PRWRECHTSANWÄLTE

WHITEPAPER

ALLABOUT COMPLIANCE

Datenschutzkonformität von Microsoft Office 365 und Microsoft Dynamics CRM Online

Edition 2016

Inhalt

I. 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 ausgewählte Microsoft Onlinedienste auf ihre Datenschutzkonformität geprüft. Grundlage dafür sind die geltenden gesetzlichen Vorschriften und die Online Services Terms von Microsoft (OST). Die OST enthalten die Bestimmungen, die für den Microsoft Kunden bei Nutzung der Microsoft Onlinedienste gelten.

Die Edition 2016 wurde notwendig, weil sich die datenschutzrechtlichen Rahmenbedingungen in der jüngsten Vergangenheit verändert haben und dieser Veränderungsprozess auch noch die Zukunft des Datenschutzes bestimmen wird.

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

Die Markenrechte an den Microsoft Produkten stehen allein Microsoft zu. Der Umgang mit diesen Marken erfolgt hier lediglich redaktionell.

RA Wilfried Reiners, MBA
RAin Janina Thieme

II. Grundlagen

1. Datenschutz im Wandel

Es ist offensichtlich, dass sich die deutsche, europäische und internationale Gesetzgebung und Rechtsprechung zum Thema Datenschutz im Umbruch befindet. Existierende Rechtsgrundlagen werden zum einen von der Rechtsprechung „gekippt“ und zum anderen von der Gesetzgebung reformiert.

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

- 1970er Jahre: 1970 Hess. Datenschutz, 1977 Bundesdatenschutzgesetz (BDSG)
- 1990er Jahre: EU-Datenschutzrichtlinie 1995[1]
- 2000er Jahre: EU-Datenschutzumsetzung in Deutschland 2005
- Seit 2009: Novellen I-III des BDSG
- EuGH – Entscheidung zu Safe Harbor vom 06.10.2015[2]; der Gerichtshof der Europäischen Union hat mit Urteil vom 06.10.2015 die unter dem Namen Safe Harbor bekannte Entscheidung der EU-Kommission für ungültig erklärt. Safe Harbor ist somit nicht länger zulässige Rechtsgrundlage für einen Datentransfer in die USA.
- Das neue EU-US-Privacy Shield[3]; die EU-Kommission und die USA haben sich über ein neues Abkommen für einen neuen Rechtsrahmen für den transatlantischen Datenaustausch als Ersatz für Safe Harbor geeinigt.
- Die neue Europäische Datenschutzgrundverordnung[4]; sie wird ab voraussichtlich Frühjahr 2018 unmittelbar in allen europäischen Staaten geltendes Recht sein und die nationalen Vorschriften im Wesentlichen ablösen.

Für die Zukunft bedeuten die neuesten Entwicklungen, dass Unternehmen das Thema Datenschutz im Blick behalten müssen. Allerdings wird es keine Phase geben, in der ein internationaler Datentransfer nicht mehr rechtmäßig möglich ist.

1 http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_de.pdf
2 http://curia.europa.eu/juris/documents.jsf?num=C-362/14
3 http://europa.eu/rapid/press-release_IP-16-433_de.htm
4 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE

So wurde zwar bereits angekündigt, dass in Folge der Safe Harbor-Entscheidung nun auch die EU-Standardvertragsklauseln rechtlich angegriffen werden. Den Angreifern obliegt aber keine Aufhebungskompetenz. Diese liegt allein beim EuGH. Bis dieser darüber entscheidet, wird ein längeres Zeitfenster ins Land gehen. Bis dahin sind die EU-Standardvertragsklauseln eine solide Rechtsgrundlage für einen internationalen Datentransfer mit angemessenem Schutzniveau.

Es gibt darüber hinaus auch Stimmen, die sagen, dass das neue EU-US-Privacy Shield einer gerichtlichen Überprüfung nicht Stand halten wird. Für diese Überprüfung wäre wiederum der EuGH zuständig. Diese wird der EuGH, sofern sie überhaupt initiiert wird, aber erst dann vornehmen, wenn er sich mit den EU-Standardvertragsklauseln befasst hat. Das wird demnach auch noch ein längeres Zeitfenster für sich in Anspruch nehmen.

Hinsichtlich des Regelungsgehalts der neuen europäischen Datenschutzgrundverordnung ist aus deutscher Sicht zu sagen, dass das Datenschutzrecht, wie wir es bisher kennen, nicht grundlegend verändert wird. Da die deutschen gesetzlichen Standards gemäß dem Bundesdatenschutzgesetz (BDSG) bisher schon im europäischen Vergleich eher streng waren, sind die neuen europäischen Standards für uns in Deutschland nicht einschneidend. Eine Ausnahme dazu werden die nun wesentlich höheren Sanktionsrahmen bei Verstößen bilden. Darüber hinaus bleibt es bei dem weiten, sachlichen Anwendungsbereich hinsichtlich der Personenbezogenheit von Daten und bei dem sogenannten Verbotsprinzip gemäß § 4 Abs. 1 BDSG. Das heißt, wie bisher bedarf jede Datenverarbeitung einer Legitimationsgrundlage.

2. Rechtliche Entwicklung des Cloud-Computings

Obwohl die Entwicklung 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. In den vorangegangenen Auflagen wurde die rechtliche Entwicklung umfassend dargestellt. Sie kann nun als bekannt vorausgesetzt werden und ist soweit Geschichte.

Wenn man dafür einen Ausblick in die Zukunft macht, ist festzustellen, dass dem Thema Cloud-Computing nach wie vor ein gewaltiger Markt vorausgesagt wird und sich entsprechend große wirtschaftliche Chancen bieten. Nach der aktuellen Studie „Cloud-Monitor 2015“ der BITKOM Research GmbH im Auftrag von KPMG nutzen derzeit 44 Prozent der Unternehmen in Deutschland Cloud-Computing und weitere 24 Prozent planen oder diskutieren den Einsatz.[5] Bis zum Jahr 2018 soll das Volumen des Cloud-Marktes im Business-Bereich in Deutschland mit jährlichen Wachstumsraten von durchschnittlich 35 Prozent den Prognosen zufolge auf rund 19,8 Milliarden Euro steigen.[6] Für IT-Anbieter ergeben sich dadurch neue Geschäftsmodelle. Zudem ist es auch politisch gewollt, dass die gesamte deutsche Wirtschaft von den Vorteilen des Cloud-Computings profitieren soll. Daher hat das Bundesministerium für Wirtschaft und Energie (BMWi) u. a. das Aktionsprogramm Cloud-Computing initiiert.[7]

3. Cloud-Computing und Datenschutz

Zum Thema Cloud-Computing und Datenschutz gibt es eine Reihe von Publikationen,
wie zum Beispiel des BMWi:

- „Trusted Cloud – Innovatives, sicheres und rechtskonformes Cloud-Computing“ (Stand Februar 2014)[8] oder
- „Mit Recht in der Cloud“ (2013)[9],

die zwar Themenstellungen aufzeigen und vor Risiken warnen, im Ergebnis jedoch wenig konkret werden.

5 Vgl. https://www.bitkom.org/Publikationen/2015/Studien/Cloud-Monitor-2015/Cloud-Monitor-2015-KPMG-Bitkom-Research.pdf
6 http://www.bitkom-research.de/Presse/Pressearchiv-2014/Markt-fuer-Cloud-Computing-waechst-ungebrochen
7 Vgl. http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/aktionsprogramm-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf
8 http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/trusted-cloud-cloud-computing-version-2,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf
9 http://www.bmwi.de/Dateien/BMWi/PDF/Monatsbericht/Auszuege/09-2013-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf

Die Publikationen der Vergangenheit rankten sich allgemein 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[10]. Zwei Jahre später erklärte das ULD in einer Pressemitteilung vom 13.07.2012: „Datenschutzkonformes Cloud-Computing ist möglich"[11], 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 Artikel-29-Gruppe[12] hat die Datenschutzanforderungen weiter konkretisiert: Neben Verfügbarkeit, Vertraulichkeit und Integrität müssen die Schutzziele Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit umgesetzt werden. Die Übermittlung personenbezogener Daten in unsichere Drittstaaten außerhalb des Europäischen Wirtschaftsraums (EWR) ist nur unter bestimmten Voraussetzungen, z. B. bei Verwendung der Standardvertragsklauseln, zulässig.

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. Im Ergebnis stellt sich also die Frage, wie funktioniert datenschutzkonformes Cloud-Computing in der Praxis und was ist dabei zu beachten.

4. On-Premise oder Cloud-basiert

Bevor im Weiteren konkret auf diese Frage und die einzelnen rechtlichen Aspekte eingegangen wird, soll aber zunächst die Abgrenzung von Arbeiten On-Premise und Cloud-Computing noch einmal kurz dargestellt werden: On-Premise ist ein Nutzungsmodell für serverbasierte Computerprogramme (Software). Dabei erwirbt der Nutzer ein Computerprogramm und betreibt dieses im eigenen Rechenzentrum, also auf eigener oder eigenverwalteter Hardware.

Unter Cloud-basiertem Arbeiten versteht man die Ausführung von Programmen, die nicht auf dem lokalen Rechner installiert sind, sondern auf einem anderen Rechner, der aus der Ferne über das Internet aufgerufen wird.

Hinsichtlich Microsoft Online-Produkten liegen die Programme und Daten dann entsprechend in der Microsoft Cloud. Microsoft verfolgt bei den Rechenzentren eine an den Regionen orientierte Strategie. Das Land oder die Region des Kunden, das oder die der Administrator bei der erstmaligen Einrichtung der Dienste eingibt, bestimmt den primären Speicherort für die Daten des Kunden. Für deutsche Kunden werden derzeit standardmäßig die wesentlichen Kundendaten (Core Customer Data) der Microsoft Enterprise Services (Office 365, Microsoft Azure, CRM, Windows Intune) in den Microsoft Rechenzentren in Dublin und Amsterdam gespeichert.

Die hier im Fokus stehenden Microsoft Produkte können sowohl On-Premise als auch Cloud-basiert installiert werden. Die nachfolgenden Ausführungen beziehen sich auf die Microsoft Online-Produkte.

10 https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html
11 https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.html
12 Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes

5. Datenverlust

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.

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

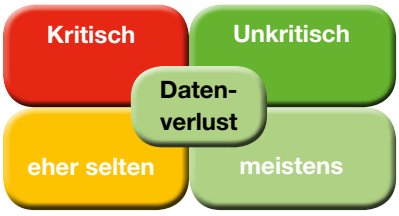
Dieser Kantinenplan unterliegt nicht dem Datenschutz, weil er keine personenbezogenen Daten enthält und wenn er in der Folgewoche abhandenkommt, ist der Datenverlust auch nicht unverschmerzbar oder kritisch.

Machen Sie folgenden Test:
Fragen Sie einen IT-Verantwortlichen, ob ein 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 ein Datenverlust kritisch oder unkritisch ist und bitten Sie um eine schnelle Antwort. Sie erhalten nahezu immer die Antwort: **Eher unkritisch!**

Datenverlust

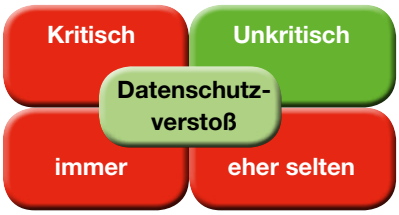
Im Wesentlichen kommt es also darauf an, wen Sie fragen. Im Ergebnis ist eine gesamtheitliche Betrachtung das Beste.



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

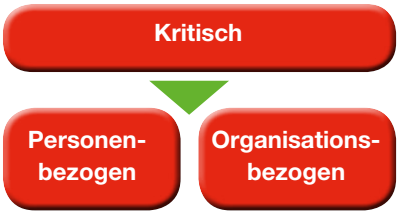
Datenschutzverstoß

Da es sich um einen Verstoß gegen eine gesetzliche Vorschrift handelt, ist der Datenschutzverstoß 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 als auch personenbezogene Daten kritisch sein.

Wichtig sind somit Datensicherheit und Datenschutz.



6. Datensicherheit

Die Datensicherheit beschreibt alle Maßnahmen, die ein Unternehmen vornimmt, um Informationen oder Daten vor dem unrechtmäßigen Zugriff Dritter zu schützen. Die Datensicherheit steht in engem Zusammenhang mit den organisatorischen und technischen Anforderungen des § 9 BDSG[13], denn erst durch die ergriffenen Maßnahmen bei der Datensicherheit wird die Datenverarbeitung sozialverträglich.[14]

13 Vgl. Gola / Schomerus, Bundesdatenschutzgesetz Kommentar, 12. Auflage 2015, § 9 Rn. 1
14 Vgl. Peter Nitsch, Datenschutz und Informationsgesellschaft, ZRP 1995, 361-365

Auch der § 203 StGB i.V.m. § 13 StGB wird immer wieder im Zusammenhang mit Datensicherheit beim Cloud-Computing angesprochen. § 203 StGB regelt die Strafbarkeit bei Verletzungen von Privatgeheimnissen und § 13 StGB regelt das Begehen von Straftaten durch Unterlassen. Zur Verschwiegenheit sind verschiedene Personenkreise gemäß § 203 StGB verpflichtet. Seit dem 22.08.2006 zählt zu dieser Gruppe auch der Datenschützer eines Unternehmens oder einer öffentlichen Einrichtung.[15] Daraus ergibt sich für den Datenschützer die Verpflichtung zu prüfen, ob im Unternehmen ausreichende Sicherungsmaßnahmen für den Umgang mit personenbezogenen Daten implementiert sind.

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/IEC 27001 und ISO/IEC 27018 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.

7. 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 fährt, muss sich seines Risikos bewusst sein. Dieser Grundsatz gilt auch im Datenschutz. Der mögliche Bußgeldbescheid ist dort in der Regel aber deutlich höher.

Es wird in diesem Kontext häufig gerade von kleineren und mittelständischen Unternehmen gefragt, wie groß denn die Wahrscheinlichkeit sei, als „nicht datenschutzkonform handelnd“ erwischt zu werden?

Dazu kann hier keine abschließende Prognose abgegeben werden. 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[16] 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 bestellten Person an der erforderlichen Qualifikation mangelt (vgl. § 4f Abs. 2 Satz 1 BDSG). Nach anderer Ansicht liegt schon keine wirksame Bestellung vor. Beide Ansichten führen aber unstreitig zu einer Ordnungswidrigkeit im Sinne des § 43 Abs. 1 Nr. 2 BDSG, 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 etwaigen Schadensersatzansprüchen ausgesetzt sein.

15 Vgl. Thomas Fischer, in Fischer StGB Kommentar, 63. Auflage 2016, § 203 Rn. 29a
16 Die Website wird betrieben von PR-COM Gesellschaft für strategische Kommunikation mbH

8. Auftragsdatenverarbeitung nach BDSG

Das Bundesdatenschutzgesetz (BDSG) 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).

Das BDSG ist also im privatwirtschaftlichen Sektor im Zusammenhang mit Cloud Computing immer 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. Diese dürfen grundsätzlich nur dann an einen Dritten übermittelt werden, wenn der Betroffene seine Einwilligung erteilt hat oder ein gesetzlicher Erlaubnistatbestand vorliegt (§ 4 BDSG). Werden Daten im Auftrag verarbeitet, kommt es laut Gesetz zu einer Privilegierung (§3 VIII BDSG). Der Auftragnehmer ist datenschutzrechtlich betrachtet dann kein „Dritter“ und es greift § 11 BDSG.

Die gesetzlichen Vorschriften zur Datenverarbeitung im Auftrag – verkürzt auch Auftragsdatenverarbeitung genannt – dienen dazu, das Outsourcing von Datenverarbeitung datenschutzrechtlich abzusichern. Cloud-Computing ist eine Form des Outsourcings. In Deutschland ist die Datenverarbeitung im Auftrag u. a. in § 11 BDSG und § 80 SGB X (Zehntes Buch Sozialgesetzbuch) geregelt.

Voraussetzung für eine rechtskonforme Auftragsdatenverarbeitung ist ein schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer (Vertrag zur Auftragsdatenverarbeitung, der sogenannte ADV-Vertrag). Dabei verbleibt die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber. Der Cloud-Provider (Auftragnehmer) 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

Die Landesdatenschutzgesetze sind die in den 16 Bundesländern verabschiedeten landesrechtlichen Pendants zum Bundesdatenschutzgesetz. Die Landesdatenschutzgesetze regeln den Umgang mit personenbezogenen Daten durch die Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände sowie sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Eine Übersicht der Landesdatenschutzgesetze findet sich auf der Website www.datenschutz.de[17]. 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.[18]

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.

17 http://www.datenschutz.de/recht/gesetze/
18 http://www.baden-wuerttemberg.datenschutz.de/auftragsdatenverarbeitung-und-funktionsubertragung/

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.[19]
Diese können an die jeweilige Situation vor Ort angepasst werden.

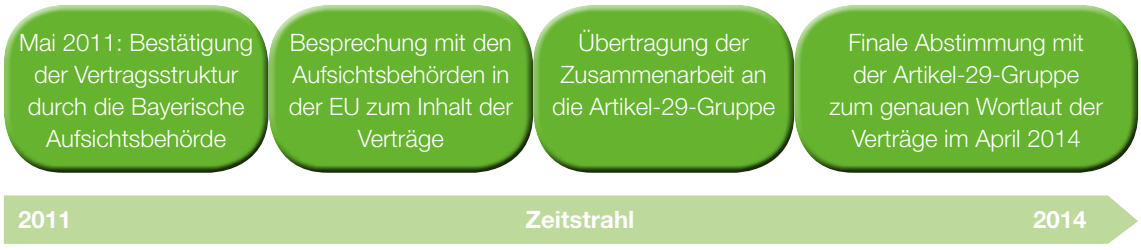
Die Evangelische Kirche
In der Evangelischen Kirche erfolgte dies auf der höchsten Ebene durch das Datenschutzgesetz der Evangelischen Kirche Deutschland (DSG-EKD) vom 12.11.1993. Um auf die fortschreitenden Entwicklungen im Datenschutz in der elektronischen Datenverarbeitung zu reagieren, ist das DSG-EKD im Februar 2013 novelliert worden.[20]

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.[21]

III. Microsoft und die Zusammenarbeit mit den Datenschutzbehörden

1. Vier Meilensteine

Für die Produktwelten von Microsoft werden einige 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 Zusammenarbeit mit den Datenschutzbehörden berichtet. Im Wesentlichen hat Microsoft seit 2011 vier Meilensteine verabschiedet.[22]



19 http://www.datenschutz-kirche.de
20 http://www.kirchenrecht-ekd.de/document/25764
21 http://www.kirchenrecht-ekd.de/document/27085
22 Vgl. Dr. Dirk Bornemann, Alexandra Buchberger, Rechtsabteilung Microsoft Deutschland GmbH, Vortrag in München am 20.02.2014

Obwohl der Konzern als Auftragnehmer hinsichtlich dem Vertrag zur Auftragsdatenverarbeitung (ADV-Vertrag) grundsätzlich nicht in der Verantwortung ist, hat man zu diesem Thema den Kontakt mit den nationalen Aufsichtbehörden sowie mit den Aufsichtsbehörden der EU gesucht. Microsoft hat für die eigenen Kunden eine standardisierte Erklärung für die Auftragsdatenverarbeitung ausgearbeitet und stellt diese im Rahmen der OST zur Verfügung. Darüber hinaus sind die EU-Standardvertragsklauseln Vertragsbestandteil. Die Klauseln wurden seitens der EU-Kommission als Rechtsgrundlage für den internationalen Datentransfer entwickelt. Sie sind unverändert zu übernehmen und als Ergänzung dem eigentlichen Vertrag beizufügen. Unternehmen und Kunden können diese Klauseln untereinander vereinbaren, und stellen damit individuell das erforderliche Datenschutzniveau her. Microsoft hat seinen Kunden also sowohl hinsichtlich des ADV-Vertrages als auch hinsichtlich der EU-Standardvertragsklauseln die Vertragsgestaltung im Rahmen der standardisierten OST abgenommen.[23]

Seit Dezember 2011: Angebot der EU Model Clauses

EU Model Clauses

⊕

Standardisierte Erklärung zur Auftragsdaten-verarbeitung (ADV/DPA)

„Office 365 ist die erste und derzeit **einzige Cloud-basierende Produktivitätslösung**, die jedem Kunden die EU Model Clauses als Standardvertragsklauseln anbietet."

Wir kombinieren diese Standardvertragsklauseln mit einer ebenfalls standardisierten Erklärung zur **Auftragsdatenverarbeitung** (Data Processing Agreement).

2. Zertifizierungen

Im Zuge der Erreichung der datenschutzrechtlichen Anforderungen und Sicherheitsstandards und um den eigenen Kunden eine gewisse Sicherheit zu geben, hat Microsoft darüber hinaus verschiedene Zertifizierungen an seinen Produkten durchführen lassen. Die erste Zertifizierung ist die ISO/IEC 27001.

Seit August 2014 gibt es darüber hinaus einen neuen internationalen Standard für den Datenschutz in der Cloud, die ISO/IEC 27018. Inhaltlich baut die Norm auf bereits existierende Sicherheitsstandards – insbesondere ISO/IEC 27001 – auf. Allerdings befasst sich ISO/IEC 27018 speziell mit der Regulierung der Verarbeitung von personenbezogenen Daten in der Cloud und ist somit der erste internationale Standard für Datenschutz in der Cloud basierend auf EU Datenschutzrecht.[24]

In der Praxis ist der Einsatz anerkannter Sicherheitsverfahren oder aber die Zertifizierung durch unabhängige Dritte ein entscheidendes Kriterium für die Auswahl des Cloud-Anbieters. Dies gilt umso mehr für die Kontrollrechte des Auftraggebers im Rahmen einer Auftragsdatenverarbeitung nach § 11 Abs. 2 Nr. 7 BDSG. Die ISO/IEC 27018 legt datenschutzrechtliche Anforderungen für die Anbieter von Cloud-Diensten fest und formuliert Überwachungsmechanismen und Richtlinien für die Implementierung von Maßnahmen, die den Schutz personenbezogener Daten in einer Cloud-Umgebung sicherstellen sollen.

Die Microsoft Online-Produktwelt hat seit Februar 2015 die ISO/IEC 27018-Zertifizierung und erfüllt somit international höchste Standards. Des Weiteren ist Microsoft durch die Artikel-29-Datenschutzgruppe positiv bewertet worden. In ihrer Auffassung betont die Artikel-29-Datenschutzgruppe wie wichtig es ist, einen Anbieter von Cloud-Diensten auszuwählen, der seine Datenschutzpraktiken transparent macht und die Schutzwürdigkeit von Kundendaten respektiert.[25] Die Artikel-29-Datenschutzgruppe bestätigt, dass Microsoft Cloud-Verträge die hohen Anforderungen im Bereich des EU-Datenschutzrechts einhalten und dass durch diese rechtliche Absicherung alle Microsoft Cloud-Kunden profitieren werden.

23 Vgl. Florian Müller, Lösungsberater Productivity Microsoft Deutschland GmbH, „Microsoft Online Services und ihre Sicherheitsleistungen im Überblick", Vortrag im Rahmen der Microsoft Cloud Events am 25.04.16 in München
24 Vgl. Bettina Sonnemann und Dr. Swantje Richters, Rechtsabteilung Microsoft Deutschland GmbH, „Microsoft Cloud Services – Seattle, Dublin, Frankfurt calling", Vortrag im Rahmen der Microsoft Cloud Events am 25.04.16 in München
25 Vgl. https://products.office.com/de-de/business/office-365-trust-center-top-privacy-questions

IV. Die unterschiedlichen Microsoft Cloud-Modelle

1. Die europäische Microsoft Cloud

Bei der Frage, welches Datenschutzrecht in welchem Cloud-Modell Anwendung findet, ist zum einen ein genauerer Blick auf die Standorte des Anbieters und der Nutzer der Cloud-Dienste notwendig und zum anderen muss die aktuelle, geltende Rechtslage beachtet und zeitgleich die anstehende europaweite Novellierung bereits reflektiert werden.

Microsoft betreibt seine europäischen Cloud-Rechenzentren in den Niederlanden und in Irland (Standorte Amsterdam und Dublin).

Befindet sich der Cloud-Anbieter innerhalb der EU und hat ein Cloud-Kunde seinen Wohnsitz in Deutschland, findet in Umsetzung der Europäischen Datenschutzrichtlinie (RL 95/46/EG)[26] aktuell deutsches Datenschutzrecht Anwendung, wenn es sich bei den in der Cloud gespeicherten Daten um „personenbezogene Daten" gem. § 3 Abs. 1 BDSG handelt. Gemäß der Richtlinie stellt eine grenzüberschreitende Datenverarbeitung innerhalb der EU 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.

Für eine Auftragsdatenverarbeitung benötigt man, wie bereits festgestellt, einen ADV-Vertrag. Mindestvoraussetzung für datenschutzkonformes Cloud-Computing in Europa ist also das Vorliegen eines schriftlichen Vertrages, der Regelungen zum Umfang der Datenverarbeitung, Festlegungen über Datenschutz- und Datensicherheitsmaßnahmen des Auftragnehmers (Sicherheitskonzept) und die Weisungsbefugnis des Auftraggebers bei allen datenschutzrelevanten Sachverhalten enthält.

Microsoft bietet im Rahmen der eigenen OST einen Vertrag zur Auftragsdatenverarbeitung an, der diese und viele andere Merkmale enthält (siehe obige Ausführungen). Die europäischen Standorte Niederlande und Irland sind somit datenschutzrechtlich unbedenklich.

In naher Zukunft wird die Datenschutzrichtlinie von der neuen Europäischen Datenschutzgrundverordnung[27] (DS-GVO) abgelöst. Zielsetzung der Verordnung ist es einerseits, die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen europaweit zu vereinheitlichen und andererseits die Betroffenenrechte zu stärken.

Im Gegensatz zur Datenschutzrichtlinie 95/46/EG, die von den EU-Mitgliedsstaaten in nationales Recht umgesetzt werden musste, wird die europäische Datenschutzgrundverordnung ohne Umsetzungsakt unmittelbar in allen EU-Mitgliedsstaaten gelten. Art. 99 DS-GVO regelt, dass die Verordnung am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft tritt und zwei Jahre nach ihrem Inkrafttreten gilt (voraussichtlich im Frühjahr 2018).

Am sachlichen Anwendungsbereich des Datenschutzrechts ändert sich im Vergleich zum aktuell geltenden BDSG zunächst wenig. Der Begriff der personenbezogenen Daten bleibt auch im Rahmen der DS-GVO bestehen und weit gefasst. Die europäische Verordnung beantwortet nicht – wie erhofft – die streitige Auslegungsfrage, was genau personenbezogene Daten sind und wie weit dieser Rechtsbegriff auszulegen ist. Eine Auslegungstendenz geht gemäß Art. 4 Abs. 1 DS-GVO aber eindeutig weiterhin zu einem weiten Begriff des Personenbezugs und somit zu dem Bestreben, den Anwendungsbereich des Datenschutzrechts möglichst weit zu fassen.

26 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE
27 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=DE

Hinsichtlich des territorialen Anwendungsbereichs bringt die DS-GVO gemäß Art. 3 Abs. 1 Neuerungen. Anders als nach bisherigem Recht ist es für die Anwendbarkeit unerheblich, ob die Datenverarbeitung in Europa stattfindet. Maßgeblich ist vielmehr die Niederlassung. Sobald ein Unternehmen in Europa eine Niederlassung unterhält, ist die DS-GVO anwendbar. Darüber hinaus ist die Verordnung auch dann einschlägig, wenn es zwar keine europäische Niederlassung gibt, aber das Verhalten eines EU-Bürgers auf dem Territorium der EU seitens eines Unternehmens „überwacht" wird. Der territoriale Geltungsanspruch des europäischen Datenschutzrechts wird somit erheblich erweitert. Es wird eine europaweite, einheitliche Rechtsanwendung im Bereich des Datenschutzes angestrebt.[28]

Zusammenfassend ist also zu sagen, dass die DS-GVO zwar das BDSG im Wesentlichen ablösen wird, aber die bekannten datenschutzrechtlichen Grundsätze weiterhin gelten werden. Es bleibt bei dem Verbotsprinzip mit Erlaubnisvorbehalt. Darüber hinaus müssen die bestehenden Vertragswerke innerhalb der nächsten zwei Jahre vor dem Hintergrund der DS-GVO überprüft und angepasst werden.

2. Die US-Cloud und Drittländer

Zunächst muss klargestellt werden, dass ein internationaler Datentransfer sowohl in der Vergangenheit rechtmäßig erfolgen konnte als auch in der Gegenwart immer noch erfolgen kann.

Die Begründung liefert Art. 2 f der aktuell noch geltenden europäischen Datenschutzrichtlinie 95/46/EG:[29]
„[...] Dritter (ist) jede [...] Stelle, außer [...] dem Auftragsverarbeiter [...]."

Es ergibt sich insoweit keine örtliche Einschränkung. Daher genießen Auftragsdatenverarbeiter außerhalb der EU grundsätzlich dieselben Rechte wie europäische Stellen. In anderen EU-Staaten ist dies auch in nationales Recht umgesetzt worden. In Deutschland haben wir insoweit eine Verböserung gegenüber der Richtlinie.

Nach dem Urteil des EuGH in den Rechtssachen C-468 und 469/10 vom 24.11.2011[30] 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. Insoweit kann also auch mit einem Dienstleister außerhalb Europas ein ADV-Vertrag geschlossen werden, bzw. die Daten an dessen Standort transferiert werden. Es ist jedoch bei einem internationalen Datentransfer zu beachten, dass dieser neben dem bereits angesprochenen ADV-Vertrag einer zusätzlichen Rechtsgrundlage bedarf, um ein angemessenes Datenschutzniveau zu gewährleisten.

Bei der Übermittlung personenbezogener Daten aus Deutschland an eine Stelle in einem außereuropäischen Staat, der auch nicht sicherer Drittstaat ist, wie z. B. die USA, muss ein wirksamer Schutz der Persönlichkeitsrechte der Betroffenen sichergestellt werden. Dies war bisher möglich durch:

- Einwilligung
- EU-Standardvertragsklauseln
- Processor BCRs (sogenannte Binding Corporate Rules)
- und auf Grundlage des Safe Harbor Abkommens (Safe Harbor-Entscheidung der Europäischen Kommission (2000/520/EG))

28 Vgl. Prof. Niko Härting, Datenschutzgrundverordnung – IT-Rechtsfragen aus der Praxis, in ITRB 2/2016, S.36-40, sowie Janina Thieme, PRW Rechtsanwälte, „Welche Neuerungen bringt die Europäische Datenschutzgrundverordnung?", Whitepaper, Stand Februar 2016
29 http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_de.pdf
30 http://curia.europa.eu/juris/document/document.jsf?docid=115205&doclang=DE

Der Gerichtshof der Europäischen Union hat mit Urteil vom 06.10.2015 die unter dem Namen Safe Harbor bekannte Entscheidung der EU-Kommission für ungültig erklärt.[31] Davon betroffen sind Datentransfers in die USA.[32] Für die Praxis bedeutet das, dass ein Rückgriff auf Safe Harbor als Rechtsgrundlage in Zukunft ausscheidet. Darüber hinaus werden seitens der nationalen Datenschutzbehörden Genehmigungen für internationale Datentransfers, beruhend auf „Binding Corporate Rules“ oder Exportverträgen, nicht länger erteilt.

Die Anforderungen an das Institut hinsichtlich der Einwilligung werden im Rahmen der neuen Rechtsprechung ebenfalls noch strenger ausgelegt. Insoweit sollen Einwilligungen in Zukunft nur zulässig sein, wenn es nicht zu einer wiederholten, massenhaften oder routinemäßigen Übertragung kommt.

Zu den EU-Standardvertragsklauseln hat der EuGH keine Aussage getroffen. Deshalb sind nach aktueller Rechtslage die EU-Standardvertragsklauseln die einzige, rechtlich solide Grundlage für einen internationalen Datentransfer mit angemessenem Schutzniveau. Microsoft stützt, wie oben bereits ausgeführt, seine Verträge auf die Standardvertragsklauseln. Wie der Vertrag zur Auftragsdatenverarbeitung, werden dem Kunden auch die EU-Standardvertragsklauseln im Rahmen der Online Services Terms als Vertragsgrundlage bereitgestellt.

Es ist zu erwarten, dass die nationalen Datenschutzbehörden auch die EU-Standardklauseln in naher Zukunft gerichtlich überprüfen lassen werden. Sie möchten nun auch hierzu eine EuGH Entscheidung. Es ist an dieser Stelle aber noch einmal ausdrücklich darauf hinzuweisen, dass allein der EuGH Aufhebungskompetenz hat.

Der Safe Harbor-Nachfolger, das EU-US-Privacy Shield[33], soll in den kommenden Monaten im Detail ausgearbeitet werden. Sollten die EU-Standardvertragsklauseln tatsächlich durch eine höchstrichterliche Entscheidung fallen, kann das in der Zwischenzeit gereifte Abkommen als neue Rechtsgrundlage für einen Datentransfer in die USA dienen.

Auch dieses steht bereits wieder in der allgemeinen Kritik. Aber auch für diese rechtliche Überprüfung wäre allein der EuGH zuständig. Eine Befassung würde allerdings erst im Anschluss an die Entscheidung über die EU-Standardvertragsklauseln erfolgen.

Insoweit wird immer eine geltende Rechtsgrundlage für einen internationalen Datentransfer zur Verfügung stehen.

3. Die deutsche Microsoft Cloud – das neue Treuhandmodell

Darüber hinaus entwickelt Microsoft das bestehende Cloud-Modell durch die Option der deutschen Datentreuhand noch einen Schritt weiter. Die neue deutsche Microsoft Cloud stellt die Microsoft-Dienste Azure, Office 365 sowie Dynamics CRM Online aus lokalen deutschen Rechenzentren bereit, die über ein eigenständiges deutsches Netzwerk miteinander verbunden sind.

Durch diese Architektur wird sichergestellt, dass die Kundendaten ausschließlich in Deutschland gespeichert werden und die Kontrolle über den Zugriff auf Kundendaten, einschließlich der Infrastruktur und der Systeme, auf denen die Kundendaten gespeichert werden, einem deutschen Unternehmen, konkret der Deutschen Telekom mit ihrer Tochter T-Systems, als Datentreuhänder übertragen wird. Der Datenabgleich zwischen den Rechenzentren erfolgt über ein eigenständiges deutsches Netzwerk, um die Aufrechterhaltung des Betriebs sowie die Wiederherstellung in Notfällen sicherzustellen. Diese einzigartige Architektur stellt sicher, dass die Kundendaten innerhalb Deutschlands transportiert und gespeichert werden.

31 http://curia.europa.eu/juris/documents.jsf?num=C-362/14
32 Vgl. Prof. Georg Borges, Datentransfer in die USA nach Safe Harbor, in NJW 2015, 3617
33 http://europa.eu/rapid/press-release_IP-16-433_de.htm

Die Vorteile der neuen Microsoft Cloud mit dem deutschen Datentreuhand-Modell sind:[34]

- Innovation: Es kommen die globalen Technologien lokal zur Anwendung mit dem gleichen hohen Service-Level.
- Sicherheit: Die Kundendaten werden unter Verwendung derselben Sicherheitstechnologien und -prozesse geschützt, die in Microsofts weltweiten Rechenzentren zum Einsatz kommen. Die Daten werden jedoch ausschließlich in Deutschland gespeichert.
- Datenschutz und Kontrolle: Die Microsoft Cloud für Deutschland stellt sicher, dass jeglicher Zugriff auf Kundendaten von einem unabhängigen deutschen Unternehmen, dem Datentreuhänder oder direkt vom Kunden kontrolliert wird. Ein Datenzugriff erfordert die Zustimmung des Datentreuhänders. Microsoft hat keinen Zugriff auf die Kundendaten.
- Transparenz: Die Kunden wissen, was mit ihren Kundendaten geschieht.
- Compliance: Microsoft hilft ihnen dabei, ihre regulatorischen Verpflichtungen zu erfüllen, indem sie relevante deutsche Gesetze und zentrale internationale Standards einhalten.

Hinsichtlich des Datenschutzes werden in deutschen Rechenzentren die Vorschriften des BDSG zur Anwendung kommen. Da diese auf der EU-Datenschutzrichtlinie beruhen, ist auch hier von einer Datenschutzkonformität auszugehen. Hinzukommen dürfte in diesem Fall aber noch ein zusätzlicher Auftragsdatenverarbeitungsvertrag mit dem Treuhänder T-Systems.

V. Datenschutzrechtliches Wissen/Datenschutzkonformität von Office 365

1. Findet Datenschutz überhaupt Anwendung?

Zunächst muss geklärt werden, welche Daten über Microsoft Office 365 verarbeitet werden. Haben diese Personenbezug? Wenn nein, findet der Datenschutz keine Anwendung. Wenn ja, ist zu prüfen, ob mit einer angemessenen Verschlüsselung gearbeitet wird, wenn ja findet das Datenschutzgesetz keine Anwendung.

2. Datenschutzprüfung

Kommt man zu dem Ergebnis, dass personenbezogene Daten verarbeitet werden, sind folgende Feststellungen zu treffen:

a) Zunächst ist festzuhalten, dass jedes Unternehmen mit Sitz in Deutschland, das bei der Verarbeitung von personenbezogenen Daten einen Cloud-Dienst nutzt, datenschutzrechtlich die verantwortliche Stelle i.S.d § 3 Abs. 7 BDSG bleibt. Das gilt selbstverständlich auch für die Nutzung der Microsoft Cloud-Dienste.

b) Es besteht zwischen dem Unternehmen, das die Microsoft Cloud-Dienste nutzt, und Microsoft ein so genanntes Auftragsdatenverarbeitungsverhältnis. Voraussetzung ist, dass die besonderen vertraglichen Anforderungen eingehalten werden. Dass dies der Fall ist, darf unterstellt werden (s.o.), da Microsoft in seinen Online Services Terms (OST) darauf verweist.

c) Findet die Datenverarbeitung innerhalb der EU statt, genügt der Abschluss eines Vertrages zur Auftragsdatenverarbeitung. Dieser liegt vorunterschrieben seitens Microsoft vor.

d) Findet die Auftragsdatenverarbeitung außerhalb der EU in datenschutzrechtlich „unsicheren Drittstaaten“, wie zum Beispiel den USA, statt, ist der Abschluss sog. EU-Standardvertragsklauseln erforderlich. Diese dienen dazu, das Datenschutzniveau an das der EU anzupassen.

e) Für eine rechtmäßige Auftragsdatenverarbeitung in der Cloud ist es zudem notwendig, dass dem Auftraggeber Kontrollrechte beim Auftragnehmer eingeräumt werden. Es können – mit Ankündigung – Vor-Ort-Kontrollen durch einen Mitarbeiter des Auftraggebers durchgeführt werden. Das muss aber nicht sein. Eine Kontrolle der Einhaltung datenschutzrechtlicher Vorgaben kann aber auch durch die Vorlage von Zertifikaten, Gutachten oder Auditberichten unabhängiger Prüfer erfolgen.

34 Vgl. https://www.microsoft.com/de-de/cloud/deutsche-datentreuhand.aspx

f) Microsoft hat bei den relevanten Cloud-Diensten die ISO/IEC 27018, einen internationalen Standard für Datenschutz in der Cloud, umgesetzt. Die Vorlage einer Bestätigung der Umsetzung dieses Standards ist als Umsetzung von Kontrollrechten zu werten.

Damit ist das Arbeiten mit Office 365 aus datenschutzrechtlicher Sicht unbedenklich.

3. Microsoft Trust Center

Auf einer gesonderten Plattform (sogenanntes Trust Center) hat sich Microsoft für seine Kunden noch einmal öffentlich mit dem Thema Datenschutz befasst und stellt alle relevanten Informationen zur Verfügung.[35] Die bereitgestellten Hinweise können ihre Geltung bezüglich der gesamten Microsoft Cloud-Produktwelt entfalten. Microsoft weist dort noch einmal ausdrücklich auf die Stellungnahmen vom 1. Juli 2012 der Artikel-29-Datenschutzgruppe zum Cloud-Computing hin. Die Auffassung der Artikel-29-Datenschutzgruppe stellt einen Leitfaden für aktuelle und potenzielle Cloud-Benutzer dar. Die Fragen und Antworten hat Microsoft auf der angegebenen Seite aufgeführt.

VI. Grundlagen zu Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online ist eine CRM-Lösung aus dem Hause Microsoft, die mithilfe von Informationen aus Social Media, Business Intelligence und Kampagnenmanagement in der Cloud, vor Ort oder im Rahmen eines Hybridangebots das Kundenmanagement eines Unternehmens verbessern soll.[36] Mithilfe der Kombination aus Microsoft Dynamics CRM Online und Office 365 können Unternehmen die vertrauten Lösungen mit einheitlichen Oberflächen auf dem PC, mobilen Endgeräten und im Webbrowser nutzen. Außerdem können Unternehmen ortsunabhängig im Online- oder im Offlinemodus auf ihre Informationen und Anwendungen zugreifen und diese bearbeiten. Microsoft Dynamics CRM Online sorgt zusätzlich für eine nahtlose Zusammenarbeit einzelner Abteilungen innerhalb des Unternehmens, da Dateien und Informationen mit anderen internen und externen Anwendern gemeinsam per Onlinekonferenz bearbeitet werden können.[37]

Microsoft Dynamics CRM Online umfasst u. a. folgende Funktionen:

- Marketing: flexible Segmentierungswerkzeuge, vereinfachte Funktionen für die Kampagnensteuerung, intuitives Response-Tracking, aussagekräftige Analysen
- Vertrieb: volle Lead-to-Cash-Transparenz, Verfolgung von Leads und Verkaufschancen, optimierte Genehmigungsverfahren und Vertriebsforecasts in Echtzeit
- Kundenservice: Werkzeuge, die das Fallmanagement vereinfachen, Eskalationsprozesse verkürzen, den Austausch von Wissen verbessern und ein effektiveres Kundenmanagement ermöglichen
- Erweitertes CRM: Eine flexible Applikation, mit der individuelle Anwendungen und komplexe Branchenlösungen erstellt werden können.

Immer wieder wurden und werden CRM-Systeme allgemein als datenschutzkritisch bezeichnet. Kritikpunkt war u. a. die mögliche Speicherung personenbezogener Kundendaten auf den Datenbänken von Unternehmen. Keine Frage, das ist technisch möglich und (unter Umständen) unzulässig. Es macht jedoch wenig Sinn, ein System so zu parametrisieren, dass es gesetzeswidrig arbeitet. Bußgelder oder Reputationsschäden durch die nicht sachgemäße Anwendung von CRM-Systemen würden dem klaren Vorteil der Anwendung des Systems zuwiderlaufen.

Es kann auch dahinstehen, dass ein CRM-System in den USA anders aufgestellt ist als in Europa. Nachfolgend wird von einer datenschutzkonformen Einrichtung in Deutschland und damit in Europa ausgegangen. Für ein CRM-System gelten in Deutschland im Umgang mit personenbezogenen Daten aktuell die verschiedenen nationalen Datenschutzgesetze, allen voran das Bundesdatenschutzgesetz. Im Folgenden werden die wichtigsten rechtlichen Prinzipen des BDSG dargestellt.

35 Vgl. https://products.office.com/de-de/business/office-365-trust-center-cloud-computing-security und https://products.office.com/de-de/business/office-365-trust-center-top-privacy-questions
36 Vgl. http://www.microsoft.com/de-de/dynamics/crm.aspx
37 Vgl. http://www.microsoft.com/de-de/dynamics/crm-office-365.aspx

1. Zweckbindungsgrundsatz

Personenbezogene Daten dürfen nach § 14 BDSG durch öffentliche und durch nicht öffentliche Stellen verwendet werden, wenn das zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist und die Daten auch schon zu diesem Zweck beschafft wurden (Datenschutz, Datenverarbeitung). Von dem Grundsatz bestehen jedoch zahlreiche Ausnahmen (offensichtliches Eigeninteresse des Betroffenen, Überprüfungen, Gefahrenabwehr, Strafverfolgung, wissenschaftliche Forschung). Nicht öffentliche Stellen (also die Privatwirtschaft) dürfen darüber hinaus auch ihre eigenen berechtigten Interessen wahren (z. B. Forderungseinziehung) sowie Werbe-, Markt- und Meinungsforschungszwecke verfolgen. Im Bereich privater Wirtschaftsunternehmen stellt § 28 Abs. 1 BDSG auf den „eigenen Geschäftszweck“ ab. In diesem Rahmen ist die Datenverarbeitung unter bestimmten weiteren Voraussetzungen zulässig. Soll ein anderer Zweck verfolgt werden, so stellt § 28 Abs. 2 BDSG klar, dass hierfür weitere und engere Voraussetzungen erforderlich sind. Gemäß § 28 Abs. 3 BDSG ist die Verarbeitung von personenbezogenen Daten zum Zwecke der Werbung zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach § 28 Abs. 3a BDSG (elektronische Einwilligung) verfährt. Dies bedeutet für Unternehmen, die mithilfe eines CRM ein Mailing durchführen wollen, dass auch hier das Opt-In Verfahren nicht vergessen werden darf. In diesem Zusammenhang sollte ein CRM-System über ein Verfahren verfügen, das auch aufzeichnet, wenn ein Kunde seine Einwilligung widerrufen hat und somit keine Werbeaktion vom Unternehmen mehr zugestellt werden darf.

2. Trennungsgebot

Der zweite wichtige Grundsatz ist das sogenannte Trennungsgebot. Gemäß der Anlage zu § 9 Satz 1 Nr. 8 BDSG sind Maßnahmen zu treffen, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben worden sind, auch getrennt verarbeitet werden. Dies bedeutet für datenschutzkonforme CRM-Systeme, dass die erhobenen Daten von Kunden ihrem Zweck nach differenziert verarbeitet und gespeichert werden müssen. Das CRM muss es dem Nutzer ermöglichen, verschiedene Gruppen einzurichten (wie z. B. Daten für Marketing-zwecke, Daten für Verkaufszwecke und Daten für Servicezwecke).

Ein datenschutzkonformer Betrieb eines CRM-Systems ist also durchaus möglich. Es sind eben nur einige Parameter aus den Gesetzen dabei zu beachten.

3. Herkunftsnachweis

Mit der Neufassung des Bundesdatenschutzgesetzes im Jahr 2009 wurde nochmals klargestellt, dass die Verwender von Daten grundsätzlich die Betroffenen über deren Herkunft informieren müssen, soweit dies erfragt wird. Dies kann nur dann erfolgen, wenn diese hinterlegt sind. Ohne die Möglichkeit der Rückverfolgbarkeit wird eine CRM-Software nicht datenschutzkonform genutzt werden können.

Das Recht ist in § 19 BDSG (betreffend Datenverarbeitung öffentlicher Stellen) und § 34 BDSG (betreffend Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen) festgelegt.

4. Datenlöschung

Im BDSG widmet sich in erster Linie der § 35 BDSG dem Löschen und Sperren personenbezogener Daten. Neben den Festlegungen des BDSG können auch andere Quellen Festlegungen treffen. So finden sich etwa im Telekommunikationsrecht oder im Steuerrecht (z. B. § 147 Abgabenordnung – AO) Regelungen, aus denen sich Fristen zur Aufbewahrung ableiten. Gemäß § 3 Abs. 4 Nr. 5 BDSG ist unter Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten zu verstehen.

Personenbezogene Daten sollten gelöscht werden, wenn für deren Speicherung keine Rechtsgrundlage existiert oder diese Rechtsgrundlage später weggefallen ist. Die Rechtsgrundlage besteht etwa dann nicht mehr, wenn eine Einwilligung in die Verarbeitung und Nutzung personenbezogener Daten widerrufen wurde. Der Wegfall der Rechtsgrundlage führt dazu, dass die entsprechenden Informationen gelöscht werden müssen.

Personenbezogene Daten müssen auch dann gelöscht werden, wenn der Zweck ihrer Speicherung erreicht wurde und daher ihre Kenntnis für die Erreichung des Zwecks nicht mehr erforderlich ist (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG). Allerdings kann es passieren, dass diese eigentlich zu löschenden personenbezogenen Daten nicht gelöscht werden dürfen, weil etwa gesetzliche Regelungen eine Aufbewahrung vorschreiben (s.o. § 147 AO).

Es ist gesetzlich nicht vorgeschrieben, dass und wie dokumentiert werden muss, dass personenbezogene Daten gelöscht wurden. Allerdings kann eine Dokumentation die Beweisführung erleichtern, dass bestimmte personenbezogene Daten zu einem bestimmten Zeitpunkt gelöscht wurden.

VII. Datenschutzkonformität von Microsoft Dynamics CRM Online

CRM-Systeme können natürlich immer so administriert werden, dass ihr Gebrauch nicht mit den Grundsätzen des Datenschutzes in Einklang steht. Darum geht es hier aber nicht. Hier geht es ausschließlich um die Frage, ob Microsoft Dynamics CRM Online datenschutzkonform aufgesetzt werden kann. Der Wille zur gesetzeskonformen Administration wird also nachfolgend unterstellt.

1. Trennungsgebot

Microsoft Dynamics CRM Online ist in verschiedene Hauptarbeitsfelder unterteilt:

- Vertrieb
- Service
- Marketing

Diese Aufteilung ermöglicht es dem Nutzer, die personenbezogenen Daten, wie vom Gesetzgeber gefordert, getrennt nach ihrem Verwendungszweck zu verwalten. Grundlage dazu bildet das Sicherheitskonzept. Dadurch werden die Datenintegrität und die Geheimhaltung von Daten gewährleistet. Außerdem werden damit ein effizienter Datenzugriff und eine effiziente Zusammenarbeit unterstützt. Die Vorgaben des Modells sind:

- Ermöglichung von Benutzerzugriffen ausschließlich auf die Informationsebenen, die die Benutzer zum Ausführen ihrer Aufgaben benötigen
- Kategorisierung von Benutzern und Teams nach Sicherheitsrollen und Beschränkung des Zugriffs basierend auf diesen Rollen
- Vermeidung des Zugriffs auf Objekte, die ein Benutzer nicht besitzt oder freigibt

Das Trennungsgebot wird somit durch das Sicherheitskonzept erreicht. Details zu den Sicherheitskonzepten für Microsoft Dynamics CRM hat Microsoft für seine Partner auf der Online TechNet-Bibliothek zusammengestellt.[38]

2. Berechtigungskonzept

In den Einstellungen von Microsoft Dynamics CRM Online lassen sich zudem bestimmte Berechtigungen festlegen (wie z. B. Lesen, Schreiben und Löschen).

So können Berechtigungssätze gemeinsam in Rollen gruppiert werden, die die Aufgaben beschreiben, die von einem Benutzer oder einem Team ausgeführt werden können. Microsoft Dynamics CRM Online enthält einen Satz vordefinierter Sicherheitsrollen, die jeweils einen Satz von Berechtigungen darstellen. Diese wurden zusammengefasst, um das Sicherheitsmanagement zu erleichtern. Die meisten Berechtigungen definieren die Möglichkeit, Datensätze eines bestimmten Typs zu erstellen, zu lesen, zu schreiben, zu löschen oder freizugeben.

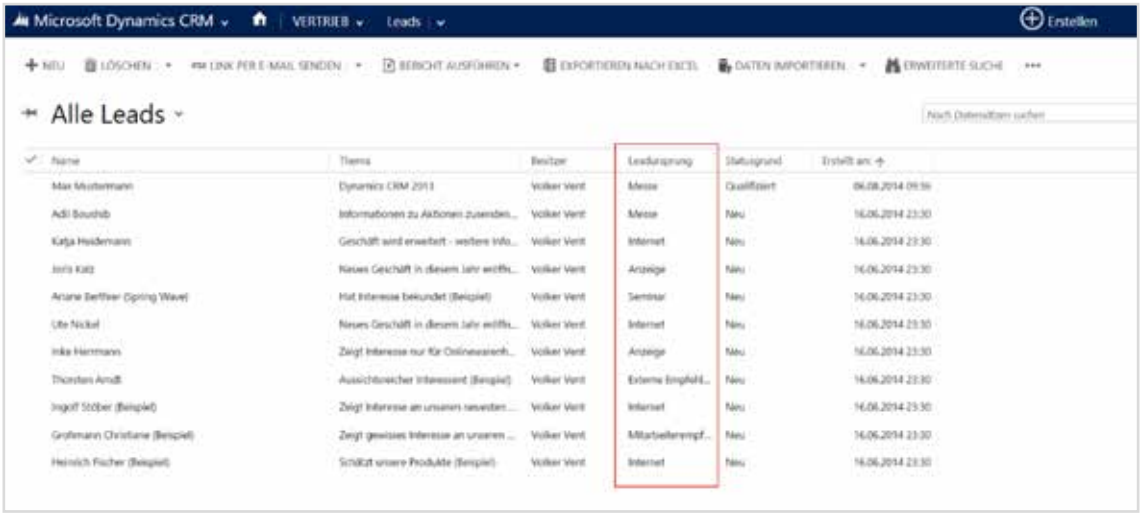
Jede Berechtigung definiert auch, wie weit die Berechtigung geht. Also etwa auf Benutzerebene, auf Unternehmenseinheitenebene, für eine bestimmte Unternehmenshierarchie oder für die gesamte Organisation. Wenn sich zum Beispiel ein Benutzer anmeldet, dem die Rolle „Vertriebsmitarbeiter“ zugewiesen ist, so hat er die Berechtigungen zum Lesen, Schreiben und Freigeben für die gesamte Organisation. Er kann jedoch nur Accountdatensätze löschen, deren Besitzer er selbst ist. Außerdem hat er keine Berechtigung zur Systemverwaltung, wie etwa zum Installieren von Produktaktualisierungen, oder um Benutzer zum System hinzuzufügen.

38 https://technet.microsoft.com/de-de/library/hh699698.aspx

Ein Benutzer, dem die Rolle „Vertriebsleiter“ zugewiesen wurde, kann mehr Aufgaben ausführen (und besitzt eine größere Anzahl von Rechten) im Zusammenhang mit der Anzeige und Änderung von Daten und Ressourcen, als ein Benutzer mit der Rolle „Vertriebsmitarbeiter“. Ein Benutzer mit der Vertriebsleiterrolle kann beispielsweise jedes Konto im System lesen und allen Benutzern zuweisen, während ein Vertriebsmitarbeiter dies nicht kann. Es gibt zwei Rollen mit sehr umfassenden Berechtigungen: Systemadministrator und Anpasser. Die Verwendung dieser beiden Rollen sollte auf wenige Personen in der Organisation eingeschränkt sein.

3. Herkunft der Daten

Außerdem bietet Microsoft Dynamics CRM Online die Möglichkeit, die Herkunft der personenbezogenen Daten zu dokumentieren und zu protokollieren. Diese sind bei der Leadverwaltung im System enthalten und können den unterschiedlichsten Kundenanforderungen angepasst werden. Im „Leadursprung“ ist die Herkunft der Daten dokumentiert.



4. Datenlöschung

Zudem lassen sich in Microsoft Dynamics CRM Online Konzepte für die Löschung von Datensätzen anlegen, um nicht mehr benötige Daten aus der Datenbank zu entfernen.
Mit der Massenlöschung werden nicht mehr benötigte Datensätze gelöscht.

So können beispielsweise die folgenden Daten in einem Massenvorgang gelöscht werden:

- Veraltete oder nicht mehr benötigte Daten
- Nicht benötigte Test- oder Beispieldaten
- Daten, die von anderen Systemen nicht ordnungsgemäß importiert wurden

Mit der Massenlöschung können die folgenden Vorgänge ausgeführt werden:

- Daten löschen über mehrere Entitäten
- Löschen von Datensätzen für eine bestimmte Entität
- Löschen von Daten in regelmäßigen Intervallen

Informationen dazu, wie Massenlöschungen in den Code implementiert werden können, finden sich unter „Massenlöschung von Daten“.[39]

39 https://msdn.microsoft.com/de-de/library/gg334418.aspx

5. Anonymisierung und Verschlüsselung

Bei Statistiken, die keine Personalisierung der Daten benötigen, bietet Microsoft Dynamics CRM Online eine Anonymisierung der Daten an. Bei der Erstellung von Statistiken bzw. Berichten nutzt Microsoft Dynamics CRM Online dabei unterschiedliche Technologien. Für die Erstellung von Berichten können die SQL Server Reporting Services SSRS genutzt werden. Für Statistiken, die auf den Systemmasken (Forms) angezeigt werden, können mittels jQuery die Abfragen realisiert werden. Beide Technologien bieten somit die Möglichkeit, die Daten zu anonymisieren. Details zur Verschlüsselung von Daten sind auf den Seiten Vaultive for Dynamics CRM Online beschrieben.

6. Datensicherheit

Wie bereits zuvor erwähnt, spielt die Datensicherheit in einem Cloud-basierten CRM-System eine besondere Rolle, nicht zuletzt aufgrund des § 203 StGB i.V.m. § 13 StGB. Zur tatsächlichen IT-Sicherheit von Microsoft Cloud-Anwendungen können wir abschließend keine Bewertung vornehmen. Des Weiteren gelten die obigen Ausführungen zu Datensicherheit und Zertifizierungen.

Ein Unternehmen sollte sich bei der Einführung von Microsoft Dynamics CRM Online immer zuvor die Frage stellen, ob die eigene IT-Infrastruktur im Bereich IT-Sicherheit besser ist als die, die Microsoft verwendet. In den meisten Fällen werden Unternehmen dann sagen müssen, dass aus technischer Sicht eine Microsoft Cloud-Lösung in der Regel „besser“ im Sinne von sicherer ist.

7. Microsoft Dynamics CRM Online und Microsoft Social Listening

In der heutigen Zeit ist die Verwendung von Social Media nicht nur auf den privaten Bereich beschränkt, auch immer mehr Unternehmen haben den Nutzen von Social Media erkannt. Auch Microsoft Dynamics CRM Online bietet Unternehmen die Möglichkeit, mithilfe von Microsoft Social Listening[40] mehr über ihre Kunden und Zielgruppen zu erfahren, um somit ihre Marketingabteilung, Vertriebsabteilung oder ihren Service zu verbessern.

In diesem Zusammenhang ist Unternehmen jedoch zu raten, dass sie sich ausreichend rechtlich absichern, bevor sie Social Media Programme in ihre Organisation aufnehmen. Unternehmen sollten sogenannte Social Media Guidelines implementieren, um zu regeln, welche Angestellten wann und wie Social Media Angebote beruflich oder privat nutzen dürfen. Auch das Urheberrecht sollte ein Unternehmen in diesem Zusammenhang nicht vergessen. Wenn zum Beispiel Angestellte den Content auf der eigenen Social Media Seite mit urheberrechtlich geschützter Musik hinterlegen, kann dies erhebliche Konsequenzen für das Unternehmen haben. Zusätzlich sollten Unternehmen das Telemediengesetz (z. B. Impressumspflicht etc.) und das Gesetz gegen den unlauteren Wettbewerb (z. B. Online-Marketing etc.) in diesem Zusammenhang nicht vergessen.

Unser Hauptthema, der Datenschutz, muss natürlich noch genannt werden. Der Datenschutz in sozialen Medien findet natürlich Anwendung und sollte von Unternehmen beachtet werden. Besonders bei der Einbindung von sogenannten „Social-Plugins“ müssen Nutzer der Webseite in den Datenschutzerklärungen explizit auf die Verwendung dieser Plugins hingewiesen werden.

Grundsätzlich kann das Social Media Tool von Microsoft Dynamics CRM Online von Unternehmen genutzt werden. Jedes Unternehmen ist jedoch selbst dafür verantwortlich, wie es das Tool verwendet und welche rechtlichen Anforderungen es in seiner Organisation implementiert, um Reputationsschäden oder anderen Konsequenzen aus dem Weg zu gehen.

40 Vgl. https://www.microsoft.com/de-de/dynamics/crm-social.aspx

VIII. 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:

- Bessere Technologie als bisher
- Gesicherte Integration in die Organisation
- Unbedenklichkeitserklärung zur Rechtslage

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 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.[41]
Fragen Sie uns gerne hierzu.

IX. Hotline

Wir haben uns intensiv mit der Datenschutzkonformität von Microsoft Cloud-Produkten befasst. Wenn Sie als Microsoft Partner 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 89 210977-0
Stichwort: Microsoft Cloud-Hotline

Sie werden dann mit einem kompetenten Kollegen verbunden oder zurückgerufen.

X. Fazit

Wie in den vorherigen Kapiteln gezeigt, gibt es eine ganze Reihe von relevanten Datenschutzvorschriften zum Thema Cloud-Computing. Die beschriebenen Microsoft Produkte in ihrer Online-Version (Online Services) erfüllen diese Vorschriften nach deutschem und europäischem Datenschutzrecht. Darüber hinaus ist auch ein internationaler Datentransfer mit den entsprechenden Rechtsgrundlagen möglich.

Microsoft hat umfangreiche Maßnahmen im Bereich Datenschutz und Datensicherheit für seine Cloud-Dienste ergriffen. Die Zertifizierungen, die technischen Maßnahmen, die Online Services Terms und die im Rahmen dieser zur Verfügung gestellten ADV-Verträge und EU-Standardvertragsklauseln sowie die hohe Fachkompetenz im Bereich IT, sind Vorteile, die durch die Verwendung von Microsoft Produkten entstehen und genutzt werden können.

Wer sicher sein möchte, dass alle Vorschriften im eigenen System rechtskonform umgesetzt wurden, sollte sich auditieren lassen. Sprechen Sie uns bei Interesse einfach an.

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

XI. 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.

Autoren

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 27 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.

Rechtsanwältin Janina Thieme
Studium der Rechtswissenschaften und Referendariat in München mit Stationen in Hamburg und Washington D.C. Nach einer mehrjährigen Tätigkeit als wissenschaftliche Mitarbeiterin während der Ausbildung in den Bereichen Wirtschaftsprivatrecht und IT-Recht, ist sie seit 2016 zur Anwaltschaft zugelassen und angestellte Rechtsanwältin bei PRW Rechtsanwälte.

Mitgliedschaften

EuroITcounsel London
Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltsverein (DAVIT)
Deutsche Gesellschaft für Recht und Informatik e. V. (DGRI)
Computer Law Association (heute TechLaw)

PRWRECHTSANWÄLTE

PRW Rechtsanwälte
Reiners Wilser Schloßmacher Herrmann PartG mbB
Leonrodstr. 54
D-80636 München
Telefon: +49 89 210977-0
Telefax: +49 89 210977-77
E-Mail: reiners@prw.de · mailto:office@prw.de
Web: www.prw.de