

DPA & TOMs



amber Data Processing Agreement

Version: July 2026

To	Our (prospective) customers/partners
	- Hereinafter referred to as the "Client" -
From	amber Tech GmbH Jülicher Str 72a 52070 Aachen
	- Hereinafter referred to as the "Contractor" -

Contact person	Bastian Maiworm
Contact	
Mobile	+49 (0) 157 3707 3220
Landline	+49 (0) 241-559708-12
Email	Bastian@amber.de

Preamble

The Controller has engaged the Processor under the contract already concluded (hereinafter the “Main Agreement”) to provide the services set out therein. The processing of personal data forms part of the performance of that contract. Art. 28 GDPR in particular imposes certain requirements on such processing on behalf of a controller. In order to meet these requirements, the Parties enter into the following data processing agreement (hereinafter the “Agreement”), the performance of which is not remunerated separately unless expressly agreed otherwise.

We would also point out that amber Tech GmbH is ISO 27001 certified.

§ 1 Definitions

- (1) Controller means, pursuant to Art. 4(7) GDPR, the body which alone or jointly with other controllers determines the purposes and means of the processing of personal data.
- (2) Processor means, pursuant to Art. 4(8) GDPR, a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
- (3) Personal data means, pursuant to Art. 4(1) GDPR, any information relating to an identified or identifiable natural person (hereinafter “Data Subject”); a natural person is regarded as identifiable who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more special characteristics which express the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- (4) Personal data requiring special protection means personal data pursuant to Art. 9 GDPR revealing the racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of Data Subjects, personal data pursuant to Art. 10 GDPR relating to criminal convictions and offences or related security measures, as well as genetic data pursuant to Art. 4(13) GDPR, biometric data pursuant to Art. 4(14) GDPR, health data pursuant to Art. 4(15) GDPR and data concerning the sex life or sexual orientation of a natural person.
- (5) Processing means, pursuant to Art. 4(2) GDPR, any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- (6) Supervisory authority means, pursuant to Art. 4(21) GDPR, an independent public authority which is established by a Member State pursuant to Art. 51 GDPR.

§ 2 Subject Matter of the Agreement

- (1) The Processor provides the services set out in the Main Agreement for the Controller. In doing so, the Processor obtains access to personal data which the Processor processes for the Controller exclusively on behalf of and in accordance with the instructions of the Controller. The scope and purpose of the data processing by the Processor are set out in the Main Agreement and any associated service descriptions. The Controller is responsible for assessing the lawfulness of the data processing.

(2) The Parties enter into this Agreement in order to specify their mutual rights and obligations under data protection law. In case of doubt, the provisions of this Agreement take precedence over the provisions of the Main Agreement.

(3) The provisions of this Agreement apply to all activities connected with the Main Agreement in which the Processor and its employees, or persons engaged by the Processor, come into contact with personal data originating from the Controller or collected on behalf of the Controller.

(4) The term of this Agreement follows the term of the Main Agreement, unless the following provisions give rise to obligations or termination rights extending beyond that term.

§ 3 Right to Issue Instructions

(1) The Processor may collect, process or use data only within the scope of the Main Agreement and in accordance with the Controller's instructions. Where the Processor is required to carry out further processing by the law of the European Union or of the Member States to which it is subject, it shall inform the Controller of those legal requirements prior to processing.

(2) The Controller's instructions are initially laid down in this Agreement and may thereafter be amended, supplemented or replaced by the Controller in writing or in text form by means of individual instructions (individual instruction). The Controller is entitled to issue such instructions at any time. This includes instructions regarding the rectification, erasure and blocking of data.

(3) All instructions issued must be documented by the Controller. Instructions that go beyond the services agreed in the Main Agreement shall be treated as a request for a change of services.

(4) If the Processor takes the view that an instruction of the Controller infringes data protection provisions, it shall notify the Controller thereof without delay. The Processor is entitled to suspend the implementation of the instruction concerned until it has been confirmed or amended by the Controller. The Processor may refuse to carry out a manifestly unlawful instruction.

§ 4 Types of Data Processed, Categories of Data Subjects, Third Countries

(1) In the course of performing the Main Agreement, the Processor obtains access to the personal data specified in more detail in Annex 1.

(2) The categories of persons affected by the data processing are set out in Annex 2.

(3) A transfer of personal data to a third country (outside the EEA) may take place subject to the conditions of Art. 44 et seq. GDPR.

§ 5 Protective Measures of the Processor

(1) The Processor is obliged to comply with the statutory provisions on data protection and not to disclose information obtained from the Controller's sphere to third parties or to expose such information to their access. Documents and data must be secured against access by unauthorised persons, taking into account the state of the art.

(2) Within its area of responsibility, the Processor shall organise its internal operations in such a way that they meet the specific requirements of data protection. It has implemented the technical and organisational measures set out in Annex 3 for the appropriate protection of the Controller's data pursuant to Art. 32 GDPR, which the Controller acknowledges as appropriate. The Processor reserves the right to amend the security measures taken, whereby it shall ensure that the contractually agreed level of protection is not undermined.

(3) Persons employed by the Processor in the processing of data are prohibited from collecting, processing or using personal data without authorisation. The Processor shall place a corresponding obligation on all persons entrusted by it with the handling and performance of this Agreement (hereinafter "Employees") (obligation of confidentiality, Art. 28(3)(b) GDPR) and shall ensure compliance with this obligation with due care.

(4) The Processor has appointed a data protection officer. The Processor's data protection officer is heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

For clients with the corresponding service package:

(5) The Processor undertakes, when processing the Controller's personal data as instructed, to comply with the confidentiality rules relevant to this engagement where such data are subject to professional secrecy within the meaning of § 203 of the German Criminal Code (StGB). The Processor is obliged to maintain secrecy with respect to all facts which become known to it in connection with the engagement and to which the Controller has granted it access. The Processor is further obliged to bind the employees and sub-processors engaged in the performance of the Agreement to secrecy in accordance with § 203(4) StGB and to supervise them in their activities.

§ 6 Information Obligations of the Processor

(1) In the event of disruptions, suspected data protection breaches or breaches of the Processor's contractual obligations, suspected security-relevant incidents or other irregularities in the processing of personal data by the Processor, by persons employed by it in connection with the engagement or by third parties, the Processor shall inform the Controller without delay. The same applies to audits of the Processor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of personal data records concerned;

b) a description of the measures taken or proposed by the Processor to address the breach and, where appropriate, measures to mitigate its possible adverse effects;

c) a description of the likely consequences of the personal data breach.

(2) The Processor shall take the necessary measures without delay to secure the data and to mitigate possible adverse consequences for Data Subjects, shall inform the Controller thereof and shall request further instructions.

(3) The Processor is further obliged to provide the Controller with information at any time to the extent that the Controller's data are affected by a breach pursuant to paragraph 1.

(4) The Processor shall notify the Controller of any material change to the security measures pursuant to § 5(2).

§ 7 Audit Rights of the Controller

(1) The Controller may satisfy itself of the Processor's technical and organisational measures before the start of the data processing and thereafter on an annual basis. For this purpose it may, for example, request information from the Processor, have existing expert attestations, certifications or internal audit reports presented to it, or inspect the Processor's technical and organisational measures itself in person during normal business hours following timely coordination, or have them inspected by a qualified third party, provided that such third party is not in a competitive relationship with the Processor. The Controller shall carry out audits only to the extent necessary and shall not disproportionately disrupt the Processor's business operations in doing so.

(2) The Processor undertakes to provide the Controller, upon its oral or written request and within a reasonable period, with all information and evidence required to carry out an audit of the Processor's technical and organisational measures.

(3) The Controller shall document the audit result and communicate it to the Processor. In the event of errors or irregularities which the Controller identifies, in particular when reviewing the results of the engagement, it shall inform the Processor without delay. If circumstances are identified during the audit whose future avoidance requires changes to the prescribed procedures, the Controller shall notify the Processor of the necessary procedural changes without delay.

§ 8 Engagement of Service Providers

(1) The contractually agreed services are performed with the involvement of the service providers listed in Annex 4 (hereinafter "Sub-processors"). The Controller grants the Processor its general authorisation within the meaning of Art. 28(2) sentence 1 GDPR to engage further Sub-processors, or to replace Sub-processors already engaged, within the scope of its contractual obligations.

(2) The Processor shall inform the Controller of any intended change relating to the addition or replacement of a Sub-processor. The Controller may object to an intended addition or replacement of a Sub-processor on important data protection grounds.

(3) An objection to the intended addition or replacement of a Sub-processor must be raised within 2 weeks of receipt of the information about the change. If no objection is raised, the addition or replacement shall be deemed approved. If important data protection grounds exist and no mutually agreeable solution can be found between the Controller and the Processor, the Processor shall have a special right of termination effective as of the end of the month following the objection.

(4) When engaging Sub-processors, the Processor shall bind them in accordance with the provisions of this Agreement.

(5) A sub-processing relationship within the meaning of these provisions does not exist where the Processor engages third parties for services which are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services without any specific connection to services which the Processor provides for the Controller, and security services. Maintenance and inspection services constitute sub-processing relationships requiring consent to the extent

that they are provided for IT systems which are also used in connection with the provision of services for the Controller.

(6) A transfer of personal data to a third country (outside the EEA) may take place subject to the conditions of Art. 44 et seq. GDPR.

§ 9 Requests and Rights of Data Subjects

(1) The Processor shall, as far as possible, assist the Controller with appropriate technical and organisational measures in fulfilling its obligations under Art. 12–22 and Art. 32 to 36 GDPR.

(2) If a Data Subject asserts rights, such as the right to information, rectification or erasure of their data, directly against the Processor, the Processor shall not act on its own initiative but shall refer the Data Subject to the Controller and await the Controller's instructions.

§ 10 Liability

(1) As between the Parties, the Controller alone is responsible vis-à-vis the Data Subject for compensating any damage suffered by a Data Subject as a result of data processing or use that is unlawful or incorrect under data protection law in the context of the processing on behalf of the Controller.

(2) The Processor shall be liable for damages without limitation to the extent that the cause of the damage is based on an intentional or grossly negligent breach of duty by the Processor, its legal representative or its agents.

(3) For negligent conduct, the Processor shall be liable only in the event of a breach of a duty whose performance is a prerequisite for the proper performance of the Agreement in the first place and on whose observance the Controller regularly relies and may rely, but limited to the damage typically foreseeable under such a contract. In all other respects, the liability of the Processor – including for its agents and vicarious agents – is excluded.

(4) The limitation of liability pursuant to § 10.3 does not apply to claims for damages arising from injury to life, body or health or from the assumption of a guarantee.

§ 11 Termination of the Main Agreement

(1) Upon termination of the Main Agreement, the Processor shall return to the Controller all documents, data and data carriers provided to it or – at the Controller's request, unless there is an obligation to store the personal data under Union law or other applicable national law – erase them. This also applies to any data backups held by the Processor. The Processor shall, upon request, provide documented evidence of the proper erasure.

(2) The Controller has the right to verify, in an appropriate manner, the complete return or erasure of the data by the Processor in accordance with the Agreement.

(3) The Processor is obliged to treat as confidential, also beyond the end of the Main Agreement, the data which have become known to it in connection with the Main Agreement. This Agreement shall remain in force beyond the end of the Main Agreement for as long as the Processor holds personal data which were transferred to it by the Controller or which it collected on the Controller's behalf.

§ 12 Final Provisions

(1) To the extent that the Processor does not expressly perform support activities under this Agreement free of charge, it may invoice the Controller a reasonable fee for such activities, unless the Processor's own acts or omissions made that support directly necessary.

(2) Amendments and supplements to this Agreement must be made in text form. This also applies to any waiver of this formal requirement. The priority of individual contractual arrangements remains unaffected.

(3) Should individual provisions of this Agreement be or become wholly or partly legally invalid or unenforceable, the validity of the remaining provisions shall not be affected thereby.

(4) This Agreement is governed by German law.

Annexes

Annex 1: Description of the Data / Data Categories

Type of data

The following types/categories of data are the subject of the processing of personal data (list/description of the data categories):

- ☒ Personal master data
- ☒ Communication data (e.g. telephone, e-mail)
- ☒ Contract master data (contractual relationship, product or contract interest)
- ☒ Contract billing and payment data
- ☒ Planning and control data
- ☒ Information obtained (from third parties, e.g. credit agencies, or from public registers)
- ☒ Contents of indexed or searched files (e.g. text and images), insofar as these contain personal data
- ☒ Search queries and chat histories, insofar as these contain personal data
- ☒ Usage and log data

Annex 2: Description of the Data Subjects / Groups of Data Subjects

The categories of persons affected by the processing include:

- ☒ Customers
- ☒ Prospective customers
- ☒ Employees
- ☒ Suppliers
- ☒ Commercial agents
- ☒ Contact persons
- ☒ The categories of data of data subjects that may be processed cannot be determined precisely, as they are a by-product of the service. All categories may therefore be affected.

Annex 3: Technical and Organisational Measures of the Processor

1.1. Processor

The processor pursuant to Art. 4(8) of the EU General Data Protection Regulation (GDPR) is amber Tech GmbH, Jülicher Straße 72a, 52070 Aachen, Germany, e-mail: info@amber.de. We are legally represented by Philipp Reissel, Bastian Maiworm, Igli Manaj.

1.2. Data Protection Officer

Our data protection officer is heyData GmbH, Schützenstraße 5, 10117 Berlin, www.heydata.eu, e-mail: datenschutz@heydata.eu.

1.3. Subject Matter of this Document

This document summarises the technical and organisational measures taken by the Processor within the meaning of Art. 32(1) GDPR. These are measures by which the Processor protects personal data. The purpose of this document is to support the Controller in fulfilling its accountability obligation under Art. 5(2) GDPR.

Confidentiality (Art. 32(1)(b) GDPR)

Physical access control

Denying unauthorised persons physical access to data processing equipment with which personal data are processed or used.

Technical measures	Organisational measures
Alarm system	Identity checks at the gatehouse / reception
Chip card / transponder locking system	Working from home: instruction to employees to work, where possible, in a study separate from living areas
Video surveillance of entrances	Careful selection of cleaning staff
Automatic access control system	Visitors only when accompanied by employees
Locking system with code lock	Careful selection of security staff
Manual locking system (e.g. keys)	Logging of visitors (e.g. visitors' book)
	Identity checks at the gatehouse or reception

System access control

Preventing data processing systems from being used by unauthorised persons

Technical measures	Organisational measures
Authentication with user name + password	Management of user authorisations
Encryption of data carriers	"Secure password" policy / central password rules
Use of anti-virus software	Identity checks at the gatehouse or reception
Use of mobile device management	Logging of visitors (e.g. visitors' book)

Use of VPN technology for remote access	General company policy on data protection or security
Blocking of external interfaces (e.g. USB ports)	Company policy on secure passwords
Automatic desktop lock	Company policy on "erasure/destruction"
Encryption of notebooks / tablets	Company "clean desk" policy
Creation of user profiles	Company policy on the use of mobile devices
	General instruction to lock the desktop manually when leaving the workstation

Data access control

Ensuring that persons authorised to use a data processing system can access only the data covered by their access authorisation, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

Technical measures	Organisational measures
Use of document shredders (with cross-cut function)	Reducing the number of administrators to the "absolute minimum"
Physical erasure of data carriers before their reuse	Management of user rights by system administrators
Logging of access to applications, in particular when entering, changing and deleting data	Instruction to employees that only strictly necessary data are printed
Logging of the destruction of data	Secure storage of data carriers
Use of an authorisation concept	Management of user rights by system administrators
	Instruction to employees that data are only deleted after consultation

Separation control

The following measures ensure that personal data collected for different purposes are processed separately:

Technical measures	Organisational measures
Separation of production and test systems	Creation of an authorisation concept
Logical multi-tenant separation (software-based)	Definition of database rights
For pseudonymised data: separate storage of the assignment file on a separate, secured IT system (encrypted where possible)	Tagging of data records with purpose attributes/data fields
	Internal instruction to anonymise/pseudonymise personal data, where possible, in the event of a transfer or after expiry of the statutory retention period.

Integrity (Art. 32(1)(b) GDPR)

Transfer control

Ensuring that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which bodies a transfer of personal data by means of data transmission facilities is envisaged.

Technical measures	Organisational measures
Setting up of VPN tunnels	Documentation of the recipients of data and of the periods of the planned provision or agreed erasure periods
Wi-Fi encryption (WPA2 with a strong password)	Creation of an overview of regular retrieval and transmission processes
Logging of access and retrievals	Careful selection of transport personnel and vehicles
Provision of data via encrypted connections such as SFTP or HTTPS	Prohibition on uploading company data to servers outside the company
Use of signature procedures	Working from home: employer's right of remote erasure

Input control

Ensuring that it is possible to verify and establish retrospectively whether and by whom personal data have been entered into, altered in or removed from data processing systems.

Technical measures	Organisational measures
Technical logging of the entry, alteration and deletion of data	Overview of which programs can be used to enter, change or delete which data
Manual or automated review of the logs	Traceability of the entry, alteration and deletion of data through individual user names (not user groups)
Retention of forms whose data have been transferred into automated processing	Assignment of rights to enter, change and delete data on the basis of an authorisation concept

Availability and resilience (Art. 32(1)(b) GDPR)

Availability control

Ensuring that personal data are protected against accidental destruction or loss.

Technical measures	Organisational measures
Uninterruptible power supply (UPS)	Creation of a backup and recovery concept
Fire extinguishers in server rooms	Creation of a contingency plan
Fire and smoke detection systems	Monitoring of the backup process
Air conditioning in server rooms	Regular data recovery tests and logging of the results

Protective power strips in server rooms	No sanitary facilities in or above the server room
Data protection safe	Hosting (at least of the most important data) with a professional hosting provider
Video surveillance in server rooms	
Regular backups	

Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

Data protection management

Ensuring that the requirements of the GDPR have been implemented in a verifiable manner.

Technical measures	Organisational measures
Central documentation of all data protection procedures and rules, with access for employees as required/authorised (intranet, etc.)	Appointment of heyData as data protection officer
The effectiveness of the technical protective measures is reviewed at least annually	Regular data protection training for employees
Use of the heyData platform for data protection management	Obligation of employees to maintain data secrecy
	Maintaining a record of processing activities (Art. 30 GDPR)

Incident response management

Ensuring that, following an incident, the Client receives information about the incident where its data were affected.

Technical measures	Organisational measures
Monitoring of data access	Notification process for personal data breaches pursuant to Art. 4(12) GDPR vis-à-vis the supervisory authorities (Art. 33 GDPR)
Alarm systems in the event of a data breach	Notification process for personal data breaches pursuant to Art. 4(12) GDPR vis-à-vis the data subjects (Art. 34 GDPR)
	Involvement of the data protection officer in security incidents and data breaches
	Use of anti-virus software

Privacy-friendly default settings (Art. 25(2) GDPR)

Ensuring that personal data are erased in accordance with a defined time limit.

Technical measures	Organisational measures
Automatic software support	Training of employees in "privacy by design" and "privacy by default"
	Manual erasure on request
	No more personal data are collected than are necessary for the respective purpose.

Order control

Ensuring that personal data processed on behalf of a controller can only be processed in accordance with the Client's instructions.

Technical measures	Organisational measures
	Selection of the contractor on the basis of due-diligence criteria <i>(in particular with regard to data security)</i>
	Ongoing review of the contractor and its activities
	Confirmation from contractors that they bind their own employees to data secrecy (typically in the data processing agreement)
	Written instructions to the contractor or instructions in text form (e.g. by means of a data processing agreement)
	Ensuring the destruction of data after the end of the engagement, e.g. by requesting corresponding confirmations
	Ensuring the destruction of data after the end of the engagement, e.g. by requesting corresponding confirmations

Other technical or organisational measures relating to the engagement

Technical measures	Organisational measures
• Use only operating systems and software for which security updates are still provided in a timely manner • Use of backup and synchronisation mechanisms to prevent major data loss in the event of loss or theft • Use of strong encryption on mobile devices (e.g. hard disk encryption, container solutions) • Block server-local services against external access by means of a firewall on the servers • Use of the HTTPS protocol in line with the state of the art (TLS 1.2 or TLS 1.3) • Protection of databases on the web server by means of firewalls • Separation of web server, application logic and data storage of a web application by dedicated servers integrated into a suitable firewall architecture (e.g. DMZ – demilitarised zone) • Blocking of all services that are not required (e.g. VoIP, peer-to-peer, Telnet) • Use of a web proxy through which all HTTP(S) connections must pass • Defined process for the proper configuration of the firewalls and regular review of the	• Employees working from home are instructed on the secure use of home office solutions and are made aware of specific risks • System and security tests, such as code scans, are carried out regularly • Penetration tests are carried out by external service providers • Sufficient test cycles are taken into account • Ongoing inventory of the versions of software or components (e.g. frameworks, libraries) and their dependencies • Use only service providers that are able to provide the guarantees (in documented form) • In the case of processing on behalf of a controller, data are effectively erased (at the latest) after the end of the contract • Regular review of the processor with regard to security practices and service provision

same (e.g. as to the necessity of permissions) • No archiving on data carriers that are unsuitable for long-term storage (e.g. rewritable DVDs) • No retention of archive data in production databases; instead, archive data are transferred from production systems to the archive systems • Creation of a concept for logging user activities, technical system events, error states and internet activities, taking data protection requirements into account (including employee data protection) • Storage of the log files on a dedicated log server for 120 days • Regular review of the log files without specific cause in order to identify unusual entries – preferably: automatic heuristics • Asymmetric encryption in line with the state of the art, e.g. RSA 2048 bit (or higher), EC 256 bit (or higher) • Obtaining SSL certificates from trustworthy certification authorities	
---	--

Annex 4: Sub-processors

Name of the sub-processor	Address of the sub-processor	Service	Remarks & appropriate safeguards pursuant to Art. 28 / Art. 44 et seq. GDPR
Telekom Deutschland GmbH	Landgrabenweg 151 53227 Bonn Germany	Open Telekom Cloud and LLM hosting	Provision of the core software and the data holdings Data processing agreement (DPA) pursuant to Art. 28 GDPR Processing pursuant to § 203 StGB provided for.
*Microsoft Deutschland GmbH	Walter-Gropius-Strasse 5 80807 München Germany	Azure OpenAI – Europe region	Optional for certain AI models Data processing agreement (DPA) pursuant to Art. 28 GDPR
*Google Cloud EMEA Ltd	70 Sir John Rogerson's Quay Dublin 2, D02 R296 Ireland	Google Cloud Platform EMEA	Optional for certain AI models Data processing agreement (DPA) pursuant to Art. 28 GDPR
*Brave Software Inc	580 Howard St, Unit 402 San Francisco, CA 94105 United States	Web search API	Optional for web connectivity EU standard contractual clauses (SCC)
XQueue GmbH Maileon	XQueue GmbH Christian-Pleiß-Str. 11-13 63069 Offenbach am Main	Information on authorisation changes & product updates	Data processing agreement (DPA) pursuant to Art. 28 GDPR; data processing exclusively within the EU.
*CORDNET OÜ Featurebase	Harju maakon Viimsi vald	Rating features	Optional

	Haabneeme alevik Kaluri tee 4-32 74001, Estonia		Data processing agreement (DPA) pursuant to Art. 28 GDPR
*ElevenLabs Inc.	ElevenLabs Inc., 169 Madison Ave, #2354, New York, NY 10016, USA	Provision of AI-based audio and speech synthesis services (e.g. text-to-speech, speech- to-text); provision of the software infrastructure.	Data processing agreement (DPA) pursuant to Art. 28 GDPR in conjunction with: EU-US Data Privacy Framework (DPF) (where actively certified at the time of retrieval); additionally/subsidiarily: EU standard contractual clauses (SCCs), Module 2 (controller to processor) or Module 3 (processor to processor), incorporated in the ElevenLabs DPA, with Irish jurisdiction.
*Perplexity AI, Inc.	555 De Haro St, Suite 400, San Francisco, CA 94107, USA	Provision of the search and web API (Perplexity API) for web connectivity.	Data processing agreement (DPA) pursuant to Art. 28 GDPR is concluded via the commercial API DPA. Third-country transfer / safeguard: EU standard contractual clauses (SCC) – Module 2 (controller-to- processor) are incorporated in the DPA. In addition, the EU-US Data Privacy Framework (DPF) applies where certification is active at the time of processing. Data are not used to train the AI.
*staan.ai	2 rue Kellermann 59100 Roubaix France	Provision of the search and web API for web connectivity.	Art. 28: General Terms and Conditions (DPA) concluded. Art. 44 et seq.: Not applicable (server location & processing in the EU).

*Customers have the option of deactivating optional services in the administration interface.

Annex 5: Person Authorised to Issue Instructions

At the Client (please complete)

Surname, first name	
Address	
Telephone	
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.

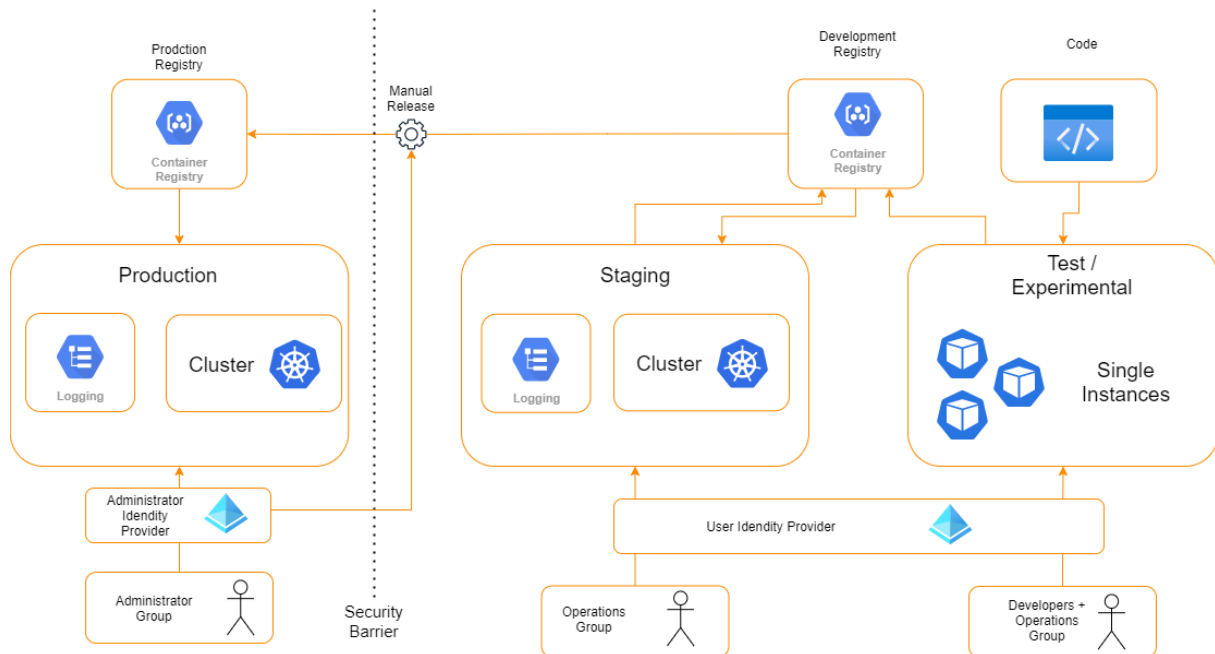


Figure 1: Different Environments and Interconnection at amber

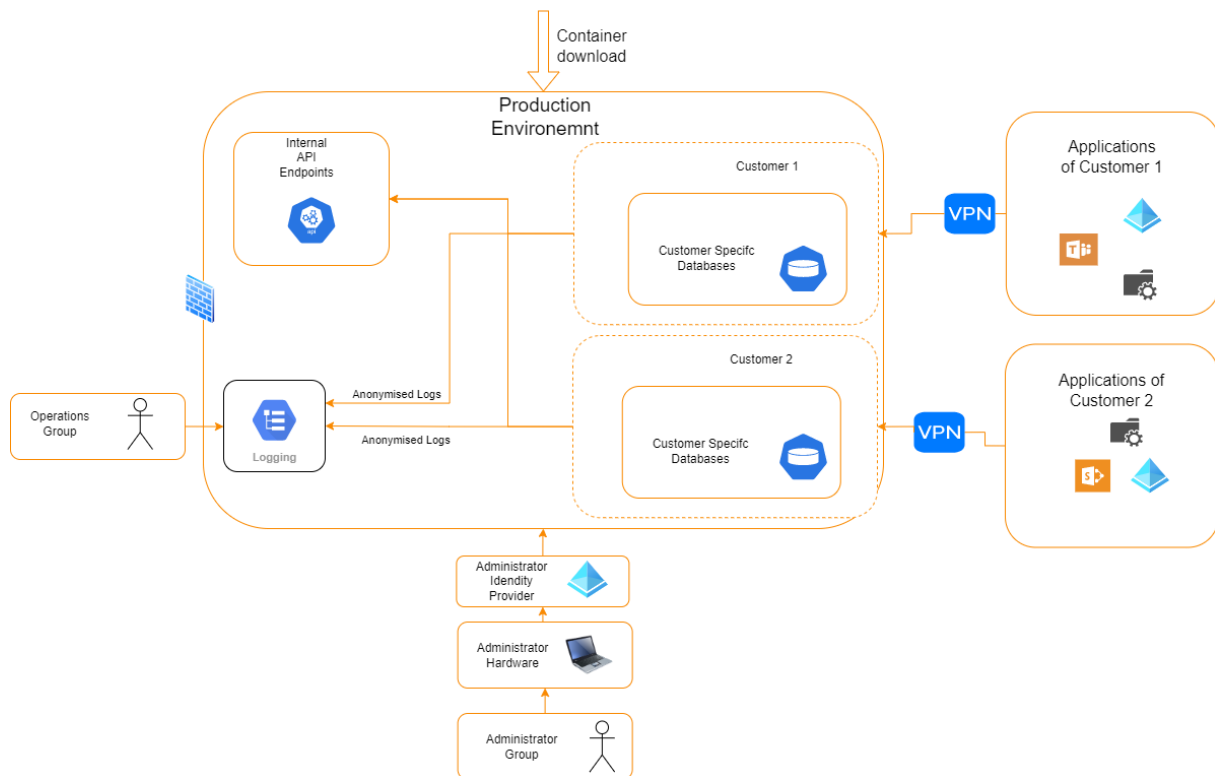


Figure 2: Detail View on Connectivity of the Production Environment

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)