Product Description
d.velop cloud platform

1 Overview

In addition to this "Product Description d.velop cloud platform", the functionalities of the software acquired by the Customer are described in the product-specific product descriptions.

The services support, availability and updating of the d.velop cloud platform are described in the "Service Level Agreement Cloud and SaaS".

1.1 Scope of Functions of the d.velop cloud Platform

The d.velop cloud platform enables customers to purchase and use IT resources and applications by accessing them via the Internet. A separate, secured cloud area (hereinafter referred to as "d.velop cloud tenant" or "tenant" for short) is created for each customer, in which functional applications (hereinafter referred to as "apps") can be purchased. The functions offered by the individual apps are determined by the respective app provider and listed in the product description of the individual apps. When created, a tenant already contains some basic apps that are available in every tenant, which are described in this product description (see 1.2 "d.velop cloud platform basic apps").

An app is a functionally and technically self-contained part of the overall system and has no or as few dependencies as possible to other apps. If multiple apps are integrated, this is usually done using links. Examples:

- The task app is responsible for managing tasks, which users can edit and forward. If a task includes documents, for example, they are only linked to the task.
- The user management app is responsible for managing users and groups.
- The identity provider app is responsible for authenticating users. It is not responsible for authorization within the app.

Authorization, i.e. the provision of access to certain business objects, is not part of the identity provider; rather, it is controlled by the individual functional apps. We use OpenID Connect to authenticate users, which means that the user's login credentials remain under the control of the OpenID provider.

1.2 d.velop cloud Platform Basic Apps

The d.velop cloud platform is provided with the following basic apps and their scope of functions:

- home app
  - Your d.velop cloud homepage
  - Lists the functions of the purchased apps that are available to the current user
- config app
  - Lists the configuration options for the purchased apps
- shell app
  - Shared layout and navigation elements
- task app
  - Send tasks to users and groups

- d.velop cloud center
  - Manage d.velop cloud tenants
  - Purchase and cancel apps
- d.velop cloud login
  - Authenticate users
- identity provider app
  - Integrate the d.velop cloud with identity systems such as d.velop cloud login or Active Directory
- user management app
  - Manage users and group assignments
- userprofile app
  - User absence management
- notification app
  - Sends e-mail notifications to users
- process app
  - Provides technical functions for execution, monitoring and administration of simple BPMN processes.
- connect for integration platform app
  - Provides services to interact with integration platforms such as Microsoft PowerAutomate. For example, to accept receipts and to hand them over for further storage in your d.velop documents.
- openID provider app
  - Provides services to integrate the d.velop cloud as a login service with OpenID-Connect.
- theming app
  - Centralized design management

1.3 Integration Options

Integration in Your Application

You can integrate content from the d.velop cloud into your application using parameterized calls. For example, you can use HTTPS to display a document in an iFrame in your application.

Documentation with examples can be found at https://developer.d-velop.de/

Integrated Authentication

The identity provider app enables central authentication of users. Users can use their d.velop cloud login credentials for authentication. You also have the option of

establishing a trust relationship to external identity systems via OpenID Connect. This makes it possible for users to log in via their leading system, such as Salesforce or On-Premises Active Directory.

Integration via APIs

The d.velop cloud apps provide APIs for integrating your system with the d.velop cloud.

Documentation with examples can be found at https://developer.d-velop.de/.

1.4 Rights to Content

You grant us a simple right of use for all content imported or created by you or your employees in the d.velop cloud, limited in time and place to the purpose of operating the cloud. All rights of exploitation, modification, etc. remain with you for as long as you hold them.

2 Administration

2.1 Backup and Disaster Recovery

d.velop regularly backs up the content of the d.velop cloud platform basic apps.

- 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.

Storage media on which persistent data is stored are backed up using snapshots and stored redundantly in multiple data centers. Likewise, relational databases and associated transaction logs are backed up using snapshots and can be recovered up to a point in time desired by the customer. For data already stored redundantly in object storage, the term backup does not refer to another copy of the data but rather to versioning mechanisms that allow the data to be restored after unintentional deletion. All backups are protected against inadvertent deletion by the implementation of multi-factor authentication. Depending on the preceding event, restoration is carried out either by d.velop or at the customer's request. The data is restored by activating the backup in parallel and then migrating the data to the production system. If the data loss was caused by the customer's actions, a fee will be charged for the recovery according to the service flat rate. The duration of the recovery depends on the scope of the event that occurred. The target is a recovery time objective (RTO) of 48 hours.

2.2 Deletion of Data

Data is deleted at the customer's request (text form is sufficient) or after the appropriate period of time following a contract termination.

If the customer requested the deletion of their data, d.velop AG will retain the data for 30 days before it is finally and irretrievably deleted.

3 Information Security

The security of data in the d.velop cloud is ensured by a series of technical and organizational measures.

3.1 Data Location

d.velop cloud platform is operated by d.velop in Gescher as well as by the external IT service provider in the greater metropolitan area of Frankfurt am Main, Germany.

The external IT service provider’s data centers are certified according to the following guidelines, among others:

- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- C5

The content of the customer in the d.velop cloud platform basic apps is always stored only in Germany (exception: incoming e-mails can be processed app-specifically via other locations within the EU). If the customer use third-party apps, data may be temporarily or permanently transmitted to other locations. Additional information can be found in the product description of the apps.

3.2 Encryption of Content (Data at Rest)

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

Currently, stored data is encrypted using the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) with 256-bit encryption keys. d.velop reserves the right to reevaluate this regularly according to current recommendations of the Federal Office for Information Security and to adapt it if necessary.

3.3 Transport Encryption (Data in Transit)

Transport encryption according to current industry standards is used for communication between the application components. This is re-evaluated at regular intervals to ensure compliance with any new requirements and recommendations of the Federal Office for Safety in Information Technology. At the time this document was created, this means at least TLS version 1.2 for HTTPS connections. For other connections (depending on the application), either TLS or comparable transport encryption is used.

3.4 Tenant Isolation

The data of different tenants is strictly separated in our d.velop cloud. The data is separated based on a leading tenant ID. This ID is used by the d.velop cloud platform basic apps to identify the correct isolated storage location for the tenant within the apps' data storage.

3.5 App Isolation

Each app is strictly isolated from the other apps using technical means, meaning it is not possible for the apps to independently access data from other apps. If an app needs to access the data of another app, the data is accessed via HTTPS using defined interfaces while maintaining the authorizations of the user who called the request.

3.6 Access Logging

There is a permanent logging of successful and failed administrative access attempts to cloud systems.

3.7 Access control

During regular operation, the access to the data takes place exclusively via technical processes (for the purpose of data-in-use, e.g. provision of the documents or full-text search). d.velop employees work in the standard mode with authorizations that have no possibility to access the data. Only in case of error or failure, privileged authorizations are used, if necessary. In this case, access to the technical infrastructure takes place via a VPN dial-in and after strong authentication with a second factor. The login is provided by using the Segregation of Duties (SOD) principle, similar to a four-eyes principle. Due to the privileged access via the technical infrastructure potential access to customer data is possible.