Durchführung von

Transfer Impact Assessments

v. 01-2024

Dieses Dokument dient ausschließlich zu Informationszwecken.
Es fasst Informationen über die aktuellen Angebote der Produkte von der ATOSS Software AG und ihren verbundenen Unternehmen (nachfolgend "ATOSS") zusammen, die von Zeit zu Zeit geändert und aktualisiert werden können.
Die aktuelle Version dieses Dokuments steht in unserer ATOSS Kundenlounge (ATOSS Kundenlounge) zum Download bereit (siehe Abschnitt "Datenschutz").

Die Ausführungen in diesem Dokument begründen keine verbindlichen Zusagen, Zusicherungen oder Gewährleistungen von ATOSS und ihren Unterauftragsverarbeitern oder Lizenzgebern. Überdies ersetzen sie keine (datenschutz)rechtliche Beratung des Kunden. Es gelten die Angaben in den Vertragsunterlagen in Bezug auf das konkrete ATOSS Produkt.

Ungeachtet dessen möchte ATOSS den Kunden auf relevante Informationen zur Durchführung einer Transfer-Folgenabschätzung (nachfolgend: Transfer Impact Assessments - kurz: "TIA") für ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services im Lichte des "Schrems II"-Urteils des Gerichtshofs der Europäischen Union und der Empfehlungen des Europäischen Datenschutzausschusses (kurz: "EDSA") hinweisen. Siehe dazu EDSA-Empfehlungen.

Hinweis zur Geschlechterneutralität: Die gewählten Formulierungen gelten uneingeschränkt für die weiteren Geschlechter.

Vorwort – Die Verantwortlichkeit bei der Datenübermittlung

Die Datenschutz-Grundverordnung ("DSGVO") dient dazu, in der EU ein einheitliches Datenschutzniveau zu gewährleisten. Daher gibt es bestimmte Voraussetzungen, die erfüllt werden müssen, wenn Daten außerhalb der EU verarbeitet werden sollen. Im Falle von Datenverarbeitungen außerhalb der EU (sog. Drittstaatentransfers) ist ein Transfer Impact Assessment in Bezug auf die Nutzung von ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services, die personenbezogene Daten verarbeiten, durchzuführen.

Eine Transfer-Folgenabschätzung identifiziert und bewertet das Datenschutzniveau und ggf. zusätzliche Garantien gemäß Art. 46 DSGVO, soweit ein Angemessenheitsbeschluss der EU-Kommission nicht vorliegt.

Wie der Europäische Datenschutzausschuss (kurz: "EDSA") zusammenfasst (vgl. EDSA-Empfehlungen), ist das Recht auf Datenschutz ein Grundrecht des Einzelnen, das angemessene Garantien vorsieht, um den Kern dieses Rechts zu wahren.

Die Datenverarbeitung muss daher verhältnismäßig und notwendig sein und tatsächlich den von der Europäischen Union anerkannten Zielen des Allgemeininteresses oder der Notwendigkeit, die Rechte und Freiheiten anderer zu schützen, entsprechen. Das Recht auf den Schutz personenbezogener Daten ist jedoch kein absolutes Recht. Es muss immer im Verhältnis zu seiner Funktion betrachtet und gemäß dem Grundsatz der Verhältnismäßigkeit abgewogen werden.

Da solche Abschätzungen rechtliche Interpretationen und Analysen beinhalten, kann ATOSS seinen Kunden hierzu keine Rechtsberatung anbieten. Ungeachtet dessen möchten wir unseren Kunden eine Hilfestellung bei der Durchführung eines Transfer Impact Assessment für ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services im Lichte des "Schrems II"-Urteils des Gerichtshofs der Europäischen Union und der Empfehlungen des EDSA bieten und in diesem Whitepaper auf relevante Informationen hinweisen.

In Anlehnung an die Empfehlungen des EDPB bietet sich ein Transfer Impact Assessment in den folgenden sechs Schritten an:

Schritt 1 Kennen Sie Ihre Datenübermittlungen

In diesem Schritt sollen alle Übermittlungen von personenbezogenen Daten des Kunden erfasst werden. Die Erfassung, wohin die personenbezogenen Daten übermittelt werden, wird als notwendig angesehen, um sicherzustellen, dass überall dort, wo diese personenbezogenen Daten verarbeitet werden, ein im Wesentlichen gleichwertiges Datenschutzniveau gewährleistet ist.

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

Ein zweiter Schritt besteht darin, zu überprüfen, ob ein Übermittlungsinstrument, welches eine geeignete Garantie nach Kapitel V der DSGVO darstellt, vorliegt.

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 Übermittlungsinstrumente beeinträchtigen.

Schritt 4 Identifizieren und ergänzen Sie zusätzliche Maßnahmen, wo erforderlich

Ein vierter Schritt ist die Ermittlung von zusätzlichen Garantien und deren Erforderlichkeit, um das Datenschutzniveau der übermittelten personenbezogenen Daten auf den geltenden EU-Standard anzuheben, soweit ein Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO) nicht vorliegt.

Dieser Schritt ist nur notwendig, wenn Ihre Bewertung ergibt, dass die Rechtsvorschriften und / oder Praktiken des Drittlandes die Wirksamkeit eines Übermittlungsinstruments nach Art. 46 DSGVO beeinträchtigen.

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

Ein fünfter Schritt besteht darin, alle formalen Verfahrensschritte zu unternehmen, die Ihrer Annahme nach erforderlich sind, um eine angemessene Garantie nach Art. 46 DSGVO zu erhalten.

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

In diesem Schritt sollen alle Übermittlungen von personenbezogenen Daten des Kunden erfasst werden. Die Erfassung, wohin die personenbezogenen Daten übermittelt werden, wird als notwendig angesehen, um sicherzustellen, dass überall dort, wo diese personenbezogenen Daten verarbeitet werden, ein im Wesentlichen gleichwertiges Datenschutzniveau gewährleistet ist.

Beteiligte und Rollen bei der Auftragsverarbeitung

Welche Rolle hat der Kunde im Zusammenhang mit der Verarbeitung und Übermittlung seiner personenbezogenen Daten an ATOSS?	Im Sinne der DSGVO ist der Kunde der "**Verantwortlicher**". Soweit der Kunde seinen verbundenen Unternehmen die Nutzung der lizenzierten ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services gestattet, werden seine verbundenen Unternehmen bei der Nutzung der ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services für deren personenbezogene Daten ebenfalls zu "Verantwortlichen". Der Kunde bleibt nach ATOSS Vertrag alleiniger Vertragspartner und damit einziger Ansprechpartner für ATOSS. Dies gilt nicht nur für die eigenen Interessen des Kunden, sondern auch für die seiner verbundenen Unternehmen, die die ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services ebenfalls für ihre personenbezogenen Daten nach Maßgabe des jeweiligen Vertrages nutzen dürfen. Weitere Einzelheiten finden Sie in der Präambel der ATOSS AVV, die auf unserer Website um Download bereitsteht.
Welche Rolle haben ATOSS und die von ATOSS beauftragten Unternehmen im Zusammenhang mit der Verarbeitung und Übermittlung von personenbezogenen Daten des Kunden?	ATOSS und die von ATOSS beauftragten Unternehmen sind "**Auftragsverarbeiter**" des Kunden. Das Gleiche gilt in Bezug auf die verbundenen Unternehmen des Kunden, wenn diese ebenfalls die ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services für ihre personenbezogenen Daten nutzen. ATOSS ist dabei der direkte Vertragspartner des Kunden und damit ein **Auftragsverarbeiter auf erster Stufe**. Daneben ist ATOSS befugt, weitere Unternehmen, die Hilfsdienste im Fall eines ATOSS Cloud Services zu erbringen, einzusetzen. Diese von ATOSS 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 Unterauftragsverarbeiter von ATOSS finden Sie im AVV-Anhang III der AVV, die auf unserer Website um Download bereitsteht.

Ergänzende Hinweise zur Liste der Unterauftragsverarbeiter von ATOSS

Als europäischer Anbieter von HR-Workforce-Management Lösungen setzt ATOSS auf namhafte Unterauftragsverarbeiter, die Hilfsdienste im Fall eines ATOSS Cloud Services erbringen. Der Einsatz dieser Unterauftragsverarbeiter dient dazu, die ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services im Lichte einer DSGVO-Konformität, nach Stand der Technik und nach einem Best-of-Breed-Ansatz sowie unter Reduzierung eines Vendor-Lock-in im Rahmen einer Multi-Scaler-Strategie für unsere Kunden bereitzustellen.
Unter Multi-Scale verstehen wir, dass ATOSS zwischen den in dem AVV-Anhang III aufgeführten Unterauftragsverarbeitern auswählen und wechseln kann, da die Unterauftragsverarbeiter bereits während der Verarbeitung personenbezogener Daten durch den Kunden beauftragt sind. ATOSS behält sich das Recht vor, nicht jeden der in AVV-Anhang III aufgeführten Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten einzusetzen.

Was ist der Vorteil der ATOSS Multi-Scaler-Strategie für ATOSS Cloudkunden?

- Diese ermöglicht den Aufbau und Betrieb einer IT-Cloud-Infrastruktur auf dem neuesten Stand der Technik, die u.a. aus modernen Applikationsservern & Container-Orchestrierungsclustern, georedundanten Backup- und Disaster-Recovery-Services sowie einem Servermanagement & System-monitoring durch IT-Experten und Spezialisten besteht.
- Hierdurch können zertifizierte Hochsicherheits-Rechenzentren nach internationalen Standards (z.B. DIN EN ISO/IEC 9001, DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27017, DIN EN ISO/IEC 27018) genutzt werden.

Übermittelt ATOSS personenbezogene Daten des Kunden an einen von ATOSS direkt beauftragten Unterauftragsverarbeiter mit registriertem Firmensitz außerhalb der EU?

Wie Sie dem AVV-Anhang III entnehmen können, haben alle ATOSS-Gesellschaften und alle Unterauftragsverarbeiter, mit denen ATOSS Unterverträge abgeschlossen hat, derzeit ihren registrierten Sitz innerhalb der EU oder der Schweiz. Den AVV-Anhang III finden Sie in unserer AVV, die auf unserer Website um Download bereitsteht.

Insbesondere die von ATOSS beauftragten Unterauftragsverarbeiter, die Hilfsdienste im Fall eines ATOSS Cloud Services erbringen, haben ihren angemeldeten Firmensitz entweder innerhalb der EU und unterliegen damit direkt dem Geltungsbereich der DSGVO und der Aufsicht der europäischen Datenschutzbehörden oder unterliegen dem reformierten Schweizer Datenschutzgesetz.

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

Mit Abschluss des ATOSS Vertrags erteilt der Kunde ATOSS die generelle Erlaubnis für den Einsatz aller in AVV-Anhang III gelisteten Unterauftragsverarbeiter. Zugleich behält sich ATOSS das Recht vor, nicht jeden der dort aufgeführten Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten einzusetzen. Unter Berücksichtigung von Kapazitäts- und Ressourcenplanungen, wird ATOSS den Einsatz der Unterauftragsverarbeiter auf das für die Leistungserbringung erforderliche Maß beschränken. Dementsprechend kann ATOSS während des Zeitraums der

	Verarbeitung der personenbezogenen Daten des Kunden jederzeit nach eigenem Ermessen zwischen den gelisteten Unterauftragsverarbeitern auswählen und wechseln.
Kann der Kunde die Liste der genehmigten Unterauftragsverarbeiter auf eine individuelle Auswahl von Unterauftragsverarbeitern beschränken?	Eine Löschung oder Beschränkung auf bestimmte Unterauftragsverarbeiter von ATOSS durch den Kunden ist nicht möglich. ATOSS möchte seine ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services stets bestmöglich für den Kunden gestalten, wozu – nicht nur im Interesse der Ressourcen– und Kapazitätsplanung –, sondern auch die Vermeidung von vermeintlichen Sicherheitsgefahren wie bei einem Vendor Lock-in gehört. Gleichzeitig kann ATOSS seine hohe Innovationskraft nur erhalten und ausbauen, wenn ATOSS seine Produkte und Dienstleistungen nach dem Best-of-Breed-Ansatz ausrichtet und mit diversen Unterauftragsverarbeitern kooperiert, die ATOSS über die gesamte Vertragslaufzeit des Kunden mit ausgewählten Technologien versorgen. Mit Blick auf die Servicequalität und unser vertragliches Versprechen zu kontinuierlichen Anpassungen braucht ATOSS daher die Flexibilität, um seinen Kunden stets hervorragende Leistungen anbieten zu können.
Wie wählt ATOSS seine Unterauftragsverarbeiter aus?	Jeder Unterauftragsverarbeiter von ATOSS wird vor Aufnahme der Verarbeitungstätigkeiten schriftlich verpflichtet, die gleichen, d.h. inhaltlich mindestens gleichwertige Datenschutzverpflichtungen einzuhalten, wie sie in der ATOSS AVV mit dem Kunden vereinbart sind. Die Unterauftragsvereinbarung muss dabei mindestens das in der AVV zwischen ATOSS und dem Kunden geforderte Datenschutzniveau gewährleisten. ATOSS legt zudem großen Wert darauf, dass alle Unterauftragsverarbeiter von ATOSS angemessene Sicherheits- und Datenschutzkriterien für ihre spezifischen Verarbeitungstätigkeiten gewährleisten. Dazu gehören in der Regel Sicherheitsmaßnahmen wie die verschlüsselte Datenübertragung und der durch Standardsicherheitsmechanismen pro Zugriffstiefe gesicherte Zugriff sowie der Einbezug von Vertraulichkeitsklauseln und den Nachweis von internationalen Zertifikaten.
Wo verarbeitet und speichert ATOSS die personenbezogenen Daten des Kunden im Falle der Nutzung der ATOSS Cloud Services?	ATOSS speichert und verarbeitet die personenbezogenen Daten des Kunden in den auf unserer Website angegebenen geographischen Regionen. - Link: Data Residency

Ist ATOSS bekannt, dass ATOSS Unterauftragsverarbeiter, die Hilfsdienste im Zusammenhang mit einem ATOSS Cloud Service erbringen, personenbezogene Daten des Kunden an andere (Unter-)Auftragsverarbeiter außerhalb der EU / des EWR übermitteln können?

ATOSS überprüft die Vereinbarungen mit seinen Unterauftragsverarbeitern regelmäßig. In Bezug auf die weiteren Verarbeitungstätigkeiten kann Folgendes zusammengefasst werden:

Telekom Deutschland GmbH:
ATOSS hat die Telekom Deutschland GmbH (kurz: "Telekom") als einen Hosting-Dienstleister für die Bereitstellung und den Betrieb von Cloudinfrastrukturen und damit zusammenhängenden Supportleistungen beauftragt.
Gemäß Auftragsverarbeitungsvereinbarung mit Telekom findet eine Datenverarbeitung durch Telekom und ihre (Unter-)Unterauftragsverarbeitern in Drittländern, d.h. Ländern außerhalb der EU, nicht statt.

Darüber hinaus verweisen wir auf die verschiedenen Zertifikate und Prüfberichte der Telekom zum Thema Cloud Privacy und Informationssicherheit.

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-Dienstleister für die Bereitstellung und den Betrieb von Cloud-infrastrukturen und damit zusammenhängenden Supportleistungen beauftragt.
Gemäß Auftragsverarbeitungsvereinbarung mit UMB dürfen die personenbezogenen Daten der Kunden nur an (Unter-)Unterauftragsverarbeiter weitergegeben werden, die innerhalb der EU, des EWR oder der Schweiz ansässig sind. Eine Datenverarbeitung in Drittländern, d.h. Ländern außerhalb der EU, oder des EWR oder der Schweiz findet somit nicht statt.

Auf Wunsch können wir für Schweizer Kunden jederzeit entsprechende Zertifikate ausstellen.

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 die Google Ireland Ltd. keine Datenverarbeitungstätigkeiten in Bezug auf personenbezogene Daten mehr durchführt, auch wenn ATOSS weiterhin bestimmte Cloud Services der Google Ireland Ltd. für die Bereitstellung des ATOSS (Mobile) Push Notification Service nutzt.

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 Verschlüsselungsverfahren 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 die Google Ireland Ltd. 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.

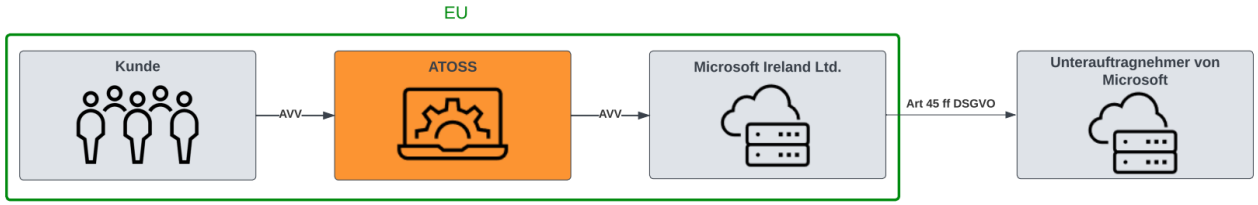
Weitere Informationen finden Sie in einem Auditbericht einer unabhängigen Sicherheitsberatung, die den Test explizit für den ATOSS Staff Center (Mobile) Push Notification Service durchgeführt hat. Für den ATOSS Time Control (Mobile) Push Notification Service wurde kein Audit durchgeführt, da die Implementierung und Nutzung von Google Cloud Messaging identisch ist. Der Auditbericht für den ATOSS Staff Center (Mobile) Push Notification Service steht unseren Kunden der ATOSS Staff Efficiency und ATOSS Startup Edition in der ATOSS Kundenlounge zur Verfügung oder kann Ihnen auf Anfrage jederzeit zugesandt werden.

Microsoft Ireland Ltd.

ATOSS hat Microsoft Ireland Ltd ("Microsoft") als Hosting Service Provider mit der Bereitstellung und dem Betrieb von Cloud-Infrastrukturen und damit verbundenen Supportleistungen beauftragt. In diesem Zusammenhang ist bekannt, dass Microsoft Rechenzentren in wählbaren Regionen weltweit anbietet. Im Sinne der DSGVO-Konformität kann ATOSS zum Vorteil der Kunden Rechenzentren in verschiedenen Regionen nutzen. Bei der Auswahl von Rechenzentren für Kunden berücksichtigt ATOSS die aktuellen Gegebenheiten (z.B. das Vorliegen eines Angemessenheitsbeschlusses o.ä.) und wählt in der Regel Rechenzentrumsregionen aus, die nahe am Standort des Kunden liegen und damit die Leistungsfähigkeit und Servicequalität sicherstellen sollen. Nach aktuellen Informationen von Microsoft können Datenverarbeitungsaktivitäten außerhalb der EU von (Unter-)Verarbeitern durchgeführt werden, die direkt von Microsoft beauftragt werden (siehe Abbildung 1).

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

Abbildung 1



Spezielle ATOSS Zusatzvereinbarung <EU Data Boundary> auf Kundenwunsch möglich

ATOSS ist in der Lage, auf Kundenwunsch die Vorteile des Microsoft <EU Data Boundary> Konzepts an den Kunden, der die ATOSS CLOUD24/7 lizenziert, weiterzugeben. Die <EU Data Boundary> wird von Microsoft als eine geographisch definierte Grenze definiert, innerhalb derer sich Microsoft verpflichtet hat, Daten zu speichern und zu verarbeiten, wobei unter bestimmten Umständen Daten auch außerhalb der EU Data Boundary weiterverarbeitet werden können.

Siehe Erklärungen und Dokumentation von Microsoft über die EU-Datengrenze.

Wesentliche Fakten zu den ATOSS CLOUD24/7-Angeboten mit EU Data Boundary Zusatzvereinbarung:

Soweit ergänzend vereinbart, wird ATOSS das Cloud Hosting und damit zusammenhängende Cloud Operation Services im Rahmen der Microsoft EU Data Boundary wie folgt anbieten:

- **ATOSS wählt standardmäßig Microsoft Rechenzentrumsregionen aus, die in <Europa> liegen.** Folglich werden personenbezogene Kundendaten in Europa gespeichert. Microsoft kann diese Daten in andere Rechenzentren in Europa replizieren, um die Datenresilienz zu verbessern. Microsoft speichert oder übermittelt jedoch diese Kundendaten nicht außerhalb Europas.

  Siehe Erklärungen und zusätzliche Informationen von Microsoft über die Data Residency in Azure.

- **ATOSS hat die zusätzliche Zugriffskontrolle namens "Microsoft Kunden-Lockbox" für Microsoft Azure Support Services aktiviert.** In der Regel erfordern die meisten Operationen, 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-Anwendungsinstanz des Kunden und den damit verbundenen technischen Diensten verarbeitet werden. Microsoft kann jedoch nicht ausschließen, dass unter besonderen Umständen ein Microsoft-Supporttechniker 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 Microsoft Customer Lockbox eine Schnittstelle, um Datenzugriffsanfragen von Microsoft-Mitarbeitern zu prüfen und zu genehmigen oder abzulehnen. Zu Überwachungszecken werden die von Microsoft-Mitarbeitern durchgeführten Aktionen in den Aktivitätsprotokollen über die Microsoft Kunden-Lockbox protokolliert.

  Siehe Erklärungen und zusätzliche Informationen von Microsoft zur Kunden-Lockbox für Microsoft Azure.

Beschreibung der Datenverarbeitungen

Was bedeutet "Verarbeitung personenbezogener Daten" im Sinne der DSGVO?	Datenverarbeitung beschreibt zunächst die allgemeine Verwendung von jeglichen Daten. Um die DSGVO zu interpretieren, muss jedoch der Begriff "**Verarbeitung personenbezogener Daten**" berücksichtigt werden. Die DSGVO gilt nicht für alle Daten, sondern nur für die spezielle Kategorie: "**personenbezogene Daten**". Die DSGVO versteht den Begriff "Verarbeitung personenbezogener Daten" sehr weit, so dass im Prinzip jede Nutzung personenbezogener Daten auch eine "Verarbeitung personenbezogener Daten" im rechtlichen Sinne ist. In diesem Sinne ist etwa eine Datenspeicherung und -übertragung zwischen verschiedenen Systemen und Anwendungen in einer von ATOSS oder dessen Unterauftragsverarbeitern technisch administrierten Cloudumgebung eine "Verarbeitung personenbezogener Daten". Zugleich ist darunter aber auch z.B. ein real-time Fernzugriff (z.B. in Supportsituationen) zu verstehen.
Welche Kategorien von personenbezogenen Daten verarbeitet ATOSS im Zusammenhang mit ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services?	Der AVV-Anhang I enthält die relevanten Informationen über die Datenkategorien von personenbezogenen Daten, die ATOSS verarbeiten und übermitteln darf. Die Auflistung der Datenkategorien beinhaltet dabei **exemplarisch** die typischen Datenkategorien, die typischerweise verarbeitet werden, soweit der Kunde die ATOSS Cloud Services innerhalb der Standardfunktionen und im Rahmen der typischen geschäftlichen Zwecke nutzt. Dazu gehören insbesondere geschäftliche Nutzungen für die Durchführung von Zeit- und Anwesenheitsmanagement, Schichtmanagement und Personalplanung. Ob eine dort aufgelistete Kategorie tatsächlich verarbeitet wird, hängt von der individuellen Auswahl der Module durch den Kunden und seinen eigenen Konfigurationen ab. Bitte beachten Sie, dass der Kunde seine Konfigurationen selbständig jederzeit ändern kann und damit die volle Kontrolle darüber hat, welche Datenkategorien tatsächlich verarbeitet werden. Der AVV-Anhang I finden Sie in unserer AVV, die auf unserer Website um Download bereitsteht.

Verarbeitet ATOSS sensible personenbezogenen Daten im Sinne des Art 9 DSGVO?	Da ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services prinzipiell hochgradig durch den Kunden parametrisierbar sind, hängt die Auswahl der Datenkategorien und deren Beschaffenheit von der Wahl der individuellen Konfigurationen des Kunden ab - vgl. Frage zuvor. Beispiel: Bei der Konfiguration der Einstellungen kann der Kunde entscheiden, "Informationen über geplante und tatsächliche Abwesenheiten" zu verarbeiten. Ob diese Informationen zu sensiblen Gesundheitsdaten werden, hängt davon ab, ob der Kunde statt einfacher "Abwesenheitsmeldungen" Buttons oder dienstliche Meldungen, z.B. mit dem Namen "Krankheit", erstellt, oder ob er Verknüpfungen zwischen der persönlichen Abwesenheit und anderen Daten, wie z.B. der Arbeitsunfähigkeitsbescheinigung wegen Krankheit o.ä., herstellt. Generell empfehlen unsere ATOSS Berater dem Kunden stets die Konfigurationen mit seinem internen oder externen Datenschutzbeauftragten zu klären. In den Standardfunktionen der ATOSS Module in der ATOSS Staff Efficiency Suite/ATOSS Startup Edition (ASE/S) kann der Kunde über die Konfiguration von sog. Abwesenheitscodes entscheiden. Diese vom Kunden frei wählbaren Abwesenheitscodes können mit den im Abrechnungssystem des Kunden bereits definierten Codes gemappt werden. Sollten Sie produktspezifische und kommerzielle Informationen zu unseren ATOSS Cloud Services benötigen, kontaktieren Sie jederzeit gerne Ihren zuständigen Account Manager
Zu welchen Zwecken werden personenbezogene Daten des Kunden übermittelt?	Relevante Informationen zu den Zwecken der Verarbeitungstätigkeiten innerhalb der ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services finden Sie in AVV-Anhang I. Dieser ist Bestandteil unserer AVV, die auf unserer Website zum Download bereitsteht.
Wird im Zuge der Nutzung der ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services eine Auftragsverarbeitungsvereinbarung (kurz: "AVV") abgeschlossen?	Eine AVV gemäß DSGVO ist immer Bestandteil eines schriftlich (auch in elektronischer Form als Teil des ATOSS-Angebots) abgeschlossenen Leistungsvertrages zwischen der vertragsschließenden ATOSS-Gesellschaft und dem Kunden. Unsere aktuelle AVV steht Ihnen auf unserer Website um Download bereit.

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

Ein zweiter Schritt besteht darin, zu überprüfen, ob ein Übermittlungsinstrument, welches eine geeignete Garantie nach Kapitel V (Art. 44 – 50) der DSGVO darstellt, vorliegt.

Folgende Übermittlungsinstrumente kommen in Bezug auf die ATOSS Cloud Services in Betracht:

Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO)	**Standardvertragsklauseln (Art. 46 Abs 2 lit c DSGVO)**	**Verbindliche Unternehmensdatenschutzvorschriften (Art. 47 DSGVO)**
☒	☒	☐
Einwilligung der betroffenen Person (Art. 49 lit a DSGVO)	**Sonstige außerordentliche Rückstellungen (Art. 49 DSGVO)**	**Weitere:**
☐	☐	☐

Kommen Angemessenheitsbeschlüsse der EU-Kommission (Art. 45 DSGVO) für Datenverarbeitungen in Betracht?

Die EU-Kommission ist befugt, auf der Grundlage von Art. 45 DSGVO zu entscheiden, ob ein Land außerhalb der EU (=Drittland) ein angemessenes Datenschutzniveau bietet. Der entsprechende Mechanismus hierfür ist der Erlass eines Angemessenheitsbeschlusses. Hat die EU-Kommission einen Angemessenheitsbeschluss erlassen, sind keine zusätzlichen geeigneten Garantien (Art. 46 DSGVO) im Hinblick auf Datenverarbeitungen in diesem Land erforderlich.

Bitte beachten Sie die Liste der Angemessenheitsbeschlüsse der EU-Kommission. Diese aktuelle Liste steht auf der Website der EU-Kommission zum Herunterladen bereit, wo Sie sich auch über Änderungen informieren können.

Wir möchten an dieser Stelle hervorheben, dass ATOSS und sämtliche von Unterauftragsverarbeiter, die ATOSS direkt beauftragt (vgl. AVV-Anhang III) ihren Firmensitz innerhalb der EU oder der Schweiz haben.

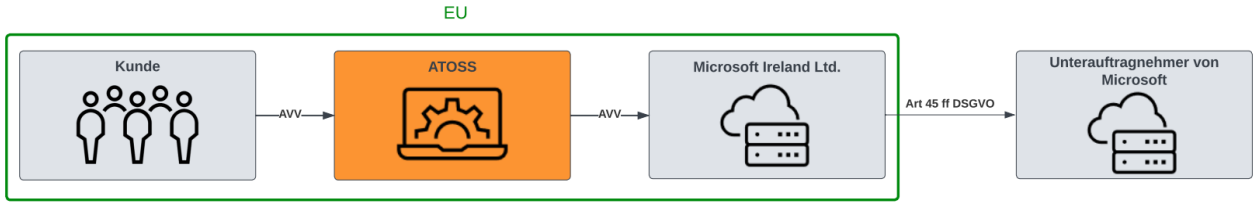
Die Schweiz ist zwar nicht Mitglied der Europäischen Union, allerdings liegt für die Schweiz ein Angemessenheitsbeschluss durch die EU-Kommission vor.

Das weitere Transfer Impact Assessment beschränkt sich auf Microsoft.

Nach aktuellen Angaben von Microsoft kann es zu Weiterverarbeitungen außerhalb der EU durch (Unter-)Unterauftragsverarbeiter, die Microsoft direkt beauftragt, kommen (siehe Abbildung 1).

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

Abbildung 2



Neubewertung in Bezug auf mögliche Datenverarbeitungen in die U.S.:

In Bezug auf die U.S. wurde am 10. Juli 2023 ein Angemessenheitsbeschluss - **das EU-U.S. Data Privacy Framework** – erlassen. Mit diesem Angemessenheitsbeschluss hat die EU-Kommission für die U.S. ein angemessenes Datenschutzniveau bescheinigt. Damit der Angemessenheitsbeschluss für U.S.-Unternehmen Anwendung findet, müssen sich diese entsprechend den Vorgaben des EU-U.S. Data Privacy Framework zertifizieren.
Welche Unternehmen zertifiziert sind, ist unter diesem offiziellen Link einzusehen.

Folgende Effekte ergeben sich durch das in Kraft getretene neue EU-U.S. Data Privacy Framework:

- Keine zusätzlichen Garantien nach Art. 46 DSGVO für zertifizierte U.S.-Unternehmen notwendig
- Keine Standardvertragsklauseln ("Standard Contractual Clauses" – kurz: "SCC") mit U.S.-Unternehmen notwendig
- Keine Durchführung eines umfassenden Transfer Impact Assessment bzgl. Datentransfers in die U.S. notwendig

Der neue Angemessenheitsbeschluss für die U.S. sorgt für die lang erwartete Rechtssicherheit. Diese bietet einen weiteren Vertrauensbaustein in die ATOSS Cloud Services und die Sicherheitsstrategie, die ATOSS zum Schutz und zur sicheren Verarbeitung Ihrer Daten mit technischen, vertraglichen und organisatorischen Maßnahmen getroffen hat.

Kommen weitere Übermittlungsinstrumente (Art. 46 DSGVO) für Datenverarbeitungen in Betracht?	Für Fälle, in denen kein Angemessenheitsbeschluss vorliegt, listet Art. 46 DSGVO mehrere Instrumente als sog. "**angemessene Garantien**" auf, die ebenfalls für die Übermittlung personenbezogener Daten in Länder außerhalb der EU verwendet werden können. Entsprechend der Rechtslage haben ATOSS und Microsoft schon vor dem Erlass des EU-U.S. Data Privacy Frameworks die geltenden **SCC** abgeschlossen. Somit ergibt sich aus der Entscheidung der EU-Kommission in Bezug auf das direkte Unterauftragsverhältnis zwischen ATOSS und Microsoft eine **doppelte Sicherheit** für ATOSS, da die Standardvertragsklauseln nach wie vor ihre Gültigkeit behalten. Zugleich ist Microsoft verpflichtet, SCC bei einem Einsatz von weiteren Unter-Unterauftragsverarbeitern von Microsoft für Verarbeitungstätigkeiten außerhalb der EU abzuschließen. • Bitte beachten Sie die von Microsoft online verfügbaren SCC – Link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

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

In einem dritten Schritt ist zu prüfen, ob die geltenden Rechtsvorschriften und / oder Praktiken des Drittlandes die Wirksamkeit des Übermittlungsinstrumente beeinträchtigen. Der Umfang dieser Bewertung soll sich auf die Vorschriften und Praktiken beschränken, die für den Schutz der spezifischen personenbezogenen Daten, die übermittelt werden, relevant sind. Im vorliegenden Fall muss sie sich auf Informationen zur Personalverwaltung, wie etwa Mitarbeiterdaten, konzentrieren.

An dieser Stelle möchten wir Sie auf die weiterführenden Informationen hinweisen, die von Microsoft veröffentlicht wurden.

Welche Informationen hat Microsoft in Bezug auf das Hosting und den Betrieb der Cloud-Infrastrukturen veröffentlicht?	Exemplarisch hervorzuheben sind die folgenden Microsoft Privacy Principles und weiterer Vorgehensweisen zum Datenschutz: • Bitte beachten Sie die von Microsoft online verfügbaren Privacy Principles – Link: Data Protection with Microsoft Privacy Principles | Microsoft Trust Center • Bitte beachten Sie das von Microsoft online verfügbare Whitepaper – Compliance with EU transfer requirements – Link: Working white paper remake 029 FNL (microsoft.com) • Bitte beachten Sie die von Microsoft online verfügbaren Datenschutzvorkehrungen für Azure Kunden https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data • Bitte beachten Sie die von Microsoft online verfügbaren Informationen zur Defending your Data Initiative– Link: https://news.microsoft.com/de-de/datenschutz-wie-wir-unsere-kundendaten-nach-dem-schrems-ii-urteil-schuetzen/ • Microsoft bestätigt allen Kunden, ein Transfer Impact Assessment durchgeführt zu haben und, dass das Ergebnis dieser Bewertung positiv ist. Danach habe Microsoft keinen Grund zu der Annahme, dass die geltenden Rechtsvorschriften, einschließlich in jedem Land, in das sie personenbezogene Daten übermitteln, es daran hindern, die vom Kunden seine Verpflichtungen aus dem Vertrag und den SCC zu erfüllen. Abschnitt 6 "Änderungsmitteilung" des Anhangs C des Datenschutznachtrags zu den Produkten und Services von Microsoft - Link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Schritt 4 Identifizieren und ergänzen Sie zusätzliche Maßnahmen, wo erforderlich

Ein vierter Schritt ist die Ermittlung und die Ergänzung zusätzlicher Maßnahmen, soweit diese erforderlich sind, um das Datenschutzniveau der übermittelten personenbezogenen Daten auf den geltenden EU-Standard anzuheben.

Zusätzliche technische und organisatorische Maßnahmen umgesetzt durch ATOSS

Welche zusätzlichen Maßnahmen gibt es im Zusammenhang mit der Datenverarbeitung der personenbezogenen Daten des Kunden durch ATOSS	ATOSS ist laut AVV verpflichtet, **angemessene technische und organisatorische Maßnahmen** zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten des Kunden zu treffen. Bitte beachten Sie unseren AVV-Anhang II in der ATOSS AVV, welche Ihnen auf unserer Website um Download bereit steht. Die **Bereitstellung und Betrieb von den ATOSS Cloud Services** werden regelmäßig auf die Einhaltung von Sicherheitspraktiken und Informationssicherheitsrichtlinien überprüft. Um den Erwartungen unserer Kunden gerecht zu werden, sieht ATOSS den Betrieb eines Informationssicherheitsmanagementsystems nach internationalen Standard DIN EN ISO/IEC 27001 für die ATOSS Cloud Services als eine substantielle Eigenverpflichtung an. Eine Kopie des Zertifikats ist jederzeit abrufbar auf der Website. In diesem Zusammenhang führt ATOSS zudem selbst sowie durch externe Sicherheitsdienstleister regelmäßige Tests und Sicherheitsscans durch. Darüber hinaus werden regelmäßig externe Audits unter Datenschutzgesichtspunkten durchgeführt. Weiterführende Informationen stehen Ihnen in unserer ATOSS Kundenlounge (siehe Rubrik "Datenschutz") zum Download bereit.
Welche Verschlüsselung ergreift ATOSS, um die personenbezogenen Daten des Kunden vor unberechtigtem Zugriff zu schützen?	ATOSS und ihre Hyperscaler setzen bei den ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services Verschlüsselungsverfahren nach den technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dem internationalen Standard ISO/IEC 27001 ein. **Verschlüsselungsverfahren für Data at Rest** Personenbezogene Daten unserer Cloud-Kunden werden im Ruhezustand automatisch verschlüsselt (256-Bit-AES-Verschlüsselung). Weitere Informationen zur Verschlüsselung von Daten im Ruhezustand, z.B. im Zusammenhang mit der Verschlüsselung von Daten im Ruhezustand mit Microsoft Azure SQL-Datenbanken, finden Sie auf der Microsoft-Website. **Verschlüsselungsmethoden für Daten im Transit** Die Übertragung von Daten von oder zu ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services erfolgt grundsätzlich verschlüsselt und gesichert. Sofern die ATOSS Cloud Core Services und ATOSS Cloud Dedicated Services nativ in der Lage sind, die ausgetauschten Daten zu verschlüsseln, werden die Verschlüsselungsstandards

HTTPS/SFTP/LDAPS/SMTPS verwendet. Die gesamte HTTPS-Kommunikation wird über TLS nach dem empfohlenen Stand der Technik geschützt. Dateiübertragungen werden mit dem Secure File Transfer Protocol (SFTP) verschlüsselt. Terminaldaten werden sicher über HTTP2/TLS übertragen. Wenn die Terminals keine HTTPS-Verbindung unterstützen, muss ein sicherer VPN-Tunnel für die Kommunikation implementiert werden.

Für den Message-Digest-Algorithmus wird, wenn möglich, SHA512 verwendet.

Zusätzliche technische und organisatorische Maßnahmen umgesetzt durch Microsoft

Welche zusätzlichen Maßnahmen gibt es im Zusammenhang mit der Datenverarbeitung der personenbezogenen Daten des Kunden durch Microsoft?

Microsoft ist nach der AVV vertraglich verpflichtet, **angemessene technische und organisatorische Maßnahmen** zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten des Kunden zu treffen.

- Bitte beachten Sie die technischen und organisatorischen Maßnahmen, welche von Microsoft online veröffentlicht sind - Link: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA
- Bitte beachten Sie auch die diversen Zertifikate und Prüfreporte von Microsoft in Bezug auf Cloud Privacy oder Informationssicherheit wie DIN EN ISO/IEC 27001, DIN EN ISO/IEC 27017, DIN EN 27018 und das C5-Zertifikat - Link: https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-c5-germany?view=o365-worldwide

  Weiterer Link: https://servicetrust.microsoft.com/ViewPage/AllDocuments

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

Ein fünfter Schritt besteht darin, alle formalen Verfahrensschritte zu unternehmen, die für die Annahme Ihrer zusätzlichen Maßnahme(n) je nach dem Übermittlungsinstrument nach Art. 46 DSGVO, auf das Sie sich stützen, erforderlich sind. Auf der Grundlage der vorstehenden Informationen ist ATOSS der Ansicht, dass im vorliegenden Fall keine zusätzlichen Maßnahmen erforderlich sind.

Schritt 6 Führen Sie eine Neubewertung in angemessenen Abständen durch

Der sechste und letzte Schritt besteht darin, das Datenschutzniveau der übermittelten personenbezogenen Daten in angemessenen Abständen neu zu bewerten. ATOSS wird die Informationen in diesem Dokument 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.

ATOSS.COM