

Demand Intelligence Security Whitepaper

1 Summary

1.1 Purpose of this Document

This document outlines compliance information in terms of IT security and data protection, for the application Demand Intelligence, developed and operated by sovanta AG.

1.2 About Demand Intelligence

Demand Intelligence is sovanta's application for capturing and shaping product demands. A user submits a demand, and the application synthesizes it into a structured concept and set of requirements, supporting the process end-to-end with governance summaries, generated PRDs (Product Requirement Documents), and an AI chat assistant (ARK). Users can also run AI-assisted stakeholder interviews to gather input while working through a demand.

1.3 Security Objectives

Demand Intelligence implements the following objectives to ensure that a user's data is secured at all times.

- Tenant Isolation: Ensures that users can only access their own tenant's data.
- Data Confidentiality: Ensures that all data is sufficiently protected at rest and in transit.
- Access Control: Ensures that only users who are properly entitled can access the application.
- AI Data Governance: Ensures that customer data processed by AI features is never used

1 Zusammenfassung

1.1 Zweck dieses Dokuments

Dieses Dokument beschreibt Compliance-Informationen zu IT-Sicherheit und Datenschutz für die von der sovanta AG entwickelte und betriebene Anwendung Demand Intelligence.

1.2 Über Demand Intelligence

Demand Intelligence ist sovantas Anwendung zur Erfassung und Ausgestaltung von Produkthanforderungen (Demands). Ein User reicht einen Demand ein, und die Anwendung fasst diese zu einem strukturierten Konzept und einem Anforderungskatalog zusammen. Dabei wird der Prozess durchgängig durch Governance-Zusammenfassungen, generierte PRDs (Product Requirement Documents) und einen KI-Chat-Assistenten (ARK) unterstützt. Zusätzlich können User KI-gestützte Stakeholder-Interviews durchführen, um während der Bearbeitung eines Demands weiteren Input einzuholen.

1.3 Security-Ziele

Durch die folgenden Maßnahmen gewährleistet Demand Intelligence, dass die Daten der User jederzeit geschützt sind.

- Tenant-Isolation: Stellt sicher, dass User ausschließlich auf die Daten ihres eigenen Tenants zugreifen können.
- Datenvertraulichkeit: Gewährleistet, dass alle Daten in Ruhe und während der Übertragung ausreichend geschützt sind.
- Zugriffskontrolle: Stellt sicher, dass nur User mit den entsprechenden Berechtigungen auf die Anwendung zugreifen können.
- KI Data Governance: Stellt sicher, dass Kundendaten, die von KI-Funktionen

to train third-party model providers' models or ARK.

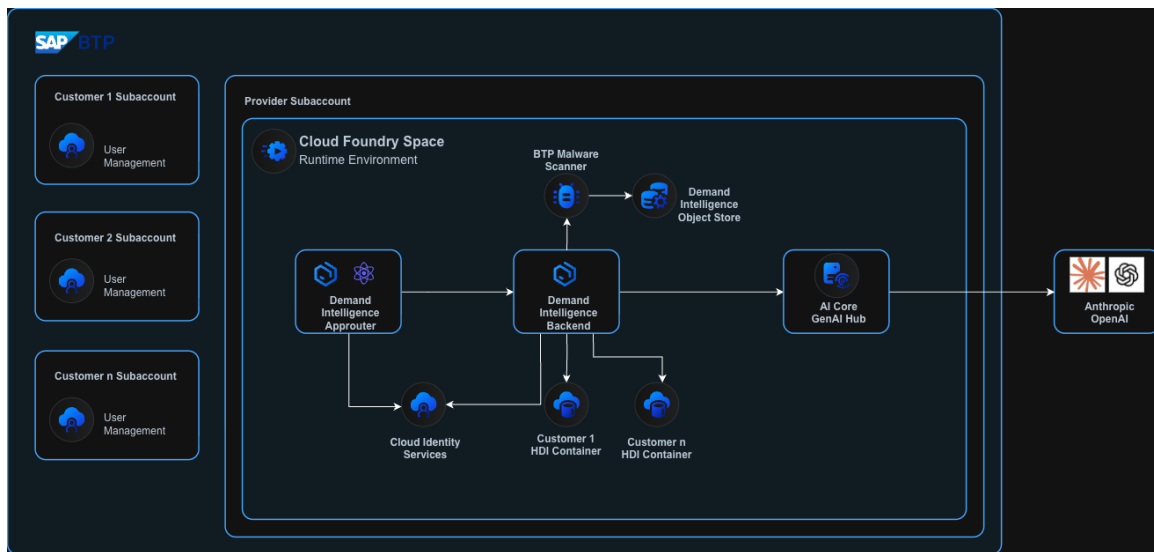
verarbeitet werden, niemals zum Training der Modelle von Drittanbietern oder von ARK verwendet werden.

2 System Architecture Overview

Demand Intelligence is a cloud-native web application, running on SAP BTP. The following picture displays the overall system architecture including the relevant SAP BTP components in use.

2 Überblick der Systemarchitektur

Demand Intelligence ist eine cloud-native Webanwendung, die auf SAP BTP läuft. Die folgende Abbildung zeigt die übergeordnete Systemarchitektur, einschließlich der relevanten genutzten SAP-BTP-Komponenten.



2.1 Components

The following components are in use to provide the application Demand Intelligence to its users.

2.1 Komponenten

Die folgenden Komponenten kommen zum Einsatz, um die Anwendung Demand Intelligence für Ihre User bereitzustellen.

2.1.1 SAP BTP

The Demand Intelligence application is implemented as a multi-tenant application (SaaS application). It is running on Cloud Foundry on SAP BTP in a provider subaccount. The subaccount is set up with the following settings:

2.1.1 SAP BTP

Die Anwendung Demand Intelligence ist als Multi-Tenant-Anwendung (SaaS-Anwendung) implementiert. Sie läuft auf Cloud Foundry auf SAP BTP in einem Provider-Subaccount. Der Subaccount ist mit folgenden Einstellungen konfiguriert:

- Provider: Amazon Web Services (AWS)
- Region: Europe (Frankfurt)
- Provider: Amazon Web Services (AWS)
- Region: Europa (Frankfurt)

Administrative access to this subaccount for operational purposes is available to a limited set of sovanta employees.

Access to the application is implemented via subscriber subaccounts which are created per customer. The subscriber subaccounts are set up in the following way:

- Provider: Amazon Web Services (AWS)
- Region: Europe (Frankfurt)

2.1.2 Backend

The backend of the application is implemented using the SAP CAP framework utilizing its many security features out of the box.

2.1.3 Frontend

The frontend of the application is implemented using React and is running on a hosted SAP Approuter.

2.1.4 Relational Data Storage

All user-generated relational data is stored in an isolated HDI container created per customer on a shared HANA Cloud instance. The HANA Cloud instance is maintained by sovanta and upgraded to the newest available revision at regular intervals.

The following categories of data are stored on HANA Cloud:

- Demands & Concepts: the requirement content itself: titles, descriptions, and fields extracted from a submitted demand.
- Attachments, PRDs & Prototypes: Metadata of uploaded and AI-generated files. Content is stored in the Object Store (see §2.1.5).
- Persons & Stakeholder Invitations: name and email of people associated with a demand, plus a hashed, single-purpose token for each stakeholder invitation link.

Eine begrenzte Anzahl von sovanta-Mitarbeitern verfügt zu betrieblichen Zwecken über Administratorrechte für diesen Subaccount.

Der Zugriff auf die Anwendung erfolgt über Subscriber-Subaccounts, die pro Kunde angelegt werden. Die Subscriber-Subaccounts sind wie folgt konfiguriert:

- Provider: Amazon Web Services (AWS)
- Region: Europa (Frankfurt)

2.1.2 Backend

Das Backend der Anwendung basiert auf dem SAP-CAP-Framework und nutzt dessen zahlreiche integrierte Sicherheitsfunktionen.

2.1.3 Frontend

Das Frontend der Anwendung ist mit React implementiert und läuft auf einem gehosteten SAP Approuter.

2.1.4 Relationale Datenspeicherung

Alle von Usern generierten relationalen Daten werden in einem isolierten HDI-Container gespeichert, der pro Kunde auf einer gemeinsam genutzten HANA-Cloud-Instanz angelegt wird. Die HANA-Cloud-Instanz wird von sovanta gepflegt und in regelmäßigen Abständen auf die neueste verfügbare Revision aktualisiert.

Auf HANA Cloud werden folgende Datenkategorien gespeichert:

- Demands & Concepts: der eigentliche Anforderungsinhalt, also Titel, Beschreibungen und aus einem eingereichten Demand extrahierte Felder.
- Attachments, PRDs & Prototypes: Metadaten hochgeladener und KI-generierter Dateien. Die Inhalte selbst liegen im Object Store (siehe §2.1.5).
- Persons & Stakeholder Invitations: Name und E-Mail-Adresse der mit einem Demand verknüpften Personen, dazu ein gehashter Single-Purpose-Token für jeden

The raw invitation token itself is never stored, only its hash.

- Stakeholder Responses & Approval Requests: contributor answers to a stakeholder interview, and approver decisions with any accompanying reasoning.
- Activity Approvers: for activities configured with a single fixed external approver, that approver's name and email, set by an administrator on the activity template.
- User Settings: a per-user identifier plus onboarding and beta-notice acknowledgement flags.
- ARK chat history: a user's chat threads and messages with the ARK assistant.
- Custom process configuration: demand types, activity templates, and AI agents/skills a tenant admin creates or customizes, including any system prompts they author for a custom AI agent.
- Governance content library: documentation, links, and assets managed in the Governance Hub.

Every record above is timestamped and attributed to the user (email) who created and last updated it.

2.1.5 Blob Storage

All user-generated blob data (e.g. uploaded files, generated PRDs and prototypes) is stored via a single SAP Object Store, following the prefix-based design pattern ([Design patterns for multi-tenant access control on Amazon S3 | Amazon Web Services](#)).

The data is stored in a bucket on AWS.

2.1.6 AI Processing

Stakeholder-Einladungslink. Der rohe Einladungs-Token selbst wird nie gespeichert, nur dessen Hash.

- Stakeholder Responses & Approval Requests: Antworten der Beitragenden in einem Stakeholder-Interview sowie Entscheidungen der Genehmigenden mit etwaiger Begründung.
- Activity Approvers: bei Activities mit einem einzelnen fest hinterlegten externen Approver dessen Name und E-Mail-Adresse, festgelegt von einem Administrator in der Activity-Vorlage.
- User Settings: ein User-Identifizier sowie Kennzeichnungen für Onboarding und die Bestätigung des Beta-Hinweises.
- ARK Chat History: die Chat-Threads und Nachrichten eines Users mit dem ARK-Assistenten.
- Custom Process Configuration: Demandtypen, Activity-Vorlagen sowie KI-Agents/Skills, die ein Tenant-Administrator erstellt oder anpasst, einschließlich selbst verfasster System Prompts für einen benutzerdefinierten KI-Agent.
- Governance Content Library: Dokumentation, Links und Assets, die im Governance Hub verwaltet werden.

Jeder der oben genannten Datensätze ist mit einem Zeitstempel versehen und dem User (E-Mail-Adresse) zugeordnet, der ihn erstellt und zuletzt aktualisiert hat.

2.1.5 Blob Storage

Alle von Usern generierten Blob-Daten (z. B. hochgeladene Dateien, generierte PRDs und Prototypen) werden über einen einzigen SAP Object Store gespeichert, nach dem präfixbasierten Design Pattern ([Design patterns for multi-tenant access control on Amazon S3 | Amazon Web Services](#)). Die Daten liegen in einem Bucket auf AWS.

2.1.6 KI-Verarbeitung

AI features are processed through SAP AI Core and the Generative AI Hub, which route requests to models from Anthropic and OpenAI. See §9 for the full list of features that use AI and how customer data is handled.

KI-Funktionen werden über SAP AI Core und den Generative AI Hub verarbeitet, die Anfragen an Modelle von Anthropic und OpenAI weiterleiten. Eine vollständige Liste der Funktionen, die KI nutzen, sowie Informationen zum Umgang mit Kundendaten finden Sie in §9.

2.2 Multitenancy approach

The application utilizes the `@sap/cds-mtxs` library to implement multitenancy with SAP CAP. User access to the application is available only after a customer tenant was subscribed to Demand Intelligence through an administrator and the respective users were manually enabled on SAP BTP. The application utilizes the [SAP Authorization and Trust Management Service](#) (XSUAA) to verify that all incoming requests are properly authenticated and authorized.

2.2 Multitenancy-Ansatz

Die Anwendung nutzt die Bibliothek `@sap/cds-mtxs`, um Multitenancy mit SAP CAP umzusetzen. User erhalten erst dann Zugriff auf die Anwendung, wenn der Kunden-Tenant per Administrator eine Subscription für Demand Intelligence erhalten hat und die jeweiligen User manuell auf SAP BTP freigeschaltet wurden. Die Anwendung nutzt den [SAP Authorization and Trust Management Service](#) (XSUAA), um sicherzustellen, dass alle eingehenden Requests ordnungsgemäß authentifiziert und autorisiert sind.

3 Tenant Management and Isolation

The Demand Intelligence application is implementing SAP's best practices for building multitenant applications on SAP BTP. Following those guidelines, multitenancy is implemented by utilizing the [SaaS Provisioning Service](#) on SAP BTP.

3 Tenant-Management und - Isolation

Die Anwendung Demand Intelligence setzt SAPs Best Practices für den Aufbau von Multitenant-Anwendungen auf SAP BTP um. Diesen Guidelines folgend wird Multitenancy über den [SaaS Provisioning Service](#) auf SAP BTP realisiert.

For each customer, a new BTP subaccount is created by an administrator at sovanta. This subaccount is then subscribed to Demand Intelligence via the [SaaS Provisioning Service](#).

Für jeden Kunden legt ein Administrator bei sovanta einen neuen BTP-Subaccount an. Dieser Subaccount erhält anschließend über den [SaaS Provisioning Service](#) eine Subscription für Demand Intelligence.

3.1 Database Level Isolation

On the subscription of a new customer, the [BTP Service Manager](#) is used to dynamically create a new HDI container on sovanta's shared HANA Cloud instance. This container is only accessible to users of that specific customer. This is guaranteed by using the multitenancy implementation of SAP CAP (MTX) which internally takes care of this.

3.1 Isolation auf Datenbankebene

Bei der Subscription eines neuen Kunden legt der [BTP Service Manager](#) dynamisch einen neuen HDI-Container auf sovantas gemeinsam genutzter HANA-Cloud-Instanz an. Auf diesen Container können ausschließlich User des jeweiligen Kunden zugreifen. Dafür sorgt die Multitenancy-Implementierung von SAP CAP (MTX), die das intern übernimmt.

Customers are offboarded after a retention period of 30 days. When a customer is offboarded by unsubscribing the customer's subaccount, the HDI container is automatically deleted by the [BTP Service Manager](#). The customer's data is then no longer recoverable.

For more details refer to [Deploy Multitenant SaaS Applications | capire](#).

3.2 File Separation on Blob Storage

The Demand Intelligence application stores all blob data uploaded by customers on one shared BTP Object Store instance. The data is prefixed by tenant ID to ensure that one tenant cannot access the data of another tenant (see §3.3 Dynamic Routing).

When a customer is offboarded, sovanta removes all of that customer's data from the shared Object Store instance as part of a documented offboarding procedure, gated by a dry run and an explicit confirmation step, carried out after the customer's subscription has ended.

3.3 Dynamic Routing

When a user accesses the Demand Intelligence application, the SAP Approuter ensures that they are properly authenticated. The user is redirected to the identity provider configured on their subscriber subaccount (SAP's default identity provider) to authenticate. Upon successful authentication, the Identity Authentication Service (IAS) on BTP issues a JWT that encodes the user's roles and the user's tenant ID. As this JWT is cryptographically signed, the properties cannot be tampered with. This ensures that the tenant ID property always reflects the customer's subaccount through which they are subscribed to the application.

CAP automatically uses this tenant ID property to retrieve the HDI container credentials of the

Kunden werden nach einer Aufbewahrungsfrist von 30 Tagen offboarded. Wird ein Kunde offboarded, indem sein Subaccount die Subscription verliert (unsubscribed), löscht der [BTP Service Manager](#) den HDI-Container automatisch. Die Daten des Kunden sind anschließend nicht mehr wiederherstellbar.

Weitere Details: [Deploy Multitenant SaaS Applications | capire](#).

3.2 Dateitrennung im Blob Storage

Die Anwendung Demand Intelligence speichert alle von Kunden hochgeladenen Blob-Daten auf einer gemeinsam genutzten BTP-Object-Store-Instanz. Die Daten werden mit der Tenant-ID präfixiert, damit ein Tenant nicht auf die Daten eines anderen Tenants zugreifen kann (siehe §3.3 Dynamic Routing).

Wird ein Kunde offboarded, entfernt sovanta sämtliche Daten dieses Kunden aus der gemeinsam genutzten Object-Store-Instanz. Das erfolgt im Rahmen einer dokumentierten Offboarding-Prozedur mit vorgeschaltetem Dry Run und einem expliziten Bestätigungsschritt, nachdem die Subscription des Kunden beendet wurde.

3.3 Dynamic Routing

Wenn ein User auf die Anwendung Demand Intelligence zugreift, stellt der SAP Approuter sicher, dass er ordnungsgemäß authentifiziert wird. Der User wird zur Authentifizierung an den auf seinem Subscriber-Subaccount konfigurierten Identity Provider weitergeleitet (SAPs Standard-Identity-Provider). Nach erfolgreicher Authentifizierung stellt der Identity Authentication Service (IAS) auf BTP ein JWT aus, das die Rollen des Users und dessen Tenant-ID codiert. Da dieses JWT kryptografisch signiert ist, können seine Attribute nicht manipuliert werden. Damit ist sichergestellt, dass das Tenant ID Attribut stets den Subaccount des Kunden widerspiegelt, über den die Subscription für die Anwendung besteht.

CAP nutzt dieses Tenant ID Attribut automatisch, um die HDI-Container-Credentials des Subscriber-

subscriber's subaccount and directs all SQL queries to the correct HDI container.

Every access to the BTP Object Store is encapsulated through a dedicated service in the application. When accessing an object, the object prefix is automatically set to the tenant ID of the incoming request, therefore ensuring that users cannot access any other data not prefixed with their tenant ID.

A separate, more limited access path exists for external stakeholders who are invited to contribute to a demand without a BTP identity: an invitation is sent to a named contributor containing a single-purpose link. The link authenticates using a hashed, single-purpose token scoped to that one invitation rather than a JWT — it grants no access beyond submitting a contribution to the specific interview it was issued for.

Subaccounts abzurufen, und leitet alle SQL-Abfragen an den richtigen HDI-Container weiter.

Jeder Zugriff auf den BTP Object Store läuft gekapselt über einen dedizierten Service innerhalb der Anwendung. Beim Zugriff auf ein Objekt wird das Objekt-Präfix automatisch auf die Tenant ID des eingehenden Requests gesetzt. So ist sichergestellt, dass User nicht auf Daten zugreifen können, die nicht mit ihrer eigenen Tenant ID präfixiert sind.

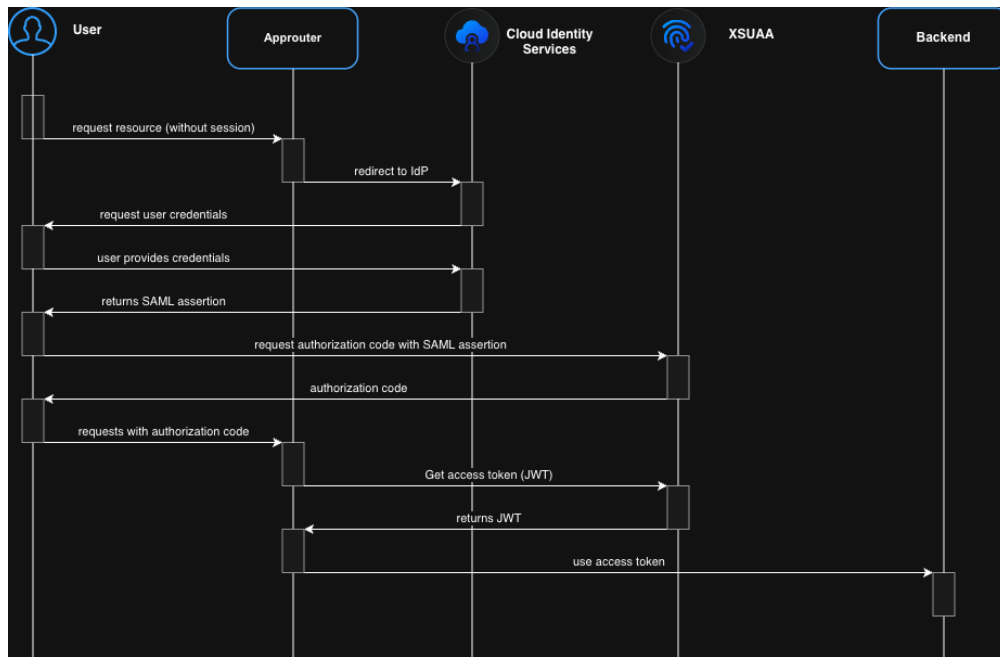
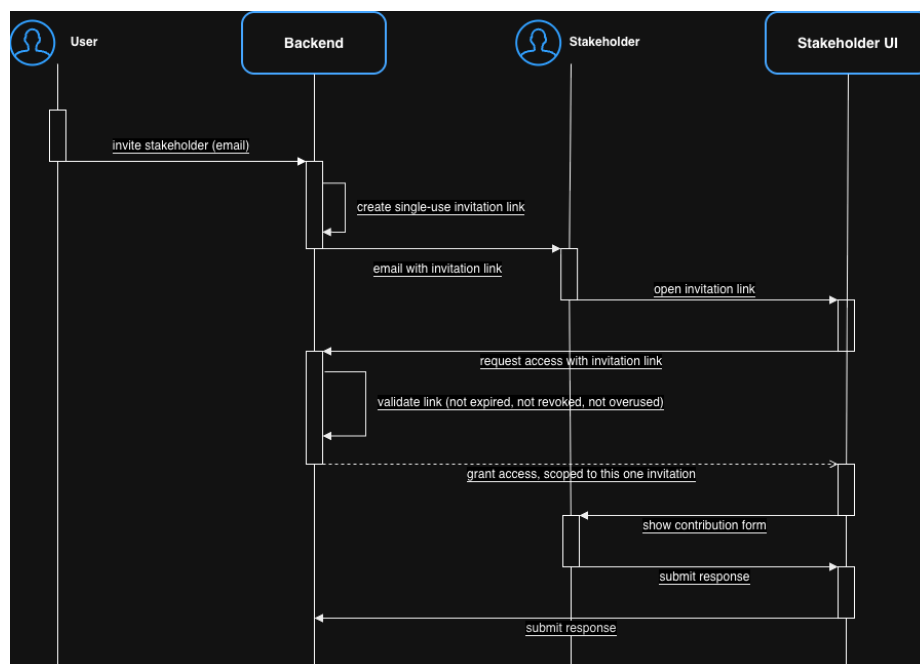
Für externe Stakeholder, die ohne eigene BTP-Identity zu einem Demand beitragen sollen, existiert ein separater, stärker eingeschränkter Zugriffspfad: Eine Einladung wird an einen namentlich genannten Mitwirkenden gesendet, die einen Einmal-Link enthält. Die Authentifizierung über diesen Link erfolgt anhand eines gehashten, auf genau diese eine Einladung begrenzten Tokens statt über ein JWT; er gewährt keinen weiteren Zugriff als die Abgabe eines Beitrags zu dem konkreten Interview, für das er ausgestellt wurde.

4 Authentication and Authorization

Demand Intelligence uses [SAP Identity Authentication](#) (IAS) and [SAP Authorization and Trust Management Service](#) (XSUAA) for the verification of authentication and authorization. All application endpoints are strictly authenticated and require valid authentication tokens (JWT). In addition, the authenticated users require an application-specific scope, which needs to be assigned via a BTP Role Collection to all eligible users. The authentication flow is implemented via OAuth2 as illustrated below:

4 Authentifizierung und Autorisierung

Demand Intelligence nutzt [SAP Identity Authentication](#) (IAS) und den [SAP Authorization and Trust Management Service](#) (XSUAA), um Authentifizierung und Autorisierung zu prüfen. Alle Endpoints der Anwendung sind strikt authentifiziert und erfordern gültige Authentifizierungs-Token (JWT). Zusätzlich benötigen authentifizierte User einen anwendungsspezifischen Scope, der allen berechtigten Usern über eine BTP Role Collection zugewiesen werden muss. Der Authentifizierungsablauf ist über OAuth2 umgesetzt, wie nachfolgend dargestellt:



5 Data Storage and Protection

Customer's data mentioned in §2.1.4 Relational Data Storage and §2.1.5 Blob Storage is stored in the following way:

5 Datenspeicherung und -schutz

Die in §2.1.4 Relationale Datenspeicherung und §2.1.5 Blob Storage genannten Kundendaten werden wie folgt gespeichert:

5.1 Relational Data

- Location: AWS, Europe (Frankfurt)
- Backup & Retention: 14 days of cloud backups
- Encryption: 256-bit Advanced Encryption Standard (AES-256)

5.2 Blob Data

- Location: AWS, Europe (Frankfurt)
- Backup & Retention: 14 days of blob data versioning
- Encryption: AWS S3 server-side 256-bit Advanced Encryption Standard (AES-256)

6 Network Security

All data traffic between applications and their used services is protected via TLS version 1.2 or higher. This is enforced through BTP itself (see [SAP Help Portal | SAP Online Help](#)). All backend endpoints are protected and require a valid JWT issued by the connected instance of XSUAA. The backend utilizes the SAP CAP library and the Node.js library [passport](#) to verify proper JWT usage.

7 Data Privacy and Compliance

7.1 GDPR

Demand Intelligence processes personal data as part of its normal operation: the names, emails, and roles of people associated with a demand, and the identity and responses of stakeholders invited to contribute to one (see §2.1.4). This data is processed on the basis of, and for the purposes described in the Data Processing Addendum. See §9 for how personal data is, and is not, used by the application's AI features.

5.1 Relationale Daten

- Standort: AWS, Europa (Frankfurt)
- Backup & Aufbewahrung: 14 Tage Cloud-Backups
- Verschlüsselung: 256-Bit Advanced Encryption Standard (AES-256)

5.2 Blob-Daten

- Standort: AWS, Europa (Frankfurt)
- Backup & Aufbewahrung: 14 Tage Blob-Daten-Versionierung
- Verschlüsselung: AWS-S3-serverseitiger 256-Bit Advanced Encryption Standard (AES-256)

6 Netzwerksicherheit

Sämtlicher Datenverkehr zwischen Anwendungen und den von Ihnen genutzten Services ist über TLS Version 1.2 oder höher geschützt. Das wird bereits von BTP selbst erzwungen (siehe [SAP Help Portal | SAP Online Help](#)). Alle Backend-Endpoints sind geschützt und erfordern ein gültiges, von der verbundenen XSUAA-Instanz ausgestelltes JWT. Das Backend nutzt die SAP-CAP-Bibliothek sowie die Node.js-Bibliothek [passport](#), um die korrekte JWT-Nutzung zu prüfen.

7 Datenschutz und Compliance

7.1 DSGVO

Demand Intelligence verarbeitet im normalen Betrieb personenbezogene Daten: Namen, E-Mail-Adressen und Rollen der mit einem Demand verknüpften Personen sowie Identität und Antworten eingeladener Stakeholder (siehe §2.1.4). Diese Verarbeitung erfolgt auf Grundlage und für die im Data Processing Addendum beschriebenen Zwecke. Wie personenbezogene Daten von den KI-Funktionen der Anwendung verwendet werden und wie nicht, ist in §9 beschrieben.

7.2 ISO 27001

ISO 27001 stands for ISO/IEC 27001 which is a globally recognized standard for an information security management system. The certification proves the fulfillment of information security requirements and the implementation of data protection measures. Sovanta AG is ISO27001-certified regarding the design, development, implementation, consulting, and operation of business software and data science solutions.

Our certificate can be found on our website:

[Compliance - sovanta AG](#)

7.3 BTP

The SAP BTP and its services are used to host the Demand Intelligence application. An overview of the compliance of the platform can be found here:

[SAP Trust Center | Security, Privacy, Cloud Status & More](#)

8 Vulnerability Management

Demand Intelligence is continuously scanning its code and dependencies for security vulnerabilities: static application security testing and secret scanning run on every change, and a software bill of materials is checked against known vulnerabilities on every build, blocking the pipeline if a critical or high-severity issue is found. Security patches for critical vulnerabilities are applied as soon as they are available. Dependencies are kept up to date through automated update tooling.

9 AI Usage

9.1 Processing

AI features in Demand Intelligence are processed through SAP AI Core and the Generative AI Hub, which

7.2 ISO 27001

ISO 27001 steht für ISO/IEC 27001, einen weltweit anerkannten Standard für Informationssicherheits-Managementsysteme. Die Zertifizierung belegt die Erfüllung der Anforderungen an die Informationssicherheit und die Umsetzung von Datenschutzmaßnahmen. Die sovanta AG ist ISO-27001-zertifiziert für Design, Entwicklung, Implementierung, Beratung und Betrieb von Business-Software und Data-Science-Lösungen.

Unser Zertifikat finden Sie auf unserer Website:

[Compliance - sovanta AG](#)

7.3 BTP

SAP BTP und die zugehörigen Services werden zum Hosting der Anwendung Demand Intelligence genutzt. Einen Überblick über die Compliance der Plattform finden Sie hier:

[SAP Trust Center | Security, Privacy, Cloud Status & More](#)

8 Schwachstellenmanagement

Demand Intelligence scannt Code und Abhängigkeiten fortlaufend auf Sicherheitslücken: Bei jeder Änderung laufen Static Application Security Testing und Secret Scanning, und bei jedem Build wird eine Software Bill of Materials gegen bekannte Schwachstellen geprüft; die Pipeline wird gestoppt, falls ein kritisches oder schwerwiegendes Problem gefunden wird. Sicherheitspatches für kritische Schwachstellen werden eingespielt, sobald sie verfügbar sind. Abhängigkeiten werden über automatisiertes Update-Tooling aktuell gehalten.

9 KI-Nutzung

9.1 Verarbeitung

KI-Funktionen in Demand Intelligence werden über SAP AI Core und den Generative AI Hub verarbeitet,

route requests to models provided by Anthropic and OpenAI.

die Anfragen an Modelle von Anthropic und OpenAI weiterleiten.

9.2 Where AI is used

- Demand intake: extracting structured fields from a submitted demand and its attachments
- Concept synthesis: turning a demand into a structured concept
- Requirement layer classification
- Governance summary generation
- Prototype generation
- Clarifying-question generation for open items
- PRD (Product Requirements Document) generation
- Recommended next actions
- Requirement-to-source citation linking
- Demand type suggestion
- Attachment content summarization
- AI chat assistant (ARK) for questions about a demand or the overall portfolio
- AI-assisted stakeholder interviews: the AI works with stakeholder roles and categories only (e.g. "Finance", "IT Security"); it does not receive or generate individual stakeholder names or contact details
- AI feedback on deliverables and requirements

9.2 Wo KI eingesetzt wird

- Demand Intake: Extraktion strukturierter Felder aus einem eingereichten Demand und dessen Anhänge
- Concept Synthesis: Verdichtung eines Demands zu einem strukturierten Konzept
- Requirement Layer Classification
- Generierung von Governance Zusammenfassungen
- Generierung von Prototypen
- Generierung von Rückfragen zu offenen Punkten
- Generierung von PRDs (Product Requirements Document)
- Empfehlungen für nächste Schritte
- Verknüpfung von Anforderungen mit Quellenangaben
- Vorschlag des Demandtyps
- Zusammenfassung von Attachment-Inhalten
- KI-Chat-Assistent (ARK) für Fragen zu einem Demand oder zum Gesamtportfolio
- KI-gestützte Stakeholder-Interviews: Die KI arbeitet ausschließlich mit Stakeholder-Rollen und -Kategorien (z. B. „Finance“, „IT Security“); sie erhält und generiert keine individuellen Namen oder Kontaktdaten von Stakeholdern.
- KI-Feedback zu Deliverables und Anforderungen

9.3 Data handling

Customer data is not used to train the model providers' models, and is not used to train ARK. The usage analysis sovanta runs through the AI Core API is telemetry for operational cost tracking, not model training, and does not change this.

9.3 Umgang mit Daten

Kundendaten werden nicht zum Training der Modelle der Modellanbieter verwendet und auch nicht zum Training von ARK. Die Nutzungsanalyse, die sovanta über die AI-Core-API durchführt, ist Telemetrie zur betrieblichen Kostenverfolgung, kein Modelltraining, und ändert daran nichts.

Where a stakeholder is invited to contribute to a demand, their name and email are used to deliver and

Wird ein Stakeholder zur Mitwirkung an einem Demand eingeladen, werden Name und E-Mail-

track that invitation; this data is not passed to an AI model. AI features that work with stakeholder input operate on role- and category-level information only, as described in §9.2.

Adresse zur Zustellung und Nachverfolgung dieser Einladung verwendet; diese Daten werden nicht an ein KI-Modell übergeben. KI-Funktionen, die mit Stakeholder-Input arbeiten, verarbeiten ausschließlich Informationen auf Rollen- und Kategorieebene, wie in §9.2 beschrieben.