

von **Dr. Sebastian Kraska**

Datenschutz und Cloud-Computing: Entschlieung der 82. Konferenz der Datenschutz- Aufsichtsbehörden

Die deutschen Datenschutz-Aufsichtsbehörden haben am 28./29. September 2011 auf der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in München eine Entschlieung zum Thema “[Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing](http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf)” verabschiedet.

Beitrag von Herrn Rechtsanwalt Dr. Sebastian Kraska, externer Datenschutzbeauftragter und Herrn Diplom-Jurist (univ.) Michael Stolze, LL.M. LL.M..

Die Orientierungshilfe

Die Datenschutz-Aufsichtsbehörden wollen unterstützend und aktiv den datenschutzgerechten Einsatz von Cloud-Computing fördern. Zu diesem Zweck haben die Arbeitskreise Technik und Medien der Konferenz eine Orientierungshilfe erarbeitet, welche sich an „Entscheidungsträger, betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche“ richtet.

Die Orientierungshilfe enthält einen Katalog von Definitionen rund ums Cloud-Computing, sensibilisiert für die datenschutzrechtlichen Schwerpunkte und enthält insbesondere eine Auflistung von vertraglichen und technisch-organisatorischen Mindestforderungen betreffend die Gestaltung und Anwendung dieser Technologie.

Cloud-Anwender, also die datenschutzrechtlich verantwortlichen Stellen, dürften Cloud-Services nur dann in Anspruch nehmen wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stellen in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben (lassen).

Der Nutzen von Cloud Computing

Cloud-Computing hat organisatorische und wirtschaftliche Vorteile. Dazu zählen insbesondere die Skalierbarkeit und die verbrauchsabhängige Bezahlung von Rechenkapazitäten je nach Bedarf. Dies bietet großes Einsparpotenzial in den Bereichen Anschaffung, Betrieb und Wartung von IT-Systemen. Nicht zuletzt ermöglicht Cloud-Computing eine optimierte Verfügbarkeit von Geschäftsanwendungen unabhängig von geographischen Standorten.

Besondere datenschutzrechtliche Risiken

In der Orientierungshilfe werden den Vorteilen von Cloud-Computing entsprechend die datenschutzrechtlichen Schwerpunkte gelegt. Diese „cloud-spezifischen“ Risiken stehen freilich neben den klassischen, wie z.B. durch Schadsoftware oder Angriffe Dritter.

Der datenschutzrechtliche Ausgangspunkt ist, dass Cloud-Anwender verantwortliche Stellen im Sinne des Bundesdatenschutzgesetzes sind und damit die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen zu gewährleisten haben.

Gemäß § 3 Abs. 7 BDSG ist eine verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt und allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Nimmt ein Cloud-Anwender von einem entsprechenden Anbieter nun Cloud-Services in Anspruch, so wird Letzterer als Auftragnehmer nach § 11 Abs. 2 BDSG tätig. Die Verantwortung für die Rechtmäßigkeit bleibt gemäß § 11 Abs. 1 BDSG beim Anwender.

Die datenschutzrechtlichen Schwerpunkte knüpfen bei dem möglichen Kontrollverlust des Anwenders über die Daten an, wenn sich die Datenverarbeitung nicht mehr vor Ort sondern ausgelagert in der „Cloud“ vollzieht und der Anwender selbst keinen konkreten Zugriff mehr auf die Daten hat. Ab dann kann es nur noch schwer nachvollziehbar sein, wo und auf welchen Systemen die Speicherung, Ausführung und Verarbeitung von Daten erfolgt. Die Unsicherheiten erhöhen sich, wenn der Cloud-Anbieter seine Dienstleistungen und Services selbst bei anderen Anbietern einkauft und damit die Transparenz verloren geht.

Mit der IT wird nicht die Verantwortung ausgelagert

Die Orientierungshilfe legt besonderen Schwerpunkt auf die Gefahr der verantwortlichen Stelle, ihrer datenschutzrechtlichen Verantwortung durch die Auslagerung der IT nicht mehr gerecht werden zu können. Die Stichworte lauten hier: Transparenz, Beeinflussung und Kontrolle der Datenverarbeitung.

Die Dokumentation und Protokollierung der Datenverarbeitungsprozesse erfolgt beim Cloud-Anbieter und ist daher für den Anwender meist intransparent, so dass eine wirksame Kontrolle der Einhaltung der datenschutzrechtlichen Pflichten schwierig ist: Könnten Daten, die am Standort X auf Wunsch des Anwenders durch den Anbieter berichtigt, gelöscht oder gesperrt wurden sind (§ 35 Abs. 1-3 BDSG) unverändert am Standort Y noch weiter existieren? Auch können vermeintlich als anonymisiert angesehene Daten (vgl. § 3 Abs. 6 BDSG) wieder re-identifizierbar werden, wenn bei der Verarbeitung in der Cloud weitere Beteiligte hinzu treten, die über Zusatzwissen verfügen und eine Re-Identifizierung möglich machen.

Die verantwortliche Stelle läuft Gefahr, die Rechtmäßigkeit der gesamten Datenverarbeitung nicht mehr gewährleisten zu können, wozu sie aber gesetzlich verpflichtet ist. Die Orientierungshilfe erinnert dabei an eventuelle haftungsrechtliche Konsequenzen durch Schadensersatzforderungen der Betroffenen und mögliche Maßnahmen der Aufsichtsbehörden, wie Bußgelder und Anordnungen (§ 38 Abs. 5 BDSG),

sollten Datenschutzbestimmungen nicht eingehalten werden.

Schwerpunkt: Datentransfers ins außereuropäische Ausland, insb. USA

Finden im Rahmen der Auslagerung von IT-Lösungen Datenverarbeitungen im außereuropäischen Ausland statt, dann gelten grundsätzlich die besonderen Anforderungen der §§ 4b, 4c BDSG. Für Cloud-Computing gelten daher keine Besonderheiten: Besteht in einem solchen „Drittland“ kein von der EU-Kommission anerkannt angemessenes Datenschutzniveau, muss die verantwortliche Stelle (also der Cloud-Anwender) das ausreichende Datenschutzniveau garantieren und vorweisen. Dies kann beispielsweise durch EU-Standardvertragsklauseln oder durch Binding Corporate Rules erfolgen. Der Cloud-Anbieter hat sich dabei zur Einhaltung des EU-Datenschutzniveaus zu verpflichten.

Seit langem gilt die Besonderheit des Safe-Harbor-Agreement mit den USA. Hier hat die Konferenz der Datenschutzbeauftragten nun erstmals konkrete Anforderungen zum Umgang mit US-Cloud-Anbietern festgelegt.

Das Safe-Harbor-Agreement privilegiert datenverarbeitende Unternehmen mit Sitz in den USA, wenn diese sich auf freiwilliger Basis gegenüber dem US-Handelsministerium zur Einhaltung der Safe-Harbor-Grundsätze durch eine Beitragserklärung verpflichten (Stichwort „Selbstzertifizierung“). Abschließend muss eine Datenschutzerklärung veröffentlicht werden. Dies reicht aus, ein „angemessenes Schutzniveau“ zu erlangen. Darüber hinaus muss sich der US-Cloud-Anbieter zur Kooperation mit den europäischen Datenschutzbehörden verpflichten.

Die Orientierungshilfe der Datenschutzbeauftragten verlangt bzw. empfiehlt (je nach Auslegung), dass Cloud-Anbieter und Cloud-Anwender nun eine vertragliche Vereinbarung treffen, die einer Auftragsdatenverarbeitung nach § 11 Abs. 2 BDSG entspricht und so die dort normierten Garantien Gegenstand des Vertrages werden.

Hintergrund ist u.a., dass keine flächendeckende Kontrolle der Selbstzertifizierungen in den USA gewährleistet ist. Sowieso entbehre die Zertifizierung nicht der eigenen Kontrolle. Deutsche Cloud-Anwender müssten vor der ersten Datenübermittlung an ein solches US-Unternehmen prüfen, ob bestimmte Mindestkriterien erfüllt sind. Dies fängt bei der Gültigkeitsprüfung des Zertifikats an und verpflichtet den Cloud-Anwender analog § 11 Abs. 2 Satz 3 BDSG, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Hervorzuheben ist, dass die oben genannten Anforderungen für alle Verträge zwischen US-Cloud-Anbietern und deutschen Cloud-Anwendern ohne Ausnahme gelten, also auch für schon bestehende Verträge. Da dies noch nicht eindeutig geregelt war, kann die Entschließung der Datenschutz-Aufsichtsbehörden die Anpassung einiger Verträge erforderlich machen.

Schwerpunkt: Technische und organisatorische Aspekte

Die Orientierungshilfe legt einen weiteren Schwerpunkt auf die technisch-organisatorische Infrastruktur. Die Entschließung der Datenschutz-Aufsichtsbehörden legt hier einige Mindest-Standards fest:

- Verfügbarkeit: personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß von autorisierten Benutzern verarbeitet werden.
- Vertraulichkeit: nur Befugte können personenbezogene Daten zur Kenntnis nehmen.
- Integrität: personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell. Die Funktionsweise der Systeme ist vollständig gegeben.
- Revisionssicherheit: es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.
- Transparenz: die Verfahrensweise bei der Verarbeitung personenbezogener Daten ist vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden kann.

Die Mindestforderungen der Konferenz

In der Presseerklärung sowie dem Fazit der Entschließung der Konferenz der Datenschutz-Aufsichtsbehörden wurden nochmals die Mindestforderungen bei der Nutzung von Cloud-Computing-Dienstleistungen zusammengefasst. Zu verlangen sind danach mindestens

- offene, transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können;
- transparente, detaillierte und eindeutige vertragliche Regelungen der cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z. B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen“ kann;
- die Umsetzung von abgestimmten Sicherheitsmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender;
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Datenzugriff von US-Ermittlungsbehörden

Wenngleich die Konkretisierungen der datenschutzrechtlichen Anforderungen durch die Aufsichtsbehörden im Sinne der Rechtssicherheit zu begrüßen sind, wird gerade der Aspekt der datenschutzrechtlich in der Regel unzulässigen Nutzung von US-Cloud-Anbietern aufgrund des potentiellen Datenzugriffs von US-Ermittlungsbehörden nicht thematisiert. Danach behalten sich US-Behörden vor, jederzeit auf die Daten von amerikanischen Unternehmen zurückgreifen zu dürfen. Wie dies in den Vorgang der datenschutzrechtlich zulässigen Gestaltung von US-Cloud-Angeboten eingebunden werden kann wurde nicht behandelt.

Autor:

Dr. Sebastian Kraska

Rechtsanwalt