Vertrag über Auftragsverarbeitung (AVV)

Fassungs-ID: dpa/2026-11/de

Anlage zu den Lizenzbedingungen Halocline Desktop und den Nutzungsbedingungen Halocline Web & XR

Fassung 2026-11, gültig ab 18.11.2026

zwischen

dem Kunden, wie er sich aus den bei der Registrierung oder Bestellung angegebenen Daten oder aus dem Angebot ergibt

– nachfolgend „Verantwortlicher“ genannt –

und

Halocline GmbH & Co. KG, Netter Platz 3, 49090 Osnabrück

– nachfolgend „Auftragsverarbeiter“ genannt –

und gemeinsam als „Vertragsparteien“ bezeichnet,

wird Folgendes vereinbart:

§ 1 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben. Dieser Vertrag gilt für alle Produkte des Auftragsverarbeiters, die der Verantwortliche nutzt (Halocline Desktop, Halocline Web & XR), soweit darin Auftragsverarbeitung nach Anhang 1 stattfindet.

§ 2 Weisungen des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

(4) Der Verantwortliche stellt sicher, dass über die Support-Kanäle des Auftragsverarbeiters keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und keine personenbezogenen Daten übermittelt werden, die für die Bearbeitung des jeweiligen Supportfalls nicht erforderlich sind.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die im Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die in Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter wesentliche Anpassungen dem Verantwortlichen unaufgefordert in Textform an die Admins des Verantwortlichen mit.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im Anhang 2 mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind. Für die in Anhang 1 ausgewiesenen Drittlandbezüge gilt die Zustimmung als erteilt.

§ 5 Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei der Erfüllung seiner Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

§ 6 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens drei Wochen im Voraus in Textform an die Admins des Verantwortlichen über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden, mit der Unterrichtung über die geplante Beauftragung zur Verfügung. Die jeweils aktuelle Liste der Unterauftragsverarbeiter ist unter https://halocline.io/de/unterauftragsverarbeiter abrufbar. Die Inanspruchnahme der in Anhang 1 zum Zeitpunkt des Vertragsschlusses aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrages genannten Voraussetzungen umgesetzt werden. Erhebt der Verantwortliche innerhalb von zwei Wochen nach Zugang der Unterrichtung begründete Einwände und finden die Parteien keine einvernehmliche Lösung, kann der Verantwortliche den Vertrag über das betroffene Produkt ohne Einhaltung einer Frist zum Zeitpunkt der beabsichtigten Beauftragung kündigen.

(2) Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Artikel 44 ff. DSGVO sicher, indem – sofern erforderlich – geeignete Garantien gemäß Artikel 46 DSGVO getroffen werden.

(4) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(5) Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach Klausel 14 der Standardvertragsklauseln (Transfer Impact Assessment) durch und stellt diese dem Verantwortlichen auf Anfrage zur Verfügung; die Pflichten aus Klausel 15 der Standardvertragsklauseln werden beachtet. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen

werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen. Die Nachweiserbringung erfolgt vorrangig durch die Bereitstellung geeigneter Dokumentation und einschlägiger Zertifizierungen; Prüfungen vor Ort kommen in Betracht, soweit diese Nachweise im Einzelfall nicht ausreichen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt. Regelprüfungen finden höchstens einmal je Kalenderjahr statt und werden mindestens vier Wochen im Voraus angekündigt; anlassbezogene Prüfungen bei Anzeichen für eine Nichteinhaltung bleiben unberührt. Die Kosten eines vom Verantwortlichen beauftragten Prüfers trägt der Verantwortliche.

(3) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 8 Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 9 Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung werden personenbezogene Daten aus den aktiven Systemen nach Wahl des Verantwortlichen gelöscht oder zurückgegeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung besteht. Die Rückgabe erfolgt durch Bereitstellung zum Abruf nach den Bedingungen des jeweiligen Produkts. Trifft der Verantwortliche bis zum Ablauf dieser Bereitstellungsfrist keine Wahl, werden die Daten gelöscht. Bestehende Sicherungskopien werden im Rahmen des regulären Sicherungszyklus turnusmäßig überschrieben und stehen nach Ablauf des in den technischen und organisatorischen Maßnahmen definierten Aufbewahrungszeitraums nicht mehr zur Verfügung; eine Wiederherstellung gelöschter Daten aus Sicherungen erfolgt nicht. Die Löschung wird dem Verantwortlichen in Textform angezeigt.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

§ 10 Zustandekommen, Form und Schlussbestimmungen

(1) Dieser Vertrag ist Anlage der Lizenzbedingungen Halocline Desktop und der Nutzungsbedingungen Halocline Web & XR. Er kommt zustande, indem der Verantwortliche im Registrierungs- oder Bestellprozess die jeweiligen Bedingungen akzeptiert oder ein Angebot des Auftragsverarbeiters annimmt, dem er beigefügt ist (Art. 28 Abs. 9 DSGVO, elektronisches Format). Maßgeblich ist die bei Abschluss gültige Fassung; der Auftragsverarbeiter stellt dem Verantwortlichen diese Fassung mit der Bestätigung des Vertragsschlusses in speicherbarer Form zur Verfügung und hält sie zum Abruf bereit.

(2) Die Laufzeit dieses Vertrags entspricht der Laufzeit des Vertrags über die Nutzung des jeweiligen Produkts. Er endet mit dessen Beendigung, soweit der Auftragsverarbeiter keine personenbezogenen Daten des Verantwortlichen mehr verarbeitet.

(3) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(4) Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann. Änderungen dieses Vertrags durch den Auftragsverarbeiter richten sich nach dem Änderungsverfahren der Bedingungen (dort E.7): Ankündigung in Textform an die Admins, Annahme durch einen Admin; ohne Annahme gilt die bisherige Fassung. Bei kostenlosen Verträgen und Bildungslizenzen ist eine Weiternutzung nach dem Wirksamwerden nur nach Annahme möglich; bei

kostenpflichtigen Verträgen gilt die geänderte Fassung ab der nächsten Verlängerung als angenommen, wenn der Verantwortliche nicht bis zum Ende der laufenden Laufzeit kündigt. Für die Beauftragung neuer Unterauftragsverarbeiter gilt ausschließlich § 6.

(5) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln in Fragen des Datenschutzes Vorrang.

(6) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Bei Abschluss über ein Angebot:

Verantwortlicher	**Auftragsverarbeiter**
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:

Anhang 1

Auflistung der beauftragten Dienstleistungen und der Unterauftragsverarbeiter einschließlich der Verarbeitungsstandorte

Lizenz-, Authentifizierungs-, Analyse- und Support-Kommunikationsdaten verarbeitet Halocline als eigenständiger Verantwortlicher (Art. 4 Nr. 7 DSGVO); die Support-Kommunikation selbst (Kontaktdaten, Fallbeschreibung, Korrespondenz) ist nicht Gegenstand dieses Vertrags. Einzelheiten ergeben sich aus der öffentlichen Datenschutzinformation zum jeweiligen Produkt (Halocline Desktop: https://halocline.io/de/datenschutz/desktop; Halocline Web & XR: https://halocline.io/de/datenschutz/web-xr). Für Anhänge, die der Verantwortliche oder seine Nutzer im Rahmen einer Supportanfrage übermitteln, gilt der nachfolgende Eintrag „Support-Anhänge“.

Welche der nachfolgenden Verarbeitungstätigkeiten im Einzelfall stattfinden, richtet sich nach dem vom Verantwortlichen genutzten Produkt und den aktivierten Funktionen.

Verarbeitungstätigkeit	**Bereitstellung und Betrieb des Cloud-Service Halocline Web & XR**
Zweck	Hosting und Verarbeitung der vom Verantwortlichen eingebrachten Daten in mandantenspezifischen Produktdatenbanken und Dateicontainern
Datenkategorien	Vom Verantwortlichen und dessen Nutzern eingegebene oder hochgeladene Inhalte, soweit sie personenbezogene Daten enthalten (z. B. Namen in Planungsständen, Kommentaren, Dateien); Bearbeiter- und Änderungszuordnungen
Rechtsgrundlage	Verarbeitung im Auftrag des Verantwortlichen (Art. 28 DSGVO); die Rechtsgrundlage der Verarbeitung bestimmt der Verantwortliche
Betroffene Personen	Nutzer des Verantwortlichen; Personen, deren Daten in den eingebrachten Inhalten enthalten sind
Empfänger / Unterauftragsverarbeiter	Microsoft Ireland Operations Limited (Azure Frankfurt/DE; SQL-Datenbanken, Blob Storage); AVV über das Microsoft Products and Services DPA. Hetzner Online GmbH (Nürnberg/DE; von Halocline administrierte Datenbanken); AVV abgeschlossen
Speicherfrist	Dauer der Auftragsverarbeitung; bei Beendigung Löschung oder Rückgabe gemäß § 9 (Löschung von Produktdatenbank und Dateicontainer als Einheit)

Verarbeitungstätigkeit	Bereitstellung und Betrieb des Cloud-Service Halocline Web & XR
Drittlandtransfer	Kein Drittlandtransfer

Verarbeitungstätigkeit	Data-Sync für Halocline Desktop (optionale Zusatzleistung, nur bei Beauftragung durch den Verantwortlichen)
Zweck	Synchronisation von Planungsdaten zwischen Geräten
Datenkategorien	Synchronisierte Projektdaten des Verantwortlichen, soweit sie personenbezogene Daten enthalten (z. B. Namen in Planungsständen, Kommentaren, Dateien); Synchronisierungsmetadaten; Bearbeiter- und Änderungszuordnungen
Rechtsgrundlage	Verarbeitung im Auftrag des Verantwortlichen (Art. 28 DSGVO); die Rechtsgrundlage der Verarbeitung bestimmt der Verantwortliche
Betroffene Personen	Nutzer des Verantwortlichen; Personen, deren Daten in den synchronisierten Projektdaten enthalten sind
Empfänger / Unterauftragsverarbeiter	Hetzner Online GmbH (Nürnberg/DE; von Halocline administrierte Datenbanken); AVV abgeschlossen. Microsoft Ireland Operations Limited (Azure Frankfurt/DE; Synchronisierungsdienst, Blob Storage); AVV über das Microsoft Products and Services DPA
Speicherfrist	Dauer der Auftragsverarbeitung; bei Beendigung Löschung oder Rückgabe gemäß § 9
Drittlandtransfer	Kein Drittlandtransfer

Verarbeitungstätigkeit	Support-Anhänge (Dateien, die der Verantwortliche oder seine Nutzer einer Supportanfrage beifügen; alle Produkte)
Zweck	Bearbeitung des jeweiligen Supportfalls
Datenkategorien	Personenbezogene Daten in beigefügten Dateien (z. B. Screenshots, Auszüge aus Planungsständen, Protokolldateien), soweit vorhanden; welche Dateien beigefügt werden, bestimmt der Verantwortliche bzw. dessen Nutzer
Rechtsgrundlage	Verarbeitung im Auftrag des Verantwortlichen (Art. 28 DSGVO); die Rechtsgrundlage der Verarbeitung bestimmt der Verantwortliche
Betroffene Personen	Nutzer des Verantwortlichen; Personen, deren Daten in den beigefügten Dateien enthalten sind
Empfänger / Unterauftragsverarbeiter	Support-Ticketsystem: Zendesk, Inc. (USA); Speicherung in der EU-Datenregion (Rechenzentrum Irland). Für Support- oder sonstige Leistungen, die Halocline bei Zendesk anfordert, können Zendesk und deren Unterauftragsverarbeiter Daten im Einzelfall außerhalb des EWR verarbeiten; der Support von Halocline gegenüber ihren Kunden ist davon nicht betroffen. Grundlage ist der Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework (Art. 45 DSGVO), nach dem Zendesk, Inc. zertifiziert ist; ergänzend gelten die genehmigten Binding Corporate Rules von Zendesk (Art. 46 Abs. 2 lit. b, Art. 47 DSGVO). AVV abgeschlossen. Bis zur Übergabe an Zendesk bei Anfragen über die Website: Hetzner Online GmbH (Nürnberg/DE, Website-Server); Löschung der Anhänge unmittelbar nach Übergabe, Sicherungen des Website-Servers werden nach 14 Tagen überschrieben. Falls Zendesk nicht erreichbar ist: Microsoft Ireland Operations Limited (Azure Communication Services, Frankfurt/DE; E-Mail-Versand an das Support-Team)

Verarbeitungstätigkeit	Support-Anhänge (Dateien, die der Verantwortliche oder seine Nutzer einer Supportanfrage beifügen; alle Produkte)
Speicherfrist	Löschung mit dem jeweiligen Ticket, spätestens 3 Jahre nach Abschluss des Supportfalls. Bei Beendigung werden die beigefügten Dateien gemäß § 9 aus den Tickets der Organisation entfernt. Auf dokumentierte Weisung werden einzelne beigefügte Dateien aus dem betroffenen Ticket entfernt; dies ist auch bei bereits geschlossenen Tickets möglich. Ist eine Entfernung für den jeweiligen Eingangskanal technisch nicht vorgesehen, erfolgt die Entfernung durch Löschung des betroffenen Tickets.
Drittlandtransfer	Im Einzelfall möglich (Zendesk, siehe Empfänger); abgesichert durch das EU-U.S. Data Privacy Framework (Art. 45 DSGVO) und Binding Corporate Rules (Art. 46 Abs. 2 lit. b, Art. 47 DSGVO)

Anhang 2

Kontaktdaten der Datenschutzbeauftragten

Rolle	Kontakt
Datenschutzbeauftragte/r des Verantwortlichen	Wie vom Verantwortlichen mitgeteilt; bei Abschluss über ein Angebot im Angebot benannt
Datenschutzbeauftragte/r des Auftragsverarbeiters	datenschutz nord GmbH, Konsul-Smidt-Str. 88, 28217 Bremen, E-Mail: office@datenschutz-nord.de

Anhang 3

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

Stand der technischen und organisatorischen Maßnahmen bei Vertragsschluss. Anpassungen richten sich nach § 3 Abs. 2 dieses Vertrags.

0. Geltungsbereich und Fortschreibung

Diese Maßnahmen gelten für den von Halocline betriebenen Cloud-Service einschließlich Data-Sync. Die lokal beim Kunden betriebene Client-Software liegt in der Betriebsverantwortung des Kunden; für sie gelten die Maßnahmen der jeweiligen Kundenorganisation.

Die Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung; sie können angepasst werden, sofern das Schutzniveau der vereinbarten Maßnahmen dabei nicht unterschritten wird. Wesentliche Anpassungen werden dem Verantwortlichen mitgeteilt.

1. Technische Maßnahmen

1.1 Verschlüsselung

Übertragung (Transit):

- Alle extern erreichbaren Endpunkte erzwingen HTTPS mit aktueller Transportverschlüsselung (TLS 1.2 oder höher; moderne TLS-Policy am Gateway, dauerhafte Umleitung unverschlüsselter Anfragen).
- Keine unverschlüsselte Übertragung personenbezogener Daten; auch die Verbindungen zu den von Halocline auf angemieteter Hosting-Infrastruktur administrierten Datenbanken erfordern TLS.

Speicherung (At-Rest):

- Microsoft Azure SQL-Datenbanken: Transparent Data Encryption (TDE).
- Azure Storage: Verschlüsselung at-rest mit Microsoft-verwalteten Schlüsseln.
- Datenträger der von Halocline auf angemieteter Hosting-Infrastruktur administrierten Datenbanken: vollständige Datenträgerverschlüsselung (Full-Disk-Encryption, AES-256); der Schutz wirkt gegen physischen Zugriff auf die Speichermedien.

Schlüsselverwaltung:

- Kryptografisches Material wird in verwalteten Key Vaults gehalten, getrennt von Anwendungs- und Middleware-Schicht; Applikationsgeheimnisse der plattform-gehosteten Dienste werden zur Laufzeit über die Managed Identity des jeweiligen Dienstes aufgelöst.
- TLS-Zertifikate werden automatisch ausgestellt und erneuert.
- Zugangsgeheimnisse außerhalb dieses Musters werden nach festem Turnus rotiert.

1.2 Zugriffskontrolle auf Produktionssysteme

- Der Zugriff auf Produktionssysteme erfolgt über personalisierte Konten mit rollenbasierter Zugriffskontrolle (RBAC) nach dem Prinzip der minimalen Rechte.
- Administrative Rechte liegen auf dedizierten, vom Alltagskonto getrennten Konten; administrative Anmeldungen an den Cloud-Management-Konsolen erfordern phishing-resistente Multi-Faktor-Authentifizierung über einen kontrollierten Netzwerkpfad; die Konsole des Hosting-Anbieters erfordert ein persönliches Konto mit zweitem Faktor. Ausgenommen sind allein versiegelte, überwachte Notfallzugangskonten.
- Versiegelte Notfallzugänge (Break-Glass) mit Anmeldealarm sind eingerichtet.
- Technische Identitäten sind inventarisiert und einer benannten verantwortlichen Person zugeordnet.
- Unternehmensgeräte werden zentral verwaltet und sind vollständig verschlüsselt; Fernsperrung und Fernlöschung stehen zur Verfügung.
- Zugriffsrechte werden zentral verwaltet und bei Ausscheiden im Rahmen des dokumentierten Offboarding-Prozesses entzogen.
- Die verwalteten Azure-Datenbanken akzeptieren keinen öffentlichen Netzwerkzugriff; Speicherkonten für Kundendaten und Sicherungen verweigern öffentlichen Netzwerkzugriff standardmäßig. Datenbanken, die Halocline in eigener Software-Verantwortung auf angemieteter Infrastruktur eines Hosting-Anbieters administriert, sind ausschließlich über kontrollierte Netzwerkpfade erreichbar; der Zugang erfordert Multi-Faktor-Authentifizierung.

1.3 Endnutzer-Authentifizierung

- Kundenauthentifizierung erfolgt über Microsoft Entra External ID (B2C) mit sicheren lokalen Konten.
- Integrierte Passwort-Komplexitätsvorgaben und Account-Lockout-Mechanismen gemäß Microsoft Entra Security Standards.
- Tokenbasiertes Session-Management; Passwörter werden nicht in Halocline-eigenen Systemen gespeichert.

- Authentifizierungsprozesse basieren auf sicheren OAuth2-/Token-Mechanismen.

Hinweis: Die Passwortqualität auf Seite der Endnutzer liegt in der Verantwortung der jeweiligen Kundenorganisation. Halocline stellt die technischen Sicherheitsmechanismen (Komplexitätsregeln, Lockout) über Entra External ID bereit, kann jedoch keine Kontrolle über das tatsächliche Nutzerverhalten ausüben.

1.4 Netzwerksicherheit

- Ausschließlich verschlüsselte externe Kommunikation (siehe 1.1).
- Netzwerksegmentierung über virtuelle Netzwerke und dedizierte Subnetze; Netzwerk-Zugriffsregeln beschränken ein- und ausgehenden Datenverkehr auf definierte Regeln.
- Eine Web Application Firewall am Gateway erkennt und protokolliert Angriffsmuster; die Authentifizierungsendpunkte unterliegen einer Ratenbegrenzung.
- Basisschutzmechanismen der Cloud-Plattform gegen volumetrische Angriffe.

1.5 Zutrittskontrolle und Mandantentrennung

Serverinfrastruktur: Halocline betreibt kein eigenes Hosting-Rechenzentrum für den Cloud-Service; die Produktionsinfrastruktur wird vollständig über Microsoft Azure (Frankfurt) und Hetzner Online GmbH (Nürnberg) bereitgestellt. Der physische Schutz der Rechenzentren obliegt den jeweiligen Anbietern (Microsoft: u. a. ISO-27001-zertifizierte Rechenzentren; Hetzner: eigene Rechenzentren in Deutschland mit Zutrittskontrollsystemen, Videoüberwachung und Sicherheitspersonal). Der unternehmenseigene Technikraum dient ausschließlich interner Build- und CI-Infrastruktur und liegt außerhalb des Kundendatenpfads.

Büroräume: Der Zugang zu den Büroräumen von Halocline ist durch ein elektronisches Zutrittskontrollsystem gesichert. Zutritt erhalten ausschließlich autorisierte Mitarbeitende.

Homeoffice: Halocline-Mitarbeitende sind vertraglich verpflichtet, ihren Arbeitsbereich im Homeoffice angemessen gegen unbefugten Zutritt zu sichern. Der Zugriff auf Unternehmenssysteme erfolgt über zentral verwaltete Geräte; administrative Zugänge erfordern Multi-Faktor-Authentifizierung (siehe 1.2).

Mandantentrennung:

- Kundendaten werden je Mandant getrennt gehalten: Produktdatenbanken und Dateicontainer sind je Kunde dediziert; ein dokumentiertes Trennungskonzept legt je Dienst fest, wie die Trennung erreicht und wo sie durchgesetzt wird.
- Mandantenübergreifender Zugriff wird durch rollen- und tokenbasierte Zugriffskontrollen der Autorisierungsschicht unterbunden.

1.6 Verfügbarkeit, Datensicherung und Wiederherstellbarkeit

- Automatisierte, regelmäßige Sicherungen der produktiven Datenbanken über definierte Aufbewahrungszeiträume: Sicherungen der selbst betriebenen Datenspeicher werden verschlüsselt an einen getrennten Standort eines anderen Anbieters übertragen; die plattformverwalteten Datenspeicher sind durch die Mechanismen der Plattform geschützt (Point-in-Time-Wiederherstellung für die verwalteten Azure-Datenbanken, Soft Delete für gespeicherte Dateien). Einzelheiten regelt das Backup- und Wiederherstellungskonzept.

- Die von Halocline auf angemieteter Hosting-Infrastruktur administrierten Datenbanken sind redundant mit automatischem Failover ausgelegt.
- Wiederherstellungen werden regelmäßig getestet; Durchführung und Ergebnis werden dokumentiert.
- Ein dokumentierter Notfall- und Wiederanlaufplan mit definierten Wiederherstellungszielen liegt vor.
- Die Verfügbarkeit der Überwachungskomponenten wird ihrerseits überwacht, ergänzt um unabhängige externe Verfügbarkeitsprüfungen außerhalb der primären Cloud-Umgebung; Störungen werden an verantwortliche Mitarbeitende alarmiert.
- Infrastruktur-Deployments erfolgen über Infrastructure as Code für konsistente und reproduzierbare Umgebungen.

1.7 Protokollierung und Nachvollziehbarkeit

- Zugriffe auf personenbezogene Daten sowie administrative Aktivitäten werden protokolliert; die Betriebsprotokollierung des Cloud-Service erfolgt innerhalb der Cloud-Plattform-Umgebung.
- Änderungen an personenbezogenen Daten und an Systemkonfigurationen sind nachvollziehbar (Protokollierung administrativer Tätigkeiten, Versionierung der Infrastruktur als Code, Deployment-Historie).
- Authentifizierungsereignisse werden über Microsoft Entra Audit Logging erfasst.
- Protokolldaten werden für den in der Logging-Richtlinie definierten Zeitraum aufbewahrt und anschließend automatisch gelöscht.
- Sicherheitsrelevante Ereignisse werden automatisiert überwacht; Alarme werden nach Schweregrad priorisiert.
- Der Zugriff auf Protokolldaten ist über rollenbasierte Zugriffskontrollen geregelt.

1.8 Schwachstellen- und Patch-Management, sichere Entwicklung

- Sicherheitsupdates werden innerhalb definierter Zeitfenster eingespielt; die Serverhosts unter eigener Betriebssystem-Verantwortung erhalten planmäßige signaturbasierte Schadsoftware-Prüfungen und automatische Sicherheitsupdates.
- Host-Konfigurationen werden regelmäßig gegen dokumentierte Härtungs-Baselines geprüft.
- Der Entwicklungsprozess umfasst Code-Reviews durch qualifizierte Entwickler, statische Analyse des eigenen Quellcodes und die kontinuierliche Auswertung bestätigter Schwachstelleninformationen für eingesetzte Fremdbibliotheken; Funde werden nach definierten Schweregradkriterien klassifiziert und innerhalb definierter Zeitfenster behoben.
- Sicherheits- und Datenschutzanforderungen sind in den Entwicklungsprozess integriert.

1.9 Trennung von Test- und Produktivumgebungen

- Produktivumgebungen sind von Test- und Entwicklungsumgebungen durch getrennte Subskriptionen und getrennte Deployments logisch separiert; Daten aus der Produktivumgebung werden nicht in Test- oder Entwicklungsumgebungen verwendet.

- Eine geteilte Analysekomponente nimmt ausschließlich Telemetrie der Client-Software auf (aus produktiver und interner Nutzung gemeinsam); Daten aus dem Betrieb des Cloud-Service werden dort nicht verarbeitet. Zugriffe und Datenbestände sind strikt über Indizes und Zugriffsrechte getrennt, der Zugriff liegt bei wenigen benannten Administratoren, Kunden haben keinen Zugriff.

2. Organisatorische Maßnahmen

2.1 Governance, Verantwortlichkeiten und Wirksamkeitsprüfung

- Halocline betreibt ein strukturiertes Informationssicherheits-Governance-Framework; Informationssicherheitsverantwortlichkeiten sind klar definierten Rollen zugewiesen (CISO, externer Datenschutzbeauftragter).
- Verarbeitungstätigkeiten werden hinsichtlich technischer und organisatorischer Sicherheitsmaßnahmen risikobasiert gemäß Art. 32 DSGVO bewertet; die Bewertungen werden dokumentiert.
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen ist etabliert: interne Audits, Management-Review im Jahresturnus sowie definierte technische Prüfungen je Maßnahmenbereich.

2.2 Vertraulichkeit, Schulung und Sensibilisierung

- Mitarbeitende mit Zugriff auf personenbezogene Daten sind arbeitsvertraglich auf Vertraulichkeit verpflichtet.
- Regelmäßige Datenschutz- und Informationssicherheitsschulungen werden durchgeführt; die Teilnahme wird dokumentiert.

2.3 Management von Unterauftragsverarbeitern

- Dienstleister werden anhand definierter Sicherheits- und Datenschutzkriterien ausgewählt; neue Dienstleister durchlaufen vor dem Onboarding eine interne Prüfung.
- Mit allen relevanten Dienstleistern werden Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO abgeschlossen.
- Die Einhaltung der Anforderungen wird anhand der vertraglich vorgesehenen Nachweise überprüft; die Prüffrequenz folgt der Risikoklassifizierung des Dienstleisters.

2.4 Privacy by Design und by Default

- Personenbezogene Daten werden auf das für den Verarbeitungszweck notwendige Minimum beschränkt (Datenminimierung).
- Tracking- und Analysedaten werden ohne direkte Identifikatoren (Name, E-Mail-Adresse) verarbeitet.

2.5 Umgang mit Sicherheitsvorfällen und Datenschutzverletzungen

- Ein dokumentierter Prozess zur Identifikation, Bewertung, Klassifizierung und Eskalation von Sicherheitsvorfällen ist etabliert; eine benannte Response-Funktion mit Vertretungsregelung koordiniert die Behandlung.

- Bei Verletzungen des Schutzes personenbezogener Daten wird der Verantwortliche unverzüglich unterrichtet, mit den Angaben nach Art. 33 Abs. 3 DSGVO (Art der Verletzung, betroffene Kategorien und ungefähre Zahl, Kontaktstelle, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen), damit der Verantwortliche seine Melde- und Benachrichtigungspflichten (Art. 33, 34 DSGVO) fristgerecht erfüllen kann.
- Halocline unterstützt den Verantwortlichen bei der Untersuchung, bei Meldungen an Aufsichtsbehörden und bei der Benachrichtigung betroffener Personen im Rahmen der vertraglichen Pflichten.
- Sicherheitsvorfälle werden dokumentiert; nach Abschluss werden die Behebung festgehalten und betroffene Kunden gemäß den vertraglichen Vereinbarungen informiert.

2.6 Löschung und Rückgabe personenbezogener Daten

- Mit Beendigung der Auftragsverarbeitung werden personenbezogene Daten nach Wahl des Verantwortlichen gelöscht oder zurückgegeben, soweit keine gesetzliche Aufbewahrungspflicht besteht; die Löschung wird in Textform angezeigt.
- Die Löschung erfolgt auf Mandantenebene: die Produktdatenbank und der Dateicontainer des Kunden werden als Einheit gelöscht.
- Bestehende Sicherungskopien werden im Rahmen des regulären Sicherungszyklus turnusmäßig überschrieben und stehen spätestens 379 Tage nach der Löschung aus den aktiven Systemen nicht mehr zur Verfügung (Aufbewahrung von zwölf Monatsgenerationen zuzüglich 14 Tage Löschschutz des Sicherungsspeichers); eine Wiederherstellung gelöschter Daten aus Sicherungen erfolgt nicht.
- Ein dokumentiertes Löschkonzept regelt Zuständigkeiten, Fristen und Nachweise.