DocuWare

White Paper DocuWare Cloud

Zu DocuWare ab Version 7.6

Juni 2022

Dieses Dokument wurde erstellt mit AuthorIT.

DocuWare GmbH
Planegger Straße 1
82110 Germering
www.docuware.com

Inhalt

1. Einleitung 4
   - 1.1 Zielsetzung des White Papers 4
   - 1.2 Einführung in DocuWare Cloud 4

2. Sicherheit 5
   - 2.1 IT-Sicherheit 5
   - 2.2 Datensicherheit und Datenschutz 8

3. Skalierbarkeit 11

4. Integrierbarkeit 12

5. System-Support mit 24/7-Erreichbarkeit 13

6. Datenübergabe bei Vertragsende 15

7. Compliance und Rechtliches 16

1 Einleitung

1.1 Zielsetzung des White Papers

DocuWare Cloud ist eine mandantenfähige Cloud-Lösung für Dokumenten-Management und Workflow-Automation. Dieses White Paper beschreibt die technischen Leistungsmerkmale von DocuWare Cloud und widmet sich dabei vor allem den technischen und organisatorischen Maßnahmen, die DocuWare in den Bereichen Sicherheit (IT-Sicherheit und Datenschutz) und Skalierbarkeit ergreift. Weitere Themen sind Support, zum Beispiel bei einer Datenmigration, sowie Compliance und Zertifizierungen. Das White Paper richtet sich primär an technische Mitarbeiter von Interessenten, Kunden und Vertriebspartnern sowie von Beratungsunternehmen oder Fachmedien.

1.2 Einführung in DocuWare Cloud

DocuWare Cloud ist eine „Software as a Service"-Lösung (SaaS). DocuWare wiederum setzt für sein Angebot auf die Dienste von Microsoft Azure als „Platform as a Service" (PaaS). Alle Dokumente, Dateien und Metadaten der Kunden werden auf Azure Storage gespeichert. Die Datenbanken werden von Azure SQL (Managed Service) gehostet.

Das vorliegende White Paper beschränkt sich auf die direkten Leistungen von DocuWare. Microsoft beschreibt auf seiner eigenen Webpräsenz die Leistungen von Microsoft Azure sowie die zugehörigen Maßnahmen für IT-Sicherheit und Datenschutz, auf die DocuWare aufsetzt.

2 Sicherheit

Kundendaten in DocuWare Cloud sind entsprechend den allgemein anerkannten Regeln der Technik geschützt. Dafür sorgen die IT-Infrastruktur und die Technologien von Microsoft Azure Security Services und von DocuWare sowie deren Ausrichtung an den aktuellen Datenschutzrichtlinien.

2.1 IT-Sicherheit

Durch die Verschlüsselung der Dokumente und der Kommunikation, ein ausgefeiltes Rechtekonzept, Zugriffsbegrenzungen sowie Sicherheitsaudits gewährleistet DocuWare Cloud die Sicherheit Ihrer Daten.

Verschlüsselung der Dokumente

Alle Dokumente, die in DocuWare Cloud archiviert werden, werden automatisch mit dem AES-Verfahren (Advanced Encryption Standard) verschlüsselt. Dokumente, die von DocuWare On-Premises-Systemen migriert werden, können im Nachhinein verschlüsselt werden. AES ist ein symmetrisches Kryptoverfahren, das höchste Sicherheitsanforderungen erfüllt. Als Verschlüsselungsstandard ist es zum Beispiel von der US-Regierung für Dokumente mit der höchsten Geheimhaltungsstufe (Top Secret) zugelassen.

Im AES-Verfahren wird für jedes Archiv ein asymmetrisches Schlüsselpaar generiert. Der private Schlüssel wird dazu verwendet, wiederum die symmetrischen Schlüssel zu verschlüsseln, die bei der Verschlüsselung der Dokumente eines Archivs entstehen. Der private Schlüssel des Archivs wird dann nochmals mit einem Master Key verschlüsselt.

Für einen maximalen Schutz setzt DocuWare bei der Verschlüsselung mit AES auf eine Schlüssellänge von 256 Bit. Für die Verschlüsselung der symmetrischen Schlüssel kommt eine Schlüssellänge von 1024 Bit zum Einsatz. Dabei wird für jedes Dokument ein neuer symmetrischer Schlüssel generiert. Dadurch können selbst bei einer Kryptoanalyse keine Muster erkannt und es können somit keine Schlüssel errechnet werden.

Verschlüsselung der Kommunikation

Innerhalb eines von DocuWare genutzten Rechenzentrums sind alle Kundendaten über ein VPN (Virtual Private Network) abgesichert. Die Netzwerkinfrastruktur ist zudem virtualisiert und das virtuelle Netzwerk nach außen hin abgeschottet.

Für die Verschlüsselung des Datenverkehrs zwischen den Nutzern und dem Rechenzentrum wird das aktuelle TLS-Protokoll (Nachfolgeprotokoll von SSL) verwendet, sofern es von dem jeweiligen genutzten Browser unterstützt wird. TLS wird für den gesamten Verkehr auf Basis von HTTP (HTTPS) und TCP eingesetzt. Dabei sehen die Nutzer im Browser sofort, ob ihre Verbindung sicher und validiert ist: Bei einer sicheren Verbindung färbt sich die URL-Adressleiste grün (außer bei Google Chrome).

Für einen weiteren Schutz vor Angriffen von außen gibt es zusätzliche Sicherheitsschichten und -funktionen, zum Beispiel HSTS zum Schutz gegen Protokoll-Downgrade-Attacken und Cookie Hijacking.

Authentifizierung

Für eine sichere und komfortable Authentifizierung können Sie Single Sign-On (SSO) verwenden, um die Anmeldedaten nur eines Accounts für alle DocuWare-Anwendungen zu verwenden. Dazu müssen Sie Ihre Organisation mit einem Identity Provider verbinden. DocuWare unterstützt Microsoft Azure Active Directory und Microsoft Active Directory Federation Services (4.0) als Identity Provider.

Mit einem Klick auf den Single-Sign-On-Button im Login-Dialog von DocuWare wird der Benutzer zum Identity Provider weitergeleitet. Nach der erfolgreichen Authentifizierung erfolgt die Anmeldung in DocuWare automatisch, dabei spielt es keine Rolle, ob der Benutzer sich über den DocuWare Client, DocuWare Mobile, die Desktop Apps, in der Konfiguration oder der Administration anmeldet.

Weiterhin unterstützt DocuWare Microsoft Active Directory Federation Services (ADFS) für das SSO. DocuWare nutzt dabei OpenID Connect, daher ist die Version ADFS in Windows Server 2016 oder höher notwendig, denn nur darin wird OpenID Connect unterstützt.

Dabei ist zu beachten, dass Microsoft in Azure Active Directory einige Voreinstellungen zum Logout bei Single Sign-On trifft, und zwar zur Persistenz von Browsersitzungen und zur Gültigkeitsdauer von Token. Ausführliche Dokumentationen dazu finden Sie auf der Website von Microsoft:

- https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime
- https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes

Rechtekonzept

DocuWare Cloud verfügt über ein ausgefeiltes Rechtesystem. Grundlegend für die Rechteverwaltung in DocuWare ist die Unterscheidung in funktionale Rechte und Archivrechte.

Funktionale Rechte werden jeweils pro DocuWare-Organisation vergeben und beziehen sich auf bestimmte Funktionen. Dazu gehören beispielsweise:

- Benutzer verwalten
- Archive und Briefkörbe konfigurieren
- Workflows designen
- Stempel verwenden
- Konfigurationen von DocuWare-Komponenten wie z.B. Connect to Outlook, Smart Connect oder DocuWare Forms erstellen und bearbeiten

Archivrechte beziehen sich auf ein bestimmtes Archiv und die darin gespeicherten Dokumente. Zu den Archivrechten gehören:

- administrative Berechtigungen, zum Beispiel Rechte oder Dialoge verwalten oder Dokumente migrieren
- allgemeine Berechtigungen bezüglich der Dokumente im Archiv, zum Beispiel Dokumente ablegen, suchen, bearbeiten oder löschen
- Overlay-Berechtigungen, zum Beispiel Dokumente stempeln, Anmerkungen und grafische Elemente auf Dokumente aufbringen oder Anmerkungen löschen
- Indexfeld-Berechtigungen, zum Beispiel Feldinhalte ändern oder Feldeinträge verwenden, die nicht in einer Auswahlliste vorhanden sind.

Rechte für Benutzer und Administratoren

Für alle Konfigurationen von DocuWare Cloud, zum Beispiel für Briefkörbe, Archive oder Formulare, vergeben Sie Berechtigungen – entweder an Benutzer direkt oder über Rollen. Dabei gibt es zwei verschiedene Arten von Berechtigungen: Mit dem Benutzerrecht lässt sich das betreffende Objekt verwenden. Das Administratorrecht erlaubt es, das Objekt bzw. die zugehörige Konfiguration zu ändern.

Zugriffsbegrenzung durch Datentrennung

DocuWare Cloud trennt strikt die Kundendaten, nämlich eine DocuWare Organisation pro Kunde, von den Systemdaten.

Die Administratoren der DocuWare Cloud-Systeme erhalten lediglich Zugriff auf die Systemdaten, die für den Betrieb dringend benötigt werden. Siehe auch Kapitel Support > Wartung.

Die DocuWare-Administratoren der Kunden haben vollen Zugriff auf deren jeweilige Organisationseinstellungen, nicht aber auf die Einstellungen des DocuWare-Systems.

Sicherheitsaudit

Regelmäßige externe und interne Penetrationstests helfen, die Sicherheit der Systeme immer auf dem Niveau der allgemein anerkannten Regeln der Technik zu halten. Die Ergebnisse der Penetrationstests werden während der regelmäßigen Zertifizierung für den Standard SOC2 kritisch von den externen Auditoren hinterfragt.

Außerdem findet über die Azure Security Services ein detailliertes Risk Reporting statt, sodass aufseiten von Microsoft Azure auftretende Probleme umgehend behoben werden können.

Kunden können innerhalb ihrer Organisation Protokollierungen auf Dokument-, Archiv und Organisationsebene durchführen und diese zur leichten Auswertbarkeit im universellen CSV-Format exportieren. So ist beispielsweise ersichtlich, wer wann welche Einstellungen geändert oder Dokumente abgelegt bzw. gelöscht hat. Mit Protokollierungen lässt sich beispielsweise die Einhaltung von gesetzlichen Richtlinien belegen, zum Beispiel der deutschen GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff, siehe unten „Rechtlicher Hinweis für Kunden mit Sitz in Deutschland“).

Analysen von Telemetrie-Daten

In Echtzeit-Sicherheitsanalysen von Telemetrie-Daten wird geprüft, ob innerhalb der DocuWare-Systeme im Vergleich zum Normalbetrieb ungewöhnliche Ereignisse stattfinden. Im Falle der Erkennung solcher Ereignisse werden entsprechende Maßnahmen ergriffen. Die Untersuchungen umfassen:

- Datenbank-Zugriffe (Zugriffsort und Befehlssemantik)
- Fehlerrate
- Performance-Veränderungen
- Anmeldeversuche
- kritische Systemupdates
- Netzwerkverkehr

2.2 Datensicherheit und Datenschutz

DocuWare Cloud gewährleistet bei korrekter Konfiguration und Handhabung zuverlässig die Sicherheit, den Schutz und die Wiederherstellungsmöglichkeit der Kundendaten. Dadurch unterstützt es den Kunden bei seiner Compliance mit dem jeweils gültigen regionalen Datenschutzrecht. Datenschutz durch Technikgestaltung (Privacy by design) ist für DocuWare seit Gründung des Unternehmens im Jahr 1988 ein maßgeblicher Grundsatz. Die technischen und organisatorischen Maßnahmen (TOMs) sind hier beschrieben.

Datensicherheit

Alle Dokumente, mit denen die Kunden arbeiten (Produktivdaten), werden in einem Rechenzentrum von Microsoft Azure gespeichert (Hauptstandort). Das gilt sowohl für die Dokumente in Archiven als auch jene in Briefkörben. In diesem Rechenzentrum werden zusätzlich zwei Kopien jedes einzelnen Dokuments gespeichert, und zwar unmittelbar nachdem es in DocuWare gelangt ist oder verändert wird.

Um den gesamten Produktivdaten-Bestand für große Schadensereignisse wie zum Beispiel Erdbeben oder Flugzeugabstürze abzusichern, werden darüber hinaus drei Kopien von jedem Dokument in ein zweites Rechenzentrum kopiert, das sich an einem anderen Standort in derselben Region befindet (georedundante Speicherung, GRS).

An beiden Standorten befindet sich immer die aktuelle Fassung eines jeden Dokuments.

Datenschutz

Der Betrieb der Kundensysteme unterliegt dem jeweils regional geltenden Datenschutzrecht.

Standorte der Datenzentren: Die Daten der Kunden werden in Datenzentren von Microsoft Azure in den folgenden Regionen gehostet: EU, USA, Japan und Australien.

Region	Hauptstandort	GRS-Standort
EU	North Europe, Irland	West Europe, Niederlande
USA	Central US, Bundesstaat Iowa	East US 2, Bundesstaat Virginia
Japan	Japan East, Tokio/Saitama	Japan West, Osaka
Australien	Australia East, New South Wales	Australia Southeast, Victoria

Landesspezifische Zuordnung zu den Datenzentren: Eine detaillierte Liste mit der landesspezifischen Zuordnung von DocuWare Cloud Kunden zu den regionalen Datenzentren von Microsoft Azure finden Sie hier.

Verwendung von Microsoft Office Online mit DocuWare: Bei der Verwendung von Microsoft Office Online wird das Dokument an ein Datenzentrum von Microsoft Azure übergeben, meistens an eines nahe dem geografischen Standort des Benutzers. DocuWare kann hier jedoch keinen Einfluss auf die Auswahl des verwendeten Datenzentrums nehmen, daher kann nicht garantiert werden, dass Dokumente nicht die jeweilige Region – EU, USA, Japan, Australien – des von DocuWare verwendeten Datenzentrums verlassen.

Backup

Mit der in DocuWare Cloud enthaltenen Backup-Strategie ermöglicht DocuWare die Wiederherstellung von Dokumenten und Metadaten, um die Geschäftstätigkeit von Kunden jetzt und in Zukunft zu schützen.

Dokumente: Zusätzlich zu den im Abschnitt Datensicherheit erwähnten redundanten Kopien der verschlüsselten Produktivdaten wird eine weitere Kopie erstellt und in einem kontinuierlichen Backup gespeichert. Dies geschieht, kurz nachdem das Dokument in DocuWare abgelegt oder verändert wurde. Die Sicherung nach einer Dokumentänderung erzeugt eine neue Kopie des Dokuments. Diese wird zusätzlich zu den bestehenden Sicherungen des Dokuments gespeichert. Dies gilt immer, unabhängig davon, ob die Dokumentversionierung in DocuWare aktiviert oder deaktiviert ist. Der Vorteil der aktivierten Dokumentversionierung ist, dass der Kunde direkt in DocuWare auf ältere Dokumentversionen zugreifen kann. Das Wiederherstellen einer früheren Dokumentversion folgt den gleichen Regeln wie die Dokumentwiederherstellung, siehe unten.

Metadaten: Vollständige Datenbanksicherungen der Metadaten erfolgen wöchentlich, differenzielle Sicherungen alle 12 bis 24 Stunden und Sicherungen von Transaktionsprotokolle alle 5 bis 10 Minuten. Die Häufigkeit der Sicherungen von Transaktionsprotokollen richtet sich nach der Größe des Rechners und dem Umfang der Datenbankaktivität. Weitere Informationen finden Sie unter https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview.

Cold Storage: Um eine Wiederherstellung zu ermöglichen, sichert DocuWare sowohl die Metadaten als auch die Dokumente in einem separaten Cold Storage. Dieser Cold Storage befindet sich in einem Microsoft-Rechenzentrum innerhalb der jeweiligen Region, derzeit

in Amsterdam (Niederlande) für die EU, im Bundesstaat Washington (USA) für Amerika, in Osaka für Japan und in Victoria für Australien. Der Cold Storage ist physisch vollständig von der bzw. den DocuWare Domäne(n) getrennt und unterliegt erweiterten Sicherheitsbestimmungen, sodass die Daten auch vor möglichen Schadensereignissen in einer DocuWare Domäne (z.B. Cyberattacken) geschützt sind.
Die vollständigen Datenbank-Backups der Metadaten werden an Wochenenden, meist zur regionalen Nachtzeit, im Cold Storage durchgeführt. Die Dokumente werden direkt im Cold Storage gesichert.
Die Erstellung von Backups im Cold Storage wird automatisch kontinuierlich überwacht. Produktivdaten werden (wie im Cloud Service-Vertrag beschrieben) im Zeitraum von 60 bis 90 Tagen nach Vertragsende gelöscht. Die Backups werden im Zeitraum von 10 bis 20 Tagen nach der Löschung der Produktivdaten gelöscht.

Wiederherstellung: Eine punktgenaue Wiederherstellung von Dokumenten ist zu jedem Zeitpunkt innerhalb der Aufbewahrungsfrist von **7 Tagen** möglich. DocuWare benötigt vom Kunden eine Information darüber, wann das wiederherzustellende Dokument noch abrufbar war. Der Kunde muss die Anfrage spätestens **5 Tage** nach dem Löschen oder Ändern des Dokuments an den DocuWare Support (https://support.docuware.com) senden. Die Wiederherstellung von Dokumenten nach 7 Tagen muss in Zusammenarbeit mit dem DocuWare Support geprüft werden.
Dokumente und Metadaten können innerhalb der Aufbewahrungsfrist von 3 Monaten auf den Stand eines beliebigen Wochenendes und innerhalb der Aufbewahrungsfrist von 12 Monaten auf den Stand des ersten Wochenendes eines Monats zurückgesetzt werden. Nach 12 Monaten können Dokumente und Metadaten bis zur Vertragsbeendigung auf den Stand des ersten Wochenendes eines jeden Kalenderjahres wiederhergestellt werden.

Aufbewahrungsfrist	**Wiederherstellung**	**DocuWare Support informieren**
Innerhalb von 7 Tagen	Zeitpunkt (Point in Time)	Nicht später als 5 Tage
Innerhalb von 3 Monaten	Auf den Stand eines beliebigen Wochenendes	Nicht später als 80 Tage
Innerhalb von 12 Monaten	Auf den Stand des ersten Wochenendes eines Monats	Nicht später als 350 Tage
Bis Vertragsbeendigung	Auf den Stand des ersten Wochenendes eines Kalenderjahres	Keine Limitierung oder Einschränkung

Eine Wiederherstellung ist nur in Zusammenarbeit mit dem DocuWare Support möglich. Wenn eine Wiederherstellung aufgrund einer Fehlbedienung durch den Kunden erforderlich ist (z.B. durch versehentliches Löschen oder Verändern von Dokumenten), werden die Kosten für die Wiederherstellung zusätzlich in Rechnung gestellt.

3 Skalierbarkeit

Sowohl DocuWare selbst als auch Microsoft Azure im Rahmen seiner PaaS-Infrastruktur (Platform as a Service) bieten umfangreiche Methoden und Technologien zur Skalierbarkeit.

Skalierbarkeit je Kunde

DocuWare Cloud unterstützt Teams verschiedenster Art und Größe. Es kann flexibel in Bezug auf Speichervolumen und Anzahl von Anwenderlizenzen an die jeweilige Unternehmensgröße und an das Dokumentaufkommen angepasst werden.

Wenn bestimmte Speichergrenzen erreicht oder überschritten werden, versendet DocuWare automatisch E-Mail-Benachrichtigungen an den Organisationsadministrator und den ADP-Kontakt. Dies gilt jeweils für das Erreichen oder Überschreiten von 85%, 90%, 95%, 99%, 100% des Speicherlimits.

- Bei Erreichen oder Überschreiten von 85% des Speicherlimits gehen diese Benachrichtigungen bei einem indirekten Kunden an dessen ADP-Kontakt, bei einem direkten Kunden an dessen Organisationsadministrator.
- Bei Erreichen oder Überschreiten von 90%, 95%, 99% und 100% des Speicherlimits gehen die Benachrichtigungen bei einem indirekten Kunden an dessen Organisationsadministrator und dessen ADP-Kontakt, bei einem direkten Kunden nur an dessen Organisationsadministrator.

Die Benachrichtigungen werden versandt, wenn das verbleibende Speichervolumen für weniger als 100 Tage bestehen bleibt. Der Berechnung liegt das Ablageverhalten der letzten 30 Tage zugrunde.

Skalierung des Cloud-Systems

Das DocuWare Cloud System wird automatisch skaliert je nach Anzahl der Nutzer, Anzahl der Anfragen dieser Nutzer und der sich daraus ergebenden Last auf das System. In den Zeitfenstern, in denen besonders viele Nutzer gleichzeitig mit DocuWare arbeiten, werden automatisch weitere Server gestartet, um damit die höhere Last abzufangen. Da es sich bei DocuWare Cloud um eine sogenannte Public Cloud handelt, findet die Skalierung pro System statt und nicht pro Kundenorganisation.

4 Integrierbarkeit

Um maximalen Nutzen aus Dokumenten-Management und Workflow-Automation zu erzielen, lässt sich DocuWare Cloud mit nahezu jeder anderen Unternehmensanwendung verbinden. Dies funktioniert unabhängig davon, ob diese Anwendung als On-Premises-System betrieben wird oder auch cloudbasiert ist. Mehr Informationen dazu erhalten Sie im DocuWare White Paper Integration.

5 System-Support mit 24/7-Erreichbarkeit

Monitoring

Im Datencenter bei Microsoft Azure findet ein ständiges automatisches Monitoring aller Vorgänge statt. Auffällige Vorkommnisse werden automatisch an den System-Support von DocuWare berichtet. Zu dem Monitoring gehören:

- Konstante Performance-Kontrollen
- Regelmäßige komplette Tests der DocuWare-Grundfunktionen
- Statistische Erhebungen zum Nutzungsverhalten durch Kunden, zum Beispiel dazu, wie viele Aktionen durch Kunden in einem bestimmten Zeitfenster ausgeführt werden (z.B. Dokumentsuche und -ablage, Login), um Performance-Verbesserungen zu ermöglichen

Bei Unregelmäßigkeiten greift der System-Support von DocuWare mit 24/7-Erreichbarkeit unverzüglich ein.

Hotfixes und Upgrade

Ein- bis zweimal pro Jahr wird die jeweils neue DocuWare-Version in die Kunden-Organisationen eingespielt. Dafür wird die entsprechende Organisation offline geschaltet, das Upgrade ausgeführt und die Organisation anschließend mit der neuen DocuWare-Version wieder online geschaltet.

DocuWare informiert die Kunden vier Wochen im Voraus über die geplante Aktualisierung. Im Fehlerfall wird die Organisation mit der vorherigen DocuWare-Version wieder online gestellt, sodass keine längeren Ausfallzeiten entstehen.

Die lokal installierten Komponenten (Desktop Apps) sollten Kunden stets auf dem neuesten Stand halten. Entsprechende Updates können problemlos von den Anwendern selbst ausgeführt werden, sofern sie zur lokalen Installation von Software berechtigt sind. Anderenfalls kann der IT-Administrator das Update mithilfe einer Software-Management-Lösung als unbeaufsichtigte Installation (Silent Install) durchführen.

Wartung

Für bestimmte Wartungstätigkeiten sind volle oder umfangreiche Administrationsrechte an den DocuWare Cloud-Systemen notwendig. Um auch hierbei eine Datensicherheit zu gewährleisten, die den allgemein anerkannten Regeln der Technik entspricht, unterliegen Zugriffe durch Wartungsadministratoren der Protokollierung.

Darüber hinaus greifen die folgenden Sicherheitsmechanismen:

- Alle Zugriffe auf DocuWare Cloud-Systeme erfolgen per RDP-Sitzung.
- Um eine RDP-Sitzung starten zu können, muss sich ein Administrator über definierte, besonders geschützte IP-Adressen in ein VPN einwählen, das über Zertifikate abgesichert ist und nur den Administratoren zur Verfügung steht.

- Jeder Administrator von DocuWare Cloud hat seine eigene Kennung. So kann immer nachvollzogen werden, wer sich an welchem System angemeldet hat.
- Alle Administratoren sind geschult und wurden insbesondere auf einen höchst sensiblen, geschützten Umgang mit Daten wie Zertifikaten und Passwörtern hingewiesen.

6 Datenübergabe bei Vertragsende

Kundendaten gehören dem Kunden – immer

Sollte sich ein Kunde zur Beendigung des Vertragsverhältnisses entschließen, unterstützt DocuWare ihn auf Wunsch dabei, seine Dokumente vom DocuWare Cloud System herunterzuladen und/oder in ein anderes System zu migrieren. Dafür gibt es zwei Möglichkeiten:

1. Kleinere Mengen an Dokumenten, die nicht zeitnah oder gar nicht mehr bearbeitet werden müssen, können mit DocuWare Request in Form von Stand-alone-Archiven exportiert und genutzt werden. Diese Option ist auf maximal 50.000 Dokumente oder 10 GB Speichervolumen begrenzt.
2. Bei größeren Datenmengen und vielen Dokumenten, die in aktuelle Prozesse eingebunden sind, helfen die Spezialisten von DocuWare Professional Services. Deren kostenpflichtige Dienstleistungen haben folgende Vorteile:
   -- Nach Absprache mit dem Kunden erfolgt der Zugriff auf die Dokumente direkt im Datencenter und so, dass große Datenmengen in kürzester Zeit übergeben werden.
   -- Lebende sowie in aktuelle Prozesse eingebundene Dokumente werden zeitnah in die Prozesse eines neuen Systems migriert und damit Unterbrechungen der Arbeitsabläufe minimiert.
   -- Es werden speziell auf die Arbeitsabläufe und die verwendeten Dokumenttypen des Kunden zugeschnittene Lösungen entwickelt.

Im Anschluss an die Beendigung des Vertragsverhältnisses werden alle Kundendaten innerhalb des DocuWare Cloud-Systems sowie alle Backup-Daten sicher und unwiderruflich gelöscht: nach 60 bis 90 Tagen am Hauptstandort und am GRS-Standort, im folgenden Quartal dann im Cold Storage.

Ein Wiederherstellen der Daten ist ab diesem Zeitpunkt nicht mehr möglich.

7 Compliance und Rechtliches

Zertifizierungen und Compliance von DocuWare und DocuWare Cloud

DocuWare ist zertifiziert und unterstützt Sie bei der Compliance in Ihrem Business. Produkt, Unternehmen und Plattform erfüllen alle Standards und Normen, um Ihre Informations- und Datensicherheit zu gewährleisten, zum Beispiel GoBD, DSGVO, ISO 9001, DIN EN ISO/IEC 27001, GeBüV, SOC 2, Typ 2 und viele mehr.

Die Zertifizierungen, die sich auf eine Software-Version beziehen, werden nicht für jede neue Version durchgeführt, aber in regelmäßigen Abständen erneuert. Erfahren Sie mehr über die Zertifizierungen von DocuWare.

Zertifizierungen von Microsoft Azure

Microsoft ist Vorreiter der Cloud-Branche bei der Festlegung und konsistenten Einhaltung klarer Anforderungen an Sicherheit und Datenschutz. Azure hält eine Vielzahl internationaler und branchenspezifischer Compliance-Standards ein, beispielsweise die Datenschutz-Grundverordnung (DSGVO), ISO 27001, HIPAA, FedRAMP, SOC 1 und SOC 2 sowie länderspezifische Standards wie Australia IRAP, UK G-Cloud und Singapore MTCS. In Audits durch Drittanbieter – zum Beispiel durch das British Standards Institute – wird überprüft, ob Azure die von diesen Standards geforderten strengen Sicherheitskontrollen einhält. Weitere Informationen zu den Zertifizierungen von Microsoft Azure.

Rechtlicher Hinweis für Kunden in Deutschland

Für Unternehmen mit Sitz in Deutschland gilt die deutsche Abgabenordnung (AO): Soweit mit der Nutzung von DocuWare elektronische Bücher und sonst erforderliche elektronische Aufzeichnungen oder Teile davon außerhalb des Geltungsbereiches der AO geführt und aufbewahrt werden, bedarf dies gemäß § 146 Abs. 2a AO einer Bewilligung durch die zuständige Finanzbehörde.

Eine unverbindliche Formulierungshilfe für einen entsprechenden Antrag ist hier verfügbar.

Änderungen des White Paper Cloud

DocuWare behält sich das Recht vor, den Inhalt des White Paper Cloud, insbesondere hinsichtlich der beschriebenen Leistungen und Standards, aus berechtigten Gründen anzupassen, sofern dies für den Kunden zumutbar ist. Ein berechtigter Grund liegt insbesondere aufgrund technischer Weiterentwicklung, der Einführung neuer Leistungen oder Standards, Änderungen des Leistungsangebots eingesetzter Dienstleister (insbesondere Microsoft) oder aufgrund geänderter gesetzlicher beziehungsweise behördlicher Vorgaben vor.