Product Description
d.velop cmis services for SAP Solutions

1 Summary

Supplementary to the "Product Description d.velop cloud platform," this document describes the product-specific functions of d.velop cmis services for SAP Solutions. Services relating to support, availability and updates for d.velop cmis services for SAP Solutions are described in the "Service Level Agreement".

2 Licensing

By purchasing d.velop cmis services for SAP Solutions, you receive the following quantity-related usage right:

- License metric: productive SAP instance (SaaS service)
- Quantity: 1

3 Scope of Functions

d.velop cmis services for SAP Solutions is a web-based application (app) that is operated/hosted via the basic d.velop cloud platform app. d.velop cmis services for SAP Solutions enables the customer to connect its SAP systems to d.velop documents via the SAP CMIS interface. The functions available to the customer have been tested for proper storage and display of documents as part of the interface certification process required by SAP (S/4-BTP-CMIS 1.0).

In order to connect the SAP cloud systems to the respective d.velop cloud tenant, the customer must have implemented the SAP Business Technology Platform (BTP) with the Document Management Service, Integration Option.

The SAP BTP with the Document Management Service, Integration Option is also required to connect the SAP on-premises systems to the respective d.velop Cloud tenant. In addition, the SAP Cloud Connector is required in order to connect the on-premises SAP systems. The customer is obliged to obtain the aforementioned software directly from SAP SE and implement it on its systems.

4 Administration

4.1 Backup and Disaster Recovery

d.velop carries out regular backups of the content of the d.velop cmis services for SAP Solutions app.

- Backups are created at least once a day, depending on technical capabilities. The recovery point objective (RPO) is 24 hours.
- Backups are retained for 30 days.
- Disaster recovery tests are performed twice per year.

Data stores containing persistent data are backed up by snapshot and stored redundantly in several data centers. The document-oriented database and associated transaction logs are also backed up by snapshot and can be restored to a customer-requested point in time (RPO).

4.2 Temporary Files / SAP Draft Versions

When processing documents in SAP, e.g. SAP DMS (Fiori apps document management system), the data is not stored in an audit-proof manner during processing (draft). By saving the draft version in S/4HANA Cloud, public edition, or releasing the document, the documents are then transferred to d.velop documents in an audit-proof manner. d.velop AG assumes no responsibility for documents that are kept in draft status for more than 30 days and have not been released in the meantime. Furthermore, d.velop AG reserves the

option to delete such documents following a retention period of 30 days or to transfer them to a forced release.

In the event of data loss, documents in a draft version cannot be recovered. Due to the SaaS architecture, d.velop cmis services for SAP Solutions cannot inform the connected SAP systems about the loss of data, meaning that document links in SAP have to be cleaned up manually by the customer.

5 Information Security

Data security in d.velop cmis services for SAP ERP is ensured through a series of technical and organizational measures.

5.1 Data Location

d.velop cmis services for SAP ERP is provided in data centers with locations in Germany and Western Europe. Our partner's data centers are certified according to the following guidelines, among others, and can be viewed at https://open-telekom-cloud.com/en/security/data-protection-and-compliance:

- ISO/IEC 27017
- ISO/IEC 27001
- ISO/IEC 27018ISO 9001
- ISO 14001
- ISO/IEC 20000-1
- ISO 22301
- SOC 1
- SOC 2
- SOC 3

5.2 Encryption of Content (Data at Rest)

All data and content that is stored and processed by the basic d.velop cloud platform apps is stored in encrypted form and according to the current industry standard. This applies to content provided by the customer, meta data for the content, as well as content created or derived for the purpose of providing the service (e.g. full text information, preview graphics). Separate keys are used to encrypt the data in different storage media (databases, hard drives). An access log records access to the keys.

d.velop reserves the right to regularly reassess this in accordance with the current recommendations of the Federal Office for Information Security, and to make any necessary adjustments.

5.3 Tenant Isolation

The data of different tenants is strictly separated in d.velop cloud. A leading tenant ID is used for this purpose. This is used by the interface to select the correct virtual tenant in the data store.

5.4 Access Logging

Successful and failed administrative access attempts to cloud systems are permanently logged.

5.5 Authentication

Through the client structure, we rely on the authentication methods of the connected platforms (d.velop documents and SAP S/4HANA Cloud)