d.velop cloud Plattform Leistungsbeschreibung

Freigegeben am 04/03/2021

d.velop AG
Schildarpstraße 6–8
Germany, 48712 Gescher

Fon +49 2542 9307-0
Fax +49 2542 9307-20
d-velop.com
info@d-velop.com

Handelsregister Coesfeld
HRB 4903
Geschäftsführer
Christoph Pliete
Mario Dönnebrink

d.velop

Inhalt

1 Überblick

1.1 Funktionsumfang d.velop cloud Plattform

Die d.velop cloud Plattform bietet Kunden die Möglichkeit, IT-Ressourcen und Anwendungen auf Abruf über das Internet zu buchen und zu nutzen. Zur Buchung von fachlichen Anwendungen (im Folgenden als "App" bezeichnet) wird ein eigener abgesicherter Cloudbereich (im Folgenden "d.velop cloud Mandant" oder kurz "Mandant") je Kunde erstellt in dem Apps gebucht werden können. Die angebotenen Funktionen der einzelnen Apps werden durch den jeweiligen App Anbieter bestimmt und in der Leistungsbeschreibung der einzelnen Apps aufgeführt. Ein erstellter Mandant enthält unabhängig von weiteren Buchungen bereits einige Basis-Apps die in jedem Mandant verfügbar sind und Gegenstand der vorliegenden Leistungsbeschreibung sind (vgl. Zif. 1.2 "d.velop cloud platform Basis Apps").

Eine App bildet einen fachlich und technisch in sich abgeschlossenen Teil des Gesamtsystems ab und hat keine oder möglichst wenige Abhängigkeiten zu anderen Apps. Findet eine Integration von mehreren Apps statt, passiert dies typischerweise über Links. Beispiele:

- Die Task-App ist zuständig für die Verwaltung von Aufgaben, welche User bearbeiten und weiterleiten können. Sollten zu einer Aufgabe beispielsweise Dokumente gehören, wird auf diese nur verlinkt.
- Die Usermanagement-App ist zuständig für die Verwaltung von Usern und Gruppen
- Die Identityprovider-App ist zuständig für die Authentifizierung von Benutzern. Sie ist nicht zuständig für die Autorisierung innerhalb von Apps.

Die Autorisierung, d.h. der Zugriff auf bestimmte Businessobjekte ist nicht Teil des Identityproviders sondern liegt in der Hoheit der einzelnen fachlichen Apps. Zur Authentifizierung von Benutzern verwenden wir OpenID Connect, womit die Zugangsdaten des Benutzers in der Hoheit des OpenID Providers bleiben.

1.2 d.velop cloud plattform Basis Apps

Die d.velop cloud Plattform beinhaltet die im Folgenden aufgelisteten Apps und Ihren Funktionsumfang, welche als Basis bereitgestellt werden:

- **Home-App**
  - Startseite Ihrer d.velop cloud
  - Listet für den aktuellen Benutzer verfügbare Funktionen der gebuchten Apps auf
- **Config-App**
  - Konfigurationsoptionen der gebuchten Apps auflisten
- **Shell-App**
  - Gemeinsam genutzte Layout- und Navigationselemente
- **Task-App**
  - Aufgaben an Benutzer und Gruppen senden
- **d.velop cloud center**
  - Verwaltung von d.velop cloud Mandanten
  - Buchen und Kündigen von Apps
- **d.velop cloud login**

    - Authentifizierung von Benutzern
- **IdentityproviderApp**
    - Integration der d.velop cloud mit Identitätssystemen wie zum Beispiel dem d.velop cloud login oder Active Directory
- **UsermanagementApp**
    - Verwaltung von Benutzern und Gruppenzugehörigkeiten
- **UserprofileApp**
    - Verwaltung von Abwesenheiten
- **Notification App**
    - Sendet E-Mail-Benachrichtigungen an Benutzer
- **Process-App**
    - Bereitstellung von technischen Funktionen für die Ausführung, Überwachung und Administration einfacher BPMN Prozesse.

1.3 Integrierbarkeit

Integration in ihre Anwendung

Über parametrisierte Aufrufe können Sie Inhalte aus der d.velop cloud in Ihre Anwendung integrieren. Sie können zum Beispiel ein Dokument über HTTPS in ein iFrame in ihrer Anwendung anzeigen lassen.

Eine Dokumentation mit Beispielen finden Sie unter https://developer.d-velop.de/.

Integrierte Authentifizierung

Die Identityprovider-App stellt die zentrale Authentifizierung von Benutzern. Hierbei kann zur Anmeldung der d.velop cloud-Login verwendet werden. Optional besteht die Möglichkeit, eine

Vertrauensstellung zu externen Identitätssystemen via OpenID Connect herzustellen. Auf diesem Weg kann eine Anmeldung über das bei Ihnen führende System, wie z.B. Salesforce oder ein On-Premises Active Directory, ermöglicht werden.

Integration via APIs

Die Apps der d.velop cloud stellen APIs zur Verfügung, über die Sie Ihr System mit der d.velop cloud integrieren können.

Eine Dokumentation mit Beispielen finden Sie unter https://developer.d-velop.de/.

1.4 Rechte an Inhalten

Sie räumen uns an allen Inhalten, die von Ihnen oder Ihren Mitarbeitern in der d.velop cloud importiert oder erstellt werden, ein einfaches zeitlich und örtlich auf die Zwecke des Cloudbetriebes beschränktes Nutzungsrecht ein. Sämtliche Verwertungs- Veränderungsrechte etc. verbleiben natürlich bei Ihnen, sofern Sie diese innehaben.

2 Administration

2.1 Support

Siehe d.velop cloud Support Richtlinien.

2.2 Backup und Disaster Recovery

d.velop führt regelmäßige Backups der Inhalte der d.velop cloud platform Basis Apps durch.

- Die Erstellung der Backups erfolgt in Abhängigkeit der technischen Möglichkeiten mindestens einmal pro Tag (RPO: 24 Stunden)
- Die Vorhaltezeit der Backups beträgt 30 Tage
- Es werden halbjährlich Disaster Recovery Tests durchgeführt

Datenspeicher, auf denen persistente Daten liegen, werden per Snapshot gesichert und redundant in mehreren Rechenzentren abgelegt. Relationale Datenbanken und zugehörige Transaktionsprotokolle werden gleichermaßen per Snapshot gesichert und können auf einen vom Kunden gewünschten Zeitpunkt wiederhergestellt werden. Im Kontext von bereits mehrfach redundant abgelegten Daten in Objektspeichern bezieht sich der Begriff Backup nicht auf eine weitere Kopie der Daten, sondern auf Versionierungsmechanismen, welche die Wiederherstellung der Daten nach unbeabsichtigter Löschung ermöglichen. Alle Backups sind durch die Implementierung von Multifaktor-Authentifizierung vor unbeabsichtigter Löschung geschützt. Die Wiederherstellung erfolgt abhängig von dem vorausgegangenen Ereignis entweder durch die d.velop oder durch Aufforderung des Kunden. Die Wiederherstellung der Daten erfolgt durch parallele Aktivierung des Backups und einer anschließenden Datenmigration in das Produktivsystem. Bei hervorgerufenen Datenverlusten durch Aktivität des Kunden wird die Wiederherstellung gemäß der Dienstleistungspauschale berechnet.

2.3 Datenlöschung

Die Löschung der Daten wird nach Auftrag durch den Kunden (Textform ausreichend) bzw. nach entsprechendem Fristablauf anschließend einer Vertragsbeendigung durchgeführt.

Hat der Kunde die Löschung seiner Daten beantragt, wird die d.velop AG die Daten noch für 30 Tage vorhalten, bevor Sie endgültig und nicht wiederherstellbar gelöscht werden.

3 Informationssicherheit

Die Sicherheit von Daten wird in der d.velop cloud durch eine Reihe technischer und organisatorischer Maßnahmen sichergestellt.

3.1 Datenstandort

Die d.velop cloud platform wird von uns für Sie im Großraum Frankfurt am Main betrieben. Die Rechenzentren unseres Partners sind unter anderem gemäß der folgenden Richtlinien zertifiziert:

- ISO 9001

- ISO 27001
- ISO 27017
- ISO 27018
- C5

Ihre Inhalte der d.velop cloud platform Basis Apps werden grundsätzlich in Deutschland gespeichert/verarbeitet (Ausnahme: Eingehende E-Mails können App-spezifisch über weitere Standorte innerhalb der EU verarbeitet werden). Bei Nutzung von Apps Dritter können Daten temporär oder permanent in andere Standorte übertragen werden. Informationen dazu finden Sie in der Leistungsbeschreibung der gebuchten Apps.

3.2 Verschlüsselung von Inhalten ("data at rest")

Alle Daten und Inhalte, die von den d.velop cloud platform Basis Apps gespeichert und verarbeitet werden, werden nach aktuellem Industriestandard verschlüsselt abgelegt. Dies gilt für Inhalte des Kunden, Meta-Daten zu den Inhalten, sowie für Inhalte, die für die Bereitstellung des Dienstes erstellt oder abgeleitet werden (z.B. Volltextinformationen, Vorschaugrafiken). Es werden getrennte Schlüssel für die Verschlüsselung der Daten in unterschiedlichen Speichern (Datenbanken, Festplatten) verwendet. Der Zugriff auf die Schlüssel wird über ein Zugriffs-Log protokolliert.

Aktuell wird zur Verschlüsselung Advanced Encryption Standard (AES) im Galois/Counter Mode (GCM) mit 256-Bit-Schlüsseln verschlüsselt gespeichert. d.velop behält sich vor, dies regelmäßig gemäß aktueller Empfehlungen des Bundesamt für Sicherheit in der Infomationtechnik neu zu bewerten und ggfs. anzupassen.

3.3 Transportverschlüsselung ("data in transit")

Für die Kommunikation der Anwendungskomponenten untereinander wird eine Transportverschlüsselung nach aktuellen Industriestandards verwendet. Dies wird in regelmäßigen Abständen reevaluiert, um ggfs. neuen Anforderungen und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu entsprechen. Zum Zeitpunkt der Erstellung dieses Dokumentes heißt dies für HTTPS-Verbindungen mindestens TLS-Version 1.1. Für andere Verbindungen wird (je nach Anwendungsfall) auch entweder TLS, oder eine vergleichbare Transportverschlüsselung verwendet.

3.4 Isolation von Mandanten

Unsere d.velop cloud sieht eine strikte Trennung der Daten unterschiedlicher Mandanten vor. Hierzu wird eine führende Mandanten-ID verwendet. Diese wird von den d.velop cloud platform Basis Apps verwendet, um in deren Datenspeichern den korrekten, isolierten Speicher des Mandanten auszuwählen.

3.5 Isolation von Apps

Jede App ist technisch von anderen Apps streng isoliert, sodass es für die Apps nicht möglich ist, selbstständig auf Daten anderer Apps zuzugreifen. Muss eine App auf die Daten einer anderen App zugreifen, findet dies unter Einhaltung der Berechtigungen des aufrufenden Benutzers via definierter Schnittstellen über HTTPS statt.

3.6 Protokollierung von Zugriffen

Alle Zugriffe auf die d.velop cloud platform Basis Apps werden protokolliert.

3.7 Multifaktor-Authentifizierung

Durch technische Maßnahmen stellen wir sicher, dass keine Eskalation von Privilegien durch einzelne Mitarbeiter der d.velop cloud platform stattfinden kann.

Zur Anpassung von Berechtigungen sind gesonderte Rechte notwendig. Um diese Rechte zu erhalten, müssen mehrere Faktoren bestätigt werden. Diese Faktoren sind auf getrennte Personenkreise aufgeteilt. So ist es nicht möglich, dass ein einzelner Benutzer seine Berechtigungen eskalieren kann.