PRWRECHTSANWÄLTE

ALLABOUT

IT-Compliance

Cloud-Dienste für die öffentliche Hand

- Die Zulässigkeit ist keine Frage des „OB“, sondern des „WIE“ -

Version V1 vom 27. August 2014

Inhalt

I. Grundsätzliches

1. Hinweise

ALLABOUT ist seit 2006 eine Whitepaper Reihe, die von PRW Rechtsanwälte herausgegeben wird. Sie befasst sich mit ausgewählten Themen aus dem Bereich IT-Compliance.

In dieser Ausgabe werden die Möglichkeiten der Cloud-Nutzung durch die öffentliche Hand beleuchtet.

Aus Gründen der sprachlichen Vereinfachung wurde auf die geschlechterspezifische Sprachform verzichtet, stellvertretend auch für die weibliche wurde die männliche Form gewählt.

RA Wilfried Reiners, MBA

2. Ausgangslage

Die Geschichte des Cloud Computing ist noch nicht so alt, dennoch ist die Geschichte dieser Technologie von Beginn an mit rechtlichen Bedenken behaftet gewesen. Zu Unrecht sagen diejenigen, die die gesetzlichen Grundlagen kennen und ihre Vorgaben beachten. Kenner wissen, dass Cloud-Computing sehr viel gemein hat mit einem Begriff, der auch in der öffentlichen Hand schon lange bekannt ist. Wir reden über IT-Outsourcing. Dazu wird an dieser Stelle auf die umfassende Studie *Sicheres IT-Outsourcing für Kommunen* hingewiesen[1].

Die öffentliche Hand hat im Vergleich zur Privatwirtschaft zum Teil andere rechtliche Herausforderungen zu meistern. Auf alle Besonderheiten der öffentlichen Hand kann an dieser Stelle nicht eingegangen werden, einige Besonderheiten werden aber nachfolgend beleuchtet. Dabei ist zu beachten, dass an einigen Punkten noch keine vollständige rechtliche Absicherung existiert. Dies ist allerdings die Ausnahme. Schon heute gibt es mehr Gründe für die öffentliche Hand sich dem Thema Cloud-Computing zu öffnen als ihm mit Bedenken gegenüber zu stehen.

Schon im Jahr 2013 schrieben die Verfasser der Studie *Sicheres IT-Outsourcing für Kommunen*, dass rechtskonformes Cloud Computing keine Frage des „OB" sondern des „WIE" sei. Obwohl diese These das „JA" bereits impliziert, kommt es doch auf die konkrete Gestaltung im Einzelfall an, was auch die Verfasser der zitierten Studie hervorheben. Daher gilt der Grundsatz, je sensibler die Daten sind, je höhere Schutzmaßnahmen nach dem T/O/R Prinzip müssen getroffen werden.

3. Das T/O/R Prinzip

Die Vorteile von Cloud-Computing sind weitgehend bekannt. Die Risiken können nach dem von PRW entwickelten **T/O/R²®** ermittelt werden. Danach kann die Auslagerung von Daten auf **t**echnologische, **o**rganisatorische und **r**echtliche Risiken stoßen.

[1] http://www.bay-innovationsstiftung.de/fileadmin/docs/Cloud_Stiftung_2013.pdf

[2] T/O/R ist markenrechtlich geschützt.

Drei wesentliche Punkte, die immer bei einer Auslagerung von Diensten in die Cloud zu beachten sind:

- Handelt es sich um eine sichere Cloud, im Sinne von Datensicherheit? (Technik)
- Ist der Betreiber der Cloud zuverlässig? (Organisation)
- Darf der Dienst in die Cloud ausgelagert werden oder besteht ein gesetzliches Verbot? (Recht)

Merke: Ist nur einer der drei T/O/R Faktoren nicht erfüllt, steht die Ampel für das weitere Vorgehen auf R/O/T.

4. Risiken und Chancen abwägen

Es geht für die öffentliche Hand nicht darum alle Risiken auszuschließen, sondern Risiken und Chancen angemessen abzuwägen. Der Grundsatz der Angemessenheit wird dem in Artikel 20 Absatz 3 des Grundgesetzes (GG) verankerten Rechtsstaatsprinzip und den Grundrechten entnommen. Er hat daher Verfassungsrang und ist mittlerweile auch gewohnheitsrechtlich anerkannt. Er findet zum Beispiel eine explizite Erwähnung im Bundesdatenschutzgesetz (BDSG)

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Angemessen ist eine Maßnahme, wenn der Nachteil und der erstrebte Erfolg in einem vernünftigen Verhältnis zueinander stehen.

Darüber hinaus gilt es eine Reihe von Fragestellungen im Einzelfall zu prüfen. Im Zweifel sind dazu auf Cloud-Computing spezialisierte Experten aus den drei Bereichen

Technologie, Organisation und Recht einzubinden. In jedem Fall sollte die Stelle, die sich mit einem Cloud-Projekt befasst, eine Checkliste erstellen und diese qualifiziert abarbeiten.

II. Das „OB“

1. Zulässigkeit nach Art 33 Abs. 4 Grundgesetz (GG)

Die Ausübung hoheitsrechtlicher Befugnisse ist als ständige Aufgabe in der Regel Angehörigen des öffentlichen Dienstes zu übertragen, die in einem öffentlich-rechtlichen Dienst- und Treueverhältnis stehen.

Im Kern bedeutet dies, dass eine originär staatliche Aufgabe nicht auf private Dritte zur Entscheidung übertragen werden darf. Möglich ist jedoch, die Ausführung bestimmter Aufgaben auf Private zu übertragen, solange und soweit die Verantwortung und die Entscheidung weiter bei der öffentlichen Hand liegt[3]. Was im privaten Sektor der Erfüllungsgehilfe ist (§ 278 BGB), ist im hier angesprochenen Bereich der Verwaltungshelfer. Er ist eine private Person, die von der Verwaltung bei der Erfüllung ihrer Aufgaben eingeschaltet wird; ihr werden - anders als dem Beliehenen - keinerlei Entscheidungsbefugnisse übertragen und sie erledigt lediglich technische Aufgaben.

Unter Beachtung dieser Vorgaben ist somit Cloud-Computing im Bereich der öffentlichen Hand zulässig.

Würde ein Anbieter von Cloud-Services alle Anforderungen nach dem T/O/R Prinzip (also das „OB“ und das „WIE“ erfüllen, wäre es grundsätzlich möglich, dort Server oder Data Services, etc. in Anspruch zu nehmen.

2. Datenschutz nach BDSG und LDSG

Das Bundesdatenschutzgesetz regelt den Umgang mit personenbezogenen Daten durch öffentliche Stellen des Bundes. Darüber hinaus gilt es für nicht-öffentliche Stellen, soweit sie personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Dies gilt nicht, wenn diese Handlungen

[3] Miriam Ballhausen, IT-Einsatz in der Justiz, S. 120 ff

ausschließlich für persönliche oder familiäre Tätigkeiten erfolgen. Daneben gibt es bereichsspezifische Vorschriften in anderen Gesetzen (z.B. Telekommunikationsgesetz, Telemediengesetz). Die Datenschutzgesetze des Bundes und der Länder dienen teilweise der Umsetzung der EU-Richtlinien zum Datenschutz in deutsches Recht.

Landesdatenschutzgesetze sind die in den 16 Bundesländern verabschiedeten landesrechtlichen Pendants zum Bundesdatenschutzgesetz. Die Landesdatenschutzgesetze regeln den Umgang mit personenbezogenen Daten durch die Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Eine Übersicht der Landesdatenschutzgesetze findet sich auf der Website www.datenschutz.de[4]. Die Vorschriften nach den jeweiligen LDSG und dem BDSG sind in vielen Bereichen inhaltsgleich. Im Rahmen der Auftragsdatenverarbeitung nach Landesrecht wird zumeist auf die Vorschriften des BDSG verwiesen. Hier ein Bespiel des Landesbeauftragten für den Datenschutz in Baden-Württemberg[5]. Der Einfachheit halber wird nachfolgend auf das Bundesdatenschutzgesetz (BDSG) Bezug genommen

3. Datenschutz als Ordnungsvorschrift

Häufig wird gefragt, wie groß denn die Wahrscheinlichkeit sei, als nicht datenschutzkonform aufzufallen? Dazu wird hier keine Prognose abgegeben. In der Privatwirtschaft mag dieses im Rahmen des Risikomanagements diskutiert werden, die öffentliche Hand jedoch ist an Recht und Gesetz gebunden (Art 20 Abs. 3 GG). Fest steht, dass die Bundesländer mit den zuständigen Behörden ihre Aktivitäten im Datenschutz deutlich erhöht haben. Details lassen sich in den Tätigkeitsberichten der Landesdatenschutzbeauftragten nachlesen. Wer das Thema Datenschutzverstöße gerne etwas öffentlichkeitswirksamer vorgetragen hat, der möge einen Blick auf die nicht amtliche Website www.projekt-datenschutz.de[6] werfen. Wer dann noch daran festhält, den Datenschutz zwar als gesetzliche Grundlage wahrgenommen, aber auch ignoriert zu haben, handelt vorsätzlich. Gemäß § 43 Abs. 1 Nr. 2 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 4f Abs. 1 Satz 1 oder 2 BDSG, jeweils auch in

[4] http://www.datenschutz.de/recht/gesetze/

[5] http://www.baden-wuerttemberg.datenschutz.de/auftragsdatenverarbeitung-und-funktionsubertragung/

6 Die Website wird betrieben von PR-COM Gesellschaft für strategische Kommunikation mbH.

Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt. Von dem Tatbestandsmerkmal „nicht in der vorgeschriebenen Weise“ sollen auch Fälle erfasst sein, in denen es der zum Beauftragten für den Datenschutz bestellen Person an der erforderlichen Qualifikation mangelt (vgl. § 4f Abs. 2 Satz 1 BGSG). Nach anderer Ansicht liegt erst keine wirksame Bestellung vor. Beide Ansichten stellen aber unstreitig eine Ordnungswidrigkeit im Sinne des § 43 Abs. 1 Nr. 2 BDSG dar, die mit einer entsprechenden Geldbuße geahndet werden kann. Daneben kann ein Verstoß gegen § 4f Abs. 2 Satz 1 BDSG aber insbesondere Schadensersatzpflichten auslösen. Zum anderen kann in diesen Fällen auch der Datenschutzbeauftragte selbst etwaigen Schadensersatzansprüchen ausgesetzt sein. Das muss nicht sein.

4. Der fachkundige Datenschutzbeauftragte (DSB)

Nachfolgend soll das Vorgehensmodell daher aus der Sicht des fachkundigen Datenschutzbeauftragten beschrieben werden. Fachkunde besitzt demnach derjenige, der in der Lage ist, die ihm durch Gesetz auferlegten Aufgaben ordnungsgemäß zu erfüllen. Entscheidend ist, dass der DSB den Aufgaben gewachsen ist. So bestimmt auch § 4f Abs. 2 Satz 2 BDSG, dass sich „das Maß der erforderlichen Fachkunde […] insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf personenbezogener Daten, die die verantwortliche Stelle erhebt oder verwendet [bestimmt]“. Die heute maßgeblichen Kriterien sind nicht starr fixiert, sondern entwickeln sich mit dem technischen Fortschritt und den an das Berufsbild des Beauftragten für den Datenschutz geknüpften Erwartungshaltungen fort.[7] Ausgehend von diesen Grundlagen geht der kundige Datenschutzbeauftragte wie folgt vor:

Das BDSG ist im Zusammenhang mit Cloud Computing nur dann anwendbar, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden (§§ 1, 3 BDSG).

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Personenbezogene Daten dürfen nur dann an einen Dritten, den Cloud Anbieter,

[7] Simitis, in: ders., BDSG, 7. Auflage 2011, § 4f Rn. 85ff.

übermittelt werden, wenn der Betroffene seine Einwilligung erteilt hat oder ein gesetzlicher Erlaubnistatbestand vorliegt (§ 4 BDSG).

Die Einwilligung zu erhalten, kann sich in der Praxis als Herausforderung darstellen, denn die Einwilligung ist nur rechtswirksam, wenn sie freiwillig und grundsätzlich schriftlich erteilt worden ist. Wo eine solche Einwilligung vorliegt, ist die Datenverarbeitung in der Cloud einfach. Doch wie sieht es aus mit dem gesetzlichen Erlaubnistatbestand? Als solcher kommt § 28 BDSG in Betracht.

„Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig.
(1.) wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
(2.) soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt…“.

In der Regel ist die erste Alternative (1.) bei einem Outsourcing von IT-Diensten in eine Cloud nicht erfüllt, da der Zweck eines Vertrages, den ein Cloud Provider mit dem Cloud Nutzer geschlossen hat, nicht umfasst, dass personenbezogene Daten in eine Cloud übermittelt werden.

Bei der Interessenabwägung zwischen den berechtigten Interessen des Cloud Anbieters und denen des Cloud Nutzers in Alternative (2.) ist ein strenger Maßstab anzulegen. Das bedeutet, dass im Zweifel das schutzwürdige Interesse des Betroffenen, dass seine Daten gerade nicht in der Cloud gespeichert werden, überwiegt.

Die Anwendung von § 28 BDSG kann somit nicht als Lösung gesehen werden, wenn auf die Cloud Dienste reflektiert wird.

5. Auftragsdatenverarbeitung nach BDSG

Die Datenverarbeitung im Auftrag – auch Auftragsdatenverarbeitung (ADV) genannt – dient dazu, das Outsourcing von Datenverarbeitung datenschutzrechtlich abzusichern. Dabei verbleibt die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber. In Deutschland ist die Datenverarbeitung im Auftrag u. a. in § 11 BDSG und z.B. in Sondersetzen wie dem § 80 SGB X (Zehntes Buch Sozialgesetzbuch), dem § 30 ff Abgabenordnung, dem § 5 MRRG (für das Meldewesen), dem § 106 Abs. 1, 111 BBG (für Personalakten), etc. geregelt. Voraussetzung ist immer zumindest ein schriftlicher Vertrag mit klaren Regelungen. Zum Teil sind weitere Einschränkungen vorzunehmen. Der Nutzer der Cloud (Auftraggeber) bleibt damit für die Verarbeitung der in die Cloud übermittelten personenbezogenen Daten verantwortlich.

Auszug aus § 11 BDSG
„Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich...“.

Das Erarbeiten eines angemessenen Vertrages zur Auftragsdatenverarbeitung oder eines Vertrages auf Grundlage einer spezialgesetzlichen Regelung bietet damit die Rechtsgrundlage für bestimmte Dienste in der Cloud.

6. Fazit zum „OB“

Die Nutzung von Cloud-Diensten ist der öffentlichen Hand grundsätzlich erlaubt, es sei denn, sie ist ihr untersagt[8]. Im Bereich des Cloud-Computings ist besonderes Augenmerk auf die vertragliche Ausgestaltung mit dem Erfüllungsgehilfen oder Verwaltungshelfer zu legen.

[8] Das umfassende Thema der Beschaffung insbesondere §§ 97 ff GWB wurde hier nicht betrachtet.

III. Das „WIE“

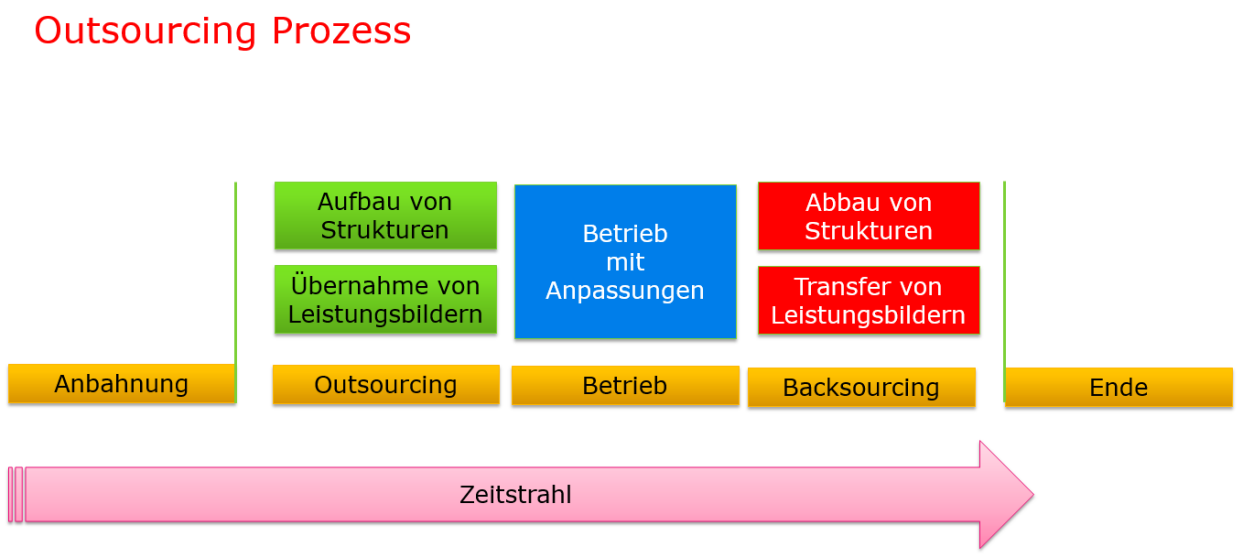
Wenn das Rechtliche geklärt ist, müssen die technischen und organisatorischen Maßnahmen geklärt werden.

1. Datensicherheit in der Cloud (Technik)

Welche technische IT-Infrastruktur ist besser ausgestattet im Sinne von sicherer, die der öffentlichen Hand (im Beispiel nachfolgend die Kommune XY) oder die des Cloud-Anbieters? Hier ist ein ordentliches technisches Benchmark vorzunehmen. Dabei ist auf beiden Seiten (Kommune XY eigene Infrastruktur) und Cloud-Anbieter Infrastruktur sicherzustellen, dass mit den gleichen Maßstäben bei Zertifizierungen, Standards etc. gemessen wird.

2. Zuverlässigkeit des Cloud-Betreibers (Organisation)

Hierunter wird die Abhängigkeit vom Cloud-Anbieter verstanden. Daher ist es ratsam den Weg in die Cloud so zu vereinbaren, dass auch eine Remigration zu einem späten Zeitpunkt möglich ist



Des Weiteren wird darunter die Auswahl des Cloud-Anbieters verstanden. Dieser muss somit sorgfältig ausgewählt werden. Hierbei kann durchaus auf die Grundsätze des Zivilrechts zurückgegriffen werden

Auswahlverschulden (lat. culpa in eligendo) bezeichnet einen Sachverhalt, bei dem der Auswählende (öffentliche Hand) bei der Erfüllung seiner Verbindlichkeit einen Dritten eingeschaltet hat, der erkennbar ungeeignet oder dessen Einschaltung doch zumindest mit erkennbaren Risiken verbunden ist. Realisiert sich die mit der Einschaltung des Dritten verbundene Gefahr, so haftet der Auswählende hierfür aus eigenem Verschulden. Diese Grundsätze sind nach herrschender Meinung auch auf verwaltungsrechtliche Schuldverhältnisse anwendbar, soweit diese schuldrechtsähnliche Pflichten begründen und die Eigenart des öffentlichen Rechts nicht entgegensteht[9].

3. Compliance-Festigkeit

Wer Wert darauf legt, die beschriebenen Cloud Dienste in seine Organisation einzubinden, dem wird als Vorgehensweise das T/O/R-Prinzip empfohlen.
Diese Orientierung nach Technik, Organisation und Recht stellt eine Abdeckung des gesamten Risikobereiches sicher. Somit ist eine umfassende Behandlung des Themas Compliance gewährleistet.

„Compliance-Festigkeit“ wird somit durch folgendes Vorgehen erreicht:

- Bessere **T**echnologie als bisher
- Gesicherte Integration in die **O**rganisation
- Unbedenklichkeitserklärung zur **R**echtslage

Die Praxis hat gezeigt, dass eine eigene Beschreibung des Vorgehens vielfach für die Praxis nicht ausreicht. Begründung: Eine solche Beschreibung informiert weder über die Qualität der Maßnahmen, noch kann umfassend nachvollzogen werden, wie der Entscheider der öffentlichen Hand seine Entscheidung begründet hat. Stattdessen empfiehlt sich folgendes strukturiertes Vorgehen:

[9] Ossenbühl/Cornils, Staatshaftungsrecht, 6. Aufl., 2013, S. 403 ff.; 435 f

a) Team-Building

Das Team, das die Zulässigkeit des Outsourcing Vorhabens prüft, sollte interdisziplinär zusammengesetzt sein. Zum Team gehören Mitglieder:

- Mit rechtlicher Kompetenz zum Thema Cloud-Dienste (insbesondere Ausschreibungspflicht, Datenschutz und IT-Vertragsgestaltung).
- Mit kaufmännischer Kompetenz zum Thema Cloud-Dienste (insbesondere bezogen auf die Wirtschaftlichkeitsbetrachtung des Cloud Vorhabens).
- Mit technischer Kompetenz zum Thema Cloud-Dienste (insbesondere beste technische Bestückung des Cloud Vorhabens)
- Mitarbeiter der handelnden öffentlichen Hand (insbesondere Fachabteilung, IT-Abteilung und ggf. Personalrat und/oder Datenschutzbeauftragter).

b) Projektcontrolling / Audit

In solchen Fällen empfiehlt sich die Durchführung eines Cloud Compliance Audits, das die drei T/O/R Dimensionen im Hinblick auf die Cloud Dienste berücksichtigt[10].

4. Fazit zum „WIE“

Die technischen Gegebenheiten sollten bei den Cloud-Diensten besser sein als bei der Vorhaltung der eigenen IT-Infrastruktur durch die öffentliche Hand. Besser heißt zum Beispiel:

- Wirtschaftliche Vorteile (Senkung der Investitionskosten)
- Rückgriff auf Spezialisten
- Verteilung der Ressourcen
- Vorteile für E-Goverment
- Etc.

Zu den organisatorischen Maßnahmen gehört die sachgerechte Auswahl des Cloud-Anbieters.

Die Compliance-Festigkeit sollte durch die Berufung eines interdisziplinären Team gewährleistet sein.

[10] Die PRW Consulting GmbH (www.prw-consulting.de) hat sich auf diesen Bereich spezialisiert. Sie arbeitet mit PRW Rechtsanwälten im rechtlichen Bereich eng zusammen.

IV. Ergebnis

Cloud Computing im Tätigkeitsfeld der Öffentlichen Hand ist grundsätzlich möglich. Einige Spezialbereiche bleiben davon ausgeschlossen. Im nicht ausgeschlossenen Bereich sind die notwendigen technischen, organisatorischen und rechtlichen Maßnahmen zu beachten. Die Grundlagen für die Entscheidungsfindung für ein Pro oder Contra zum Thema Nutzung von Cloud Diensten sollten durch ein interdisziplinäres Team im konkreten Einzelfall getroffen werden.

5. Fact Sheet / Kontaktdaten

PRW Rechtsanwälte

PRW RECHTSANWÄLTE hat sich auf ausgewählte Gebiete des nationalen und internationalen IT-Rechts spezialisiert, das in erheblichem Umfang auch den Bereich der IT-Compliance-relevanten Vorschriften umfasst. Der Branchenfokus der Kanzlei liegt auf der Informationstechnologie. In diesem Umfeld wurde die Kanzlei vielfach ausgezeichnet.

Autor

Rechtsanwalt Wilfried Reiners, MBA

Studium der Rechts- und Wirtschaftswissenschaften in München und San Diego (MBA).

Nach einer mehrjährigen Tätigkeit für eine internationale Unternehmensberatung ist er seit 1989 zur Anwaltschaft zugelassen. Wilfried Reiners ist heute Managing Partner von PRW Rechtsanwälte in München und Geschäftsführer der PRW Consulting GmbH.

RA Reiners ist seit 24 Jahren auf die Beratung im IT-Umfeld spezialisiert und hat zahlreiche Veröffentlichungen zum IT-Recht publiziert. Seit 1998 ist er Lehrbeauftragter an der Europäischen Privathochschule MUNICH BUSINESS SCHOOL für die Fächer IT Law and Management Liability.

Mitgliedschaften:

EuroITcounsel London

Arbeitsgemeinschaft IT-Anwälte im Deutschen Anwaltsverein

Deutsche Gesellschaft für Recht und Informatik e.V.

Computer Law Association (heute TechLaw)

Kontaktdaten

PRW Rechtsanwälte

Reiners Wilser Schloßmacher Herrmann PartG mbB

Leonrodstr. 54

D-80636 München

Telefon: +49 - (0) 89 - 21 09 77-0

Telefax: +49 - (0) 89 - 21 09 77-77

E-Mail: reiners@prw.de mailto:office@prw.de; Web: www.prw.de