

Dr. Ivo Geis

Cloud Archiving

Eine archivrechtliche und
datenschutzrechtliche Bewertung

Hamburg, September 2009
<http://www.ivo-geis.de/>
geis@ivo-geis.de

Cloud Archiving – eine archivrechtliche und datenschutzrechtliche Bewertung

Literatur

Geis/Helfrich, Datenschutzrecht, 1. Aufl., München 2007.

Jotzo, Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232 ff.

Niemann/Paul, Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings, K&R 2009, 444.

Pohle/Ammann, Über den Wolken...- Chancen und Risiken des Cloud Computing, CR 2009, 273 ff.

Simitis, Bundesdatenschutzgesetz, 2. Aufl., Baden-Baden, 2006.

Söbbing, Cloud und Grid Computing: IT-Strategien der Zukunft rechtlich betrachtet, MMR 5/2008, XII.

Spieß, USA: Cloud Computing – Schwarze Löcher im Datenschutzrecht, MMR 5/2009, XI.

Abkürzungen

CR Computer und Recht, Verlag Dr. Otto Schmidt, Köln.

K&R Kommunikation & Recht, Verlag Recht und Wirtschaft, Frankfurt am Main.

MMR MultiMediarecht, Beck Verlag, München.

Das elektronische Archivieren erlebt durch das Cloud Archiving einen radikalen Umbruch. Die Dokumente werden nicht mehr lokal in einem Rechenzentrum gespeichert, sondern in weltweit vernetzten Rechenzentren, der Cloud. In dieser Cloud wechseln die Dokumente in Sekundenbruchteilen den Speicherplatz. Der Nutzer kann damit nicht feststellen an welchem Ort, ob im Inland oder im Ausland, sich die Daten physisch befinden. Diese neue Dimension der Unbestimmbarkeit des Archivierungsortes und der Internationalität der Cloud sind archivrechtlich (1.0) und datenschutzrechtlich (2.0) kritisch. Um das Cloud Archiving, dem für die nächsten Jahre ein breites Wachstum prognostiziert ist, rechtlich abzusichern, werden Vereinbarungen zwischen dem Anbieter der Dienstleistung „Cloud Archiving“ und dem Nutzer empfohlen (3.0).

1.0 Aufbewahrungspflichten

Das Archivieren in globalisierten Cloud Systemen ist steuerrechtlich problematisch, denn grundsätzlich sind steuerlich relevante Aufzeichnungen im Inland zu führen und aufzubewahren, § 146 Abs. 2 Satz 1 AO. Nur unter strengen Anforderungen ist die Archivierung im europäischen Ausland (1.1) und nicht-europäischen Ausland (1.2) möglich.

1.1 Archivierung im europäischen Ausland

Ausnahmsweise kann die zuständige Finanzbehörde entsprechend dem zum 1.1.2009 eingefügten § 146 Abs. 2a AO auf Antrag bewilligen, dass steuerrechtlich relevante Dokumente in einem EU-Mitgliedstaat oder einem EWR-Mitgliedstaat mit Amtshilfeübereinkommen¹ archiviert werden. Dem muss die ausländische Finanzbehörde zustimmen und die deutsche Finanzbehörde muss auf die archivierten Dokumente zugreifen können. Die Archivierung außerhalb der EU-Grenzen bleibt problematisch. Wenn § 146 Abs. 2a AO als abschließende Spezialnorm bewertet wird, die das Archivieren nur innerhalb des EU-Raums einschließlich der EWR-Staaten erlaubt, dann wäre es steuerrechtlich nur möglich, Cloud-Systeme zu nutzen, die auf den EU-Raum und die EWR-Staaten beschränkt sind. Dies käme einem steuerrechtlichen Verbot gleich, dass Unternehmen Cloud-Systeme außerhalb des EU-Raums nutzen. In einer globalisierten Wirtschaft wäre dies eine realitätsferne Interpretation des § 146 Abs. 2a AO. Näher liegt es, die Regelung des § 146 Abs. 2a AO als

¹ Island, Liechtenstein und Norwegen.

ein Privileg für den EU-Raum zu interpretieren, das durch die räumliche Nähe der Cloud-Systeme für deutsche Finanzbehörden begründet ist.²

1.2 Archivierung im nicht-europäischen Ausland

Das Nutzen von Cloud-Systemen außerhalb des EU-Raums steht unter den strengen Anforderungen des § 148 AO: Die Aufbewahrung im nicht europäischen Ausland kann von der Finanzbehörde bewilligt werden, wenn das Aufbewahren im Inland für den Steuerpflichtigen Härten mit sich bringt und die Besteuerung nicht beeinträchtigt wird. Härten könnten in dem Verzicht auf organisatorisch sinnvolle Lösungen wie die zentrale Archivierung für einen globalisierten Konzern bestehen. Die Besteuerung wird nicht beeinträchtigt, wenn das Cloud Archiving nach den Grundsätzen der ordnungsmäßigen Archivierung organisiert ist und damit die Integrität der archivierten Dokumente gesichert ist und sie in angemessener Zeit wieder auffindbar sind. Vorbehalte der Finanzbehörden, dass diese Funktionalitäten in weltweit vernetzten Rechnersystemen erfüllt werden, sind berechtigt. Deshalb sollten vertragliche Regeln zwischen dem Anbieter des Cloud Archiving und dem Nutzer entwickelt werden, die das Cloud Archiving nach den Anforderungen der ordnungsmäßigen Archivierung sicherstellen. Das handelsrechtliche Aufbewahrungsrecht kann eine Stütze für die Argumentation sein, das Cloud Archiving zu bewilligen, denn dieses Aufbewahrungsrecht verlangt nicht, dass Buchungsbelege und Handelsbriefe im Inland aufbewahrt werden. Verlangt wird, dass die elektronisch archivierten Dokumente während der gesetzlichen Aufbewahrungsfrist von 10 Jahren verfügbar sind und jederzeit innerhalb angemessener Frist lesbar gemacht werden können, § 257 Abs. 3 Satz 1 HGB. Handelsrechtlich ist damit das globalisierte Cloud Archiving nicht untersagt. Im Ergebnis kann das globalisierte Cloud Archiving nach § 148 AO bewilligt werden, wenn dies nach den Grundsätzen der ordnungsmäßigen Archivierung organisiert und vertraglich zwischen Nutzer und Anbieter abgesichert wird. In diesem Vertrag müssen sich der Anbieter des Cloud Archiving und der Nutzer auch verpflichten, die datenschutzrechtlichen Anforderungen zu erfüllen.

² In diesem Sinne auch die Auslegung des § 146 Abs. 2a AO von *Niemann/Paul*, K&R 2009, 444, 450 f.

2.0 Datenschutzrecht

Archiviert ein Unternehmen Dokumente in einer globalisierten Cloud, so werden mit den Dokumenten personenbezogene Daten von Mitarbeitern und Kunden gespeichert. Diese Daten sind durch die Regeln der Auftragsdatenverarbeitung (2.1) und der Datenübermittlung (2.2) geschützt.

2.1 Auftragsdatenverarbeitung

Für die Auftragsdatenverarbeitung nach § 11 BDSG ist charakteristisch, dass der Auftraggeber dafür verantwortlich ist, dass die datenschutzrechtlichen Vorschriften beachtet werden. Die technisch-organisatorische Komplexität vernetzter Rechnersysteme, in denen die Daten ständig ihren Standort wechseln, macht es fragwürdig, ob das Rechtsmodell der Auftragsdatenverarbeitung angewendet werden kann. Wie soll der Auftraggeber für die Daten verantwortlich sein, wenn er nicht weiß, wo sich die Daten befinden, und wenn er wesentliche Funktionen auf den Betreiber des Cloud Archiving als Auftragnehmer übertragen hat?³

Auftragsdatenverarbeitung für das üblicherweise angebotene globalisierte Cloud Archiving kommt schon deshalb nicht in Frage, weil diese Vorschrift auf den EU-Raum als den Geltungsbereich der EU Datenschutzrichtlinie beschränkt ist.⁴ Aus diesen Gründen kann die Auftragsdatenverarbeitung nach § 11 BDSG nicht als eine sichere Rechtsgrundlage für das Cloud Archiving bewertet werden. Im Ergebnis sollte eine Lösung nach den Grundsätzen der Datenübermittlung gesucht werden.

2.2 Datenübermittlung

Wenn Cloud Archiving nicht als Auftragsdatenverarbeitung zu bewerten ist, sondern als Datenübermittlung, dann gelten die Regeln der Interessenabwägung nach § 28 Abs. 1 Nr. 2 BDSG (2.2.1). Werden im Rahmen des globalisierten Cloud Archiving personenbezogene Daten in das nicht europäische Ausland übermittelt, so gelten zusätzlich die Anforderungen an das angemessene Datenschutzniveau nach § 4c Abs. 2 BDSG (2.2.2).

2.2.1 Die Interessenabwägung

Nach § 28 Abs. 1 Nr. 2 BDSG ist zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen abzuwägen. Verantwortliche Stelle ist der Nutzer eines Cloud-Dienstes, Betroffene sind deren Daten als Bestandteile der

³ Zur Abgrenzung von Auftragsdatenverarbeitung und Funktionsübertragung siehe *Walz* in *Simitis* (Hrsg.), BDSG, 6. Aufl. 2006, § 11 Rn. 17 ff.

⁴ Siehe hierzu *Walz* in *Simitis* (Hrsg.), BDSG, 6. Aufl. 2006, § 11 Rn. 4.

Dokumente, die dem Cloud-Anbieter zum Archivieren übermittelt werden. Der Nutzer eines Cloud-Dienstes ist als verantwortliche Stelle an einer effektiven Unternehmensinfrastruktur interessiert. Die Arbeitnehmer und Kunden sind daran interessiert, dass ihre Daten rechtskonform gespeichert werden.⁵ Diese datenschutzrechtlichen Anforderungen decken sich mit den Anforderungen an die ordnungsmäßige Archivierung: Die Daten müssen integer und wieder auffindbar sein, sie müssen vor dem Zugriff Unberechtigter geschützt sein und dürfen nicht Dritten übermittelt werden.

2.2.2 Das angemessene Datenschutzniveau

Die globalisierte Cloud-Dienstleistung ist mit dem datenschutzrechtlichen Vorbehalt belastet, dass ein angemessenes Datenschutzniveau außerhalb des EU-Raums nicht angenommen wird. Deshalb muss sich der Nutzer des Cloud Archiving nach § 4c Abs. 2 Satz 1 BDSG als die datenschutzrechtlich verantwortliche Stelle von der zuständigen Aufsichtsbehörde das globalisierte Cloud Archiving genehmigen lassen.⁶ Dafür muss er der Aufsichtsbehörde ausreichende Garantien vorweisen, dass das Persönlichkeitsrecht der Betroffenen geschützt und sie die damit verbundenen Rechte ausüben können. Die Garantien können sich aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Als ausreichende Garantien gelten die Klauseln der Standverträge I und II der EU Kommission im Sinne von Artikel 26 Absatz 2 der Richtlinie 95/46/EG.⁷ Diese Klauseln können in Binding Corporate Rules integriert werden. Binding Corporate Rules (BCR) gelten EU-rechtlich als die angebrachte Lösung, dass multinationale Unternehmen für die Übermittlung personenbezogener Daten außerhalb der Europäischen Union einen datenschutzrechtlichen Standard sichern.⁸ Solche Regeln schaffen ein System, an das sich die Nutzer der Dokumente halten können und das für die Betroffenen den Umgang mit ihren Daten transparent macht.⁹ Dieses Garantiesystem sollte die Aufsichtsbehörde überzeugen, einen Vertrag über das globalisierte Cloud Archiving zu genehmigen.

⁵ Siehe näher zur Interessenabwägung *Simitis* in *Simitis* (Hrsg.), BDSG, 6. Aufl. 2006, § 28 Rn. 133-183.

⁶ Siehe zu den genehmigungspflichtigen Ausnahmen *Simitis* in *Simitis* (Hrsg.), BDSG, 6. Aufl. 2006, § 4c Rn. 29-68.

⁷ Ziffer 28a und 28b in *Geis/Helfrich*, Datenschutzrecht, 2007, München.

⁸ Working Paper 155 der Article 29 Data Protection Working Party.

⁹ Siehe zu dieser Lösung: *Spieß*, MMR 5/2009, XI; *Söbbing*, MMR 5/2008, XII f.; *Jotzo*, MMR 2009, 232 ff. und *Pohle/Ammann*, CR 2009, 273, 277.

3.0 Ergebnis

Die technisch-organisatorische Komplexität des globalisierten Cloud Archiving bestimmt die archivierungsrechtlichen und datenschutzrechtlichen Bestandteile eines Vertrages zwischen Nutzer und Anbieter des Cloud Archiving. Archivierungsrechtlich muss geregelt sein, dass die Dokumente integer und wieder auffindbar archiviert werden.

Dadurch werden zugleich die datenschutzrechtlichen Anforderungen gesichert, dass der Betroffene den Auskunftsanspruch wahrnehmen kann, die Daten vor dem Zugriff Unberechtigter geschützt sind und die Daten nicht Dritten übermittelt werden.

Damit ist auch ein angemessenes Datenschutzniveau gegeben, sodass die Dokumente mit den personenbezogenen Kunden- und Mitarbeiterdaten im Rahmen des globalisierten Cloud Archiving in einem nicht europäischen Staat gespeichert werden können. Dies ist die Grundlage, dass die Datenschutzaufsichtsbehörde die erforderliche Genehmigung für den Vertrag über das globalisierte Cloud Archiving erteilt.