Leistungsbeschreibung
d.velop cloud platform

1 Überblick

Ergänzend zu dieser Leistungsbeschreibung werden die Funktionalitäten der vom Kunden erworbenen Software in den produktspezifischen Leistungsbeschreibungen beschrieben.

Die Leistungen Support, Verfügbarkeit und Aktualisierung von der d.velop cloud platform werden im "Service Level Agreement" beschrieben.

1.1 Funktionsumfang d.velop cloud platform

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. Ziff. 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 der 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
- Identityprovider-App
  - Integration der d.velop cloud mit Identitätssystemen wie zum Beispiel dem d.velop cloud login oder Active Directory
- Usermanagement-App
  - Verwaltung von Benutzern und Gruppenzugehörigkeiten
- Userprofile-App
  - 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
- Document Intelligence Hub (DIH)
  - Schnittstelle zur Anbindung KI-basierter Dienste zur automatisierten Dokumentenerkennung. Diese App dient lediglich als Schnittstelle. Die Bereitstellung konkreter KI-Dienste erfolgt gesondert und ausschließlich nur auf gesonderte Weisung des Kunden.
- OpenID Provider-App
  - Bereitstellen von Diensten zur Integration der d.velop cloud als Anmeldeservice mit OpenID-Connect
- Theming-App
  - Zentrale Verwaltung der Designs

1.3 Integrierbarkeit

Integration in ihre Anwendung

Über parametrisierte Aufrufe kann der Kunde Inhalte aus der d.velop cloud in seine Anwendung integrieren. Der Kunde kann zum Beispiel ein Dokument über HTTPS in ein iFrame in seiner Anwendung anzeigen lassen.

Eine Dokumentation mit Beispielen findet der Kunde 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 dem Kunden 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 der Kunde sein System mit der d.velop cloud integrieren kann.

Eine Dokumentation mit Beispielen findet der Kunde unter https://developer.d-velop.de/.

1.4 Rechte an Inhalten

Der Kunde räumt d.velop an allen Inhalten, die von dem Kunden oder seinen 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 dem Kunden, sofern er diese innehat.

2 Administration

2.1 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. Das Recovery Point Objective (RPO) ist 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. Die Dauer der Wiederherstellung ist abhängig vom Umfang des eingetretenen Ereignisses. Zielvorgabe ist ein Recovery Time Objective (RTO) von 48 Stunden.

2.2 Datenlöschung

Die Löschung der Daten wird nach Weisung des Kunden oder nach Wegfall der Rechtsgrundlage für ihre Speicherung durchgeführt. In beiden Fällen wird d.velop die Daten noch für 90 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 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 Informationstechnik neu zu bewerten und ggf. anzupassen.

3.2 Transportverschlüsselung ("data in transit")

Für die Kommunikation der Anwendungskomponenten untereinander wird eine Transportverschlüsselung nach aktuellen Industriestandards verwendet. Dies wird in regelmäßigen Abständen reevaluiert, um ggf. 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 1.2. Für andere Verbindungen wird (je nach Anwendungsfall) auch entweder TLS, oder eine vergleichbare Transportverschlüsselung verwendet.

3.3 Isolation von Mandanten

Die 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.

3.4 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.

3.5 Protokollierung von Zugriffen

Es erfolgt eine dauerhafte Protokollierung von erfolgreichen und fehlgeschlagenen administrativen Zugangsversuchen zu Cloud-Systemen.

3.6 Zugriffskontrolle

Im Regelbetrieb erfolgt der Zugriff auf die Daten ausschließlich durch technische Prozesse (zwecks Data-in-Use, z.B. Bereitstellung der Dokumente oder Volltextsuche). d.velop Angestellte arbeiten im Standard mit Berechtigungen, die keine Möglichkeit haben, auf die Daten zuzugreifen. Nur im Fehlerfall oder bei einem Ausfall wird ggf. mit privilegierten Berechtigungen gearbeitet. Dabei erfolgt ein Zugriff auf die technische Infrastruktur über eine VPN-Einwahl und nach starker Authentifizierung mit einem zweiten Faktor. Der Login wird über das Prinzip Segregation of Duties (SOD), ähnlich eines vier Augen Prinzips, vergeben. Durch den daraus resultierenden privilegierten Zugriff über die technische Infrastruktur ist potenziell ein Zugriff auf die Kundendaten möglich.