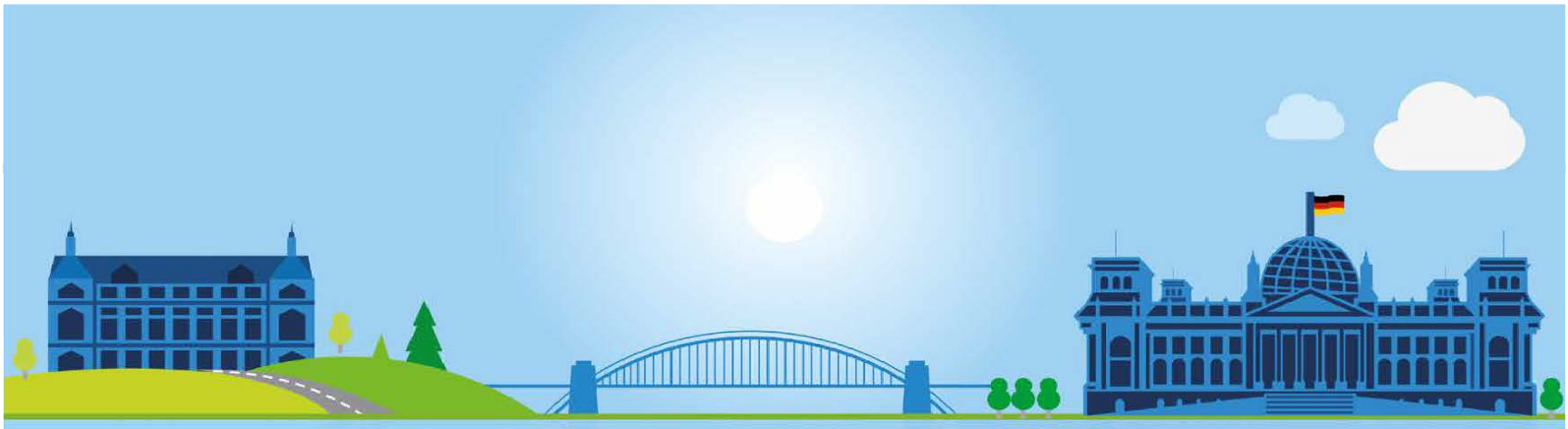


Microsoft Cloud Deutschland

Das Datentreuhändermodell und das Cloud Control Center für die deutsche Microsoft Cloud

Microsoft

Dieses Paper wurde von Microsoft mit Unterstützung der KPMG AG Wirtschaftsprüfungsgesellschaft erstellt, um interessierten Unternehmen einen Überblick über die Besonderheiten der Microsoft Cloud Deutschland zu geben. Das Dokument basiert auf den öffentlich verfügbaren Informationen sowie eigenen Angaben von Microsoft in Bezug auf die deutsche Cloud. Microsoft bietet bezüglich der hier zur Verfügung gestellten Informationen keine ausdrücklichen oder impliziten Garantien.

KPMG

Mit Unterstützung von
T · · Systems ·

HERAUSGEBER
Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München

www.microsoft.de

Informationen zu den Microsoft Datenschutzbestimmungen finden Sie unter http://aka.ms/privacy
Widerspruch der Datennutzung zu postalischen Marketing-zwecken: formlose Mitteilung unter Bezugnahme auf 534261 per Post an Microsoft Deutschland GmbH, Abteilung Rückläufer oder per E-Mail an gerdnc@microsoft.com
Geschäftsführer • Sabine Bendiek (Vorsitzende), Benjamin O. Orndorff, Keith Dolliver
Amtsgericht München, HRB 70438 • USt-IdNr. DE 129415943

Microsoft

Microsoft Cloud Deutschland:

Das Datentreuhändermodell und das Cloud Control Center für die deutsche Microsoft Cloud

Zusammenfassung

Microsoft engagiert sich bei seinen Cloud-basierten Diensten für die Sicherheit und den Schutz vertraulicher Kundendaten. „Die Microsoft Cloud Deutschland ist unsere Antwort auf die wachsende Nachfrage nach Microsoft Cloud-Diensten in Deutschland und Europa. Azure Deutschland unterstützt unsere Kunden dabei, zukunftsfähige Lösungen zu entwickeln und gleichzeitig ihre Compliance-Richtlinien einzuhalten“, sagt Sabine Bendiek, Vorsitzende der Geschäftsführung von Microsoft Deutschland. Dazu erklärt Brad Smith, President und Chief Legal Officer von Microsoft Corporation: „Als weltweit tätiges Unternehmen wissen wir, dass die Menschen in aller Welt der von ihnen genutzten Technologie nur dann vertrauen können, wenn sie die Gewissheit haben, dass ihre persönlichen Daten durch die Gesetze in ihrem eigenen Land geschützt sind.“

Um die Anforderungen von Kunden und Interessenten in der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) zu erfüllen und deren Bedenken zu Sicherheit und Schutz ihrer Online-Daten entgegenzutreten, hat Microsoft als separate Instanz die Microsoft Cloud Deutschland (MCD) entwickelt. Die MCD umfasst führende Cloud-Dienste, die unter besonderen Schutzmaßnahmen ausschließlich in Deutschland gehostet und betrieben werden. Dabei kontrolliert ein lokales Unternehmen den Zutritt, den Zugang und den Zugriff auf Kundendaten, soweit dieser nicht vom Kunden oder seinen Endnutzern selbst durchgeführt oder freigegeben wird. Damit wird gewährleistet, dass der Dateneigentümer die Hoheit und Entscheidungsgewalt über seine Daten behält – insbesondere auch gegenüber Dritten wie in- und ausländischen Aufsichts- und Strafverfolgungsbehörden, denen ausschließlich auf Basis und unter den Voraussetzungen des deutschen Rechts Zugang gewährt wird.

Das vorliegende Dokument besteht aus drei Abschnitten und beginnt im ersten Teil mit einer Einführung in die Microsoft Cloud Deutschland und einer Beschreibung des deutschen Datentreuhänders, eines in Deutschland agierenden deutschen Unternehmens, das den Zugang auf Kundendaten und die damit verbundene Infrastruktur kontrolliert. Zudem wird eine Übersicht zu der Vertragskonstellation bei der Nutzung der deutschen Cloud-Dienste gegeben.

Im zweiten Abschnitt erfahren Sie, auf welche Weise der Betrieb, die Steuerung und Überwachung in der Microsoft Cloud Deutschland gewährleistet ist. Des Weiteren wird der Genehmigungsprozess des deutschen Datentreuhänders für den zeitlich begrenzten, beschränkten und kontrollierten Zugang auf die Kundendaten durch Microsoft oder anderen Drittparteien detailliert dargestellt.

Das Dokument geht im dritten Abschnitt auf Compliance Roadmap für die deutsche Cloud ein. Zuletzt erfolgt eine Aufschlüsselung von verschiedenen Datenkategorien, auf die Microsoft direkt zugreifen kann, und eine Darlegung des Umgangs mit der Offenlegung von Kundendaten.

Überblick über die Microsoft Cloud Deutschland

Microsoft weiß, dass Unternehmenskunden die Vorteile des Cloud Computing nur dann nutzen können, wenn sie bereit sind, ihrem Anbieter für Cloud-Dienste eine ihrer wichtigsten Ressourcen anzuvertrauen: ihre Daten. Die Cloud-Dienste von Microsoft sind global ausgelegt, allerdings ist klar, dass eine Lösung „von der Stange“ nicht immer geeignet ist. Aus diesem Grund hat Microsoft die deutsche Cloud für Unternehmenskunden in der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) eingeführt.

Mithilfe der Microsoft Cloud Deutschland können Kunden ihre Daten jetzt unter Geltung entsprechender deutscher Gesetze und Vorschriften sowie wichtiger internationaler Standards speichern und verwalten. Ermöglicht wird dies für

Kunden in Europa durch das von Microsoft entwickelte Datentreuhändermodell. Zudem wird dadurch sichergestellt, dass ausländische Aufsichtsbehörden nur unter Einhaltung internationaler Rechtshilfeverfahren Zugang auf Kundendaten haben, die in der Microsoft Cloud Deutschland liegen.

Einführung in die deutsche Cloud und das Datentreuhändermodell

Die Microsoft Cloud Deutschland bietet separate Instanzen von Microsoft Azure Deutschland, Office 365 Deutschland und (ab Frühjahr 2017) Dynamics 365 Deutschland an, die von deutschen Rechenzentren zur Verfügung gestellt werden. Die souveränen Dienste heißen Microsoft Azure Deutschland, Office 365 Deutschland und Dynamics 365 Deutschland. Die Rechenzentren sind innerhalb Deutschlands über ein eigenes Netzwerk miteinander verbunden, das von den globalen Cloud-Diensten von Microsoft getrennt ist. Beim Datentreuhändermodell werden alle Daten, die Kunden aus Deutschland bzw. aus dem Gebiet der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) gehören, ausschließlich in Rechenzentren in Deutschland gespeichert.

Ein designiertes deutsches Unternehmen – der deutsche Datentreuhänder – kontrolliert den Zutritt und den Zugang auf Kundendaten sowie die Systeme und Infrastruktur, auf denen die Kundendaten gespeichert sind. Die Kundendaten unterliegen damit dem Anwendungs- und Geltungsbereich des deutschen Rechts.

Beim deutschen Datentreuhänder handelt es sich um ein unabhängiges, deutsches Unternehmen – es hat seinen Sitz in Deutschland, ist dort eingetragen und registriert, und unterliegt deutschem Recht. Für die Microsoft Cloud Deutschland wurde T-Systems International GmbH, eine Tochtergesellschaft der Deutschen Telekom AG, als Datentreuhänder von Microsoft unter Vertrag genommen. Die Besonderheit des Datentreuhändermodells liegt darin, dass Microsoft nur in vertragskonformen Fällen vom deutschen Datentreuhänder oder mit Erlaubnis des Kunden Zugang auf Kundendaten erhält und dabei von der genehmigenden Instanz überwacht wird. Zugleich sind in der Microsoft Cloud Deutschland Sicherheitsmaßnahmen nach dem neuesten Stand der Technik und dem globalen Standard der Rechenzentren von Microsoft integriert.

Die Rechenzentren in Deutschland wurden gemäß den weltweiten gültigen Kriterien für die kommerzielle Microsoft-Cloud ausgewählt. Der Datentreuhänder steuert durch das Cloud Control Center Deutschland die Rechenzentren für Microsoft in der Rechenzentrumsregion Deutschland. Microsoft betreibt aber die souveräne Instanz der deutschen Microsoft Cloud Services. Der Datentreuhänder als Auftragsdatenverarbeiter hat dabei nur die Funktion, die Zugriffs- und Zugangsanfragen auf Kundendaten zu kontrollieren, soweit dieser nicht vom Kunden selbst oder seinen Endnutzern durchgeführt oder freigegeben wird.

Abgrenzung der Microsoft Cloud Deutschland zu anderen Microsoft Cloud-Diensten

Microsoft Kunden können zwischen verschiedenen Cloud-Diensten wählen. Für europäische Kunden hält Microsoft insbesondere zwei Angebote vor: die globale Cloud und die souveräne Cloud in Deutschland. Das globale Cloud-Angebot ermöglicht die Nutzung der global vernetzten Cloud-Dienste wie Azure, Office 365 und Dynamics 365 und wird durch regionale EU-Microsoft-Rechenzentren wie zum Beispiel aus Dublin und Amsterdam für den Raum Europa bereitgestellt. Für beide Cloud-Angebote sind die EU-Standardvertragsklauseln 2010/87/EU für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern Vertragsbestandteil.

Deutsche und europäische (EU/EFTA) Organisationen und Unternehmen aller Größen und Branchen können die Microsoft-Dienste Microsoft Azure Deutschland, Office 365 Deutschland und Dynamics 365 Deutschland über die Microsoft Cloud Deutschland beziehen. Das neue lokale Angebot richtet sich besonders an Organisationen und Unternehmen in datensensiblen Bereichen wie dem öffentlichen, dem Finanz-, Energie- oder dem Gesundheitssektor und ermöglicht die Nutzung der Cloud-Dienste unter Berücksichtigung deutscher Compliance-Anforderungen. Das Besondere an der Microsoft Cloud Deutschland in dieser Hinsicht ist, dass ausschließlich der Datentreuhänder die Kontrolle über den Zugriff auf Kundendaten, soweit der Zugriff nicht vom Kunden oder von Endnutzern des Kunden ausgeht, hat. Der Datentreuhänder operiert unter deutschem Recht.

Microsoft hat nach dem neuesten Stand der Technik und dem globalen Standard der Rechenzentren Sicherheitsmaßnahmen implementiert – einschließlich einer 24-Stunden-Überwachung und –sicherheitdienstes. Zudem sind physische Barrieren, Zäune und umfassende Schutzvorkehrungen eingerichtet.

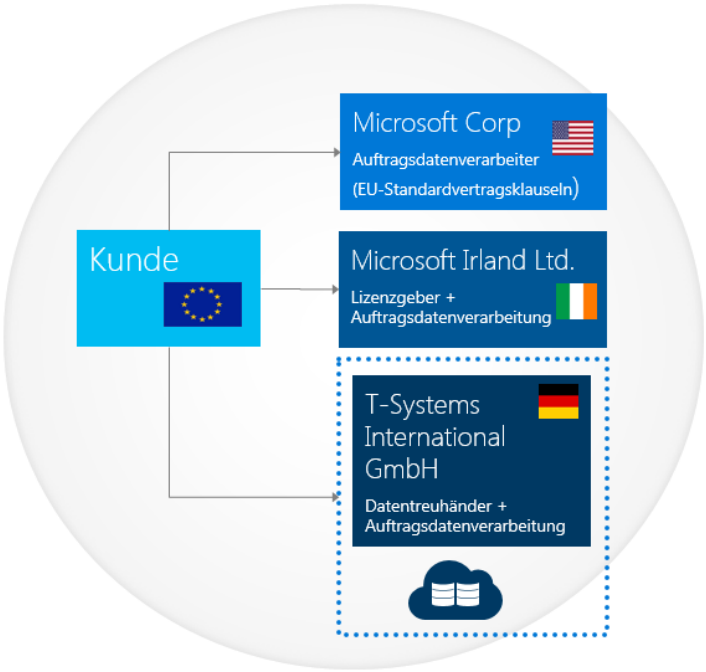
Zusammengefasst ergeben sich folgende besondere Eigenschaften der Microsoft Cloud Deutschland, die in den darauffolgenden Abschnitten näher dargestellt werden:

1. Bei der Microsoft Cloud Deutschland werden die Daten nur in deutschen Rechenzentren gespeichert.
2. Die Rechenzentren befinden sich in Deutschland und der (physische) Zutritt wird von einem namhaften deutschen Datentreuhänder (T-Systems International) kontrolliert.
3. In Abhängigkeit von dem genutzten deutschen Cloud-Dienst findet ein stetiger Datenabgleich zwischen den beiden Rechenzentren in Deutschland statt, um den Geschäftsablauf zu sichern und eine Notfall-Wiederherstellung zu ermöglichen.
4. Der Zugriff auf die Kundendaten steht unter Kontrolle des Datentreuhänders.
5. Der Datentreuhänder operiert unter deutschem Recht.

Vertragskonstellation zur Nutzung der Microsoft Cloud Deutschland

Für die deutsche Cloud bietet Microsoft für alle Kunden in der Europäischen Union (EU) und der Europäischen Freihandelszone (EFTA) eine spezielle Vertragsausgestaltung an, die den Besonderheiten des Datentreuhändermodells gerecht wird. Diese besteht aus drei Vereinbarungen:

1. Abschluss des Volumen-Lizenzvertrags inklusive eines Auftragsdatenverarbeitungsvertrags sowie eine Zusatzvereinbarung für die Microsoft Cloud Deutschland mit Microsoft Ireland Operations,
2. Abschluss der EU-Standardvertragsklauseln mit Microsoft Corporation als Auftragsdatenverarbeiter sowie
3. Abschluss eines Auftragsdatenverarbeitungsvertrages mit dem Datentreuhänder T-Systems International GmbH, eine Tochtergesellschaft der Deutschen Telekom, sogenannter Datentreuhändervertrag.



Microsoft bleibt gegenüber dem Kunden für SLAs (Service-Level-Vereinbarungen) verantwortlich. Als Bestandteil des Abschlusses der Kundenverträge schließt der Datentreuhänder einen Auftragsdatenverarbeitungsvertrag mit dem Kunden ab, der den Datentreuhänder vertraglich dazu verpflichtet, seine Rolle ausschließlich in Übereinstimmung mit den vereinbarten Vertragsbedingungen auszuüben. In diesem Vertragszusatz ist u. a. geregelt, dass der Datentreuhänder ausschließlich dann Daten an Dritte herausgibt, wenn der Kunde es erlaubt oder deutsches Recht es erfordert.

Auch Microsoft schließt einen Auftragsdatenverarbeitungsvertrag inklusive der EU-Standardvertragsklauseln mit dem Kunden ab. Obwohl Kundendaten ausschließlich in Deutschland gespeichert werden und der Datentreuhänder für alle Aufgaben mit Bezug zu Kundendaten zuständig ist, gibt es Umstände, unter denen Unterstützung von Microsoft benötigt wird, z.B. um eine Störung der Dienste zu lösen oder beim Kundensupport Hilfe zu leisten.

In solchen Fällen gewährt der Datentreuhänder Microsoft Remote-Zugang zu den entsprechenden Systeme, jedoch nur für begrenzte Zeit und unter der Aufsicht des Datentreuhänders. Ein solcher Zugang erstreckt sich üblicherweise auf die zugrundeliegenden Systeme, nicht auf die Kundendaten selbst. Da die Möglichkeit des Remote-Zugriffs auf Kundendaten (einschließlich personenbezogener Daten) besteht, könnte die Remote-Zugriffssitzung nach europäischem Recht als „Datenübertragung" betrachtet werden, obwohl keine Daten außerhalb Deutschlands gespeichert werden. Die EU-Standardvertragsklauseln bieten ein rechtliches Instrument, um solche „Datenübertragungen" im Einklang mit europäischem Datenschutzrecht zu gestalten. Dies gilt auch, wenn der Kunde seine Kundendaten Microsoft unmittelbar mitteilt, z.B. während einer Kundensupport-Interaktion.

Microsoft verpflichtet sich vertraglich dazu, dass der Datentreuhänder (und ggf. auch künftige) die folgenden Vorgaben erfüllt:

1. Er muss alle Verpflichtungen einhalten, die im Datentreuhändervertrag genannt sind;
2. Er muss in Übereinstimmung mit deutschem Recht handeln;
3. Es muss sich um eine deutsche Gesellschaft mit Sitz in Deutschland handeln, bzw. um eine solche Gesellschaft, an der eine deutsche Gesellschaft mit Sitz in Deutschland eine beherrschende Beteiligung hält; und
4. Er muss finanziell von Microsoft unabhängig sein. Falls ein Kunde Einwände gegen einen etwaigen neuen Datentreuhänder erhebt, steht es ihm frei, die Dienste sanktionslos zu kündigen

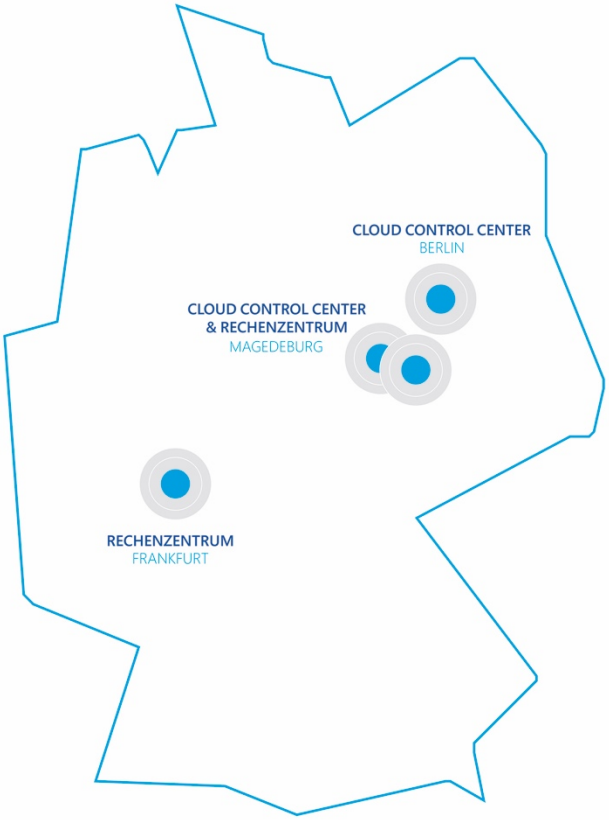
Microsoft orientiert sich bei den Cloud-Angeboten weltweit an den Bedürfnissen ihrer Kunden und bietet Leistungen zu wettbewerbsfähigen Preisen an. Im Preis für die neuen Dienste spiegelt sich der Mehraufwand für die besondere Architektur dieser souveränen Cloud-Lösung wider. Dabei verwaltet Microsoft alle Aspekte des Betriebs sowie die Bereitstellung der Microsoft-Cloud-Deutschland-Dienste, die keinen Zugang zu Kundendaten erfordern.

Das Datentreuhändermodell und die Rollenverteilung in der deutschen Cloud

Das Datentreuhändermodell erfüllt das Ziel, Rechenzentrumsstandorte nur im jeweiligen Land bereitzustellen, sodass ausländische Behörden oder Organisationen nachweislich keine Kontrolle darüber haben. Um die für das Datentreuhändermodell erforderliche physische und logische Trennung der Infrastruktur zu erreichen, hat Microsoft eine separate Instanz für die Online-Dienste Microsoft Azure Deutschland, Office 365 Deutschland und Dynamics 365 Deutschland implementiert, die ausschließlich in Deutschland gehostet und betrieben werden.

Betrieb, Steuerung und Überwachung in der Microsoft Cloud Deutschland

Cloud Control Center Deutschland
Deutschlandkarte

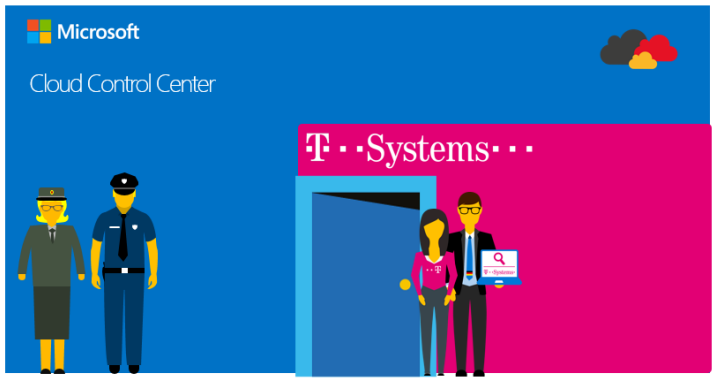


Der Datentreuhänder hat bei der Microsoft Cloud Deutschland die Funktion, die Zugangsanfrage auf Kundendaten zu kontrollieren. Dabei betreibt Microsoft die souveräne Instanz der deutschen Microsoft Cloud-Dienste. Die Rechenzentren in Deutschland befinden sich in zwei deutschen Regionen, Frankfurt am Main und Magdeburg, womit sichergestellt wird, dass Kundendaten in Deutschland verbleiben.

Diese beiden Rechenzentren befinden sich aus Gründen der Ausfallsicherheit in unterschiedlichen Teilen Deutschlands und sind über ein privates, vom öffentlichen Internet getrenntes Datennetzwerk miteinander verbunden. Um die Ausfallsicherheit (Business Continuity) und die Wiederherstellung von Daten und Diensten (Disaster Recovery) in Notfällen zu ermöglichen, findet ein kontinuierlicher Datenabgleich zwischen den Rechenzentren statt. Die technischen Mitarbeiter, die den Dienst verwalten, arbeiten in Cloud Control Centren in Magdeburg und Berlin.

Die Rechenzentren der Microsoft Cloud Deutschland werden durch zwei Cloud Control Center an den Standorten Berlin und Magdeburg gesteuert, sodass durch diesen redundanten Aufbau der Ausfall eines Control Centers problemlos abgefangen werden kann. An beiden Standorten werden Zugangsanfragen von Microsoft-Mitarbeitern von der T-Systems International GmbH als Datentreuhänder geprüft, nur bei Vorliegen der vertraglichen und rechtlichen Voraussetzungen gewährt und gewährte Zugänge dann überwacht.

Jegliche von Microsoft durchgeführte Betriebsaktivitäten, durch die potenziell auf Kundendaten zugegriffen werden könnte – wie z.B. Störungsmanagement und Softwareaktualisierungen – unterliegen technischen Kontrollen, die eine Genehmigung der Zugangsanfrage durch den Datentreuhänder oder den Kunden erfordern. Bei Autorisierung durch den Datentreuhänder werden diese Zugänge ebenfalls beaufsichtigt. Die Mitarbeiter des Datentreuhänders und von Microsoft sind an die strengen Anforderungen von Microsoft bezüglich des Betriebs von Rechenzentren gebunden. Die Microsoft Deutschland GmbH ist ein durch das Bundesministerium für Wirtschaft und Energie betreutes Unternehmen im Programm „Geheimschutz in der Wirtschaft".



Die Cloud Control Center Deutschland (CCCD) stehen unter der Kontrolle des Datentreuhänders. Der Datentreuhänder hat in Berlin einen klar festgelegten, separierten Bereich im CCCD, wohingegen Microsoft keinen festen Arbeitsplatz im CCCD und insbesondere keinen Zugang zum Datentreuhänderbereich hat. Microsoft-Mitarbeiter, die sogenannten „Microsoft Verbindungsmanager", sind nur in Ausnahmefällen vor Ort.

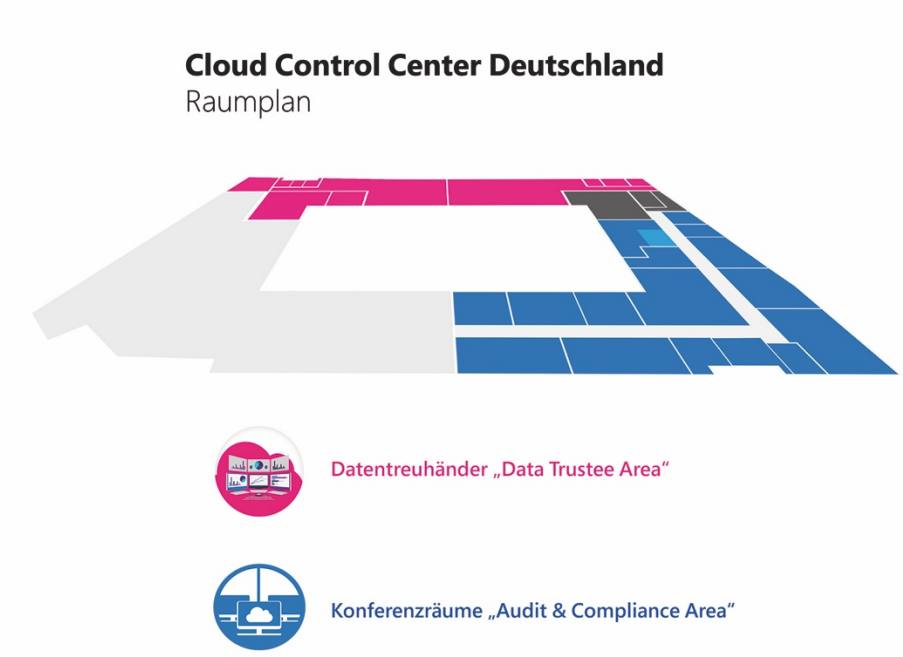
Das Cloud Control Center Deutschland in Berlin besteht aus den im Folgenden beschriebenen drei separaten Bereichen:

(1) **Sicherheits-Bereich:** Hier befinden sich die Sicherheitskräfte, die den physischen Zutritt zum Cloud Control Center überprüfen und nur in rechtskonformen Fällen Zutritt gewähren und die Begleitung dieser Personen durch den Datentreuhänder initiieren.

(2) **Datentreuhänder-Bereich:** In dem T-Systems Cloud Control Center Deutschland-Bereich befinden sich die Mitarbeiter des Datentreuhänders, die ihre regulären Betriebs-, Steuer- und Escort-Aktivitäten durchführen. Microsoft-Mitarbeiter haben keinen Zutritt zu diesem Bereich, außer, es liegt eine vertragskonforme Anfrage bzw. ein Bedarf vor. In diesem Fall werden sie durch einen Mitarbeiter des Datentreuhänders begleitet.

(3) **Konferenzbereich:** Kunden und Microsoft-Mitarbeiter können diese Räume im Rahmen von notwendigen Besprechungen vor Ort nutzen (zum Beispiel für IT-Audit-Projekte).

Die folgende Grafik stellt einen Lageplan für das Cloud Control Center Deutschland in Berlin dar:



Die Mitarbeiter des Datentreuhänders, die mit dem Betrieb, der Steuerung und Überwachung der Microsoft Cloud Deutschland involviert sind, bilden eine Abteilung der Datentreuhänder-Organisation (in diesem Fall T-Systems) und sind logisch und physisch von der restlichen T-Systems-Organisation getrennt, um einen Informationsaustausch zu unterbinden und Interessenkonflikte zu vermeiden. Selbstverständlich ist vertraglich festgelegt, dass T-Systems keine treuhänderisch verwalteten Daten (Kundendaten oder Daten über den Kunden) für andere Zwecke nutzen darf.

Microsoft betreibt gegenwärtig über 100 Rechenzentren, die teilweise in deren Eigentum stehen und teilweise von Microsoft gemietet werden. Aus Sicherheitsgründen gibt Microsoft nicht bekannt, welche Rechenzentren bzw. Einrichtungen gemietet werden und welche Microsofts Eigentum sind. Microsofts langjährige Erfahrung ermöglicht es, branchenführende Geschäftsansätze, Datenschutzrichtlinien, Compliance-Programme und Sicherheitsmaßnahmen zu entwickeln, die in der Cloud-Rechenumgebung eingesetzt werden.

Kunden haben die Möglichkeit, das Cloud Control Center Deutschland zu besuchen, wenn sie den entsprechenden Zutrittsprozess befolgen und die erforderlichen Unterlagen vorzeigen. Dazu müssen sie sich bei dem Datentreuhänder anmelden und eine Zutrittsgenehmigung für das CCCD erfragen. Zudem müssen sie ein gültiges Ausweisdokument vorweisen und die Cloud Control Center Policies bzw. die Hausregeln zur Kenntnis nehmen und unterschreiben. Der Datentreuhänder prüft die Anfrage und erteilt bei positivem Ergebnis das Zugangsrecht und eskortiert den Kunden.

Bei Nutzung der Microsoft Cloud Deutschland steht ein spezifisches Service- und Support-Modell durch Microsoft zur Verfügung. Das Supportmodell umfasst den in Deutschland basierten technischen Support für Office 365 Deutschland und Dynamics 365 Deutschland, welches rund um die Uhr und an sieben Tagen in der Woche zur Verfügung steht. Für Microsoft Azure Deutschland gilt ein EU-basiertes Supportmitarbeitermodell. Das bedeutet, dass während der Geschäftszeiten der Support aus Deutschland und außerhalb der deutschen Geschäftszeiten aus der EU kommt.

Darüber hinaus zeichnet sich der Support wie im Folgenden beschrieben aus:

(1) Die Antwortzeiten, Support-Level und -pläne richten sich für die Microsoft Cloud Deutschland nach denen der globalen Cloud Modelle.

(2) Jede Supportanfrage, welche den Zugang zur Plattform erfordert, muss durch einen Mitarbeiter des Datentreuhänders genehmigt, überwacht und protokolliert werden.

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

(4) Die bisher verwendeten Tools und Prozesse im Support-Modell der öffentlichen Cloud Dienste wurden so angepasst, dass sie den Anforderungen des Datentreuhändermodells für die Microsoft Cloud Deutschland entsprechen.

(5) Wenn nötig, ist es möglich, auch Mitarbeiter außerhalb Deutschlands zur Lösung von speziellen Herausforderungen der Kunden mit einzubeziehen.

Aufgaben und Verantwortlichkeiten von Microsoft und dem Datentreuhänder

Microsoft verwaltet alle Aspekte des Betriebs und der Bereitstellung der Microsoft-Cloud-Deutschland-Dienste, die keinen Zugang zu Kundendaten erfordern. Zudem wird sichergestellt, dass keine Verbindung mit anderen Microsoft Public Cloud Diensten vorhanden ist. Der deutsche Datentreuhänder führt hingegen jegliche Vorgänge oder Aufgaben durch, die den logischen oder physischen Zugang zu Kundendaten oder der Infrastruktur in Deutschland, auf der die Kundendaten gespeichert sind, erfordern, entweder selbst aus oder überwacht sie. Microsoft bleibt gegenüber dem Kunden für SLAs

(Service-Level-Vereinbarungen) sowie für die meisten Betriebsaspekte, bei denen es keine Zugriffsmöglichkeit auf Kundendaten gibt, verantwortlich.

Der Datentreuhänder übernimmt u. a. die folgenden (regulären) Aufgaben im Rahmen des Rechenzentrumbetriebs für die Microsoft Cloud Deutschland:

Incident Management

- Überwachung der eingehenden Plattformvorfälle und Supportfälle sowie der Bereitstellungsprobleme und neuer Serviceanforderungen
- Priorisierung eingehender Vorfälle anhand einer Bewertung der geschäftlichen Auswirkungen
- Regelmäßige Berichterstattung an Microsoft zur Integrität der Services und betrieblichen Verfahren der Microsoft Cloud Deutschland
- Hilfe bei der Wiederherstellung nach Ausfällen

Network Management

- Wartung der Netzwerkinfrastruktur
- Durchführung von System- und Softwareupdates/-upgrades unter Anleitung der Teams von Microsoft
- Regelmäßige Überprüfung der Protokollierungsgenauigkeit

Datacenter Management

- Vor-Ort-Support für Systeme im Rechenzentrum
- Unterstützung, bei denen ein physischer Zugang zu Servern, entsprechenden Geräten bzw. Netzwerkhardware erforderlich ist

Risk Management

- Implementierung von Sicherheitskontrollen
- Fortlaufende Überwachung des Status und der Effektivität der Compliance im gesamten Microsoft Cloud Deutschland-System und Bereitstellung von Berichten und Eskalation
- Aufstellung von Plänen für Skalierung, Ausführung und Abstimmung von Audits
- Darüber hinaus ist nicht vorgesehen, dass Mitarbeiter des Datentreuhänders eigene Sicherheitsüberprüfungen oder Audits durchführen.

Der Genehmigungsprozess und das Escort-Modell im deutschen Datentreuhändermodell

Der deutsche Datentreuhänder verpflichtet sich gegenüber Kunden vertraglich, Microsoft und seinen Subunternehmern keinen Zugang zu Kundendaten zu gewähren, außer unter den folgenden Bedingungen:

(1) Microsoft oder ein Subunternehmer muss ein Kundenproblem lösen oder eine Störung der Microsoft Cloud Deutschland beheben, die nicht von T-Systems behoben werden kann.

(2) Microsoft oder ein Subunternehmer muss Wartungs- oder Verbesserungsarbeiten an der Microsoft Cloud Deutschland ausführen.

Die Microsoft Cloud Deutschland setzt die „Zero Administrative Privilege"-Richtlinie um: Tritt eine der beiden oben genannten Bedingungen ein und Microsoft oder ein Subunternehmen benötigt Zugang auf die Systeme der Microsoft Cloud Deutschland, wird für einen definierten und dokumentierten Zweck eine Begleitung angefragt. Wird die Anfrage durch den Datentreuhänder genehmigt, leitet der deutsche Datentreuhänder eine von zwei Verfahrensweisen ein, die der Microsoft-Bereitschaftstechniker einhalten muss, um sicherzustellen, dass der deutsche Datentreuhänder die Kontrolle über den Zugang zu bzw. Zugriff auf die Kundendaten behält.

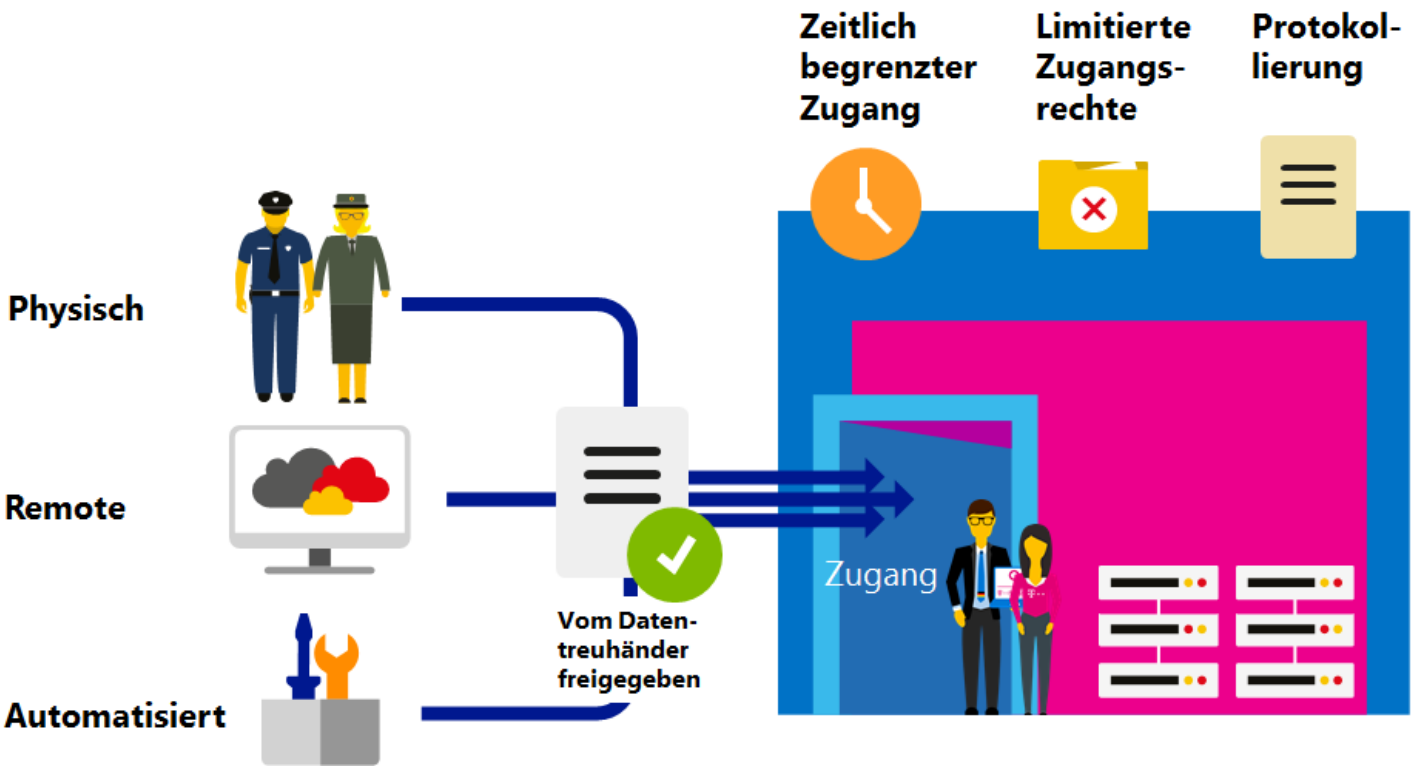
Beim ersten Ansatz – dem physischen Escort-Modell – kann der deutsche Datentreuhänder dem Microsoft-Bereitschaftstechniker vorübergehend Zugang unter seiner Aufsicht auf die Infrastruktur gewähren, auf der die Kundendaten gespeichert werden. Beim zweiten Ansatz – dem Remote Escort-Modell auf Basis eines technischen Genehmigungstools (z. B. das Lockbox-System für Microsoft Office 365 Deutschland) – verfügt der deutsche Datentreuhänder über die Möglichkeit, Microsoft oder dem Subunternehmen für eine begrenzte Zeit und zur Ausführung einer explizit erklärten Aufgabe remote den Zugriff auf die Microsoft Cloud Deutschland zu gewähren. Beide Verfahrensweisen werden nachfolgend beschrieben.

Physischer Escort: Unter bestimmten Umständen teilt ein Microsoft-Bereitschaftstechniker oder Subunternehmer dem deutschen Datentreuhänder mit, dass aus geschäftlichen Gründen die physische Anwesenheit in einem Microsoft Cloud Deutschland-Rechen- oder Betriebszentrum zur Problemlösung erforderlich ist. Wenn der deutsche Datentreuhänder die Anfrage genehmigt, erhält der Bereitschaftstechniker im Rahmen des Escort-Modells vorübergehend Zugang, wobei sichergestellt wird, dass der deutsche Datentreuhänder alle Handlungen des Microsoft-Mitarbeiters persönlich überwachen kann. Der deutsche Datentreuhänder kontrolliert den physischen Zutritt zu den Betriebs- und Rechenzentrumseinrichtungen, in denen Kundendaten gespeichert sind. Bei nicht vertragskonformen Anfragen wird der physische Zugang vom Datentreuhänder verweigert.

Hinweis: Ersthelfer in Notfällen – z.B. Feuerwehr, Rettungssanitäter – benötigen keine Begleitung.

Remote-Escort: In einem typischen Escort-Szenario stellt der deutsche Datentreuhänder die Verbindung zu einer virtuellen Maschine her und lädt den Microsoft-Bereitschaftstechniker dazu ein, die Sitzung zu begleiten. Anschließend übergibt der deutsche Datentreuhänder die entsprechenden temporären Rechte dem Microsoft-Bereitschaftstechniker und beaufsichtigt die gesamte Sitzung, während der Bereitschaftstechniker die genehmigten Aufgaben ausführt. Der deutsche Datentreuhänder kann bei Bedarf jederzeit die Sitzung beenden. In diesem Fall wird die Verbindung des Microsoft-Bereitschaftstechnikers sofort unterbrochen.

Abgesehen davon, dass der Zugang nur für eine begrenzte Zeit gewährt wird, werden lediglich minimale Zugangsrechte für die Durchführung der genau definierten Aufgabe vergeben. Der deutsche Datentreuhänder kontrolliert den Zugang und erhält Protokolle über jeden gewährten Zugang sowie über die Ausführung von Aufgaben. Die Protokollierung der Aktivitäten in der Microsoft Cloud Deutschland erfolgt in der Regel durch den (Video-)Mitschnitt der begleiteten Online-Sessions. Zudem erfolgt eine eigenverantwortliche Sichtung und Prüfung der relevanten Logging-Daten, ausgeführten Skripte und Kommandozeilen durch den Datentreuhänder. Sämtliche Dokumentationen und Nachweise werden beim Datentreuhänder aufbewahrt und in der Microsoft Cloud Deutschland gesichert. Microsoft hat damit keine Möglichkeit, die Protokoll-Daten zu beeinflussen oder im Nachhinein zu modifizieren.



In den Fällen, in denen Microsoft-Mitarbeiter Zugangsrechte für die deutsche Cloud benötigen, kann der deutsche Datentreuhänder diese für jeden Mitarbeiter mit speziellen Tools zur Zugangskontrolle (Role Based Access Control, RBAC) festlegen. Durch RBAC wird der Zugang zu Kundendaten autorisiert und protokolliert. Die Zugangsrechte sind jeweils auf die zu erledigenden Aufgaben zugeschnitten. Die Rechte sind in einem internen Tool zur Identitätsverwaltung definiert und werden über ein in Deutschland bereitgestelltes Active Directory durchgesetzt. Sobald die vom deutschen Datentreuhänder gewährte Zeit um ist, erlischt das Zugangsrecht. Bei Bedarf kann der deutsche Datentreuhänder den Zugang außerdem jederzeit während der genehmigten Zugriffsdauer vorzeitig beenden.

Der deutsche Datentreuhänder prüft pro Vorfall jeweils die Zugangsanfragen und gewährt einzeln den Zugang. Liegen Umstände wie die oben beschriebenen vor, dann erhalten die Microsoft-Techniker nur für die Zeit Zugang, die sie benötigen, um das Problem zu lösen.

In diesem Fall begleitet und protokolliert der deutsche Datentreuhänder die Aktivitäten der Techniker und entzieht den Zugang, sobald das Problem gelöst ist oder, falls erforderlich, jederzeit während der Aufgabenbearbeitung. Kunden sind ebenfalls in der Lage, Microsoft-Mitarbeitern selbst den Zugang zu gewähren, wenn sie Unterstützung bei der Lösung von Kundenproblemen benötigen.

Microsoft erhält somit keinen Zugang zu Kundendaten in der Microsoft Cloud Deutschland, es sei denn, der folgende Genehmigungsprozess wird eingehalten:

(1) Microsoft beantragt den Zugang als Reaktion auf bestimmte Anforderungen (z.B. um ein Problem zu lösen, dass der deutsche Datentreuhänder nicht selbst lösen kann).

(2) Der deutsche Datentreuhänder prüft, ob die Anfrage einem erlaubten Zweck gilt und genehmigt sie oder lehnt ab.

(3) Nach erfolgter Genehmigung gewährt der deutsche Datentreuhänder den Zugang. Die Genehmigung gilt nur für eine spezifische Aufgabe und für die Zeit, die benötigt wird, um den genehmigten Zweck zu erfüllen. Während der

Zugangsphase werden alle Aktivitäten der Microsoft-Mitarbeiter protokolliert und vom deutschen Datentreuhänder überwacht.

(4) Sobald die Aufgabe abschließend bearbeitet worden ist, wird das Zugangsrecht entzogen. Falls mehr Zeit benötigt wird, müssen die Microsoft-Mitarbeiter eine neue Genehmigung beantragen.

Dieser Genehmigungsprozess ist in der nachfolgenden Abbildung dargestellt:

Nachdem der deutsche Datentreuhänder Microsoft den Zugang gewährt hat, benutzen Microsoft-Techniker entweder automatisierte Tools oder lösen das Problem manuell. Beide Szenarien sind in den folgenden Abschnitten detailliert dargestellt.

Automatisierter Zugang: Falls Microsoft-Bereitschaftstechniker Zugang zu Bereichen in der Microsoft Cloud Deutschland benötigen, die keine Kundendaten enthalten, wird eine Zugangsanfrage gestellt. Nach erfolgter Genehmigung setzt Microsoft automatisierte Tools in der Microsoft Cloud Deutschland ein, um die Maßnahme ohne Zugang zu Kundendaten zu bearbeiten.OBJ

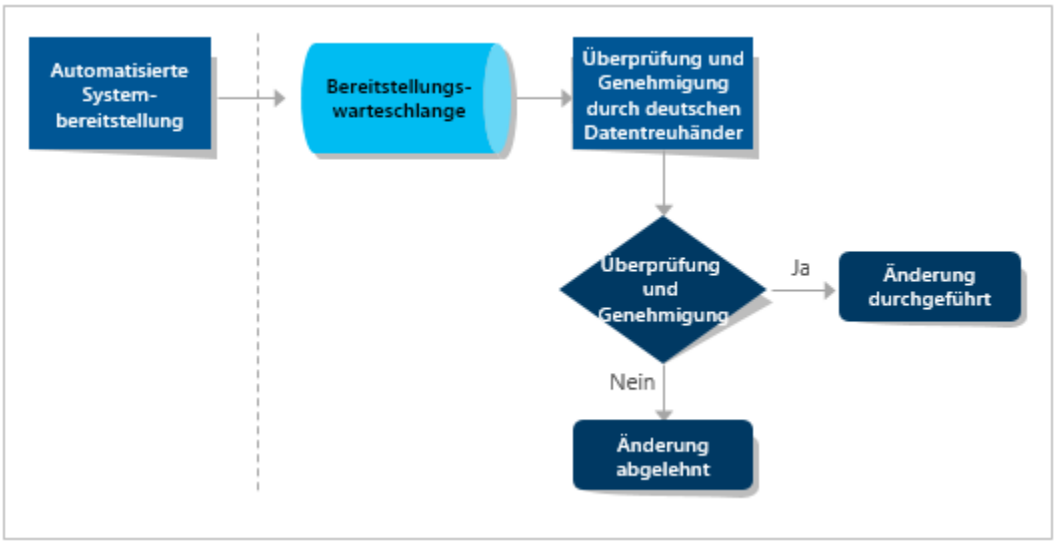
Beispiele für den automatischen Zugang:

- Aktualisierungen für neue Software Features, Upgrades,
- Umgebungsausbau oder
- Wartungsarbeiten wie Patches etc.

Der Ablauf für den automatisierten Zugang ist wie folgt:

1. Microsoft-Techniker beantragen den Einsatz des automatisierten Systems.
2. Die Anfrage wird in die Bereitstellungswarteschlange eingestellt.
3. Der deutsche Datentreuhänder überprüft die Anfrage auf Vertragskonformität und genehmigt sie oder lehnt sie ab.

4. Wenn sie genehmigt wurde, kommen „automatisierte Tools“ zum Einsatz, um die Änderung durchzuführen. Das bedeutet, dass diese Tools durch den Microsoft-Techniker mit vordefinierten und durch den Datentreuhänder freigegebenen Befehlsketten versehen bzw. konfiguiert und diese Aufgaben dann automatisiert abgearbeitet werden.



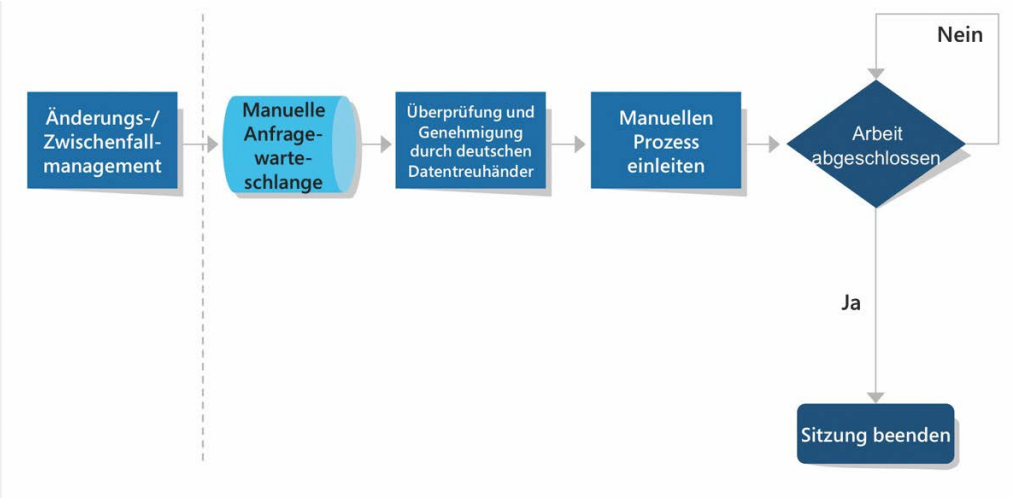
Manueller Zugang: Es gibt Fälle, in denen ein Microsoft-Bereitschaftstechniker Maßnahmen ergreifen muss, die nicht ohne potenziellen Zugang zu Kundendaten oder auf Systeme, auf denen Kundendaten gespeichert werden, durchgeführt werden können.

Beispiele für den manuellen Zugang:

- Change und Incident Management,
- Untersuchung von Fehlern oder Problemen sowie
- Einsatz bei Schwierigkeiten mit dem automatisierten Deployment.

In solchen Fällen hält der Microsoft–Bereitschaftstechniker das folgende Protokoll ein:

1. Dem Microsoft–Bereitschaftstechniker liegt eine Änderungs-/Zwischenfallmanagementanfrage vor, die manuellen Zugang erfordert.
2. Der Microsoft–Bereitschaftstechniker beantragt den Zugang beim deutschen Datentreuhänder.
3. Der deutsche Datentreuhänder überprüft die Anfrage und genehmigt sie oder lehnt sie ab.
4. Wenn er sie genehmigt, erlangt der Microsoft–Bereitschaftstechniker Zugang entweder über die physische Escort- oder die Remote-Escort-Methode.
5. Der Microsoft–Bereitschaftstechniker führt den manuellen Vorgang aus.
6. Der Microsoft–Bereitschaftstechniker schließt seine Arbeit ab.
7. Die vom deutschen Datentreuhänder gewährte Bearbeitungsperiode läuft ab oder der deutsche Datentreuhänder beendet die Sitzung.



Wartung und Verbesserung: Szenarien für den Genehmigungsprozess im Escort-Modell

Wird ein Wartungsfall bekannt bzw. ist eine Verbesserung an Systemen oder der Infrastruktur für die Dienste aus der Microsoft Cloud Deutschland erforderlich, wird seitens des Datentreuhänders überprüft, ob er diesen Fall selbstständig bearbeiten kann. In den Fällen, in denen Microsoft-Bereitschaftstechniker zur Behandlung des Falls benötigt werden, wird der Genehmigungsprozess initiiert.

Es wird zwischen zwei unterschiedlichen Szenarien für Wartungs- und Verbesserungsarbeiten differenziert:

(1) physische Wartung oder Verbesserung (zum Beispiel an Hardware), die durch einen Microsoft-Bereitschaftstechniker vor Ort durchgeführt werden muss oder

(2) logische Wartung oder Verbesserung (zum Beispiel an der Software), die der Microsoft-Bereitschaftstechniker remote durchführen kann.

In jedem Fall beschreibt Microsoft in einem Standardtemplate die Ausgangssituation bzw. den Bedarf und die geplanten Tätigkeiten (inkl. einzuspielende Skripte) und übersendet es dem Datentreuhänder. Dieser erhält die Zugangsanfrage und die Informationen zur Überprüfung und bewertet u.a.

(1) ob davon Kundendaten betroffen sind,

(2) ob unrechtmäßige Befehle vorhanden sind, die den sicheren Zugang zur Microsoft Cloud Deutschland umgehen könnten (wie zum Beispiel „Backdoors“) und

(3) ob verdächtige Veränderungen an Daten bzw. Systemen und Prozessen, die Daten manipulieren können, geplant sind (zum Beispiel Veränderung von Kundendaten durch einzuspielende Skripte, unrechtmäßige Veränderungen innerhalb der Umgebung).

Für jede Anfrage trifft der Datentreuhänder die Entscheidung, ob diese genehmigt oder abgelehnt wird und ob zusätzliche Informationen erforderlich sind. Falls der Datentreuhänder eine Zutrittsgenehmigung erteilt und Microsoft-Bereitschaftstechniker ihre Aufgabe vor Ort durchführen, werden sie die gesamte Zeit von einem Mitarbeiter des Datentreuhänders begleitet und kontrolliert. In den Fällen, in denen die Microsoft-Bereitschaftstechniker remote die Aufgabe erledigen können, baut der Datentreuhänder eine sichere Verbindung mit der Microsoft Cloud Deutschland auf und lädt den Microsoft-Mitarbeiter dazu ein. In dieser Konstellation – also unter der Aufsicht des Datentreuhänders –

werden die genehmigten Verbesserungen bzw. -änderungen vorgenommen. Der Datentreuhänder zeichnet die Sitzung auf und archiviert dieses Video mit den eingespielten Skripten, Kommandobefehlen und Logging-Daten. Sobald die Aufgabe abgeschlossen ist, wird die Verbindung getrennt.

Sicherheit & Compliance in der Microsoft Cloud Deutschland

Regionale und lokale Sicherheits- und Compliance-Anforderungen der Kunden und entsprechende Maßnahmen werden kontinuierlich durch Microsoft evaluiert. Microsoft verpflichtet sich der Entwicklung und Aufrechterhaltung eines angemessenen Compliance-Portfolios, um dem Bedarf der Kunden und Partner entegegenzukommen.

Transparenz für Kunden

Die deutschen Rechenzentren nutzen die gleichen Technologien und bieten die gleichen hohen Sicherheitsstandards wie die globalen Cloud-Angebote von Microsoft. Dazu gehören Multi-Faktor-Authentifizierungen, biometrische Scans, Smartcards, Datenverschlüsselungen nach TLS-Protokollen, physische Sicherheitsmaßnahmen, Sicherungen gegen Naturkatastrophen und Stromausfälle. Es gelten zusätzlich die weiter oben im Dokument erwähnten Richtlinien zur datentreuhänderischen Zugangskontrolle.

Innerhalb der Microsoft Cloud Deutschland findet der Datenverkehr und die Replikation der beiden Rechenzentren über ein eigenes dediziertes, von den übrigen Rechenzentren abgesondertes, Netzwerk statt. Damit kann sichergestellt werden, dass die Daten innerhalb der deutschen Landesgrenzen bleiben und die Datensicherheit und Compliance gewährt ist. Einzig der ausgehende Datenverkehr wird über direkte Internetanbindungen mit minimaler Latenz abgewickelt.

Die Server der Microsoft Cloud Deutschland werden durch Zertifikate der Zertifizierungsstelle der Bundesdruckerei GmbH, D-TRUST, gesichert. D-TRUST stellt für die Server TLS-Zertifikate aus, die die Kommunikation zwischen den Anwendern von Microsoft Azure Deutschland, Office 365 Deutschland und Dynamics 365 Deutschland sowie den Servern in den neuen deutschen Rechenzentren absichern. Zudem haben Kunden und Partner (gegen Aufpreis) die Option, auch ihre eigenen Anwendungen in Microsoft Azure Deutschland mit den Zertifikaten der D-TRUST abzusichern.

Microsoft bietet Kunden die Basis, um Compliance für ihre eigenen Anwendungen zu erreichen. Microsoft-Kunden erhalten detaillierte Informationen über Microsoft-Sicherheits- und Compliance-Programme, einschließlich Audit-Berichten und Compliance-Paketen, um Microsoft-Dienste gegenüber ihren eigenen rechtlichen und regulatorischen Anforderungen zu bewerten. Das zuständige Microsoft-Team für Compliance-Fragen arbeitet außerdem mit Microsoft-

Engineering- und Betriebsteams aller Cloud-Dienste ebenso wie mit externen Aufsichtsbehörden zusammen, um dabei zu helfen, sicherzustellen, dass die Anforderungen von Kunden erfüllt werden.

In der nachfolgenden Abbildung ist die aktuelle Compliance-Roadmap für die Microsoft Cloud Deutschland abgebildet und gibt einen Überblick über durchgeführte und geplante Maßnahmen:

Das „IT Grundschutz Compliance Workbook Microsoft Azure Germany” zum Beispiel unterstützt Kunden mit Empfehlungen, wie sie ihr „IT Grundschutz“-Zertifikat erhalten. Weitere Informationen über die weltweiten Microsoft-Dienste erhalten Sie im Microsoft Trust Center: https://azure.microsoft.com/de-de/support/trust-center/.

Bei der Microsoft Cloud Deutschland handelt es sich um die dritte Generation von Microsoft-Technologie, die es einem lokalen Operator erlaubt, sämtliche Aspekte des Dienstes zu kontrollieren, bei denen es um Kundendaten geht. Microsoft benutzt in seinen weltweiten Diensten ähnliche Tools zur rollenbasierten Zugriffskontrolle (Role-Based Access Control „„RBAC“), um Zugriffe des Betriebspersonals zu steuern. Bei den globalen Diensten von Microsoft müssen Mitarbeiter, die Zugang benötigen, hierzu die Genehmigung von dazu berechtigten Microsoft-Mitarbeitern erhalten (z.B. von einem Supervisor). Bei der Microsoft Cloud Deutschland ist es der Datentreuhänder, der dazu befugt ist, Zugangsberechtigungen zu erteilen.

Diese einzigartige Technologie der Zugangskontrolle (Patente sind angemeldet) ist erprobt und auf Technologien aufgebaut, die erstmals in China eingesetzt wurden, wo 21Vianet, ein chinesisches Unternehmen, Microsoft Azure- und Office 365-Clouddienste betreibt. Diese Technologie liegt außerdem der Microsoft Government Cloud zugrunde, bei der der Zugriff auf Kundendaten auf Mitarbeiter beschränkt ist, die strenge Überprüfungen durch den Staat erfolgreich bestanden haben.

Externe Verifizierung wird durch unabhängige Prüfungen („Audits“) gewährleistet, die in Übereinstimmung mit internationalen Normen wie ISO 27001, 27018 und SSAE 16 SOC 1 und SOC 2 durchgeführt werden. Diese Audits schließen auch Überprüfungen der Steuerungsmaßnahmen ein, die den Zugriff auf Kundendaten in der Microsoft Cloud Deutschland regeln. Allen Kunden stehen detaillierte Prüfberichte zur Verfügung.

Datenkategorien

Kundendaten werden weit definiert und umfassen „alle Daten einschließlich Text-, Ton-, Video- oder Bilddateien sowie Software, die Microsoft oder dem Datentreuhänder durch den Kunden oder im Namen des Kunden durch die Nutzung der“ Microsoft Cloud Deutschland zur Verfügung gestellt werden. Dies schließt ein:

(1) Alle Daten, die Kunden zur Speicherung oder Verarbeitung in die deutsche Cloud hochladen;

(2) Softwareanwendungen des Kunden, die auf Plattformdiensten wie Azure Deutschland gehostet werden und

(3) Informationen, die die Endnutzer des Kunden identifizieren, wie z.B. die von Kunden über Endnutzer in Azure Active Directory Deutschland gespeicherten Informationen.

Zusätzlich hierzu werden folgende Informationen mit denselben Restriktionen gehandhabt wie Kundendaten:

(1) Metadaten, aus denen sich Kundendaten ableiten lassen könnten; und

(2) Anmeldeinformationen, die den Zugriff auf Kundendaten oder auf Systeme ermöglichen könnten, in denen Kundendaten enthalten sind.

Folglich sind alle der für Kunden wichtigsten Informationen in den oben dargestellten Kategorien enthalten und der Zugang wird vom Datentreuhänder streng kontrolliert.

Zusätzlich zu den Kundendatenszenarien, bei denen der Kunde und der deutsche Datentreuhänder den Zugang kontrollieren, gibt es auch bestimmte andere Datenkategorien, bei denen Microsoft über direkten Zugang verfügt, ohne dafür die Zustimmung des Kunden oder des Datentreuhänders zu benötigen. Hierzu zählen die folgenden Informationen:

(3) **Kundenkontaktinformationen, darunter Angaben über Ansprechpartner für Rechnungslegung und Verwaltung.** Zur Inanspruchnahme von Diensten in der Microsoft Cloud Deutschland gehen Kunden direkt mit Microsoft einen Vertrag ein. Daher speichert Microsoft die benötigten Informationen, um sich mit Kunden in Verbindung zu setzen. Informationen über die einzelnen Endanwender des Kunden zählen nicht dazu.

(4) **Kundenrechnungsdaten.** Microsoft ist dafür zuständig, Kunden die konsumierten Cloud-Dienste in Rechnung zu stellen. Microsoft verfügt daher über Informationen zu Zahlungsinstrumenten und zur Dienstnutzung pro Kundenkonto (z.B. Anzahl der E-Mail-Konten, genutzte Rechen- oder Speicherleistung usw.)
Hinweis: Nutzungsinformationen einzelner Endanwender des Kunden sind hiervon ausgeschlossen.

(5) **Informationen über den Dienstzustand.** Microsoft verfügt über verschiedene technische Daten, durch die der Funktionszustand der Microsoft Cloud Deutschland überwacht wird. Hierzu zählen z. B. Angaben zur Kapazitätsauslastung und zum Serverbetrieb. Diese technischen Daten enthalten unter keinen Umständen Kundendaten oder Informationen, aus denen Kundendaten abgeleitet werden könnten.

Offenlegung von Kundendaten

Der Vertrag zwischen dem Kunden und dem Datentreuhänder legt fest, dass Kundendaten nur im Rahmen der folgenden Regelungen offengelegt werden dürfen: Der Datentreuhänder legt Kundendaten nicht gegenüber Drittparteien offen, außer

(1) der Kunde erlaubt es,

(2) die Datentreuhändervereinbarung lässt es zu oder

(3) deutsches Recht erfordert es.

Der Datentreuhänder legt Kundendaten nicht gegenüber Strafverfolgungsbehörden offen, es sei denn, deutsches Recht erfordert es. So erhalten zum Beispiel US-Behörden keine Kundendaten, die in der Microsoft Cloud Deutschland gespeichert werden, es sei denn dies ist unter deutschem Recht erforderlich (z.B. im Rahmen eines Rechtshilfeersuchens) Das bleibt auch davon unberührt,, dass Microsofts Konzernmutter sowie auch T-Systems International-Konzernunternehmen ihren Sitz in den USA haben. Anfragen von Behörden werden von T-Systems International auf Rechtmäßigkeit geprüft und Auskunft wird nur erteilt, wenn die rechtlichen Voraussetzungen unter deutschem Recht hierfür erfüllt sind.

Microsoft hat keine rechtliche und technische Möglichkeit, um an die Kundendaten in der deutschen Cloud, ohne Genehmigung durch den Datentreuhänder oder dem Kunden, zu gelangen. Zudem hat Microsoft Corporation auch keine vertragliche Beziehung gegenüber dem Datentreuhänder oder dem Kunden, die sie dazu berechtigen würde Kundendaten weiterzugeben oder eine entsprechende Anweisung zu erteilen.

Falls der Datentreuhänder auf Basis einschlägiger gesetzlicher Regelungen dazu gezwungen wird, Kundendaten gegenüber Strafverfolgungsbehörden offenzulegen, benachrichtigt er den Kunden umgehend darüber und übermittelt ihm eine Kopie der Anfrage, es sei denn, dies ist gesetzlich untersagt.

Falls der Datentreuhänder irgendwelche anderen Anfragen von Drittparteien mit der Bitte um Zugang zu Kundendaten erhält, informiert der Datentreuhänder den Kunden umgehend darüber, es sei denn, dies ist gesetzlich untersagt. Wenn der Datentreuhänder nicht gesetzlich zur Offenlegung der Kundendaten verpflichtet ist, lehnt er die Anfrage ab. Wenn das Verlangen berechtigt ist und der Datentreuhänder dazu gezwungen werden könnte, die angefragten Informationen weiterzuleiten, fordert der Datentreuhänder trotzdem zunächst die Drittpartei auf, die Kundendaten vom Kunden anzufordern. Wenn eine betroffene Person (Datensubjekt) Zugriff auf ihre eigenen Daten verlangt, leitet der Datentreuhänder die Anfrage an den Kunden weiter.

Vorbehaltlich der vorstehend genannten Bedingungen erlaubt der Datentreuhänder – ohne eine Prüfung der Anfrage auf Vertragskonformität – keiner Drittpartei:

(1) den direkten, indirekten, pauschalen oder ungehinderten Zugang zu Kundendaten;

(2) Zugang zu den Plattformverschlüsselungscodes, mit denen Kundendaten gesichert werden, oder zu Möglichkeiten, die Verschlüsselung zu umgehen oder zu durchbrechen; oder

(3) Zugang jeglicher Art zu Kundendaten, falls der Datentreuhänder davon Kenntnis hat, dass die Daten für andere Zwecke als die in der Anfrage genannten verwendet werden sollen.

Zur Umsetzung der vorstehend genannten Regelungen leitet der Datentreuhänder u.U. die grundlegenden Kontaktinformationen an die Drittpartei weiter.

Falls Microsoft von Drittparteien Anfragen erhält, werden diese an den Kunden oder an den deutschen Datentreuhänder weitergeleitet. Der deutsche Datentreuhänder verpflichtet sich gegenüber seinen Kunden vertraglich dazu, alle Anfragen von Drittparteien in Übereinstimmung mit deutschem Recht oder gemäß Kundenauftrag zu behandeln.

Da Microsoft grundsätzlich keinen Zugang auf die Daten in der Microsoft Cloud Deutschland hat, kann Microsoft Anforderungen von Behörden oder anderen Dritten nach einer Datenfreigabe selbst dann nicht nachkommen, wenn dies durch die Vollzugsbehörden oder das Rechtsprechungssystem des jeweiligen Landes angeordnet wird. Microsoft verweist daher jegliche Dritte an den Kunden bzw Datentreuhänder.

Behörden und andere Dritte haben die Möglichkeit, etwaige Ansprüche zur Herausgabe von Kundendaten gerichtlich geltend zu machen, , genau wie dies bei jedem anderen deutschen Unternehmen, das Kundendaten in Deutschland hostet, der Fall ist. In jedem Fall kann aber Microsoft solchen Herausgabeverlangen nicht nachkommen.

Weiterführende Dokumente

Um die Microsoft-Prinzipien Sicherheit, Datenschutz, Transparenz und Compliance aufrechtzuerhalten, ist Microsoft bestrebt dazu, den Kunden in aller Welt genau die auf ihre Bedenken und Anforderungen zugeschnittenen Dienste anzubieten. In Deutschland setzt Microsoft diese Bestrebungen durch die Microsoft Cloud Deutschland und das Datentreuhändermodell um und bietet seinen Kunden so die erforderlichen Zusicherungen. Da alle Kundendaten ausschließlich in Deutschland gehostet werden und ein deutscher Partner die Kontrolle über den Zugang hat, erfüllt das von uns entwickelte System viele Anforderungen unserer Kunden nicht nur in technischer, sondern auch in rechtlicher Hinsicht.

Weitere Informationen finden Sie hier:

Office 365 Security-Whitepaper
Microsoft Azure Network Security

Microsoft Cloud Deutschland

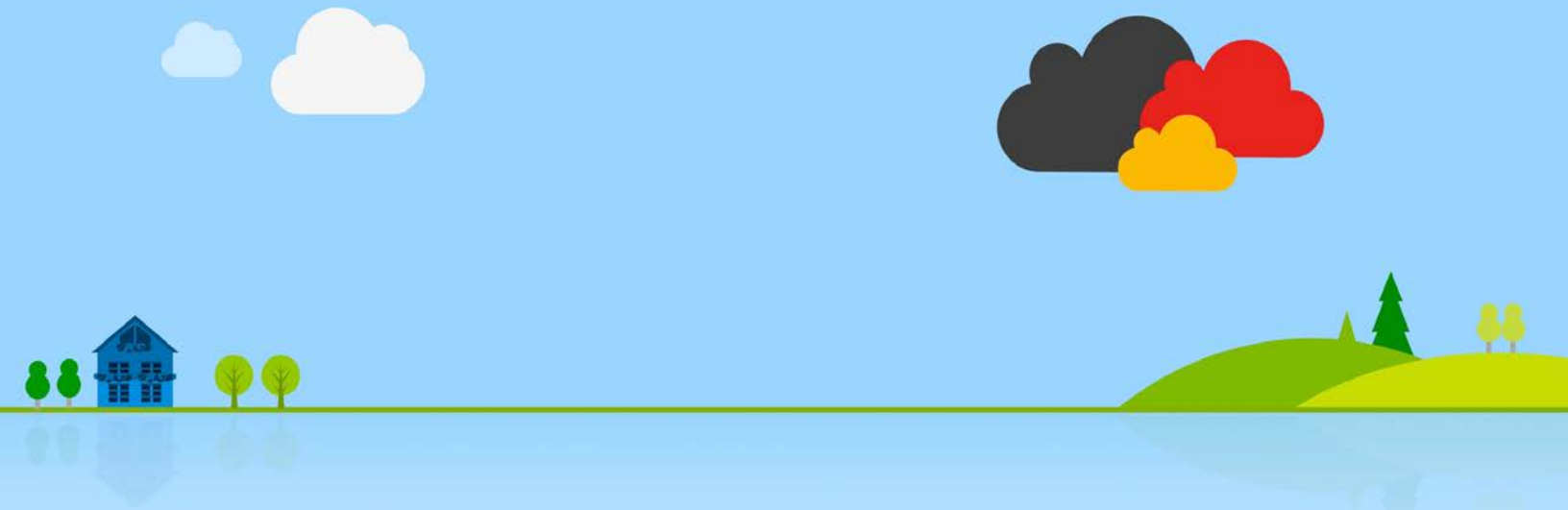
Microsoft Trust Center

IT Grundschutz Compliance Workbook Microsoft Azure Germany

Übersicht Microsoft Azure Deutschland Dienste

Microsoft Cloud Deutschland Pressemappe

Denkschrift "Cloud for Global Good": Vertrauen, Verantwortung, Teilhabe



Microsoft