Datenschutzkonzept für den Einsatz von semantha in der Cloud

Data Protection and Privacy Concept for the Use of semantha in the Cloud

Stand: 15.12.2022 As of: 2022-12-15

Convenience Translation

semantha

semantha wird dazu genutzt, Dokumente zu analysieren. Die Software ermittelt dabei inhaltliche Übereinstimmungen zwischen Textpassagen, extrahiert spezifische Daten aus Prosa und kann die extrahierten Daten auf Basis eines benutzerdefinierten Regelwerks bearbeiten/interpretieren.

semantha ist zwar ein KI-System, sie verwendet die analysierten Dokumente jedoch nicht zum Training und speichert Anfragen bzw. analysierte Dokumente auch nicht ab. Aus Sicht von semantha sind die analysierten Dokumente reine Nutzdaten, die basierend auf einer Konfiguration (Konfigurationsdaten), die üblicherweise keine personenbezogene Daten (“pbD”) enthält, verarbeitet werden. Die Nutzdaten werden nicht in semantha persistiert, sondern sie arbeitet zustandslos: Ein Nutzer übermittelt in der Anfrage die Nutzdaten an semantha, diese analysiert sie und antwortet mit dem Analyseergebnis. Weder Nutzdaten noch Analyseergebnis werden im System gespeichert.

Kein Datentransfer in DS-GVO-Drittstaaten

Entsprechend der oben beschriebenen Vorgänge übermitteln wir aktiv keine (personenbezogenen) EU-Daten in DS-GVO-Drittstaaten.

semantha

semantha is used to analyze documents. The software determines content matches between text passages, extracts specific data from prose and can manipulate/interpret the extracted data based on a user-defined set of rules.

Even though semantha is an AI system, she does not use the analyzed documents for training and does not store queries or analyzed documents. From semantha's point of view, the analyzed documents are pure user data that are processed based on a configuration (configuration data) that usually does not contain any personal data ("pbD"). The user data is not persisted in semantha, but it works stateless: a user submits the user data to semantha in the request, it analyzes it and responds with the analysis result. Neither user data nor analysis results are stored in the system.

No Data Transfer to GDPR Third Countries

In accordance with the processes described above, we do not actively transfer any (personal) EU data to GDPR Third Countries.

Wir setzen bei der Bereitstellung unserer SaaS-Anwendung semantha auf etablierte Cloud-Anbieter, bei denen wir Infrastructure-as-a-Service anmieten (vgl. Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO als Anlage zu unserem SaaS-Nutzungsvertrag). Wir stellen semantha für Kunden aus der EU ausschließlich in/auf/aus Rechenzentren bereit, die sich innerhalb der EU befinden. Der Standort des Rechenzentrums einer konkreten semantha-Instanz kann vom Support erfragt werden.

Eine Instanz von semantha ist und arbeitet autark, d.h. es findet bei der Datenverarbeitung softwareseitig keine weitere Übermittlung von Daten (bspw. zu weiteren Sub-Dienstleistern) statt – die gesamte Verarbeitung erfolgt innerhalb der von thingsTHINKING administrierten Systeme in den EU-Rechenzentren.

Kein DS-GVO-Drittlandzugriff durch Subunternehmer

Ein geplanter bzw. von uns autorisierter Zugriff durch Dritte (oder Mitarbeiter von Dritten) auf die Systeme, die wir zur Leistungserbringung einsetzen z.B. im Rahmen eines technischen Supports, einer Fernwartung oder aufgrund von Schnittstellen zu einem Drittstaat außerhalb der EU, erfolgt nicht. Da semantha zudem keine Nutzdaten persistiert, wäre eine Kenntnisnahme im Rahmen von Fernwartung o.Ä. auch nicht möglich.

Im Folgenden ist beschrieben, wie die einzelnen Schutzziele bei der Arbeit mit semantha erreicht werden.

Vertraulichkeit

We rely on established cloud providers for the provision of our SaaS application semantha, from whom we rent Infrastructure-as-a-Service (see contract for commissioned processing pursuant to Art. 28 DS-GVO as an attachment to our SaaS usage agreement). We provide semantha for customers from the EU exclusively in/on/from data centers located within the EU. The location of the data center of a specific semantha instance can be requested from support.

An instance of semantha is and works self-sufficiently, i.e. no further transfer of data (e.g. to further sub-service providers) takes place on the software side during data processing – all processing takes place within the systems administered by thingsTHINKING in the EU-based data centers.

No GDPR-third-country access by subcontractors

There is no planned or authorized access by third parties (or employees of third parties) to the systems we use to provide services, e.g., in the context of technical support, remote maintenance or due to interfaces to a third country outside the EU. Since semantha does not persist any user data, it would also not be possible to gain knowledge in the context of remote maintenance or similar.

The following describes how the individual protection goals are achieved when working with semantha.

Protection of Confidentiality

Vertraulichkeitsschutz: Der Zugriff auf semantha und damit alle auf der Plattform gespeicherten Daten ist mit einem Zugangscode geschützt.

Ein Zugangscode gewährt Zugriff auf eine (oder mehrere) benannte Datenbank(en) und ermöglicht so dem Inhaber des Zugangscodes, Einsicht in die Daten zu nehmen. Datenbanken sind technisch voneinander getrennt, sodass ein Zugriff auf fremde Daten unterbunden wird.

Zugangscodes werden durch tT mit einem kryptografisch abgesicherten Verfahren erzeugt und verschlüsselt verwaltet. Manuelle Einsichtnahme in die gesamte Liste der Zugangscodes ist nicht möglich; Mitarbeiter können lediglich Zugangscodes erzeugen und bestehende Codes an die zugeordnete E-Mail-Adresse senden. Wird ein Zugangscode kompromittiert, kann er gesperrt oder neu ausgestellt werden. Administrative Interaktion mit der Verwaltung der Zugangscodes wird automatisch protokolliert.

Verschiedene Instanzen von semantha speichern ihre Datenbanken auf unterschiedlichen Datenträgern. Der Zugriff auf einen Datenträger einer fremden semantha-Instanz ist technisch nicht möglich.

Kontrollziele, sofern nicht bereits aufgeführt:

Ziel	**Umsetzung**
Zutritt: Unbefugten ist der räumliche Zutritt zu Datenverarbeitungsanlagen zu verwehren.	Die Datenverarbeitung erfolgt auf virtuellen Rechnersystemen, die in Rechenzentren von Drittanbietern (Cloudanbietern) betrieben werden. Der physische Zutritt zu den Rechenzentren unterliegt den Einschränkungen, die der jeweilige Cloudanbieter auferlegt und sicherstellt.

Confidentiality: Access to semantha and thus all data stored on the platform is protected with an access key.

An access key grants access to one (or more) named database(s) and thus enables the holder of the access key to view the data. Databases are technically separated from each other so that unauthorized access of data is prevented.

Access codes are generated and managed in encrypted form by tT using a cryptographically secured process. Manual inspection of the entire list of access codes is not possible; authorized employees can only generate access codes and send existing codes to the assigned e-mail address. If an access code is compromised, it can be blocked or re-issued. Administrative interaction with access code management is automatically logged.

Different instances of semantha store their databases in different database instances. Accessing another semantha instance's database instance from a semantha instance is technically not possible.

Objectives, if not already listed:

Objective	**implementation**
Admission Control: Unauthorized persons are to be denied access to data processing systems.	Data processing takes place on virtual computer systems that are operated in data centers which are operated by third-party providers (cloud providers). Physical access to the data centers is subject to the restrictions imposed and ensured by the respective cloud provider.

	Zutritt zu den Räumen der tT ist grundsätzlich ausschließlich Mitarbeitern der tT gestattet.		In general, only tT employees are permitted to enter tT premises.
Zugang: Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Der Zugang zum Frontend bzw. der REST-API ist wie oben beschrieben mit Zugangscodess gesichert. Es gibt keine Schnittstelle zu semantha, die nicht über einen Zugangscode abgesichert ist. Zugriff auf die virtuellen Serversysteme ist ausschließlich über eine SSH-verschlüsselte Verbindung für ausgewählte Mitarbeiter von tT möglich. Der Zugriff ist zudem nur innerhalb eines dedizierten VPN-Netzwerks möglich. Ein passwortbasierter SSH-Zugang ist nicht zugelassen. Zugang zur Verwaltungsoberfläche der Cloudanbieter ist ausgewählten Mitarbeitern der tT vorbehalten und mit Zweifaktor-Authentifizierung gesichert.	Entry Control: It must be prevented that data processing systems can be used by unauthorized persons.	Access to the user interface and the REST API is secured with access keys as described above. There is no interface to semantha that is not secured by an access key. Access to the virtual server systems is only possible via an SSH-encrypted connection for selected tT employees. To access the SSH ports, the client has to be in a dedicated VPN. Password-based SSH access is not permitted. Access to the administration interface of the cloud provider is reserved for selected tT employees and is secured with two-factor authentication.
Zugriffe: Es ist zu gewährleisten, dass systemische Datenzugriffsmöglichkeiten nur im Umfang von Befugnissen und Erforderlichkeiten bestehen, z.B. durch Verschlüsselung.	Die Datenübertragung zwischen semantha und dem zugreifenden Klienten (z. B. semanthas Weboberfläche) wird ausschließlich über verschlüsselte Verbindungen abgewickelt, wobei derzeit zwingend	Transmission Control: It must be ensured that systemic data access options only exist within the scope of authorizations and requirements, e.g., through encryption.	The data transfer between semantha and the accessing client (e.g., semantha's web interface) is handled exclusively via encrypted connections, with TLS 1.2 (TLS 1.3 also being used on selected servers).

	TLS 1.2 (auf ausgewählten Servern auch TLS 1.3) zum Einsatz kommt. Die REST-API ist ebenso ausschließlich über TLS gesichert erreichbar.		The REST API can also only be reached securely via TLS.
Weitergabe: Es ist zu gewährleisten, dass auf personenbezogene Daten bei Übertragung, Transport oder auf Datenträgern nicht unbefugt zugegriffen und dass festgestellt werden kann, welchen Stellen die Daten offengelegt wurden, z.B. durch Verschlüsselung.	Übernimmt der Auftraggeber das Einpflegen/Hochladen der Daten in die Datenbank von semantha, so erfolgt dies - wie oben beschrieben - ausschließlich über verschlüsselte Kommunikationswege. Erfolgt das Einpflegen der Daten durch die tT nach Datenweitergabe vom Auftraggeber, erfolgt diese auf einem vom Auftraggeber festzulegenden Weg. Die Absicherung der Kommunikation zwischen dem Auftraggeber und tT obliegt dem Auftraggeber (Verschlüsselung der Verbindung, Zugriffsschutz auf Austauschlaufwerke u.Ä.). tT übernimmt dann die Datenpflege innerhalb von semantha. Die Datenübertragung zwischen dem Mitarbeiter von tT und semantha erfolgt - wie oben beschrieben - ausschließlich über verschlüsselte Kommunikationswege. Die Windows- und Linux Arbeitsplätze der tT sind mit Passwortschutz	Circulation: It must be ensured that personal data is not accessed by unauthorized persons during transmission, transport or on data carriers and that it can be determined to whom data has been disclosed, e.g., by using encryption.	If the client enters / uploads data into the semantha database, this is done - as described above - exclusively via encrypted communication channels. If the data is entered by tT after the data has been sent to tT by the customer, the mode of transfer is at the sole discretion of the customer. Securing communication between the customer and tT is the responsibility of the customer (encryption of the connection, access protection to file sharing services, etc.). tT then performs the data maintenance within semantha. The data transmission between the tT employee and semantha takes place - as described above - exclusively via encrypted communication channels. The Windows and Linux workstations at tT are password-protected and have hard drives encrypted with OS-based encryption (e.g. bitlocker). There is no additional data transfer.

	versehen und verfügen über mit Betriebssystem-Bordmitteln verschlüsselte Festplatten (z.B. bitlocker). Einer weitergehende Datenweitergabe erfolgt nicht.

Integrität

Integritätsschutz: Im Rahmen der Verarbeitung soll durch tT keine Veränderung der Daten (insbesondere der personenbezogenen) erfolgen. Sofern der Auftraggeber eine Änderung der Daten wünscht, stellt er neue Daten zum Import bereit oder aktualisiert sie selbstständig über die Webschnittstelle von semantha.

semantha arbeitet Dokument-orientiert; der Inhalt von Dokumenten ist veränderbar. Aus den Server-Logs ist ersichtlich, welcher Zugangscode zum Anlegen, Bearbeiten oder Löschen eines Datensatzes verwendet wurde.

Kontrollziele, sofern nicht bereits aufgeführt:

Ziel	**Umsetzung**
Eingabe: Es ist zu gewährleisten, dass festgestellt werden kann, ob und von wem personenbezogene Daten verarbeitet wurden.	Der Zugriff auf semantha wird unter Bezugnahme auf den zum Zugriff verwendeten Zugangscode (siehe Abschnitt Vertraulichkeit) protokolliert. Im Protokoll ist die ID des jeweiligen Datensatzes vermerkt, auf den zugegriffen wurde.

Integrity

Integrity protection: When processing data, tT should not modify the data (in particular personal data). If the client wishes to modify the data, the customer provides new data for import or updates the data via the semantha web interface.

semantha works document-oriented; the content of documents can be altered. The server log shows which access key was used to create, update, or delete a data record.

Objectives, if not already listed:

Objective	**Implementation**
Input: It must be ensured that it can be determined whether and by whom personal data has been processed.	Access to semantha is logged with reference to the access key used for access (see section Confidentiality). The ID of the respective data record that was accessed is noted in the log.

Datentrennung:

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

semantha stellt je Anwendungsfall (und je Kunde) einen Co-Worker (das ist eine Datenbank zzgl. Anwendungsfall-spezifischer Konfiguration) bereit. Der Zugriff auf einen Co-Worker ist nur dann möglich, wenn ein entsprechender Zugangscode verwendet wird.
Verschiedene Co-Workers sind zum einen logisch voneinander getrennt (d.h. Jeder Co-Worker verfügt über einen eigenen Speicherbereich im Dateisystem), zum anderen laufen nicht alle Kunden auf derselben Installation.
tT empfiehlt für jeden Verarbeitungszweck einen separaten Co-Worker zu verwenden und die Zugriffsrechte so auszugestalten, dass zweckübergreifender Zugriff nicht möglich ist. Die konkrete Ausgestaltung obliegt dem Auftraggeber.
Nach Absprache zwischen tT und dem Auftraggeber kann dem Kunden gegen ein zu vereinbarendes Entgelt zudem ein oder mehrere dedizierte Server eingerichtet werden. So kann einerseits eine physische Trennung von anderen Kunden der tT und andererseits eine physische Trennung von verschiedenen

Data Separation:

It must be ensured that data collected for different purposes can be processed separately.

semantha provides a Co-Worker (that is a database plus use case-specific configuration) for each use case (and per customer). Access to a Co-Worker is only granted if a corresponding access key is used.
On the one hand, the Co-Workers are logically separated from each other (i.e. each Co-Worker has its own storage area in the file system and database). On the other hand, not all customers run on the same instance.
tT recommends using a separate Co-Worker for each processing purpose and structuring the access rights in such a way that cross-purpose access is not possible. The specific design is the sole responsibility of the customer.
Upon agreement between tT and the customer, tT can also set up one or more dedicated servers specifically for the customer for an additional fee to be agreed on. In this way, physical data separation from other customers of tT and physical separation of different processing purposes can be achieved.

Verarbeitungszwecken erreicht werden.

Verfügbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen Verlust geschützt sind.

Die Datenbank von semantha wird täglich automatisch gesichert. Hierzu werden die vom Cloudanbieter bereitgestellten Sicherungstechniken verwendet. Die Entscheidung, welche Sicherungstechnik zum Einsatz kommt, obliegt allein der tT.

Variante 1: Datensicherung. Es wird der Speicherbereich gesichert, der die Konfiguration und die Datenbanken enthält. Dieser kann unabhängig von der Serverinstanz wiederhergestellt werden. Es können vollständige oder inkrementelle Sicherungen angelegt werden.

Variante 2: Systemsicherung. Hierbei handelt es sich um eine vollständige Sicherung des virtuellen Serversystems. Die Wiederherstellung ist unabhängig vom konkreten virtuellen Server möglich.

Sicherungsdateien werden 30 Tage aufbewahrt und anschließend automatisch gelöscht.

Availability

It must be ensured that personal data is protected against loss.

The semantha database is automatically backed up daily. The backup techniques provided by the cloud provider are used for this purpose. The decision as to which backup technology and strategy is used is at the sole discretion of tT.

Variant 1: data backup. The storage area that contains the configuration and the databases is backed up. This can be restored regardless of the server instance. Full or incremental backups can be made.

Variant 2: system backup. This is a full backup of the virtual server system. The recovery is possible regardless of the specific virtual server.

Backup files are kept for 30 days and are then deleted automatically.

Unterauftragsverarbeiter

tT setzt für die Bereitstellung der Cloud-Dienste Unterauftragsverarbeiter zum Zwecke der Bereitstellung von Rechenleistung und Datenspeicher für den

Sub-processors

tT uses sub-processors for the provision of cloud services, for the purpose of providing computing power and data storage, for the operation of (virtual)

Betrieb (virtueller) Server und Plattformen, für die Datensicherung und dafür notwendige (Internet-)Konnektivität (Infrastructure-as-a-Service, IaaS, sowie Platform-as-a-Service, PaaS) ein. Die Unterauftragsverarbeiter stellen lediglich die Infrastruktur für die virtuellen Server bereit. Die Pflege, der Betrieb von semantha usw. erfolgt ausschließlich durch die tT.

Microsoft Azure

1. Unternehmen und Sitz: Microsoft Corporation, Redmond; Microsoft Ireland Operations, Ltd., Dublin
2. Auftragsleistungen: IaaS, PaaS.
3. Art der verarbeiteten personenbezogenen Daten: Alle in semantha verarbeiteten Daten.

Amazon Web Services

1. Unternehmen und Sitz: Amazon Web Services EMEA SARL, Luxemburg; Amazon Web Services EMEA SARL, Niederlassung Deutschland, Sitz der Zweigniederlassung: München
2. Auftragsleistungen: IaaS, PaaS.
3. Art der verarbeiteten personenbezogenen Daten: Alle in semantha verarbeiteten Daten.

Hinweis: Für die Verarbeitung von Daten aus der EU werden ausschließlich (virtuelle) Server in Rechenzentren innerhalb der EU eingesetzt.

Atlassian PTY Ltd. – Jira, Confluence (Cloud)

1. Unternehmen und Sitz: Atlassian PTY Ltd., Australien
2. Auftragsleistungen: (Jira) Customer Service Desk
3. Art der verarbeiteten personenbezogenen Daten: Benutzeraccounts, E-Mail-Adressen, die im Rahmen von Fehlerberichten und Supportanfragen etc. anfallen.

servers and platforms, for data backup, and the (Internet) connectivity required for this (Infrastructure-as-a-Service, IaaS , and Platform-as-a-Service, PaaS). The sub-processors only provide the infrastructure for the virtual servers. The maintenance and operation of semantha etc. is carried out exclusively by tT.

Microsoft Azure

1. Company and headquarters: Microsoft Corporation, Redmond; Microsoft Ireland Operations, Ltd., Dublin
2. Contracted services: IaaS, PaaS.
3. Type of personal data processed: All data processed in semantha.

Amazon Web Services

1. Company and headquarters: Amazon Web Services EMEA SARL, Luxembourg; Amazon Web Services EMEA SARL, Germany branch, branch office: Munich
2. Contracted services: IaaS, PaaS.
3. Type of personal data processed: All data processed in semantha.

Note: Only (virtual) servers in data centers within the EU are used to process data from the EU.

Atlassian PTY Ltd. – Jira, Confluence (Cloud)

1. Company and headquarters: Atlassian PTY Ltd., Australia
2. Contracted Services: (Jira) Customer Service Desk
3. Type of personal data processed: User accounts, email addresses and data in/for/from bug reports and support requests etc.

Zuständige Aufsichtsbehörde

In Baden-Württemberg, Deutschland:
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Competent Supervisory Authority

In Baden-Württemberg, Germany:
Baden-Wuerttemberg State Commissioner for Data Protection and Freedom of Information