PRWRECHTSANWÄLTE

WHITEPAPER

# ALLABOUT COMPLIANCE

## Datenschutzkonformität von Microsoft Office 365 und Windows Azure

# Inhalt

# 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 Microsoft Cloud Produkte Office 365 und Windows Azure auf ihre Datenschutzkonformität geprüft.

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

Office 365 ist ein Online-Dienst aus dem Hause Microsoft. Windows Azure (kurz: Azure) ist einer von mehreren Cloud-Diensten im Rahmen der Microsoft Cloud Plattform.

Die Markenrechte an Windows Azure und Office 365 stehen allein Microsoft zu. Der Umgang mit diesen Marken erfolgt hier lediglich redaktionell.

RA Wilfried Reiners, MBA

# 2. Ausgangslage

Nachhaltiger Unternehmenserfolg ist kein Zufall. Er ist vielmehr das Ergebnis strategischer Planungen und Umsetzungen, verbunden mit einem jahrelangen und fortdauernden Verbesserungsprozess. In diesem Umfeld sollte auch das Thema IT-Compliance und darin der Datenschutz im Zusammenhang mit Cloud-Lösungen als Teilbereich gesehen werden. *Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software*[1]. Bis 2020 soll der Cloud Computing-Markt weltweit bei über 241 Milliarden Dollar liegen[2]. Dies ist zweifellos ein gewaltiger Markt.

Die Entwicklung des Datenschutzrechts kann grob schematisch wie folgt dargestellt werden:

| | |
|---|---|
| 1970er Jahre: | 1970 Hess. Datenschutz, 1977 Bundesdatenschutzgesetz (BDSG) |
| 1990er Jahre: | EU Datenschutzrichtlinie 1995 |
| 2000er Jahre: | EU Datenschutzumsetzung in Deutschland 2005 |
| Seit 2009 | Novellen I-III des BDSG |

Obwohl die Geschichte von Cloud Computing noch nicht so weit zurückreicht (die ersten Websites mit Cloud Computing-Services für Unternehmen und Verbraucher gingen 1999 online), ist die Geschichte dieser Technologie von Beginn an mit datenschutzrechtlichen Bedenken behaftet gewesen. Zu Unrecht sagen diejenigen, die die gesetzlichen Grundlagen kennen und ihre Vorgaben beachten.

1 https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html
2 http://www.salesforce.com/de/socialsuccess/cloud-computing/die-geschichte-von-cloud-computing.jsp

# 3. Rechtliche Entwicklung des Cloud Computings

Cloud Computing bietet Unternehmen die Möglichkeit, Software, Speicherkapazitäten und Rechenleistung kundenspezifisch über das Internet zu beziehen. Damit ist eine bedarfsgerechte und flexible Nutzung möglich, bei der z. B. nach Funktionsumfang, Nutzungsdauer und Anzahl der Nutzer abgerechnet wird[3]. Der ortsunabhängige Zugang wird durch verschiedene Endgeräte (z. B. Laptop, Tablet-PC, Smart Phone) ermöglicht. Damit kann nahezu jederzeit auf die erforderlichen Informationen (z. B. E-Mails, Geschäftsanwendungen) zugegriffen werden. Für IT-Anbieter ergeben sich neue Geschäftsmodelle. Die gesamte deutsche Wirtschaft soll von den Vorteilen des Cloud Computings profitieren. Daher hat das Bundesministerium für Wirtschaft und Energie (BMWi) das Aktionsprogramm Cloud Computing initiiert[4].

Es gibt auch eine Reihe von Publikationen des Bundes, z. B.

- *„Innovatives, sicheres und rechtskonformes Cloud Computing"[5] (2012) oder*
- *„Mit Recht in der Cloud"[6] (2013),*

die zwar Themenstellungen aufzeigen und vor Risiken warnen, im Ergebnis jedoch wenig konkret werden. Cloud Computing mag technologisch als interessante Entwicklung mit neuen Chancen gesehen werden, rechtlich wurde es bereits angeprangert, bevor es inhaltlich durchdrungen wurde. Die Publikationen der Vergangenheit rankten sich in ihrer rechtlichen Bewertung zum Cloud Computing im Wesentlichen zwischen „geht nicht" über „vielleicht" und „ja, aber Vorsicht und nur in Deutschland". So schrieb das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) im Jahre 2010: *„Das derzeit noch bestehende Grundprinzip der „freien Cloud" genügt nicht den Anforderungen eines modernen Datenschutzes und kann nur als Spiel- oder Versuchsapplikation verstanden werden, aus der sich „trusted and trustworthy Clouds" entwickeln, bei denen Datenschutz- und Datensicherheitsgarantien integriert sind"[7]*. Zwei Jahre später erklärt das ULD in einer Pressemitteilung vom 13.07.2012: *„Datenschutzkonformes Cloud Computing ist möglich"*, zugleich führt das ULD aber aus: *Wer personenbezogene Daten in der Cloud verarbeiten lässt, ist gesetzlich dazu verpflichtet, den bzw. die Dienstleister sorgfältig auszuwählen. Ein Blick auf die Datensicherheit genügt dabei nicht. Die Art. 29-Gruppe[8] hat die Datenschutzanforderungen, die sich auch im neuen Landesdatenschutzgesetz von Schleswig-Holstein wiederfinden, konkretisiert: Neben Verfügbarkeit, Vertraulichkeit und Integrität müssen die Datenschutz-Schutzziele Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit umgesetzt werden. Die Übermittlung personenbezogener Daten in unsichere Drittstaaten außerhalb des EWR ist nur unter bestimmten Voraussetzungen, z. B. bei einer Verwendung sogenannter Standardvertragsklauseln oder verbindlicher Unternehmensregelungen, zulässig. Bei einer Datenübermittlung in die Vereinigten Staaten von Amerika kann sich die verantwortliche Stelle nach Auffassung der Art. 29-Gruppe nicht auf eine Selbstzertifizierung nach den Safe Harbor Prinzipien verlassen. Sie muss die Zertifizierung und die Einhaltung der Prinzipien selbst überprüfen[9]*. Weiter heißt es vom ULD: *„Cloud Computing ist eine technische Realität, bei der die Beachtung der Datenschutzvorschriften zwingend gefordert ist[10]".*

Die Anerkennung einer Realität ist das Eine. Auf eine „Selbstverständlichkeit" zurückzugreifen, die sich in Wirklichkeit aber aus allgemein verbindlichen gesetzlichen Regelungen ergibt und somit ohnehin von jedem zwingend zu beachten ist, ist nicht förderlich. Inzwischen ist völlig unstreitig, dass Cloud Computing nicht per se gegen das Datenschutzrecht verstößt, denn überall dort, wo personenbezogene Daten nicht involviert sind, findet das Datenschutzrecht keine Anwendung und dort wo personenbezogene Daten betroffen sind, sind die datenschutzrechtlichen Vorschriften anzuwenden. So einfach ist das.

Im **Ergebnis** stellen sich die Datenschützer die Frage, wie funktioniert datenschutzkonformes Cloud Computing in der Praxis, und was ist zu beachten?
Es ist in der Regel eben nicht das Datenschutzrecht, das ein Cloud Computing in Europa schwierig gestaltet, sondern andere Normen, etwa die zu den Geheimhaltungsstufen[11].

3 Siehe oben RN 1
4 http://www.bmwi.de/DE/Themen/Digitale-Welt/Internet-der-Zukunft/cloud-computing.html
5 http://www.bmwi.de/DE/Mediathek/publikationen,did=523348.html
6 http://www.bmwi.de/Dateien/BMWi/PDF/Monatsbericht/Auszuege/09-2013-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf
7 Thilo Weichert, Cloud Computing und Datenschutz, 07.06.2010, https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html

# 4. Datenverlust kritisch oder unkritisch

Ist ein **Datenverlust** kritisch oder unkritisch? Und ist ein **Datenschutzverstoß** kritisch oder unkritisch? Wenn Sie analysieren, ob in der IT mehr kritische oder mehr unkritische Daten vorhanden sind, wird der Regelfall so verlaufen, dass die Infrastrukturen 80% unkritische und 20% kritische Daten enthalten.

## Machen Sie folgenden Test:

Fragen Sie einen IT-Verantwortlichen, ob Datenverlust kritisch oder unkritisch ist und bitten Sie um eine schnelle Antwort. Sie erhalten nahezu immer die Antwort: **Kritisch!**
Machen Sie einen weiteren Test. Erläutern Sie die wahre Sachlage (80:20) und fragen Sie einen Statistiker, ob Datenverlust kritisch oder unkritisch ist und bitten Sie um eine schnelle Antwort. Sie erhalten nahezu immer die Antwort: **Eher unkritisch!**
Das betrifft Datenverluste On Premis und in der Cloud gleichermaßen. Hier ist somit kein Unterschied.


Der digitale Kantinenplan einer Mensa der letzten Woche mag von den Studenten kritisch bewertet werden. Die Realität sieht indes anders aus.

Dieser Kantinenplan unterliegt nicht dem Datenschutz, weil er keine personenbezogenen Daten enthält und wenn er in der Folgewoche abhandenkommt, ist der Datenverlust auch nicht unverschmerzbar oder kritisch.

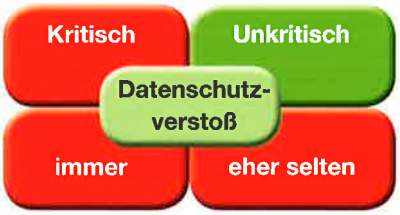
## Datenverlust

Im Wesentlichen kommt es somit darauf an, wen Sie fragen. Im Ergebnis ist eine gesamtheitliche Sicht die Beste.


## Datenschutzverstoß

Etwas anders sieht es beim Datenschutz aus. Die Grundgesamtheit ist viel kleiner, weil er nur personenbezogene Daten betrifft, also eine Untermenge von allen Daten und eine Referenzmenge zu den wirklich kritischen Daten.

Da es sich um einen Verstoß gegen eine gesetzliche Vorschrift handelt, ist der Datenschutz-Verstoß quasi von Haus aus kritisch. Ein unkritischer Datenschutzverstoß wird eher selten vorkommen. Die Praxis gibt es vielleicht her. Das Gesetz nicht.




Zusammenfassend können also sowohl organisationsbezogene Daten kritisch sein als auch personenbezogene.

**Wichtig sind somit Datensicherheit und Datenschutz.**


8 Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes
9 https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.htm
10 Ebenda
11 z. B. in § 2 der Geheimschutzordnung des Deutschen Bundestages (Anlage 3 zur GO-BT), in der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen – Verschlusssachenanweisung (VS-Anweisung – VSA)[3] und in § 4 SÜG

# 5. Datensicherheit

Selbstverständlich sind auch nicht personenbezogene Daten, wie Daten aus Forschung und Entwicklung, technische Daten und kaufmännische Finanzdaten für ein Unternehmen besonders schutzwürdig. Wenn derartige Daten – auf die unbefugte Dritte keinen Zugriff haben sollen – an den Cloud-Provider übermittelt werden, sollte ein angemessenes IT-Sicherheitsniveau sicher gestellt sein. Microsoft sichert eine Verfügbarkeit der Dienste von 99,95 % zu.

Zur tatsächlichen IT-Sicherheit der Microsoft Cloud können hier keine abschließenden Aussagen gemacht werden. Sicher ist aber, dass die Microsoft Cloud Dienste u. a. nach ISO 27001 und anderen Normen von unabhängigen Dienstleistern zertifiziert sind. Details können durch technische Consultants von Microsoft oder seinen zertifizierten Partnern bereitgestellt werden.
Auch hier wieder eine Frage an den IT-Verantwortlichen: Welche technische IT-Infrastruktur ist besser ausgestattet im Sinne von sicherer, die Ihres Unternehmens oder die der Microsoft Cloud? In den meisten Fällen wird vermutet, dass die Microsoft Cloud Infrastruktur mit großem Abstand besser im Sinne von sicherer ist, als die eigene IT-Infrastruktur.

Die Produktbeschreibungen für Office 365[12] und Windows Azure[13] finden sich auf den entsprechenden Webseiten von Microsoft. Hier soll insbesondere auf die Aussagen von Microsoft selbst auf deren eigenen Webseiten verwiesen werden. Auszug[14]:
*„Bei Microsoft kommt auch die Sicherheit nicht zu kurz: Als Betreiber zahlreicher Rechenzentren ist Microsoft immer auf dem neusten Stand der Sicherheitstechnik und zertifiziert nach ISO 27001, EU Safe Harbor und SAS 70 Type II. Weitere Informationen finden Sie im Office 365-Trust Center und im CRM Online-Trust Center."*

Auf den Seiten von **Windows Azure** finden Sie ausführliche Informationen über das Produkt mit weiterführenden Beschreibungen auf verlinkten Seiten[15].
Auf den Seiten des **Office 365-Trust Center** finden sich viele Antworten auf technische, organisatorische und rechtliche Fragen. Auf der Seite der Top 10-Listen[16] finden sich die wichtigsten Fragen, die Sie Ihrem Anbieter von Cloud-Diensten stellen sollten, wenn Sie die Auslagerung Ihrer IT-Dienste in die Cloud in Betracht ziehen und die Antworten, die Microsoft Office 365 hierzu bereithält. Sie finden außerdem die zehn wichtigsten Sicherheits- und Datenschutzfunktionen von Office 365. Ferner werden auch wichtige Verträge, Zertifizierungen, Standards und Bestimmungen, die die Einhaltung von behördlichen Vorschriften sicherstellen, dort offeriert. Die Entscheidung sich aus technischer Sicht für Microsoft Cloud Lösungen zu entscheiden ist damit in der Regel durchaus gerechtfertigt.

# 6. Datenschutz als Ordnungsvorschrift

Beim Datenschutz handelt es sich im Wesentlichen um eine Ordnungsvorschrift, ähnlich einem Verkehrsschild. Wer bei vorgegebenen 60 Km/h stattdessen 80 Km/h fahre, muss sich seines Risikos bewusst sein. Dieser Grundsatz gilt auch im Datenschutzbereich. Der mögliche Bußgeldbescheid ist dort in der Regel deutlich höher. Hinzu kommt der Reputations- und Reparationsschaden hin zur Datenschutzkonformität. Weiter wird häufig gerade bei kleineren und mittleren Unternehmen gefragt, wie groß denn die Wahrscheinlichkeit sei, als nicht datenschutzkonform erwischt zu werden? Dazu wird hier keine Prognose abgegeben. Feststeht aber, 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**[17] 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 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. Diese können zum einen die verantwortliche Stelle selbst nach § 7 BDSG oder wegen einer Verletzung ihrer Organisationspflicht nach § 823 Abs. 1 BGB treffen, wenn den Betroffenen bei der Verarbeitung ihrer Daten durch die mangelnde Fachkunde oder Zuverlässigkeit des Beauftragten Schäden verursacht wurden. Zum anderen kann in diesen Fällen auch der Datenschutzbeauftragte selbst etwaigen Schadensersatzansprüchen ausgesetzt sein. Das muss nicht sein.

## 7. 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.[18] Ausgehend von diesen Grundlagen geht unser Datenschutzbeauftragter 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. Wer also z. B. Azure einsetzt, um größere Mengen an Produktionsdaten, die nicht personenbezogen sind, zu verwalten, kann dies ohne weiteres tun.

Personenbezogene Daten dürfen nur dann an einen Dritten, den Cloud Anbieter Microsoft, 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 von Office 365 und Azure reflektiert wird.

12 http://office.microsoft.com/de-de/business/office-365-fur-unternehmen-plane-vergleichen-FX102918419.aspx
13 http://www.windowsazure.com/de-de/?WT.mc_id=AzureBG_Germany_SEM
14 http://www.microsoft.com/de-de/cloud/default.aspx
15 http://www.microsoft.com/de-de/cloud/services/windows_azure.aspx
16 http://office.microsoft.com/de-DE/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy-FX104029824.aspx#shouldAskACloudServiceProvider
17 Die Website wird betrieben von PR-COM Gesellschaft für strategische Kommunikation mbH
18 Simitis, in: ders., BDSG, 7. Auflage 2011, § 4f Rn. 85ff

# 8. Auftragsdatenverarbeitung nach BDSG

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 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.

Die Datenverarbeitung im Auftrag – auch Auftragsdatenverarbeitung genannt – dient dazu, das Outsourcing von Datenverarbeitung datenschutzrechtlich abzusichern. Cloud Computing ist eine Form des Outsourcings. Dabei verbleibt die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber. In Deutschland ist die Datenverarbeitung im Auftrag u. a. in § 11 BDSG und § 80 SGB X (Zehntes Buch Sozialgesetzbuch) geregelt. Voraussetzung ist ein schriftlicher Vertrag mit klaren Regelungen. Der Nutzer der Cloud (Auftraggeber) bleibt damit für die Verarbeitung der in die Cloud übermittelten personenbezogenen Daten verantwortlich. Der Cloud-Provider erbringt quasi als Gehilfe des Cloud-Nutzers (Auftraggeber) die an ihn ausgelagerten IT-Leistungen. Dabei handelt der Gehilfe nach den Weisungen des Cloud-Nutzers.

*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...".*

# 9. Auftragsdatenverarbeitung nach LDSG

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[19]. 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 Beispiel des Landesbeauftragten für den Datenschutz in Baden-Württemberg[20].

# 10. Auftragsdatenverarbeitung bei den Kirchen

Öffentlich-rechtliche Religionsgemeinschaften haben das Recht, ihre Angelegenheiten selbstständig innerhalb der Schranken der für alle geltenden Gesetze zu ordnen und zu verwalten. Eine dieser Schranken ist das Recht auf informationelle Selbstbestimmung, welches dem Selbstverwaltungsrecht Grenzen setzt. Infolge dessen müssen die öffentlich-rechtlichen Religionsgemeinschaften, auch den Datenschutz in ihrem Zuständigkeitsbereich selbst regeln.

### Die Katholische Kirche

Mit Erlass der neuen Anordnung über den Kirchlichen Datenschutz (KDO-2014) haben die Diözesanbischöfe daher die Anforderungen für eine datenschutzgerechte Auftragsdatenverarbeitung genau festgelegt. Dabei sind folgende Gesichtspunkte entscheidend:

- Der Auftraggeber bleibt datenschutzrechtlich verantwortlich!
- Der Auftragnehmer muss durch einen schriftlichen Auftrag zur Einhaltung datenschutzrechtlicher Regeln verpflichtet werden.
- Das bei der Durchführung des Auftrags angewandte Verfahren muss schriftlich vereinbart werden, einschließlich der Sicherheitsmaßnahmen.
- Unterauftragsverhältnisse, Speicherung, Sperrung und Löschung von Daten, einschließlich der Herausgabe an den Auftraggeber, müssen von Anfang an geregelt sein.

Um die Verwirklichung dieser Anforderungen zu erleichtern, werden Mustervereinbarungen angeboten[21]. Sie können an die jeweilige Situation vor Ort angepasst werden. Selbstverständlich ist der Diözesandatenschutzbeauftragte bereit, die Schaffung datenschutzgerechter Lösungen zu begleiten, soweit Probleme mit der Anpassung der Muster bestehen sollten.

**Die Evangelische Kirche**

In der Evangelischen Kirche erfolgte dies auf der höchsten Ebene durch das Datenschutzgesetz der Evangelischen Kirche Deutschland (DSG-EKD) vom 12.11.1993. Um auf die fortschreitenden Entwicklungen im Datenschutz in der elektronischen Datenverarbeitung zu reagierten, ist das DSG-EKD im Februar 2013 novelliert worden.

Der § 11 DSG-EKD entspricht nun dem § 11 BDSG. Das Vertragswerk zur Auftragsdatenverarbeitung muss sich inhaltlich an dem Regelungskatalog des § 11 Abs. 2 DSG-EKD orientieren. Die verantwortliche Stelle ist ferner zur regelmäßigen Überprüfung der Dienstleister verpflichtet[22].

Landesdatenschutzgesetze sind die in den 16 Bundesländern verabschiedeten landesrechtlichen Pendants zum Bundesdatenschutzgesetz (für Behörden des Bundes und private Unternehmen). Sie gelten für die jeweiligen Landesbehörden und Kommunalverwaltungen.

## 11. Microsoft und die Zusammenarbeit mit den Datenschutzbehörden

Würden somit die Voraussetzungen von Auftragsdatenverarbeitung vorliegen, wäre der Weg zu den Microsoft Cloud Lösungen eröffnet. Aus datenschutzrechtlicher Sicht sollten daher vor der Inanspruchnahme von Cloud-Diensten einige Prüfungen vorgenommen werden. Für die Produkte Office 365 und Azure werden von Microsoft Informationen zum Thema Datenschutz bereitgestellt. Auf Informationsveranstaltungen, die Microsoft unter inhaltlicher Federführung ihrer deutschen Rechtsabteilung an verschiedenen Orten durchführt, wird auch über den aktuellen Stand der Diskussionen mit den Datenschutzbehörden berichtet. Im Wesentlichen hat Microsoft seit 2011 vier Meilensteine verabschiedet.[23]


## 12. Datenschutzrechtliches Wissen zu Office 365 und Azure

Auf einer gesonderten Seite hat sich Microsoft auch intensiv mit dem Thema Datenschutz befasst[24]. Die darin enthaltenen Hinweise können ihre Geltung bezüglich der gesamten Microsoft Cloud Produkte entfalten. So weist Microsoft ausdrücklich auf die Stellungnahmen vom 1. Juli 2012 der EU-Arbeitsgruppe zum Datenschutz „Artikel 29-Gruppe" zum Cloud Computing (05/2012) hin. In ihrer Auffassung betont die EU-Arbeitsgruppe zum Datenschutz „Artikel 29-Gruppe", wie wichtig es ist, einen Anbieter von Cloud-Diensten auszuwählen, der seine Datenschutzpraktiken transparent macht und die Schutzwürdigkeit von Kundendaten respektiert. Die Auffassung der EU-Arbeitsgruppe zum Datenschutz „Artikel 29-Gruppe" stellt einen Leitfaden für aktuelle und potenzielle Cloud-Benutzer dar. Die Fragen und Antworten hat Microsoft auf der angegebenen Seite dargestellt.

19 http://www.datenschutz.de/recht/gesetze/
20 http://www.baden-wuerttemberg.datenschutz.de/auftragsdatenverarbeitung-und-funktionsubertragung/
21 http://www.datenschutz-kirche.de/auftragsdatenverarbeitung/
22 http://www.datenschutz-cert.de/news/datenschutz-news/beitrag/thema/datenschutz-allgemein/artikel/novellierung-des-datenschutzgesetzes-der-evangelischen-kirche-deutschland.html
23 Quelle: Dr. Dirk Bornemann, Alexandra Buchberger Rechtsabteilung Microsoft Deutschland GmbH am 20.02.2014 Vortrag in München
24 http://office.microsoft.com/de-de/business/office-365-trust-center-fragen-zum-datenschutz-FX104027280.aspx

So stellt Microsoft zum Beispiel einen umfassenden Auftragsdatenverarbeitungsvertrag (ADV bzw. Data Processing Agreement, DPA) bereit, der die EU-Standardvertragsklauseln ebenso wie die Selbstzertifizierung gemäß den Vereinbarungen zwischen dem US-Handelsministerium und der EU („Safe Harbor") umfasst[25].
Dies wurde Microsoft durch die ARTICLE 29 Data Protection Working Party mit Schreiben vom 02.04.2014 aus Brüssel schriftlich bestätigt.

## 13. Europäische Microsoft-Cloud

Bei der Frage, welches Datenschutzrecht Anwendung findet, ist ein genauerer Blick auf Anbieter und Nutzer des Cloud-Dienstes notwendig. Ein deutsches Unternehmen möchte Microsoft Cloud Dienste einkaufen.

Das Deutsche Datenschutzrecht findet auf Cloud Computing dann Anwendung, wenn es sich bei den in der Cloud gespeicherten Daten um „personenbezogene Daten" gem. § 3 Nr. 1 BDSG handelt. Die rechtliche Möglichkeiten bei Personenbezug sind die Auftragsdatenverarbeitung (§ 11 BDSG) oder die Funktionsübertragung nach § 28 BDSG (Datenerhebung und -speicherung für eigene Geschäftszwecke).
Es gibt unterschiedliche Voraussetzungen für die Auftragsdatenverarbeitung. Mindestvoraussetzungen sind aber immer, das Vorliegen eines schriftlichen Vertrages, Regelung zum Umfang der Datenverarbeitung, Festlegungen über Datenschutz- und Datensicherheitsmaßnahmen des Auftragnehmers (Sicherheitskonzept) und die Weisungsbefugnis des Auftraggebers bei allen datenschutzrelevanten Sachverhalten. Microsoft bietet auf seiner Website im Trustcenter einen Vertrag zur Auftragsdatenverarbeitung an, der diese und viele andere Merkmale enthält. Da Microsoft nicht im Rahmen einer Funktionsübertragung tätig wird, kann die Regelung des § 28 BDSG hier außer Acht gelassen werden.

Microsoft betreibt seine europäischen Cloud Rechenzentren in den Niederlanden und in Irland. Befindet sich der Cloud-Anbieter innerhalb der EU und hat ein Cloud-Kunde seinen Wohnsitz in Deutschland, findet deutsches Datenschutzrecht Anwendung. Nach der Europäischen Datenschutzrichtlinie (RL 95/46/EG) stellt eine grenzüberschreitende Datenverarbeitung innerhalb der EU nämlich kein rechtliches Hindernis dar (vgl. Art. 1 Abs. 2 EU-DSRL). Deutsches Datenschutzrecht ist also immer anwendbar, wenn personenbezogene Daten einer Person mit Wohnsitz in Deutschland von einem Cloud-Anbieter mit Niederlassung in der EU verarbeitet werden.

> *Art. 1 EU-DSRL*
> *(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.*
> *(2) Die Mitgliedstaaten beschränken oder untersagen nicht den freien Verkehr personenbezogener Daten zwischen Mitgliedstaaten aus Gründen des gemäß Absatz 1 gewährleisteten Schutzes.*

## 14. USA Microsoft-Cloud

Zunächst muss einmal klargestellt werden, dass es kein generelles Verbot des Datentransfers in die USA oder andere Regionen gibt. Es sind jedoch bestimmte Voraussetzungen zu schaffen. Eine Legitimierung ist also z. B. möglich durch:

- Einwilligung
- Standard Contract Clauses (SCC)
- Safe Harbor Abkommen
- Processor BCRs (Binding Corporate Rules)
- Vertrag zur Auftragsdatenverarbeitung (ADV)

Die Begründung ergibt sich unmittelbar aus Art. 2 f) der europäischen Datenschutzrichtlinie 95/46/EG: „'Dritter' [ist] jede ... Stelle, **außer ... dem Auftragsverarbeiter ...".**
Aus der europäischen Datenschutzrichtlinie ergibt sich keine örtliche Einschränkung, daher genießen Auftragsdatenverarbeiter außerhalb der EU dieselben Rechte. In anderen EU Staaten ist es auch so in das nationale Recht umgesetzt worden. In Deutschland haben wir insoweit eine Verböserung gegenüber der EU Richtlinie.

25 Vgl. ebenda

Nach dem Urteil des EUGH in den Rechtssachen C-468 u 469/10 vom 24.11.2011 ist die Datenschutzrichtlinie „nicht auf eine Mindestharmonisierung beschränkt", sondern erfordert „grundsätzlich umfassende Harmonisierung" (Rn. 29).
Die Regelungen der EU Richtlinie gelten abschließend. Das gilt auch dann, wenn nationale Gesetzgeber an die Zulässigkeit einer Datenverarbeitung (wie etwa einer Weitergabe an Dritte) höhere Maßstäbe setzen. Ergo: Das nationale Recht darf nicht schärfer sein, ansonsten ist es unwirksam. Die EU Datenschutzrichtlinie gilt dann unmittelbar (Rn. 31).
Daraus leitet sich ab, dass auch für nicht europäische Clouds das Privileg der Auftragsdatenverarbeitung gilt. Nachdem Microsoft diesen Bestimmungen zugestimmt hat, kann auch die US-Cloud genutzt werden.
Die EU Kommissionsentscheidung vom 05.02.2010 über die Verwendung der Standardvertragsklauseln (EU-SCC) für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern kann hier ergänzend auch noch angeführt werden.
Die EU Standardvertragsklauseln sind gerade für Auftragsdatenverarbeiter in Drittländern (USA) gemacht. Im Hinblick auf die Auftragsdatenverarbeiter wird auf die EU Datenschutzrichtlinie verwiesen. Danach ist eindeutig, dass auch Dienstleister außerhalb der EU (und gerade um die geht es bei den EU-SCC), Auftragsdatenverarbeiter sein können.

## 15. Compliance-Festigkeit

Wer Wert darauf legt, die beschriebenen Microsoft 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 Unternehmensbereiches sicher. Somit ist eine umfassende Behandlung des Themas Compliance gewährleistet.

„Compliance-Festigkeit" wird somit durch folgendes Vorgehen erreicht
- Besserer **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 Wirtschaftsprüfer nicht ausreicht. Begründung: Eine solche Beschreibung informiert weder über die Qualität der Maßnahmen, noch kann nachvollzogen werden, wie der der Verfasser seine Stellungnahme begründet hat. In solchen Fällen empfiehlt sich die Durchführung eines Cloud Compliance Audits durch einen unabhängigen Dritten, der die drei T/O/R Dimensionen im Hinblick auf die Microsoft Cloud Dienste durchdrungen hat[26].

## 16. Hotline

Wir haben uns intensiv rechtlich mit der Datenschutzkonformität von Microsoft Office 365 und Windows Azure befasst. Wenn Sie hierzu Fragen haben, rufen Sie uns einfach an, wir geben unser Wissen gerne weiter. Selbstverständlich ist dieser Service für Sie – bis auf Ihre Telefongebühren – kostenfrei.
Telefon: +49 - (0) 89 - 21 09 77-0 · Stichwort: Microsoft Cloud-Services Hotline. Sie werden dann mit einem kompetenten Ansprechpartner verbunden oder zurück gerufen.

## 17. Fazit

Die von Microsoft angebotenen Cloud Lösungen sind nach deutschem und europäischem Datenschutzrecht, datenschutzkonform einsetzbar. Sie bieten zudem ein sehr hohes Maß an Datensicherheit, das von vielen Unternehmen so selbst nicht vorgehalten werden kann. Unter den rechtlichen Gesichtspunkten eines Risikomanagements sind sie daher ohne Bedenken zu empfehlen. Zudem wird nach Einführung der Cloud Dienste eine Auditierung empfohlen, um den Nachweis zu erbringen, dass die Cloud Dienste rechts- und regelkonform in die Organisation integriert wurden.

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

# 18. 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)

PRWRECHTSANWÄLTE

**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