Bei der Betrachtung von Cloud-Computing zum Speichern und Auswerten von Geodaten spielen neben Funktionalität und Preis auch Aspekte der Datensicherheit eine große Rolle. Quelle: © bloomua – Fotolia.com.

Geodaten in der Cloud – so geht's rechtssicher!

Das Cloud-Computing hat weite Teile der Wirtschaft, Verwaltung und Wissenschaft erreicht – trotz anfänglicher Zweifel an Rechtssicherheit und Datenschutz. Aber auch für die Geo-Cloud sind die rechtlichen Anforderungen mit einem praxisnahen Ansatz gut lösbar. Voraussetzung ist, dass Anbieter von Geo-Clouds und die Kunden ihre „Hausaufgaben" machen.

Die bedarfsgerechte Bereitstellung von IT-Leistungen und -Infrastrukturen wie Rechenkapazität, Datenspeicher oder auch fertige Software via Internet – kurz „Cloud-Computing" – hat mittlerweile erheblichen Einfluss auf die IT-Landschaft. Immer mehr Unternehmen, Behörden und wissenschaftliche Einrichtungen profitieren von der flexiblen Inanspruchnahme nutzungsabhängig kostenpflichtiger „Cloud-Services".

In (datenschutz-)rechtlicher Hinsicht war das Cloud-Computing in den letzten Jahren Gegenstand kontroverser Diskussionen – die zuletzt durch die mediale Aufmerksamkeit um PRISM, Tempora und die NSA wieder beflügelt wurden. Die Bedenken auf Kundenseite reichen von der Befürchtung eines Datenverlusts über Zweifel an der Einhaltung des Datenschutzrechts bis hin zu der Angst vor einem Zugriff auf internationale Clouds durch Regierungen oder deren Behörden.

Viele Diensteanbieter und Rechenzentrumsbetreiber haben auf derartige Bedenken reagiert und bieten ihren Kunden in rechtlicher, technischer und organisatori-

scher Ebene qualitativ hochwertige Cloud-Services.

Die Verarbeitung, Nutzung und Bereitstellung von georeferenzierten Informationen unterliegt bekanntlich diversen rechtlichen Anforderungen. Für die Speicherung und Verarbeitung von Geoinformationen in einer Cloud-Umgebung ist in erster Linie ein Blick auf die gesetzlichen Anforderungen des Datenschutzes angebracht.

Geoinformationen und Datenschutz

Die Übertragung von Geoinformationen auf Server des Cloud-Diensteanbieters unterliegt erst dann den gesetzlichen Anforderungen an den Datenschutz, wenn unter den Geodaten auch sogenannte personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG) beziehungsweise der jeweiligen Landesdatenschutzgesetze vorhanden sind. Personenbezogene Daten – nennen wir sie kurz „Personendaten" – sind solche Informationen und Angaben, anhand derer natürliche Personen identifiziert werden können. Typische Personendaten sind der Name der Person, deren Anschrift – auch die E-Mail-Adresse –, weiter deren Alter, Geschlecht, Hobbys, aber gegebenenfalls auch Fotos, Kfz-Kennzeichen oder IP-Adressen.

Geoinformationen können unter gewissen Umständen Aussagen über natürliche Personen „hinter" dem Objekt oder der Fläche treffen. Wann aber Geoinformationen nun tatsächlich einen datenschutzrechtlich relevanten Personenbezug aufweisen, ist bisher nicht abschließend geklärt. Einigkeit dürfte jedenfalls darin bestehen, dass Flächendaten im Maßstab 1:10.000 und kleiner kaum einen Personenbezug aufweisen können. Auch Luftbilder, Satellitenaufnahmen und Orthophotos, deren Auflösung gröber als 40 Zentimeter pro Pixel ist, werden mangels der Erkennbarkeit einzelner Personen datenschutzrechtlich nicht relevant sein. Anders sieht es dagegen aus bei der Erfassung einzelner Grundstücke von Privatpersonen per Koordinaten oder gar per Anschrift. Auch Standortdaten, wie sie bei der Handy-Ortung anfallen und immer häufiger für standortbezogene Dienste erhoben und verarbeitet werden, stellen datenschutzrelevante Personendaten dar.

Damit ergibt sich aus der Art der zu verarbeitenden Geodaten maßgeblich, ob bei deren Erfassung und Verarbeitung datenschutzgesetzliche Belange berührt werden. Soweit die betreffenden Geodaten einen Personenbezug aufweisen, kann dieser gegebenenfalls vor Übermittlung der Daten in die Geo-Cloud mittels Maßnahmen wie Anonymisierung oder Aggregierung wieder „zerstört" werden. Damit sind Techniken gemeint, durch welche die Personendaten von der relevanten Person „getrennt" werden (etwa durch Unkenntlichmachung der Person oder durch Ersatz des Personennamens durch eine anonyme Nummer), oder durch welche die Personendaten derart zusammengefasst werden, dass sie einer einzelnen Person nicht mehr zugeordnet werden können.

Auftragsdatenverarbeitung

Soweit (auch) personenbezogene Geodaten in einer Cloud-Umgebung verarbeitet werden sollen, lässt sich deren Übermittlung in die Cloud mittels der sogenannten Auftragsdatenverarbeitung legitimieren. Das in § 11 des Bundesdatenschutzgesetzes (BDSG) festgelegte „rechtliche Konstrukt" beschreibt die rechtlichen, technischen und organisatorischen Anforderungen an die Übermittlung von Personendaten durch den Auftraggeber (in diesem Fall der Cloud-Kunde) an den Datenverarbeiter (in diesem Fall der Cloud-Diensteanbieter). Auf Ebene der Bundesländer enthalten die Landesdatenschutzgesetze überwiegend korrespondierende Regelungen, wenn auch mit Abweichungen in den Details.

Werden diese Anforderungen bei der Bereitstellung und Nutzung des Geo-Cloud-Dienstes eingehalten, ist die Übermittlung (auch) der personenbezogenen Geodaten in die Cloud in aller Regel rechtlich zulässig. Die Speicherung und Verarbeitung der Geodaten in der Cloud unterliegt dann (nicht cloudspezifisch) den gleichen gesetzlichen Anforderungen, die auch bei einer Speicherung und Verarbeitung auf den eigenen Servern des Kunden einschlägig wären.

Kein „Hexenwerk"

Für die Einhaltung der gesetzlichen Anforderungen an die Auftragsdatenverarbeitung greift die Cloud-Praxis auf bewährte Techniken zurück – etwa aus dem Outsourcing – und adaptiert diese für die Cloud-Umgebung.

Insbesondere muss der Cloud-Provider in seinem Verantwortungsbereich (also in seinen Rechenzentren) wirksame technische und organisatorische Maßnahmen für den Schutz und die Sicherheit der Kundendaten treffen. Die meisten Provider stellen ihren Kunden mittlerweile eine ausführliche Beschreibung dieser Maßnahmen zur Verfügung. Das ist nicht zuletzt deshalb erforderlich, weil die konkrete und schriftliche Vereinbarung dieser in § 9 BDSG abstrakt beschriebenen Maßnahmen zwingender Bestandteil einer rechtskonformen Auftragsdatenverarbeitung ist.

Auch darüber hinaus bietet eine solche Dokumentation den Parteien einen Mehrwert, weil der Cloud-Provider mit der Beschreibung der Maßnahmen die hohe Sicherheit seiner (Geo-)Cloud-Dienste dokumentiert, während der Kunde eine für das eigene IT-Risikomanagement bedeutsame Unterlage erhält.

Soweit der Cloud-Provider Unterauftragnehmer einsetzt, müssen die technischen und organisatorischen Maßnahmen über die gesamte Vertrags- und Leistungskette hinweg etabliert und dokumentiert werden.

Eine ordnungsgemäße Auftragsdatenverarbeitung erfordert weiter die vertragliche Festlegung der in § 11 BDSG skizzierten Regelungspunkte – hierunter beispielsweise die Pflicht des Providers zu einer Berichtigung, Sperrung und Löschung der Kundendaten nach Weisung des betreffenden Kunden. Die meisten Cloud-Diensteanbieter bieten ihren Kunden hierzu mittlerweile ausgewogene und praktikable Vertragsmuster.

Der Vertragsschluss muss zwingend schriftlich erfolgen. Unproblematisch ist dabei aber der Abschluss des Cloud-Vertrags per „Mausklick", wenn dieser dann von einer schriftlichen Vereinbarung über die Anforderungen der Auftragsdatenverarbeitung „flankiert" wird.

Verantwortlichkeit und Prüfungspflichten

Entgegen verschiedentlicher Auffassung führt die Nutzung der Cloud keineswegs zu einer Verlagerung der datenschutzrechtlichen Verantwortung auf den Cloud-Provider. Vielmehr bleiben sowohl Provider als auch dessen Kunde in dem jeweils eigenen Verantwortungsbereich für die Einhaltung der gesetzlichen Anforderungen ver-

Die rechtlichen, technischen und organisatorischen Anforderungen an die Übermittlung von Personendaten werden im Bundesdatenschutzgesetz beschrieben. Quelle: © Gunnar Assmy – Fotolia.com.

antwortlich. Für den Kunden bedingt dieser Umstand vor Vertragsschluss einen sorgfältigen und gesamtheitlichen Blick auf die rechtliche Seite des Datenschutzes und auf deren Umsetzung bei dem (Geo-) Cloud-Anbieter.

Für eine gesetzeskonforme Auftragsdatenverarbeitung ist der Kunde weiter gehalten, vor der ersten Nutzung des Cloud-Dienstes eine „Überprüfung" der bei dem Provider getroffenen Datenschutzmaßnahmen vorzunehmen – und hiernach regelmäßig, beispielsweise im Jahresrhythmus. Weil § 11 BDSG keine persönliche Vor-Ort-Prüfung durch den Kunden voraussetzt, ist die Erfüllung dieser Compliance-Anforderung auch in der Cloud möglich. Hierfür haben sich praktikable Prüfungsmethoden etabliert, bei welchen der Provider eine regelmäßige Prüfung der technischen und organisatorischen Maßnahmen durch fachkundige unabhängige Stellen veranlasst, beispielsweise durch einen Datenschutz-Auditor.

Als besonders hochwertige Alternative hat sich die Zertifizierung der Cloud-Rechenzentren nach ISO/IEC 27001 etabliert. Denn diese umfangreiche Norm deckt im Rahmen ihrer Befassung mit dem Informationssicherheits-Management einen erheblichen Teil der gesetzlichen Anforderungen an Datenschutz und Datensicherheit ab. Zudem ist die jährliche Prüfung der Zertifizierungsanforderungen durch eine hierzu berechtigte Stelle ein zwingender Bestandteil des Zertifikats.

Geo-Clouds in „Übersee"

Aufgrund des innerhalb der Europäischen Union relativ einheitlichen Datenschutzniveaus kann aus Rechtssicht eine Cloud-Datenverarbeitung grundsätzlich in jedem EU-Staat erfolgen – solange die gesetzlichen Anforderungen an die Auftragsdatenverarbeitung eingehalten werden. Außerhalb der EU fehlt allerdings in den meisten Staaten ein ausreichendes gesetzliches Datenschutzniveau für die Durchführung einer Auftragsdatenverarbeitung – so beispielsweise in den USA und in Indien.

Für die Nutzung einer außerhalb der EU stationierten Geo-Cloud müssen daher weitergehende Maßnahmen getroffen werden. Zunehmend verwenden die internationalen Cloud-Provider hierfür die sogenannten EU-Standardvertragsklauseln. Deren verbindliche Vereinbarung in unveränderter Form – beispielsweise als Anhang zu dem eigentlichen Cloud-Vertrag – führt nach wohl einhelliger Auffassung in rechtlicher Sicht zu einem ausreichenden vertraglichen Datenschutzniveau des Cloud-Providers. Damit ist auch die Nutzung von Geo-Clouds in „Übersee" im Einklang mit deutschem Datenschutzrecht möglich – wenn gleichzeitig die Anforderungen an die Auftragsdatenverarbeitung eingehalten werden.

Für in den USA ansässige Provider ist auf ähnliche Weise ein Rückgriff auf die Grundsätze des „Safe Harbor" möglich. Hierbei handelt es sich um ein Abkommen zwischen der EU-Kommission und der US-Regierung, das ebenfalls Maßnahmen für Datenschutz und Datensicherheit beschreibt. Weil die Safe-Harbor-Grundsätze innerhalb der EU allerdings verschiedentlich in die Kritik geraten sind, hat die Legitimierung der Cloud-Datenverarbeitung mittels Safe Harbor in der letzten Zeit bei mehreren US-Cloud-Anbietern an Bedeutung verloren.

Welche der etablierten Wege der Anbieter einer „Übersee"-Cloud auch geht: Er ist gut damit beraten, die Einhaltung der zusätzlich getroffenen Maßnahmen und deren Aufrechterhaltung regelmäßig gegenüber seinen Kunden belastbar zu dokumentieren. Für einen solchen Nachweis bieten sich wiederum Prüfberichte oder Testate externer Prüfer an. Interessenten einer Geo-Cloud, deren Server sich in einem Staat ohne gesetzlich etabliertes Datenschutzniveau befinden, sollten den Provider vor Vertragsschluss nach derartigen Unterlagen ausdrücklich fragen und diese im Zweifel zur Prüfung anfordern.

Datenspionage

Nicht zuletzt durch die mediale Berichterstattung der letzten Monate hat sich die Angst vor Zugriffen auf die eigenen Daten bei vielen Unternehmen wieder vergrößert. Dabei ist es eigentlich keine neue Erkenntnis, dass es eine vollständige Sicherheit der an das Internet angebundenen Datenverarbeitungsanlagen kaum geben kann. Wie auch in anderen Bereichen ergibt sich das technische Sicherheitsniveau der datenverarbeitenden Server zumeist aus einem wirtschaftlich tragbaren Kompromiss zwischen Kosten und Nutzen.

Bereits seit Längerem sahen sich insbesondere US-Cloud-Provider der Furcht potenzieller Kunden vor staatlich oder behördlich angeordneter Offenlegung der anvertrauten Kundendaten ausgesetzt. Ursache ist der „USA Patriot Act" („Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act") aus dem Jahre 2001. Nach diesem Gesetz können US-Ermittlungsbehörden und US-Geheimdienste unter bestimmten Voraussetzungen von US-Unternehmen die Herausgabe von (Kunden-)Daten verlangen.

Manche US-Cloud-Provider bieten ihren Kunden daher einen Cloud-Vertragsschluss mit einer innerhalb der EU ansässigen Tochtergesellschaft. Damit soll das

EU-Datenschutzrecht, das die Herausgabe von Personendaten an Institutionen aus „Übersee“ grundsätzlich nicht gestattet, dabei helfen, dass der US-Anbieter sich einem Herausgabeverlangen erfolgreich widersetzen kann. Andere US-Provider nehmen in ihre Cloud-Verträge eine „Abwehrklausel“ auf, nach welcher sie versprechen, sich gegen behördliche Herausgabeverlangen auf dem Rechtswege zur Wehr zusetzen.

Insbesondere durch die Enthüllungen um die Tätigkeit der NSA hat die Furcht vor Datenspionage in den letzten Monaten eine weitere Ebene erreicht. Auch aus anderen Richtungen sind gezielte Angriffe auf Datenverarbeitungssysteme zwecks der Entwendung von Daten längst an der Tagesordnung und werden wohl weiter zunehmen. Dabei könnten die Rechenzentren der Cloud-Provider vermehrt im Fokus stehen. In aller Regel werden dort aber auch die Sicherheitsmaßnahmen um ein Vielfaches höher sein als auf den Servern der meisten Unternehmen, Behörden und wissenschaftlichen Einrichtungen – wo bekanntlich ebenfalls das Kosten-Nutzen-Prinzip gelten muss.

Fazit und Ausblick

Die (datenschutz-)rechtlichen Anforderungen sind für den Bereich der Geo-Clouds mit überschaubarem Aufwand gut umsetzbar. Insbesondere wenn der Geo-Cloud-Provider bereits bei der Gestaltung seines Geo-Cloud-Services die rechtliche Seite sorgfältig und kundenorientiert im Blick hatte, wird für seine Kunden der Weg zu einer rechtskonformen Nutzung der Geo-Cloud in aller Regel erfreulich kurz sein. Auch Besonderheiten auf Ebene des Landesdatenschutzes lassen sich zumeist ohne Weiteres berücksichtigen.

Im Hinblick auf die Sicherheit der „in der Cloud“ verarbeiteten Geodaten empfiehlt sich vorab eine sorgfältige Auswahl und Betrachtung der infrage kommenden Cloud-Provider. Eine sorgfältige Prüfung, ob und welche Daten und Informationen man intern oder extern verarbeiten (lassen) möchte, ist ohnehin unverzichtbarer Bestandteil des IT-Risikomanagements und sollte auch für den Bereich der Geo-Clouds nicht vernachlässigt werden. Mit alledem dürften Cloud-Infrastrukturen auch für Geodaten eine attraktive und zukunftsfähige Schlüsseltechnologie darstellen.

Autor und Kontakt:

Jan Schneider

Fachanwalt für IT-Recht und Partner der Sozietät SKW Schwarz Rechtsanwälte im Büro Düsseldorf, berät seit vielen Jahren in allen Bereichen des IT-Rechts. Er ist Autor zahlreicher Veröffentlichungen und häufig angefragter Referent und Keynote-Speaker.

T: +49 (0) 211.82 89 59-0

E: j.schneider@skwschwarz.de

I: www.skwschwarz.de