Product Description
d.velop cloud platform

1 Summary

Supplementary to this Product Description, the functions of the software purchased by the customer are described in the product-specific product descriptions.

Services relating to support, availability and updates for the d.velop cloud platform are described in the "Service Level Agreement".

1.1 Scope of functions of d.velop cloud platform

The d.velop cloud platform offers customers the opportunity to purchase and use IT resources and applications on demand over the Internet. To enable the purchase of specialist applications (hereinafter referred to as "apps"), a separate, secure cloud area (hereinafter referred to as the "d.velop cloud tenant" or "tenant" for short) is created for each customer in which apps can be purchased. The functions offered by the individual apps are determined by the respective app provider and are listed in the product descriptions of the individual apps. Regardless of what other apps are purchased, once created a tenant already contains certain basic apps that are available in every tenant and that are the subject of this product description (see section 1.2 "d.velop cloud platform basic apps").

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

- The task app is responsible for managing tasks, which users can process and forward. If there are documents which belong to a task, for example, the app merely links to these documents.
- 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 apps.

Authorisation, i.e. allowing access to specific business objects, is not part of the identity provider but rather is the responsibility of the individual specialist apps. We use OpenID Connect to authenticate users, which means that the user's credentials remain under the control of the OpenID provider.

1.2 d.velop cloud platform basic apps

The d.velop cloud platform contains the apps listed below and their range of functions, which are provided as a basis, according to the edition:

d.velop cloud plattform Basis	d.velop cloud plattform Basis T Cloud Public
• Home app (only for some existing customers) or dashboard app – The d.velop cloud home page – Lists available functions from the current user's purchased apps • Config app – Lists configuration options for the purchased apps	• Dashboard app – The d.velop cloud home page – Lists available functions from the current user's purchased apps • Config app – Lists configuration options for the purchased apps

• Shell app – Shared layout and navigation items • 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 – Authenticates users • Identity provider app – Integrates d.velop cloud with identity systems such as d.velop cloud login or Active Directory • User management app – Manage users and group assignments • User profile app – Manage absences • Notification app – Send e-mail notifications to users • Process app – Provides technical functions for executing, monitoring and administering simple BPMN processes • Document Intelligence Hub (DIH) – Interface for connecting AI-based services for automated document recognition. This app is only an interface. The specific AI services are provided separately and only at the customer's express direction. • OpenID provider app – Provides services for integrating d.velop cloud with OpenID Connect as the login service • Theming app – Centrally manage designs • Billing App and Consumption Tracker – Collection of billing-relevant data for processing within the d.velop billing systems	• Shell app – Shared layout and navigation items • 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 – Authenticates users • Identity provider app – Integrates d.velop cloud with identity systems such as d.velop cloud login or Active Directory • User management app – Manage users and group assignments • User profile app – Manage absences • Messaging app – Send e-mail notifications to users • Process app – Provides technical functions for executing, monitoring and administering simple BPMN processes • Document Intelligence Hub (DIH) – Interface for connecting AI-based services for automated document recognition. This app is only an interface. The specific AI services are provided separately and only at the customer's express direction. • OpenID provider app – Provides services for integrating d.velop cloud with OpenID Connect as the login service • Theming app – Centrally manage designs • Billing App and Consumption Tracker – Collection of billing-relevant data for processing within the d.velop billing systems

• Comissioning – Manages provisioning of platform components based on assigned entitlements • d.velop audit trail – Logging of security-related events	– The apps are also executed at Amazon Web Services in the edition T Cloud Public • Comissioning – Manages provisioning of platform components based on assigned entitlements • d.velop audit trail – Logging of security-related events

1.3 Integration

Integration into your application

The customer can use parameterized calls to integrate content from the d.velop cloud into their application. For example, the customer can display a document via HTTPS in an iFrame in their application.

Documentation with examples is available to the customer at https://help.d-velop.de/.

Integrated authentication

The identity provider app handles the centralized authentication of users. The d.velop cloud login credentials can be used to log in. The customer also has the option to establish a trust relationship with external identity systems via OpenID Connect. This enables the customer to log in from their leading system, such as Salesforce or an on-premises Active Directory.

Integration via APIs

The d.velop cloud apps provide APIs that the customer can use to integrate their system with d.velop cloud. The interfaces are accessed via HTTPs.

Documentation with examples is available to the customer at https://help.d-velop.de/.

1.4 Rights to content

The customer grants d.velop a simple right of use, limited in time and place to the purposes of operating the cloud, to all content imported or created by the customer or their employees in the d.velop cloud. All rights of utilization, modification, etc. remain with the customer, provided the customer holds these in the first place.

2 Administration

2.1 Backup and disaster recovery

d.velop performs regular backups of the contents 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.
- Backups are stored in encrypted form

Data stores containing persistent data are backed up by snapshot and stored redundantly in several data centers. Relational databases and associated transaction logs are also backed up by snapshot and can be restored to a customer-requested point in time. For data stored redundantly in object storage, the term

'backup' does not refer to a further copy of the data, but rather to versioning mechanisms that enable the data to be restored after unintentional deletion. All backups are protected against unintentional deletion through the implementation of multi-factor authentication. Depending on the precipitating event, the data is restored either by d.velop or at the request of the customer. The data is restored by activating the backup in parallel and then migrating the data to the live system. In the event of data loss caused by the customer's actions, recovery will be billed at the flat-rate service fee. The time required for recovery depends on the extent of the event that has occurred. The recovery time objective (RTO) is 48 hours.

2.2 Deletion of data

The deletion of the data will be carried out in accordance with the customer's instructions or after the legal basis for their storage has ceased to apply. In both cases, d.velop will store the data for another 90 days before it is permanently and irreversibly 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 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.

Currently, the Advanced Encryption Standard (AES) is used for encryption in Galois/Counter Mode (GCM) with 256-bit encryption 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.

To protect against malware, d.velop recommends providing all end devices of the customer with an endpoint protection solution to protect against malware in order to guarantee secure operation. The responsibility for access control and identity management lies with the customer. d.velop recommends the use of the provided Single Sign On (SSO) mechanisms.

3.2 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.

3.3 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 d.velop cloud platform basic apps to select the correct, isolated memory belonging to their tenant in the data storage system.

3.4 App isolation

Each app is strictly isolated from other apps on a technical level so that it is not possible for the apps to unilaterally access data from other apps. If an app needs to access the data of another app, this takes place via defined interfaces over HTTPS in accordance with the authorizations of the calling user.

3.5 Logging of security-related events

Security-related events are logged to ensure security, traceability and the detection of misuse.

These include, amongst others:

- Logging of read and write access (documents, files)
- Authentication processes (logins, failed attempts, logouts)
- Changes to user and role management
- Password changes
- Configuration changes (logging, restriction sets, retention periods)
- Creation/deletion of API key

The retention period for logged events is 180 days.

3.6 Access control

In regular operation, data is accessed exclusively via technical processes (for data-in-use purposes, e.g. provision of documents or full-text search). By default, d.velop employees have permissions that do not allow them to access the data. Privileged permissions are only used in the event of an error or failure. In such cases, the technical infrastructure is accessed via VPN after strict authentication with a second factor. The login is assigned via the segregation of duties (SOD) principle. Due to the resulting privileged access via the technical infrastructure, access to customer data is potentially possible. In regular operation, access to (the decrypted) data takes place exclusively through technical processes (data-in-use, e.g. provision of documents or full-text search). d.velop employees work with authorizations that have no possibility of accessing the decrypted data. Privileged authorizations are only used in the event of an error or failure. In this case, access to the technical infrastructure takes place via a VPN dial-in and after strong authentication with a second factor. The resulting privileged access via the technical infrastructure means that access to customer data may be possible.