App Nutzungsbedingungen

Stand: 11. November 2024

1 Gegenstand

1.1 Augnect GmbH, geschäftsansässig Freiherr-vom-Stein-Straße 13, 55131 Mainz, eingetragen unter HRB 51500 Amtsgericht Mainz („Augnect“), stellt die Augnect Software („Augnect App“) cloudbasiert als individualisierbare Software-as-a-Service („SaaS“) an Kunden bereit.

1.2 Gegenstand ist die mietweise Bereitstellung von Augnect in der Weise und mit den Funktionen gemäß der jeweils aktuellen „App Leistungsbeschreibung“ einschließlich Rechenleistung und Speicherplatz zum Zweck der Nutzung als Wissensplattform durch den Kunden selbst über das Internet gegen Vergütung („Zusammenarbeit“). Der Quellcode und die Bereitstellung der Internetverbindung sind nicht Leistungsgegenstand.

1.3 Für die Geschäftsbeziehung zwischen Augnect und dem Kunden gelten ausschließlich diese „App Nutzungsbedingungen“. Der Kunde akzeptiert diese mit der Bestellung von Augnect. Abweichende oder entgegenstehende Bedingungen des Kunden werden von Augnect nicht anerkannt, soweit Augnect diesen nicht ausdrücklich in Textform zugestimmt hat.

2 Nutzungsrecht

2.1 Augnect gewährt dem Kunden ein einfaches, nicht übertragbares, nicht unterlizenzierbares Recht zur Nutzung der Augnect App als Wissensplattform gemäß diesen Nutzungsbedingungen mit Zugang für Mitarbeitende und Geschäftspartner des Kunden sowie sonstige in Verbindung mit dem Kunden stehende Dritte während einer Lizenzperiode („Lizenz“).

2.2 Die Lizenz gilt nur für den Kunden und mit ihm verbundene Unternehmen im Sinne der §§ 15 ff AktG. Der Kunde darf die Augnect App weder entgeltlich noch unentgeltlich sonstigen Dritten überlassen oder zur Nutzung bereitstellen, soweit dies nicht ausdrücklich in Textform vereinbart wird oder der Kunde entgeltlich weitere Lizenzen für bestimmte Dritte hinzubucht.

2.3 Die Lizenz gilt nur für den Funktionsumfang des jeweils bestellten Leistungspakets. Updates, Upgrades und neue Versionen sind vorbehaltlich Ausnahmen gemäß Ziffer 5.4 von der Lizenz miterfasst.

2.4 Geistiges Eigentum, Schutzrechte und Knowhow an der Software verbleiben allein bei Augnect. Die Überlassung an den Kunden erfolgt frei von Rechten Dritter, die in Widerspruch zur Nutzung als Augmented Reality Wissensplattform stehen. Der Kunde darf die Augnect App oder Teile hiervon nicht vervielfältigen, verändern, verbreiten, verkaufen, vermieten, bearbeiten, umgestalten oder zweckentfremden, insbesondere nicht zurückentwickeln

(„Reverse Engineering“) oder den Quellcode extrahieren, soweit nicht gemäß §§ 69d, 69e UrhG zugelassen oder ausdrücklich von Augnect in Textform erlaubt.

3 Bereitstellung

3.1 Für die Funktionen des jeweils bestellten Leistungspaketes gilt die App Leistungsbeschreibung.

3.2 Augnect stellt dem Kunden eigenen Speicherplatz für eingehende Hinweise und damit zusammenhängende Informationen bereit. Augnect ergreift für den Kunden geeignete Maßnahmen gegen Datenverlust und zur Verhinderung unbefugter Zugriffe Dritter.

3.3 Augnect entwickelt die Augnect App kontinuierlich weiter und arbeitet unter Beibehaltung bestehender Sicherheitsstandards Verbesserungen und weitere Funktionen ein. Augnect schuldet dem Kunden jedoch nur die Funktionen gemäß der jeweils aktuellen App Leistungsbeschreibung.

3.4 Der Kunde kann ein bestelltes Leistungspaket jederzeit auf ein solches mit höherer Lizenzgebühr aktualisieren, nicht jedoch zu einer niedrigeren Lizenzgebühr wechseln. Die Vorteile einer Paketänderung werden sofort wirksam. Augnect stellt dann lediglich den Differenzbetrag zwischen der neuen und der bisherigen Lizenzgebühr in Rechnung.

3.5 Bei Beendigung der Zusammenarbeit obliegt es dem Kunden, einen Export seiner Daten schriftlich bei Augnect einzufordern. Augnect löscht die Daten frühestens 14 Tage nach Beendigung, jedenfalls aber im Rahmen der gesetzlichen Bestimmungen.

4 Verfügbarkeit, Sicherheit, Pflege

4.1 Augnect stellt eine Betriebs- und Funktionsfähigkeit der Augnect App gemäß der App Leistungsbeschreibung entsprechend den gesetzlichen Regeln mit einer Verfügbarkeit von 97% je Kalenderjahr sicher. Geplante und angekündigte Zeiten zur Softwarepflege gelten nicht als Ausfallzeiten, soweit diese nicht insgesamt 0,5% der Verfügbarkeit übersteigen.

4.2 Augnect stellt die Sicherheit der Software nach dem Stand der Technik im Rahmen der Bereitstellung (Hosting) von internetbasierten Software-Anwendungen sicher. Augnect erstellt täglich Backups der Daten und speichert diese für 30 Tage.

4.3 Der Kunde kann sich stets in Textform zur zeitnahen Beantwortung bzgl. etwaiger technischer Störungen oder Softwarefehler an Augnect wenden.

4.4 Augnect führt technische Änderungen und Ergänzungen an der Augnect App sowie Maßnahmen, die der Feststellung und Behebung von Funktionsstörungen dienen (insgesamt „Softwarepflege“), nach Möglichkeit an Wochenenden zwischen Samstag 08:00 Uhr und Sonntag 24:00 Uhr oder wochentags nachts in der Zeit zwischen 22:00 Uhr und 08:00 Uhr durch. Soweit eine Softwarepflege zu Ausfallzeiten von mehr als 60 Minuten führt, kündigt Augnect dies 5 Werktage zuvor dem Kunden in Textform an. In Ausnahme- und dringenden Fällen kann eine Softwarepflege unter Berücksichtigung der geringstmöglichen Beeinträchtigung des laufenden Betriebs auch ohne Ankündigung und während aller übrigen Zeiten durchgeführt werden.

5 Lizenzgebühren, Abrechnung, Zahlung

5.1 Der Kunde zahlt Augnect für die Bereitstellung der Augnect App ein Entgelt, welches sich nach dem ausgewählten Leistungspaket richtet.

5.2 Augnect kann die Entgelte ändern, jedoch erstmals mit Wirkung nach Ablauf der vereinbarten Mindestvertragslaufzeit und frühestens 12 Monate nach Vertragsschluss. Änderungen orientieren sich an etwa veränderten Kosten für das Hosting, Funktionserweiterungen der Software sowie die Sicherheit der Software sowie der Daten und werden ab dem folgenden Zahlungslauf wirksam.

5.3 Augnect teilt Änderungen der Entgelte dem Kunden spätestens 20 Werktage vor deren Wirksamwerden in Textform mit. Die Zustimmung des Kunden gilt als erteilt, wenn der Kunde nicht bis dahin seine Ablehnung mitteilt. Auf diese Genehmigungswirkung weist Augnect den Kunden jeweils besonders hin. Lehnt der Kunde ab, wirkt dies als Kündigung zum Ende der laufenden Lizenzperiode.

5.4 Werden im Vergleich zur App Leistungsbeschreibung zu Beginn der Lizenzperiode weitere Funktionen in Augnect geschaffen, kann Augnect diese auch optional gegen zusätzliches Entgelt bereitstellen.

5.5 Alle Entgelte sind in Euro, netto und zuzüglich der gesetzlichen Umsatzsteuer, soweit diese anfällt, vereinbart. Soweit nicht anders vereinbart sind alle Entgelte im Voraus zur Bereitstellung von Augnect für die jeweilige Lizenzperiode fällig. Augnect stellt die Rechnungen hierüber dem Kunden in Textform zur Verfügung. Der Kunde kann Augnect ein Lastschriftmandat zur Abbuchung fälliger Entgelte erteilen.

6 Pflichten des Kunden

6.1 Der Kunde darf Augnect ausschließlich vertrags- und bestimmungsgemäß als Wissensplattform mit den Funktionen gemäß App Leistungsbeschreibung verwenden.

6.2 Der Kunde ist für die inhaltliche, rechtliche und datenschutzkonforme Nutzung einschließlich der editierbaren Inhalte und Texte in Augnect allein verantwortlich.

6.3 Unbeschadet der Datensicherung durch Augnect ist der Kunde selbst für die Eingabe und Pflege seiner Daten und Informationen verantwortlich. Der Kunde prüft seine Daten vor einer Speicherung auf dem Speicherplatz unter Einsatz entsprechender Schutzprogramme nach dem Stand der Technik auf Viren oder sonstige schädliche Komponenten.

6.4 Bereitstellung (mobiler) Endgeräte mit marktüblichen Internetbrowsern sowie ausreichender Internetverbindung zur Nutzung der Augnect App obliegt allein dem Kunden.

6.5 Das für den Kunden registrierte Zugangskonto ist nicht auf Dritte übertragbar und darf ausschließlich von der in der Nutzungsvereinbarung genannten hauptverantwortlichen Person („Administrator“) und den von dieser eingeladenen weiteren Bearbeitenden genutzt werden. Dritte dürfen die Augnect App nicht mit Zugangsdaten anderer registrierter Personen nutzen.

6.6 Die hauptverantwortliche Person des Kunden sowie die weiteren Bearbeitenden vergeben eigene Passwörter, halten die ihnen zugeordneten Zugangsdaten geheim und vor dem Zugriff durch Dritte geschützt, und geben diese nicht an unberechtigte Dritte weiter. Der Kunde

teilt Augnect das Ausscheiden oder den Wechsel berechtigter Mitarbeitender zur Aktualisierung der Zugangsdaten mit. Die hauptverantwortliche Person des Kunden (Administrator) kontrolliert regelmäßige erfolgte Aktivitäten in der Augnect App, um unbefugte Nutzung festzustellen und informiert Augnect unverzüglich in Textform darüber, wenn Zugangsdaten verloren gehen oder der Verdacht unberechtigter Kenntnis Dritter besteht.

7 Laufzeit, Kündigung

7.1 Eine Lizenzperiode läuft 12 Monate. Die Zusammenarbeit verlängert sich automatisch, soweit der Kunde nicht bis 3 Monate vor Ablauf der laufenden Lizenzperiode kündigt. Jede Kündigung wird am Ende des letzten Tages der laufenden Lizenzperiode wirksam.

7.2 Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Augnect kann insbesondere fristlos kündigen, wenn der Kunde gegen diese Nutzungsbedingungen verstößt, Augnect den Kunden mindestens 14 Tage zuvor in Textform abgemahnt und der Kunde den Verstoß nicht beseitigt hat.

7.3 Jede Kündigung bedarf der Textform. Regelungen zu Vertraulichkeit, Datenschutz und Haftung überleben jede Kündigung.

8 Datenschutz

8.1 Beide Parteien erfüllen die jeweils anwendbaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) und verpflichten ihre bei der Zusammenarbeit eingesetzten Mitarbeitenden auf Vertraulichkeit und das Datengeheimnis.

8.2 Alle Daten des Kunden, die in die Augnect App gelangen, sind Eigentum des Kunden. Erhebt, verarbeitet oder nutzt der Kunde personenbezogene Daten, ist er als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO selbst für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich.

8.3 Augnect ist als Auftragsverarbeiter gemäß Art. 28 DSGVO für den Kunden tätig. Dazu gelten die jeweils aktuellen Bedingungen zur Auftragsverarbeitung (AVV) von Augnect.

9 Kommunikation, Vertraulichkeit, Referenz

9.1 Augnect sendet dem Kunden Benachrichtigungen etwa zu Softwarepflege und neuen Funktionen, Mitteilungen, Rechnungen etc. an die in der Nutzungsvereinbarung genannte hauptverantwortliche Person des Kunden und/oder in Textform an die bei Bestellung seitens des Kunden angegebene verantwortliche Person/E-Mailadresse. Textform meint in der Zusammenarbeit der Parteien die Kommunikation per E-Mail.

9.2 Augnect und der Kunde sind nicht berechtigt, voneinander erhaltene vertrauliche Informationen an Dritte weiterzugeben. Der Kunde darf erhaltene Kenntnisse über Augnect nicht nutzen, um selbst oder durch Dritte eine ähnliche Software zu entwickeln.

9.3 Augnect darf die Zusammenarbeit mit dem Kunden unter Verwendung des Kundenlogos und Verweis auf die Website des Kunden als Referenz veröffentlichen, soweit der Kunde nicht ausdrücklich in Textform ablehnt.

10 Haftung

10.1 Augnect haftet nur für Betriebs- und Funktionsfähigkeit von Augnect gemäß Software Leistungsbeschreibung. Eine verschuldensunabhängige Haftung von Augnect für bei Vertragsschluss vorhandener Mängel (§ 536a BGB) ist ausgeschlossen.

10.2 Augnect haftet für Schäden nur aufgrund vorsätzlicher oder grober Fahrlässigkeit, auch ihrer gesetzlichen Vertreter oder Erfüllungsgehilfen. Bei leichter Fahrlässigkeit haftet Augnect nur für vertragstypische, vorhersehbare Schäden aus Verletzung von für die Zusammenarbeit wesentlicher Pflichten.

10.3 Augnect haftet unbeschränkt nur für vorsätzlich oder fahrlässig verursachte Schäden aus Verletzung des Lebens, des Körpers oder der Gesundheit. Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

10.4 Augnect haftet nicht für Schäden aus Umständen, welche außerhalb des zu erwartenden Einflussbereichs liegen, insbesondere (i) Folgen feindlicher Angriffe auf die Software; (ii) Folgen aus höherer Gewalt wie etwa Pandemie, Streik, Aussperrung, Krieg, Naturkatastrophen; (iii) Fehler in der Software, welche durch falsche Verwendung oder Missbrauch durch den Kunden selbst oder Dritte verursacht werden.

10.5 Augnect haftet nicht für den Verlust von Daten, soweit diese darauf beruhen, dass es der Kunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verloren gegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.

11 Allgemeine Bestimmungen

11.1 Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts. Gerichtsstand für alle Streitigkeiten ist – soweit wirksam vereinbar – der Sitz von Augnect.

11.2 Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen dieser Nutzungsbedingungen, auch dieser Bestimmung, bedürfen der Textform. § 305b BGB bleibt unberührt.

11.3 Diese App Nutzungsbedingungen, App Leistungsbeschreibung und Bedingungen zur Auftragsverarbeitung (AVV) können jederzeit in ihrer aktuellen Fassung eingesehen werden unter https://augnect.com/agb.

11.4 Änderungen dieser Nutzungsbedingungen und Entfall wesentlicher Leistungen teilt Augnect dem Kunden spätestens 20 Werktage vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens in Textform mit. Die Zustimmung des Kunden gilt als erteilt, wenn der Kunde nicht bis dahin seine Ablehnung mitteilt. Auf diese Genehmigungswirkung weist Augnect den Kunden jeweils besonders hin.

11.5 Sollten einzelne Bestimmungen ganz oder teilweise unwirksam, auslegungs- oder ergänzungsbedürftig sein, so erfolgt die Auslegung bzw. Ergänzung danach, welche Regelung dem sonstigen Inhalt und Zweck der Zusammenarbeit vernünftigerweise am ehesten entspricht.

11.6 Sollten die Vertragsunterlagen neben der deutschen Sprache in weiteren Sprachen bereitgestellt werden, ist die deutsche Fassung maßgeblich.

Bedingungen zur Auftragsverarbeitung (AVV)

personenbezogener Daten gemäß Art. 28 DSGVO

Stand: 11. November 2024

1 Vorbemerkung

1.1 Die Augnect GmbH, geschäftsansässig Freiherr-vom-Stein-Straße 13, 55131 Mainz, eingetragen unter HRB 51500 Amtsgericht Mainz („Auftragnehmer“), stellt auf Grundlage der App Nutzungsvereinbarung nebst App Nutzungsbedingungen („Hauptvertrag“) die Augmented Reality Wissensplattform „Augnect App“ cloudbasiert als individualisierbare Software-as-a-Service („SaaS“) an Kunden („Auftraggeber“) bereit.

1.2 Auftraggeber und Auftragnehmer vereinbaren mit Abschluss des Hauptvertrages ausdrücklich auch nachfolgende Bedingungen zur Auftragsverarbeitung und schließen damit eine Vereinbarung zur Auftragsverarbeitung (AVV), mit welcher die damit verbundenen datenschutzrechtlichen Verpflichtungen geregelt werden.

2 Umfang der Beauftragung

2.1 Diese AVV gilt für Zugang und Zugriff des Auftragnehmers zu personenbezogenen Daten (Daten), für die der Auftraggeber verantwortlich ist, im Rahmen der hauptvertraglichen Leistungserbringung des Auftragnehmers. Der Auftragnehmer verarbeitet Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere der DSGVO, und der gesetzlichen Betroffenenansprüche im Hinblick auf die Daten.

2.2 Gegenstand, Zweck und Art der Verarbeitung, Art der Daten und Kategorien der betroffenen Personen sind:

(a) Gegenstand, Art und Zweck der Verarbeitung: Verwaltung von Kundendaten, Verbesserung von Dienstleistungen und Produkten

(b) Arten personenbezogener Daten: Personenstammdaten (Vorname, Name, Titel/akademischer Grad), Kommunikationsdaten (Telefon, E-Mail), berufs- und tätigkeitsbezogene Daten, Profilbild.

(c) Kategorien der betroffenen Personen: Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen: Mitarbeiter

2.3 Neben personenbezogenen Daten werden Session-Daten und Metadaten nur erhoben und verarbeitet, soweit zum Betrieb der Software unbedingt erforderlich und soweit diese vollständig anonymisiert sind. Die Software verwendet Cookies nur in Bezug auf die Session-Daten und stets ohne Erhebung oder Auslesen personenbezogener Daten.

2.4 Die Verarbeitung findet innerhalb der Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (EWR) statt. Der Auftragnehmer darf Auftraggeberdaten unter Einhaltung der Bestimmungen dieser AVV auch außerhalb des EWR verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44 bis 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

3 Weisungsbefugnis

3.1 Der Auftragnehmer verarbeitet die Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, soweit er nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In einem solchen Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern sich dies nicht aufgrund wichtigen öffentlichen Interesses verbietet.

3.2 Weisungen des Auftraggebers sind grundsätzlich abschließend in den Allgemeinen Nutzungsbedingungen und dieser AVV geregelt. Einzelweisungen, die hiervon abweichen oder zusätzliche Anforderungen aufstellen, bedürfen vorheriger Zustimmung des Auftragnehmers und erfolgen nach Maßgabe des in den Allgemeinen Nutzungsbedingungen festgelegten Änderungsverfahrens. Im Übrigen gilt für Weisungsbefugnis des Auftraggebers und Weisungsbindung des Auftragnehmers Art. 28 und 29 DSGVO.

3.3 Die weisungsbefugte Person benennt der Auftraggeber im Hauptvertrag mit mindestens einem Hauptverantwortlichen („Administrator“). Der Auftraggeber kann die weisungsberechtigte Person jederzeit unter Mitteilung an den Auftragnehmer in Textform auswechseln.

3.4 Der Auftraggeber erteilt Weisungen klar und nachvollziehbar. Weisungen dürfen nicht gegen geltendes Recht verstoßen. Ist eine Weisung aus der Sicht des Auftragnehmers unklar, weist er unverzüglich darauf hin und erbittet Klarstellung. Hält der Auftragnehmer eine Weisung für einen Verstoß gegen diese AVV oder geltendes Recht, macht er Mitteilung an den Auftraggeber und kann die Ausführung bis zu einer Bestätigung durch den Auftraggeber aussetzen. Die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Daten liegt beim Auftraggeber.

4 Verantwortlichkeit des Auftraggebers

4.1 Der Auftraggeber gemäß Art. 28 Abs. 3 lit. e DSGVO ist im Verhältnis zum Auftragnehmer für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich. Der Auftragnehmer unterstützt nach Möglichkeit mit geeigneten Maßnahmen. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Daten nach Maßgabe dieser Vereinbarung Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

4.2 Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig über festgestellte Fehler oder Unregelmäßigkeiten im Hinblick auf datenschutzrechtliche Bestimmungen oder Weisungen.

4.3 Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Daten des Auftraggebers zu erteilen oder mit solchen Stellen anderweitig zusammenzuarbeiten, unterstützt ihn der Auftraggeber auf erstes Anfordern bei der Erteilung von Auskünften und der Erfüllung anderweitiger Verpflichtungen.

5 Anforderung an Personal

Der Auftragnehmer setzt ausschließlich Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheit unterliegen.

6 Technisch-organisatorische Maßnahmen

Der Auftragnehmer ergreift gemäß Art. 32 DSGVO die nachfolgenden erforderlichen und geeigneten Maßnahmen, die unter Berücksichtigung des Standes der Technik, Implementierungskosten, Art, Umfang, Umständen und Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein angemessenes Schutzniveau für die Daten des Auftraggebers zu gewährleisten („technisch-organisatorische Maßnahmen“). Der Auftragnehmer darf diese während der Verarbeitung ändern und anpassen, solange sie weiterhin den gesetzlichen Anforderungen genügen. Der Auftragnehmer stellt dem Auftraggeber auf dessen Verlangen eine konkrete Beschreibung der jeweils aktuell ergriffenen technisch-organisatorischen Maßnahmen bereit.

6.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die Rechenzentren sind umfassend durch Einlasskontrollen und Sicherungsmechanismen gesichert, um einen unbefugten Zutritt zu Datenverarbeitungsanlagen zu verhindern (u.a. Alarmanlage, Wachdienst, Protokollierung des Zutritts usw.). Ein Zutritt ist nur autorisierten Mitarbeitern gestattet.
- Zugangskontrolle: Keine unbefugte Systembenutzung. Der Auftragnehmer setzt sichere und komplexe Passwörter ein, um eine unbefugte Systembenutzung auszuschließen. Die Inhalte werden durch AES mit 256 Bit verschlüsselt. Backend-User erhalten neben einem Passwort einen persönlichen Secret Key. 2-Faktor-Authentifizierung. Es besteht ein umfassender Malware-Schutz auf Arbeitsplatzrechnern und Servern. Technische Sperre des Arbeitsplatzes bei Nicht-Aktivität. TLS-Verschlüsselung.
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen innerhalb des Systems durch ein entsprechendes Berechtigungskonzept.
- Trennungskontrolle: Trennung von Entwicklungs-, Test- und Produktivsystem.

6.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern, Entfernen bei elektronischer Übertragung oder Transport durch eine industrieübliche SSL-Verschlüsselung, Verschlüsselung von Passwörtern, Richtlinie zu Homeoffice/Telearbeit, Verpflichtung der Mitarbeiter zur Verschwiegenheit, auf das Fernmeldegeheimnis und auf das Sozialgeheimnis.

6.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle: Es werden täglich Backups angefertigt, um einen Verlust der Daten zu minimieren. Wir setzen einen industrieüblichen Virenschutz ein. Die Microsoft Azure Cloud (ISO/IEC 27001, ISO/IEC 27018, SOC 1, SOC 2, SOC 3, CSA STAR), Google Cloud (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC

1, SOC 2, SOC 3, CSA STAR) und PTC Cloud (ISO/IEC 27001, SOC 2 Type II, TISAX, FedRAMP) setzen eine umfassende USV ein und weitere Schutzmaßnahmen um (Firewall, Meldewege und Notfallpläne).
- Widerstandsfähigkeits- und Ausfallsicherheitskontrolle: Es sind u.a. redundante Datenanbindungen und Ausweichserver vorhanden.

6.4 Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DSGVO)

- Der Auftragnehmer strebt den kontinuierlichen Aufbau und die Implementierung eines umfassenden Datenschutz-Management-Systems an, einschließlich der Etablierung einer Governance zur DSGVO, eines Verarbeitungsverzeichnisses, der Benennung einer für den Datenschutz verantwortlichen Person sowie Schulungs- und Sensibilisierungsmaßnahmen für die Mitarbeiter.
- Ein Incident-Response-Management entsprechend den Vorgaben der DSGVO befindet sich in der Entwicklung.
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) werden sukzessive eingeführt.
- Die getroffenen Sicherheitsmaßnahmen werden regelmäßig überprüft und weiterentwickelt, um den Anforderungen zu entsprechen.
- Auftragskontrolle: Der Auftragnehmer überprüft kontinuierlich sein Datenschutz-Management und arbeitet daran, die datenschutzrechtliche Zuverlässigkeit seiner Unterauftragnehmer sicherzustellen.

7 Unterauftragsverarbeiter

7.1 Der Auftragnehmer darf Unterauftragsverarbeiter zur Verarbeitung hinzuzuziehen („Subunternehmer“), soweit sichergestellt ist, dass diese die Voraussetzungen von Art. 28 DSGVO und Ziffer 2.4 erfüllen.

7.2 Subunternehmer ist, wer Leistungen in direktem Zusammenhang mit Verarbeitung des Auftragnehmers erbringt. Wer lediglich Nebenleistungen erbringt, wie etwa Prüfung oder Wartung von Verarbeitungsverfahren oder -anlagen durch andere Stellen, Telekommunikationsleistungen, Post- und Transportdienstleistungen oder Benutzerservice sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Verarbeitungsanlagen, ist kein Subunternehmer.

7.3 Derzeit eingesetzte Subunternehmer sind (nach Unternehmen, Anschrift, Zweck, Ort der Verarbeitung):

(a) Inheaden GmbH
Hilpertstraße 31
64295 Darmstadt, Germany
inheaden.io
Dienstleister für Entwicklung und Betrieb der Software

7.4 Der Auftragnehmer darf Subunternehmer jederzeit austauschen, soweit er die Übertragung der Pflichten aus dieser AVV sicherstellt. Der Auftragnehmer teilt dem Auftraggeber jeden neuen Subunternehmer vorab in Textform mit. Soweit der Auftraggeber innerhalb von 30 Tagen nach Benachrichtigung keinen Widerspruch erhebt, gilt das Einverständnis als

erteilt. Erhebt der Auftraggeber aus wichtigem, dem Auftragnehmer nachgewiesenen Grund Widerspruch, darf der Auftragnehmer die Zusammenarbeit mit einer Frist von 3 Monaten kündigen.

8 Rechte der Betroffenen

8.1 Der Auftragnehmer unterstützt den Auftraggeber mit technisch-organisatorischen Maßnahmen in zumutbarem Maß, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der betroffenen Personen zustehenden Rechte nachzukommen. Soweit eine betroffene Person einen Anspruch auf Wahrnehmung der ihr zustehenden Rechte unmittelbar gegenüber dem Auftragnehmer erhebt, leitet der Auftragnehmer das Ersuchen zeitnah, spätestens innerhalb von 5 Werktagen, weiter.

8.2 Der Auftragnehmer teilt dem Auftraggeber Informationen über gespeicherte Daten, Empfänger auftragsgemäßer Weitergabe von Daten und Zweck der Speicherung mit, sofern dem Auftraggeber diese Informationen nicht selbst vorliegen oder er sie sich selbst beschaffen kann.

8.3 Der Auftragnehmer ermöglicht dem Auftraggeber, in erforderlichem und zumutbarem Maß, sowie gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten, Daten des Auftraggebers zu berichtigen, zu löschen, ihre weitere Verarbeitung einzuschränken oder auf Verlangen die Berichtigung, Sperrung oder Einschränkung der weiteren Verarbeitung selbst vorzunehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

9 Mitteilungen und Unterstützung

Der Auftragnehmer unterstützt den Auftraggeber gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Einhaltung der in den Art. 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und vorherige Konsultationen. Hierzu gehören

(a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, welche die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen sowie

(b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,

(c) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung und

(d) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

10 Datenlöschung

10.1 Der Auftraggeber definiert die Aufbewahrungs- und Löschfristen für Meldungen und deren Verarbeitung selbständig im Rahmen der ihm obliegenden rechtlichen Vorgaben. Nach Entfall der definierten Aufbewahrungspflicht sind die Daten vom Auftraggeber zu löschen.

10.2 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.3 Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen datenschutzgerecht zu vernichten oder, wenn explizit aufgefordert, dem Auftraggeber gegen eine Gebühr auszuhändigen. Gleiches gilt für Test- und Ausschussmaterial.

10.4 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

11 Nachweise und Überprüfung

11.1 Der Auftragnehmer stellt dem Auftraggeber auf Anforderung alle erforderlichen und vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach dieser AVV zur Verfügung. Der Auftraggeber darf die Einhaltung der Regelungen dieser AVV, insbesondere die Umsetzung der technischen-organisatorischen Maßnahmen, überprüfen. Dabei gilt was folgt:

11.2 Überprüfungen finden zu üblichen Geschäftszeiten ohne Störung des Betriebsablaufs beim Auftragnehmer sowie unter Beachtung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers statt. Der Auftraggeber informiert den Auftragnehmer in der Regel mindestens 14 Tage vorher über alle mit der Durchführung zusammenhängenden Umstände. Der Auftraggeber darf eine Überprüfung pro Kalenderjahr durchführen. Weitere Überprüfungen erfolgen gegen Kostenerstattung und nach Abstimmung mit dem Auftragnehmer.

11.3 Der Auftragnehmer darf nach eigenem Ermessen unter Berücksichtigung gesetzlicher Verpflichtungen Informationen zurückhalten, (i) welche sensibel im Hinblick auf seine Geschäfte sind, oder (ii) deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstößt. Der Auftraggeber erhält keinen Zugang zu Daten oder Informationen über (i) andere Kunden des Auftragnehmers, (ii) Kosten, (iii) Qualitätsprüfung- und Managementberichte sowie (iv) andere vertrauliche Daten des Auftragnehmers, die nicht unmittelbar relevant für die Auftragsverarbeitung sind.

11.4 Beauftragt der Auftraggeber einen Dritten mit der Durchführung, verpflichtet er diesen schriftlich (i) wie auch er gegenüber dem Auftragnehmer verpflichtet ist sowie (ii) auf Verschwiegenheit und Geheimhaltung, wenn der Dritte keiner beruflichen

Verschwiegenheitspflicht unterliegt. Auf Verlangen legt er die Verpflichtungserklärung vor. Es darf kein Wettbewerber des Auftragnehmers beauftragt werden.

11.5 Nach Wahl des Auftragnehmers kann der Nachweis durch Vorlage eines geeigneten, aktuellen Testats oder Berichts unabhängiger Instanzen (Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder geeigneter Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits (etwa BSI-Grundschutz) (insgesamt Prüfungsbericht) erbracht werden, wenn der Prüfungsbericht dem Auftraggeber ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

12 Dauer und Kündigung

Die Dauer der Verarbeitung sowie die Laufzeit und Kündigung dieser AVV richten sich nach der Laufzeit und Kündigung des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser AVV. Jede isolierte Kündigung dieser AVV ist ausgeschlossen. Die Bestimmungen der Ziffern 5 und 10 bleiben auch nach Beendigung des Hauptvertrages gültig.

13 Haftung

Die Haftung für die Auftragsverarbeitung richtet sich nach Art. 82 DSGVO. Im Übrigen richtet sich die Haftung nach dem Hauptvertrag.

14 Allgemeine Bestimmungen

14.1 Die Vergütung des Auftragnehmers ergibt sich aus dem zugrundeliegenden Hauptvertrag. Im Fall von Widersprüchen zwischen diesen AVV und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor. Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervor unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

14.2 Änderungen und Ergänzungen dieser Vereinbarung müssen in Textform erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

14.3 Diese Vereinbarung unterliegt deutschem Recht.

14.4 Sofern der Zugriff auf die Daten, die der Auftraggeber dem Auftragnehmer zur Datenverarbeitung übermittelt hat, durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat der Auftragnehmer den Auftraggeber unverzüglich hierüber zu benachrichtigen.

14.5 Die Einrede des Zurückbehaltungsrechts gemäß § 273 BGB wird hinsichtlich der verarbeiteten Daten und der dazugehörigen Datenträger ausgeschlossen.

App Leistungsbeschreibung

Stand: 11. November 2024

Bereitstellung

- Bereitstellung als cloudbasierte Software-as-a-Service (SaaS)
- Verfügbarkeit von 97% (Service Level)
- Einfaches Nutzungsrecht (Lizenz) zur Softwarenutzung
- Applikation ist über den Apple AppStore (ab iOS 14) und Google PlayStore (ab Android 11) verfügbar
- Kundensupport über support@augnect.de

Funktionen

- Augmented Reality und NFC-Wissensplattform
- Erstellung und Verwaltung von Wissensinhalten in verschiedenen Formaten (Text, Bild, Video, Link, PDF)
- Verankerung der Wissensinhalte an physische Objekte mithilfe verschiedener Technologien
- Menüführung in Deutsch und Englisch
- Speicherung unbegrenzter Datenmengen in Anlehnung an die Preisstaffelung
- Benachrichtigungsfunktionen per E-Mail

Kundenseitige Anpassungsmöglichkeiten

- Logo frei anpassbar (Design)

Datenschutz und Informationssicherheit der Softwareumgebung

- Hosting in der Microsoft Azure Cloud (ISO/IEC 27001, ISO/IEC 27018, SOC 1, SOC 2, SOC 3, CSA STAR), Google Cloud (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1, SOC 2, SOC 3, CSA STAR) und PTC Cloud (ISO/IEC 27001, SOC 2 Type II, TISAX, FedRAMP) setzen eine umfassende USV ein und weitere Schutzmaßnahmen um (Firewall, Meldewege und Notfallpläne).
- Konformität mit den Anforderungen der EU-Datenschutz-Grundverordnung (DSGVO)
- Auftragsverarbeitung mit Angabe der technisch-organisatorischen Maßnahmen
- Serverseitige Datenverschlüsselung
- TLS Transport-Verschlüsselung der Daten
- Zugang zu Unternehmensbereichen nur mit eindeutigen Registrierungscode und Email Verifizierung