PRWRECHTSANWÄLTE

WHITEPAPER

ALLABOUT COMPLIANCE

Datenschutzkonformität von Microsoft Dynamics CRM Online

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 wird Microsoft Dynamics CRM Online auf seine Datenschutzkonformität geprüft. Hierbei wird zum Teil auf andere Publikationen aus unserer Kanzlei zum Thema Microsoft Online Services Bezug genommen.

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

Die Markenrechte an Microsoft Dynamics CRM Online stehen allein Microsoft zu. Der Umgang mit diesen Marken erfolgt hier lediglich redaktionell.

RA Wilfried Reiners, MBA

II. 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.[1] 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.[2]

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.[3]

In den folgenden Kapiteln wird aufgezeigt, welche Anforderungen Microsoft Dynamics CRM Online bereitstellen muss, um datenschutzkonform aufgesetzt werden zu können.

1 Vgl. http://www.microsoft.com/de-de/dynamics/crm.aspx
2 Vgl. http://www.microsoft.com/de-de/dynamics/crm-office-365.aspx
3 Vgl. http://www.microsoft.com/de-de/cloud/services/dynamics_crm_online.aspx

III. Grundlagen

1. Begriffe CRM und Cloud-Computing

Das Customer-Relationship-Management, kurz auch CRM genannt, bezeichnet die systematische Bearbeitung von Kundenbeziehungen in einem Unternehmen. Die hierzu erhobenen Daten von Kunden werden in einer Datenbank gespeichert und unterstützen den Kundensachbearbeiter bei seiner Arbeit. Aufgrund dessen können drei Hauptabteilungen aufgezeigt werden, für die das CRM von besonderer Bedeutung ist: Verkauf, Service und Marketing. Ein erfolgreich geführtes CRM hat somit die Aufgabe, klare Ziele, Strategien und Konzepte im Bereich der Kundenbeziehung zu erstellen, damit die bereits vorhandenen Geschäftsprozesse in einem Unternehmen optimiert werden.

Unter dem Begriff Cloud-Computing wird u. a. die Möglichkeit verstanden, Daten auf einem entfernten Server oder Rechenzentrum zu speichern sowie Programme zu nutzen, die nicht auf dem lokalen Rechner installiert sind.[4] Cloud-Computing bietet somit 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. Der ortsunabhängige Zugang wird durch verschiedene Endgeräte (z. B. Laptops, Tablet-PC's, Smart Phones) ermöglicht. Damit kann nahezu jederzeit auf die erforderlichen Informationen oder Geschäftsanwendungen zugegriffen werden. Cloud-Computing wird eine große Zukunft vorausgesagt, weil dadurch u. a. Skaleneffekte genutzt werden können, die die Anwendungskosten reduzieren. Nach Angaben des Hightech-Verbandes BITKOM nutzen zurzeit 40 % der Unternehmen in Deutschland Cloud-Computing. Für IT-Anbieter ergeben sich dadurch neue Geschäftsmodelle.[5] Es ist 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.[6]

2. CRM und Datenschutz

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 ein Reputationsschaden 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 die verschiedenen Datenschutzgesetze. Zu nennen sind hier vor allem die Datenschutzgesetze der Länder und der Kirchen und allen voran das Bundesdatenschutzgesetz (BDSG), worauf wir nachfolgend referenzieren. Zunächst einige Grundsätze:

a. 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-,

4 Vgl. http://de.wikipedia.org/wiki/Cloud_Computing
5 Vgl. http://www.bitkom.org/files/documents/140203_CC_neue_Geschaeftsmodelle.pdf
6 Vgl. http://www.bmwi.de/DE/Themen/Digitale-Welt/Internet-der-Zukunft/cloud-computing.html

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 mit Hilfe 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.

b. 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 Marketingzwecke, 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.

c. 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.

d. Datenlöschung

Im BDSG widmet sich in erster Linie § 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.

3. Cloud-Computing und Datenschutz

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

- „Innovatives, sicheres und rechtskonformes Cloud-Computing“[7] (2012) oder
- „Mit Recht in der Cloud“[8] (2013),

die zwar Themenstellungen aufzeigen und vor Risiken warnen, im Ergebnis jedoch wenig konkret werden. 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“[9]. Zwei Jahre später erklärte das ULD in einer Pressemitteilung vom 13.07.2012: „Datenschutzkonformes Cloud-Computing ist möglich“[10], 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[11] 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.“[12] Weiter heißt es vom ULD: „Cloud-Computing ist eine technische Realität, bei der die Beachtung der Datenschutzvorschriften zwingend gefordert ist.“[13]
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.

4. Auftragsdatenverarbeitung

Die Datenverarbeitung im Auftrag – verkürzt 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 von ihm in die Cloud übermittelten personenbezogenen Daten verantwortlich. 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...“.

7 Vgl. http://www.bmwi.de/DE/Mediathek/publikationen,did=523348.html
8 Vgl. http://www.bmwi.de/Dateien/BMWi/PDF/Monatsbericht/Auszuege/09-2013-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de
9 Thilo Weichert, Cloud-Computing und Datenschutz, 07.06.2010, https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html
10 PRESSEMITTEILUNG, ULD: „Datenschutzkonformes Cloud Computing ist möglich“, 13.07.2012, https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.htm
11 Die Artikel-29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes
12 PRESSEMITTEILUNG, ULD: „Datenschutzkonformes Cloud Computing ist möglich“, 13.07.2012, https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.htm
13 PRESSEMITTEILUNG, ULD: „Datenschutzkonformes Cloud Computing ist möglich“, 13.07.2012, https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.htm

5. Datensicherheit

Die Datensicherheit beschreibt alle Maßnahmen, die ein Unternehmen vornimmt, um Informationen oder Daten vor dem unrechtmäßigen Zugriff Dritter zu schützen. Beim Cloud-Computing werden mitunter sensible Daten auf Servern des Cloud-Betreibers gespeichert. Die Datensicherheit steht im engen Zusammenhang mit den organisatorischen und technischen Anforderungen des § 9 BDSG.[14] Denn erst durch die ergriffenen Maßnahmen bei der Datensicherheit, wird die Datenverarbeitung sozialverträglich.[15] 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 und seit dem 22.08.2006 zählt zu dieser Gruppe auch der Datenschützer eines Unternehmens oder einer öffentlichen Einrichtung.[16] Daraus ergibt sich für den Datenschützer die Verpflichtung zu prüfen, ob im Unternehmen ausreichende Sicherungsmaßnahmen für den Umgang mit personenbezogenen Daten implementiert sind.

IV. Datenschutzkonformität von Microsoft Dynamics CRM Online

CRM-Systeme können natürlich auch 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 und administriert werden kann. Der Wille zur gesetzeskonformen Administration wird also nachfolgend unterstellt.

1. Das 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 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 zum Sicherheitskonzept hat Microsoft auf einer extra Website beschrieben[17].

14 Vgl. Gola / Schomerus, Bundesdatenschutzgesetz Kommentar, 11. Auflage 2012, § 9 Rn. 1
15 Vgl. Peter Nitsch, Datenschutz und Informationsgesellschaft, ZRP 1995, 361-365
16 Vgl. Thomas Fischer, StGB Kommentar, 57. Auflage 2010, § 203 Rn. 29a
17 Vgl. http://www.microsoft.com/en-us/download/details.aspx?id=40861

2. Berechtigungskonzept

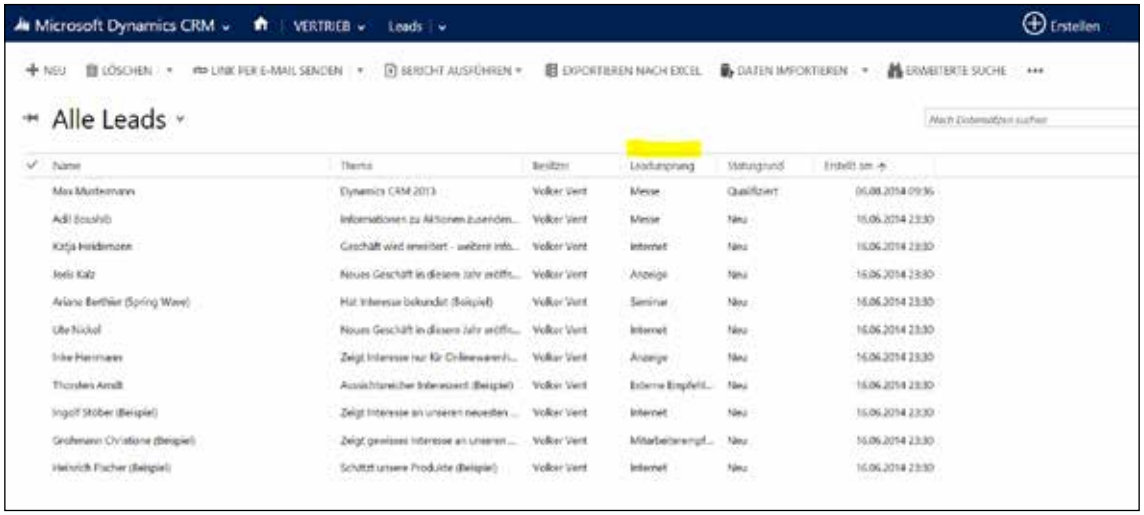
In den Einstellungen von Microsoft Dynamics CRM Online lassen sich zudem bestimmte Berechtigungen festlegen (wie z. B. Lesen, Schreiben und Löschen).

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.

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

Microsoft Dynamics CRM Online bietet 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

In Microsoft Dynamics CRM Online lassen sich Konzepte für die Löschung von Datensätzen anlegen, um nicht mehr benötige Daten aus der Datenbank zu entfernen.

Massenlöschung von Datensätzen

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, finden sich unter „Massenlöschung von Daten“.[18]

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.[19]

6. 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 incl. Microsoft Dynamics CRM Online und Microsoft Azure werden von Microsoft 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 Diskussionen mit den Datenschutzbehörden berichtet. Im Wesentlichen hat Microsoft seit 2011 vier Meilensteine verabschiedet.[20]

18 http://msdn.microsoft.com/en-us/library/gg334418.aspx
19 Vgl. http://www.vaultive.com/solution/vaultive-dynamics/
20 Vgl. Dr. Dirk Bornemann, Alexandra Buchberger, Rechtsabteilung Microsoft Deutschland GmbH, Vortrag in München am 20.02.2014

7. Microsoft Dynamics CRM Online

Wir haben das Microsoft CRM-System positiv auf seine Datenschutztauglichkeit geprüft. In der zweiten Stufe sind die Microsoft-Cloud-Services einer datenschutzrechtlichen Prüfung zu unterziehen, um zu einer abschließenden Feststellung zu gelangen, ob Microsoft Dynamics CRM Online nach deutschem und europäischem Datenschutzrecht rechtskonform genutzt werden kann. Microsoft Dynamics CRM Online hat seine „Heimat" auf der Plattform von Windows Azure und Microsoft Office 365. Beginnen wir dort.

8. Datenschutzrechtliches Wissen zu Office 365 und Azure

Auf einer gesonderten Seite hat sich Microsoft auch intensiv mit dem Thema Datenschutz befasst.[21] 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-Datenschutzgruppe zum Cloud-Computing (05/2012) hin. In ihrer Auffassung betont die EU-Arbeitsgruppe zum Datenschutz, wie wichtig es ist, einen Anbieter von Cloud-Diensten auszuwählen, der seine Datenschutzpraktiken transparent macht und die Schutzwürdigkeit von Kundendaten respektiert. 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.

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.[22]

9. 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 Abs. 1 BDSG handelt. Die rechtlichen 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, die 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.

Die Standorte Niederlande und Irland sind datenschutzrechtlich somit unbedenklich.

21 Vgl. http://office.microsoft.com/de-de/business/office-365-trust-center-fragen-zum-datenschutz-FX104027280.aspx
22 Vgl. http://office.microsoft.com/de-de/business/office-365-trust-center-fragen-zum-datenschutz-FX104027280.aspx

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.

10. 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.

Nach dem Urteil des EUGH in den Rechtssachen C-468/10 und 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 Drittländer kann hier auch noch ergänzend 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.

11. Datensicherheit in der Microsoft-Cloud

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 Aussagen treffen. Es ist jedoch festzuhalten, dass Microsoft auf ihrer Homepage http://www.microsoft.com/de-de/dynamics/crm-trust-center.aspx einige Sicherheitsverfahren für Microsoft Dynamics CRM Online aufzählt. Auf der Seite der Top 10-Listen[23] finden sich die wichtigsten Fragen, die man seinem Anbieter von Cloud-Diensten stellen sollte, wenn man die Auslagerung der IT-Dienste in die Cloud in Betracht zieht. Ferner werden dort auch wichtige Verträge, Zertifizierungen, Standards und Bestimmungen, die die Einhaltung von behördlichen Vorschriften sicherstellen, offeriert.

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 wohl besser ist.

12. Zertifizierungen von Microsoft

Im Zuge der Erreichung der datenschutzrechtlichen Anforderung und Sicherheitsstandards und um Unternehmen eine gewisse Sicherheit zu geben, hat Microsoft verschiedene Zertifizierungen an seinen Produkten durchführen lassen. Die erste Zertifizierung ist die ISO 27001. Aufgrund dieser anerkannten internationalen Norm muss ein Unternehmen geeignete IT-Sicherheitsmaßnahmen implementiert haben, die mit der Organisation des Unternehmens übereinstimmen.

Außerdem hat sich Microsoft verpflichtet, die Grundsätze des Safe Harbor einzuhalten. Safe Harbor ist eine im Jahr 2000 getroffene Vereinbarung zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, die es ermöglichen soll, personenbezogene Daten in die USA zu übermitteln, ohne gegen die Vorschriften der Art. 25 und 26 der Europäischen Datenschutzrichtlinie zu verstoßen. US Unternehmen müssen die folgenden 7 Prinzipien einhalten, damit sie ein geeignetes Datenschutzniveau vorweisen.[24]

1. Informationspflicht: Unternehmen müssen die Betroffenen darüber informieren, welche Daten sie für welche Zwecke erheben und welche Rechte die Betroffenen haben.
2. Wahlmöglichkeit: Unternehmen müssen den Betroffenen ein Widerspruchsrecht einräumen, das die Weitergabe an Dritte oder die Nutzung für andere Zwecke verbietet.
3. Weitergabe: Sollte ein Unternehmen personenbezogene Daten an einen Dritten weitergeben, muss es die Betroffenen darüber informieren und auf die Wahlmöglichkeit nach Nr. 2 aufmerksam machen.
4. Zugangsrecht: Betroffene müssen ihre personenbezogenen Daten einsehen können und ggfs. berichtigen, ergänzen oder löschen können.
5. Sicherheit: Unternehmen müssen geeignete Sicherheitsmaßnahmen treffen.
6. Datenintegrität: Unternehmen haben die Pflicht sicherzustellen, dass die von ihnen erhobenen personenbezogenen Daten korrekt, vollständig und zweckdienlich sind.
7. Durchsetzung: Unternehmen verpflichten sich, Mechanismen einzubauen, sodass Betroffene ihre Beschwerden und Klagen untersuchen lassen können.

Eine weitere Zusatzleistung von Microsoft ist die Einführung der EU-Standardvertragsklauseln der Europäischen Union in ihre Verträge für die Auftragsdatenverarbeitung. Die EU-Standardvertragsklauseln sind als Ergänzung zum Safe Harbor Abkommen zu sehen, da einige Datenschutzaufsichtsbehörden der Meinung sind, dass die Safe Harbor Bestimmungen für Cloud-Dienste nicht ausreichen würden.[25]

23 Vgl. http://office.microsoft.com/de-DE/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy-FX104029824.aspx#shouldAskACloudServiceProvider
24 Vgl. http://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html?nn=5217132
25 Vgl. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF

Abschließend ist noch zu sagen, dass Microsoft durch die EU-Arbeitsgruppe zum Datenschutz Artikel-29-Datenschutzgruppe positiv bewertet worden ist. 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.[26] 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.

13. 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, mit Hilfe von Microsoft Social Listening[27] 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.

14. 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 **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 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.[28] Fragen Sie uns gerne hierzu.

26 Vgl. http://office.microsoft.com/de-de/business/office-365-trust-center-haufig-gestellte-fragen-zu-eu-standardvertragsklauseln-datenschutz-in-der-cloud-FX104033856.aspx
27 Vgl. http://www.microsoft.com/de-de/dynamics/crm-social.aspx?CR_CC=200482732&WT.mc_id=DynGB_de_de_SEM_GOOG&WT.srch=1&DYNCRM-SEARCH
28 Die PRW Consulting GmbH (www.prw-consulting.de) hat sich auf diesen Bereich spezialisiert. Sie arbeitet mit PRW Rechtsanwälte im rechtlichen Bereich eng zusammen

15. Hotline

Wir haben uns intensiv mit der Datenschutzkonformität von Microsoft Dynamics CRM Online 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 89 210977-0 · Stichwort: Microsoft Dynamics CRM Online Hotline. Sie werden dann mit einem kompetenten Kollegen verbunden oder zurückgerufen.

V. Fazit

Wie in den vorherigen Kapiteln gezeigt, gibt es eine ganze Reihe von relevanten Datenschutz-Vorschriften für CRM-Produkte. Die beschriebene Microsoft Dynamics CRM Online-Version erfüllt diese Vorschriften nach deutschem und europäischem Datenschutzrecht. Microsoft hat umfangreiche Maßnahmen im Bereich Datenschutz und Datensicherheit seiner Cloud-Dienste ergriffen. Die Zertifizierungen, ADV-Verträge und technischen Maßnahmen, die vereinbarten SLA sowie die hohe Kompetenz im Bereich IT von Microsoft sind Vorteile, die durch die Verwendung von Microsoft Dynamics CRM Online entstehen.

Wer sicher sein möchte, ob er alle Vorschriften in seinem System rechtskonform umgesetzt hat, sollte sich auditieren lassen. Sprechen Sie uns bei Interesse einfach an.

VI. 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)

Hyperlink-Verzeichnis

Seite 3
http://www.microsoft.com/de-de/dynamics/crm.aspx
http://www.microsoft.com/de-de/dynamics/crm-office-365.aspx
http://www.microsoft.com/de-de/cloud/services/dynamics_crm_online.aspx

Seite 4
http://de.wikipedia.org/wiki/Cloud_Computing
http://www.bitkom.org/files/documents/140203_CC_neue_Geschaeftsmodelle.pdf
http://www.bmwi.de/DE/Themen/Digitale-Welt/Internet-der-Zukunft/cloud-computing.html

Seite 6
http://www.bmwi.de/DE/Mediathek/publikationen,did=523348.html
http://www.bmwi.de/Dateien/BMWi/PDF/Monatsbericht/Auszuege/09-2013-cloud-computing,property=pdf,bereich=bmwi2012,sprache=de
https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-und-datenschutz.html
https://www.datenschutzzentrum.de/presse/20120713-datenschutzkonformes-cloud-computing.htm

Seite 7
http://www.microsoft.com/en-us/download/details.aspx?id=40861

Seite 9
http://msdn.microsoft.com/en-us/library/gg334418.aspx
http://www.vaultive.com/solution/vaultive-dynamics/

Seite 10
http://office.microsoft.com/de-de/business/office-365-trust-center-fragen-zum-datenschutz-FX104027280.aspx

Seite 12
http://office.microsoft.com/de-DE/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy-FX104029824.aspx#shouldAskACloudServiceProvider
http://www.bfdi.bund.de/DE/Europa_International/International/Artikel/SafeHarbor.html?nn=5217132
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF

Seite 13
http://office.microsoft.com/de-de/business/office-365-trust-center-haufig-gestellte-fragen-zu-eu-standardvertragsklauseln-datenschutz-in-der-cloud-FX104033856.aspx
http://www.microsoft.com/de-de/dynamics/crm-social.aspx?CR_CC=200482732&WT.mc_id=DynGB_de_de_SEM_GOOG&WT.srch=1&DYN-CRM-SEARCH

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