Microsoft Cloud Deutschland – Datenschutz und Datensicherheit

Office 365

Microsoft Azure

Raphael Köllner
MVP Office Server & Services

Danke Hamburg!

Danke -> Adobe Engineering GmbH

Raphael Köllner

RaKöllner

Microsoft® Most Valuable Professional

Office Server and Services MVP
Windows Insider MVP

Bechtle IT-Systemhaus Köln

Mitglied der Deutschen Gesellschaft für Recht und Informatik e.V.
WissMit in einer Rechtsanwaltskanzlei
Rechtswissenschaftler im IT & IP Recht

Community Lead: Office 365, Windows Insider Germany

@ra_koellner / raphael.koellner@rakoellner.com
www.rakoellner.de

Agenda

1. Aktuelle Ereignisse
2. Microsoft Cloud Deutschland Basics
3. Das Kontrollzentrum
4. Ein Blick in die Verträge
5. Zusammenfassung
6. Q&A

Aktuelle Ereignisse

Privacy Shield Framework

President Trump

Privacy Shield

The White House
Office of the Press Secretary

For Immediate Release January 25, 2017

Executive Order: Enhancing Public Safety in the Interior of the United States

EXECUTIVE ORDER

- - - - - - -

ENHANCING PUBLIC SAFETY IN THE INTERIOR OF THE UNITED STATES

Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

We are aware of the executive order on public safety. The U.S. Privacy Act has never offered data protection rights to Europeans. The Commission negotiated two additional instruments to ensure that EU citizens' data is duly protected when transferred to the U.S.:

- *The EU-U.S. Privacy Shield, which does not rely on the protections under the U.S. Privacy Act.*
- *The EU-U.S. Umbrella Agreement, which enters into force on 1 February. To finalise this agreement the U.S. Congress adopted a new law last year, the U.S. Judicial Redress Act, which extends the benefits of the U.S. Privacy Act to Europeans and gives them access to U.S. courts.*

We will continue to monitor the implementation of both instruments and are following closely any changes in the U.S. that might have an effect on European's data protection rights.

EU-Kommission

Jan Philipp Albrecht @JanAlbrecht 12h
If this is true @EU_Commission has to immediately suspend #PrivacyShield & sanction the US for breaking EU-US umbrella agreement. #CPDP2017

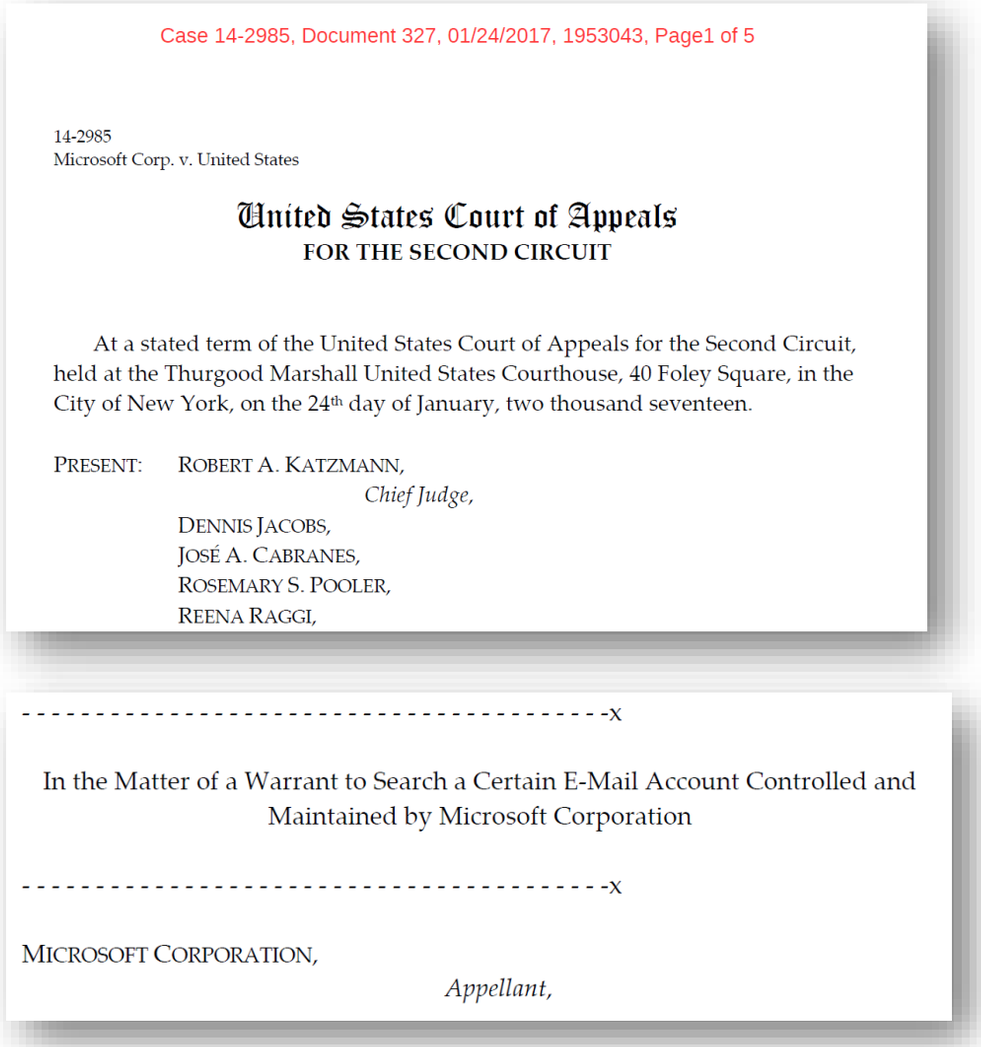
> **Cobun Keegan** @cobun
>
> Trump's Executive Order on "public safety" directs all federal agencies to exclude non-citizens and LPRs from #Privacy Act protections.
>
> Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.

1,1K 824 Übersetzung anzeigen

Privacy Shield Framework

RaKöllner

14-2985: Microsoft Corp. v. United States



Case 14-2985, Document 327, 01/24/2017, 1953043, Page1 of 5

14-2985
Microsoft Corp. v. United States

United States Court of Appeals
FOR THE SECOND CIRCUIT

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 24th day of January, two thousand seventeen.

PRESENT: ROBERT A. KATZMANN,
Chief Judge,
DENNIS JACOBS,
JOSÉ A. CABRANES,
ROSEMARY S. POOLER,
REENA RAGGI,

----------x

In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation

----------x

MICROSOFT CORPORATION,
Appellant,

- Microsoft muss keine Kundendaten, die in einem RZ einer Tochterfirma in Dublin gespeichert werden an die US Behörden weitergeben!
- Letzter Rechtszug: Surpreme Court
- vorheriges Urteil aus Juli 2016 bestätigt
- Stored Communication Act ist nicht anwendbar
- Widerspruch von einem Richter: *„ wesentliche Werkzeuge der Behörden eingeschränkt"*

RaKöllner

Trumps Executive Order

The White House
Office of the Press Secretary

For Immediate Release January 25, 2017

Executive Order: Enhancing Public Safety in the Interior of the United States

EXECUTIVE ORDER

ENHANCING PUBLIC SAFETY IN THE INTERIOR OF THE UNITED STATES

„Sec. 14. Privacy Act. Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."

Gesetzesentwurf zur DSGVO

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680

(Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

A. Problem und Ziel

Am 25. Mai 2018 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU L 119 vom 4.5.2016, S. 1) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der Verordnung (EU) 2016/679 ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten (Erwägungsgrund 10). Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die Verordnung (EU) 2016/679 sieht eine Reihe von Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Verordnung (EU) 2016/679 konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergibt sich gesetzlicher Anpassungsbedarf im nationalen Datenschutzrecht.

Darüber hinaus dient der vorliegende Gesetzentwurf der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU L 119 vom 4.5.2016, S. 89), soweit die der Richtlinie unterfallenden Staaten nach deren Artikel 63 verpflichtet sind, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen. Die Umsetzung der Richtlinie (EU) 2016/680 wird über die im vorliegenden Gesetzentwurf enthaltenen relevanten Regelungen hinaus auch noch gesondert im Fachrecht erfolgen.

Abschnitt 2

Besondere Verarbeitungssituationen

§ 26

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in

RaKöllner

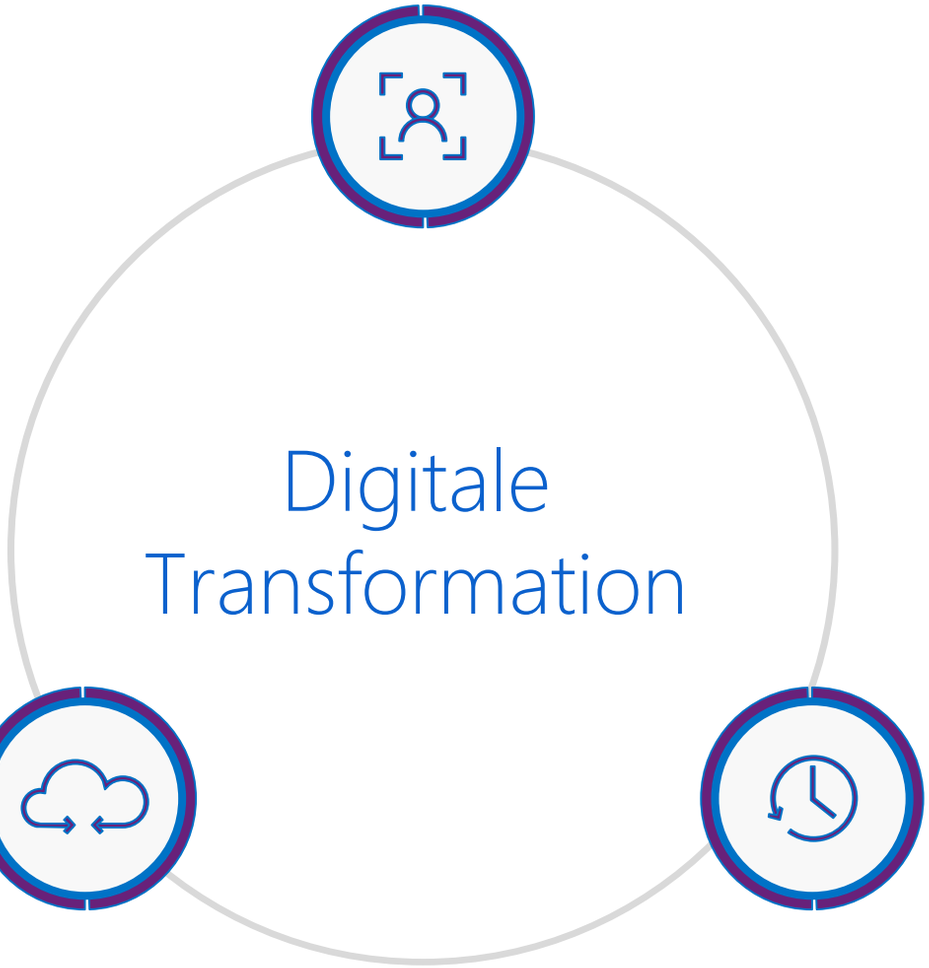
Microsoft Cloud Deutschland

Basics

RaKöllner

Digitale Transformation

Create more
personal computing

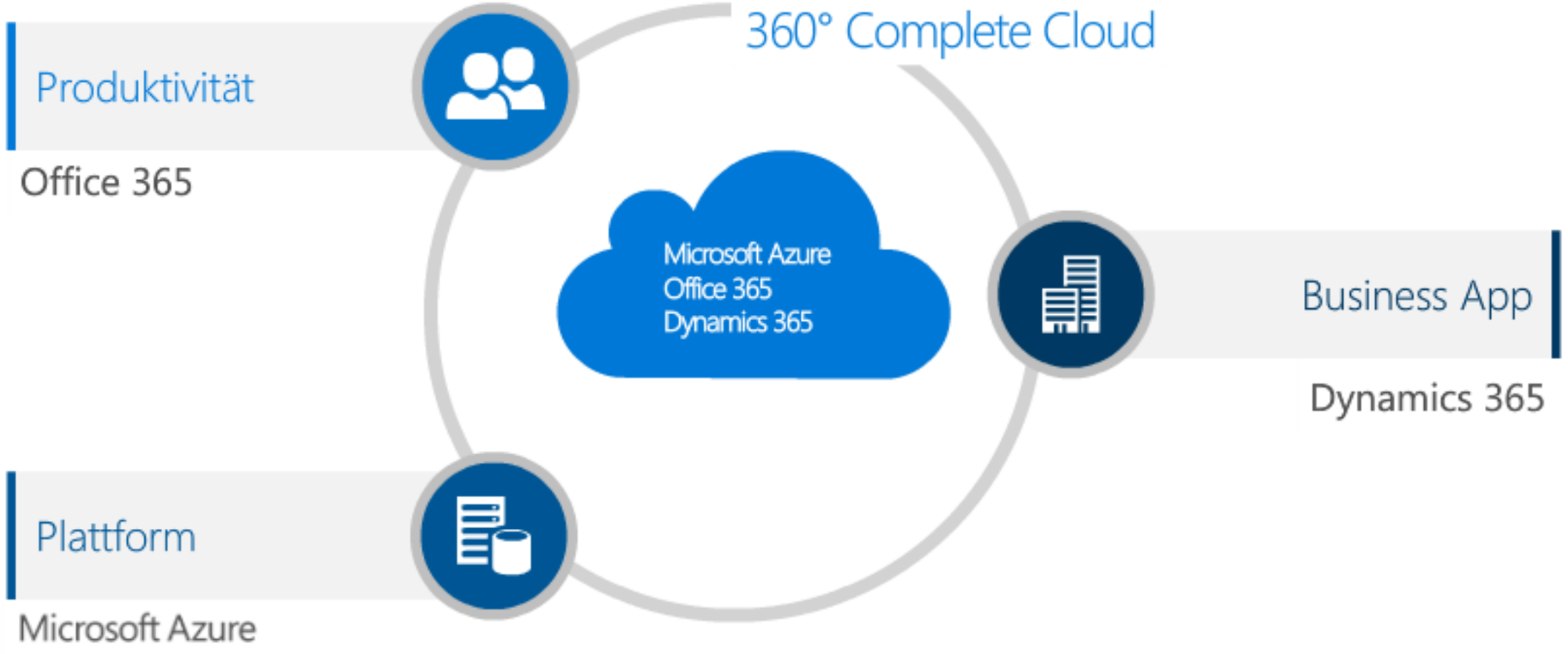


Build the intelligent
and secure cloud
platform

Reinvent productivity
& business processes

RaKöllner

Alles aus einer Cloud bei Microsoft



RaKöllner

Cloud Computing

Voraussetzungen

RaKöllner

Cloud Computing

rechtliche Voraussetzungen

rechtliche
Voraussetzungen

Auszug:

Gesetze, Richtlinien, Verordnungen, DSGVO, Datenschutzbeauftragte, Richtlinien der Industrie, individual rechtliche Verträge

Impliziert

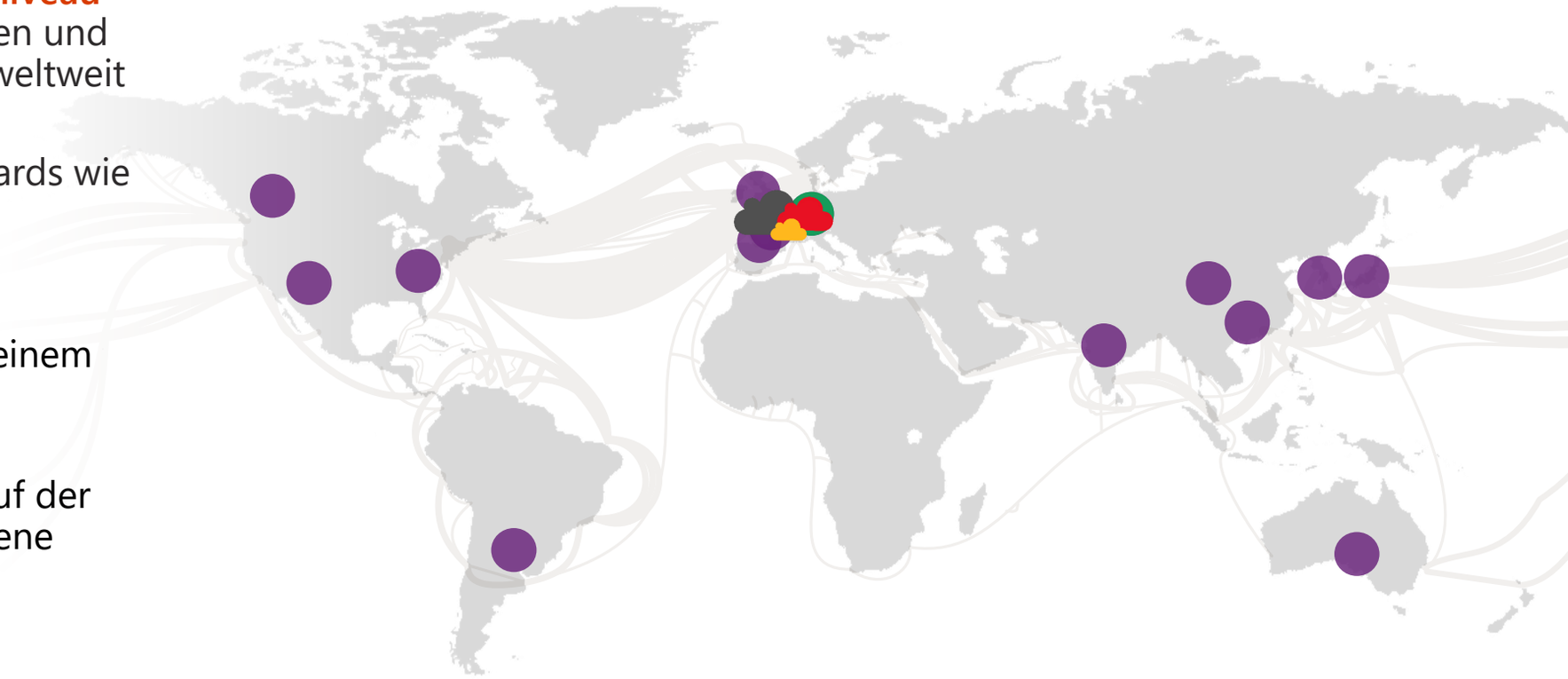
- technisch-organisatorische Maßnahmen
  - Prozesse definiert
  - Auswahl & regelmäßige Kontrolle des Anbieters
  - Benennung von Positionen
  - Berechtigungskonzept

Buchtipp:
Cloud Computing
Prof. Borges

RaKöllner

Globale, hyperskalierende und für Unternehmen konzipierte Infrastruktur,
die in 14 Regionen weltweit Datenstandorte bietet

- ✓ **Zuverlässigkeit auf Unternehmensniveau** dank der mehr als 100 Rechenzentren und einem der drei größten Netzwerke weltweit
- ✓ **Führend bei Compliance** mit Standards wie ISO ISO 27001, FISMA und EU-Standardvertragsklauseln
- ✓ **Transparentes Betriebsmodell** mit einem finanziell abgesichertem 99,9% SLA
- ✓ **Eingebaute Sicherheit** umgesetzt auf der physischen, logischen und Datenebene



RaKöllner

Microsoft Security
Entwicklung in den letzten 14 Tagen

DOD Level 5 – Azure und Office 365

- US Verteidigungsministerium erteilt
- Einzige kommerzielle Cloud

➢ Microsoft Azure Government

➢ Office 365 US Government Defense mit L5-Autorisierung

FedRAMP High
FedRAMP Moderate

DoD Impact Level 2 PA
DoD Impact Level 4 PA
DoD Impact Level 5 PA

ITAR

CJIS
24 states

HIPAA

IRS 1075

RaKöllner

Trusted Application API

- **Meeting Management:**
  - Schedule or manage on-demand meetings like a contact center application.
  - Create on demand meetings to handle customer calls and add customer service representatives to the meeting.
- **Attendant console:**
  - Voice based call answering and routing bots.
- **Value Add solutions:**
  - Business-to-consumer Remote Advisor functionality like Telehealth appointments or Banking consults
  - Recording
  - Compliance
- **Customer care:**
  - Click-to-chat
  - Click-to-call

RaKöllner

GFPR Compliance

- General Data Protection Regulation (GDPR)
  - Umsetzung bis 25.05.2018

Microsoft:

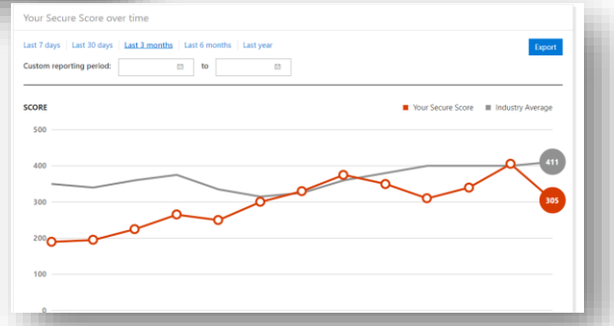
- Sicherheit
- Privatsphäre
- Transparenz
- Complaince

- Datenzugriffs- und Löschregeln
- Risikobewertungsverfahren
- Rolle der Datenschutzbeauftragten für viele Organisationen und Datenverletzungsbenachrichtigungsprozesse

RaKöllner

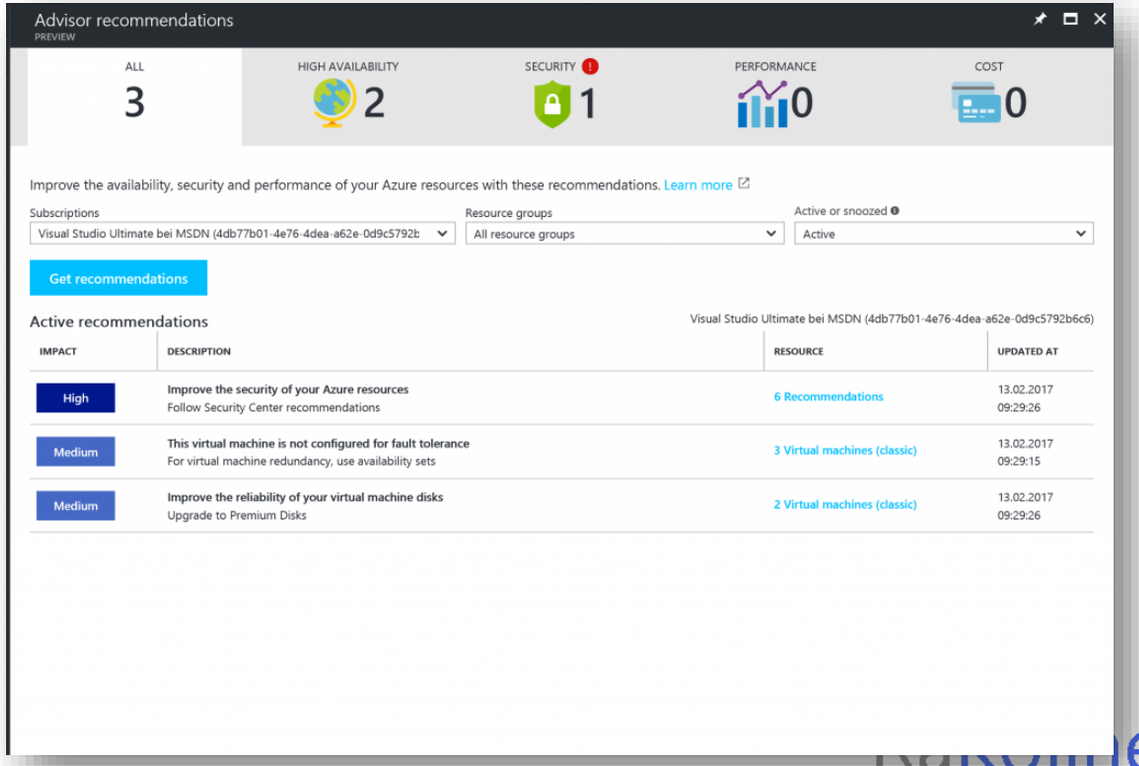
Office 365 Secure Score & Azure Advisor

Office 365 Secure Score



https://securescore.office.com/

Azure Advisor



Warum eine deutsche Cloud?

Compliance

Spezifische lokale deutsche Zertifizierungen eröffnet

Europäische Gesetze

§

Die europäischen Regelungen z.B. zum Datenschutz zählen zu den weltweit strengsten.

Datenschutz

Das BDSG und ab Mitte 2018 die DSGVO regeln den Umgang mit personenbezogenen Daten.

Leistung

Latenz und Geschwindigkeitsvorteile

Standort

Datenverarbeitung in Deutschland

Vertrauen

„Trust is the key“ – Brad Smith

RaKöllner

Zeitstrahl – Microsoft Cloud Deutschland

29.01.2017

Office 365

RaKöllner

Neue Endpunkte

Funktion	URL/Suffix
Portal	https://protal.microsoftazure.de
Office 365	Https://portal.office.de
Storage	Core.cloudapi.de
Websites	Azurewebsites.de
AzureSQL	Database.cloudapi.de
Traffic Manager	Azuretrafficmanager.de
KeyVault	Vaul.microsoftazure.de

Ein deutscher Datentreuhänder kontrolliert den Zugang

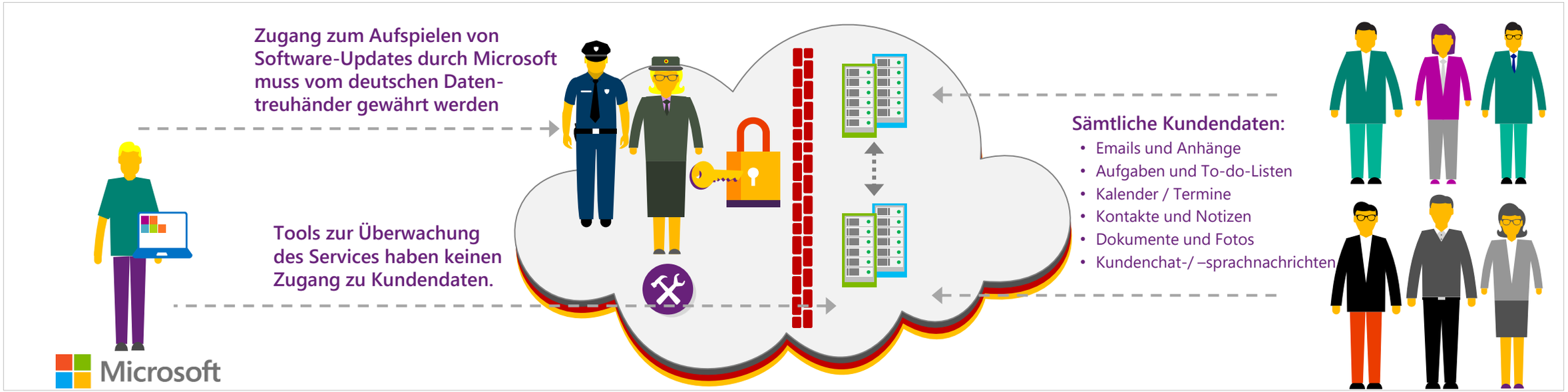
Bei der Microsoft Cloud Deutschland führt ein namhafter deutscher Datentreuhänder selbst alle Handlungen oder Aufgaben durch, für die Zugang zu Kundendaten erforderlich ist, oder überwacht diese.

Mithilfe der Role Based Access Control (RBAC)-Tools wird der Zugang zu Kundendaten kontrolliert.

Ausschließlich der deutsche Datentreuhänder hat die Kontrolle über den Zugang zu Servern mit Kunden-daten.

Mitarbeiter von Microsoft haben keinerlei Rechte, um Zugang auf Kundendaten zu gewähren

Mitarbeiter von Microsoft können sich ohne Über-wachung durch den Daten-treuhänder nicht auf Servern mit Kundendaten einloggen.



RaKöllner

Die Microsoft Cloud Deutschland

ein neu konzipiertes, souveränes Cloud-Modell

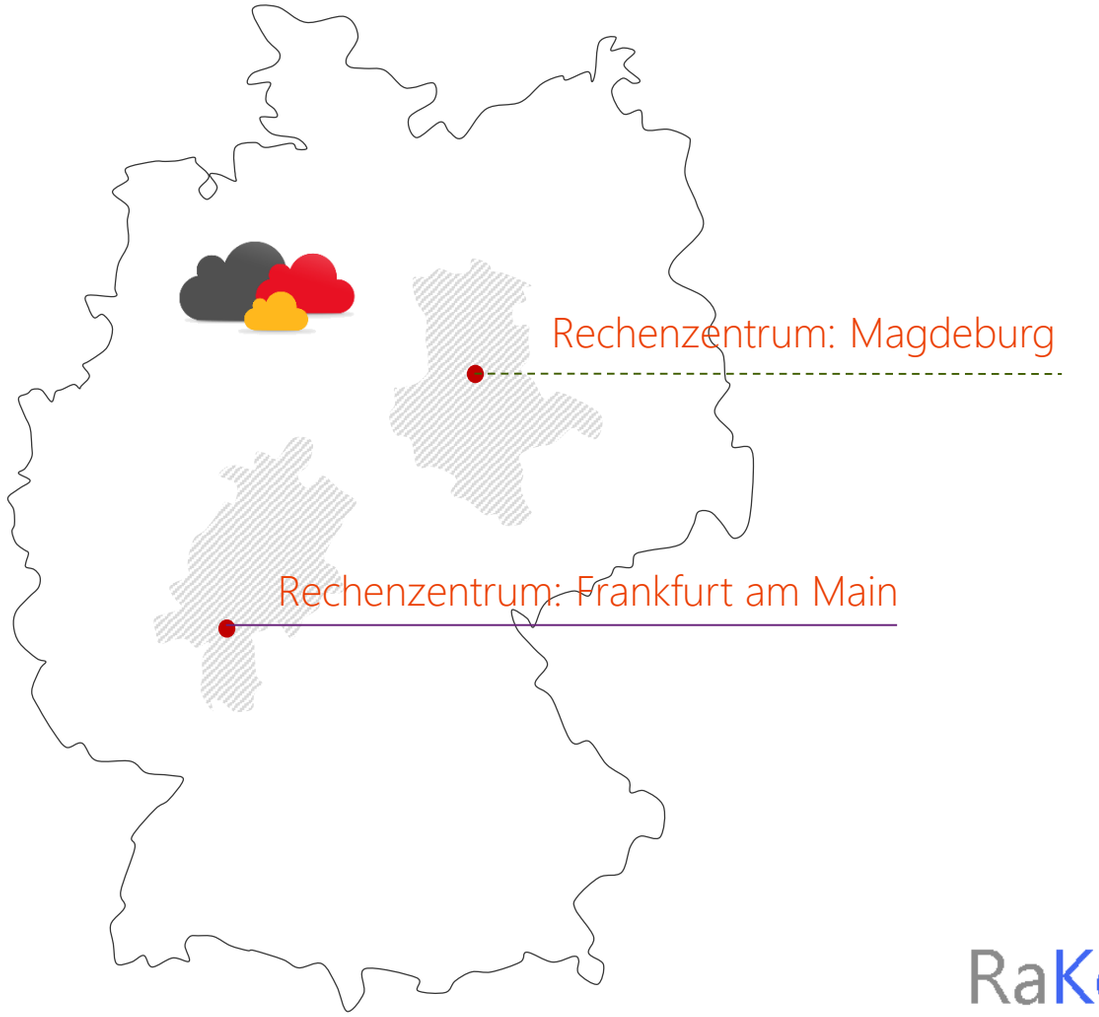
Verfügbarkeiten

Azure — September 2016

Januar 2017

Regionen

German South West	German Central



RaKöllner

Office 365 Deutschland – voraussichtliche Service Verfügbarkeit

Seit 24. Januar 2017

- Office 365 ProPlus*
- Exchange Online
- SharePoint Online
- OneDrive for Business
- Skype for Business
- Office Online
- Office 365 Video
- Project Online
- Visio Online
- Groups
- Exchange Online Protection
- Information Protection (Compliance Center)
- Customer Lockbox
- Advanced eDiscovery
- Advanced Threat Protection
- Power BI

2. Jahreshälfte KJ 2017

- Information Rights Management
- Skype Meeting Broadcast
- Cloud PBX
- EMS
- Usage Reports in Admin Center

In Planung

- Sway
- Planner
- PSTN Calling
- PSTN Conferencing
- MyAnalytics
- Outlook for iOS/Android
- Advanced Security Management
- Microsoft Teams
- Delve Profile
- Service Health API

Die Office 365 E5 Suite und Secure Productive Enterprise (SPE) Suite werden zu einem späteren Zeitpunkt, nach der allgemeinen Verfügbarkeit, angeboten.

Yammer ist in Office 365 Deutschland nicht verfügbar.

*Einige Pläne für Office 365 Deutschland umfassen auch Desktop-Anwendungen, die auf Endbenutzergeräten installiert und ausgeführt werden, wie zum Beispiel Office 2016 und Office 365 ProPlus. Die Desktop-Anwendungen werden nicht ausschließlich in Rechenzentren in Deutschland betrieben und können Endbenutzern auch Zugriff auf Online-Dienste ermöglichen, welche nicht von den deutschen Microsoft Rechenzentren bereitgestellt werden. Desktop-Anwendungen sind keine deutschen Online-Dienste im Sinne Ihres Vertrages mit Microsoft. Die Verpflichtungen zur Datenspeicherung in Deutschland und die Zugangskontrolle durch einen deutschen Datentreuhänder gelten nur für deutsche Online-Dienste.

Sicherheit in der MCD

Built-In-Security

Alle baulichen Maßnahmen zum Schutz Ihrer Daten innerhalb des Rechenzentrums

Werbung

Keine Durchsuchung Ihrer Daten für Werbezwecke

Mehrfachauthentifizierung

Mehrfachauthentifizierung (Multi-Faktor) über App, Telefon bzw. SMS

Verschlüsselung

Backend Verschlüsselung der Daten (Fort-Knox) über mehrere Knoten

Passwortschutz

Erzwingung von starken Kennwörtern und verschlüsselte Verbindungen

Datensicherheit

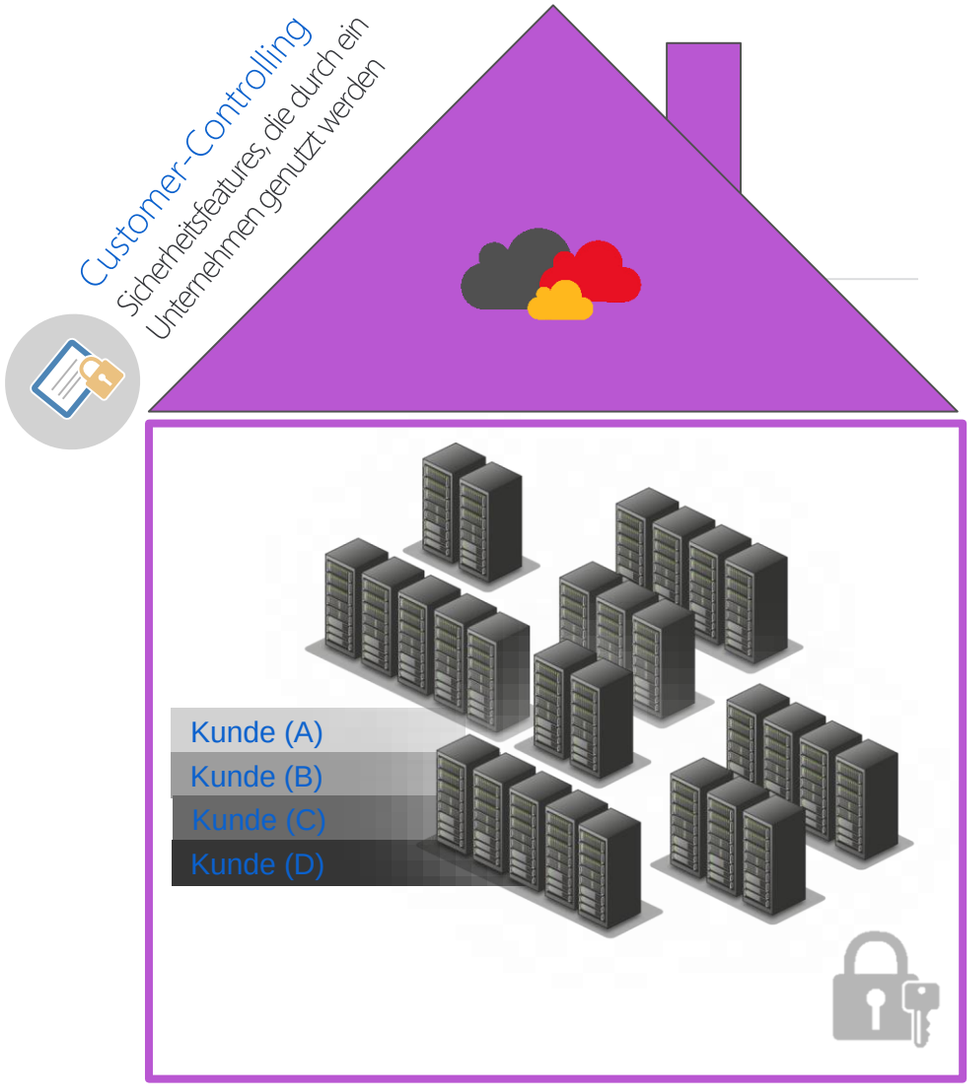
Sicherung ihrer Daten

Datenzugriff

Keinen Zugriff auf Ihre Daten ohne ihr Wissen und nur für autorisierte Mitarbeiter über mehrere Sicherheitsebenen

Security-Features

Einrichten und Konfiguration von ***Encryption Gateway***, ***Data loss prevention*** (DLP) oder ***Rights Management***



# Compliance	# 99,99%	# Bewegungsmelder	# Biometrieleser	# Videoüberwachung
ISO 27001 / EU-Standardvertragsklausen	Verfügbarkeit	Alarmierung bei Sicherheitsverletzungen		

ISO Zertifizierungen DE Cloud

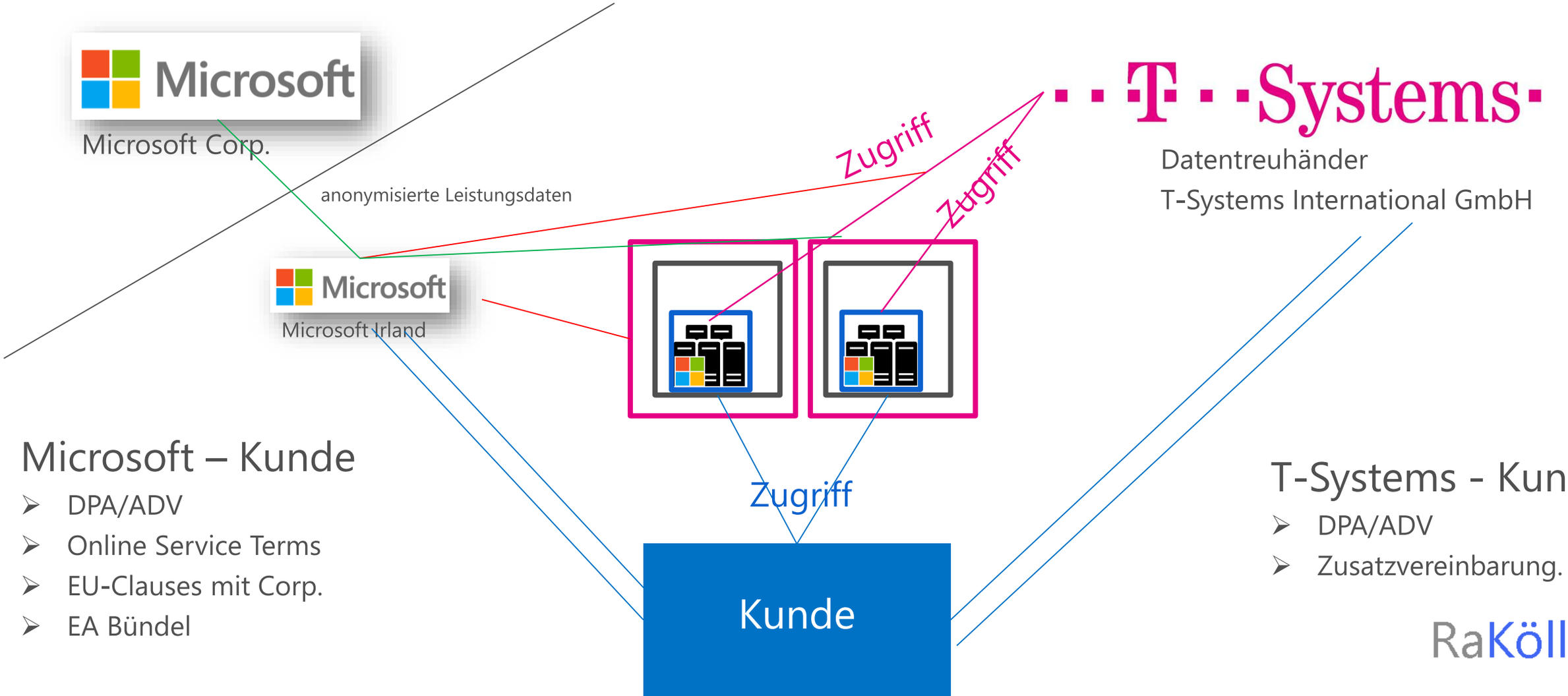
- Azure-Germany-ISO-27001-Certificate-44121161106-Year-2017
- Azure-Germany-ISO-27018-Certificate-44999161106-Year-2017

Download: www.rakoellner.de

RaKöllner

Microsoft Cloud Deutschland

Ein neues Cloudkonzept in der praktischen Umsetzung



Microsoft – Kunde

- DPA/ADV
- Online Service Terms
- EU-Clauses mit Corp.
- EA Bündel

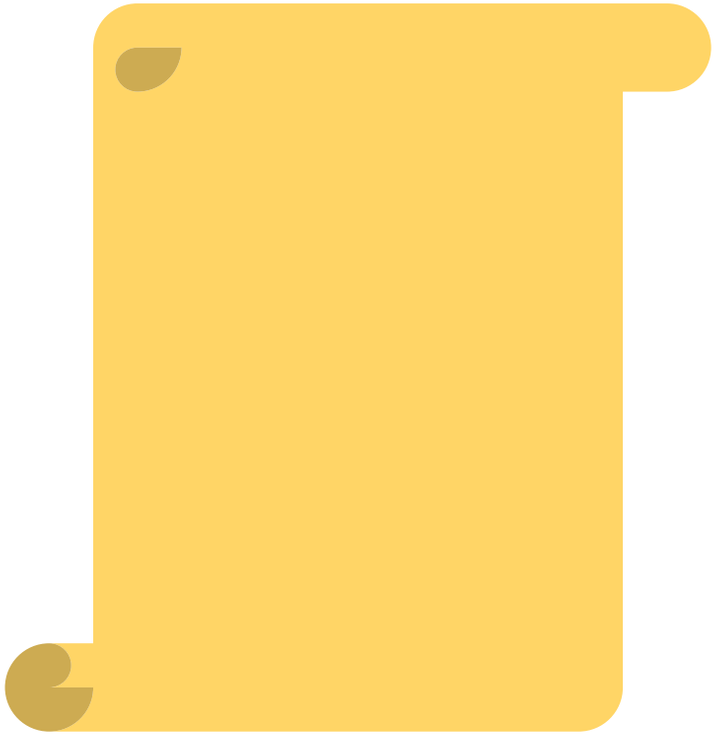
T-Systems - Kunde

- DPA/ADV
- Zusatzvereinbarung.

RaKöllner

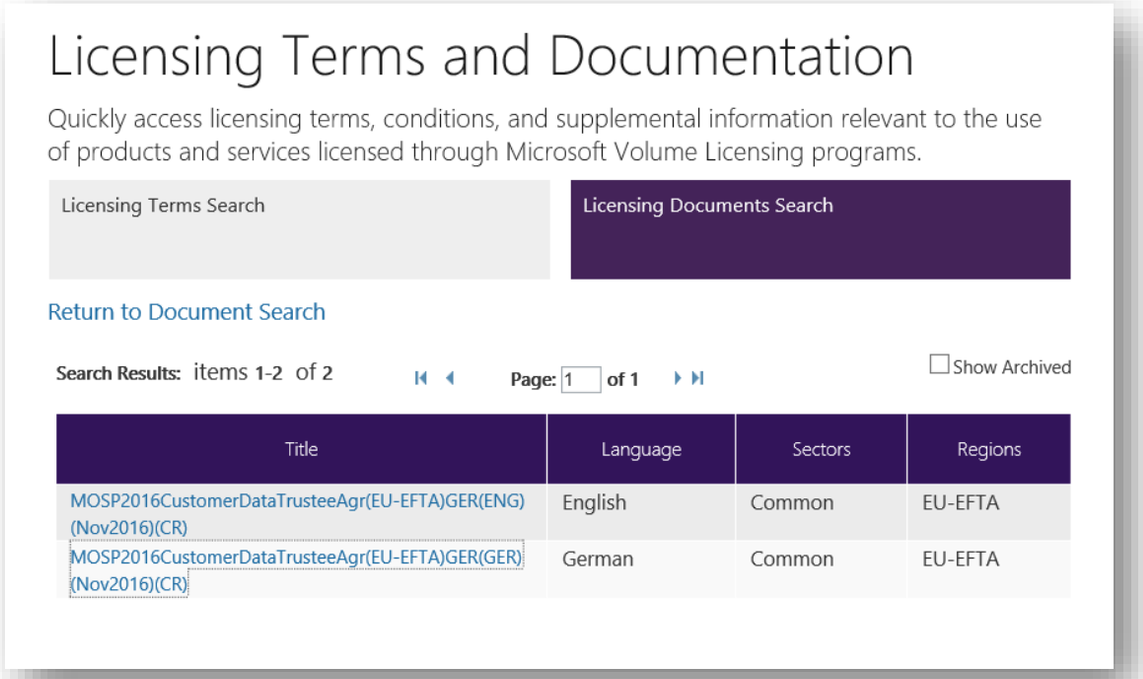
Verträge Microsoft Cloud Deutschland

- Microsoft Online Terms
  (Version: gültig bei Anschluss/ aktuell: Januar 2017)
- Datentreuhänder
- EA (Bündel)
- ggf. Service Termins und weitere



Office

Customer Data Trustee Agreement



Licensing Terms and Documentation

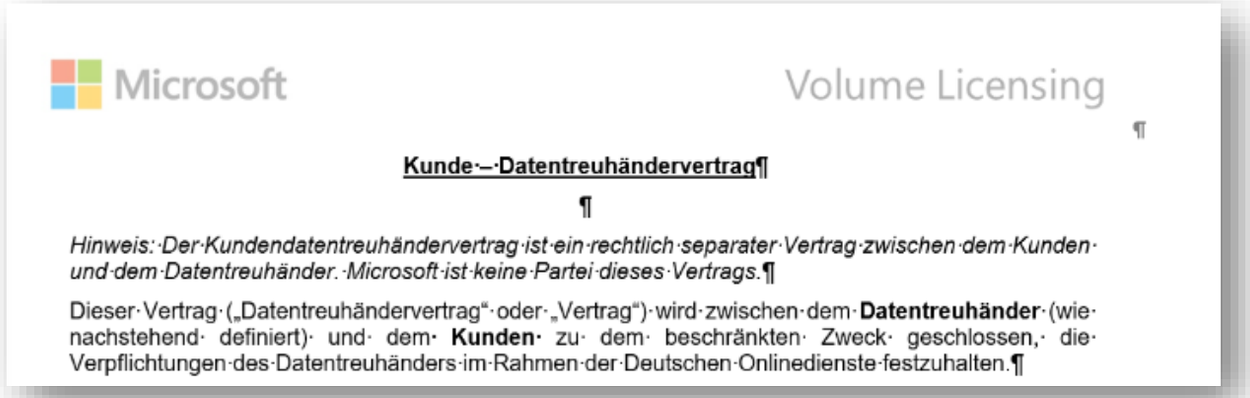
Quickly access licensing terms, conditions, and supplemental information relevant to the use of products and services licensed through Microsoft Volume Licensing programs.

Licensing Terms Search | Licensing Documents Search

Return to Document Search

Search Results: items 1-2 of 2 Page: 1 of 1 Show Archived

Title	Language	Sectors	Regions
MOSP2016CustomerDataTrusteeAgr(EU-EFTA)GER(ENG)(Nov2016)(CR)	English	Common	EU-EFTA
MOSP2016CustomerDataTrusteeAgr(EU-EFTA)GER(GER)(Nov2016)(CR)	German	Common	EU-EFTA



Microsoft Volume Licensing

Kunde·–·Datentreuhändervertrag

Hinweis:·Der·Kundendatentreuhändervertrag·ist·ein·rechtlich·separater·Vertrag·zwischen·dem·Kunden·und·dem·Datentreuhänder.·Microsoft·ist·keine·Partei·dieses·Vertrags.

Dieser·Vertrag·(„Datentreuhändervertrag“·oder·„Vertrag“)·wird·zwischen·dem·**Datentreuhänder**·(wie·nachstehend·definiert)·und·dem·**Kunden**·zu·dem·beschränkten·Zweck·geschlossen,·die·Verpflichtungen·des·Datentreuhänders·im·Rahmen·der·Deutschen·Onlinedienste·festzuhalten.

- Vereinbarung ausschließlich zwischen dem Kunden und dem Datentreuhänder
- In deutscher oder englischer Sprache

http://microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=56

RaKöllner

Inhalt Datentreuhänder Vertrag

Ziel, Umfang und Zweck der Datenverarbeitung durch Datentreuhänder – Bestimmungen für Onlinedienste

Der **Datentreuhänder ist ein Datenverarbeiter** (oder, wenn der Kunde selbst der Datenverarbeiter ist, ein Unterauftragsverarbeiter), der im beschränkten Auftrag bzw. Namen des Kunden handelt und Aufgaben wahrnimmt und überwacht, die den Personalzugriff auf Kundendaten oder auf die Infrastruktur, in der Kundendaten residieren, erfordern. Diese Aufgaben werden von dem Datentreuhänder oder aber direkt von dem Kunden ausgeführt bzw. überwacht.

Vorbehaltlich der in diesem Vertrag definierten Rolle des Treuhänders als Datenverarbeiter ist Microsoft der Datenverarbeiter (oder, wenn der Kunde selbst der Datenverarbeiter ist, der Unterauftragsverarbeiter), der in allen sonstigen Belangen im Auftrag des Kunden handelt, um die deutschen Onlinedienste wie im Microsoft-Vertrag (der die Microsoft-Vereinbarungen zum Servicelevel einschließt) vorgesehen bereitzustellen. Der Klarheit halber wird festgehalten, dass weder der Datentreuhänder ein Unterauftragsverarbeiter von Microsoft ist noch umgekehrt.

Als Datenverarbeiter (bzw. Unterauftragsverarbeiter) handelt der Treuhänder nur auf Weisung des Kunden.

Zugriff auf Kundendaten

Ausschließlich der Datentreuhänder hat die Kontrolle über den Zugang zu den Kundendaten, soweit der Zugang nicht vom Kunden oder Endnutzer des Kunden ausgeht. Microsoft-Personal hat keinen Zugriff auf Kundendaten, außer,

(1) wenn der Datentreuhänder Microsoft Zugriff zu dem beschränkten Zweck gewährt, eine Kundensupportanfrage oder ein Problem mit den Deutschen Onlinediensten zu behandeln, oder wenn Microsoft-Personal den Zugriff zur Durchführung von Wartung oder Verbesserungen an den Deutschen Onlinediensten benötigt. Unter diesen bestimmten Umständen wird der Datentreuhänder den Zugriff nur für die zur Erledigung der Sache notwendige Dauer gewähren. Der Zugriff wird vom Datentreuhänder überwacht und gesperrt, sobald die betreffende Sache erledigt ist.

oder

(1) wenn ein solcher Zugriff Microsoft-Mitarbeitern direkt vom Kunden gewährt wird (z. B. weil der Kunde einen Desktop für einen Microsoft-Supporttechniker freigeben oder dem Microsoft-Supporttechniker eine Datei per E-Mail senden möchte). Der Datentreuhänder steht nicht in der Pflicht, diesen Zugriff zu kontrollieren oder zu überwachen.

Unterauftragsverhältnis

Vertragspartner und Verbundene Unternehmen

Der Datentreuhänder ist nicht berechtigt, einen Teil seiner Kundendatenverarbeitung ohne schriftliche Genehmigung des Kunden unterzuvergeben.

Der Datentreuhänder ist berechtigt, die folgend genannten verbundenen Unternehmen mit bestimmten Aufgaben der Datenverarbeitung zu betrauen, und der Kunde stimmt dem hiermit zu:

Deutsche Telekom Regional Services and Solutions GmbH (RSS)

Adresse: Lübecker Straße 2, 39124 Magdeburg, Deutschland

T-Systems on site services GmbH (OS)

Adresse: Holzhauser Straße 4 – 8, 13509 Berlin, Deutschland

I.T.E.N.O.S. International Telecom Network Operation Services GmbH (ITENOS)

Adresse: Lievelingsweg 125, 53119 Bonn, Deutschland

T-Systems Multimedia Solutions GmbH (MMS)

Adresse: Riesaer Str. 5, 01129 Dresden, Deutschland

Deutsche Telekom Technischer Service GmbH (DTTS)

Adresse: Friedrich-Ebert-Allee 71-77, 53113 Bonn, Deutschland

Telekom Deutschland GmbH

Adresse: Landgrabenweg 151, 53227 Bonn, Deutschland

Deutsche Telekom AG

Adresse: Friedrich-Ebert-Allee 140, 53113 Bonn, Deutschland

Datenschutzbeauftragter

- Kommunikation soll auch an Microsoft gehen (Kopie)

Kontaktperson·für·Privacy·und·Datenschutz¶

Der·Datenschutzbeauftragte·des·Datentreuhänders·ist·unter·der·folgenden·Anschrift·erreichbar:¶

Deutsche·Telekom·AG¶
Konzerndatenschutz·/·Group·Privacy·¶
Konzernbeauftragter·für·den·Datenschutz·/·CPO·¶
Dr.·Claus-Dieter·Ulmer¶
Friedrich-Ebert-Allee·140·¶
D-53113·Bonn,·Deutschland¶

Datenschutz@telekom.de¶

Microsoft Online Terms

Volume Licensing

Bestimmungen für Onlinedienste
1. Januar 2017

Bestimmungen für die Datenverarbeitung

Die Bestimmungen für die Datenverarbeitung (Data Processing Terms oder DPT) beinhalten die Bestimmungen dieses Abschnitts.

Die Bestimmungen für die Datenverarbeitung umfassen auch die „Standardvertragsklauseln" gemäß dem Beschluss der Europäischen Kommission vom 5. Februar 2010 zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern gemäß der EU-Datenschutzrichtlinie. Die Standardvertragsklauseln finden Sie in Anhang 3. Darüber hinaus

- Die Erfüllung des Volumenlizenzvertrages beinhaltet die Erfüllung von Anhang 3, die von Microsoft Corporation gegengezeichnet ist.
- Bilden die Bestimmungen im Volumenlizenzvertrag des Kunden, einschließlich der DPT, einen Datenverarbeitungsvertrag, unter dem Microsoft Auftragsverarbeiter ist.
- Haben die DPT Vorrang vor uneinheitlichen oder widersprüchlichen Bestimmungen im Volumenlizenzvertrag des Kunden und bleiben vollständig für jedes Abonnement wirksam, bis alle zugehörigen Kundendaten von den Microsoft-Systemen in Übereinstimmung mit den DPT gelöscht worden sind.

Der Kunde kann die „Standardvertragsklauseln" oder Bestimmungen für die Datenverarbeitung vollständig ausschließen. Hierfür muss der Kunde folgende Informationen in Form einer schriftlichen Mitteilung (gemäß den Bestimmungen des Volumenlizenzvertrages des Kunden) an Microsoft senden:

- Den vollständigen rechtlichen Namen des Kunden und der Verbundenen Unternehmen, die diese Bestimmungen ausschließen möchten.
- Wenn der Kunde mehrere Volumenlizenzverträge hat, muss mitgeteilt werden, für welchen Volumenlizenzvertrag der Ausschluss gilt.
- Wenn der Kunde die gesamten DPT vollständig ausschließen möchte, muss vom Kunden (oder dem verbundenen Unternehmen) eine Erklärung zum vollständigen Ausschluss der Bestimmungen für die Datenverarbeitung abgegeben werden.
- Wenn der Kunde nur den Standardvertragsklauseln zustimmen möchte, muss vom Kunden (oder dem Verbundenen Unternehmen) eine Erklärung abgegeben werden, das nur den Standardvertragsklauseln zugestimmt wird.

In Ländern, in denen eine behördliche Zulassung für die Verwendung der Standardvertragsklauseln erforderlich ist, kann der Datenexport aus dem Land nicht auf Grundlage der Standardvertragsklauseln gemäß dem Beschluss der Europäischen Kommission 2010/87/EU (vom Februar 2010) legitimiert werden, es sei denn, der Kunde verfügt über die erforderliche behördliche Genehmigung.

In den DPT bezieht sich der Begriff „Onlinedienste" nur auf die in der nachstehenden Tabelle angegebenen Dienste – jegliche Previews sind ausgenommen –, und „Kundendaten" umfassen lediglich jene Kundendaten, die im Rahmen der Verwendung dieser Onlinedienste bereitgestellt werden.

Service und Support Modelle

Das Support-Modell für die Microsoft Cloud Deutschland umfasst in Deutschland basierten technischen Support für Office 365 und Dynamics 365, rund um die Uhr und an sieben Tagen die Woche.

Für Microsoft Azure gilt ein EU-basiertes Supportmitarbeitermodell (während der Geschäftszeiten in Deutschland, außerhalb der deutschen Geschäftszeiten aus der EU).

Die Antwortzeiten, Support-Level und -Pläne für die deutsche Cloud richten sich nach dem öffentlichen Cloud-Modell.

Jeder Support, der Zugang zur Plattform erfordert (d.h. auf die Systeme, die Kundendaten beinhalten) wird vom Datentreuhänder beaufsichtigt.

Support wird auf Deutsch (Hauptsprache) und Englisch (Zweitsprache) zur Verfügung gestellt.

Bei Tools und Prozessen werden Änderungen eingeführt, um den Datenschutzvorgaben/-beschränkungen des deutschen Cloud-Modells Rechnung zu tragen.

Wo zusätzlicher Support benötigt wird, können Support-Mitarbeiter zu weiteren Spezialisten außerhalb von Deutschland eskalieren (z.B. zur Produktgruppe).

Spezifische Support-Angebote und -Preise werden zur Verfügung gestellt, wenn das Markteinführungsdatum der deutschen Cloud-Dienste näher rückt.

RaKöllner

Microsoft kann nur unter zwei Bedingungen auf Kundendaten zugreifen

Der deutsche Datentreuhänder verpflichtet sich gegenüber Kunden vertraglich dazu, Microsoft und seinen Subunternehmern keinen Zugang zu Kundendaten zu gewähren, außer in den folgenden Fällen

Der deutsche Datentreuhänder gewährt vorübergehenden Zugang, um ein Kundensupportproblem zu lösen oder Wartungs- oder Verbesserungsarbeiten durchzuführen.

Unter solchen Umständen überwacht der deutsche Datentreuhänder den Zugang und beendet ihn, sobald das Problem gelöst wurde.

Der Kunde gewährt den Microsoft-Mitarbeitern Zugang.

Unter solchen Umständen ist der Kunde – und nicht der deutsche Datentreuhänder – dafür zuständig, den Zugang zu kontrollieren und zu überwachen.

RaKöllner

Workflow für den Zugang von Microsoft zu Systemen mit Kundendaten

1. Microsoft stellt Zugriffsanfragen nur, wenn es dafür einen speziellen Grund gibt.

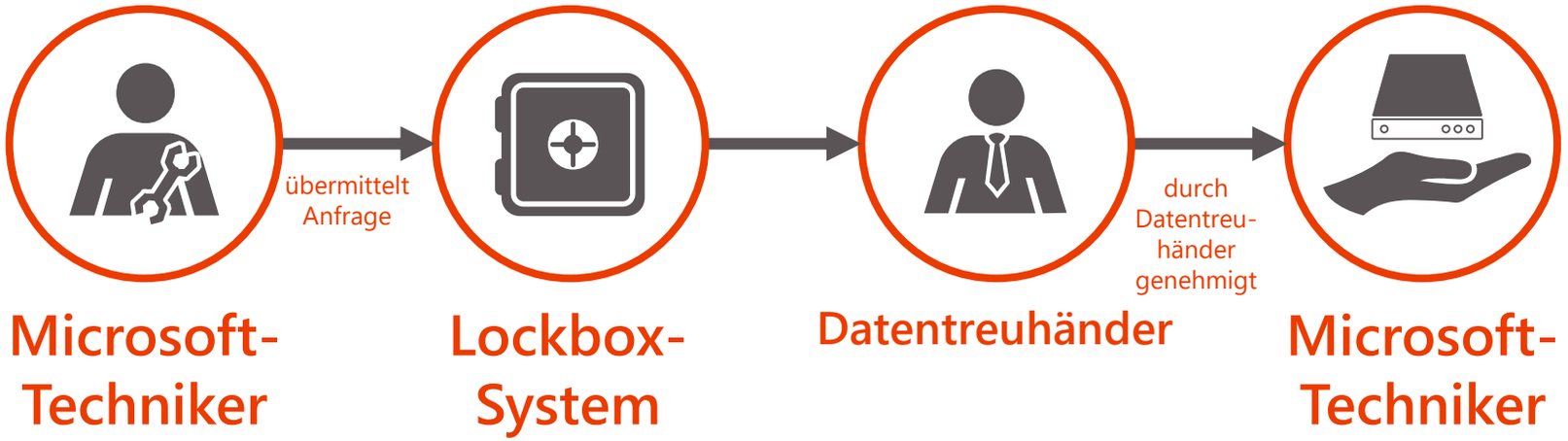
2. Der deutsche Datentreuhänder prüft, ob die Anfrage einem erlaubten Zweck gilt.

3. Der deutsche Datentreuhänder gewährt den Zugang. Die Genehmigung gilt nur für eine spezifische Dienstleistung und für die Zeit, die benötigt wird, um den erlaubten Zweck zu erfüllen. Während der Zugriffsphase werden alle Aktivitäten der Microsoft-Mitarbeiter protokolliert und in Echtzeit vom deutschen Datentreuhänder überwacht. Der Datentreuhänder kann den Zugang jederzeit sofort beenden.

4. Sobald die Aufgabe abschließend bearbeitet worden ist, wird der Zugang entzogen. Falls mehr Zeit benötigt wird, muss eine neue Genehmigung erteilt werden.

RaKöllner

Lockbox in Office 365 Deutschland
Managementsystem für die Zugangskontrolle



Genau definierter Zugang mit geringsten Rechten

Just-in-time-Zugang für begrenzte Dauer

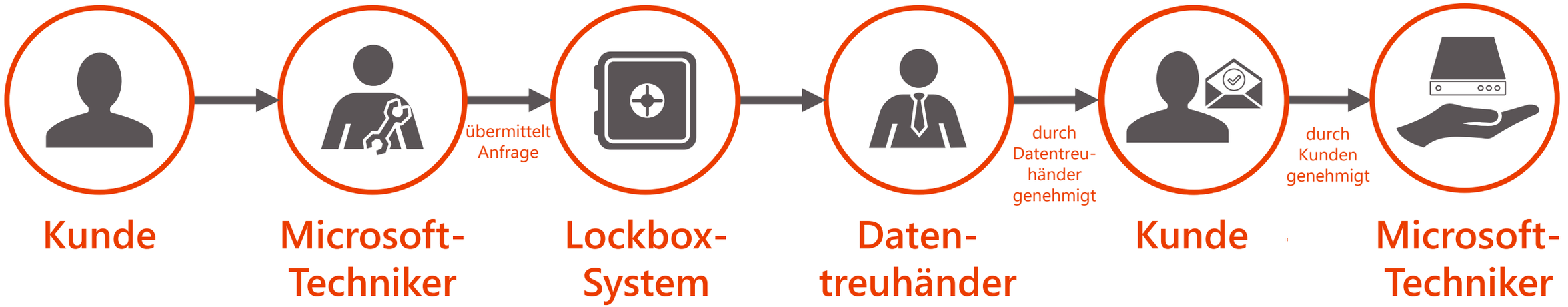
Zugang nur nach Genehmigung durch den Datentreuhänder

Für jeden Zugang sind Überwachungsprotokolle erhältlich.

RaKöllner

Lockbox-System für Kunden in Office 365 Deutschland

Escort-Modell



Kunde kontrolliert die Freigaben für den Zugang von Microsoft-Mitarbeiter

Genau definierter Zugang mit geringsten Rechten

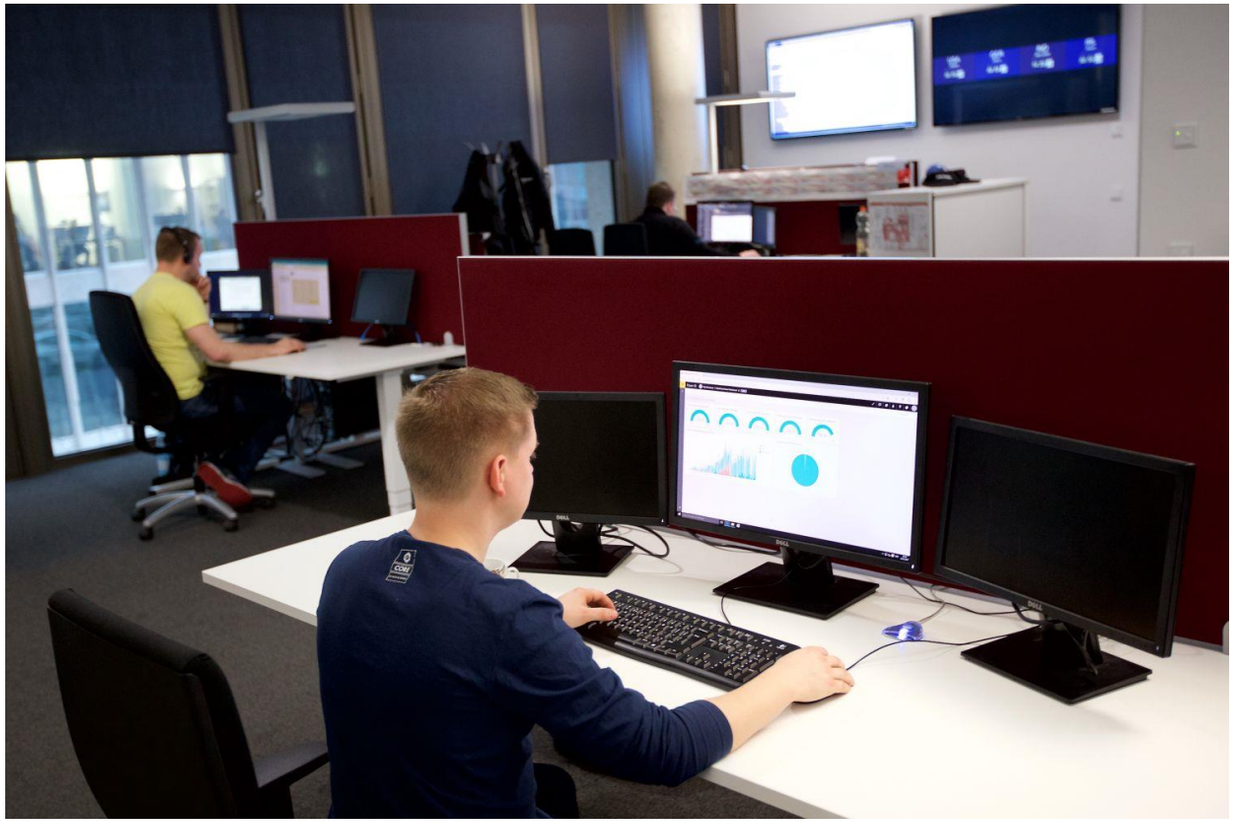
Just-in-time-Zugang für begrenzte Dauer

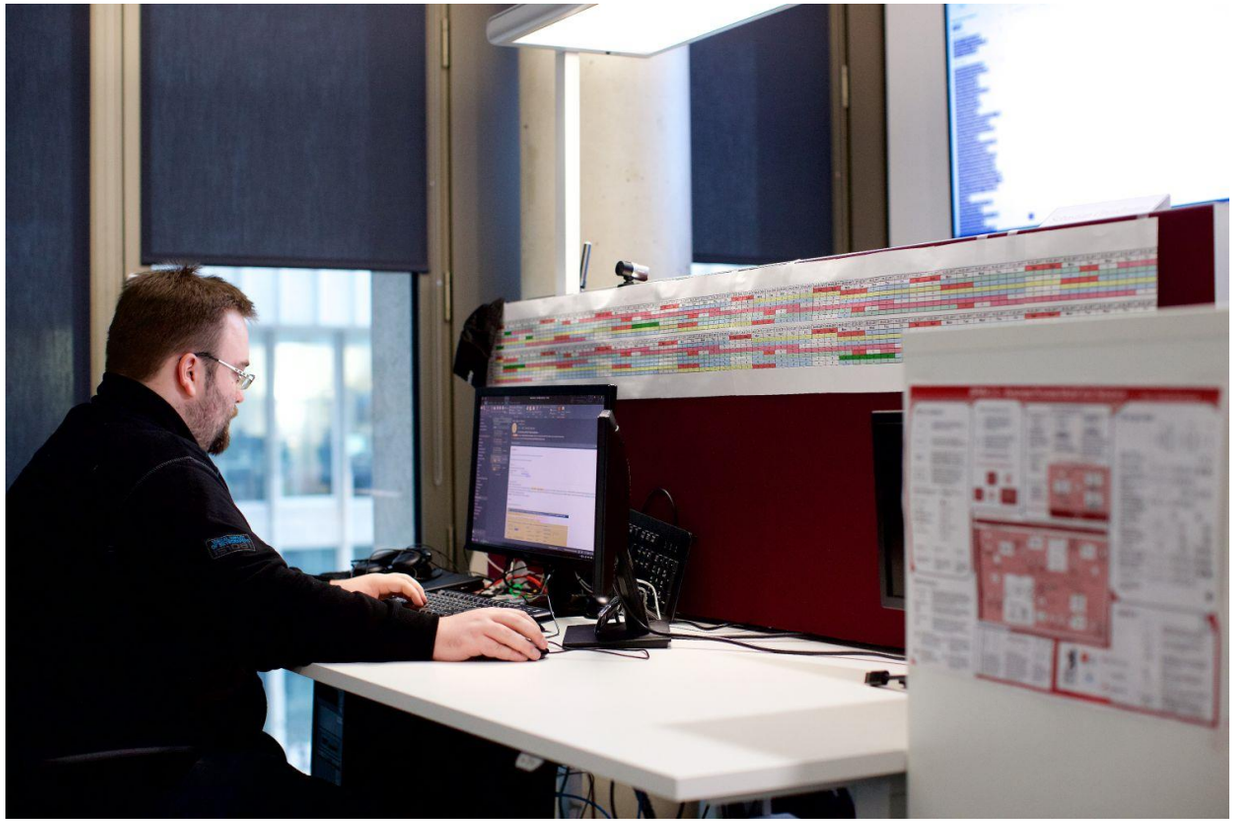
Zugang nur nach Genehmigung durch den Datentreuhänder und den Kunden

Für jeden Zugang sind Überwachungsprotokolle erhältlich.

RaKöllner

MCD – T-Systems Kontrollcenter Berlin





Bildquelle: Dr. Windows

Microsoft Transparenz Center

Quelle:
http://blogs.microsoft.com/eupolicy/transparency-center/

Office 365

Die Microsoft Cloud in Europa

Globale Angebote

Europa*

- Global vernetzte Cloud-Dienste
- Alle Kundendaten werden in Europa gespeichert
- Konform mit EU-Standardvertragsklauseln 2010/87/EU
- Azure Dienste stehen allen Public Cloud Kunden weltweit zur Verfügung; Office 365 und Dynamics 365 Dienste stehen Kunden und Partnern in Europa zur Verfügung.

United Kingdom*

- Global vernetzte Cloud-Dienste
- Alle Kundendaten werden in UK gespeichert
- Konform mit EU-Standard-vertragsklauseln 2010/87/EU
- Azure Dienste stehen allen Public Cloud Kunden weltweit zur Verfügung; Office 365 und Dynamics 365 Dienste stehen Kunden und Partnern in UK zur Verfügung.

Souveränes Cloud-Angebot

Microsoft Cloud Deutschland

- Eine physisch und logisch getrennte Instanz von Microsoft Azure, Office 365 und Dynamics 365
- Ein eigenständiges deutsches, vom öffentlichen Internet getrenntes Datennetzwerk zwischen den Rechenzentren
- Ein deutscher Datentreuhänder hat die Kontrolle über den physischen und logischen Zugang zu Kundendaten und unterliegt deutschem Recht.
- Sämtliche Kundendaten und erforderlichen Systeme befinden sich in deutschen Rechenzentren
- Verfügbar für Kunden und Partner innerhalb der EU/EFTA

*Für Azure kann eine regionale Auswahl getroffen werden, während Office 365 und Dynamics 365 regional vorgegeben sind.

RaKöllner

Raphael Köllner - Kontakt

Raphael Köllner
@ra_koellner
www.rakoellner.de
Raphael.koellner@rakoellner.com

Quelle: Twitter

Vielen Dank

Das nächste Webinar

Blockchain
Patrick Schidler