Product Description
d.velop connect for CMIS

1 Summary

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

2 Licensing

By purchasing d.velop connect for CMIS, you receive the following quantity-specific usage right:

- License metric: per live cloud instance (SaaS service)
- Quantity: 1

3 Scope of functions

d.velop connect for CMIS is a web-based application (app) that is operated/hosted via the basic d.velop cloud platform app. CMIS is an open, manufacturer-independent standard for communication with document management systems (DMS) and defines a number of possible functions that can be implemented/supported by DMS manufacturers. d.velop connect for CMIS enables the customer to connect its application to d.velop documents via the CMIS interface. d.velop connect for CMIS consists mainly of functions for working with documents and dossiers (Create, Read, Update, Delete). The exact range of functions can be found in the documentation for d.velop connect for CMIS in the d.velop service portal.

4 Administration

4.1 Backup and disaster recovery

d.velop carries out regular backups of the contents (configuration) of the d.velop connect for CMIS 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. After this period they are deleted.
- 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).

5 Information Security

Data security in d.velop connect for CMIS is ensured through a series of technical and organizational measures.

5.1 Data location

d.velop connect for CMIS 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, d.velop relies on the authentication methods of the connected platforms (d.velop documents).