

# Platform-Service Description

SmartStash

Document translated from the official german version. In case of ambiguity, the german version of the document applies.

Gertjan Rossing

Fellowmind Germany GmbH

© Fellowmind Germany GmbH. All rights reserved. This document is provided "as is". Information and views expressed in this document, including URL and internet Web site references, are subject to change without notice. The risk of use is with you. Some examples are for illustrative purposes only and are fictitious. Any resemblance to real companies or organizations is purely coincidental. This document does not transfer any intellectual property rights to a Fellowmind Germany GmbH product to you. You are authorized to copy this document and use it for your own internal reference purposes.

# Index

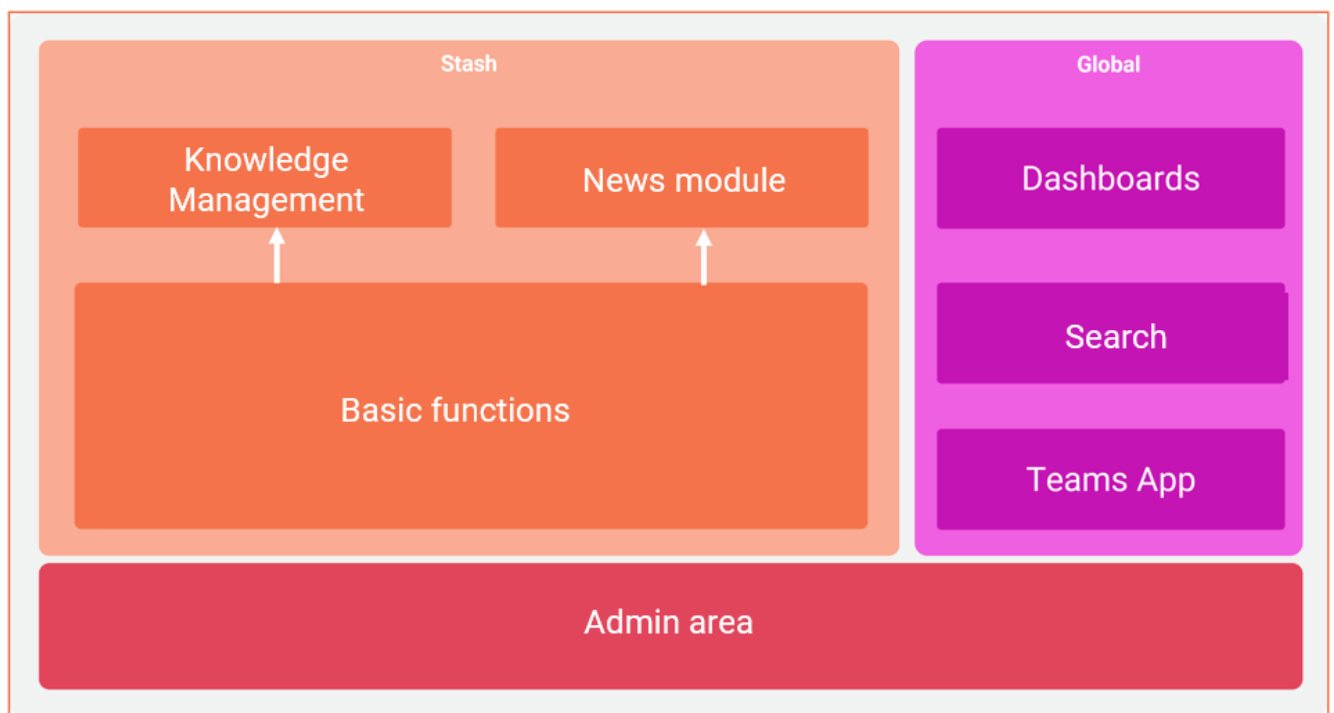
<b>1. Introduction</b>	<b>3</b>
1.1 Components Of SmartStash Cloud Services	3
1.2 SmartStash – System Requirements	5
1.3 SmartStash – Plans	5
<b>2. Data Processing Agreement</b>	<b>6</b>
<b>3. Service Provider</b>	<b>6</b>
<b>4. SmartStash – Service Level Agreement</b>	<b>6</b>
4.1 General Provisions	6
4.2 Definition of Terms	7
4.3 Claims For Non-performed Service	7
4.4 Restrictions	8
4.5 Terms of Service	8
<b>5. SmartStash – Security Of Processing / Technical And Organizational Measures</b>	<b>9</b>
5.1 Ensuring Confidentiality	10
5.2 Ensuring Integrity	11
5.3 Ensuring Availability And Resilience	12
5.4 Periodic Review, Assessment And Evaluation Procedures	13
<b>6. SmartStash – Data Storage Location</b>	<b>13</b>
<b>7. SmartStash – Release Process</b>	<b>14</b>
<b>8. Limitations And Restrictions</b>	<b>15</b>

# 1. Introduction

This document describes the SmartStash Cloud services and deliverables. SmartStash is a subscription service that ensures the most up-to-date services are always available. Software maintenance is included with an active SmartStash subscription, so the latest version of SmartStash is always available. This significantly reduces the effort involved in operating and maintaining the SmartStash platform.

## 1.1 Components Of SmartStash Cloud Services

The SmartStash cloud services are based on a central business logic management in Microsoft Azure and a number of functional building blocks that are based on SharePoint Online as an enterprise content management system. All of the content resides in SharePoint Online. The central business logic controls processes, notifications and the admin center from Azure



### Basic Functions | Knowledge Management

SmartStash is structured based on stashes. Each stash forms a container with any amount of content and its own configurations and permissions. Any number of these stashes can be added to SmartStash in a tenant.

The basic functions for knowledge management include the possibility of filing, centrally controlled structuring and control of information in the form of documents and SharePoint websites. Automatic processes enable simplified management of this information. Various designs and entry points into a stash can be configured.

### **Basic Functions | News**

As an additional use case, functions from knowledge management - such as steering and read confirmations - can also be extended to include news. There is the option of setting up a special stash type for this. News receive a special news archive view that is sorted chronologically in descending order. A configurable archive function ensures that outdated news is no longer displayed and can only be found in the search.

### **Global Functions| Dashboards**

Global dashboards are offered across stashes that serve different purposes. The personal dashboard "MyStash" with the target group "End-User" shows all posts that a user has to confirm as read or has favorited himself.

The release center clearly displays all open tasks for editors and releasers and enables them to be completed.

Various overview pages for the stashes and their content are enabled in global content dashboards. Content can be aggregated in different structures and offered to an end user.

### **Search**

A dedicated search platform for SmartStash content makes it possible to quickly search the knowledge database and filter for all stored metadata ("tags").

### **Teams App**

The SmartStash Teams app allows you to get notifications in Teams when there's something new to read or do. It provides access to personal dashboard, sharing center, global search and stashes. It is possible to store the teams app as a private app in teams or add it to a team as a tab to display content.

### **Admin area**

SmartStash's central admin area makes it possible to carry out all important configurations from one place. This includes granting access rights and licenses, configuration of tags, views, notifications and processes such as reminders and approvals. Many functions can be configured here or disabled stash-wise if required.

The SmartStash cloud services are hosted by Fellowmind Germany GmbH in the Microsoft Azure Cloud. Access is via the SmartStash SharePoint Add-In in the client's tenant and via the SmartStash Admin Center hosted centrally by Fellowmind Germany in Azure.

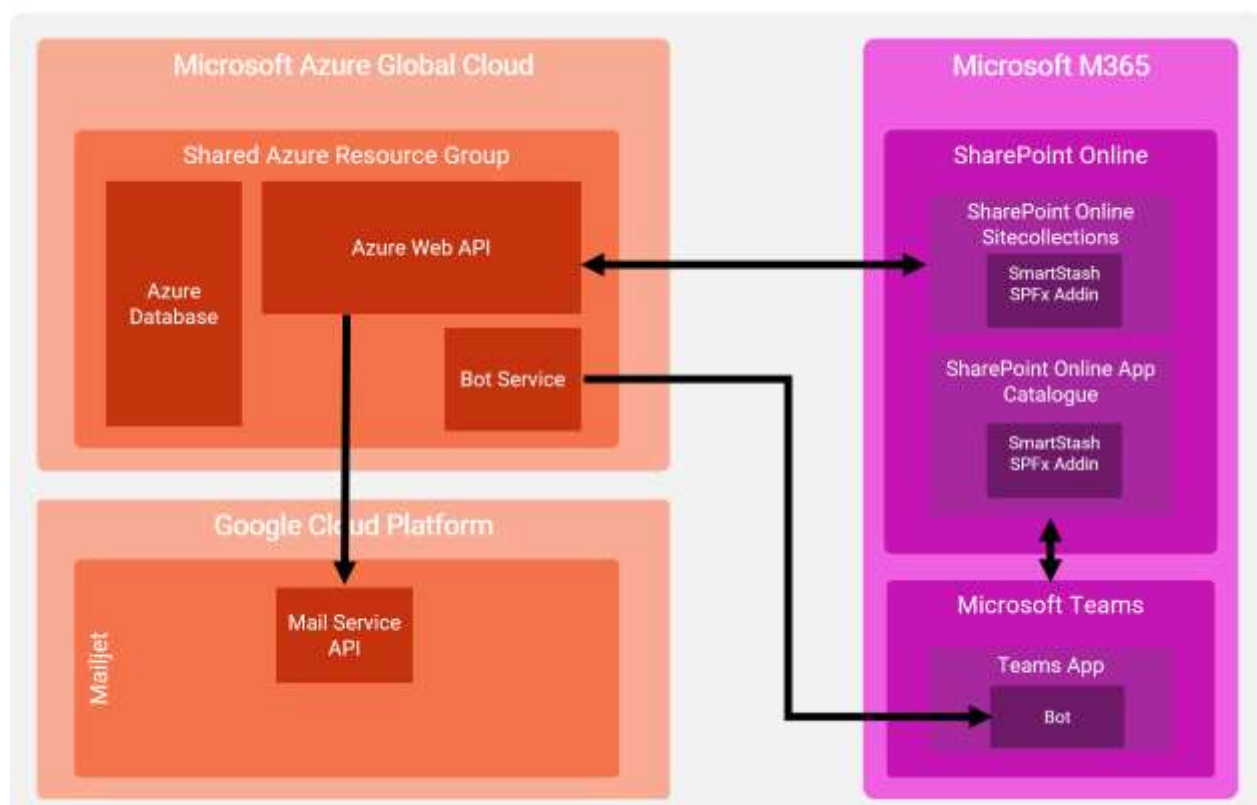
The SmartStash cloud services are hosted by Fellowmind Germany GmbH in the Microsoft Azure Cloud. Access is via the SmartStash SharePoint Add-In in the client's tenant and via the SmartStash Admin Center hosted centrally by Fellowmind Germany in Azure.

## 1.2 SmartStash – System Requirements

SmartStash is offered for Microsoft SharePoint Online and Microsoft Teams and thus implements a Microsoft Office 365 plan that includes Microsoft SharePoint Online and Microsoft Teams (<https://products.office.com/de/de/business/compare-office-365-for-business-plans>), ahead. The contractual conditions between Microsoft and the client apply here.

## 1.3 SmartStash – Plans

SmartStash is currently offered in one variant or plan. A SmartStash subscription shares a Microsoft Azure cloud infrastructure environment with multiple clients. Access is via the customer's Microsoft M365 environment through the installed SmartStash SPFx Addin. All emails generated in SmartStash are sent via the Mailjet service. The client is responsible for the Microsoft M365 environment on the customer side and is not part of the SmartStash operation.



## 2. Data Processing Agreement

The version of the “Contract of Data Processing Agreement according to Art. 28 Para. 3 GDPR” of Fellowmind Germany GmbH that is valid at the time the subscription is taken out or extended applies.

## 3. Service Provider

To provide the SmartStash Cloud Services, we work with a selection of contractors who are bound by security and privacy policies. Access to the stored data is only if this is necessary for the provision or maintenance of the services. The list below contains all current contractual partners of Fellowmind Germany GmbH who support the provision and maintenance of the SmartStash cloud services.

Company of the contractual Partner	Registered Office	Function
Microsoft Ireland operations Ltd.	Dublin, Ireland	Microsoft Services. Azure Platform
Mailjet GmbH	Berlin, Germany	E-Mail Dispatch

Between Fellowmind Germany GmbH and Microsoft Ireland Operations Ltd. the EU Standard Contractual Clauses, which are available to all cloud customers in the Online Services Terms of Use, apply.

The list of contractors does not apply to the SmartStash Cloud Services that are in preview, preview, or beta status.

## 4. SmartStash – Service Level Agreement

### 4.1 General Provisions

Fellowmind Germany GmbH grants its clients a service level for the use of the SmartStash cloud services. This Service Level Agreement for the SmartStash Cloud Services is made in connection with a SmartStash Subscription Agreement.

In the unlikely event that Fellowmind Germany GmbH is unable to maintain the service level for the SmartStash Cloud Services as described below, a portion of the monthly service fees may be credited. The service regulations are defined in Chapter 4.5.

Changes to the Service Level Agreement will not apply until the subscription contract is renewed. The version of the Service Level Agreement that is current at the time of renewal will apply throughout the renewal term.

## 4.2 Definition of Terms

Term	Definition
<b>Applicable monthly period</b>	Is related to a calendar month in which Fellowmind Germany GmbH owes a service credit, the number of days that you subscribe to a service.
<b>Applicable monthly Service Fee</b>	Are the fees actually paid by you for the provision of the SmartStash Cloud Services and applied to the month in which a Service Credit is owed.
<b>Downtime</b>	Are defined in the Service Terms below. Downtime does not include scheduled downtime. Downtime does not include unavailability of a Service due to the limitations described below and in the Terms of Service.
<b>Incident</b>	I seither a single event or a group of events that result in downtime.
<b>Planned Downtime</b>	Means downtime related to network, hardware or service maintenance or upgrades. We will post or announce these times as Downtime at least five (5) days in advance.
<b>Service credit</b>	Is the percentage of the applicable monthly service fee that will be credited after approval of the claim by Fellowmind Germany GmbH.
<b>Service Level</b>	Represents a measurable quantity of a service to which Fellowmind Germany GmbH is committed.
<b>User Minutes</b>	Is the total number of minutes in a month, minus any scheduled downtime, multiplied by the total number of users.

## 4.3 Claims For Non-performed Service

In order for claims to be considered, each claim must go through customer support ( [support@fellowmind.de](mailto:support@fellowmind.de) ) to Fellowmind Germany GmbH so that we can verify the claim. The following information must be transmitted:

1. Detailed description of the incident
2. Information on the time and duration of the failure
3. Number of affected users

4. Description of your attempts to resolve the incident after it occurred

## 4.4 Restrictions

The Service Level Agreement does not apply to performance and availability issues...

1. due to force majeure (e.g. natural disasters, wars, terrorist attacks, riots, government measures)
2. due to network and equipment failures at your location or between your location and the data centers hosting the SmartStash Cloud Services
3. due to insufficient bandwidth or the use of third-party hardware, software and services not provided by Fellowmind Germany GmbH
4. Restrictions on Microsoft Services...
5. Occurred during a preview, pre-release, trial, or beta release of any service or feature
6. caused by unauthorized action by your employees, agents, contractors or suppliers
7. caused by a failure to perform a required action by your employees, agents, contractors or suppliers
8. caused by other people using your passwords or devices to gain access to our network and services
9. that are incompatible with the features and functionality as a result of your use of the Services, such as by attempting to perform unsupported operations or comply with required configuration
10. resulting from incorrect entries or incorrect use
11. arising from operations leading to the exceeding of quotas, limits and restrictions
12. which result from the throttling on our part based on the assumption of abusive behavior

## 4.5 Terms of Service

The downtime for the SmartStash cloud services is the period when a core component such as knowledge management, news, dashboards or the admin area is not available.

Monthly Uptime Percentage is calculated using the formula below:

$$\frac{\text{User minutes} - \text{Downtime}}{\text{User minutes}} \times 100$$

Downtime is measured in user minutes. For each month, the sum of the minutes of each incident is multiplied by the number of users affected.

The Service Credit amount is based on the percentage of Monthly Uptime that is undercut.

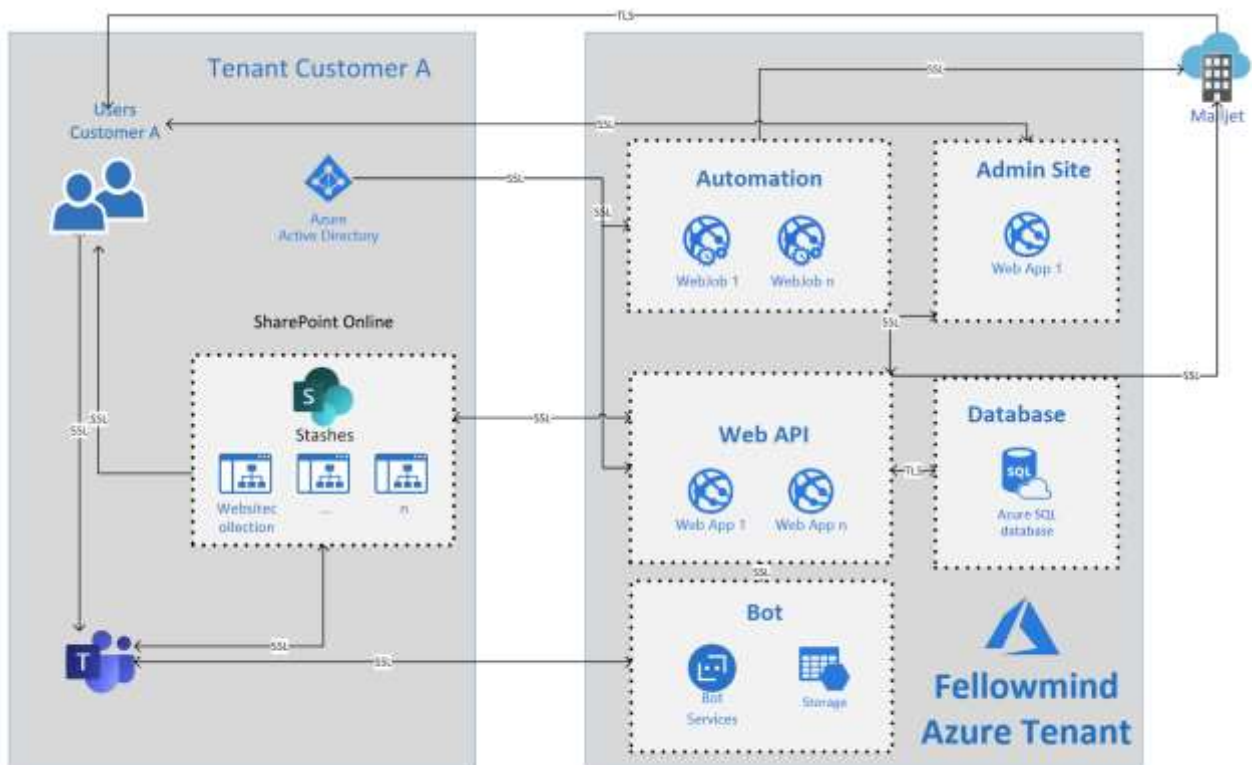


Percentage of monthly uptime	Service Credit
< 95%	25%
< 90%	50%
< 80%	100%

## 5. SmartStash – Security Of Processing / Technical And Organizational Measures

Fellowmind Germany GmbH made a conscious decision to host the SmartStash cloud services in the Microsoft Azure Cloud. With the Azure Cloud, Microsoft follows more than 70 national and international standards and compliance offers. These include ISO 9001, ISO 27001, ISO 27017 and ISO 27018. A complete list can be found on the following website: <https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>.

The figure below shows the architecture of all components and the communication paths between them



The following sections describe how the SmartStash cloud services in connection with the Microsoft Azure Cloud meet the data protection requirements.

# 5.1 Ensuring Confidentiality

## 5.1.1 PASS CONTROL

The SmartStash cloud services run based on "Infrastructure as a Service" (IaaS) in a Microsoft Azure data center. Microsoft describes the extent and manner of access control in the Online Services Terms, which can be found at <https://www.microsoft.com/en-us/licensing/product-licensing/products>. Measures for physical security and measures for the security of the environment, including physical access to facilities and physical access to components, are described in detail in this document.

Fellowmind Germany GmbH also restricts access to the IaaS services in which customer information and data are processed to designated authorized persons. An authorization concept that follows the principle of least authorization is used for this. As a result, Fellowmind Germany GmbH restricts access to the IaaS services to those people who need this access to carry out their professional activities in accordance with their job description. In addition, Fellowmind Germany GmbH keeps records of the employees who are authorized to access the IaaS services in which customer information and data are processed and automatically deactivates login data that has not been used for a period of more than 6 months. These employees of Fellowmind Germany GmbH always have personalized, individual identifiers and login data.

## 5.1.2 ACCESS CONTROL

Access to the SmartStash Cloud Services is limited to subscriptions. Use of the SmartStash Cloud Services is legitimized via the SmartStash Web API. Installing and registering the SmartStash app application registration establishes the connection between the Microsoft SharePoint Online customer environment and the SmartStash cloud services. Furthermore, the communication paths ("server to server" and "client to server") are operated by SSL-encrypted connections and unauthorized reading of the data during transmission is prevented.

## 5.1.3 ANNONIMIZATION AND PSEUDOMIZATION

There is no dedicated setup of the infrastructure environment for each client. The company or the designation of the customer is not used in the infrastructure environment. This means that no immediate or direct reference to the client can be made.

## 5.1.4 DATA PORTABILITY

A SmartStash-based business application is configured in Microsoft Office 365 mandates or in the client's Microsoft SharePoint Online system and in the central SmartStash cloud service. The configuration data is stored in the contractor's central SmartStash database. The SmartStash content remains in the customer's Microsoft SharePoint Online system. All items and documents managed with the SmartStash-based business application remain in the Office 365 customer environment at all times. The storage takes place in standard Microsoft SharePoint Online lists and libraries. This data can be exported and transferred at any time using standard mechanisms such as MS Excel export, access via WebDAV or OneDrive. This business data is not copied, synchronized or moved to the storage of the SmartStash Cloud Services for permanent or persistent storage. The processing may necessitate a temporary transfer of the data, information and documents to the RAM memory of the SmartStash cloud services. However, these are not kept there permanently and are deleted after 24 hours at the latest. SmartStash-specific metadata necessary for operation is stored in the SmartStash cloud service database.

## 5.2 Ensuring Integrity

### 5.2.1 DATA CARRIER CONTROL

The Microsoft Azure IaaS services on which the SmartStash cloud services run offer various mechanisms to prevent unauthorized reading, copying, changing and deleting of data carriers. About a comprehensive roles and rights concept, access to the data carrier is restricted to named authorized persons. Furthermore, all data carriers used to process customer data are encrypted in order to achieve the necessary level of protection.

### 5.2.2 INPUT CONTROL

With the help of multiple protocol mechanisms, it can be monitored and traced whether and which personal data processed with the SmartStash cloud services has been entered or changed. The possibilities of the Microsoft SharePoint Online platform also play a key role here, which ensures input control through versioning and the monitoring log reports.

### 5.2.3 MEMORY CONTROL

The customer data, which may be processed with the SmartStash cloud services, is stored in a so-called Microsoft SQL Server database. Access to this database is limited to administrative accounts and so-called service accounts, which are secured with complex passwords, in order to efficiently prevent unauthorized entries, unauthorized knowledge, changes and deletions of customer data. Furthermore, what is known as audit logging takes place at the SQL Server level in order to log database events that provide information about database activity, discrepancies and anomalies. In addition, all databases used by the SmartStash cloud services are encrypted using TDA (Transparent Data Encryption) to achieve the necessary level of protection. Details can be found at the following links: <https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15>

### 5.2.4 USER CONTROL

The customer data, which may be processed with the SmartStash cloud services, is stored in a so-called Microsoft SQL Server database. Access to this database is limited to administrative accounts and so-called service accounts, which are secured with complex passwords, in order to efficiently prevent unauthorized entries, unauthorized knowledge, changes and deletions of customer data. Furthermore, what is known as audit logging takes place at the SQL Server level in order to log database events that provide information about database activity, discrepancies and anomalies. In addition, all databases used by the SmartStash cloud services are encrypted using TDA (Transparent Data Encryption) to achieve the necessary level of protection. Details can be found at the following links: <https://docs.microsoft.com/de-de/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver15>

### 5.2.5 TRANSFER CONTROL

Fellowmind Germany GmbH uses various Microsoft Azure IaaS services and their configuration options in a targeted manner to encrypt data, limit access, detect and ward off attacks on the environment and to continuously monitor the status of the

anti-malware protection of the components. Monitoring is semi-automatic based on the Azure Security Center and is carried out by the Development & Operations Team at Fellowmind Germany GmbH.

#### **5.2.6 TRANSPORT CONTROL**

If it is necessary to transport data carriers containing customer data or personal data, this is always done with the proviso that the confidentiality and integrity of the data is protected. All technical and organizational measures are taken to ensure this. The transmission of customer data or personal data processed by the SmartStash cloud services is always carried out over encrypted connections to ensure confidentiality.

## **5.3 Ensuring Availability And Resilience**

#### **5.3.1 RECOVERABILITY**

The SmartStash cloud services are backed up regularly and their operability is continuously monitored to ensure recovery in the event of a failure.

#### **5.3.2 RELIABILITY**

Fellowmind Germany GmbH offers customer support so that malfunctions can be reported quickly and easily. Furthermore, the availability of the SmartStash services is continuously monitored by the Development & Operations team at Fellowmind Germany GmbH.

#### **5.3.3 DELETION OF DATA**

If the SmartStash subscription is canceled, when using a shared infrastructure (SmartStash "shared"), the customer's data records are irretrievably deleted no later than 30 days after the termination has taken effect. In principle, log entries created during operation to monitor performance, operability and freedom from errors are deleted 30 days after creation.

#### **5.3.4 DATA SECURITY**

When setting up and operating the SmartStash cloud services, Fellowmind Germany GmbH ensures compliance with standards and laws such as the General Data Protection Regulation (GDPR) and the BDSG in order to protect data and information.

All communication channels, such as communication between the end user and the SmartStash cloud services, communication between the SmartStash cloud services and the storage systems used or communication between the data centers, take place via an SSL-secured connection.

To protect the databases, backups and logs, encryption is done via TDE (Transparent Data Encryption). Details on encryption using TDE can be found on the following website. <https://docs.microsoft.com/de-de/azure/azure-sql/database/transparent-data-encryption-tde-overview?view=sql-server-ver15&tabs=azure-portal>



## 5.4 Periodic Review, Assessment And Evaluation Procedures

### 5.4.1 PRIVACY MANAGEMENT

Mitarbeiter Employees of Fellowmind Germany GmbH with access to personal data are subject to confidentiality obligations. Furthermore, Fellowmind Germany GmbH provides information about relevant security procedures, the respective tasks and possible consequences in the event of a violation of security regulations and procedures. As part of a continuous improvement process, the technical and organizational measures are regularly checked with regard to their effectiveness, topicality and possible optimization possibilities. This self-monitoring takes place regularly in the form of the data protection officer of Fellowmind Germany GmbH.

### 5.4.2 AUFTRAGSKONTROLLE

The service providers named in section 3 are carefully selected by Fellowmind Germany GmbH and committed to data secrecy. For this purpose, there are corresponding written agreements on order data processing or approved EU standard contractual clauses in the corresponding contracts between the contracting parties.

### 5.4.3 REPORTING OBLIGATION

The SmartStash cloud services are continuously monitored for operability and security. The monitoring includes attacks and threats of multiple kinds. In the unlikely event of a breach of personal data (security incident), the data protection officer at Fellowmind Germany GmbH will report this to the responsible supervisory authority within 72 hours. Furthermore, Fellowmind Germany GmbH will investigate the security incident, provide the client concerned with detailed information on the security incident and take measures to mitigate the effects

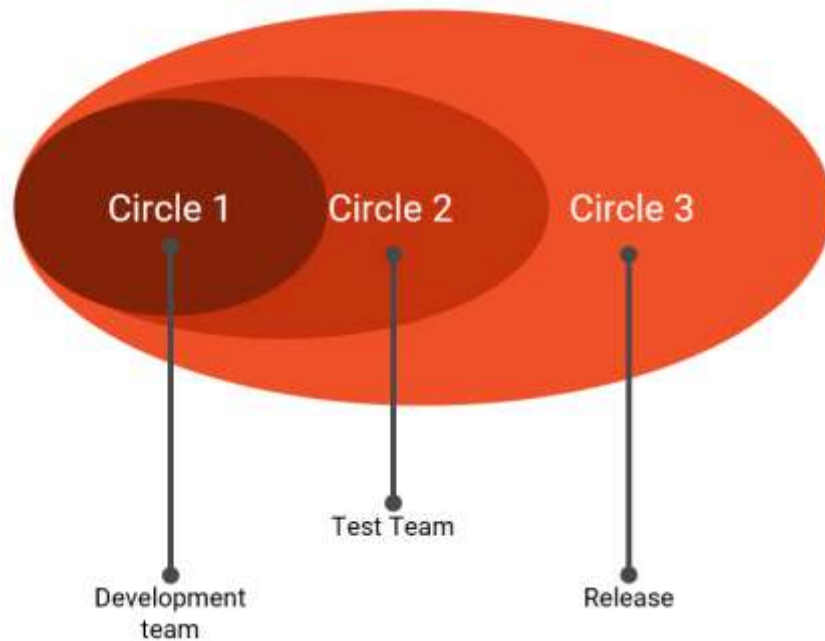
## 6. SmartStash – Data Storage Location

The SmartStash Cloud services are currently hosted in the Microsoft Azure Global Cloud in the "West Europe" data center. These can be used by Microsoft customers who rely on Office 365 from the "West Europe" data center.



## 7. SmartStash – Release Process

The SmartStash cloud services are continuously developed and optimized. Fellowmind Germany GmbH will inform you at least 30 days before an update of the services if an administrator of the client has to take action to ensure the operability after the update. Most updates to the SmartStash Cloud Services do not require action by Customer's administrators. New features and updates go through 3 so-called release circles until they are generally available



Circle 1 – The development team tests the new feature or update using predefined and automated tests.

Circle 2 - The SmartStash Test Team tests and uses the new features in SmartStash to verify general usability.

Circle 3 - The new feature will be rolled out to all SmartStash environments.


## 8. Limitations And Restrictions

In diesem Abschnitt werden die SmartStash Grenzwerte beschrieben. Die Grenzen und Beschränkungen stellen die im Abschnitt „Dienst-Bestimmungen“ zugesicherte Betriebszeit sicher. Die Softwarebeschränkungen werden pro Modul definiert und in folgende Typen unterschieden:

**Limitation** - This is a static limit that cannot be changed

**Threshold** - This is a configurable limit that can be adjusted to meet requirements

**Supported** - This is a configurable limit set to a tested value and can be adjusted.



Module	Limit	Max. Value	Limit Type	Note
<b>Basic Functions</b>	Generation of read receipt requests	1h	Limitation	Email delivery or MS Teams notifications of read receipt requests
<b>Admin-Area</b>	License Job	1h	Limitation	Licensing after adding a user in AD groups
<b>News Module</b>	Archiving Job per Stash	1-1.000/day	Threshold	Automatical archiving of news articles
<b>Basic Functions</b>	Reminder Job per Stash or Article	1-1.000/day	Threshold	Reminder of missed read receipts conditions