ecolex
FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT
JUNI 2011
06
www.ecolex.at
489–584

Marktmanipulation

Börsenrechtliches
Anleger-Irreführung

Ein neues Geschäftsmodell
Cloud Computing

Bankmanager
Variable Vergütungen

Im Focus des IZVR
Kinderfoto Natascha Kampusch

Geistiges Eigentum im
Weltraumrecht

Glücksspiel
Werbung ohne Grenzen

Versandhandel von
Arzneimitteln

MANZ

Cloud Computing – trübe Aussichten für ein neues Geschäftsmodell?

Cloud Computing gilt als Zauberwort für eine massive Kostenreduktion der IT-Ausgaben. Aber es gibt große rechtliche Unsicherheiten, vor allem aufgrund datenschutzrechtlicher Implikationen und Haftungsfragen.

RAINER KNYRIM / VIKTORIA HAIDINGER

A. Einleitung

In Weiterentwicklung von Application Service Providing (ASP) bietet Cloud Computing ein flexibles Modell, Daten und Software nicht lokal zu verarbeiten, sondern genau dort, wo Kapazitäten vorhanden sind. Dafür werden Serverfarmen, die über die ganze Welt verteilt sind, verwendet und dabei die unterschiedlichen Zeitzonen genutzt. Häufig lässt sich nicht mehr feststellen, wo genau sich die Daten physisch befinden. Gerne wird die Wendung benutzt, dass sich mit Cloud Computing Speicher, Rechenkapazitäten und Softwareanwendungen „aus der Steckdose" beziehen lassen. Je nachdem, ob die „Cloud" jedermann zugänglich ist oder nur einem beschränkten Personenkreis, wird zwischen Private und Public Clouds unterschieden. Beispiele für Public Clouds sind die Angebote von Amazon AWS, Google oder Microsoft Azure, wobei der Anwender nicht mitbestimmen kann, mit welchen weiteren Anwendern er sich die Nutzung der Cloud teilt. Eine Private Cloud steht einer „closed comunity", bspw einem Konzern, zur Verfügung.[1])

Es werden verschiedene Modelle unterschieden, je nachdem ob nur Rechenzeit (Infrastructure as a Service), Software (Software as a Service), Speicherplatz oder Entwicklungsplattformen (Platform as a Service) angeboten werden. Werden Software oder Speicher-

Dr. *Rainer Knyrim* ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte, Mag. *Viktoria Haidinger,* LL. M., ist stv. Leiterin der Stabsabteilung Statistik der WKÖ.

1) Näheres s bei *Birk/Wegener,* Über den Wolken: Cloud Computing im Überblick, DuD 9/2010.

platz zur Verfügung gestellt, so wird es häufig zur Verarbeitung personenbezogener Daten, zB von Kunden oder Mitarbeitern, kommen. Genau hier kommt es zu datenschutzrechtlichen Implikationen. Es darf vorausgeschickt werden, dass Public Clouds, wenn diese tatsächlich „in der Cloud" global betrieben werden, mit europäischem Datenschutzrecht nur schwer vereinbar sind. Datenschutzkritiker werden geneigt sein, die europäischen Datenschutzstandards als Wettbewerbshindernis bloßzustellen. UE ist jedoch genau das Gegenteil der Fall. Um mit *Weichert* zu sprechen, ist ein professioneller Einsatz dieser Systeme ohne die Gewährleistung des nötigen Schutzniveaus nicht verantwortbar.[2]) Vorauszuschicken ist aber auch, dass heute „traditionelle" ASP-Anwendungen, die in Wirklichkeit nur auf einem Server eines Anbieters laufen, aus Marketingerwägungen oft als Cloud-Systeme bezeichnet werden.[3]) Dies kann sich auf den Absatz letztlich statt positiv aufgrund vermeintlicher Datenschutzbedenken auch negativ auswirken, obwohl in Wirklichkeit rechtlich eine einfache Datendienstleistung vorliegt, die unter Einhaltung dafür entwickelter und lange erprobter datenschutzrechtlicher Lösungskonzepte problemlos genutzt werden kann.[4])

B. Anwendungsbereich des DSG 2000

Sobald personenbezogene Daten in der Cloud verarbeitet werden, ist Datenschutzrecht sachlich anwendbar (§ 1 Abs 1).[5]) Daran ändert auch die kapazitätsbedingte Aufspaltung der Daten auf verschiedene Server in der Cloud nichts.[6]) Werden anonymisierte oder Daten ohne Personenbezug verwendet, so ist das DSG 2000 nicht anwendbar, jedoch sind möglicherweise andere Vorschriften zu beachten.[7])

Österreichisches Datenschutzrecht ist nach § 3 Abs 1 anwendbar, wenn der Auftraggeber seinen Sitz in Österreich hat und die Daten im Inland verwendet werden.

C. Vertragsverhältnis Anwender – Cloud-Anbieter

1. Vertragstyp

In der dLit wird zum Vertragsverhältnis zwischen Anwender und Cloud-Anbieter vertreten, es handle sich um einen typengemischten Vertrag mit im Wesentlichen mietvertraglichem Charakter.[8]) Welche Rolle diese Bewertung nach nationalem Recht tatsächlich spielt, mag jedoch fraglich sein, denn beim Großteil der Anbieter besteht kein Spielraum für eine Vertragsgestaltung; es gilt der Grundsatz „take it or leave it": Die meisten Anbieter sehen in ihren AGB die Anwendbarkeit des US-Rechts sowie Gerichtsstände in den USA vor. Vertragsrechtliche Ansprüche wären demnach im Ausland durchzusetzen, was äußerst kompliziert sein kann. Für Verletzungen des DSG 2000 haftet der Anwender als datenschutzrechtlicher Auftraggeber voll im Inland, könnte sich aber aus den genannten Gründen meist nicht regressieren.[9])

2. Datenschutzrechtliche Stellung des Cloud-Anbieters und gesetzliche Vorgaben

Das DSG 2000 kennt drei Rollen: den Betroffenen, dessen Daten verwendet werden, den Auftraggeber, der „Herr über die Daten" ist, und den Dienstleister, dem zur Herstellung eines Werkes Daten überlassen werden (§ 4 Z 3 bis 5). Der Anwender lagert seine „eigenen" Daten in die Cloud aus, er ist somit Auftraggeber. Der Cloud-Anbieter speichert und/oder verarbeitet diese Daten in rein technischer Hinsicht, er ist daher Dienstleister.

§ 10 Abs 1 normiert die sog Dienstleisterfreiheit, dh, jeder Auftraggeber darf sich eines Dienstleisters bedienen, sofern dieser ausreichend Gewähr für eine rechtmäßige und sichere Datenverwendung bietet. Die DSK hat letztere Voraussetzung mit dem Schlagwort „Verlässlichkeit" zusammengefasst.[10])

§ 10 Abs 1 Satz 2 enthält eine Überprüfungspflicht des Auftraggebers. Diese Prüfpflicht wird von der Lit auf das Vorliegen einer entsprechenden Berufsberechtigung beschränkt.[11]) Denn es ist für die meisten Unternehmen unmöglich zu überprüfen, ob der Dienstleister bspw die Sicherheitsmaßnahmen nach § 14 einhält.[12]) § 11 Abs 1 zählt die gesetzlichen Pflichten des Dienstleisters auf, welche auch die gem § 14 erforderlichen Datensicherheitsmaßnahmen umfassen. Die nähere Ausgestaltung dieser Pflichten samt der konkreten Datenverwendung durch den Dienstleister und allfällige weitere vertragliche Bestimmungen sind zu Beweiszwecken in Schriftform festzuhalten (§ 11 Abs 2). Ergibt sich jedoch aus den AGB des Cloud-Anbieters, dass die Maßnahmen nach § 14 gerade nicht eingehalten werden, so wird die Überlassung wohl unzulässig sein.

3. Wichtige Klauseln[13])

Nachfolgend werden einige Klauseln erörtert, die neben den üblichen Bestimmungen, wie Kündigungsfristen udgl, jedenfalls in einen Cloud-Vertrag aufgenommen werden sollten, sofern dies möglich ist, da es

2) *Weichert,* Cloud Computing und Datenschutz, ULD-Website unter https://www.datenschutzzentrum.de/cloud-computing/; Pkt 13.

3) So auch *Peyerl,* Cloud Computing – Datenschutzrechtliche Aspekte bei der „Datenverarbeitung in der Wolke", JusIT 2011/30, 57. Dieser Beitrag erschien erst kurz vor Drucklegung dieses Artikels, weshalb nicht im Detail darauf eingegangen werden kann.

4) Siehe dazu schon *Knyrim,* Checkliste: Zulässigkeit eines internationalen Datenverkehrs, ecolex 2002, 470 (471 f).

5) §§-Angaben ohne Bezeichnung beziehen sich auf das DSG 2000.

6) *Conrad/Hausen,* Datenschutzrechtliche Aspekte von Data Loss Prevention und Cloud-Computing, in *Büchner/Briner* (Hrsg), DGRI Jahrbuch 2009, 40.

7) In Deutschland wird zB betreffend Buchhaltungsdaten auf das Verbot der Speicherung im Ausland verwiesen (§ 146 Abs 2 Satz 1 AO, s *Weichert* (FN 2) Pkt 13). Die BAO kennt keine korrespondierende Bestimmung.

8) *Phole/Ammann,* Über den Wolken … – Chancen und Risken des Cloud Computings, Computer und Recht 5/2009, 274.

9) *Peyerl,* Wolkig bis trüb: Wer haftet laut österreichischem Datenschutzgesetz bei Datenpannen in der Wolke, Computerwelt 19. 11. 2010.

10) Empfehlung der DSK 9. 8. 2006, K121.102/0012-DSK/2006; 24. 7. 2009, K211.897/0004-DSK/2009.

11) *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 10 Anm 3.

12) Die Pflicht zur Überprüfung vertreten zur deutschen Rechtslage *Conrad/Hausen* (FN 4) 38.

13) Siehe dazu auch den Leitfaden Cloud Computing – Recht, Datenschutz und Compliance von EuroCloud Deutschland_eco e.V. unter www.eurocloud.de/2010/12/02/eurocloud-leitfaden-recht-datenschutz-compliance/

sich, wie bereits erwähnt, bei den meisten Verträgen der Cloud-Anbieter um nicht verhandelbare AGB handelt.

a) Rechts- und Gerichtsstandswahl

Bei Gerichtsstandsklauseln ist die Schriftlichkeit zu beachten, wobei elektronische Medien diese Voraussetzung ohne elektronische Signatur häufig nicht erfüllen. So schreibt § 104 Abs 1 JN vor, dass die Vereinbarung urkundlich nachgewiesen werden muss, was von der hL und der Rsp mit Unterschriftlichkeit gleichgesetzt wird. Dazu merkt allerdings *Wong*[14]) kritisch an, dass diese Interpretation weder im Gesetzeswortlaut ausreichende Stütze finde, noch mit Hilfe der teleologischen Interpretation abgeleitet werden könne.[15]) Laut Art 23 Abs 1 EuGVVO ist die Gerichtsstandsvereinbarung *„schriftlich oder mündlich mit schriftlicher Bestätigung"* zu schließen, wobei es ausreicht, dass jene Partei unterschreibt, welche die Urkunde nicht ausgestellt hat.[16])

Hingegen muss eine zulässige Rechtswahl nach Art 3 Abs 1 Rom I-VO *„ausdrücklich erfolgen oder sich aus den Umständen des Falles ergeben"* (so auch schon das EVÜ); eine bestimme Form ist daher für die Rechtswahl nicht notwendig.

b) Service Level Agreement

Jeder Cloud-Nutzer erwartet, dass er die Cloud-Dienste jederzeit nutzen kann, insb Zugriff auf seine Daten hat. Eine 100-prozentige Verfügbarkeit bedarf aber ua eines redundanten Systems, das kaum ein Nutzer zu zahlen bereit sein wird. Besondere Vorsicht ist bei definierten Bezugsgrößen geboten: Denn eine 98-prozentige Verfügbarkeit bedeutet, dass die Leistungen des Cloud-Anbieters insgesamt 7,3 Tage pro Jahr[17]) ausfallen können. Ist diese Klausel nicht weiter beschränkt, so wäre ein Ausfall über die Dauer einer Woche möglich. Es ist daher wichtig, einen maximalen Zeitraum der Nicht-Verfügbarkeit zu definieren.

c) Inhalt laut § 11 (Dienstleistervereinbarung)

Es ist gängige Praxis, in die Vereinbarung laut § 11 Abs 2 den Inhalt des Abs 1 aufzunehmen.[18]) Hierzu kann das Muster der DSK herangezogen werden.[19]) Das Muster wurde jedoch nicht an die DSG-Nov 2010 (BGBl I 2009/133) angepasst, mit der Bestimmungen geschaffen wurden, die ebenfalls relevant für das Auftraggeber-Dienstleisterverhältnis sind: die „Data Breach Notification"[20]) (§ 24 Abs 2 a) sowie eine Weiterleitungspflicht des Dienstleisters, wenn dieser in einem Auskunftsbegehren irrtümlicherweise für den Auftraggeber gehalten wird (§ 26 Abs 10). Entsprechende Bestimmungen sollten im Mustervertrag ergänzt werden. Weiters kann es insb bei Datenüberlassungen ins Ausland vorkommen, dass Behörden Datenanforderungen an Dienstleister stellen, die mit dem EU-Datenschutzrecht nicht vereinbar wären. In solchen Fällen sollte der Cloud-Anbieter zu einer unverzüglichen Informationsweitergabe an den Cloud-Anwender verpflichtet werden.

Laut § 11 Abs 1 Z 5 ist der Dienstleister nach Beendigung der Dienstleistung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben bzw in dessen Auftrag für ihn weiter vor unbefugter Einsicht gesichert aufzubewahren oder auftragsgemäß zu vernichten. Der Muster-Vertrag der DSK enthält auch diese Klausel. Aufgrund einer rezenten OGH-E empfiehlt sich die genaue Definition, in welchem Format die Daten dem Auftraggeber zurückzugeben sind.[21]) Der OGH stellte mit Beschluss vom 15. 4. 2010, 6 Ob 40/10 s fest, dass mangels ausdrücklicher Vereinbarung aus § 11 Abs 1 Z 5 keine Verpflichtung des Dienstleisters bestünde, die vorhandenen Daten in einem ganz bestimmten, für den Auftraggeber am besten zu handhabenden Format zu übergeben.

d) Beendigung des Vertragsverhältnisses

Schon erwähnt wurde der Aspekt des Datenformats bei Beendigung des Vertragsverhältnisses. Wichtig sind darüber hinaus Bestimmungen, wie im Falle der Insolvenz des Cloud-Anbieters die Daten des Anwenders geschützt werden oder ob ein Source Code Deposit existiert. Gleichfalls sinnvoll wäre eine Regelung zur Verfügbarkeit der Anwendung, auch wenn fraglich bleibt, ob diese tatsächlich kurzfristig durchgesetzt werden kann.

4. Internationaler Datenverkehr – Genehmigungspflicht

Wesen einer „echten" Cloud ist die physische Verteilung der Daten auf den gesamten Globus, weil so ua Zeitzonen zur Bewältigung von Kapazitätsspitzen ausgenutzt werden können. § 13 Abs 1 schreibt auch für die Datenüberlassung eine Genehmigungspflicht vor, es sei denn, es ist ein Ausnahmetatbestand erfüllt. Dazu zählt nach § 12 Abs 2 der Datenverkehr mit MS des EWR sowie mit jenen Staaten, denen von der EK mittels E nach Art 25 Abs 6 Datenschutz-RL 95/46 ein angemessenes Datenschutzniveau bescheinigt wurde.[22]) Ferner dürfen Daten an US-amerikanische Unternehmen, die sich den „Safe Harbor"-Regeln unterworfen haben, genehmigungsfrei überlassen werden. Allerdings vertritt zB *Weichert,*[23]) dass *„allein die Selbstzertifizierung von US-Unternehmen zu Safe Harbor (…) in keinem Fall* [*genügt*], *um ein den EU-Standards entsprechendes Datenschutzniveau zu erreichen"*. Einem solchen Zertifikat sollte daher gerade zur Risikobewertung einer möglichen Haftung kein allzu großes Vertrauen geschenkt werden. Dem

14) *Wong,* Gerichtsstandsvereinbarugnen in AGB, in *Knyrim/Leitner/Perner/Riss,* Aktuelles AGB-Recht 194.

15) IdS auch *Simotta* in *Fasching*[2] § 104 JN 37.

16) OGH 28. 4. 2000, 1 Ob 358/99 z RdW 2000/728 = JBI 2001, 117 = ecolex 2001/16 = ZfRV 2001, 34.

17) 2% von 365 Tagen sind 7,3 Tage.

18) So auch die Empfehlung von *Dohr/Pollirer/Weiss/Knyrim,* DSG[2] § 10 Anm 5.

19) Verfügbar unter https://www.dsk.gv.at/site/6208/default.aspx

20) Siehe dazu *Knyrim,* Die neue „Data Brach Notification Duty im DSG", in *Jahnel* (Hrsg), Jahrbuch Datenschutzrecht 10, 59 und *Dohr/Pollirer/Weiss/Knyrim,* DSG[2] § 24 Anm 10 ff.

21) Siehe auch die Glosse zur zit E von *Staudegger/Thiele,* JusIT 2010/61, 136.

22) Siehe http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

23) *Weichert* (FN 2) Pkt 11.

Wortlaut des Gesetzes nach müsste es aber dennoch von einer Genehmigungspflicht befreien.

Geht die Cloud über diese Staaten hinaus bzw hat der Cloud-Anbieter kein Safe-Harbor-Zertifikat, so muss bei der DSK um Genehmigung des internationalen Datenverkehrs für *alle* zusätzlich für die Cloud in Frage kommenden Staaten nach § 13 angesucht werden. Dies – mangels derzeitiger spezifischer Lösungsmodelle für Cloud-Systeme – unter Rückgriff auf „traditionelle" Lösungen, wie der Vorlage vertraglicher Zusicherungen in Form der „Standardvertragsklauseln", die von der EK veröffentlicht werden und von den MS als geeigneter Nachweis für ein angemessenes Datenschutzniveau anzuerkennen sind.[24]) Diese sind dann von allen potenziellen Datenhostern in der Cloud zu unterschreiben, wobei die neuen Standardvertragsklauseln aus 2010 erstmals die Möglichkeit zur Heranziehung von Sub-Dienstleistern vorsehen.

Die bisherigen Ausführungen sind für Private und Public Clouds gleichermaßen von Bedeutung, wobei es wohl nicht immer ganz einfach sein wird, herauszufinden, in welche Staaten der Cloud-Anbieter die Daten transferiert, insb wenn er Sub-Dienstleister heranzieht. Eine Lösung für konzernumspannende Private Clouds wären sog Binding Corporate Rules („BCR"). Bei diesen handelt es sich um ein Regelwerk, in dem sich die Konzernmutter zur Einhaltung des europäischen Datenschutzrechts konzernweit, und damit oft weltweit, verpflichtet. Die von den Datenschutzbehörden der MS zu genehmigenden BCR befreien zwar nicht von der Genehmigungspflicht, jedoch kann sich der Auftraggeber bei jedem Datentransfer darauf berufen.[25])

D. Haftung Dritten gegenüber

Wer haftet nun, wenn in der Cloud eine Datenschutzverletzung passiert und daraus dem Betroffenen ein Schaden entsteht? Mit § 33 gibt es eine ausdrückliche Regelung zum Schadenersatz. Grds gilt auch hier die Verschuldenshaftung, allerdings mit Beweislastumkehr zulasten des Auftraggebers (§ 33 Abs 3). Immaterielle Schäden sind nach § 33 Abs 1 Satz 2 nur dann zu ersetzen, wenn bestimmte Daten betroffen sind (sensible Daten, strafrechtlich relevante Daten, Daten zur Kreditwürdigkeit aus einem Auskunftssystem) und die Verletzung einer Bloßstellung iSd § 7 MedienG gleichkommt.[26]) Nach § 33 passivlegitimiert sind sowohl Auftraggeber als auch der Dienstleister direkt, wobei sich ein österreichischer Geschädigter mit sehr hoher Wahrscheinlichkeit an den österreichischen Auftraggeber halten wird statt an den ausländischen Cloud-Anbieter. Es stellt sich daher die Frage, in welchem Umfang der Cloud-Anwender für rechtswidriges[27]) und schuldhaftes Verhalten des Cloud-Anbieters haftet. Aus dem Wortlaut des § 10 Abs 1, dem zufolge nur dann ein Dienstleister in Anspruch genommen werden darf, wenn dieser ausreichend Gewähr für eine rechtmäßige und sichere Datenverwendung bietet, könnte man eine Haftung des Auftraggebers für Auswahlverschulden ableiten.[28]) Zum gleichen Ergebnis gelangt man, wenn man den Dienstleister als Besorgungsgehilfe iSd § 1315 ABGB qualifiziert. Dies wird häufig zutreffen, denn der Cloud-Anwender verarbeitet Kunden- oder Mitarbeiterdaten in der Cloud, was eher nur in Ausnahmefällen zur Vertragserfüllung geschehen wird. Jedoch war genau das Gegenteil die Absicht des Gesetzgebers, denn es schien ihm sachgemäß, die Bestimmungen des § 1313a ABGB für Datenschutzverletzungen zu übernehmen, eben weil diese häufig außerhalb von Vertragsverhältnissen erfolgen. Daher bestimmt § 33 Abs 2 eine Leutehaftung, wobei nach den Mat der Dienstleister und seine Leute gleichzeitig Leute des Auftraggebers sind.[29]) Wie bereits erwähnt, normiert § 33 Abs 3 eine Verschuldenshaftung mit Beweislastumkehr. Der Cloud-Anwender müsste sich daher freibeweisen, dass ihn kein Verschulden trifft. Welche Fälle könnten dies iZm Datenverwendung in der Cloud sein? Zu denken ist hier primär an eine externe Zertifizierung des Cloud-Anbieters, denn damit könnte die Wahrscheinlichkeit, dass diesem eine Datenschutzverletzung vorwerfbar ist, geringer sein.[30]) Selbstzertifizierungen wie im Rahmen von „Safe Harbor" werden diese Anforderungen nicht erfüllen können. Ebenso wenig SAS-70-Typ-II-Zertifikate, wie sie von manchen Unternehmen vorgewiesen werden, weil sie die materiellen und prozeduralen Betroffeneninteressen bei Übermittlungen unberücksichtigt lassen.[31])

24) *Jahnel,* Gesetzgebungsmonitor Datenschutz: Meldefreiheit für bestimmte Videoüberwachungen, neue Standardvertragsklauseln, JusIT 2010, 141.

25) Näheres dazu unter http://ec.europa.eu/justice/policies/privacy/binding_rules/index_en.htm#

26) *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 33 Anm 2.

27) Im Einzelfall können die Bestimmungen des DSG 2000 als Schutzgesetz iSd § 1311 ABGB greifen (ErläutRV zur Stammfassung des DSG 2000, abgedruckt in *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 33).

28) So *Peyerl* (FN 7).

29) Mat abgedruckt in *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 33.

30) Vgl auch *Peyerl* (FN 7) und *Weichert* (FN 2) Pkt 9.

31) So *Weichert* (FN 2) Pkt 12. Vgl auch die Information von Fabasoft auf der Website www.foliocloud.com: „Statement on Auditing Standards Nr 70" (SAS 70) ist ein international anerkannter Standard, der gezielt für die Prüfung von Outsourcing-Geschäften angelegt ist. Grds bescheinigt ein solcher Bericht, dass ein Unternehmen über ein funktionierendes Kontrollsystem verfügt.

SCHLUSSSTRICH

Die derzeit am Markt verfügbaren Angebote für echte, globale Clouds sind kaum mit europäischen Datenschutzstandards zu vereinbaren. Man liest, dass manche Cloud-Anbieter mittlerweile zusichern, dass die Daten nur in Europa verarbeitet werden, was die datenschutzrechtliche Problematik teilweise entschärft, vermutlich aber auch gesondert zu entlohnen sein wird. Eine Verringerung des Haftungsrisikos kann dadurch erreicht werden, dass ein Cloud-Anbieter ausgesucht wird, der mittels geeigneter Zertifikate nachweisen kann, dass er den datenschutzrechtlichen EU-Standards genügt. Zu hinterfragen ist jeweils, ob tatsächlich eine Cloud vorliegt oder nicht nur traditionelle – datenschutzrechtlich vielleicht unproblematischere – ASP-Lösungen unter diesem Schlagwort angeboten werden.