen) wird zur Beschreibung einer großen Menge sowohl strukturierter als auch unstrukturierter Daten verwendet, die so umfangreich ist, dass sie mit herkömmlichen Datenbanktechniken und herkömmlicher Software nicht verarbeitet werden kann. Siehe “Big data: The next frontier for innovation, competition, and productivity” Mai 2011, McKinsey Global Institute, http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation.

Geräte. Sofern diese riesigen Datenmengen personenbezogene Daten enthalten, treten spezifische Risiken für die Privatsphäre und den Datenschutz auf, die eine Prüfung und die Entwicklung angemessener Garantien erfordern.

23. Das Cloud Computing wirft eine Reihe von Problemen beim Schutz der Privatsphäre und personenbezogener Daten auf, denen bei der Entwicklung und Einführung von Diensten gebührend Rechnung zu tragen ist. Die meisten dieser Bedenken sind unabhängig vom Dienst und vom Rollout-Modell von Bedeutung. Einige Cloud-Computing-Modelle beinhalten ferner Auslagerung, Fernzugang und Multi-Tenant-IT-Infrastrukturen, und die mit diesen Merkmalen verbundenen Datenschutzrisiken sind ebenfalls zu berücksichtigen.

24. Erstens: In Cloud-Umgebungen ist der genaue physische Ort, an dem die Daten gespeichert sind, dem Anwender üblicherweise nicht bekannt, und für den Dienst selbst ist er im Prinzip auch irrelevant. Aus der Perspektive des Dienstes ist es wichtiger zu fragen, von wo auf die Daten zugegriffen werden kann. Die Frage des Speicherortes der Daten bleibt allerdings im Hinblick auf die Anwendbarkeit nationalen Rechts von Bedeutung. Noch deutlicher wird dies, wenn (nationale) Behörden physisch auf die Daten zugreifen können müssen.

25. Zweitens: Die bereits beschriebene Asymmetrie in den Verträgen zwischen Diensteanbietern und Kunden macht es Cloud-Anwendern, die als für die Verarbeitung Verantwortliche auftreten, sehr schwer oder sogar unmöglich, in einer Cloud-Computing-Umgebung den Anforderungen an die Verarbeitung personenbezogener Daten Genüge zu tun. Die Asymmetrie könnte auch zu einer unerwünschten Zuweisung von Verantwortung für die Einhaltung der Datenschutzvorschriften führen. Sollte die Einstufung als für die Verarbeitung Verantwortlicher und Auftragsverarbeiter nicht angemessen das Ausmaß der Kontrolle über die Verarbeitungsmittel wiedergeben, besteht sogar die Gefahr, dass sich die Verantwortung für den Schutz personenbezogener Daten bei der Nutzung des Cloud Computing in Luft auflöst.

26. Drittens: Beim Cloud Computing arbeiten normalerweise verschiedene Akteure der End-to-End-Wertschöpfungskette zusammen, um dem Kunden einen Dienst zu erbringen. Auch dies wirft komplexe Fragen nach der Verteilung der Verantwortlichkeiten auf, vor allem, wenn man Anforderungen an die Verarbeitung personenbezogener Daten wie Sicherheit der Daten, Zugang und Überprüfung bedenkt. Dies kann sich noch erheblich verschärfen, wenn während des Betriebs dynamisch neue Anbieter dem Dienst hinzugefügt werden können[20].

27. Viertens: Cloud Computing hat zur Folge, dass erheblich mehr Übermittlungen personenbezogener Daten über Netzwerke stattfinden, viele verschiedene Parteien daran beteiligt sind und dabei Grenzen zwischen Ländern überschritten werden, auch außerhalb der EU. Je nach Art des angebotenen Dienstes können Daten an einer Vielzahl von Orten repliziert werden, damit sie von jedem Ort der Welt aus besser zugänglich sind. Werden bei diesen Diensten personenbezogene Daten verarbeitet, haben für die Verarbeitung Verantwortliche und Auftragsverarbeiter

[20] Auf die Schwierigkeiten bei der Zuweisung von Verantwortlichkeiten an die verschiedenen Beteiligten wie für die Verarbeitung Verantwortliche und Auftragsverarbeiter (wie in den Punkten 25 und 26 erwähnt) wird in Abschnitt IV.2 näher eingegangen.

dafür zu sorgen, dass diese Übermittlungen im Einklang mit den Datenschutzvorschriften geschehen.

28. Schließlich gilt nach wie vor, dass sich das Cloud Computing weiter entwickelt. Die technologischen Merkmale und die Entwicklung neuer Trends im Cloud Computing werden für den Datenschutz neue Herausforderungen mit sich bringen. Die weitere Entwicklung des Cloud Computing lässt sich nicht genau voraussagen. Daher stützt sich die vorliegende Stellungnahme auf die Tendenzen, die sich derzeit im Cloud Computing beobachten lassen[21].

III. ÜBERBLICK ÜBER DEN AUF CLOUD COMPUTING ANZUWENDENDEN DATENSCHUTZRECHTSRAHMEN DER EU

III.1. Derzeitiger EU-Rechtsrahmen

29. In einer Cloud-Computing-Umgebung vorgenommene Datenverarbeitungen, die in den räumlichen Anwendungsbereich des EU-Datenschutzrechts fallen[22], haben im Einklang mit dem derzeit in der Richtlinie 95/46/EG niedergelegten Datenschutzrahmen der EU zu stehen. Die Stellungnahme der Artikel-29-Datenschutzgruppe leistet Hilfestellung bei der Beantwortung der Frage, wie die Grundsätze und Vorschriften in der allgemeinen Datenschutzrichtlinie auf die Cloud-Computing-Umgebung anzuwenden sind[23].

30. Sofern die Verarbeitung in einer Cloud-Computing-Umgebung die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen (Telekombetreiber) umfasst, muss die Verarbeitung auch im Einklang mit der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[24] stehen.

31. Die Richtlinie über den elektronischen Geschäftsverkehr 2000/31/EG[25] enthält Vorschriften über bestimmte Aspekte von Diensten der Informationsgesellschaft. Cloud-Computing-Dienste fallen gewöhnlich unter die Definition der Dienste der

---

[21] Einige dieser Fragen sind auch Gegenstand des *Sopot Memorandum*, angenommen am 2. April 2012 von der Berlin International Working Group on Data Protection in Telecommunications, http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083.

[22] Verarbeitungsvorgänge fallen in den Anwendungsbereich des EU-Datenschutzrechts, wenn sie automatisiert verarbeitete personenbezogene Daten umfassen und die Verarbeitung im Zusammenhang mit den Tätigkeiten eines Betriebs des für die Verarbeitung Verantwortlichen mit Sitz in der EU oder durch einen für die Verarbeitung Verantwortlichen mit Sitz außerhalb der EU erfolgen, der in der EU befindliche Ausrüstung benutzt, gemäß Artikel 3 und 4 der Richtlinie 95/46/EG.

[23] Siehe Fußnote 8.

[24] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37, geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. L 337 vom 18.12.2009, S. 11.

[25] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17.7.2000, S. 1.

Informationsgesellschaft. Die Richtlinie über den elektronischen Geschäftsverkehr enthält eine beschränkte Verantwortlichkeit von Vermittlern für die Rechtmäßigkeit von Inhalten, die auf Abruf des Empfängers des Dienstes übermittelt oder gehostet werden. Artikel 1 Absatz 5 Buchstabe b der Richtlinie über den elektronischen Geschäftsverkehr besagt deutlich, dass ihre Bestimmungen unbeschadet der Datenschutzvorschriften der Richtlinie 95/46/EG gelten. Gemäß der Richtlinie 95/46/EG fällt die Verarbeitung personenbezogener Daten durch Internetdiensteanbieter in den Anwendungsbereich des Datenschutzrechts. Das Ausmaß ihrer Verantwortlichkeit mag variieren, je nachdem, ob sie als Auftragsverarbeiter oder für die Verarbeitung Verantwortliche auftreten. Im ersten Fall beschränkt sich ihre Haftung auf die Gewährleistung der Vertraulichkeit und der Sicherheit der Daten, während sie im zweiten Fall die volle Verantwortung für die Einhaltung der Datenschutzanforderungen tragen. In vielen Fällen, in denen Online-Vermittler Mehrwertdienste bereitstellen (z. B. soziale Netzwerke und Cloud-gestützte Dienste), kann davon ausgegangen werden, dass sie als für die Verarbeitung Verantwortliche auftreten[26] (siehe die detaillierte Analyse weiter unten in Abschnitt IV.2).

III.2. Der Vorschlag für eine Datenschutzverordnung

32. Ziel des von der Kommission am 25. Januar 2012 angenommenen Vorschlags für eine Datenschutzverordnung ist es, ein einheitliches Regelwerk in der EU für die Verarbeitung personenbezogener Daten durch Privatunternehmen und den öffentlichen Sektor zu schaffen[27]. Als Teil der Reform wird der räumliche Geltungsbereich des EU-Datenschutzrechts neu festgelegt. Die vorgeschlagenen Vorschriften bauen auf den allgemeinen Grundsätzen der Richtlinie 95/46/EG mit dem Ziel auf, sie an das digitale Umfeld anzupassen, einen Teil des Verwaltungsaufwands (wie Vorabmeldungen) zu verringern und die Rechte natürlicher Personen, die Verantwortung von für die Verarbeitung von personenbezogenen Daten Verantwortlichen sowie von Auftragsverarbeitern und die Befugnisse der nationalen Aufsichtsbehörden zu stärken.

33. Der Verordnungsvorschlag enthält eine Reihe neuer Pflichten für für die Verarbeitung Verantwortliche, so z. B. „eingebauten Datenschutz“ und „Datenschutz durch datenschutzfreundliche Voreinstellungen“, Rechenschaftspflicht, Datenschutz-Folgenabschätzungen, Meldungen von Datenschutzverletzungen sowie das Recht auf Vergessenwerden und das Recht auf

---

[26] Siehe insbesondere Erwägungsgrund 47 der Richtlinie 95/46/EG: „Wird eine Nachricht, die personenbezogene Daten enthält, über Telekommunikationsdienste oder durch elektronische Post übermittelt, deren einziger Zweck darin besteht, Nachrichten dieser Art zu übermitteln, so gilt in der Regel die Person, von der die Nachricht stammt, und nicht die Person, die den Übermittlungsdienst anbietet, als Verantwortlicher für die Verarbeitung der in der Nachricht enthaltenen personenbezogenen Daten. *Jedoch gelten die Personen, die diese Dienste anbieten, in der Regel als Verantwortliche für die Verarbeitung der personenbezogenen Daten, die zusätzlich für den Betrieb des Dienstes erforderlich sind*“ (Hervorhebung durch uns). Siehe beispielsweise die Stellungnahme 5/2009 der Artikel-29-Datenschutzgruppe zur Nutzung sozialer Online-Netzwerke, angenommen am 12. Juni 2009, S. 5, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf.

[27] Gemäß Artikel 2 Absatz 2 Buchstabe e findet die vorgeschlagene Verordnung keine Anwendung auf die Verarbeitung personenbezogener Daten, die vorgenommen wird „zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden“.

Datenübertragbarkeit. Da diese neuen Vorschläge am technologisch neutralen Ansatz des EU-Datenschutzes festhalten und auf keine konkrete Technologie abheben, umfassen sie auch die Cloud-Computing-Umgebung und sind auf sie anzuwenden.

III.3. Bedeutung der Gewährleistung eines hohen Datenschutzniveaus bei Cloud-Computing-Diensten

34. Auf internationaler Ebene haben die Datenschutzbehörden vor kurzem unterstrichen[28], dass unbedingt darauf zu achten ist, dass die bei der Nutzung von Cloud-Computing-Diensten auftretenden Herausforderungen nicht dazu führen dürfen, dass die Datenschutzstandards unter die herkömmlicher Verarbeitungsvorgänge fallen.

35. Der EDSB weist nachdrücklich darauf hin, dass bei der Verarbeitung personenbezogener Daten durch Anbieter von Cloud-Computing-Diensten alle in Artikel 6 der Richtlinie 95/46/EG und in Artikel 5 der vorgeschlagenen Verordnung festgeschriebenen Grundsätze des Datenschutzes (wie Verarbeitung nach Treu und Glauben, Rechtmäßigkeit, Zweckbegrenzung, Verhältnismäßigkeit, Richtigkeit, kurze Datenaufbewahrungsfristen) in vollem Umfang zu berücksichtigen sind.

36. Insgesamt sollten in Anbetracht der Vielfalt verfügbarer Cloud-Computing-Angebote und in Ermangelung allgemein anerkannter rechtlicher und vertraglicher Standards, die alle Schichten der Cloud-Computing-Architektur abdecken, die Auswirkungen der einzelnen Cloud-Computing-Dienste auf den Datenschutz im Einzelfall geprüft werden, damit die jeweils besten Garantien angewandt werden können.

IV. ANALYSE DER AUSWIRKUNGEN DER VORGESCHLAGENEN DATENSCHUTZVERORDNUNG AUF CLOUD-COMPUTING-DIENSTE

37. Der Verordnungsvorschlag bietet einen aktualisierten Rahmen für den Datenschutz, der technologischen Entwicklungen Rechnung trägt, gleichzeitig aber technologisch neutral bleibt. Er enthält Bestimmungen, die für die Cloud-Computing-Umgebung von besonderer Relevanz sind.

38. In diesem Kapitel der Stellungnahme wird untersucht, wie der Verordnungsvorschlag dazu beitragen könnte, von Cloud-Computing-Diensten aufgeworfene Probleme zu lösen, und werden andere Fragen erörtert, die vom Gesetzgeber im Gesetzgebungsverfahren zu berücksichtigen sind. Weiterhin schildert er vorbildliche Vorgehensweisen bei der Datenverarbeitung durch Cloud-Computing-Dienste.

IV.1. Klärung der Anwendbarkeit des EU-Datenschutzrechts auf Verarbeitungen durch Cloud-Computing-Dienste

39. Gegenstand von Artikel 2 der vorgeschlagenen Verordnung ist ihr sachlicher Anwendungsbereich. Dort heißt es unter anderem, dass die vorgeschlagene Verordnung keine Anwendung findet auf die Verarbeitung „durch natürliche

[28] Siehe Fußnote 10.

Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht“ (so genannte „Ausnahmeklausel für Privathaushalte“). In Erwägungsgrund 15[29] heißt es jedoch, dass von der vorgeschlagenen Verordnung nicht ausgenommen werden sollten für die Verarbeitung Verantwortliche oder Auftragsverarbeiter, die die Instrumente für die Verarbeitung personenbezogener Daten für solche persönlichen oder familiären Tätigkeiten bereitstellen. Diese Klarstellung ist für Anbieter von Cloud-Diensten für Verbraucher von Bedeutung. Auch wenn Verbraucher die Dienste zu persönlichen Zwecken nutzen, ist der Anbieter doch ein Unternehmen, das einerseits die Instrumente für die Verarbeitung bereitstellt, und andererseits dies zu kommerziellen Zwecken tut. Daher gilt die „Ausnahmeklausel für Privathaushalte“ für diese Anbieter nicht.

40. Bezüglich der Nutzer stellt der EDSB fest, dass im Verordnungsvorschlag in der „Ausnahmeklausel für Privathaushalte“ nicht erläutert wird, was unter einer persönlichen Tätigkeit mit Bezug auf „andere“ Nutzer zu verstehen ist (beispielsweise Kontakte oder Freunde oder soziale Netzwerke oder Dritte ganz allgemein). Damit bleibt die Frage der Anwendung der Ausnahme auf Fälle offen, in denen ein Nutzer - über Cloud-Dienste - personenbezogene Daten verarbeiten kann, auf die unbegrenzt viele Personen Zugriff haben. Der EDSB hat bereits darauf hingewiesen[30], dass die Anwendung der Ausnahme auf derartige Fälle nicht im Einklang mit den Urteilen des Gerichtshofs in den Rechtssachen *Lindqvist* und *Satamedia*[31]. stehen würde.

41. So könnte beispielsweise eine Person des öffentlichen Lebens auf ihrer Seite in einem sozialen Netzwerk zur Förderung einer Kulturinitiative die vollständigen Namen ihrer „Freunde“ oder Anhänger einstellen. In einem solchen Szenario dürfte die Person des öffentlichen Lebens mit ihrer Verarbeitung keine Gewinnerzielungsabsicht verfolgen. Die personenbezogenen Daten können jedoch sehr wohl einer unbegrenzten Anzahl von Personen zugänglich gemacht werden, und zwar nicht nur auf der Seite des sozialen Netzwerks[32], sondern möglicherweise auch durch Suchmaschinen. In diesem Fall würde die Ausnahmeregelung für Privathaushalte für den Teilnehmer nicht gelten; er würde also auch den Datenschutzvorschriften unterliegen[33].

42. Bezüglich des räumlichen Anwendungsbereichs geht Artikel 3 der vorgeschlagenen Verordnung in zweierlei Hinsicht über die bestehenden Vorschriften hinaus: Zum einen heißt es dort ausdrücklich, dass die Niederlassung[34] eines Auftragsverarbeiters in der EU Auslöser für die Anwendbarkeit der Verordnung ist, und zum anderen wird dort das neue Kriterium eingeführt, betroffenen Personen in der Union „Waren oder Dienstleistungen anzubieten“ oder „ihr Verhalten zu

---

[29] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 93, zum Wortlaut von Erwägungsgrund 15.

[30] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 91.

[31] Siehe Urteil des EuGH vom 6. November 2003, *Lindqvist*, C-101/01, [2003] Slg. I-12971 und Urteil des EuGH vom 16. Dezember 2008, *Satamedia*, C-73/07, [2008] Slg. I-983.

[32] Vorausgesetzt, die Privatsphäre-Einstellungen der Person lassen dies zu.

[33] Der Nutzer wäre als für die Verarbeitung Verantwortlicher zu betrachten, da er die Mittel der Verarbeitung (den Anbieter des Cloud-Dienstes) auswählt und in gewisser Weise auch den Zweck der Verarbeitung bestimmt.

[34] Siehe auch die Stellungnahme des EDSB zum Datenschutzreformpaket, Punkte 106 und 107, mit einer kritischen Anmerkung zur Definition der „Hauptniederlassung“.

beobachten“. Der EDSB hat diese Entwicklung in seiner Stellungnahme zum Datenschutzreformpaket begrüßt[35], und sie ist besonders relevant im Zusammenhang mit Cloud Computing.

43. Betrachtet man konkrete mögliche Beispiele von Beziehungen zwischen Cloud-Diensteanbieter und Cloud-Anwender, sind mehrere Szenarien denkbar. Nach den neuen Vorschriften ist eine breite räumliche Anwendbarkeit der vorgeschlagenen Verordnung auf Cloud-Computing-Dienste möglich, aus der sich komplexe Situationen ergeben können; wie jedoch im Folgenden erläutert, könnten mit einer geringfügigen Änderung des Wortlauts von Artikel 3 Zweifel bei der Auslegung ausgeräumt werden.

Der Cloud-Diensteanbieter als Auftragsverarbeiter

44. Wie im Folgenden erörtert, ist in manchen Fällen der Anbieter von Cloud-Diensten eher als Auftragsverarbeiter denn als für die Verarbeitung Verantwortlicher zu betrachten. Befände sich in diesen Fällen die Niederlassung des Cloud-Anwenders (des für die Verarbeitung Verantwortlichen) im Hoheitsgebiet der Union, stünde die Anwendbarkeit der vorgeschlagenen Verordnung auf den für die Verarbeitung Verantwortlichen und aufgrund des Vertrags auch auf den Auftragsverarbeiter außer Frage.

45. Auch wenn der Auftragsverarbeiter/Anbieter seinen Sitz in der EU hätte und der Anwender/für die Verarbeitung Verantwortliche seinen Sitz nicht in der EU hätte, würde die Verordnung auf alle Verarbeitungstätigkeiten des Auftragsverarbeiters Anwendung finden. Das würde bedeuten, dass Cloud-Anbieter mit Sitz in der EU den ihnen aus der vorgeschlagenen Verordnung erwachsenden Verpflichtungen nachkommen und möglicherweise auch die Folgen von Verstößen gegen diese Verpflichtungen tragen müssten. Gemäß Artikel 27 der vorgeschlagenen Verordnung darf der Auftragsverarbeiter personenbezogene Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten, „sofern er keinen anders lautenden, aus dem Unionsrecht oder dem mitgliedstaatlichen Recht erwachsenden Pflichten unterliegt“. Das bedeutet, dass ein in der EU niedergelassener Cloud-Anbieter/Auftragsverarbeiter stets im Einklang mit dem EU-Datenschutzrecht zu handeln hat, auch wenn er damit entgegen den Weisungen des (nicht in Europa ansässigen) Anwenders/für die Verarbeitung Verantwortlichen handelt[36]. Wie bereits gesagt, ist unbedingt darauf zu achten, dass durch die Probleme im Zusammenhang mit der Nutzung von Cloud-Computing-Diensten die Datenschutzstandards der EU nicht gesenkt werden. Artikel 27 des Verordnungsvorschlags ist daher als Garantie für das Cloud-Umfeld zu begrüßen.

---

[35] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 99.

[36] Die Anwendung der EU-Vorschriften sollte jedoch keinen übermäßigen Aufwand für europäische Unternehmen bezüglich der Verantwortlichkeiten nicht europäischer für die Verarbeitung Verantwortlicher mit sich bringen. Diesbezüglich enthält der Wortlaut der vorgeschlagenen Verordnung die Möglichkeit, den (für die Verarbeitung Verantwortlichen oder) Auftragsverarbeiter von der Haftung für Schäden zu befreien, wenn er nachweist, dass ihm der Umstand, durch den der Schaden eingetreten ist, nicht zur Last gelegt werden kann (Artikel 77 Absatz 3). In Artikel 79 wird ferner ausdrücklich klargestellt, dass sich die Höhe möglicher von der Aufsichtsbehörde zu verhängender Sanktionen bei Verstößen auch nach dem „Grad der Verantwortung der natürlichen oder juristischen Person“ bemisst (Artikel 79 Absatz 2).

Der Cloud-Diensteanbieter als für die Verarbeitung Verantwortlicher

46. Gilt der Cloud-Diensteanbieter als für die Verarbeitung Verantwortlicher, und ist er in der EU niedergelassen, dürften keine Auslegungszweifel bezüglich der Anwendbarkeit der vorgeschlagenen Verordnung auf seine Verarbeitungstätigkeiten entstehen.

47. Ein anderes Szenario bietet sich, wenn der Cloud-Diensteanbieter als für die Verarbeitung Verantwortlicher fungiert – oder sogar als einziger für die Verarbeitung Verantwortlicher –, und nicht nur als Auftragsverarbeiter[37], seinen Sitz aber nicht in der EU hat. Häufig sind Cloud-Diensteanbieter außerhalb der EU ansässig und bieten ihre Dienste in der EU über das Internet an. Sofern auf dem Hoheitsgebiet der EU keine Ausrüstung vorhanden ist, würde nach den derzeit geltenden Vorschriften die EU-Regelung auf die Verarbeitungstätigkeiten keine Anwendung finden[38]. Nach den vorgeschlagenen Vorschriften könnte die Verarbeitung personenbezogener Daten von in der EU ansässigen betroffenen Personen durch nicht in der EU ansässige Cloud-Diensteanbieter (die als für die Verarbeitung Verantwortliche eingestuft werden könnten) in den Anwendungsbereich des Verordnungsvorschlags fallen, wenn sie auf betroffene Personen in der Union abhebt. Ausgelöst würde die Anwendbarkeit der vorgeschlagenen Verordnung durch das neue Kriterium „[diesen] Personen in der Union Waren und Dienstleistungen anzubieten“ in Artikel 3 Absatz 2 Buchstabe a. Da gemäß der Begriffsbestimmung in Artikel 4 nur eine natürliche Person betroffene Person sein kann, könnte der Wortlaut diese Artikels dahingehend ausgelegt werden, dass nur Verarbeitungen im Zusammenhang mit den Angebot von Waren oder Dienstleistungen an in der Union ansässige *natürliche Personen* in den Anwendungsbereich der Verordnung fallen würden.

48. Beim Cloud Computing wenden sich die Angebote jedoch häufig an Unternehmen aller Größenordnungen, also an juristische Personen, die gemäß dem EU-Recht nicht als betroffene Personen gelten[39]. Wenn auch aus kommerzieller Sicht der Dienst Unternehmen in der EU angeboten wird (also keinen „betroffenen Personen“), ist der EDSB der Auffassung, dass die Bestimmungen des Verordnungsvorschlags auch gelten sollten, wenn der Dienst die Verarbeitung personenbezogener Daten von in der Union ansässigen natürlichen Personen beinhaltet. Um Zweifel bei der Auslegung zu vermeiden, könnte der Wortlaut des Vorschlags dahingehend geändert werden, dass es Artikel 3 Absatz 2 Buchstabe a heißt „diesen Personen Waren oder Dienstleistungen *einschließlich der Verarbeitung personenbezogener Daten dieser* betroffenen Personen in der Union anzubieten“. Alternativ könnte in einem neuen Erwägungsgrund verdeutlicht werden, dass die Verarbeitung personenbezogener Daten von betroffenen Personen in der Union durch für die Verarbeitung Verantwortliche, die nicht in der Union niedergelassen sind, ebenfalls in den räumlichen Anwendungsbereich des Verordnungsvorschlags fällt.

---

[37] Wenn beispielsweise der Diensteanbieter personenbezogene Daten für seine eigenen Zwecke verarbeitet.

[38] Es sei allerdings darauf hingewiesen, dass Cookies, die vom Anbieter auf dem Gerät des Anwenders/Kunden platziert werden, nach den EU-Rechtsvorschriften als „Ausrüstung“ auf dem Hoheitsgebiet der EU gelten.

[39] Siehe die Definition des Begriffs „betroffene Person“ im Wortlaut der vorgeschlagenen Verordnung, Artikel 4 Absatz 1.

IV.2. Bessere Zuordnung von Aufgaben und Verantwortlichkeiten (die Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“)

49. Die Anwendbarkeit der Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ im Cloud-Computing-Umfeld gehört zu den zentralen Aspekten der Datenschutzregelung für dieses Geschäftsmodell. Entscheidend ist die Frage, wie die Verantwortung für die Einhaltung der Datenschutzvorschriften zugeordnet wird[40].

50. Die Stellungnahme der Artikel-29-Datenschutzgruppe geht der Frage nach, wie die Beziehung zwischen Cloud-Diensteanbieter und Cloud-Anwender vor dem Hintergrund der derzeit geltenden Bestimmungen der Richtlinie 95/46/EG einzuordnen ist. Im Wesentlichen bestimmt der Cloud-Anwender letztendlich den Zweck der Verarbeitung und entscheidet über die Auslagerung dieser Verarbeitung und die Übertragung aller oder eines Teils der Verarbeitungstätigkeiten an eine externe Organisation. Somit sollte er als für die Verarbeitung Verantwortlicher betrachtet werden. Folglich sollte der Cloud-Anwender als für die Verarbeitung Verantwortlicher – normalerweise über angemessene vertragliche Garantien – sicherstellen, dass bei den Verarbeitungen durch den Diensteanbieter die geltenden Datenschutzvorschriften eingehalten werden. Stellt der Cloud-Diensteanbieter im Namen des Cloud-Anwenders die Mittel und die Plattform bereit, gilt er normalerweise als für die Verarbeitung Verantwortlicher gemäß der Richtlinie 95/46/EG[41]. Um die Einhaltung der Vorschriften durch den Auftragsverarbeiter zu gewährleisten, wird eine strenge Anwendung der Anforderungen von Artikel 17 der Richtlinie vorgeschlagen.

51. Die Stellungnahme der Artikel-29-Datenschutzgruppe räumt ein, dass in manchen Fällen der Anbieter von Cloud-Diensten je nach den Gegebenheiten entweder als gemeinsam für die Verarbeitung Verantwortlicher oder als eigenständiger für die Verarbeitung Verantwortlicher betrachtet werden kann. Dies könnte beispielsweise gegeben sein, wenn der Anbieter Daten für seine eigenen Zwecke verarbeitet.

52. Der EDSB schließt sich der Auffassung der Artikel-29-Datenschutzgruppe bezüglich der Einstufung der Beziehung zwischen Cloud-Diensteanbieter und Anwender auf der Grundlage der derzeit geltenden Vorschriften an. Er stellt allerdings fest, dass die im Cloud-Umfeld eingesetzten technischen Mittel unterdessen so kompliziert geworden sind, dass hinzugefügt werden muss, dass der Cloud-Anwender/für die Verarbeitung Verantwortliche vielleicht nicht die einzige Stelle ist, die allein über die „Zwecke und Mittel“ der Verarbeitung entscheidet. Immer häufiger ist es nicht der Cloud-Anwender, der die wesentlichen Elemente der Mittel festlegt, was ja ein Vorrecht des für die Verarbeitung Verantwortlichen ist. In diesem Zusammenhang ist es der Cloud-Diensteanbieter, der normalerweise die IT-Infrastruktur für das Cloud Computing entwirft, betreibt und pflegt (seien es nun die Basis-Hardware und Software-Dienstleistungen in IaaS oder die Plattform

---

[40] Siehe die Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ der Artikel-29-Datenschutzgruppe, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

[41] Die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, Richtlinie 95/46/EG, Artikel 2 Buchstabe e.

in PaaS oder das Gesamtdienstleistungspaket einschließlich Anwendersoftware wie in SaaS).

53. Wie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme ausgeführt hat, ist oft der Cloud-Diensteanbieter die Partei, die auf der Grundlage ihrer technischen Infrastruktur und ihres Unternehmenstyps Standardverträge oder Leistungsvereinbarungen ausarbeitet, die den Cloud-Anwendern angeboten werden. Dieser verfügt daher über keinen oder nur einen kleinen Spielraum für eine Änderung der technischen oder vertraglichen Gestaltung des Dienstes. Dies gilt umso mehr in Anbetracht der in Abschnitt II.3 bereits angesprochenen Konsolidierung des Cloud-Computing-Marktes. Es könnte also besonders schwierig sein, die Einhaltung der Datenschutzvorschriften sicherzustellen.

54. Ein Blick auf die Begriffsbestimmungen in der vorgeschlagenen Verordnung zeigt, dass für die Verarbeitung Verantwortlicher die natürliche oder juristische Person ist, die „allein oder gemeinsame mit anderen über die Zwecke, *Bedingungen* und Mittel“[42] (Hervorhebung durch uns) der Verarbeitung von personenbezogenen Daten entscheidet. Die derzeitige Bestimmung (Artikel 2 Buchstabe d der Richtlinie 95/46/EG) enthält den Begriff „Bedingungen“ nicht. Mit dieser Änderung würde noch mehr Gewicht auf die Verantwortung derjenigen gelegt, die bestimmen, wie eine Datenverarbeitungstätigkeit konkret organisiert wird.

55. In diesem Szenario würde eine Einstufung der Beziehung zwischen Anbieter und Anwender als gemeinsam für die Verarbeitung Verantwortliche das zugrundeliegende Ausmaß des Einflusses auf die Verarbeitungstätigkeiten besser wiedergeben. Ein solcher Schritt würde zu einer realistischeren Zuweisung der Verantwortlichkeiten an die Parteien führen, die bei der Aushandlung der Dienstleistungsbedingungen berücksichtigt werden müssten. Das würde beispielsweise bedeuten, dass in den Dienstleistungsbedingungen klar festgelegt werden sollte, welcher für die Verarbeitung Verantwortliche für welche Bereiche der Verarbeitung und/oder welche Verpflichtungen gemäß den einschlägigen Datenschutzvorschriften zuständig ist. Daraus folgt, dass der Cloud-Anwender für die Teile der Verarbeitung verantwortlich sein sollte, die er wirksam kontrollieren kann. Die unterschiedliche Verhandlungsmacht der beteiligten Parteien könnte allerdings ein ausgewogenes Verhandlungsergebnis immer noch verhindern. Dieses Problem könnte durch die Ausarbeitung und Verwendung von Standardvertragsklauseln und -bedingungen gelöst werden[43].

56. Der EDSB unterstützt die Bestimmung der vorgeschlagenen Verordnung, die eine Vereinbarung zwischen gemeinsam für die Verarbeitung Verantwortlichen vorschreiben soll (Artikel 24). In einer solchen Vereinbarung sollte in allen Fällen geregelt werden, wie je nach dem tatsächlichen Einfluss verschiedener Akteure auf die verschiedenen Verarbeitungstätigkeiten die Verantwortlichkeiten auf die verschiedenen Beteiligten verteilt werden.

57. Im Fall von IaaS-Lösungen könnte der Cloud-Anwender, der üblicherweise ein Unternehmen ist, einen gewissen Einfluss auf die Bedingungen des Dienstleistungsvertrags nehmen, auch wenn er vielleicht nicht in der Lage ist, mit

[42] Artikel 4 Absatz 5.
[43] Siehe weiter unten Abschnitt V.3.

dem Cloud-Diensteanbieter Sicherheitsvorkehrungen auszuhandeln. Der Cloud-Anwender würde jedoch bezüglich der Verarbeitung der personenbezogenen Daten seiner Beschäftigten für die Verarbeitung Verantwortlicher bleiben, weil er die Mittel und Bedingungen auswählt und den Zweck der Verarbeitung durch den Cloud-Anbieter bestimmt. Im Dienstleistungsvertrag sollten die Verantwortlichkeiten beider Seiten daher ausdrücklich festgelegt werden. Bei SaaS-Lösungen wie Cloud-gestützten Office-Produktivitäts-Tools oder Business-Intelligence-Tools hat der Cloud-Anwender üblicherweise keine Möglichkeit, auf die Art der vom Anbieter angebotenen Dienste Einfluss zu nehmen. Außerdem mag die Beziehung zwischen Anbieter und Anwender keine direkten Verhandlungen umfassen und sich auf eine einfache Registrierung beschränken. Als Folge hiervon mag der Cloud-Anwender die Mittel der Verarbeitung nur in sehr geringem Maße kontrollieren können. In diesem Szenario sollte nach Auffassung des EDSB der Cloud-Diensteanbieter eher als für die Verarbeitung Mitverantwortlicher eingestuft werden.

58. Der Verordnungsvorschlag führt in Artikel 26 Absatz 4 eine neue Bestimmung ein, der zufolge ein Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, für diese Verarbeitung als für die Verarbeitung Verantwortlicher gilt und den Bestimmungen des Artikels 24 für gemeinsam für die Verarbeitung Verantwortliche unterliegt. Im Zusammenhang mit Cloud-Computing-Diensten kann diese Bestimmung von wesentlicher Bedeutung sein. Sie könnte nämlich auf Fälle Anwendung finden, in denen ein Anbieter von SaaS für Unternehmenskunden beispielweise Adressen und Kontaktlisten von Beschäftigten oder Kunden des Cloud-Nutzers verarbeitet oder sogar zur Förderung seiner Mehrwertdienste den Inhalt ihm zugänglicher E-Mails kontrolliert.

59. Zusammenfassend lässt sich sagen, dass die Komplexität der technischen IT-Infrastruktur, die der Cloud-Computing-Umgebung zugrunde liegt, eine Erweiterung der Umstände erforderlich macht, unter denen ein Cloud-Diensteanbieter als für die Verarbeitung Verantwortlicher bezeichnet werden kann. Der Wortlaut der vorgeschlagenen Verordnung kann durchaus ein neues Element der Verantwortung für die Verarbeitung enthalten („Bedingungen“), das diesem sich abzeichnenden Trend entspricht. In vielen Fällen dürfte daher die Betrachtung des Cloud-Diensteanbieters als für die Verarbeitung Mitverantwortlichen seinen tatsächlichen Einfluss auf den Zweck, die Bedingungen und die Mittel der Verarbeitung besser wiederspiegeln.

IV.3. Verantwortung und Rechenschaftspflicht in der Cloud: Gewährleistung eines wirksameren Datenschutzes

60. Die vorgeschlagene Verordnung sieht für für die Verarbeitung Verantwortliche und für Auftragsverarbeiter generell eine größere Verantwortung und Rechenschaftspflicht vor (siehe im Wesentlichen Artikel 22), führt aber auch konkrete Verpflichtungen wie Datenschutz durch Technik, Datenschutz durch datenschutzfreundliche Voreinstellungen, Meldungen von Verletzungen des Schutzes personenbezogener Daten und eine Datenschutz-Folgenabschätzung ein. Aus einem allgemeinen Blickwinkel betrachtet, gewährleisten die gesteigerten Verantwortlichkeiten des für die Verarbeitung Verantwortlichen eine durchaus zu

begrüßende Verbesserung des Schutzes der betroffenen Personen[44]. Die meisten Neuerungen können ferner als deutliche Verbesserungen in der Cloud-Computing-Umgebung gelten.

61. Auf der anderen Seite können manche Arten neuer Verpflichtungen[45] nur schwer einzuhalten sein, wenn der Cloud-Anwender als für die Verarbeitung Verantwortlicher gilt. Zwar hat der Auftragsverarbeiter gemäß Artikel 26 mit dem für die Verarbeitung Verantwortlichen zusammenzuarbeiten, damit dieser seinen Verpflichtungen bei der Wahrung der Rechte betroffener Personen nachkommen kann, und hat er den für die Verarbeitung Verantwortlichen bei der Einhaltung von Sicherheitsanforderungen, bei Meldungen von Datenschutzverletzungen, bei der Datenschutz-Folgenabschätzung und der vorherigen Konsultation zu unterstützen, doch liegt die Hauptverantwortung letztendlich nach wie vor bei dem für die Verarbeitung Verantwortlichen.

62. In einer Cloud-Computing-Umgebung würde dies bedeuten, dass der Anwender/für die Verarbeitung Verantwortliche beispielsweise in der Lage sein müsste, angemessene technische und organisatorische Maßnahmen durchzuführen und Verfahren zu entwerfen, mit denen sichergestellt wird, dass die Datenverarbeitung durch den Cloud-Diensteanbieter im Einklang mit der Verordnung geschieht (Artikel 23, Datenschutz durch Technik). Dies könnte sich als schwierig erweisen. Im Fall eines grundlegenden IaaS-Dienstes dürfte es für ein Unternehmen (vor allem ein KMU) als Anwender besonders schwierig sein, Einfluss auf die technische und organisatorische Struktur des Dienstes zu nehmen. Von einem großen Anbieter mit vielen Anwendern kann realistischerweise nicht erwartet werden, dass er seine technische Infrastruktur oder Organisation auf jeden Anwender zuschneidet, um den Compliance-Anforderungen jedes einzelnen Anwenders auf der Grundlage individuell ausgehandelter Verträge gerecht zu werden.

63. Folglich kommt der in den vorstehenden Kapiteln erläuterten angemessenen Einstufung als für die Verarbeitung Verantwortlicher und Auftragsverarbeiter eine Schlüsselrolle zu, damit den Verpflichtungen zu mehr Verantwortung und Rechenschaftspflicht auch wirksam nachgekommen werden kann.

Datenschutz-Folgenabschätzung von Cloud-Computing-Diensten

64. Gemäß Artikel 33 der vorgeschlagenen Verordnung haben der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter eine Datenschutz-Folgenabschätzung durchzuführen. Der Artikel enthält eine nicht erschöpfende Liste der Verarbeitungsvorgänge, bei denen eine solche Datenschutz-Folgenabschätzung obligatorisch sein sollte. Der EDSB hat bereits erklärt, er sei mit dieser Liste nicht völlig zufrieden, da einige Arten einschlägiger Risiken dort fehlten[46]. In Ermangelung klarer Bestimmungen im Verordnungsvorschlag oder von

[44] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 166ff.

[45] Insbesondere die Umsetzung von Maßnahmen, mit denen sichergestellt werden soll, dass die Verarbeitung personenbezogener Daten im Einklang mit der Verordnung erfolgt; Datensicherheitsanforderungen; Datenschutz-Folgenabschätzung; Datenschutz durch Technik; Meldung von Datenschutzverletzungen, insbesondere im Zusammenhang mit Artikel 31 Absatz 3 Buchstabe c und e.

[46] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 201.

Leitlinien dazu, wie eine solche Datenschutz-Folgenabschätzung vorzunehmen ist, ist die Umsetzung dieser Anforderung vollständig von der subjektiven Einschätzung jedes für die Verarbeitung Verantwortlichen abhängig, die zu unterschiedlichen Ergebnissen führen kann.

65. Die Nutzung von Cloud-Computing-Diensten für die Verarbeitung personenbezogener Daten könnte in manchen Fällen, wie in dieser Stellungnahme gezeigt, besondere Risiken für den Datenschutz beinhalten, die eine Datenschutz-Folgenabschätzung erforderlich machen, anhand derer dann angemessene Risikobegrenzungsmaßnahmen festgelegt werden könnten.

66. Der EDSB weist insbesondere auf die Bedeutung von Datenschutz-Folgenabschätzungen bei der Nutzung von Cloud-Computing-Diensten im öffentlichen Sektor hin, und hier vor allem, wenn auch sensible Daten (wie Gesundheitsdaten, Daten, aus denen die politische Meinung hervorgeht, usw.) verarbeitet werden.

67. Der EDSB empfiehlt, in einem delegierten Rechtsakt festzulegen, nach welchen Kriterien und unter welchen Bedingungen eine Datenschutz-Folgenabschätzung erforderlich ist und welche Aspekte dabei untersucht werden sollen[47]. Im Zusammenhang mit Cloud-Computing-Diensten hält es der EDSB für hilfreich, wenn die Kommission Vorlagen entwickeln könnte, mit deren Hilfe Behörden (sowie natürliche Personen und Unternehmen) Risiken bewerten und managen könnten.

Audits und Zertifizierungen

68. Generell kann sich die Anwendung der Rechenschaftspflichtanforderungen in einer Cloud-Umgebung als kompliziert erweisen, da unter Umständen verschiedene Akteure in der End-to-End-Wertschöpfungskette tätig sind, um dem Endkunden den Dienst zu erbringen. Daher verlangt das Zusammenwirken vieler Beteiligter, dass die verschiedenen Akteure gegenseitig darauf vertrauen, dass alle verantwortungsvoll handeln und die erforderlichen Maßnahmen ergreifen, um sicherzustellen, dass die Datenverarbeitungsvorgänge im Einklang mit den Datenschutzvorschriften ablaufen.

69. Diesbezüglich helfen in Fällen mit vielen Beteiligten interne Audits und Audits durch zuverlässige Dritte sowie anschließende Zertifizierungen, Verantwortung und Rechenschaftspflicht zu überprüfen. Solche Audits sollten sich wiederum auf angemessene Zertifizierungs- und Normungsmodelle stützen (die weiter unten in Abschnitt V.2 näher erörtert werden).

70. Inhaltlich sind in Artikel 22 der vorgeschlagenen Verordnung die von dem für die Verarbeitung Verantwortlichen zu ergreifenden Datenschutzmaßnahmen niedergelegt[48]. So hat gemäß Artikel 22 Absatz 3 der für die Verarbeitung

---

[47] Unterstützt wird dies auch von der Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 08/2012 mit weiteren Beiträgen zur Diskussion der Datenschutzreform vom 5. Oktober 2012, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_de.pdf.

[48] Und indirekt für Auftragsverarbeiter in Artikel 26.

Verantwortliche Verfahren zur Überprüfung der Wirksamkeit dieser Datenschutzmaßnahmen einzusetzen. Wenn dies angemessen ist, kann diese Überprüfung von unabhängigen internen oder externen Prüfern durchgeführt werden.

71. Der EDSB begrüßt diese Bestimmung, weist aber darauf hin, dass gerade beim Cloud Computing konkretere Hilfestellung zur Beantwortung der Frage notwendig ist, welche Verfahren zur Überprüfung der Wirksamkeit von Datenschutzmaßnahmen in der Praxis eingesetzt werden sollten. Solange diese Hilfestellung nicht vorliegt, besteht die Gefahr, dass diese Überprüfung der Einhaltung der Vorschriften zwar auf dem Papier, nicht jedoch in der Wirklichkeit stattfindet. Der EDSB nimmt zur Kenntnis, dass gemäß dem derzeitigen Wortlaut des Verordnungsvorschlags (Artikel 22 Absatz 4) die Kommission zum Erlass delegierter Rechtsakte ermächtigt wird, in denen unter anderem die Bedingungen für die in Artikel 22 Absatz 3 genannten Überprüfungs- und Auditverfahren festgelegt werden. Unabhängig davon, ob eine solche Bestimmung über delegierte Rechtsakte noch in der endgültigen Fassung stehen wird[49], könnten von der Branche verfasste und von den zuständigen Datenschutzbehörden gebilligte Verhaltensregeln für das Cloud Computing dazu beitragen, die Einhaltung der Vorschriften zu verbessern und das Vertrauen zwischen den verschiedenen Akteuren zu stärken[50].

IV.4. Anpassung der Verfahren für internationale Datenübermittlungen an die Cloud-Computing-Umgebung

Probleme bei der Anwendung der EU-Vorschriften für Datenübermittlungen auf die Cloud-Computing-Umgebung

72. Grundlage von Cloud-Computing-Diensten ist der kontinuierliche Fluss von Daten von Cloud-Anwendern durch die Infrastruktur des Cloud-Diensteanbieters. Die Daten werden von den Cloud-Anwendern zu den in verschiedenen Teilen der Welt befindlichen Servern und Datenzentren des Cloud-Diensteanbieters transportiert. Cloud Computing beinhaltet daher häufig massive und kontinuierliche Datenübermittlungen weltweit.

73. Die EU-Vorschriften über internationale Datenübermittlungen enthalten sowohl im jetzigen Recht als auch in der vorgeschlagenen Verordnung Bedingungen für die Übermittlung personenbezogener Daten. So hat insbesondere das Land des Empfängers ein angemessenes Schutzniveau zu bieten; ist dieses nicht gegeben[51],

---

[49] In ihrer Stellungnahme 08/2012 vom 5. Oktober 2012 mit weiteren Beiträgen zur Diskussion der Datenschutzreform schlägt die Artikel-29-Datenschutzgruppe die Streichung von Artikel 22 Absatz 4 vor, da „es nicht notwendig (zu sein scheint), weitere, in Absatz 2 nicht genannte Kriterien und Anforderungen für geeignete Maßnahmen sowie die Bedingungen für die Überprüfungs- und Auditverfahren festzulegen".

[50] Artikel 38 der vorgeschlagenen Verordnung.

[51] Gemäß dem derzeitigen Rechtsrahmen hat die Kommission mehrere Angemessenheitsbeschlüsse im Hinblick auf Andorra, Argentinien, Australien, Kanada, die Schweiz, die Färöer Inseln, Guernsey, Israel, die Isle of Man, Jersey, US PNR und US Safe Harbour angenommen. Gemäß Artikel 41 des Verordnungsvorschlag wird die Kommission ermächtigt, Angemessenheitsbeschlüsse sowie negative Angemessenheitsbeschlüsse anzunehmen, und zwar nicht nur im Hinblick auf ein Drittland, sondern auch im Hinblick auf ein Gebiet oder einen Verarbeitungssektor in diesem Drittland oder einer internationalen Organisation.

sollten angemessene Garantien geboten werden. Die Anwendung der EU-Vorschriften über Datenübermittlungen auf Verarbeitungsvorgänge, die durch Cloud-Computing-Dienste stattfinden, gilt jedoch häufig als besondere Herausforderung.

74. Erstens enthält die vorgeschlagene Verordnung keine klare Definition des Begriffs „Übermittlung" personenbezogener Daten. Dies ist im Hinblick auf Netzwerkumgebungen wie das Cloud Computing problematisch, wo Daten nicht nur aktiv übermittelt werden, sondern auch (häufig ohne Wissen des Cloud-Anwenders/Endnutzers) einer Reihe von Empfängern in verschiedenen Ländern zur Verfügung gestellt werden. Der EDSB hat in seiner Stellungnahme zum Datenschutzreformpaket eine klare Definition des Begriffs „Übermittlung" gefordert[52].

75. Zweitens stützt sich die Anwendung der Vorschriften über internationale Datenübermittlungen üblicherweise auf eine Bewertung der Frage, ob in dem Land/in den Ländern, in das/die die Daten übermittelt werden sollen, ein angemessenes Schutzniveau besteht. Bei Cloud-Computing-Diensten gibt es jedoch in den allermeisten Fällen keinen festen Standort der Daten und kann es vorkommen, dass personenbezogene Daten nicht immer am gleichen Ort gespeichert werden. Außerdem können einige Diensteanbieter Auskunft über den Standort ihrer Cloud-Server verweigern[53].

76. Drittens ist es in Fällen, in denen der Cloud-Anwender als der für die Verarbeitung der Daten Verantwortliche und vor allem als alleiniger Verantwortlicher gilt, für ihn besonders schwierig, angemessene Garantien für die internationale Übermittlung seiner Daten zu erbringen, da er nur wenig über die Gestaltung der Cloud-Architektur seines Cloud-Diensteanbieters sowie die Orte weiß, an denen dieser und andere Auftragsverarbeiter oder Unterauftragsverarbeiter die Daten verarbeiten, und/oder er darüber keine Kontrolle hat. Dies ist das Ergebnis des bereits in Abschnitt II.3 erörterten asymmetrischen Verhältnisses zwischen dem Cloud-Anwender und dem Cloud-Diensteanbieter in der Kontrolle der Verarbeitungstätigkeiten.

Erhebliche Verbesserungen in der vorgeschlagenen Verordnung, die internationale Datenübermittlungen erleichtern

77. Der Verordnungsvorschlag führt mehr Flexibilität bei der Anwendung der Vorschriften für Datenübermittlungen ein, mit der internationale Übermittlungen erleichtert und gleichzeitig das hohe Schutzniveau für diese Daten erhalten werden soll. Er enthält insbesondere eine breitere Palette von Verfahren für internationale Datenübermittlungen. Artikel 42 Absatz 1 des Verordnungsvorschlags verlangt, dass nicht nur für die Verarbeitung Verantwortliche, sondern auch Auftragsverarbeiter geeignete Garantien für internationale Datenübermittlungen vorsehen. Dies ist ein deutlicher Fortschritt, der vor allem für die Cloud-Computing-Umgebung relevant ist.

---

[52] Siehe Stellungnahme des EDSB, S. 18f.

[53] Siehe beispielsweise das beim Europäischen Gerichtshof anhängige Ersuchen um Vorabentscheidung in der Rechtssache C-131/12 Google ./. Spanien.

78. So erleichtert beispielsweise Artikel 42 der vorgeschlagenen Verordnung die Verwendung mehrerer Arten von Vertragsklauseln (von Standard- bis ad hoc-Klauseln) und stellt auch klar, dass nur ad hoc-Klauseln von einer Aufsichtsbehörde genehmigt werden müssen. Cloud-Computing-Diensteanbieter können nun die ihnen eingeräumte Flexibilität nutzen und von der Kommission oder von einer Aufsichtsbehörde im Einklang mit Artikel 42 Absatz 2 Buchstabe c angenommene Standardvertragsklauseln verwenden. Ebenso können sie ad hoc-Klauseln verwenden, die auf ihr spezifisches Umfeld zugeschnitten sind; diese müssen allerdings von der zuständigen Aufsichtsbehörde genehmigt worden sein. Unabhängig davon, für welche Klauseln sich die Cloud-Diensteanbieter entscheiden, sollten sie alle Mindestgarantien zu einigen zentralen Aspekten enthalten, so z. B. das Erfordernis einer schriftlichen Vereinbarung mit Unterauftragnehmern, in denen diese sich zur Einhaltung der gleichen Datenschutzverpflichtungen (einschließlich Sicherheitsmaßnahmen) verpflichten, ferner die vorherige Unterrichtung/Hinweise für den Cloud-Anwender auf den Einsatz von Unterauftragsverarbeitern, Auditklausel, Rechte von Drittbegünstigten, Vorschriften über Haftung und Schadenersatz, Aufsicht, usw. Diesen Kernaspekten widmen Aufsichtsbehörden bei der Ausarbeitung von Standardklauseln oder der Überprüfung von ad hoc-Klauseln zwecks Genehmigung besondere Aufmerksamkeit.

79. Artikel 43 des Verordnungsvorschlags sieht ein detailliertes Verfahren für die Verwendung verbindlicher unternehmensinterner Vorschriften (Binding Corporate Rules, BCR) vor[54], die wohl eher für multilaterale Regelungen geeignet sind. BCR sind ein Verfahren, das sich besonders gut für die Cloud-Computing-Umgebung eignet, da es Flexibilität bei der Übermittlung von Daten zwischen allen Stellen einer Organisation ermöglicht, gleichzeitig aber rechtlich verbindliche Pflichten für diese Organisation bezüglich des Datenschutzes an allen Stellen vorgibt, an denen in dieser Organisation solche Daten verarbeitet werden. Wir begrüßen, dass auch Auftragsverarbeiter diese Vorschriften verwenden können sollen, zumal Auftragsverarbeiter mit einer Niederlassung in der EU dieses Verfahren nutzen können, um innerhalb ihrer Gruppe die Datenübermittlung an außerhalb der EU ansässige Einrichtungen zu erleichtern.

Möglichkeiten in der vorgeschlagenen Verordnung für einen genaueren Zuschnitt der Datenübermittlungsverfahren auf die Cloud-Computing-Umgebung

80. Wie bereits dargelegt, weist die Cloud-Computing-Umgebung bestimmte Besonderheiten auf, denen in den bisher entwickelten Datenübermittlungsverfahren nicht in vollem Umfang Rechnung getragen wurde. Der Verordnungsvorschlag bietet nun die Möglichkeit, diese Verfahren stärker auf einen bestimmten Sektor wie das Cloud Computing zuzuschneiden. Der Europäische Datenschutzausschuss könnte in diesem Zusammenhang weitere Hilfestellung bieten[55].

i) Standardvertragsklauseln

---

[54] Verbindliche unternehmensinterne Vorschriften wurden von den in der Artikel-29-Datenschutzgruppe vertretenen Aufsichtsbehörden als weiteres Verfahren für internationale Datenübermittlungen entwickelt. (Siehe die Dokumente der Artikel-29-Datenschutzgruppe unter http://ec.europa.eu/justice/data-protection/article-29/index_de.htm). Der Verordnungsvorschlag stützt sich auf die Arbeiten der Artikel-29-Datenschutzgruppe in diesem Bereich.

[55] Siehe Stellungnahme 8/2012 der Artikel-29-Datenschutzgruppe.

81. Standardvertragsklauseln[56] sind besonders gut geeignet für Punkt-zu-Punkt-Datenübermittlungen von einem für die Verarbeitung Verantwortlichen an identifizierte Empfänger (einen oder mehrere für die Verarbeitung Verantwortliche(n), Auftragsverarbeiter und/oder Unterauftragsverarbeiter) an identifizierten Orten. In den meisten Cloud-Computing-Umgebungen dürften solche Klauseln allerdings kaum verwendbar sein, weil dort Daten kontinuierlich über eine lange Kette von Empfängern übermittelt werden.

82. Geht man davon aus, dass gemäß den von der Kommission für die Übermittlung vom für die Verarbeitung Verantwortlichen an den Auftragsverarbeiter genehmigten Standardvertragsklauseln der Cloud-Diensteanbieter der für die Verarbeitung Verantwortliche ist, ist es seine Sache, den Cloud-Anwender vor einer Weitervergabe der Verarbeitung an einen Unterauftragsverarbeiter und die Übermittlung an einen externen Dritten zu informieren und seine Einwilligung einzuholen. In vielen Fällen dürfte der Cloud-Anwender allerdings nur wenig oder keine tatsächliche Macht haben, solche Übermittlungen zu genehmigen oder zu untersagen. Sollte hingegen der Cloud-Diensteanbieter tatsächlich als für die Verarbeitung Verantwortlicher angesehen werden, wäre er in vollem Umfang dafür verantwortlich, dass seine Datenübermittlungen an Stellen innerhalb und außerhalb seiner Organisation den Vorschriften entsprechen, da er die volle Kontrolle hat und bezüglich seiner Entscheidungen über die Architektur seiner Cloud-Computing-Dienste voll rechenschaftspflichtig ist. Diesbezüglich hat der EDSB weiter oben in Abschnitt IV.2 dargelegt, dass der Cloud-Diensteanbieter in vielen Fällen als für die Verarbeitung Mitverantwortlicher zu gelten hat.

83. Derzeit gibt es noch keine Standardvertragsklauseln zur Regelung der Übermittlungen von Daten von in der EU ansässigen Auftragsverarbeitern an Auftragsverarbeiter mit Sitz außerhalb der EU. Hier besteht im Hinblick auf Cloud-Computing-Dienste eine Lücke, an deren Schließung gearbeitet werden sollte, damit hier eine Reihe angemessener neuer Klauseln bereitgestellt wird.

84. Es wäre daher hilfreich, wenn die Kommission und/oder Aufsichtsbehörden die Möglichkeiten von Artikel 42 Absatz 2 Buchstabe b und c des Verordnungsvorschlags nutzen und aktualisierte Standardvertragsklauseln annehmen würden, die auf die Cloud-Computing-Umgebung zugeschnitten sind. Gegenstand solcher Klauseln sollten insbesondere Übermittlungen von für die Verarbeitung Verantwortlichem an für die Verarbeitung Verantwortliche aus der EU heraus sein, ferner kontinuierliche Übermittlungen zwischen unterschiedlichen Rechtsgebieten, das Fehlen genauer Angaben zu dem Ort, an dem sich die Daten zu einem bestimmten Zeitpunkt befinden, sowie Verfahren für Information/Hinweise und Rechenschaftspflicht. Wie später noch in Abschnitt IV.7 ausgeführt, sollten sie sich auch mit den Bedingungen für den Zugang für Strafverfolgungsbehörden befassen.

ii) Verbindliche unternehmensinterne Vorschriften

[56] Nähere Informationen zu bestehenden Standardvertragsklauseln unter: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

85. Verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, BCR), in denen der Grundsatz der Verantwortlichkeit in vollem Umfang verankert ist, sind für Cloud-Computing-Dienste besonders gut geeignet. Cloud-Diensteanbieter sollten daher ermutigt werden, für ihre internationalen Übermittlungen dieses Verfahren zu nutzen.

86. Bezüglich der Anwendbarkeit von BCR auf externe Auftragsverarbeiter und/oder Unterauftragsverarbeiter unterstreicht der EDSB, dass BCR zwar als rechtverbindliches Verfahren für Gegebenheiten innerhalb einer Gruppe entwickelt wurden, dass sie jedoch gemäß Artikel 43 Absatz 2 Buchstabe c der vorgeschlagenen Verordnung auch für externe Organisationen rechtsverbindlich sein würden. Die aktuellen Arbeiten der Artikel-29-Datenschutzgruppe an BCR für Auftragsverarbeiter werden einen wichtigen Beitrag unter anderem zur Behandlung ihrer Rechtsverbindlichkeit für externe Unterauftragsverarbeiter leisten.

87. Gemäß Artikel 43 Absatz 3 der vorgeschlagenen Verordnung wird die Kommission ermächtigt, delegierte Rechtsakte zur Klärung der Anwendung von Artikel 43 Absatz 2 Buchstabe b, d, e und f auf BCR erlassen, die von Auftragsverarbeitern zu beachten sind. Die Artikel-29-Datenschutzgruppe[57] hat begrüßt, dass weitere Einzelheiten in einem delegierten Rechtsakt festgelegt werden sollen und hat empfohlen, dass auch der Europäische Datenschutzausschuss in dieser Frage Orientierungshilfe bietet.

88. Schließlich sei noch unterstrichen, dass die weitere Anpassung von Verfahren für internationale Datenübermittlungen deutlich auch von ergänzenden Arbeiten an Normen und Zertifizierungsregelungen profitieren würde, mit denen das geforderte Datenschutzniveau auf allen Ebenen der Verarbeitung erreicht werden könnte, was wiederum das notwendige Vertrauen seitens der Cloud-Anwender fördern würde (wie weiter unten in Abschnitt V.2 erörtert).

IV.5. Sicherheit der Verarbeitung

89. Zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten sind technische und organisatorische Maßnahmen zu ergreifen, mit denen unter anderem Zugang, Änderung, Löschung oder Entfernung durch Unbefugte verhindert wird. Gemäß der vorgeschlagenen Verordnung sind sowohl der für die Verarbeitung Verantwortliche als auch der Auftragsverarbeiter zu einer Bewertung der Risiken verpflichtet, die durch die Verarbeitung und die Art der verarbeiteten Daten entstehen können, und sie haben die entsprechenden Maßnahmen auszuwählen.

90. In Cloud-Computing-Umgebungen kommt es ganz besonders darauf an, dass alle Beteiligten, ob für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter, für die von ihnen zu verantwortende Verarbeitung eine Risikobewertung vornehmen, auch weil, wie bereits erwähnt, das Cloud Computing eine größere Komplexität mit sich bringt. Für eine umfassende Risikobewertung und umfassendes Sicherheitsmanagement sind Zusammenarbeit und Koordinierung zwischen den beteiligten Parteien erforderlich, da das Gesamtsicherheitsniveau durch das schwächste Kettenglied bestimmt wird. So kann beispielsweise ein PC oder ein Client-PC, der attackiert worden ist und Unbefugten Zugang zu den Anmeldedaten

[57] Siehe Stellungnahme 08/2012 der Artikel-29-Datenschutzgruppe, S. 37f.

des Benutzers gewährt, die Sicherheitsmaßnahmen an zentralen Speicherorten zunichtemachen. In einer Cloud-Computing-Umgebung, die von vielen Anwendern genutzt wird, könnten Sicherheitsprobleme bei einem Anwender die Sicherheit anderer Anwender beeinträchtigen, sofern der Dienst nicht kompakte und sichere Maßnahmen bereitgestellt hat, um Dienste und Daten zwischen Anwendern zu trennen und gegenseitige Interferenzen unmöglich zu machen.[58]

91. Damit Cloud-Nutzer auf ihrer Seite die notwendigen Maßnahmen ergreifen können, müssten sie über die Risikobewertung und die Sicherheitsmaßnahmen des Cloud-Anbieters unterrichtet werden und sich eine Vorstellung von deren Wirksamkeit und Grenzen machen können. Jedoch herrscht im vorgegebenen Interesse der Sicherheit in der Regel keine Transparenz bezüglich der ergriffenen IT-Sicherheitsvorkehrungen. Die Anwender erfahren häufig nichts zu den Einzelheiten von Sicherheitszwischenfällen. Das erschwert es Cloud-Anwendern, sich auch nur ein ungefähres Bild von der Sicherheit des Verarbeitungsvorgangs zu machen.

92. Für die Verarbeitung Verantwortliche können ihren Sicherheitsverpflichtungen nur nachkommen, wenn sie über umfassende und zuverlässige Informationen verfügen, anhand derer sie bewerten können, ob der Cloud-Anbieter seinen Sicherheitsverpflichtungen als Auftragsverarbeiter oder für die Verarbeitung Verantwortlicher in vollem Umfang nachkommt. Sie dürfen die Verarbeitung personenbezogener Daten nicht Cloud-Diensteanbietern überlassen, die über ihre Sicherheitsvorkehrungen nicht ausreichend und transparent Auskunft erteilen.

93. Der Verordnungsvorschlag soll eine umfassende Verpflichtung für die für die Verarbeitung Verantwortlichen schaffen, Aufsichtsbehörden und betroffene Personen über Datenschutzverletzungen in Kenntnis zu setzen. Cloud-Anbieter müssten alle in ihren Diensten vorkommenden Verletzungen des Schutzes personenbezogener Daten entweder direkt bei den Aufsichtsbehörden und gegebenenfalls den betroffenen Personen melden, falls diese als für die Verarbeitung Verantwortliche auftreten, oder beim Cloud-Anwender melden, der als für die Verarbeitung Verantwortlicher fungiert, wenn sie nur Auftragsverarbeiter sind.

94. Gemäß dem Verordnungsvorschlag wäre die Kommission ermächtigt, gegebenenfalls durch Annahme delegierter Rechtsakte, die anzuwendenden Sicherheitsanforderungen und die Kriterien und Gegebenheiten für die Feststellung von Datenschutzverletzungen sowie das Format und das Verfahren für die Meldungen festzulegen. Vor allem in einer komplexen Cloud-Computing-Umgebung sollten solche delegierten Rechtsakte darauf abzielen, Klarheit bezüglich der Verantwortung der verschiedenen Akteure zu schaffen. Sie könnten von der Ausarbeitung europäischer Normen für den Datenschutz und für IT-Sicherheit in Cloud-Computing-Umgebungen sowie von der Entwicklung und Anerkennung von in der Kommunikation angekündigten Messparameter profitieren, wie weiter unten in Kapitel V noch näher ausgeführt wird.

---

[58] Es wird gelegentlich behauptet, Cloud-Computing-Umgebungen könnten sicherer sein als herkömmliche Verarbeitungssituationen. Diese Annahme trifft jedoch nur in einigen wenigen Fällen zu, z. B. wenn die Verarbeitungsvorgänge einer kleinen Organisation oder einer Einzelperson, bei denen keine systematischen Informationssicherheitsmaßnahmen umgesetzt werden, in Cloud-Datenzentren mit professionellem Sicherheitsmanagement verlagert werden.

IV.6. Engere Zusammenarbeit und koordinierte Aufsicht über grenzüberschreitende Verarbeitungsvorgänge

95. Problematisch bei der Verarbeitung personenbezogener Daten durch Cloud-Computing-Dienste ist unter anderem, dass es für die Aufsichtsbehörden in der EU schwierig ist, alle Aspekte der in dieser Umgebung stattfindenden Verarbeitungsvorgänge zu beaufsichtigen. Für die Behörden kann es insbesondere schwierig sein, wirksam die Aufsicht über Daten zu führen, die ausländischem Recht unterliegen oder für einen Auftragsverarbeiter oder für die Verarbeitung Verantwortlichen verfügbar und zugänglich sind, der ausländischem Recht unterliegt.

96. Wie bereits in Abschnitt IV.1 erläutert, würden die neuen Bestimmungen des Verordnungsvorschlags dazu beitragen, einige dieser Bedenken zu mindern, weil Verarbeitungstätigkeiten von Cloud-Diensteanbietern mit einer Niederlassung in der EU oder bestimmte Verarbeitungstätigkeiten, die von außerhalb der EU vorgenommen werden, in den Anwendungsbereich des EU-Datenschutzrechts fallen und der Aufsicht durch die zuständigen Datenschutzbehörden in der EU unterliegen würden. Auch die Bestimmungen der vorgeschlagenen Verordnung über engere Zusammenarbeit (Artikel 55 und 56) sowie das Kohärenzverfahren (Artikel 57 bis 63) sollten den Aufsichtsbehörden in Europa bei der Zusammenarbeit und der Ausarbeitung eines koordinierten Ansatzes zu Themen helfen, die wie Cloud-Computing-Dienste ihrer Natur nach transnational sind. Schließlich würden auch die Durchsetzungsbefugnisse von Aufsichtsbehörden durch die Möglichkeit der Verhängung finanzieller Sanktionen gegen die für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter gestärkt, die gegen das EU-Datenschutzrecht verstoßen haben (geregelt in Artikel 79).

97. Die in Kapitel VII der vorgeschlagenen Verordnung vorgesehene Zusammenarbeit und das Kohärenzverfahren sind außerordentlich begrüßenswert; dessen ungeachtet ist der Gesamtzusammenhang zu betrachten, in dem die Verarbeitungsvorgänge in Cloud-Computing-Diensten ablaufen. Auf internationaler Ebene hat es mehrere Bemühungen gegeben, die notwendige grenzüberschreitende Zusammenarbeit im Bereich Schutz der Privatsphäre und Datenschutz angemessen zu behandeln.[59] 2011 forderte auch die Internationale Konferenz der Datenschutzbeauftragten eine intensivere internationale Koordinierung bei der Durchsetzung in Fragen des Schutzes der Privatsphäre und des Datenschutzes.[60]

98. Der EDSB fordert daher Kommission und Aufsichtsbehörden auf, die internationale Zusammenarbeit wirksamer zu gestalten (beispielsweise durch die Entwicklung wirksamer Verfahren für die internationale Zusammenarbeit, durch internationale Amtshilfe bei der Durchsetzung des Datenschutzrechts usw.), um auch in Fragen im Zusammenhang mit Cloud Computing zu einer intensiveren Zusammenarbeit zu

---

[59] Zum Beispiel die Empfehlung der OECD zur grenzüberschreitenden Zusammenarbeit zur Durchsetzung von Datenschutzgesetzen („Enforcement of Laws Protecting Privacy"), angenommen im Jahr 2007, und die kürzlich erfolgte Gründung des Global Privacy Enforcement Network (GPEN), https://www.privacyenforcement.net/about_the_network.

[60] Entschließung zu „Privacy Enforcement Co-ordination at the International Level", angenommen auf der 33. Internationalen Konferenz der Datenschutzbeauftragten, 1. November 2011, Mexico City.

gelangen. Der EDSB erinnert daran, dass mit diesen Aktivitäten auch schon vor dem Inkrafttreten der vorgeschlagenen Verordnung begonnen werden kann.

IV.7. Zugang von Strafverfolgungsbehörden zu personenbezogenen Daten, die durch Cloud-Computing-Dienste verarbeitet wurden

99. Durch Cloud-Computing-Dienste gespeicherte Daten können von örtlichen Strafverfolgungsbehörden des Rechtsgebiets, in dem sich die Server oder Datenzentren befinden, oder in dem der Cloud-Diensteanbieter eine Niederlassung hat, beschlagnahmt oder abgerufen werden. Entsprechende Ersuchen können nicht nur von Verwaltungs- und/oder Justizbehörden innerhalb der EU gestellt werden, sondern auch von solchen außerhalb der EU. Innerhalb Europas müssen solche Ersuchen nach einem rechtsstaatlichen Verfahren gestellt werden[61] und den Anforderungen des Datenschutzes Genüge tun[62]. Die Mitglieder des Europarates sind durch das Übereinkommen Nr. 108 über Datenschutz[63] und damit zusammenhängende Dokumente gebunden. Der Zugang durch Strafverfolgungsbehörden unterliegt ferner einer Ex-post-Kontrolle durch die Datenschutzaufsichtsbehörden. Allerdings werfen Zugangsersuchen ausländischer Strafverfolgungsbehörden im Hinblick auf den Datenschutz besondere Probleme auf, weil vor allem darauf zu achten ist, dass der natürlichen Personen in Europa gewährte Schutz ihrer Daten in einem solchen Zusammenhang nicht deutlich geschwächt oder völlig außer Acht gelassen wird.

100. So wurden beispielsweise in einigen Ländern geschäftlich tätige Cloud-Diensteanbieter gezwungen, nationalen Strafverfolgungsbehörden Zugang zu ihren Daten zu gewähren, was Befürchtungen bezüglich des Zugriffs auf im Ausland in Cloud-Computing-Diensten gespeicherte Daten hervorgerufen hat.[64] Hingewiesen wurde ferner auf die zunehmende Wahrscheinlichkeit, dass bestimmte Regierungen von Kommunikationsanbietern, die Dienste in ihrem Land anbieten, verlangen, *„dort Kommunikationsausrüstung zu belassen, um einen solchen Zugang zu erleichtern"*[65].

101. Cloud-Diensteanbieter können hier zwischen zwei einander widersprechenden gesetzlichen Anforderungen stehen: zum einen liegt ihnen ein Ersuchen einer Strafverfolgungsbehörde in einem Land vor, das sich rechtlich für zuständig erklärt, und zum anderen haben sie die Einhaltung des EU-Datenschutzrechts zu gewährleisten. In den Vertragsbestimmungen von Cloud-Anbietern heißt es häufig, dass sie Informationen aufbewahren und Strafverfolgungsbehörden offenlegen, wenn hierzu eine gerichtliche Anordnung vorgelegt wird. Der Umgang mit solchen

---

[61] In vielen Fällen stützen sich Zugangsersuchen auf ein von einer Justizbehörde genehmigtes rechtmäßiges Ersuchen.

[62] Bei der Verarbeitung von Daten durch Strafverfolgungsbehörden ist den geltenden Datenschutzanforderungen Genüge zu tun. Das Datenschutzreformpaket enthält auch einen Vorschlag für eine Datenschutzrichtlinie, mit der die Bedingungen für die Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden in der EU harmonisiert werden sollen.

[63] Übereinkommen des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, ETS Nr. 108, 28.1.1981.

[64] „Lost in the Cloud", Jonathan Zittrain, New York Times, 19. Juli 2009, http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=1.

[65] „Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future", Christopher Kuner, Universität Tilburg, Niederlande, Arbeitspapier Nr. 016/2010, Oktober 2010, S. 40.

Zugangsersuchen sollte allerdings im Einklang mit den EU-Datenschutzanforderungen erfolgen.

102. Erstens sollte einem solchen Ersuchen auf Zugang zu personenbezogenen Daten betroffener Personen in der EU nur nach rechtsstaatlichen Grundsätzen stattgegeben werden und sollte es seine angemessene Rechtsgrundlage geben, die die Datenübermittlung erlaubt.[66] Diesbezüglich hat der EDSB in seiner Stellungnahme zum Datenschutzreformpaket[67] die Aufnahme einer Bestimmung in den verfügenden Teil des Verordnungsvorschlags gefordert, in der die Bedingungen für solche Zugangsersuchen festgelegt werden. In solchen Fällen sollten geeignete Garantien bestehen, zu denen auch gerichtliche Garantien sowie Datenschutzgarantien gehören, einschließlich internationaler oder bilateraler Kooperationsabkommen zu einzelnen Fragen (z. B. Rechtshilfeabkommen). Vorteilhaft wäre es auch, wenn dieses Thema in anderen Arten internationaler Instrumente wie Handelsabkommen mit Drittländern behandelt würde. Weiter sollte, wie der EDSB bereits ausgeführt hat[68], der Frage nachgegangen werden, wie in einem solchen Fall die Aufsichtsbehörde eingreift, ob mit einer Stellungnahme oder einer Genehmigung der Übermittlung. Hierzu könnte es erforderlich sein, in den Verordnungsvorschlag eine entsprechende Bestimmung aufzunehmen.

103. Zweitens muss weiter an der Verbesserung und Standardisierung der Behandlung von Zugangsersuchen von Strafverfolgungsbehörden in den Vertragsbedingungen der Cloud-Diensteanbieter gearbeitet werden (hierauf wird in Abschnitt V.3 noch näher eingegangen).

104. Schließlich besteht eindeutiger Bedarf an einer Diskussion auf internationaler Ebene über den Zugang zu Daten für Strafverfolgungsbehörden. In diesem Zusammenhang sollten die Bedingungen klargestellt werden, unter denen Strafverfolgungsbehörden Zugang zu Daten verlangen können, die in Cloud-Computing-Diensten gespeichert sind; es sollten auf internationaler Ebene vor allem gemeinsame Auffassungen und Grundsätze zu folgenden Fragen entwickelt werden:

- Gegenstand dieser weltweiten Standards sollten sein die Zugangsbedingungen, die Sicherheitsvorkehrungen, die für die Übergabe der Daten an Strafverfolgungsbehörden gelten[69], die Rechte der betroffenen Personen, Aufsicht und Rechtsbehelfsverfahren.

- Es ist zu klären, was der Begriff „Zugang“ in diesem Zusammenhang bedeutet, ob er nur das Auffinden oder auch das Kopieren von in einer bestimmten Vorrichtung gespeicherten Daten bezeichnet. Hier ist zu berücksichtigen, dass der Zugang zu Daten, die in Cloud-Computing-Diensten verarbeitet wurden, häufig die Lokalisierung der entsprechenden Daten und ihre Wiederzusammenstellung oder Umwandlung in eine lesbare Form erfordert.

---

[66] Siehe Erwägungsgrund 90 der vorgeschlagenen Datenschutzverordnung.
[67] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkte 229 bis 232.
[68] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 231.
[69] Wie Verschlüsselung zum Schutz der Daten und sicherer Zugang zum Entschlüsselungscode.

- Es sollte geprüft werden, ob der Zugang zu in einer privaten Cloud-Infrastruktur gespeicherten Daten genauso behandelt werden soll wie der Zugang zu in einer öffentlichen Cloud-Infrastruktur gespeicherten Daten.

- Die Entwicklung von Zertifizierungsregelungen für Cloud-Computing-Dienste könnte ebenfalls Hinweise darauf geben, ob und wie personenbezogene Daten gegen einen solchen Zugang geschützt sind.

105. Abschließend fordert der EDSB die Aufnahme einer spezifischen Bestimmung in die vorgeschlagene Verordnung, in der die Bedingungen festgelegt sind, unter denen ein Zugang aus Nicht-EWR-Ländern zulässig wäre. Eine solche Bestimmung könnte auch die Verpflichtung für den Empfänger des Ersuchens enthalten, in bestimmten Fällen die zuständige Aufsichtsbehörde in der EU zu informieren und zu konsultieren. Die Frage des Zugangs zu Daten durch Strafverfolgungsbehörden sollte auf internationaler Ebene behandelt werden, und die Kommission und die Mitgliedstaaten sollten sich ernsthaft um die Ausarbeitung gemeinsamer Vorschriften und Grundsätze auf dieser Ebene bemühen. Darüber hinaus sollten sie systematisch entsprechende Bestimmungen und Garantien in dieser Frage in die verschiedenen internationalen Abkommen (einschließlich Handelsabkommen) mit Nicht-EWR-Ländern aufnehmen.

V. SPEZIFISCHE KOMMENTARE ZUR MITTEILUNG DER KOMMISSION

106. In der Mitteilung der Kommission wird eine Reihe von Maßnahmen beschrieben, die von der Kommission ergriffen oder gefördert werden sollen, um die Einführung von Cloud-Computing-Diensten in Europa zu unterstützen. Unter anderem sind folgende Maßnahmen vorgesehen: Bereitstellung von Orientierungshilfen, Förderung angemessener Normungs- und Zertifizierungsregelungen, Ausarbeitung von Mustervertragsklauseln und von Verhaltensregeln, Aufbau einer Europäischen Cloud-Partnerschaft und Fortsetzung ihres internationalen Dialogs mit Drittländern und in multinationalen Gremien.

107. Der EDSB begrüßt, dass dem Datenschutz in der Mitteilung eine zentrale Rolle zukommt und dass mit den geplanten politischen Initiativen im Bereich von Cloud-Computing-Diensten das hohe Datenschutzniveau beibehalten werden soll.

V.1. Bereitstellung weiterer Orientierungshilfen

108. Der EDSB begrüßt die Absicht der Kommission, in enger Zusammenarbeit mit Datenschutzbehörden weitere Orientierungshilfen zur Anwendung des Datenschutzrechts auf Cloud-Computing-Dienste bereitzustellen. Er begrüßt, dass der Stellungnahme der Artikel-29-Datenschutzgruppe Rechnung getragen wurde und unterstreicht, dass die vorliegende Stellungnahme ebenfalls Hilfestellung bezüglich des vorgeschlagenen Datenschutzrahmens bietet.

109. Zu arbeiten ist noch an der Klarstellung bewährter Verfahrensweisen in konkreten Punkten wie Verantwortung des für die Verarbeitung Verantwortlichen/Auftragsverarbeiters, angemessene Datenspeicherung in der Cloud-Umgebung, Datenübertragbarkeit und Ausübung der Rechte betroffener

Personen. In der Stellungnahme der Artikel-29-Datenschutzgruppe mit weiteren Beiträgen zur Diskussion der Datenschutzreform[70] werden viele Bereiche aufgeführt, in denen ergänzende Vorgaben des Europäischen Datenschutzausschusses hilfreich wären, insbesondere die Sicherheit der Verarbeitung, die Kriterien zur Bestimmung konkreter hoher Risiken gemäß Artikel 34 Absatz 2 Buchstabe a sowie die Anwendung einiger BCR-Anforderungen auf Auftragsverarbeiter.

110. Der EDSB unterstützt die Ausarbeitung von Verhaltensregeln für Cloud Computing, wie sie in Artikel 38 der vorgeschlagenen Verordnung vorgesehen ist, allerdings unter der Voraussetzung, dass diese den Datenschutzanforderungen in vollem Umfang Genüge tun. Diesbezüglich unterstreicht der EDSB, dass nur die Bestätigung der Verhaltensregeln durch die Aufsichtsbehörden den Unternehmen Rechtssicherheit dahingehend bieten kann, dass sie bei Beachtung dieser Verhaltensregeln im Einklang mit den geltenden Rechtsvorschriften handeln.

V.2. Normung und Zertifizierungsregelungen

111. Im Zusammenhang mit der Schlüsselaktion 1 schlägt die Kommission Normen als wichtigen Schritt in Richtung Akzeptanz von Cloud-Computing-Diensten vor. Die Kommission sieht vor, bis 2013 einen detaillierten Plan der erforderlichen Normen aufzustellen. Diese Normen sollen unter anderem für Sicherheit, Interoperabilität, Datenübertragbarkeit und -umkehrbarkeit gelten.

112. Diese Normen könnten ein entscheidender Erfolgsfaktor für Governance- und Aufsichtsmodelle auf internationaler Ebene sein. Normen werden dazu beitragen, dass alle an der Cloud-Computing-Architektur beteiligten Akteure der Kette einschließlich der Vermittler die gleichen technischen Anforderungen anwenden. Im Sinne eines wirksamen Datenschutzes weist der EDSB allerdings darauf hin, dass diese Normen in vollem Umfang Datenschutzanforderungen erfüllen sollten, insbesondere den Grundsatz des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen, wie sie in Artikel 23 der vorgeschlagenen Verordnung vorgesehen sind. Der EDSB fordert daher die Kommission auf, verstärkt darauf hin zu arbeiten, dass die auf internationaler Ebene festgelegten Normen und Messparameter EU-Anforderungen angemessen abdecken.

113. Es sollte besonders darauf geachtet werden, dass Normen für Cloud-Computing-Dienste wirksam für ein hohes Maß an Sicherheit und Datenschutz sorgen. Dies gilt insbesondere für Folgendes:

- Interoperabilität, die als die Fähigkeit verschiedener Systeme definiert werden kann, zusammen zu funktionieren und Informationen auszutauschen. Aus technischer und wirtschaftlicher Sicht ermöglicht Interoperabilität die Integration verschiedener Datenquellen, was die Verarbeitung dieser Daten auf eine neue Ebene heben kann. Das potenzielle Risiko, dass personenbezogene Daten für einen Zweck verarbeitet werden, der nicht mit dem vereinbar ist, für den sie erhoben wurden, sollte durch Berücksichtigung

[70] Siehe Fußnote 47.

des Grundsatzes der Zweckbegrenzung bei der Anwendung der Interoperabilität auf personenbezogene Daten aufgegriffen werden.

- Datenübertragbarkeit, in Artikel 18 der vorgeschlagenen Verordnung definiert als das Recht der betroffenen Person, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem strukturierten gängigen elektronischen Format zu verlangen. Zur Wahrnehmung dieses Rechts kommt es darauf an, dass die Daten nach ihrer Übermittlung keine Spuren im ursprünglichen System hinterlassen.[71] Technisch sollte es möglich sein, die zuverlässige Löschung von Daten zu überprüfen.

114. Diese Normen sollten Cloud-Diensteanbietern dabei helfen, in der Praxis ihrer Rechenschaftspflicht nachzukommen. Die Kombination von Normen und Zertifizierung durch unabhängige Stellen kann das Vertrauen in Cloud-Dienste stärken und für die Verarbeitung Verantwortlichen und Auftragsverarbeitern dabei behilflich sein, den Regelungsrahmen einzuhalten.

V.3. Ausarbeitung von Mustervertragsbedingungen

115. Der EDSB räumt ein, dass in Anbetracht der deutlich ungleichen Verteilung der Verhandlungsmacht auf Cloud-Diensteanbieter und Cloud-Anwender den Beteiligten bei der Ausarbeitung von Standardvertragsklauseln geholfen werden muss. Wie bereits erörtert, sind Cloud-Diensteanbieter häufig in der Lage, ihren Kunden nicht verhandelbare Vertragsbedingungen zu diktieren. Der EDSB begrüßt daher, dass im Rahmen der Schlüsselaktion 2 der Mitteilung die Kommission Mustervertragsbedingungen ausarbeiten wird, die dazu beitragen werden, dass datenschutzrechtlichen Pflichten und den Rechten betroffener Personen in den kommerziellen Angeboten der Cloud-Diensteanbieter an Kunden (in der Leistungsvereinbarung) und an Verbraucher (in den Vertragsbedingungen) angemessen Rechnung getragen wird.

116. Mit diesen Mustervertragsbedingungen soll erreicht werden, dass in die kommerziellen Angebote an Cloud-Anwender Standardbedingungen aufgenommen werden. Sie unterscheiden sich von den Standardvertragsklauseln, die verwendet werden, um angemessene Garantien für internationale Datenübermittlungen vorzusehen. Auch wenn im Mittelpunkt der Schlüsselaktion 2 nicht Standardvertragsklauseln für internationale Übermittlungen stehen, begrüßt der EDSB dennoch, dass, wie vorstehend in Abschnitt IV.4 dargelegt, in der Mitteilung eine Überprüfung der Standardvertragsklauseln für internationale Übermittlungen und ihre Anpassung an die Cloud-Computing-Umgebung vorgesehen ist.

117. In der Mitteilung werden mehrere datenschutzrechtliche Fragen aufgeführt, die in Mustervertragsbedingungen zu bedenken sind, wie Bewahrung der Daten nach Vertragsende, Offenlegung und Integrität der Daten, Speicherort und Übertragung von Daten, einseitige Änderungen des Dienstes durch die Cloud-Anbieter und Untervergabe. Auch die Artikel-29-Datenschutzgruppe hat Anregungen zu den

[71] Siehe Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 150 bis 152, und Stellungnahme der Artikel-29-Datenschutzgruppe zum Cloud Computing, S. 16.

Aspekten gemacht, die in dem Vertrag konkret geregelt werden sollten.[72] Der EDSB weist darauf hin, dass neben den in der Mitteilung und in der Stellungnahme der Artikel-29-Datenschutzgruppe aufgeführten Themen es vor allem darauf ankommt, dass Musterverträge und Mustervertragsbedingungen angemessene Aussagen auch zu folgenden Aspekten enthalten:

- Streichung unlauterer Klauseln, denen zufolge Cloud-Diensteanbieter die Verantwortung für die Wahrung der Vertraulichkeit und die Sicherung der Daten des Kunden oder die Haftung für den Verlust oder die Beschädigung der Daten ablehnen. Ferner sollten sie angemessene Aussagen zum anwendbaren Recht und zur Streitbeilegung machen, die den betroffenen Personen die Möglichkeit geben, bei einer Aufsichtsbehörde und/oder einem nationalen Gericht eines Mitgliedstaats in Fällen von Verstößen gegen das EU-Datenschutzrecht (z. B. bei einer Datenschutzverletzung oder bei Datenverlust) Rechtsbehelf einzulegen.

- Cloud-Anwender sollten darüber informiert werden, ob die Option besteht, Daten in einer nationalen oder regionalen Cloud zu speichern, und wenn ja, zu welchen Bedingungen.

- Bei späteren Vertragsänderungen ist zu gewährleisten, dass die Cloud-Anwender vor einer Änderung oder einem Widerruf einer Bedingung informiert und um ihre Einwilligung gebeten werden.

- Festlegung angemessener Fristen für die Datenaufbewahrung nach Vertragsende, wobei insbesondere bewährte Vorgehensweisen bezüglich der Aufbewahrungsfristen und der anschließenden Löschung der Daten zu bestimmen sind.

- Gewährleistung angemessener Information der Cloud-Anwender über die Verarbeitung personenbezogener Daten gemäß den Datenschutzanforderungen. Es sollte erwogen werden, in diese Mustervertragsbedingungen weitere Angaben aufzunehmen, die für die Nutzung von Cloud-Computing-Diensten von Bedeutung sind (z. B. anwendbares Recht, Orte, an denen die Daten verarbeitet werden können, Einhaltung von Zertifizierungsregelungen/Normen, Garantien dafür, dass auf allen Ebenen der Infrastruktur und überall da, wohin Daten übermittelt oder gespeichert werden, angemessene Garantien bestehen, konkrete Garantien für sensible Daten, Angaben zur zuständigen Aufsichtsbehörde usw.).

- Gewährleistung, dass betroffene Personen gemäß den Datenschutzanforderungen über ihre Rechte informiert werden, und dass die Standardvertragsbedingungen die Möglichkeit zur wirksamen Ausübung dieser Rechte bieten. Beim Cloud Computing ist unbedingt sicherzustellen,

[72] Siehe Stellungnahme 5/2012 der Artikel-29-Datenschutzgruppe, S. 12 bis 14. In diesen Empfehlungen geht es unter anderem um Sicherheitsmaßnahmen, Vertraulichkeit, Hinzuziehung von Unterauftragnehmern, Bedingungen für die Rückgabe oder Zerstörung der Daten bei Beendigung der Diensterbringung, Meldungen von Datenschutzverletzungen, Audits und den Umgang mit Ersuchen von Strafverfolgungsbehörden.

dass betroffene Personen wirksam das Recht auf Auskunft über ihre Daten und das Recht auf Datenübertragbarkeit wahrnehmen können.

- Bezüglich des Zugangs für Strafverfolgungsbehörden in Drittländern sollte sichergestellt werden, dass Cloud-Anwender zumindest über die rechtlichen Implikationen des Rechtssystems informiert werden, dem die Verarbeitung unterliegt/unterliegen könnte, und dass sie generell über jedes derartige Ersuchen von Strafverfolgungsbehörden unterrichtet werden. Diese Informationen sollten in die Vertragsbedingungen des Cloud-Diensteanbieters sowie in die Garantien für die Übermittlung personenbezogener Daten außerhalb der EU bzw. des EWR (z. B. Standardvertragsklauseln, BCR usw.) aufgenommen werden.

118. Im Zusammenhang mit der Europäischen Cloud-Partnerschaft wird die Kommission an konkreten Vorgaben für die Auftragsvergabe im öffentlichen Sektor arbeiten und gemeinsame Anforderungen für die Auftragsvergabe im Bereich von Cloud-Computing-Diensten festlegen. Der EDSB weist darauf hin, dass diese gemeinsamen Anforderungen für die Auftragsvergabe auch Datenschutzanforderungen einschließlich angemessener Sicherheitsvorkehrungen enthalten müssen, die auf eine den konkreten Risiken der Verarbeitung von Daten des öffentlichen Sektors in einer Cloud-Computing-Umgebung angemessenen Weise festgelegt werden sollten. Geschehen sollte dies nach einer sorgfältigen und auf die Art und Sensibilität der Verarbeitung abgestimmten Datenschutz-Folgenabschätzung (z. B. Differenzierung zwischen der Verarbeitung von Gesundheitsdaten, Daten über Straftaten, vertraulichen Daten usw. durch den öffentlichen Sektor). Im Ergebnis werden die Anforderungen in den Vergabebedingungen je nach Sensibilität der verarbeiteten Daten differenziert werden müssen, was zu unterschiedlichen Reihen gemeinsamer Anforderungen führen sollte.

V.4. Internationaler Dialog

119. Der EDSB hat in seiner Stellungnahme unterstrichen, dass weltweit mehr Zusammenarbeit zwischen Aufsichtsbehörden (Abschnitt IV.6) erforderlich ist, und dass der Behandlung konkreter Probleme im Zusammenhang mit Cloud Computing auf internationaler Ebene große Bedeutung zukommt (Abschnitte IV.5 und IV.7). Er begrüßt daher, dass in der Mitteilung zu Cloud Computing dem globalen Charakter von Cloud-Computing-Diensten gebührend Rechnung getragen wird und dass sie Aktionen zur Förderung der Entwicklung globaler Governance-Normen und zur Umsetzung wirksamerer Verfahren der Zusammenarbeit vorsieht.

120. Der Datenschutz muss zentrales Thema des internationalen Dialogs über Fragen des Cloud Computing sein. Ein solcher Dialog muss auf folgenden Ebenen geführt werden: auf technischer Ebene, um Lösungen und Normen zu schaffen, die ein angemessenes Datenschutzniveau gewährleisten (beispielsweise durch Verankerung des Datenschutzes durch Technik oder durch datenschutzfreundliche Voreinstellungen, und im Bereich Sicherheit); auf Unternehmensebene mit Lösungen, die sich auf Verantwortlichkeit und Governance-Verfahren stützen, und auf politischer Ebene, um zu erkunden, wie die Kommission zusammen mit Drittländern an der Erleichterung weltweiter Interoperabilität der verschiedenen Rechtsrahmen in zentralen Fragen wie Rechtssystem und Zugangsersuchen von Strafverfolgungsbehörden arbeiten kann.

VI. SCHLUSSFOLGERUNGEN

121. Wie es in der Mitteilung heißt, eröffnet das Cloud Computing Unternehmen, Verbrauchern und dem öffentlichen Sektor viele neue Möglichkeiten für die Verwaltung von Daten durch Nutzung entfernter externer IT-Ressourcen. Gleichzeitig bringt es viele Probleme mit sich, insbesondere bezüglich des angemessenen Datenschutzniveaus für die so verarbeiteten Daten.

122. Bei der Nutzung von Cloud-Computing-Diensten besteht die große Gefahr, dass die Verantwortung für von Cloud-Diensteanbietern vorgenommene Verarbeitungen nicht mehr zuzuordnen ist, wenn die Kriterien für die Anwendbarkeit des EU-Datenschutzrechts nicht hinreichend klar definiert sind und wenn die Verantwortung von Cloud-Diensteanbietern zu eng definiert oder interpretiert oder nicht wirksam umgesetzt wird. Der EDSB weist nachdrücklich darauf hin, dass die Nutzung von Cloud-Computing-Diensten keine Senkung von Datenschutzstandards unter die für herkömmliche Datenverarbeitungsvorgänge rechtfertigt.

123. Diesbezüglich enthält die vorgeschlagene Datenschutzverordnung in ihrer ursprünglichen Fassung viele Klarstellungen und Instrumente, mit denen gewährleistet werden könnte, dass Cloud-Diensteanbieter, die ihre Dienste Kunden mit Sitz in Europa anbieten, ein zufrieden stellendes Datenschutzniveau bieten; zu erwähnen ist insbesondere Folgendes:

- In Artikel 3 würde der räumliche Anwendungsbereich der EU-Datenschutzvorschriften klargestellt und würde ihr Anwendungsbereich auf Cloud-Computing-Dienste ausgedehnt;

- In Artikel 4 Absatz 5 würde ein neues Element für die Verantwortung eingeführt, nämlich „Bedingungen“. Dies entspräche dem sich abzeichnenden Trend, dem zufolge es in Anbetracht der der Erbringung von Cloud-Computing-Diensten zugrunde liegenden technischen IT-Komplexität erforderlich ist, den Bereich der Fälle zu erweitern, in denen ein Cloud-Diensteanbieter als für die Verarbeitung Verantwortlicher eingestuft werden kann. Dies würde das tatsächliche Ausmaß des Einflusses auf die Verarbeitungsvorgänge besser wiedergeben;

- Der Verordnungsvorschlag würde Verantwortung und Rechenschaftspflicht von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern stärken, und zwar durch konkrete Verpflichtungen wie Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Artikel 23), Meldungen von Datenschutzverletzungen (Artikel 31 und 32) und Datenschutz-Folgenabschätzungen (Artikel 33). Darüber hinaus würde er von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern den Einsatz von Verfahren verlangen, mit denen die Wirksamkeit der durchgeführten Datenschutzmaßnahmen überprüft wird (Artikel 22);

- Artikel 42 und 43 der vorgeschlagenen Verordnung würden eine flexiblere Nutzung von Verfahren für internationale Datenübermittlungen erlauben, damit Cloud-Anwender und Cloud-Diensteanbieter geeignete Datenschutzgarantien für die Übermittlung personenbezogener Daten an Datenzentren oder Server in Drittländern bereitstellen könnten;

- Artikel 30, 31 und 32 der vorgeschlagenen Verordnung würden die Verpflichtungen von für die Verarbeitung Verantwortlichen und Auftragsverarbeitern bezüglich der Sicherheit der Verarbeitung sowie Informationspflichten bei Datenschutzverletzungen regeln und damit die Grundlage für einen umfassenden und kooperativen Ansatz für das Sicherheitsmanagement zwischen den verschiedenen Beteiligten in einer Cloud-Umgebung schaffen;

- Artikel 55 bis 63 der vorgeschlagenen Verordnung würden die Zusammenarbeit zwischen Aufsichtsbehörden und ihre koordinierte Aufsicht über grenzüberschreitende Verarbeitungsvorgänge stärken, was in einer Umgebung wie dem Cloud Computing von besonderer Bedeutung ist.

124. Dessen ungeachtet schlägt der EDSB unter Berücksichtigung der Besonderheiten von Cloud-Computing-Diensten vor, in der vorgeschlagenen Verordnung folgende Aspekte zu klären:

- Bezüglich des räumlichen Anwendungsbereichs der vorgeschlagenen Verordnung sollte Artikel 3 Absatz 2 Buchstabe a folgendermaßen geändert werden: „…dazu dient, diesen Personen in der Union Waren oder Dienstleistungen *einschließlich der Verarbeitung personenbezogener Daten* anzubieten…“, oder sollte alternativ ein neuer Erwägungsgrund hinzugefügt werden, der besagt, dass die Verarbeitung personenbezogener Daten von betroffenen Personen in der Union durch nicht in der EU ansässige für die Verarbeitung Verantwortliche, die ihre Dienste juristischen Personen mit Sitz in der EU anbieten, in den Anwendungsbereich der vorgeschlagenen Verordnung fällt;

- Wie schon in seiner Stellungnahme zum Datenschutzreformpaket ausgeführt, sollte eine klare Definition des Begriffs „Übermittlung“ hinzugefügt werden;

- Es sollte eine Bestimmung hinzugefügt werden, in der die Bedingungen klargestellt werden, unter denen ein Zugang von Strafverfolgungsbehörden in Nicht-EWR-Ländern zu in Cloud-Computing-Diensten gespeicherten Daten zulässig wäre. Eine solche Bestimmung könnte auch die Verpflichtung für den Empfänger des Ersuchens enthalten, in bestimmten Fällen die zuständige Aufsichtsbehörde in der EU zu informieren und zu konsultieren.

125. Der EDSB weist ferner darauf hin, dass von Seiten der Kommission und/oder der Aufsichtsbehörden (insbesondere des künftigen Europäischen Datenschutzausschusses) zu folgenden Aspekten noch weitere Orientierungshilfen benötigt werden:

- Klarstellung der Verfahren, die zur Überprüfung der Wirksamkeit der Datenschutzmaßnahmen in der Praxis eingerichtet werden sollten;

- Unterstützung von Auftragsverarbeitern bei der Verwendung von BCR und der Einhaltung der entsprechenden Anforderungen;

- Bereitstellung bewährter Vorgehensweisen bei Themen wie Verantwortung des für die Verarbeitung Verantwortlichen/Auftragsverarbeiters, angemessene Speicherung von Daten in der Cloud-Umgebung, Datenübertragbarkeit und Wahrnehmung der Rechte betroffener Personen.

126. Der EDSB räumt ein, dass von der Branche abgefasste und von den zuständigen Aufsichtsbehörden genehmigte Verhaltensregeln einen sinnvollen Beitrag zur Einhaltung der Vorschriften und zu einem Klima des Vertrauens zwischen den verschiedenen Beteiligten leisten könnten.

127. Der EDSB unterstützt, dass die Kommission in enger Absprache mit Aufsichtsbehörden Standardvertragsklauseln für die Erbringung von Cloud-Computing-Diensten ausarbeitet, die den Datenschutzanforderungen Genüge tun, und zwar vor allem

- die Ausarbeitung von Mustervertragsbedingungen, die in die kommerziellen Angebote für Cloud-Computing-Dienste aufgenommen werden;

- die Entwicklung gemeinsamer Bedingungen und Anforderungen für die Auftragsvergabe im öffentlichen Sektor unter Berücksichtigung der Sensibilität der verarbeiteten Daten;

- den weiteren Zuschnitt der Verfahren für internationale Datenübermittlungen auf die Cloud-Computing-Umgebung, insbesondere durch Aktualisierung der derzeitigen Standardvertragsklauseln und durch Vorlage von Standardvertragsklauseln für die Übermittlung von Daten von in der EU ansässigen Auftragsverarbeitern an Auftragsverarbeiter mit Sitz außerhalb der EU.

128. Der EDSB weist darauf hin, dass bei der Entwicklung von Normen und Zertifizierungsregelungen den Datenschutzanforderungen angemessen Rechnung zu tragen ist; es geht insbesondere um Folgendes:

- Anwendung der Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen bei der Entwicklung von Normen;

- Integration von Datenschutzanforderungen wie Zweckbegrenzung und befristete Speicherung in den Entwurf von Normen;

- Verpflichtung der Anbieter, ihren Kunden die für eine solide Risikobewertung erforderlichen Informationen zu geben und über die von ihnen ergriffenen Sicherheitsvorkehrungen sowie über Alarme nach Sicherheitszwischenfällen zu informieren.

129. Schließlich unterstreicht der EDSB die Notwendigkeit einer Behandlung der durch das Cloud Computing aufgeworfenen Probleme auf internationaler Ebene. Er fordert die Kommission auf, sich am internationalen Dialog über Probleme im Bereich des Cloud Computing einschließlich Rechtssystem und Zugang durch Strafverfolgungsbehörden zu beteiligen und regt an, einen Großteil dieser Fragen in verschiedenen internationalen oder bilateralen Abkommen wie Amtshilfeabkommen oder auch Handelsabkommen anzusprechen. Auf

internationaler Ebene könnten weltweite Normen ausgearbeitet werden, in denen Mindestbedingungen und Grundsätze für den Datenzugang durch Strafverfolgungsbehörden festgelegt werden. Er unterstützt ferner die Entwicklung wirksamer Verfahren der internationalen Zusammenarbeit durch die Aufsichtsbehörden, insbesondere im Hinblick auf Probleme beim Cloud Computing.

Brüssel, den 16. November 2012

(unterzeichnet)

Peter HUSTINX
Europäischer Datenschutzbeauftragter