

## **DISCLAIMER: SVS-Chatbot**

Der SVS ist es ein großes Anliegen die Privatsphäre der Versicherten aber auch der Nutzer von Online-Services zu schützen. Daher werden alle technischen und organisatorischen Möglichkeiten ausgeschöpft um die Datensicherheit zu gewährleisten. Personenbezogene Daten, die der SVS bekannt werden, sind streng vertraulich und unter Anwendung des Datenschutzgesetzes (DSG) und der europäischen Datenschutzgrundverordnung (DSGVO) zu behandeln.

Der SVS-Chatbot basiert auf Microsoft Technologie. Das Unternehmen Microsoft verfügt über umfassende Erfahrung mit Online-Diensten für Unternehmen und hat erhebliche Investitionen in grundlegende Prozesse und Technologien getätigt, die Sicherheit und Datenschutz in Entwicklung und Betrieb integrieren. Microsoft hat außerdem branchenführende Sicherheitsmaßnahmen und Überwachungssteuerungen implementiert, um Sicherheitsprobleme zu erkennen und darauf zu reagieren. Bei der Benutzung des SVS-Chatbots erklären Sie sich einverstanden, dass Ihre Daten (ausschließlich verschlüsselt) zu Optimierungszwecken verarbeitet werden. Dazu werden die Cognitive Services genutzt, welche auf Microsoft Azure, der Cloud-Computing-Plattform von Microsoft, basieren und profitieren deswegen von den robusten Sicherheitstechnologien und -praktiken. Cognitive Services schützen APIs und Modelle, indem Sie Ihre Azure Active Directory-Dienste (Azure AD) um ein Azure-Abonnement erweitern und den Zugriff auf die APIs sowie benutzerdefinierte AI-Modelle verwalten zu können. Die Microsoft Azure-Cloud ist gemäß dem ISO / IEC 27001-Standard und seinen Sicherheitsbestimmungen zertifiziert. Die ISO / IEC 27000-Normenreihe, die vom gemeinsamen Unterausschuss ISO / IEC herausgegeben wurde, beschreibt Steuerungs- und Kontrollmechanismen, die jegliche Organisationen bei der sicheren Verwaltung von Informationsressourcen unterstützen. Diese Standards bieten einen Rahmen für Richtlinien und Verfahren, die alle rechtlichen, physischen und technischen Kontrollen umfassen, welche in den Information Risk Management-Prozessen einer Organisation umfasst werden. ISO / IEC 27001 ist ein Sicherheitsstandard, der formell ein Informationssicherheitsmanagementsystem (ISMS) spezifiziert, um Informationssicherheit unter explizite Managementkontrolle zu bringen. Als formale Spezifikation definiert sie Anforderungen, wie das ISMS installiert, überwacht, gewartet und kontinuierlich verbessert wird. Darüber hinaus enthält es eine Reihe von Best Practices, Anforderungen für Dokumentationen, Verantwortlichkeiten, Verfügbarkeiten, Zugriffssteuerung, Sicherheit, Überwachung sowie Behebung und Vermeidung enthalten. Die ISO / IEC 27001-Zertifizierung dient dafür, dass Unternehmen zahlreiche regulatorische und rechtliche Anforderungen in Bezug auf die Informationssicherheit erfüllen. Derzeit werden sowohl Azure Public als auch Azure Germany einmal jährlich von einer akkreditierten Zertifizierungsstelle auf Einhaltung der ISO / IEC 27001 auditiert. Diese Zertifizierungsstelle führt eine unabhängige Prüfung durch, um zu überprüfen, ob Microsoft die Sicherheitskontrollen implementiert hat und diese effizient funktionieren. Mit den Cognitive Services werden mehrere robuste Datenschutzmaßnahmen und dienstspezifische Datenverarbeitungspraktiken angeboten Microsoft ergreift strenge Maßnahmen, um die Daten vor unbefugtem Zugriff und unberechtigtem Zugriff zu schützen. Dazu gehört die Beschränkung des Zugriffs durch Microsoft-Mitarbeiter und Subunternehmer sowie die sorgfältige Definition von Anforderungen für die Beantwortung von Regierungsanfragen nach Kundendaten. Wenn Behörden oder Strafverfolgungsbehörden den Zugriff auf Daten - auch aus Gründen der nationalen Sicherheit - beantragen, müssen geltende rechtliche Verfahren befolgt werden, wie z. B. die Zustellung einer gerichtlichen Verfügung über Inhalte oder eine Vorladung bzgl. der Kontoinformationen. Microsoft gewährt keiner Regierung direkten oder uneingeschränkten Zugriff auf die Daten, es sei denn, es besteht eine direkte oder gesetzliche Verpflichtung.

Microsoft hat geschäftliche und technische Maßnahmen implementiert, die dazu beitragen die Daten, die Cognitive Services beinhalten, zu de-identifizieren. Die De-Identifikation anonymisiert die Daten nicht immer und zwangsläufig vollständig; es können bestimmte Arten von Daten grundsätzlich nicht de-identifiziert werden. Obwohl beispielsweise Cognitive Services keine Schritte unternimmt, um ein Foto mit einem individuellen Endbenutzer einer Organisation oder eines Entwicklers, der die kognitiven Dienste abonniert, zu verknüpfen, kann das Foto ein erkennbares sowie aussagekräftiges Bild einer Person aufweisen. Microsoft behält möglicherweise eine Kennung dieser Organisation oder des Entwicklers.

Der Dialogverlauf des Chatbots ist daher darauf ausgelegt, dass zu keinem Zeitpunkt personenbezogene Daten, die eine eindeutige Identifikation der Person zulassen, zu dessen funktionaler Nutzung benötigt werden. Die Eingabe solcher Daten widerspricht daher den Bedingungen dieser Dienstleistung. Die Microsoft-Datenschutzerklärung gilt für die Verwendung der Cognitive Services, ebenso wie die Microsoft-Onlinedienstbedingungen. Cognitive Services, die neu verfügbar sind, werden an die Azure-Services angepasst. Die Dienste "Computer Vision", "Face", "Content Moderator", "Text Analytics", "Bing-Speech" und "Language Understanding" haben diesen Übergang bereits vollzogen und unterliegen der vollständigen Kontrolle durch die Azure-Servicebedingungen und der Microsoft-Datenschutzerklärung. Der Standard ISO / IEC 27018 ist ein relativ neuer Anhang zu ISO / IEC 27001, dem ersten internationalen Verhaltenskodex für den Datenschutz in der Cloud. Auf der Grundlage der EU-Datenschutzgesetzgebung enthält der Anhang spezifische Anleitungen für CloudService-Provider (CSPs), die als Datenverarbeiter für personenbezogene Daten (PII), zur Einführung von Kontrollen zum Schutz der personenbezogenen Daten fungieren. Microsoft Azure und Azure Deutschland werden mindestens einmal jährlich von einer akkreditierten Zertifizierungsstelle auf Einhaltung der ISO / IEC 27001 und ISO / IEC 27018 auditiert. Diese Zertifizierungsstelle führt eine unabhängige Prüfung durch, um zu überprüfen, ob Microsoft die Sicherheitskontrollen implementiert hat und diese effizient funktionieren. Im Rahmen der Compliance-Überprüfung bestätigen die Auditoren in ihrer Anwendbarkeitserklärung, dass Microsoft-ISO / IEC-27018-Kontrollen zum Schutz von personenbezogenen Daten stattfinden. Kognitive Service-Daten: Gemäß den Nutzungsbedingungen für Online-Dienste vom April 2018 beziehen sich diese auf die Bedingungen für die Verwendung bestimmter Cognitive Services-Daten, ausgenommen der Cognitive Services Bing Search Services und Microsoft Translator, welche nicht im Geltungsbereich enthalten sind. Die SVS arbeitet außerdem mit sicheren Datennetzen, die durch Firewalls und Passwörter geschützt sind. Durch die Vergabe von Berechtigungen haben nur ausgewählte Personen Zugang zu diesen Daten. Diese Personen sind sowohl gesetzlich (§ 231 DSGVO), als auch vertraglich (§§ 8 Abs. 3 Dienstordnung A und Dienstordnung B, § 7 Abs. 4 Dienstordnung C) zur Verschwiegenheit und Geheimhaltung verpflichtet. Zur Optimierung des SVS-Chatbots wird der Chatverlauf daher protokolliert und in einer lokalen Instanz gespeichert. Diese Informationen sind anonym und werden nicht mit personenbezogenen Daten verbunden. Die Analyse soll uns helfen, das Informationsangebot für die Benutzer besser zu gestalten, um etwa die Dialogführung des SVS-Chatbots besser den Nutzerbedürfnissen anzupassen.