

AVV & TOM's



amber Auftragsverarbeitungsvertrag

Stand: Juli 2026

An	Unsere (potenziellen) Kunden/Partner
	- Nachfolgend "Auftraggeber" genannt -
Von	amber Tech GmbH Jülicher Str 72a 52070 Aachen
	- Nachfolgend "Auftragnehmer" genannt -

Ansprechpartner	Bastian Maiworm
Kontakt	
Mobil	+49 (0) 157 3707 3220
Festnetz	+49 (0) 241-559708-12
Email	Bastian@amber.de

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im bereits geschlossenen Vertrag (nachfolgend „Hauptvertrag“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die „Vereinbarung“), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

Zudem weisen wir darauf hin, dass die amber Tech GmbH ISO27001 zertifiziert ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „Betroffener“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogene Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrische Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Vertragsgegenstand

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen die im Hauptvertrag genannten Leistungen. Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung, so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Arten der verarbeiteten Daten, Kreis der Betroffenen, Drittland

- (1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten.
- (2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.
- (3) Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) darf unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

§ 5 Schutzmaßnahmen des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Verantwortlichen erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.
- (2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in Anlage 3 genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.
- (3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend "Mitarbeiter"), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.
- (4) Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

Für Auftraggeber mit entsprechendem Leistungspaket:

- (5) Der Auftragsverarbeiter verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Verantwortlichen, die unter ein Berufsgeheimnis im Sinne des § 203 StGB fallen, die für diesen Auftrag relevanten Geheimschutzregeln zu beachten. Der Auftragsverarbeiter ist zur Verschwiegenheit über alle Tatsachen verpflichtet, die ihm im Zusammenhang mit dem Auftrag bekannt werden und zu denen der Verantwortliche ihm den Zugang eröffnet hat. Der Auftragsverarbeiter ist ferner verpflichtet, die zur Vertragserfüllung herangezogenen Beschäftigten und Unterauftragsverarbeiter nach den Vorgaben des § 203 Abs. 4 StGB zur Verschwiegenheit zu verpflichten und bei ihrer Tätigkeit zu überwachen.

§ 6 Informationspflichten des Auftragsverarbeiters

- (1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters durch die Datenschutz-Aufsichtsbehörde. Die

Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich, mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der von dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen zu unterrichten.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann jährlich von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters erforderlich sind.

(3) Der Verantwortliche dokumentiert das Kontrollergebnis und teilt es dem Auftragsverarbeiter mit. Bei Fehlern oder Unregelmäßigkeiten, die der Verantwortliche insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragsverarbeiter unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Verantwortliche dem Auftragsverarbeiter die notwendigen Verfahrensänderungen unverzüglich mit.

§ 8 Einsatz von Dienstleistern

(1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in Anlage 4 genannten Dienstleister (nachfolgend "Unterauftragsverarbeiter") durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.

(2) Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche kann gegen eine beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters aus wichtigem datenschutzrechtlichen Grund Einspruch erheben.

(3) Der Einspruch gegen die beabsichtigte Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters ist innerhalb von 2 Wochen nach Erhalt der Information über die Änderung zu erheben. Wird kein Einspruch erhoben, gilt die Hinzuziehung oder Ersetzung als genehmigt. Liegt ein wichtiger datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösungsfindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter nicht möglich, steht dem Auftragsverarbeiter ein Sonderkündigungsrecht zum auf den Einspruch folgenden Monatsende zu.

(4) Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

(5) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.

(6) Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) darf unter den Voraussetzungen der Art. 44 ff. DSGVO stattfinden.

§ 9 Anfragen und Rechte Betroffener

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragsverarbeiter allein der Verantwortliche gegenüber dem Betroffenen verantwortlich.

(2) Der Auftragsverarbeiter haftet für Schäden unbeschränkt, soweit die Schadensursache auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung des Auftragsverarbeiters, seines gesetzlichen Vertreters oder Erfüllungsgehilfen beruht.

(3) Für fahrlässiges Verhalten haftet der Auftragsverarbeiter nur bei Verletzung einer Pflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Verantwortliche regelmäßig vertraut und vertrauen darf, jedoch beschränkt auf den vertragstypischen Durchschnittsschaden. Im Übrigen ist die Haftung des Auftragsverarbeiters - auch für seine Erfüllungs- und Verrichtungsgehilfen - ausgeschlossen.

(4) Die Haftungsbegrenzung gemäß § 10.3 gilt nicht für Schadensersatzansprüche aus der Verletzung von Leben, Körper, Gesundheit oder aus der Übernahme einer Garantie.

§ 11 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder anderem anwendbaren nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung auf Anfrage zu führen.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

(3) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 12 Schlussbestimmungen

(1) Soweit der Auftragsverarbeiter Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn, eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben diese Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht.

Anlagen

Anlage 1: Beschreibung der Daten/Datenkategorien

Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten
- ☒ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☒ Inhalte indexierter bzw. durchsuchter Dateien (z. B. Texte und Bilder), soweit diese personenbezogene Daten enthalten
- ☒ Suchanfragen und Chatverläufe, soweit diese personenbezogene Daten enthalten
- ☒ Nutzungs- und Protokolldaten

Anlage 2: Beschreibung der Betroffenen/Betroffenengruppen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☒ Interessenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☒ Handelsvertreter
- ☒ Ansprechpartner
- ☒ Die Kategorien der Daten betroffener Personen der möglicherweise verarbeiteten Daten, können nicht genau bestimmt werden, da sie Nebenprodukt der Dienstleistung sind. Es können somit alle Kategorien betroffen sein.

Anlage 3: Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1.1. Auftragsverarbeiter

Auftragsverarbeiter gem. Art. 4 Nr. 8 EU-Datenschutz-Grundverordnung (DSGVO) ist amber Tech GmbH, Jülicher Straße 72a, 52070 Aachen, Deutschland, E-Mail: info@amber.de. Gesetzlich vertreten werden wir durch Philipp Reissel, Bastian Maiworm, Igli Manaj.

1.2. Datenschutzbeauftragter

Unser Datenschutzbeauftragter ist die heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, E-Mail: datenschutz@heydata.eu.

1.3. Gegenstand des Dokuments

Dieses Dokument fasst die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Auftragsverarbeiter personenbezogene Daten schützt. Das Dokument hat den Zweck, den Verantwortlichen bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu unterstützen.

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

Zutrittskontrolle

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden zu verwehren.

Technische Maßnahmen	Organisatorische Maßnahmen
Alarmanlage	Personenkontrolle beim Pförtner / Empfang
Chipkarten- / Transponder-Schließsystem	Arbeit im Home Office: Anweisung an Mitarbeiter, wenn möglich, in von Wohnräumen abgetrennten Arbeitszimmer zu arbeiten
Videoüberwachung der Zugänge	Sorgfältige Auswahl des Reinigungspersonals
Automatisches Zugangskontrollsystem	Besucher nur in Begleitung durch Mitarbeiter
Schließsystem mit Codesperre	Sorgfältige Auswahl von Sicherheitspersonal
Manuelles Schließsystem (z.B. Schlüssel)	Protokollierung der Besucher (z.B. Besucherbuch)
	Personenkontrolle beim Pförtner oder Empfang

Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können

Technische Maßnahmen	Organisatorische Maßnahmen
Authentifikation mit Benutzernamen + Passwort	Benutzerberechtigungen verwalten
Verschlüsselung von Datenträgern	Richtlinie „sicheres Passwort“ / Zentrale Passwortregeln
Einsatz von Anti-Viren-Software	Personenkontrolle beim Pförtner oder Empfang

Einsatz von Mobile Device Management	Protokollierung der Besucher (z.B. Besucherbuch)
Einsatz von VPN-Technologie bei Remote-Zugriffen	Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit
Sperren externer Schnittstellen (z.B. USB-Anschlüsse)	Unternehmens-Richtlinie für sichere Passwörter
Automatische Desktopsperre	Unternehmens-Richtlinie "Löschen/Vernichten"
Verschlüsselung von Notebooks / Tablets	Unternehmens-Richtlinie "Cleandesk"
Erstellen von Benutzerprofilen	Unternehmens-Richtlinie zur Verwendung mobiler Geräte
	Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren

Zugriffskontrolle

Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten, ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Aktenvernichtern (mit cross cut-Funktion)	Anzahl der Administratoren auf das »Notwendigste« reduzieren
Physische Löschung von Datenträgern vor deren Wiederverwendung	Verwaltung der Benutzerrechte durch Systemadministratoren
Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	Anweisung an Mitarbeiter, dass nur unbedingt erforderliche Daten ausgedruckt werden
Protokollierung der Vernichtung von Daten	Sichere Aufbewahrung von Datenträgern
Einsatz eines Berechtigungskonzepts	Verwaltung der Benutzerrechte durch Systemadministratoren
	Anweisung an Mitarbeiter, dass Daten nur nach Rücksprache gelöscht werden

Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

Technische Maßnahmen	Organisatorische Maßnahmen
Trennung von Produktiv- und Testsystem	Erstellung eines Berechtigungskonzepts
Logische Mandantentrennung (softwareseitig)	Festlegung von Datenbankrechten
Bei pseudonymisierten Daten: Getrennte Aufbewahrung der Zuordnungsdatei auf einem getrennten, abgesicherten IT-System (möglichst verschlüsselt)	Versehen der Datensätze mit Zweckattributen/Datenfeldern
	Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist, wenn möglich, zu anonymisieren/pseudonymisieren.

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

Weitergabekontrolle

Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und das überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	Organisatorische Maßnahmen
Einrichtungen von VPN-Tunneln	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen
WLAN-Verschlüsselung (WPA2 mit starkem Passwort)	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
Protokollierung von Zugriffen und Abrufen	Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
Bereitstellung von Daten über verschlüsselte Verbindungen wie SFTP oder HTTPS	Uploadverbot dienstlicher Daten auf unternehmensfremde Server
Nutzung von Signaturverfahren	Home Office: Fernlöschungsrecht des Arbeitgebers

Eingabekontrolle

Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
Manuelle oder automatisierte Kontrolle der Protokolle	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übernommen worden sind	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	Organisatorische Maßnahmen
Unterbrechungsfreie Stromversorgung (USV)	Erstellen eines Backup- & Recovery-Konzepts
Feuerlöschgeräte in Serverräumen	Erstellen eines Notfallplans
Feuer- und Rauchmeldeanlagen	Kontrolle des Sicherungsvorgangs
Klimaanlage in Serverräumen	Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
Schutzsteckdosenleisten in Serverräume	Keine sanitären Anlagen im oder oberhalb des Serverraums
Datenschutztresor	Hosting (jedenfalls der wichtigsten Daten) mit einem professionellen Hoster
Videoüberwachung in Serverräumen	
Regelmäßige Backups	

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

Gewährleisten, dass die Anforderung der DSGVO nachprüfbar umgesetzt wurden.

Technische Maßnahmen	Organisatorische Maßnahmen
Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter bei Bedarf/Berechtigung (Intranet ...)	Bestellung des Datenschutzbeauftragten heyData
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	Regelmäßige Schulungen der Mitarbeiter im Datenschutz
Verwendung der heyData-Plattform zum Datenschutz-Management	Verpflichtung der Mitarbeiter auf das Datengeheimnis
	Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

Incident-Response-Management

Gewährleisten, dass nach einer Störung der Auftraggeber eine Information über die Störung erhält, sofern dessen Daten betroffen waren.

Technische Maßnahmen	Organisatorische Maßnahmen
Monitoring von Datenzugriffen	Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
Alarmsysteme bei Dateneinbruch	Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
	Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
	Einsatz von Anti-Viren-Software

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Gewährleisten, dass nach einer zeitlichen Vorgabe personenbezogene Daten gelöscht werden.

Technische Maßnahmen	Organisatorische Maßnahmen
Automatische Softwareunterstützung	Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
	Manuelle Löschung auf Anforderung
	Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Auftragskontrolle

Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen	Organisatorische Maßnahmen
	Auswahl des Auftragnehmers unter Sorgfalts- gesichtspunkten <i>(insbesondere hinsichtlich Datensicherheit)</i>
	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
	Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)
	Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen
	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen

Sonstige technische oder organisatorische Maßnahmen zum Auftrag

Technische Maßnahmen	Organisatorische Maßnahmen
----------------------	----------------------------

• Nur Betriebssysteme und Software einsetzen, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden • Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl • Einsatz starker Verschlüsselung der mobilen Endgeräte (z. B. Festplattenverschlüsselung, Container-Lösungen) • Serverlokale Dienste über Firewall auf Servern vor Außenzugriff blockieren • Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 oder TLS1.3) • Absicherung von Datenbanken auf dem Webserver mittels Firewalls • Trennung von Webserver, Anwendungslogik und Datenhaltung einer Webanwendung durch eigene Server, die in eine geeignete Firewall-Architektur (z. B. DMZ – Demilitarisierte Zone) eingebunden sind • Blockierung aller nicht benötigten Dienste (z. B. VoIP, Peer-to-Peer, Telnet) • Einsatz eines Web-Proxies über den alle HTTP(S)-Verbindungen gehen müssen • Geregelter Prozess zur ordnungsmäßigen Konfiguration der Firewalls und regelmäßige Überprüfung der selbigen (z. B. zu der Notwendigkeit von Freigaben) • Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind (z. B. wiederbeschreibbare DVDs) • Keine Aufbewahrung von Archivdaten in Produktivdatenbanken, sondern Überspielen von Archivdaten aus Produktivsystemen in die Archivsysteme • Konzept zur Protokollierung von Benutzeraktivitäten, technischen Systemereignissen, Fehlerzuständen und Internetaktivitäten unter Berücksichtigung datenschutzrechtlicher Anforderungen (u. a. auch Beschäftigtendatenschutz) erstellen • Speicherung der Log-Dateien auf einem eigenen Log-Server von 120 Tagen • Regelmäßige anlasslose Auswertung der Log-Dateien zur Erkennung von ungewöhnlichen Einträgen – bevorzugt: Automatische Heuristiken • Asymmetrische Verschlüsselung nach Stand der Technik mit z. B. RSA-2048 Bit (oder höher), EC-256 Bit (oder höher) • SSL-Zertifikate bei vertrauenswürdigen Zertifizierungsstellen beschaffen	• Von Heimarbeit betroffenen Mitarbeiter werden die sichere Nutzung von Home Office Lösungen erläutert und spezifische Gefahren aufgezeigt • System- und Sicherheitstests, wie z. B. Code-Scans werden regelmäßig durchgeführt • Penetrationstests werden durch externe Dienstleister durchgeführt • Ausreichende Testzyklen werden berücksichtigt • Fortlaufendes Inventarisieren der Versionen von Software oder Komponenten (z. B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten • Nur Dienstleister verwenden, die die Garantien (in Form von Dokumenten) zur Verfügung stellen können • Daten werden bei Auftragsverarbeitung (spätestens) nach Vertragsende wirksam gelöscht • Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung
---	--

Anlage 4: Unterauftragsverarbeiter

Name des Subunternehmers	Anschrift des Subunternehmers	Leistung	Anmerkung & Geeignete Garantie gem. Art. 28 / Art. 44 ff. DSGVO
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn Deutschland	Open Telekom Cloud und LLM - Hosting	Bereitstellung der Kern-Software und der Datenbestände Auftragsverarbeitungsvertrag (AVV) gem. Art. 28 DSGVO Verarbeitung gem. § 203 StGB gegeben.
*Microsoft Deutschland GmbH	Walter-Gropius-Strasse 5 80807 München Deutschland	Azure OpenAI – Region Europe	Optional für bestimmte KI-Modelle Auftragsverarbeitungsvertrag (AVV) gem. Art. 28 DSGVO
*Google Cloud EMEA Ltd	70 Sir John Rogerson's Quay Dublin 2, D02 R296 Irland	Google Cloud Plattform EMEA	Optional für bestimmte KI- Modelle Auftragsverarbeitungsvertrag (AVV) gem. Art. 28 DSGVO
*Brave Software Inc	580 Howard St, Unit 402 San Francisco, CA 94105 Vereinigte Staaten	Websearch API	Optional für Webanbindung EU-Standardvertragsklauseln (SCC)
XQueue GmbH Maileon	XQueue GmbH Christian-Pleß-Str. 11-13 63069 Offenbach am Main	Information über Berechtigungsänderungen & Produktupdates	Auftragsverarbeitungsvertrag (AVV) gem. Art. 28 DSGVO; Datenverarbeitung ausschließlich innerhalb der EU.
*CORDNET OÜ Featurebase	Harju maakon Viimsi vald Haabneeme alevik Kaluri tee 4-32 74001, Estland	Bewertungsfunktionen	Optional Auftragsverarbeitungsvertrag (AVV) gem. Art. 28 DSGVO
*ElevenLabs Inc.	ElevenLabs Inc., 169 Madison Ave, #2354, New York, NY 10016, USA	Bereitstellung von KI-gestützten Audio- und Sprachsynthesediensten (z. B. Text-to-Speech, Speech-to-Text), Bereitstellung der Software-Infrastruktur.	Auftragsverarbeitungsvertrag (AVV/DPA) nach Art. 28 DSGVO i.V.m.: EU-US Data Privacy Framework (DPF) (sofern zum Abrufzeitpunkt aktiv zertifiziert), Ergänzend/Nachgelagert: EU-Standardvertragsklauseln (SCCs), Modul 2 (Verantwortlicher zu Auftragsverarbeiter) bzw. Modul 3 (Auftragsverarbeiter zu Auftragsverarbeiter), integriert im ElevenLabs DPA, mit Gerichtsstand Irland.
*Perplexity AI, Inc.	555 De Haro St, Suite 400, San Francisco, CA 94107, USA	Bereitstellung der Such- und Web-API (Perplexity API) zur Web-Anbindung.	Auftragsverarbeitungsvertrag (AVV) gem. Art. 28 DSGVO wird über das kommerzielle API-DPA abgeschlossen. Drittlandstransfer / Garantie: EU-Standardvertragsklauseln (SCC) – Modul 2 (Controller-to-Processor) sind im DPA verankert. Ergänzend greift das EU-US Data Privacy Framework (DPF) bei

			aktiver Zertifizierung zum Verarbeitungszeitpunkt. Daten werden nicht zum Training der KI genutzt.
*staan.ai	2 rue Kellermann 59100 Roubaix France	Bereitstellung der Such- und Web-API zur Web-Anbindung.	Art. 28: AVV abgeschlossen. Art. 44 ff.: Entfällt (Serverstandort & Verarbeitung in der EU).

*Kunden haben die Möglichkeit, optionale Dienste in der Administrationsoberfläche zu deaktivieren.

Anlage 5: Weisungsberechtigte Person

Beim Auftraggeber (bitte ausfüllen)

Name, Vorname	
Anschrift	
Telefon	
E-Mail	

Security Concept



amber Managed Service Security Concept
powered by amber Tech GmbH

How amber ensures a safe and secure Managed SaaS environment for its customers

V2.0 – August 2025



EU Artificial
Intelligence Act



Contents

Introduction	3
Security Program	4
System Information	6
System Overview	6
Product Software	6
Underlying Platform Services	6
Third Party Software	7
Connectivity	7
Sensitive Data	8
AI Training.....	8
Network Diagram	9
Network diagram of the solution.....	9
Security Controls	11
Security Controls Overview	11
Malware and Vulnerability Protection	11
Network Controls	11
Incident and Vulnerability Handling - Software Updates and Security Patches	11
Remote Connectivity	12
Authentication and Authorization	12
Physical Protection.....	12
Data Protection	12
Disaster Prevention and Recovery	13
Data Deletion Concept.....	13
Compliance and Certifications.....	13
System Configuration.....	15
Modifications to the System	15
Regulatory Compliance	15
Personal Data.....	15
Contact Person	17

Introduction

To begin with, amber is ISO27001 certified. The IT-security helps our (potential) customers to understand the concept of our managed Software-as-a-Service (SaaS) solution. The concept is one of the major points to ensure:

- The confidentiality of a company and its personal data
- The integrity of the provided software services
- The availability of the offered services

To meet the highest standards in all three domains, the design, development and test stages of the product need to be aligned to these goals. Only through a foresighted and all-encompassing approach the highest standards of confidentiality, integrity and availability can be guaranteed.

The purpose of this white paper on amber's security concept is:

- To inform customers about our standards of working and how these are in place to ensure the goals of data security
- Specify which guidelines are in place and required to fulfill these high standards
- Avoiding the necessity of generic question sessions
- Providing specific and in-depth information, which can also be handed out to other stakeholders
- Supporting the administrative guidance for the integration process of amber

In general, this paper will guide the reader through the most important sections of our cloud security concept and answer as many questions as possible for the Chief Security Officer and other relevant stake holders. To ensure an easy readability the majority of amber's security concept is structured in bullet points.

The concept of our cloud security is kept on a rather broad level on purpose to ensure that no details are available. This helps to ensure that the data in our solution is even more secure, as the group of people who know the details of our security concept is kept small.

Security Program

This section contains generic information on the measures undertaken by amber to secure a safe and secure software solution.

Security by design:

The architecture is built on top of the newest and recommended approaches through the use of a micro service architecture. This containerized solution ensures that every application part only has access to the parts necessary for the steps performed in this micro service.

To add another layer of security, the infrastructure is separated into multiple independent tenants to ensure that the experimental, staging and production environment are completely separated.

The administrative interfaces of the production environment therefore uses another type of log-in provider, which is only available to administrators (see **Figure 1**).

The only interface between the different environments is the software. This software is distributed through container registry. Two different container registries exist, one for development purposes and the other one from which the final releases for the production environment are pulled. The interconnection between these two is manual, so that every release needs manual approval before it is transmitted to the production container registry.

Security testing:

The usage of State-of-the-Art micro services allows to implement a multi-stage test concept. Through these multiple levels of abstraction and automated testing it is ensured that exploits are detected early. At the same time, the staging environment mimics the production environment as close as possible to be able to detect all exploits / issues in the staging environment already.

Through the usage of containerized services, a standardized tool stack for security and vulnerability checking can be used, so that security-relevant issues are automatically detected in the built-section of these containers.

Secure configuration:

To offer every customer the best and most secure environment, we separate databases which include customer specific data into a separate virtual network environment and distinct micro services (see **Figure 2**).

For a reduction of individual security threads, which are often arising through extensive customization, we offer all clients in the same tier similar security options. Through this process we ensure that individual extensions are minimized, for which the regular security updates and checks cannot be performed (semi-) automatically.

Security training:

Security Training is an essential part of the whole security concept at amber. For improved efficiency we separate the security training into different levels for developers, operations and administrators and other employees. Thus, amber maximizes awareness through distributing relevant information to the relevant groups.

On top of that amber is overseeing the security awareness at their subcontractors as well, to ensure that there are adequate measures in place to comply with the given cloud security concept.

Vulnerability and incident notifications:

For the different groups of employees there are short communication channels, so that high-priority issues can be communicated and executed quickly. Through this we strengthen the awareness of employees for security-relevant issues.

This includes relevant manual security notifications as well as automated notifications which are sent by our automatic metrics and logging services.

For incidents the environment can be put into maintenance mode automatically, depending on the detected activities. After that, the resuming of normal operation must be triggered manually.

Other security Elements:

All data processing is performed at data centers which are managed by subcontractors. This ensures the highest level of physical security for the computational hardware and provides standard certificates for data center security for our managed software packages.

Through the usage of Infrastructure-as-a-Service (IaaS) amber makes sure that availability and security are always State-of-the-Art and updated regularly.

System Information

This section contains information on the general purpose of the software and the provided services by amber.

System Overview

The provisioned software is aimed at corporations with 50 or more employees, which are dealing with large amounts of unstructured data (documents, web applications, texts, images). The scope of the software is to achieve better information retrieval on multiple connected data sources through a single point of access.

Therefore, the software provides interfaces to applications currently deployed either on the servers of the customer or to the cloud applications used by the customer.

The access to the provisioned software is initially only made available through web browsers. Additional locally installed software (e. g. add-ons, desktop applications) are possible extensions. The software components needed for the search will be running completely on the cloud infrastructure provided by amber. Certain features (e. g. SSO with Azure AD) need an interface to the customers infrastructure and may only be accessible from inside the customers VPN.

The access to the GUI can be limited on requests to certain networks (VPNs), IP-ranges or other network limitations.

Product Software

The product itself consists of a login area, which is connected to the customers identity provider and thus allows a login with the same credentials as for other company internal applications. The identity provider is connected through an identity broker.

The software itself is maintained and updated by amber. There is only limited support for older versions and updates can only be delayed for a certain amount of time. As soon as there are new versions available for the release these will be gradually rolled out to all customers.

Interfaces to the data sources are only available in a read-scope by default to ensure that data loss is impossible due to limited restrictions. Write access is granted on user scope for triggering automated actions.

Reports about usage and abuse can be viewed by administrators from amber and named users from the customers. The view and look of these reports can be customized, whereas the underlying data format cannot be changed due to security reasons.

Underlying Platform Services

The services which provide the AI and search platform, is divided into multiple separated services. All of these services are running on a system architecture which is based on Kubernetes as an orchestration tool. For advanced security only certain specifications of nodes are used, so that nodes are running on the same OS and patches are integrated through live-patches. The security strengthened base images are provided by the IaaS Provider.

Internal networks are separated into multiple areas. The areas segregate the services by customer and by service (see **Figure 2**). The areas inside the production environment are virtually separated and provide full internal firewall functionality. Thus, the access between different areas is limited and usually only possible in one-way.

Third Party Software

Components which make use of third-party software are checked regularly for updates. This is done automatically during build operations in the continuous integration and during vulnerability checks. An overview over the currently used third party software is available in the license section of the product itself.

amber only uses third-party providers listed in the current version of the General Contractual Terms for Processing Data. Certain third-party integrations can be activated and deactivated by administrative users.

If new or updated third party APIs are used for services in the future, amber will ask for consent from every customer individually according to current regulations.

Connectivity

The environment is distinguished into two separate areas:

Internal environment and traces are only accessible for the system admin for support purposes.

The external environment is connected through an IPSec VPN bridge to the customers company internal VPN. Connections are tracked by amber to detect abuse and can be also traced and monitored by the customer.

The Types of connectivity:

1. **Web Access** through port 443 (For users to access GUI)
2. **Access to master node**, with web services running (For regular application updates)
3. **Access to other/worker nodes** with backend and supporting services running (For in-depth failure / trace analysis)
4. **Metrics and Logs Access**

1. Web Access

The technical connectivity to the application is limited so that only the essential services (GUI, log in) are accessible by the user. For that purpose, the orchestration tool separates network streams by origin (reverse proxy) and passes them on to the according customer specific environment. The separation is possible through defining domains, IP-Areas or VPCs.

All supporting services with whom the user interacts directly, are running in the separated customers environment.

2. Access to master node

Access to the master node is necessary to initiate rolling update process of the services or the orchestration tools. The master node only has limited access to the worker nodes.

The access to the master node itself is only possible for the administrator group or the IaaS Provider.

3. Access to worker node

Worker nodes itself have only limited access to the internet or any outside services, expect for the according customers VPN network.

The access to worker nodes is only possible through a terminal server (e. g. the master node) due to heavy firewall restrictions.

This type of access is not regularly used and only intended for customer specific setup or in-depth failure analysis.

4. Metrics and Logs Access

Access to the service where the metrics and logs are stored, and emergency notifications are emerging, is available for the operations team of amber. This group has a read-only access to quickly see relevant security issues and detect abuse of certain services or data. Access is possible through an amber-internal VPN.

Sensitive Data

For the creation and necessary updates of the index, the data is stored on the amber servers temporarily until the extraction of searchable information is finished. Afterwards, the file contents are deleted and the searchable information is forwarded in snippets to the search and vector index and the according databases. Sensitive data in these documents are secured through our general policy “every user only sees what he or she is allowed to see in the target applications”. Log Data is available only for technical team members for error detection or parties with legitimate interest.

As defined in the section “Product Software” the software itself relies on data provided by the client, their applications and the users. This data can consist of personal or sensitive data. The software itself does not need personal data to function in its intended way but is able to search through personal data as well.

All incoming documents or data are only temporarily stored in the customers virtual environment. After the build-up is completed, the raw data is deleted immediately and only the necessary information are stored in the according databases.

Sensitive data can only be seen by users who already have access to this data in the connected applications. The search software is not intended to extend access rights above the existing level. All access control changes must be made in the underlying applications.

Sensitive or private data which is created during the usage of the application (e. g. queries) are anonymized where possible and stored for traceability.

Any sensitive or private data can be deleted on request and will then be removed completely from all amber servers. The meta data of the deletion process will be logged. (See section “Personal Data” for more details).

AI Training

amber or its subproviders do not use customer data either directly or indirectly for training, improvement, or development of large language models (LLMs). Instead, the platform is based on an index-based approach, in which customer data is stored in a protected index and only retrieved at runtime to generate context-related responses.

Network Diagram

In this section amber provides a network diagram of the cloud architecture of amber.

Network diagram of the solution

amber runs as a managed service in the OTC of Telekom. The GUI can be accessed via the intranet or via the VPN.

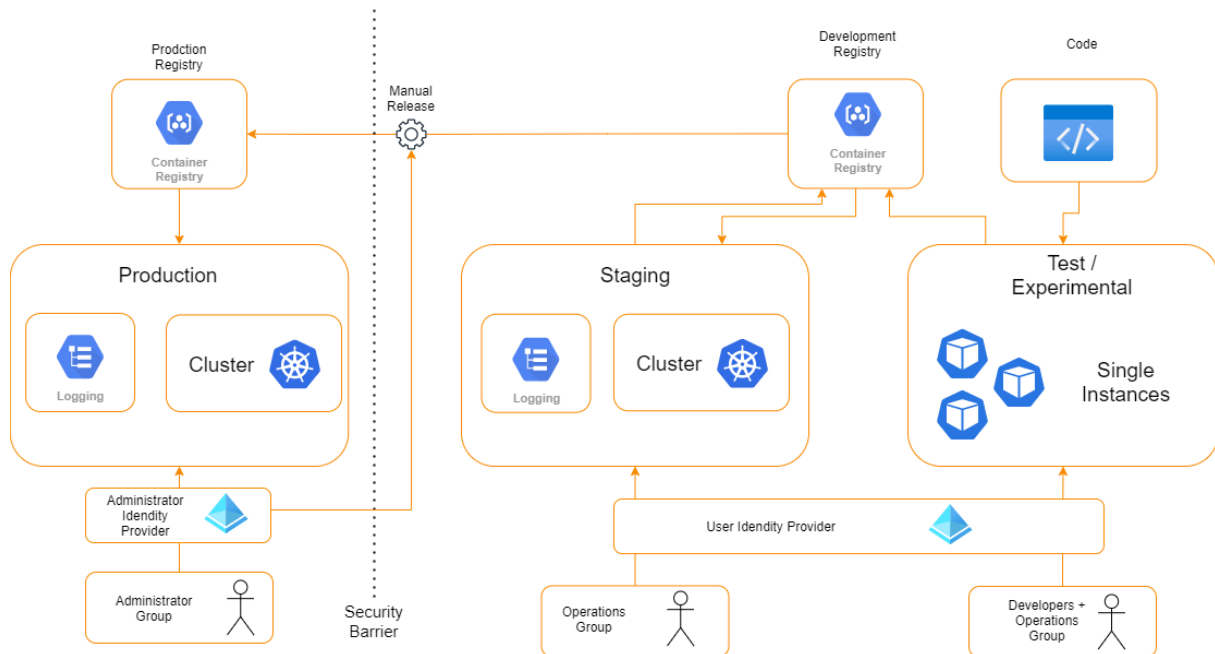


Figure 1: Different Environments and Interconnection at amber

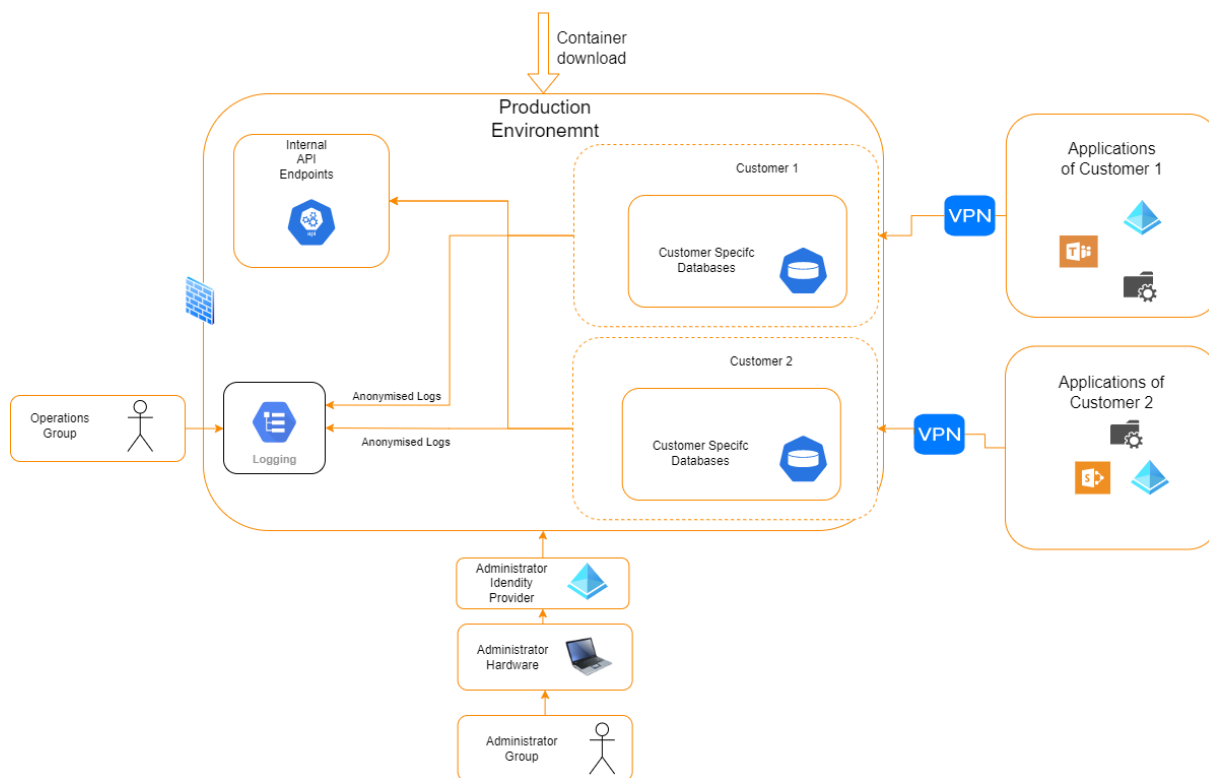


Figure 2: Detail View on Connectivity of the Production Environment

amber can search data from both on-premises and cloud solutions which are accessed via secured routes.

For the access to certain applications see the section “Components which make use of third-party software are checked regularly for updates. This is done automatically during build operations in the continuous integration and during vulnerability checks. An overview over the currently used third party software is available in the license section of the product itself.

amber only uses third-party providers listed in the current version of the General Contractual Terms for Processing Data. Certain third-party integrations can be activated and deactivated by administrative users.

If new or updated third party APIs are used for services in the future, amber will ask for consent from every customer individually according to current regulations.

Connectivity”.

Security Controls

In this section generic information on the controls of the security measures is provided. In general amber has been awarded the ISO 27001 certification and works under the given controls and measures. Amber maintains an ISMS System and continuously iterates over the improvements and implementations of the specific controls.

Security Controls Overview

See technological and organizational measures (TOM) in data processing agreement (DPA, AVV) which can be provided by amber.

Malware and Vulnerability Protection

In the given software architectures, there are multiple boundaries which are created to protect and minimize the risk of hazardous code and attacks.

Starting at the development process, every developer is instructed to use the most recent stable version of other software dependencies. Any new package or requirement is screened by the operations team. Outdated package versions are detected automatically during the container build process. Common security standard are propagated during onboarding.

Vulnerability scanning is performed regularly on all containers in the production container registry. Old containers are not used anymore as soon as a new version is available. They are removed from the production registry and archived in separate data storages.

The data center infrastructures run at a minimal software setup which only includes absolute necessary software dependencies.

Backups of sensitive data and access logs are stored in a separate read-only system. Backups there are only eligible for removal after a certain cool down period to avoid ransomware encryption.

Network Controls

Network Access are logged to a separate server. This ensures a more independent logging server compared to other services in the production environment whilst still being in the same virtual network.

Through the combined metrics and logging server suspicious patterns are detected automatically or by hand if necessary.

As an additional security procedure, the IaaS provider is monitoring network and computational resource usage to detect abuse patterns. Through IaaS' experience they are able to draw distinction between heavy use and abuse.

Every customer with on-premise data services is assigned to a separate virtual network in our cloud environment (see **Figure 2**). Each virtual private network has its own endpoints to connect if necessary to the VPN of the specific customer as well as the overall firewall protecting our production environment.

Incident and Vulnerability Handling - Software Updates and Security Patches

Incidents and vulnerabilities are collected at the build / development and operations stage. At both stages the severity is assigned in three different escalation levels. For every level there are certain time-ranges in which an action needs to take place. This includes both internally detected vulnerabilities as well as externally detected issues, which are published globally.

The incident management system afterwards is made for the goal to eliminate the severe incidents as fast as possible while preserving availability on a high level.

For the three levels there are different measures in place:

1. Critical incidents: The application is set to maintenance mode immediately, no data access is possible
2. Serious incident: A hotfix is provided as soon as possible. The application is operating normally in the meantime. A hotfix can lead to the temporary deactivation of certain features
3. Normal incident: The issue will be resolved in the next upcoming release in the normal release cycle. The application is operating normally.

Remote Connectivity

According to **Figure 2** access to certain environments is handled separately. Remote connectivity is only allowed by named users. Any machine with access to the production environment is handled differently from the other machines. Before any remote access, checks for software updates are run. Access is provided by encrypted key files with SOTA encryption algorithm (e. g. 2048-bit RSA).

For systems which need password access the password is stored only in databases with a master key. This master key is not stored anywhere electronically but still encompasses rules for password complexity. Where possible a Two-Factor-Authentication (2FA) is enabled.

The remote connection is either encrypted or uses an encrypted network (e. g. amber VPN) to prevent any man-in-the-middle attacks.

Authentication and Authorization

All service accounts and personal accounts are assigned to specific people. This person is an internal employee of amber. Administrator accounts are only handed out to a certain group of people.

Administrative accounts are further divided into read-admin and write-admin accounts. Whenever possible the user with the least access rights is used to access certain resources.

Changes to admin accounts passwords (general profile settings) are only going into effect after a certain cool-down period.

Physical Protection

Security of the physical data center is provided by our subcontractors and verified through certificates (ISO 27001, SOC 2).

The limited access to the physical devices for the access to the data center is ensured through fully encrypted disks, automated locking of unused devices and the ability to remotely deactivate the devices.

Data Protection

Data protection is secured through our external data protection officer as well as a fully GDPR-compliant software and data architecture. The data is only stored in German Data Centers. All data which cannot be recomputed in a maximum of 24 hours is backed up. Failed devices or configurations are not put back into the production environment but are instead sorted out by the data center operator.

Every worker node has fully encrypted data storage disks and the database services use encrypted memory. All backups of encrypted disks are also encrypted.

All sensitive data can be removed on request and is then completely wiped out from all amber resources.

Disaster Prevention and Recovery

To avoid permanent data losses or extensive times of unavailability amber takes measures to minimize the risks of both.

Backups are encrypted and can only be decrypted by an administrative user and by hand. For essential data, the backups are mirrored across multiple computational regions (availability zones). Additional cold storage backups are available on request.

Data Deletion Concept

Data can be deleted manually or automatically. Manual Deletions are triggered by the customers administrators, who ensures that the request is from a valid user and needs to be forwarded to the application distributor. The extent of the request is limited to data which itself emerges from the application. It cannot consist of specific data, as this needs to be handled through the automated deletion process through connected applications (see below). If a user or an administrator is requesting critical data wipeouts of portions of the data or index, this is handled through a temporary shutdown of the application in combination with the deactivation of the specific data source.

Automatic Deletion is essential to ensure that data which is deleted in the according applications is also deleted from the search application and their according indexed.

This is ensured through a routine which is running in a pre-defined fixed time range. After the successful completion of this routine updated or deleted documents are replacing their older versions. Therefore, all necessary steps that needs to be performed to delete data from the applications are automatically transferred to the search engine.

After the retention time span, this data is also deleted from the associated backup systems.

The deletion request either if it is triggered manual or automatically cannot include data which is essential for the logging or tracing of other activities due to the documentation requirements of these features in the according Laws and Standards. Backups are deleted after a cool down period of 90 days.

Compliance and Certifications

All data centers which are used for the software are compliant with the following norms:

- ISO 9001
- ISO 14001
- ISO/IEC 20000-1
- ISO 22301
- ISO 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701
- BSI C5
- TCDP 1.0

Additionally, amber ensures compliance with the GDPR through the separately provided TOM's which are laid out in the data processing agreement (AVV) (see Security Controls Overview).

System Configuration

Installation and configurations are performed through Infrastructure-as-Code (IaC) methods. Through these methods changes to computational resources are reviewed and analyzed with respect to the possible security flaws in the same way as the code itself.

amber reduces the number of different systems to a minimum and aims to support certain systems configurations. Therefore, security measures are fully adapted to this single type of infrastructure / configuration. amber is not providing any support for outdated versions, to focus on the security and completeness of the newest version at any time.

Through the IaC approach network and computational configurations are tested in the same setup and can be replicated at any time without a minimum of manual interaction. The defined infrastructure is more failure resistant than written manuals.

Modifications to the System

In alliance to the minimization of possible system configurations, amber also minimizes the possible modifications to the system. A normal user is not intended to change anything besides the layout, which is full rendered in his browser. Other adaptations can be made by customer administrators who therefore need to be pre-educated on the subject of data security.

Password or access right changes can only be performed in the underlying applications, not in the search application. Changes to the underlying interfaces to data sources (on-premise applications or cloud applications which are run by the customer) need to be actively communicated and can lead to a temporary deactivation of these connections if there are security or other technical risks which are detected by amber or one of its subcontractors.

Regulatory Compliance

amber ensures that the whole system design and development process is made with the concepts of “Privacy by Design” and “Privacy by Default” as major goals.

Privacy by Design: The privacy is ensured through only collecting and analyzing the bare minimum of data which is necessary to fulfill the intended use of the software. This is the search across unstructured data in multiple applications.

Privacy by Default: The configuration of the system and application is made so that especially users which are unaware of technical details, only transmit the data which is needed to perform the actions they intend. Additional data is only collected with user consent and can be opted-out at any time.

Both design principles enable the reduction of other technical-organizational actions and improve the simplicity of data protection in general.

Personal Data

The personal data that can be stored by the software:

- Queries which contain personal information
- Personal data (e. g. pictures, texts) in the indexed / searched files
- Chat History in personal or group chats
- Agent Instructions and default configurations

In general, all data which is customer specific is encrypted. Users are only able to request a deletion or a change of this data with approval from their respective administrator and if they have a legitimate interest.

1. Queries are transferred to a centralized logging solution to detect malicious queries or abusive behavior
 - a. Centralized logging solution is completely controlled by amber
 - b. Data can be deleted on request or after a specific retention period
 - c. Data can be exported on request to ensure data privacy rules
2. Personal data in searched / indexed files:
 - a. Is never transferred outside the customer specific virtual cloud network or agreed subprocessors
 - b. Only snippets / vectorized information is permanently stored in the index
 - c. Raw files are removed after the index process
 - d. This personal data cannot be exported from our servers
 - e. Permanent deletion of this data is possible through contract termination

Contact Person

In case you have any further questions please reach out to:

Philipp Reißel, Chief Executive Officer of amber

- Philipp@ambersearch.de

Oleh Rakovych, Chief Information Security Officer of amber

- Oleh@ambersearch.de

Contact via Phone:

- [+49 241-559708-0](tel:+492415597080)