

Datenschutzhinweise

Nutzung des Virtual Agent – Sprachportal (agree21VirtualAgent-Sprachportal)

1. Einleitung und Gegenstand dieser Datenschutzhinweise

Mit den nachfolgenden Datenschutzhinweisen informieren wir Sie gemäß Art. 13 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, nachfolgend „DSGVO“) über die Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit der Nutzung unseres telefonischen Sprachportals (Virtual Agent). Der Virtual Agent ist ein KI-gestützter SprachBot, der Ihre telefonischen Anfragen rund um die Uhr entgegennimmt und standardisierte Anliegen, wie beispielsweise Umsatzabfragen oder Überweisungen im Zahlungsverkehr, fallabschließend bearbeiten kann. Sofern der Virtual Agent Ihr Anliegen nicht abschließend bearbeiten kann, erfolgt eine Weiterleitung an einen menschlichen Mitarbeiter.

Im Folgenden erläutern wir Ihnen, welche personenbezogenen Daten wir bei der Nutzung des Sprachportals verarbeiten, zu welchen Zwecken und auf welcher Rechtsgrundlage dies geschieht, an wen Ihre Daten weitergegeben werden, wie lange wir Ihre Daten speichern und welche Rechte Ihnen in Bezug auf die Verarbeitung Ihrer Daten zustehen.

2. Verantwortliche Stelle

Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO ist die Bremische Volksbank Weser – Wümme eG, Domsheide 14, 28195 Bremen. Sie erreichen die Verantwortliche auch über das Kontaktformular auf dieser Webseite sowie per Email unter folgender E-Mail-Adresse: info@bremischevb.de.

3. Datenschutzbeauftragter

Die Kontaktdaten unseres betrieblichen Datenschutzbeauftragten lauten:

Datenschutzbeauftragter

Pascal Ritz

datenschutz@bremischevb.de

4. Verarbeitungstätigkeiten

Nachfolgend informieren wir Sie über die einzelnen Verarbeitungstätigkeiten im Zusammenhang mit der Nutzung des Virtual Agent – Sprachportal.

4.1 Anrufannahme und Anliegen-Erkennung durch den Virtual Agent

Wenn Sie unser telefonisches Sprachportal anrufen, nimmt der Virtual Agent Ihren Anruf entgegen und verarbeitet Ihre Spracheingaben, um Ihr Anliegen zu erkennen und Sie an den richtigen Servicebereich weiterzuleiten oder Ihr Anliegen direkt zu bearbeiten. Hierzu werden die nachfolgend dargestellten personenbezogenen Daten verarbeitet.

Datenkategorien	Zwecke	Rechtsgrundlage	Berechtigte Interessen (bei Art. 6 Abs. 1 lit. f DSGVO)
Telefonnummer (Anrufer-ID/CLI); Spracheingaben (Audiodaten des Gesprächs); Zeitpunkt und Dauer des Anrufs; Anliegen-Kategorie (vom Virtual Agent erkannt)	Entgegennahme und Bearbeitung Ihres telefonischen Anliegens; Erkennung und Klassifizierung Ihres Anliegens mittels KI-basierter Sprachverarbeitung; Weiterleitung an den zuständigen Servicebereich oder fallabschließende Bearbeitung	Art. 6 Abs. 1 Satz 1 lit. b DSGVO (Vertragserfüllung) sowie Art. 6 Abs. 1 Satz 1 lit. f DSGVO (berechtigte Interessen)	Das berechtigte Interesse besteht in der effizienten Bearbeitung von Kundenanfragen sowie der Bereitstellung eines rund um die Uhr erreichbaren Kundenservice zur Verbesserung der Servicequalität.

Speicherdauer: Die Audiodaten der Spracheingaben werden unmittelbar nach Abschluss der Anliegen-Erkennung und Verarbeitung durch den Virtual Agent gelöscht, sofern keine weitergehende Verarbeitung für einen nachfolgend beschriebenen Zweck erforderlich ist. Die Telefonnummer sowie die Metadaten des Anrufs (Zeitpunkt, Dauer, erkannte Anliegen-Kategorie) werden für die Dauer von 90 Tagen gespeichert, um die ordnungsgemäße Bearbeitung Ihres Anliegens sicherzustellen und eventuelle Rückfragen bearbeiten zu können. Die Frist beginnt mit dem Ende des jeweiligen Anrufs.

Verpflichtung zur Bereitstellung der Daten: Die Bereitstellung Ihrer Telefonnummer erfolgt automatisch durch Ihren Telekommunikationsanbieter, sofern Sie die Rufnummernanzeige nicht unterdrückt haben. Die Spracheingaben sind erforderlich, damit der Virtual Agent Ihr Anliegen erkennen und bearbeiten kann. Ohne die Bereitstellung dieser Daten ist eine Nutzung des Sprachportals und eine Bearbeitung Ihres Anliegens durch den Virtual Agent technisch nicht möglich.

Empfänger: Innerhalb unseres Hauses erhalten diejenigen Mitarbeiter Zugang zu Ihren Daten, die mit der Bearbeitung Ihres Anliegens oder der Administration des Sprachportals befasst sind. Darüber hinaus werden Ihre Daten an folgende Empfänger weitergegeben: Die Atruvia AG, Saonestr. 3a, 60528 Frankfurt am Main, als IT-Dienstleister und Auftragsverarbeiter gemäß Art. 28 DSGVO, die den Betrieb, die Wartung und den Support des Sprachportals erbringt. Die Genesys Cloud Services B.V., Spaces Amstel / Mr Treublaan 7, 1097 JB Amsterdam, Niederlande, als weiterer Auftragsverarbeiter (Unterauftragnehmer der Atruvia AG), die den cloudbasierten Betrieb der Sprachportal-Lösung auf Basis von Amazon Web Services (AWS) bereitstellt.

Widerspruchsrecht: Soweit die Verarbeitung auf Art. 6 Abs. 1 Satz 1 lit. f DSGVO beruht, haben Sie für diese Verarbeitungstätigkeit das Recht auf Widerspruch gemäß Artikel 21 DSGVO. Ihren Widerspruch senden Sie uns am besten per E-Mail an: info@bremischevb.de. Sie können uns den Widerspruch jedoch auch auf anderem Wege mitteilen.

4.2 Authentifizierung und Legitimation (VR-NetKey / VR SecureGo plus)

Für die Durchführung bestimmter Self-Services über den Virtual Agent, wie insbesondere Umsatzabfragen oder Überweisungen, ist eine vorherige Authentifizierung Ihrer Person erforderlich. Diese erfolgt je nach gewähltem Verfahren über die Eingabe Ihres VR-NetKey mit CallCenter-Zugang oder über die Authentifizierung mittels VR SecureGo plus.

Datenkategorien	Zwecke	Rechtsgrundlage
VR-NetKey; PIN / Zugangsdaten (werden nicht gespeichert, nur zur Prüfung übermittelt); SecureGo plus Authentifizierungsdaten; Ergebnis der Authentifizierungsprüfung (erfolgreich/nicht erfolgreich); Zeitpunkt der Authentifizierung	Verifizierung Ihrer Identität zur sicheren Durchführung von kontobezogenen Transaktionen und Abfragen; Erfüllung gesetzlicher Anforderungen an die starke Kundenauthentifizierung	Art. 6 Abs. 1 Satz 1 lit. b DSGVO (Vertragserfüllung – Durchführung von Bankgeschäften) sowie Art. 6 Abs. 1 Satz 1 lit. c DSGVO i. V. m. § 55 ZAG, Art. 97 der Richtlinie (EU) 2015/2366 (PSD2) (gesetzliche Verpflichtung zur starken Kundenauthentifizierung)

Speicherdauer: Die Zugangsdaten (PIN) werden ausschließlich für den Moment der Authentifizierungsprüfung verarbeitet und unmittelbar danach gelöscht. Sie werden nicht gespeichert. Das Ergebnis der Authentifizierungsprüfung sowie der Zeitpunkt der Authentifizierung werden im Rahmen der Protokollierung für die Dauer von 90 Tagen gespeichert, beginnend mit dem Zeitpunkt der Authentifizierung, um die Nachvollziehbarkeit sicherheitsrelevanter Vorgänge zu gewährleisten.

Verpflichtung zur Bereitstellung der Daten: Die Bereitstellung Ihrer Authentifizierungsdaten ist sowohl gesetzlich (starke Kundenauthentifizierung gemäß PSD2) als auch vertraglich erforderlich. Ohne die Bereitstellung dieser Daten können kontobezogene Self-Services, wie Umsatzabfragen oder Überweisungen, über den Virtual Agent nicht durchgeführt werden.

Empfänger: Innerhalb unseres Hauses werden die Daten an die mit der Authentifizierung und IT-Sicherheit befassten Abteilungen weitergegeben. Extern werden die Daten an die Atruvia AG als Auftragsverarbeiter gemäß Art. 28 DSGVO übermittelt, die das Kernbanksystem (agree21) und die Authentifizierungsdienste betreibt. Die

Genesys Cloud Services B.V. ist als weiterer Auftragsverarbeiter (Unterauftragnehmer) am cloudbasierten Betrieb beteiligt.

4.3 Durchführung von Self-Services (Umsatzabfrage, Überweisungen, Zahlungsverkehr)

Nach erfolgreicher Authentifizierung können Sie über den Virtual Agent verschiedene Self-Services nutzen. Hierzu gehören insbesondere die Abfrage von Kontoumsätzen und Kontostand sowie die Durchführung von Überweisungen und weiteren Zahlungsverkehrstransaktionen.

Datenkategorien	Zwecke	Rechtsgrundlage
Kontonummer / IBAN; Kontosaldo und Umsatzdaten; Empfängerdaten bei Überweisungen (Name, IBAN, Verwendungszweck, Betrag); Transaktionsdaten (Art, Zeitpunkt, Betrag); Spracheingaben zur Auftragserteilung	Durchführung der von Ihnen angeforderten Bankgeschäfte (Umsatzabfrage, Kontostandabfrage, Überweisungen); Dokumentation und Nachweisführung der durchgeführten Transaktionen	Art. 6 Abs. 1 Satz 1 lit. b DSGVO (Vertragserfüllung – Durchführung des Zahlungsdiensterahmenvertrags) sowie Art. 6 Abs. 1 Satz 1 lit. c DSGVO i. V. m. §§ 147 AO, 257 HGB (gesetzliche Aufbewahrungspflichten für Buchungsbelege und Geschäftskorrespondenz)

Speicherdauer: Die Spracheingaben zur Auftragserteilung werden nach Abschluss der Transaktion und Übernahme der Transaktionsdaten in das Kernbanksystem gelöscht. Die Transaktionsdaten (Überweisungsdaten, Umsatzdaten) werden für die Dauer der gesetzlichen Aufbewahrungsfristen gespeichert. Diese betragen gemäß §§ 147 AO, 257 HGB grundsätzlich zehn Jahre für Buchungsbelege. Die Frist beginnt mit dem Schluss des Kalenderjahres, in dem die jeweilige Transaktion durchgeführt wurde. Kontoumsätze und Kontosaldden, die lediglich zu Auskunftszwecken abgerufen werden, werden im Rahmen des Anrufs verarbeitet und nicht gesondert über die reguläre Protokollierung hinaus gespeichert.

Verpflichtung zur Bereitstellung der Daten: Die Bereitstellung der Daten ist vertraglich erforderlich. Ohne die Angabe der relevanten Kontodaten und Empfängerinformationen können die von Ihnen gewünschten Bankgeschäfte nicht durchgeführt werden. Hinsichtlich der Aufbewahrung der Transaktionsdaten besteht eine gesetzliche Pflicht gemäß §§ 147 AO, 257 HGB.

Empfänger: Innerhalb unseres Hauses erhalten die Mitarbeiter der mit der Zahlungsverkehrsabwicklung, der Buchhaltung sowie der IT-Administration befassten

Abteilungen Zugang zu den Daten, soweit dies für die Erfüllung ihrer jeweiligen Aufgaben erforderlich ist. Extern werden die Daten an die Atruvia AG als Auftragsverarbeiter übermittelt, die das Kernbanksystem (agree21) betreibt. Die Genesys Cloud Services B.V. ist als Unterauftragnehmer am cloudbasierten Betrieb beteiligt. Bei Überweisungen werden die Transaktionsdaten zudem an das kontenführende Institut des Empfängers und die beteiligten Zahlungsdienstleister im Rahmen der Zahlungsverkehrsabwicklung weitergeleitet.

4.4 Technischer Betrieb, Protokollierung und Qualitätssicherung

Um den sicheren und störungsfreien Betrieb des Sprachportals zu gewährleisten, werden technische Protokolldaten erhoben und verarbeitet. Diese dienen der Fehlererkennung, der IT-Sicherheit und der Qualitätssicherung des Dienstes.

Datenkategorien	Zwecke	Rechtsgrundlage	Berechtigte Interessen (bei Art. 6 Abs. 1 lit. f DSGVO)
Technische Verbindungsdaten (IP-Adresse des Telefonie-Gateways, Session-ID); Protokolldaten (Zeitstempel, Ereignistypen, Fehlermeldungen); Systemperformance-Daten	Gewährleistung der technischen Funktionsfähigkeit und IT-Sicherheit des Sprachportals; Fehlererkennung und -behebung; Qualitätssicherung und Optimierung des Dienstes	Art. 6 Abs. 1 Satz 1 lit. f DSGVO (berechtigte Interessen)	Das berechtigte Interesse besteht in der Sicherstellung eines störungsfreien, sicheren und verfügbaren Betriebs des Sprachportals sowie in der kontinuierlichen Verbesserung der Servicequalität.

Speicherdauer: Die technischen Protokolldaten werden für die Dauer von 90 Tagen gespeichert, beginnend mit dem Zeitpunkt der Erhebung, und anschließend automatisiert gelöscht. Dieser Zeitraum ist erforderlich, um technische Störungen zeitnah erkennen und nachverfolgen zu können.

Verpflichtung zur Bereitstellung der Daten: Die Erhebung der technischen Protokolldaten erfolgt automatisch bei der Nutzung des Sprachportals. Eine gesonderte Bereitstellung durch Sie ist nicht erforderlich. Die Verarbeitung ist technisch zwingend notwendig für den Betrieb des Dienstes.

Empfänger: Innerhalb unseres Hauses erhalten ausschließlich die mit der IT-Administration und IT-Sicherheit befassten Mitarbeiter Zugang zu den Protokolldaten. Extern werden die Daten an die Atruvia AG als Auftragsverarbeiter übermittelt, die den Betrieb, die Wartung und den Support erbringt. Die Genesys Cloud Services B.V. ist als Unterauftragnehmer am cloudbasierten Betrieb der Infrastruktur beteiligt.

Widerspruchsrecht: Sie haben für diese Verarbeitungstätigkeit das Recht auf Widerspruch gemäß Artikel 21 DSGVO. Ihren Widerspruch senden Sie uns am besten per E-Mail an: info@bremischevb.de. Sie können uns den Widerspruch jedoch auch auf anderem Wege mitteilen.

5. Automatisierte Entscheidungsfindung einschließlich Profiling

Eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO findet im Zusammenhang mit der Nutzung des Virtual Agent – Sprachportal nicht statt. Der Virtual Agent unterstützt Sie bei der Erkennung und Bearbeitung Ihrer Anliegen, trifft jedoch keine automatisierten Entscheidungen, die Ihnen gegenüber rechtliche Wirkung entfalten oder Sie in ähnlicher Weise erheblich beeinträchtigen.

6. Internationale Datenübermittlung

Im Rahmen der Nutzung des Sprachportals werden personenbezogene Daten an ein Drittland übermittelt. Die dem Sprachportal zugrunde liegende Cloud-Infrastruktur wird durch die Genesys Cloud Services B.V. auf Basis von Amazon Web Services (AWS) betrieben. Dabei kann eine Übermittlung personenbezogener Daten in die Vereinigten Staaten von Amerika (USA) erfolgen.

Für die Übermittlung personenbezogener Daten in die USA liegt ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO vor. Dieser Angemessenheitsbeschluss basiert auf dem EU-U.S. Data Privacy Framework und bestätigt, dass die beteiligten US-Unternehmen, soweit sie unter dem Data Privacy Framework zertifiziert sind, ein angemessenes Datenschutzniveau gewährleisten. Nähere Informationen zum EU-U.S. Data Privacy Framework sind abrufbar unter: <https://www.dataprivacyframework.gov>.

7. Ihre Rechte als betroffene Person

Ihnen stehen bei Vorliegen der jeweiligen gesetzlichen Voraussetzungen die folgenden Rechte gemäß der DSGVO zu:

Sie haben das Recht auf Auskunft gemäß Art. 15 DSGVO. Dies bedeutet, dass Sie von uns eine Bestätigung darüber verlangen können, ob personenbezogene Daten, die Sie betreffen, von uns verarbeitet werden. Ist dies der Fall, haben Sie ein Recht auf Auskunft

über diese personenbezogenen Daten sowie auf die in Art. 15 DSGVO im Einzelnen genannten Informationen.

Sie haben das Recht auf Berichtigung gemäß Art. 16 DSGVO. Dieses Recht umfasst die unverzügliche Berichtigung unrichtiger personenbezogener Daten, die Sie betreffen. Unter Berücksichtigung der Zwecke der Verarbeitung haben Sie zudem das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Sie haben das Recht auf Löschung gemäß Art. 17 DSGVO. Unter den in Art. 17 DSGVO genannten Voraussetzungen können Sie von uns verlangen, dass personenbezogene Daten, die Sie betreffen, unverzüglich gelöscht werden. Das Recht auf Löschung besteht unter anderem dann nicht, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Sie haben das Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO. Unter den in Art. 18 DSGVO genannten Voraussetzungen können Sie die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten verlangen.

Sie haben das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO. Soweit die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt, haben Sie das Recht, die Sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und Sie haben das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln.

8. Beschwerderecht bei einer Aufsichtsbehörde

Sie haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren, z. B. bei dem Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen, Georgstraße 122–124, 27570 Bremerhaven,