WHITEPAPER

Transfer Impact Assessment

Version: 05.03.2025

Hinweis zur Geschlechterneutralität: Alle Formulierungen gelten geschlechtsneutral.

Dieses Dokument dient nur zur Information in Bezug auf ATOSS Cloud Produkte und kann sich von Zeit zu Zeit ändern. Die aktuelle Version finden Sie auf unserer Website abrufbar via https://www.atoss.com/de/sicherheit/data-residency

Im Einzelnen beinhaltet es Informationen über die ATOSS Cloud Core Services

- ATOSS Staff Efficiency (ASES) CLOUD24/7*
- ATOSS Startup Edition (ASE) CLOUD 24/7*
- ATOSS Staff Efficiency (ASES) Cloud Solution*
- ATOSS Startup Edition (ASE) Cloud Solution*
- ATOSS Time Control (ATC) CLOUD24/7
- ATOSS Time Control (ATC) Cloud Solution

**Erläuterungen zum Abschluss einer EU Data Boundary finden Sie auf Seite 13 ff.*

die Cloud Dedicated Services

- Identity and Access management (IAM) Service
- Staff Center (Mobile) Security Gateway Service
- ATOSS Time Control (Mobile) Security Gateway Service

Details zu den Service Levels und Leistungsbeschreibungen finden Sie u.a. auf unserer Website:
https://www.atoss.com/de/agb

Es beinhaltet ausdrücklich keine Informationen in Bezug auf

- Crewmeister Produkte
- den ATOSS Connector for Workday
- das Modul Workforce Analytics
- die ATOSS-interne IT-Infrastruktur

Sollten Sie produktspezifische Informationen benötigen, kontaktieren Sie jederzeit gerne Ihren Key Account Manager.

Vorwort

Laut DSGVO gelten bestimmte Voraussetzungen für die Verarbeitung personenbezogener Daten außerhalb der EU (sog. Drittstaatentransfer).

Dabei ist u.a. ein Transfer Impact Assessment (TIA) für die Nutzung von Clouddiensten erforderlich. Ein TIA identifiziert und bewertet das Datenschutzniveau und ggf. zusätzliche Garantien gemäß Art. 46 DSGVO, soweit ein Angemessenheitsbeschluss der EU-Kommission für den Empfänger im Drittstaat nicht vorliegt. Der **Europäische Datenschutzausschuss (EDSA)** betont zugleich, dass Datenschutz stets verhältnismäßig umgesetzt werden soll. D.h., es muss stets eine Abwägung der Sachlage und Rechtsgüter erfolgen.

Wir möchten Sie darauf hinweisen, dass die Ausführungen in diesem Dokument keine verbindlichen Zusagen, Zusicherungen oder Gewährleistungen für die Lizenzprodukte begründen. Insoweit gelten ausschließlich die Angaben in den Vertragsunterlagen in Bezug auf das jeweilige Cloud Produkt. Überdies ersetzen sie keine (datenschutz-) rechtliche Beratung auf Seiten des Kunden. Bitte stimmen Sie sich im Zweifel stets mir ihrem Datenschutzbeauftragten ab.

ATOSS darf Ihnen auch keine Rechtsberatung anbieten. Wir unterstützen unsere Kunden zugleich nach bestem Umfang, indem wir Ihnen nachfolgend relevante Informationen zur eigenen Bewertung unserer Cloud Services im Lichte des "Schrems II"-Urteils des Gerichtshofs der Europäischen Union und der Empfehlungen des EDSA veröffentlichen.

Transfer Impact Assessment in sechs Schritten

Schritt 1 Kennen Sie Ihre Datenübermittlungen

Laut EDSA sollen Unternehmen nachvollziehen, welche personenbezogenen Daten sie an Empfänger in Drittländer übermitteln lassen, um sicherzustellen, dass das Datenschutzniveau dieser Empfänger dem der DSGVO entspricht.

Schritt 2 Identifizieren Sie die Übermittlungsinstrumente, auf die Sie sich verlassen

Liegt ein Drittstaatentransfer vor, dürfen personenbezogene Daten an Empfänger in Drittländer übermittelt werden, wenn die EU-Kommission ein angemessenes Schutzniveau bestätigt hat. Falls das Drittland keinen Angemessenheits-beschluss besitzt, sind alternative Übermittlungsinstrumente, wie Standardvertragsklauseln und zusätzlich implementierte Sicherheitsmaßnahmen zu evaluieren, um gleichwohl ein angemessenes Datenschutzniveau bejahen zu können.

Schritt 3 Beurteilen Sie die Wirksamkeit der Übermittlungsinstrumente in Anbetracht aller Umstände

In einem dritten Schritt soll geprüft werden, ob die geltenden Rechtsvorschriften und / oder Praktiken des Drittlandes die Wirksamkeit des verwendeten Übermittlungsinstrumente beeinträchtigen.

Schritt 4 Identifizieren und ergänzen Sie zusätzliche Maßnahmen, wo erforderlich

Nur wenn die bisherige Bewertung ein unzureichendes Datenschutzniveau erkennen lässt, müssen ergänzende Maßnahmen (entweder durch den Verantwortlichen oder Auftragsverarbeiter) in Betracht gezogen werden. Falls trotz zusätzlicher Sicherheitsmaßnahmen keine ausreichende Datensicherheit geschlussfolgert werden kann, ist die Übermittlung laut EDSA auszusetzen, um die betroffenen Rechtsgüter zu schützen.

Schritt 5 Berücksichtigen Sie Verfahrensschritte, wenn Sie zusätzliche Maßnahmen für effektiv bewerten

Der fünfte Schritt umfasst alle nötigen Verfahren zur Sicherstellung einer angemessenen Garantie nach Art. 46 DSGVO. Zusätzliche Sicherheitsmaßnahmen müssen also DSGVO-konform sein und ggf. mit Datenschützern und Datenschutzbehörden abgestimmt werden.

Schritt 6 Führen Sie eine Neubewertung in angemessenen Abständen durch

Der sechste und letzte Schritt besteht darin, das Datenschutzniveau in angemessenen Abständen neu zu bewerten und zu überwachen.

Schritt 1 Kennen Sie Ihre Datenübermittlungen

Laut EDSA sollen Unternehmen nachvollziehen, welche personenbezogenen Daten sie an Empfänger in Drittländer übermitteln lassen, um sicherzustellen, dass das Datenschutzniveau dieser Empfänger dem der DSGVO entspricht.

Prüfpunkte im Überblick:

- ✓ Verantwortlicher und Auftragsverarbeiter
- ✓ Datenexporteur: Name und Beschreibung der Organisation (entweder ein Verantwortlicher oder ein (Unter-)Auftragsverarbeiter), der die Datenübermittlung in das Drittland unmittelbar durchführt
- ✓ Datenimporteur: Name und Beschreibung der Organisation und Angaben zu etwaigen Unterauftragnehmern, die sich außerhalb des Europäischen Wirtschaftsraums (EWR) befinden und personenbezogene Daten von einem Datenexporteur erhalten.
- ✓ Kategorien der betroffenen Personen und Daten
- ✓ Verarbeitungszwecke

Verantwortlicher und Auftragsverarbeiter

Die DSGVO definiert zwei relevante Rollen in der Datenverarbeitung den Verantwortlichen und Auftragsverarbeiter (Kapitel 4 DSGVO). Jede Übermittlung personenbezogener Daten ist nur dann zulässig, wenn Verantwortliche und Auftragsverarbeiter die allgemeinen Grundsätze der Datenübermittlung einhalten – und zwar auch für Drittstaatenübermittlungen (Art. 44 DSGVO)

Welche Rolle hat der Kunde bezogen auf Datenübermittlungen seiner personenbezogenen Kundendaten in den ATOSS Cloud Produkten?

Bezogen auf den Cloud Service-Vertrag ist der Kunde der "**Verantwortliche**" seiner personenbezogenen Kundendaten. Gestattet der Kunde seinen verbundenen Unternehmen die Mitnutzung der lizenzierten Cloud Produkte, werden diese verbundenen Unternehmen ebenfalls zu "Verantwortlichen" für deren personenbezogene Unternehmensdaten. Der Kunde bleibt allerdings der alleinige Vertragspartner und ist damit einziger Ansprechpartner für ATOSS. Weitere Einzelheiten zu den Fallkonstellationen finden Sie in der Präambel der ATOSS AVV, die Sie auf unserer Website abrufen können.

Welche Rolle hat ATOSS bezogen auf Datenübermittlungen seiner personenbezogenen Kundendaten in den ATOSS Cloud Produkten?

Bezogen auf den Cloud Service-Vertrag sind ATOSS, einschließlich die mit ATOSS verbundenen Unternehmen, und die von ATOSS beauftragten Unternehmen zusammen "**Auftragsverarbeiter**" des Kunden. Das Gleiche gilt für im Verhältnis zu den mitnutzenden verbundenen Unternehmen des Kunden.

- Die vertragschließende ATOSS Gesellschaft (ATOSS) ist der Vertragspartner des Kunden, also einziger direkter Ansprechpartner und damit **Auftragsverarbeiter auf erster Stufe**.
- Die mit ATOSS verbundenen Unternehmen und beauftragten Unternehmen sind **Unterauftragsverarbeiter von ATOSS** und somit **Auftragsverarbeiter auf zweiter Stufe**. ATOSS trägt die Sorge für den Einsatz und die sorgfältige Auswahl seiner Unterauftragsverarbeiter. Die Liste der Unterauftrags-verarbeiter von ATOSS finden Sie in der AVV auf unserer Website.

Wird eine Auftragsverarbeitungsvereinbarung (kurz: "AVV") zwischen dem Kunden und ATOSS abgeschlossen?

Durch expliziten Einbezug formt die AVV immer einen integralen Bestandteil des ATOSS-Angebots bzw. des Cloud Service-Vertrags zwischen der vertragsschließenden ATOSS-Gesellschaft und dem Kunden.

Beauftragt ATOSS einen Unterauftragsverarbeiter mit der Durchführung bestimmter Auftragsverarbeitungstätigkeiten, so verpflichtet ATOSS diesen Unterauftragsverarbeiter zu im Wesentlichen denselben Datenschutzpflichten wie diejenigen, die für ATOSS um Kundenverhältnis gelten. ATOSS stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen ATOSS entsprechend dieser AVV und gemäß der DSGVO unterliegt.

Wie wählt ATOSS seine Unterauftragsverarbeiter aus?

ATOSS legt großen Wert darauf, dass alle Unterauftragsverarbeiter von ATOSS das vereinbarte Datenschutzniveau gleichermaßen bezogen auf ihre spezifischen Verarbeitungstätigkeiten gewährleisten. Dazu gehören in der Regel implementierte Sicherheitsmaßnahmen nach Best-Industry-Practices, wie die verschlüsselte Datenübertragung und der durch Standardsicherheitsmechanismen pro Zugriffstiefe gesicherte Zugriff sowie der Einbezug von Vertraulichkeitsklauseln, bis hin zu dem Nachweis von internationalen Zertifikaten.

Kommen alle in der AVV gelisteten Unterauftragsverarbeiter von ATOSS beim Kunden zum Einsatz?

Mit Abschluss der AVV besitzt ATOSS die allgemeine Erlaubnis des Kunden alle in AVV-Anhang III gelisteten Unterauftragsverarbeiter während der Vertragslaufzeit einzusetzen und zu wechseln (Multi-Scale-Strategie). ATOSS behält sich das Recht vor, nicht jeden der dort aufgeführten Unterauftragsverarbeiter für den Kunden einzusetzen. Dieses Vorgehen ermöglicht ATOSS effiziente und kurzfristige Kapazitäts- und Ressourcenplanungen, und bietet besondere Vorteile für Geschäfts-Kontinuitäts- und Ausfallsicherheits-Strategien. ATOSS wird den Einsatz der Unterauftragsverarbeiter zugleich auf das für die Leistungserbringung erforderliche Maß beschränken.

Beachten Sie ferner, dass Konfigurations- und Parametrisierungsleistungen innerhalb einer Kunden-Cloudinstanz nur erbracht werden können, soweit der Kunde hierzu einen User Account freischaltet. Das User und Access Management steuert folglich allein der Kunde.

Kann der Kunde die Liste der genehmigten Unterauftragsverarbeiter auf eine individuelle Auswahl von Unterauftragsverarbeitern beschränken?

Eine Löschung oder Beschränkung auf bestimmte Unterauftragsverarbeiter ist kundenindividuell nicht möglich. Denn ATOSS muss in der Lage sein, seine Leistungen stets bestmöglich für den Kunden zu gestalten, wozu – nicht nur ein effizientes Ressourcen– und Kapazitätsmanagement –, sondern auch die Vermeidung von Sicherheitsgefahren, wie einem Vendor Lock-in oder Serviceausfälle, gehören. ATOSS ist im Kundeninteresse bemüht eine hohe Innovationskraft aufrechtzuerhalten und kontinuierlich im Lichte eines Best-of-Breed-Ansatzes zugunsten der Servicequalität auszubauen. Bezogen auf diese Servicequalität und unser vertragliches Versprechen zu kontinuierlichen Modifikationen braucht ATOSS daher die Flexibilität modernste Technologien auszuwählen und wirksame Cloud-Prozesse zu etablieren, um seinen Kunden hervorragende Leistungen anbieten zu können.

Datenexporteur und Datenimporteur

Die Begriffe **Datenimporteur** und **Datenexporteur** stammen nicht aus der DSGVO, sondern aus den **Standardvertragsklauseln (SCC, Standard Contractual Clauses)** der Europäischen Kommission. Diese Rollen sollen den Übermittler und Empfänger von personenbezogenen Daten in ein Drittland näher beschreiben. Der EDSA hat dazu sogar Kriterien festgelegt, um eine sog. internationale Übermittlung konkret zu ermitteln.

Man kann festhalten: Wenn ein Unternehmen personenbezogene Daten außerhalb der EU/des EWR übermittelt, handelt es sich bei dem übermittelnden Unternehmen um einen Datenexporteur und der Empfänger im Drittland ist der Datenimporteur.

Laut EDSA ist zwar auch der bloße Fernzugriff aus einem Drittland auf personenbezogene Daten eine relevante Datenverarbeitung, d.h. also keine Speicherung von Daten in diesem Drittland ist erforderlich. Zugleich betont der EDSA, dass das bloße Risiko, dass Personen aus Drittländern auf in der EU/EWR gespeicherte Daten aus der Ferne zugreifen können, noch keine Weiterübermittlung gemäß Kapitel V DSGVO darstellt.

Informationen des EDSA finden Sie online abrufbar auf der Website der EU-Kommission:
https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en

Führt die Lizenzierung der ATOSS Cloud Produkte zu einer Übermittlung von personenbezogenen Daten an einen Empfänger in einem Land außerhalb der EU/des EWR?

Als Cloud-Dienstanbieter von Workforce-Management Lösungen hat sich ATOSS als einer der führenden Anbieter im deutschen und europäischen Raum sowie auch international etabliert. Zu den Kunden von ATOSS gehören u.a. deutsche und europäische Behördenträger, aber auch europäische und international ansässige Finanz-, Handels, Logistik-, Industrieunternehmen sowie Unternehmen auf dem Gesundheits- und Dienstleistungssektor.

Bei der Zusammenstellung unserer Lizenzangebote und dem Design unserer Cloud Services gilt es diese Kundenerwartungen zu berücksichtigen. Insbesondere setzt ATOSS hierbei erfolgreich auf ausgewählte moderne Cloud-Technologien und namhafte Hosting-Service-Provider (Hyperscaler) mit global verfügbaren Diensten. Denn es ist uns ein strategisches Anliegen, die am Markt vorhandenen Innovationsmöglichkeiten und globalen Entwicklungen in neuartige Technologien für unsere Cloud Services und Kunden nutzbar zu machen. Dies vorausgesetzt, lassen sich internationale Übermittlungen nicht vollständig ausschließen.

Nachfolgend beschreiben wir die Hintergründe und Gesamtumstände:

ATOSS und deren verbundenen Unternehmen

Die Muttergesellschaft, ATOSS Software SE, ist ein bayrisches Unternehmen (München, Deutschland), das sich auf die Entwicklung und den Vertrieb von Cloud- -Softwarelösungen für Workforce Management (Arbeitszeitmanagement und Personaleinsatzplanung)spezialisiert hat. Zur ATOSS Gruppe gehören weitere Tochtergesellschaften innerhalb der EU, mit denen unsere Kunden Cloud-Service-Verträge nach lokalem Recht abschließen können (dann vertragsschließende ATOSS-Gesellschaft) oder die als Auftragsverarbeiter (z.B. Support Hotline, Consulting) unter dem Cloud-Service-Vertrag mit dem Kunden involviert sein können.

- ATOSS Unternehmen mit EU-Firmensitz, die unmittelbar dem EU-Datenschutzrecht unterliegen

ATOSS Kunden

Für EU-Kunden gilt direkt das EU-Datenschutzrecht. Da keine internationalen Übermittlungen im Direkt-Verhältnis zwischen ATOSS und dem EU-Kunden erfolgen, gelten für Weiterübermittlungen in der (Unter-)auftragskette die AVV-Bestimmungen.

Erlaubt ein **EU-Kunde seinem verbundenen Unternehmen im Drittstaat (Drittstaat-Unternehmen)** die Mitnutzung der ATOSS Cloud-Produkte (z.B. mandantenbasiert), bitten wir um frühzeitige Information. Denn das Drittstaat-Unternehmen ist sodann ein Datenimporteur und ATOSS ein Datenexporteur. Diese internationale Übermittlung sollte durch ein Privacy Addendum auf Basis von Standardvertragsklauseln und einer konkreten Drittstaat-Rechtsprüfung legitimiert werden.

Da unsere **internationalen Vertragskunden mit Firmensitz im Drittland** ebenfalls als Datenimporteure und ATOSS als Datenexporteur qualifiziert werden, sollten ATOSS und der Kunde diese internationalen Übermittlungen im Direkt-Verhältnis überprüfen und durch ein Privacy Addendum auf Basis von Standardvertragsklauseln und der Berücksichtigung des Rechts im Drittstaat legitimieren.

ATOSS Unterauftragsverarbeiter

Für unsere EU-Kunden ist mithin nur die Bewertung einer internationalen (Weiter-)übermittlung im Lichte der Unterauftragskette von Relevanz.

In Betracht kommen solche Unterauftragsverarbeiter, welche moderne Cloud-Technologien zur Erbringung ihrer Leistungen im Unterauftrag erbringen.

Welche Unterauftragsverarbeiter von ATOSS sind als Datenimporteure zu qualifizieren? Welche nicht und wie ist das jeweils zu begründen?

Unser Cloud Productportfolio folgt dem Ansatz einer Multi-Skalierung. Dazu gehört auch, die zeitgleiche Nutzung verschiedener Service-Hosting-Provider für unsere Cloud Services und Service-Komponenten.

Im Einzelnen:

Telekom Deutschland GmbH

ATOSS hat die Telekom Deutschland GmbH (kurz: "Telekom") als einen Hosting-Service-Provider für die Bereitstellung und den Betrieb von Cloud Infrastrukturen und damit zusammen-hängenden Supportleistungen beauftragt. Die Telekom ist unserer Kenntnis nach nicht als Datenimporteur zu klassifizieren.

Data Hosting
Das Data Hosting erfolgt in Rechenzentren der Telekom und ihrer Unterauftragsverarbeiter, EU. Die Telekom behält sich das Recht vor, die Standorte ihrer Rechenzentren jederzeit innerhalb der EU-Region zu ändern.

Datenverarbeitungen
Gemäß Auftragsverarbeitungsvereinbarung mit der Telekom finden Datenverarbeitungen außerhalb der EU nicht statt.

Zertifikate und Sicherheitsmaßnahmen
Link - https://geschaeftskunden.telekom.de/hilfe-und-service/downloads/zertifikate
Link - https://www.qbeyond.de/auszeichnungen-zertifikate/

UMB AG

ATOSS hat die UMB AG (kurz: "UMB") als einen Hosting-Service-Provider für die Bereitstellung und den Betrieb von Cloud Infrastrukturen und damit zusammen-hängenden Supportleistungen beauftragt. Die UMB ist unserer Kenntnis nach nicht als Datenimporteur zu klassifizieren.

Data Hosting
Das Data Hosting erfolgt in Rechenzentren der UMB und ihrer Unterauftragsverarbeiter, Schweiz. Die UMB behält sich das Recht vor, die Standorte ihrer Rechenzentren jederzeit innerhalb der Schweiz-Region zu ändern.

Datenverarbeitungen
Gemäß Auftragsverarbeitungsvereinbarung mit der UMB finden Datenverarbeitungen außerhalb der Schweiz, der EU und des EWR nicht statt.

Zertifikate und Sicherheitsmaßnahmen
Link: https://www.umb.ch/unternehmen/vision-mission
Auf Wunsch können wir für Schweizer Kunden jederzeit entsprechende Kopien der Sicherheitszertifikate vorlegen.

Google Ireland Ltd.

Bei Lizenzierung unserer ATOSS Mobile Apps, ATOSS Staff Center (Mobile) und ATOSS Time Control (Mobile) ist eine Technologie enthalten, die sicherstellen soll, dass Google Ireland Ltd. (kurz: „Google“) keine Daten-verarbeitungstätigkeiten in Bezug auf personenbezogene Daten durchführt, auch wenn ATOSS weiterhin bestimmte Cloud Services von Google für die Bereitstellung des ATOSS (Mobile) Push Notification Service nutzt. Google ist unserer Kenntnis nach nicht als Datenimporteur zu klassifizieren.

Der ATOSS (Mobile) Push Notification Service ermöglicht es dem Kunden, eine automatische Push-Benachrichtigung an die Nutzer der ATOSS Mobile Apps zu senden, z.B. "Ein neuer Urlaubsantrag wartet auf Genehmigung". Dieser Service muss vom Kunden explizit eingerichtet werden. Wird dieser ATOSS (Mobile) Push Notification Service vom Kunden nicht eingerichtet, wird keine Push-Nachricht versendet. Darüber hinaus kann der Empfang von Push-Nachrichten durch den einzelnen Nutzer des mobilen Endgerätes jederzeit zugelassen oder blockiert werden. Die in solchen Push-Nachrichten enthaltenen Informationen werden ausschließlich über eine sichere Verbindung (https) mit einem zusätzlichen symmetrischen Verschlüsselungs-verfahren zwischen der ATOSS Mobile App auf dem Endgerät des Nutzers und der ATOSS Staff Efficiency Suite/ATOSS Startup Edition bzw. ATOSS Time Control übertragen.

Dies bedeutet, dass Google nicht an der Übertragung der in den Push-Nachrichten enthaltenen personenbezogenen Daten beteiligt ist. Dennoch muss sich die ATOSS Staff Efficiency Suite/ATOSS Startup Edition bzw. ATOSS Time Control gegenüber einem Messaging Backend Server authentifizieren, um Push-Benachrichtigungsanfragen an mobile Endgeräte zu senden. Durch eine spezielle technische Implementierung konnte ATOSS sicherstellen, dass bei der erforderlichen Authentifizierung unter Verwendung des Google Firebase Cloud Messaging keine personenbezogenen Daten verarbeitet werden. Die Authentifizierung erfolgt mittels eines individuellen Tokens/Schlüssels (Firebase Token), der durch die Einbindung von Google Firebase Cloud Messaging generiert wird. Dieser Firebase Token dient ausschließlich als Signal/Trigger an die ATOSS Mobile App, um den aktuellen Status der Push-Nachricht direkt über die Datenbank der ATOSS Staff Efficiency Suite/ATOSS Startup Edition bzw. ATOSS Time Control abzufragen.

Weitere Informationen kann Ihnen Ihr Key Account Manager auf Anfrage in einem Auditbericht einer unabhängigen Sicherheitsberatung zur Verfügung stellen.

Hinweis: Für den ATOSS Time Control (Mobile) Push Notification Service wurde kein Audit durchgeführt, da die Implementierung und Nutzung von Google Cloud Messaging identisch ist.

Microsoft Ireland Ltd.

ATOSS hat Microsoft Ireland Ltd. (kurz: "Microsoft") als einen Hosting-Service-Provider für die Bereitstellung und den Betrieb von Cloud Infrastrukturen und damit zusammenhängenden Supportleistungen beauftragt. Microsoft ist unserer Kenntnis nach vorliegend als Datenimporteur zu klassifizieren.

Data Hosting

Microsoft bietet Rechenzentren in wählbaren Regionen weltweit an. Bei der Auswahl von Rechenzentren für Kunden berücksichtigt ATOSS die konkreten Umstände (z.B. das Vorliegen eines Angemessenheitsbeschlusses o.ä.) und wählt bevorzugt Rechenzentrumsregionen aus, die nahe am Standort des Kunden liegen, um damit die Leistungsfähigkeit und Servicequalität sicherzustellen. Für EU-Kunden (ohne verbundene Drittstaats-Unternehmen) wählen wir somit sinnvollverweise und in der Regel verfügbare georedundante MS Azure Regionen innerhalb der EU/des EWR und der Schweiz aus. Microsoft behält sich das Recht vor, die konkreten Standorte ihrer Rechenzentren jederzeit innerhalb der vereinbarten MS Azure Regionen zu ändern. Informationen zu den MS Azure Rechenzentrumsregionen finden Sie hier: What are Azure regions?

Zertifikate und Sicherheitsmaßnahmen

Link: https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-c5-germany?view=o365-worldwide

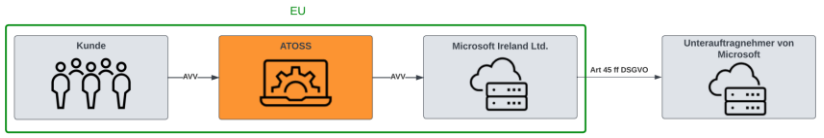
Link: https://servicetrust.microsoft.com/ViewPage/AllDocumentsA

Datenverarbeitungen

Gemäß Auftragsverarbeitungsvereinbarung mit Microsoft gilt das Microsoft Products and Service Data Protection Addendum (DPA), öffentlich abrufbar hier: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Nach aktuellen Informationen von Microsoft können folglich bestimmte Datenverarbeitungsaktivitäten außerhalb der EU auch durch (Unter-)unterauftragsverarbeiter von Microsoft durchgeführt werden.

Abbildung 1



Link - Microsoft Allgemein - Liste der Unterprozessoren für Online-Dienste

In der Regel erfordern die meisten Cloudoperationen, der Support und die Fehlerbehebung im Rahmen von Standardbetriebsverfahren, die von Microsoftpersonal und seinen Unterauftragsverarbeitern durchgeführt werden, keinen Zugriff auf personenbezogene Daten, die auf der Cloud-Instanz des Kunden und den damit verbundenen technischen Diensten verarbeitet werden.

Microsoft kann jedoch nicht ausschließen, dass unter besonderen Umständen ein Microsoft-Supporttechniker aus der Ferne auf Daten zugreifen muss, sei es als Reaktion auf ein von ATOSS Cloud-Experten initiiertes Support-Ticket oder auf ein von Microsoft identifiziertes Problem.

Für solche Fälle bietet die „Kunden-Lockbox für Microsoft Azure“ ein besonderes Feature, um Datenzugriffsanfragen von Microsoftpersonal durch unsere ATOSS Cloud-Experten zu prüfen und zu genehmigen oder abzulehnen. Zu Überwachungszwecken werden die Zugriffsanfragen sowie die von Microsoftpersonal durchgeführten Aktionen in den Aktivitätsprotokollen über diese Kunden-Lockbox protokolliert. Bitte beachten Sie die Erklärungen und zusätzliche Informationen von Microsoft zur **Kunden-Lockbox für Microsoft Azure**.

Hat ATOSS die "Kunden-Lockbox für Microsoft Azure“ im Standard aktiviert?

Ja, das ist zutreffend. Folglich profitieren alle ATOSS Cloudkunden von dieser zusätzlichen Zugriffsüberwachung bezogen auf Datenverarbeitungen von Microsoft.

ATOSS Zusatzvereinbarung <EU Data Boundary>

Für EU-Kunden (ohne verbundene Drittstaat-Unternehmen) bietet ATOSS auf Anfrage eine sog. EU-Datengrenze für das Data Hosting per Vertragszusatz an. Dabei wird die sog. <EU Data Boundary> durch Microsoft als eine geographische Grenze definiert, innerhalb derer sich Microsoft verpflichtet hat, personenbezogene Daten zu speichern und zu verarbeiten, wobei unter besonderen Umständen Daten auch außerhalb der EU Data Boundary weiterverarbeitet werden können. Bitte beachten Sie die Erklärungen und zusätzliche Informationen von Microsoft zur **EU-Datengrenze**.

In unserem ATOSS Vertragszusatz zur EU Data Boundary geben wir Ihnen die vertragliche Bestätigung, dass wir nur Rechenzentrumsregionen gemäß Microsoft EU-Datengrenze auswählen und die Kunden-Lockbox für Microsoft Azure im Standard aktiviert ist. Die Option „EU Data Boundary“ bieten wir für die folgenden Cloud Produkte an; ATOSS Time Control Cloud-Produkte sind ausgeschlossen:

- ATOSS Staff Efficiency (ASES) CLOUD24/7
- ATOSS Startup Edition (ASE) CLOUD 24/7
- ATOSS Staff Efficiency (ASES) Cloud Solution
- ATOSS Startup Edition (ASE) Cloud Solution
- Identity and Access management (IAM) Service

Bitte stimmen Sie die Details und ggf. weiteren Lizenzkosten mit Ihrem Key Account Manager ab

Kategorien der betroffenen Personen und Daten

Die DSGVO gilt nur für personenbezogene Daten und betrifft somit ausschließlich natürliche Personen. Im Workforce-Management sind dies Beschäftigte, Beamtinnen und Beamte, Anwärterinnen und Anwärter der Länder, Tarifbeschäftigte, Auszubildende sowie weitere vom Kunden berechtigte Nutzer der Cloud Produkte.

Welche konkreten Kategorien von personenbezogenen Daten werden in den ATOSS Cloud Produkten verarbeitet?

Unsere AVV enthält in AVV-Anhang I eine sehr detaillierte Liste der typischerweise zu verarbeitenden Datenkategorien die Kunden bei der Nutzung der Cloud Produkte innerhalb der Standardfunktionen und im Rahmen der typischen geschäftlichen Zwecke für Zeit- und Anwesenheits-management, Schichtmanagement und Personalplanung verarbeiten lassen können.

Hinweis: Unsere flexibel konfigurierbaren Lösungen ermöglichen es Kunden, über ihre Key User selbst zu steuern, welche Datenkategorien verarbeitet werden – abhängig von der Modulwahl und den kundenindividuellen Konfigurationen. Alle Funktionen werden in der technischen Dokumentation beschrieben. Diese Dokumentation wird per technischer Online-Hilfe mitgeliefert und von ATOSS aktuell gehalten.

Verarbeitet ATOSS sensible personenbezogenen Daten im Sinne des Art 9 DSGVO?

Wie zuvor erläutert, hängt die Auswahl und Sensibilität der Datenkategorien maßgeblich von der Kundenkonfiguration ab. Unsere Sicherheitsvorkehrungen ermöglichen die Verarbeitung sensibler Daten (siehe AVV-Anhang I).

Sollten Sie produktspezifische Informationen benötigen, kontaktieren Sie jederzeit gerne Ihren Key Account Manager.

Zu welchen Zwecken werden personenbezogene Daten des Kunden verarbeitet?

Unsere AVV enthält in AVV-Anhang I die Beschreibung der Zwecke für die beauftragten Auftragsverarbeitungen.

Schritt 2 Identifizieren Sie die Übermittlungsinstrumente, auf die Sie sich verlassen

Liegt ein Drittstaatentransfer vor, dürfen personenbezogene Daten an Empfänger in Drittländer übermittelt werden, wenn die EU-Kommission ein angemessenes Schutzniveau bestätigt hat. Falls das Drittland keinen Angemessenheits-beschluss besitzt, sind alternative Übermittlungsinstrumente, wie Standardvertragsklauseln und zusätzlich implementierte Sicherheitsmaßnahmen zu prüfen, um gleichwohl ein angemessenes Datenschutzniveau bejahen zu können.

Prüfpunkte im Überblick:

- ✓ Angemessenheitsbeschlüsse der EU-Kommission
- ✓ Einbezug von Standardvertragsklauseln
- ✓ zusätzlich implementierte Sicherheitsmaßnahmen

Berücksichtigt ATOSS die Angemessenheitsbeschlüsse der EU-Kommission und den Einbezug von Standardvertragsklauseln?

Die EU-Kommission kann Drittländer per Angemessenheitsbeschluss (Art. 45 DSGVO) als datenschutzkonform einstufen. Zusätzliche Garantien (Art. 46 (2) lit. c) DSGVO) sind dann nicht nötig. Die aktuelle Liste der Beschlüsse finden Sie auf der Website der EU-Kommission.

Schweiz (UMB AG)

Laut Kommissionsbeschluss wird ein angemessenes Schutzniveau in der Schweiz gewährleistet und personenbezogene Daten können dorthin übermittelt und gespeichert werden, ohne dass zusätzliche Garantien erforderlich sind. Die Entscheidung ist relevant für das Data Hosting und Auftragsverarbeitungen durch die UMB AG.

USA (Microsoft Ireland Ltd)

Seit 10. Juli 2023 bescheinigt das EU-U.S. Data Privacy Framework den USA ein angemessenes Datenschutzniveau, vorausgesetzt U.S.-Unternehmen haben sich entsprechend zertifiziert. Microsoft US-Entitäten, die von der Datenschutz-Framework -Zertifizierung abgedeckt sind finden Sie über die Microsoft-Website: https://www.microsoft.com/de-de/privacy/entity-list-adhering-to-privacy-shield

Die aktiven Unternehmens-Zertifikate für Microsoft finden Sie auf der Data Privacy Framework Liste: https://www.dataprivacyframework.gov/list

Weltweit (Microsoft Ireland Ltd.)

In unseren Cloud Produkten gibt es vielfältige Komponenten, die teils regional oder global und teils unterschiedlich konfiguriert sind. Für wesentliche Cloud-Komponenten, wie etwa Datenbanken, NetAPP Files, nutzen wir sog. georedundante Speicher (Geo-redundant storage -GRS) innerhalb von Microsoft Azure. So sind Ihre Kundendaten vor lokalen Standortausfällen geschützt und die Datensicherung kann mit den hohen Anforderungen an die Cloud-Verfügbarkeit, Informationssicherheit und Notfallwiederherstellung kombiniert werden. Bitte beachten Sie die online verfügbaren Microsoft Informationen - Link: https://learn.microsoft.com/en-us/azure/storage/files/files-redundancy#redundancy-in-a-secondary-region

Entsprechend der Rechtslage haben ATOSS und Microsoft die geltenden Standardvertragsklauseln (SCC) abgeschlossen. Zugleich hat sich Microsoft verpflichtet, auch bei einem Einsatz von weiteren Unter-Unterauftragsverarbeitern diese SCC für Verarbeitungstätigkeiten außerhalb der EU abzuschließen. Die online verfügbaren SCC von Microsoft finden Sie im Link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Erläuterungen zu den Zertifikaten und zusätzlich implementierten Sicherheitsmaßnahmen finden Sie in den vorherigen Abschnitten auf den Seiten 12 ff.

Schritt 3 Bewerten Sie, ob das Übermittlungsinstrument in Anbetracht aller Umstände der Übermittlung wirksam ist

In einem dritten Schritt soll geprüft werden, ob die geltenden Rechtsvorschriften und / oder Praktiken des Drittlandes die Wirksamkeit des verwendeten Übermittlungsinstrumentes beeinträchtigen. Relevant sind vorliegend internationale Rechenzentren, die globalen Service-Komponenten und internationalen Weiterübermittlungen von Microsoft.

Im Einzelnen:

Weltweit (Microsoft Ireland Ltd.)

Bitte beachten Sie die online verfügbare Microsoft Defending your Data Initiative– Link: https://news.microsoft.com/de-de/datenschutz-wie-wir-unsere-kundendaten-nach-dem-schrems-ii-urteil-schuetzen/

Bitte beachten Sie das online verfügbare Microsoft DPA mit Anhang C (zusätzliche Schutzmaßnahmen). Microsoft bestätigt ein positives Transfer Impact Assessment und sieht keine rechtlichen Hindernisse für die Erfüllung der vertraglichen Verpflichtungen und SCC. - Link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Bitte beachten Sie die online verfügbaren Microsoft Privacy Principles – Link: Data Protection with Microsoft Privacy Principles | Microsoft Trust Center

Bitte beachten Sie das online verfügbare Microsoft Whitepaper – Compliance with EU transfer requirements – Link: Working white paper remake 029 FNL (microsoft.com)

Bitte beachten Sie die online verfügbaren Microsoft Security Fundamentals für Azure Kunden: https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data

Schritt 4 Identifizieren und ergänzen Sie zusätzliche Maßnahmen, wo erforderlich

Nur wenn die Bewertung ein unzureichendes Datenschutzniveau ergibt, sind zusätzliche Maßnahmen erforderlich. Reichen diese nicht aus, muss die Übermittlung laut EDSA ausgesetzt werden.

Nach umfassender interner Bewertung durch ATOSS gewährleisten die bestehenden Sicherheitsmaßnahmen aus unserer subjektiven Sicht ein angemessenes Schutzniveau, was zugleich durch Sicherheitszertifikaten und unabhängigen Prüfreporten objektiv belegt ist.

Schritt 5 Ergreifen Sie formale Verfahrensschritte, wenn Sie zusätzliche Maßnahmen ermittelt haben

Der fünfte Schritt umfasst alle nötigen Verfahren zur Sicherstellung einer angemessenen Garantie nach Art. 46 DSGVO. Zusätzliche Sicherheitsmaßnahmen müssen also DSGVO-konform sein.

Das ATOSS ISO27001- Zertifikat für die Cloud Services finden Sie zum Download auf unsere Website https://www.atoss.com/de/sicherheit.
Zugleich kann Ihnen Ihr Key Account Manager auf Anfrage einen DSGVO-Report übermitteln.
Die aktiven U.S Unternehmens-Zertifikate von Microsoft finden Sie auf der Data Privacy Framework Liste: https://www.dataprivacyframework.gov/list.

Schritt 6 Führen Sie eine Neubewertung in angemessenen Abständen durch

Der sechste und letzte Schritt besteht darin, das Datenschutzniveau in angemessenen Abständen neu zu bewerten und zu überwachen. ATOSS wird die Dokumentenangaben regelmäßig überprüfen, um sicherzustellen, dass unsere Kunden in der Lage sind, ihre Transfer Impact Assessments effektiv durchzuführen. Wir behalten daher uns vor, diese Inhalte von Zeit zu Zeit zu ändern und Änderungen nachzupflegen.