Product Describtion
d.velop contracts for Microsoft 365

1 Brief Description of the Scope of Functions

Digital contract management with SharePoint and Microsoft 365. d.velop contracts for Microsoft 365 extends SharePoint with digital contract management capabilities that allow contract files to be created and managed.

2 General

d.velop contracts for Microsoft 365 is a SaaS application. The software is operated by d.velop as cloud software. All metadata and documents are stored in a Microsoft 365 SharePoint site belonging to the customer. The SharePoint site is located in the customer's Microsoft 365 tenant. Users work with the data via a provided application interface. The SharePoint site serves as the data repository.

The software is multi-tenant capable. Because it is cloud software, patches, updates, and new features are made available automatically.

The customer's Microsoft Entra ID is used for user sign-in. All communication with SharePoint is conducted via official SharePoint APIs and Microsoft Graph endpoints through Microsoft Entra enterprise applications in a user context. Using Microsoft Entra authentication makes its security and compliance features available. The SharePoint permission model also applies through the use of Microsoft Entra ID..

3 Purchased Scope of Functions

By purchasing d.velop contracts for Microsoft 365, the customer receives the corresponding right of use. The functions are divided into the following tiers::

Working with contract files	basic	business
Wizard for step-by-step creation of a contract file	●	●
Automatic extraction of properties from a contract document in the wizard *		●
Editing contract properties, including term information	●	●
Clause review of a contract document based on predefined review criteria *		●
Creating tasks (including notification function)	●	●
Extending the contract file with list-based data objects (e.g., risks, costs, notes)	●	●
Linking contracts to one another (e.g., for framework agreements)	●	●

* d.velop AI Credits must be purchased to use AI-based automatic property extraction and clause review.

Document management	basic	business
Document organization in contract files	●	●
Basic template mechanism (copying a template into the contract file)	●	●
Advanced template mechanism (copying the template and replacing placeholders)		●

Deadline calculation and notifications	basic	business
Option to automatically calculate the termination deadline and contract end date	●	●
If the termination deadline passes and the contract has not been terminated, the system calculates a new termination deadline based on the rules.	●	●
Termination deadline notification for responsible persons and additionally specified persons	●	●
Notification when a task is due or assigned	●	●
Notification when permissions or responsibility are assigned	●	●
Email content can be customized using available placeholders	●	●

Dashboard	basic	business
Quick search for contract files using a single search field	●	●
Tabular display of contracts and tasks (customizable across up to five tabs)	●	●
Fact sheet providing quick access to selected contract information	●	●
Display of search templates and navigation to Advanced Search	●	●
Pie chart showing contracts by contract status	●	●

Advanced Search	basic	business
Advanced search for contracts, documents, and tasks by filtering on various contract properties	●	●
Tabular display of search results with filtering options*	●	●
Export of search results as an Excel file*	●	●
Saving and retrieving search templates	●	●

* Up to 500 search results are displayed. Additional search results can be exported. The applicable limits are described in the documentation.

Berechtigungsregelwerk	basic	business
When a contract file is created or changed, the system can determine access rights (read or write access) and apply them to the entire contract file.	●	●
Definition of rules for applying permissions based on contract properties	●	●

Administration und Konfiguration	basic	business
Administration interface with links to relevant SharePoint pages	●	●
Creation of new contract types, including contract details	●	●
Creation of new document types, including document details	●	●
Customization of the interface with an individual color scheme and logo	●	●
Extending the contract file with list-based data objects (e.g., risks, costs, notes)	●	●

Integrationen	basic	business
Integration of contract management into Microsoft Teams		●
Signing documents with d.velop sign*	●	●
Signing documents with DocuSign**	●	●
Document automation with dox42***	●	●

* An additional d.velop sign license is required for use.

** In addition to a DocuSign account, integrating DocuSign requires purchasing the DocuSign interface from Paperless-Solutions GmbH.

*** dox42 can be configured in d.velop contracts for Microsoft 365. An additional license is required for use.

4 Information on Using AI Functions

4.1 Use of External AI Providers

LLMs are subject to ongoing development and are provided by external providers (hereinafter: AI Providers). Further information can be found in the data processing agreement, including its annexes. To provide the features described above, we transmit user input—in particular all processed documents and user prompts—to the AI Provider. Transmission takes place via encrypted communication using an API provided by the provider.

4.2 Service Limits and Known Limitations

d.velop does not warrant that the results generated using d.velop contracts for Microsoft 365 (e.g., extraction of document properties) or other LLM-based content are complete, appropriate, oraccurate.
You are solely responsible for verifying and ensuring that

- LLM-based software may be used for your intended purpose; and
- documents and prompts imported by you do not infringe third-party rights. Where applicable, you must obtain the necessary consent or licenses from those third parties in advance.

4.3 Service Limits and Known Limitations

The AI functions are subject to the following limitations:

- Long response times – LLMs are based on computationally intensive processes. In individual cases, this may result in waiting times of 20–30 seconds for individual requests.
- Hallucination – LLMs operate stochastically. Despite our efforts to prevent incorrect, incomplete, or inappropriate output, d.velop pilot or the underlying LLM may, in certain cases and non-deterministically, generate such information. This includes, in particular, non-factual, "invented" statements. This issue, known as "hallucination," is a fundamental limitation of current LLMs. d.velop is not liable for cases in which the software hallucinates and thereby produces invented statements.

5 Setup and Operating Information

The customer requires the following cloud services, which may incur additional costs, to operate d.velop contracts for Microsoft 365:

- Microsoft 365 SharePoint Online with the appropriate user licenses
- An empty SharePoint team site

Setup instructions for d.velop contracts for Microsoft 365

Setup of the enterprise applications in Microsoft Entra ID (see documentation

6 Administration

6.1 Support

The parties agree separately on product support in the "Service Level Agreement."

6.2 Backup und Disaster Recovery

d.velop performs regular backups of the content of d.velop contracts for Microsoft 365.

- Backups are created, subject to technical capabilities, at least once per day (RPO: 24 hours)
- Backups are retained for 30 days
- Disaster recovery tests are performed every six months

The backups cover only the configurations stored in d.velop contracts for Microsoft 365. Content such as list items or documents stored in the customer's Microsoft 365 tenant is not included. The customer is responsible for backing up and restoring content such as list items or documents stored in the customer's Microsoft 365 tenant.

Depending on the preceding event, restoration is carried out either by d.velop or at the customer's request. Data is restored by activating the backup in parallel and subsequently migrating the data to the production system. If data loss is caused by customer activity, restoration by d.velop will be charged according to the applicable service prices and the effort incurred.

6.3 Data Deletion

Data is deleted upon instruction by the customer (text form is sufficient) or after the applicable retention period following termination of the contract.

If the customer has requested deletion of its data, d.velop AG will retain the data for a further 30 days before it is permanently and irretrievably deleted.

This applies only to data stored in d.velop contracts for Microsoft 365. Content in the customer's Microsoft 365 tenant remains unaffected by the deletion.

6.4 Information Security

Data security in d.velop contracts for Microsoft 365 is ensured through a range of technical and organizational measures.

6.4.1 Encryption of content ("data at rest")

All data and content stored and processed by d.velop contracts for Microsoft 365 is encrypted at rest in accordance with current industry standards (AES-256-CBC). This applies to personal data stored by d.velop and any metadata that may need to be stored. Separate keys are used to encrypt data in different storage systems. Access to the keys is recorded in an access log

6.4.2 Transport encryption ("data in transit")

At least TLS version 1.2 or comparable transport encryption is used for communication between the application components.

6.4.3 Access logging

All access to the infrastructure of d.velop contracts for Microsoft 365 is logged.

The customer can review access to the customer tenant and the content and data stored there, including sign-ins to d.velop contracts for Microsoft 365 apps, in the Microsoft 365 audit log. To do so, the audit log must be activated and configured in the customer's Microsoft 365 tenant.

6.4.4 Authentication

The customer's users authenticate exclusively via Microsoft Entra ID using the user accounts created in the customer's tenant. For d.velop contracts for Microsoft 365 to access data in the customer's SharePoint tenant, the user must consent to the app accessing data in the customer's tenant. As a rule, however, this is done tenant-wide for all users by a customer administrator.

A distinction is made between delegated permissions and application permissions. If a regular user is involved, only delegated permissions are required. The permissions configured in SharePoint are not overwritten or bypassed. The permissions requested by the app represent only the maximum permissions required by d.velop contracts for Microsoft 365 to provide its full scope of functions. What an

individual user is permitted to do, and whether and to what extent the user may access a SharePoint site, continues to be determined exclusively in the customer's tenant.

Certain functions of d.velop contracts for Microsoft 365 require access to contract information in SharePoint when no user is active. For this purpose, a system user is configured and used in the context of the Entra ID enterprise app for communication between SharePoint Online and d.velop contracts for Microsoft 365. Details about the system user can be found in the product's system requirements.

6.4.5 Responsibilities

Because list items, metadata, documents, and user accounts are stored and managed in the customer's tenant, they—as well as the devices operated by the customer (smartphones and PCs)—are the customer's responsibility. Responsibility for password security, the use of two-factor authentication, and the general security of accounts, permissions, and devices therefore lies with the customer.

Despite all measures taken by d.velop AG, the performance of d.velop contracts for Microsoft 365 may be affected by throttling in your tenant. This may occur, for example, due to excessively used automations (imports) or bulk uploads via the client.

The customer must ensure compliance with the SharePoint limits published by the manufacturer.