DocuWare Security FAQs

Alles über die Informationssicherheit und Compliance-Maßnahmen
von DocuWare für DocuWare Cloud und die DocuWare Organisation

August 2025

DocuWare GmbH
Planegger Str.1
82110 Germering
Germany
www.docuware.com

1 DocuWare Cloud – the product

1.1 General

Can you share any kind of evidence or proof of your statements, like screenshots?
Due to the sensitive nature of our systems, we cannot share evidence like screenshots yet. We can only provide information that does not put our company or customers' data at risk.

Is it possible to view audit reports?
DocuWare does not publish audit reports for the general public. Customers and partners can receive a copy of the SOC 2 Type 2 report after signing an NDA.

1.1.1 Cloud Provider

Which cloud provider is used?
DocuWare Cloud uses the Microsoft Azure public cloud.

Where are the provider's data centers located?
Customer data is hosted in Microsoft Azure data centers in the following regions: EU, US, Japan, and Australia.
A detailed list with the country-specific mapping of DocuWare Cloud customers to Microsoft Azure regional data centers can be found here:
DocuWare Cloud: Regional mapping of countries to Microsoft Azure data centers

1 DocuWare Cloud – das Produkt

1.1. Allgemeine Informationen

Können Sie irgendwelche Nachweise oder Belege für Ihre Aussagen vorlegen, beispielsweise Screenshots?
Aufgrund der vertraulichen Beschaffenheit unserer Systeme können wir derzeit keine Nachweise wie Screenshots vorlegen. Wir können nur Informationen bereitstellen, die weder unser Unternehmen noch die Daten unserer Kunden gefährden.

Ist es möglich, Auditberichte einzusehen?
DocuWare veröffentlicht keine Auditberichte für die allgemeine Öffentlichkeit. Kunden und Partner können nach Unterzeichnung einer Vertraulichkeitsvereinbarung eine Kopie des SOC 2 Typ 2-Berichts erhalten.

1.1.1 Cloud-Anbieter

Welcher Cloud-Anbieter wird genutzt?
DocuWare Cloud nutzt die Microsoft Azure Public Cloud.

Wo befinden sich die Rechenzentren des Anbieters?
Die Kundendaten werden in Microsoft Azure-Rechenzentren in den folgenden Regionen gehostet: EU, USA, Japan und Australien.
Eine detaillierte Liste mit der länderspezifischen Zuordnung der DocuWare Cloud Kunden zu den regionalen Microsoft Azure-Rechenzentren finden Sie hier:
DocuWare Cloud: Regionale Zuordnung von Ländern zu Microsoft Azure-Rechenzentren

1.1.2 Cloud service model

Which cloud service model is in place?

DocuWare Cloud uses a public cloud SaaS model. However, stored data (documents) and databases are strictly separated per customer. Only computing or networking resources are shared.

1.1.3 Cloud service stack

Which service stack is in use?

DocuWare Cloud Services are delivered and updated in the cloud by using docker containers. This ensures that the software tested in pre-production systems reaches production in exactly the same version and configuration as the one which was tested. In addition, it enables seamless rollback, when updated software in rare cases shows bugs in production.

1.1.4 Operating DocuWare Cloud

Who is operating DocuWare Cloud and how do you handle varying load and resource demands on productive systems?

DocuWare Cloud is operated and monitored by a dedicated DocuWare team with 24x7 standby: Cloud Operations (DevOps).

Automated scaleout ensures that request peaks are automatically answered by starting up more computing resources for the services showing high load. Automatic scale down is also in place. Health-checks trigger alerts in case one of the services provided shows performance degradation or even failures.

1.1.2 Cloud Service Model

Welches Cloud-Service-Modell gibt es?

DocuWare Cloud nutzt ein Public Cloud SaaS-Modell. Die gespeicherten Daten (Dokumente) und die Datenbanken sind jedoch strikt nach Kunden getrennt. Nur Computer- oder Netzwerkressourcen werden gemeinsam genutzt.

1.1.3 Cloud Service Stack

Welcher Service Stack wird verwendet?

Die DocuWare Cloud Services werden mithilfe von Docker-Containern in der Cloud bereitgestellt und aktualisiert. Auf diese Weise wird sichergestellt, dass die in den Vorproduktionssystemen getestete Software in genau der gleichen Version und Konfiguration in die Produktion gelangt wie die getestete. Darüber hinaus ermöglicht es ein nahtloses Rollback, wenn aktualisierte Software in seltenen Fällen Fehler in der Produktion aufweist.

1.1.4 Betrieb von DocuWare Cloud

Wer betreibt DocuWare Cloud und wie gehen Sie mit unterschiedlichen Auslastungen und Ressourcenanforderungen an produktiven Systemen um?

Die DocuWare Cloud wird von einem eigenen DocuWare Team mit 24x7-Bereitschaft betrieben und überwacht: Cloud Operations (DevOps).
Das automatische Scaleout sorgt dafür, dass auf Anfragespitzen automatisch reagiert wird, indem mehr Rechenressourcen für die Dienste mit hoher Auslastung bereitgestellt werden. Ein automatisches Scaledown ist ebenfalls vorgesehen. Health-Checks lösen Warnungen aus, wenn einer der angebotenen Dienste Leistungseinbußen oder sogar Ausfälle aufweist.

What is the 24x7 standby team?
Cloud Operations team has 24x7 standby shifts and is alerted about any deviations from normal operation by a modern alerting system. An urgency handling process ensures that upon a suspected incident or problem, any DocuWare employee can immediately alert responsible standby operators at any point in time (24x7).
See also section 2.6 Human Resources security.

Was ist der 24/7-Bereitschaftsdienst?
Das Cloud Operations-Team hat rund um die Uhr Bereitschaftsschichten und wird über ein modernes Warnsystem über jede Abweichung vom Normalbetrieb informiert. Ein nach Dringlichkeit abgestuftes Verfahren stellt sicher, dass jeder DocuWare Mitarbeiter bei einem vermuteten Vorfall oder Problem zu jedem Zeitpunkt (24x7) sofort den zuständigen Bereitschaftsdienst alarmieren kann.
Siehe auch Abschnitt 2.6 Sicherheit des Personals.

Security first – what does that mean?
Security is a core aspect of the DocuWare product and considered with every business decision to prevent harm. This includes many facets, like how access is controlled, how data is treated safely, or how personnel is trained.
Data and database contents of DocuWare Cloud customers is encrypted “at rest” (when stored at the storage location or in the database) and therefore not accessible even to DocuWare Cloud operators.
The Cloud Operations team accesses cloud resources only from a restricted and separated network. Access is secured by VPN connections. Any actions performed by the Cloud Operations team are recorded in audit logs.

Sicherheit geht vor – was bedeutet das?
Sicherheit ist ein zentraler Aspekt des DocuWare Produkts und wird bei jeder geschäftlichen Entscheidung berücksichtigt, um Schäden zu vermeiden. Dies umfasst viele Aspekte, beispielsweise die Art und Weise, wie der Zugriff kontrolliert wird, wie Daten sicher behandelt werden oder wie Mitarbeiterinnen und Mitarbeiter geschult wird.
Daten und Datenbankinhalte von DocuWare Cloud Kunden werden „at rest“ (bei der Sicherung am Speierort oder in der Datenbank) verschlüsselt und sind daher auch für DocuWare Cloud Operatoren nicht zugänglich.
Das Cloud-Operations-Team greift nur über ein eingeschränktes und getrenntes Netzwerk auf Cloud-Ressourcen zu. Der Zugang ist durch VPN-Verbindungen gesichert. Alle vom Cloud-Operations-Team durchgeführten Aktionen werden in Audit-Protokollen aufgezeichnet.

What is the cloud management portal?
By using a cloud management portal, key indicators like memory usage, CPU load, version of deployed services for running systems and the number of scaled-out systems can be easily monitored and configured.
Roll-out of production-ready minor updates for running services can be scheduled from this portal, too. Such minor updates do not cause any downtime for customers, as the updates are done one-by-one only on the services to be updated.

1.1.5 Data protection in the cloud

How is data protection ensured in DocuWare Cloud?
The operation of DocuWare Cloud customer systems is subject to applicable regional data protection legislation. Data of one customer always stays in one privacy region.
Customer data is hosted in Microsoft Azure data centers in the following regions: EU, US, Japan, and Australia.
For the country-specific mapping of DocuWare Cloud customers, see our detailed list:

Regional mapping of countries to Microsoft Azure data centers

For information about data protection at DocuWare as an organization, see section 2.5 Data privacy compliance.

Which data protection laws does DocuWare Cloud support?

Due to its flexible configuration possibilities, DocuWare Cloud helps you meet data privacy standards such as GDPR, CCPA, HIPAA, APPI, and POPIA.
Please see our compliance and certification page at:

Compliance and certifications

Was ist das Cloud-Management-Portal?
Mithilfe eines Cloud-Management-Portals können Schlüsselindikatoren wie Speichernutzung, CPU-Last, Version der bereitgestellten Dienste für laufende Systeme und die Anzahl der Scaled-out-Systeme leicht überwacht und konfiguriert werden.
Das Rollout von produktionsreifen kleineren Updates für laufende Dienste kann ebenfalls über dieses Portal geplant werden. Solche kleineren Aktualisierungen verursachen keine Ausfallzeiten für die Kunden, da die Aktualisierungen nur für die zu aktualisierenden Dienste einzeln durchgeführt werden.

1.1.5 Datenschutz in der Cloud

Wie wird der Datenschutz in der DocuWare Cloud gewährleistet?
Der Betrieb der DocuWare Cloud Kundensysteme unterliegt den geltenden regionalen Datenschutzgesetzen. Die Daten eines Kunden bleiben immer in einer Datenschutzregion.
Die Kundendaten werden in Microsoft Azure-Rechenzentren in den folgenden Regionen gehostet: EU, USA, Japan und Australien.
Die länderspezifische Zuordnung der DocuWare Cloud Kunden finden Sie in unserer detaillierten Liste:

Regionale Zuordnung von Ländern zu Microsoft Azure-Rechenzentren

Informationen zum Datenschutz bei DocuWare als Organisation finden Sie im Abschnitt 2.5 Einhaltung des Datenschutzes.

Welche Datenschutzgesetze werden von DocuWare Cloud unterstützt?
DocuWare Cloud hilft Ihnen, Datenschutzstandards wie DSGVO, CCPA, HIPAA, APPI und POPIA zu erfüllen.
Bitte beachten Sie unsere Seite zu Compliance und Zertifizierungen unter:

Compliance und Zertifizierungen

1.1.6 Certifications and standards

What certifications does DocuWare Cloud hold?
DocuWare Cloud holds all relevant certifications, such as SOC 2 Type 2, GoBD, ISO 27001, ISO 9001, GeBüV, and undergoes recertification on a regular basis. All certifications of DocuWare Cloud can be found in this list:
DocuWare certifications and awards
In addition, you can find all Microsoft Azure certifications here.

To which degree does the DocuWare Cloud comply with the BSI standards?
Microsoft Azure, the infrastructure that the DocuWare Cloud is running on, complies with the "Catalogue of Requirements for Cloud Computing" (C5) of the BSI (Germany's Federal Cyber Security Authority).

1.2 Security aspects

1.2.1 Encryption

Is sensitive data encrypted over public network?
Yes. DocuWare Cloud leverages TLS 1.2 (no previous versions allowed), secure cipher suites, HSTS and PFS. For more information, see:
Security aspects of DocuWare Cloud

1.1.6 Zertifizierungen und Normen

Über welche Zertifizierungen verfügt DocuWare Cloud?
DocuWare Cloud verfügt über alle relevanten Zertifizierungen, wie SOC-2-Typ-2, GoBD, ISO 27001, ISO 9001, GeBüV, und unterzieht sich regelmäßig einer Rezertifizierung. Alle Zertifizierungen von DocuWare Cloud finden Sie in dieser Liste:
DocuWare Zertifizierungen und Auszeichnungen
Darüber hinaus finden Sie alle Microsoft Azure-Zertifizierungen hier.

Inwieweit entspricht die DocuWare Cloud den BSI-Standards?

Microsoft Azure, die Infrastruktur, auf der die DocuWare Cloud läuft, entspricht dem „Cloud Computing-Konformitätskriterienkatalog" (C5) des BSI (Bundesamt für Sicherheit in der Informationstechnik).

1.2 Sicherheitsaspekte

1.2.1 Verschlüsselung

Werden sensible Daten im öffentlichen Netz verschlüsselt?
Ja. DocuWare Cloud nutzt TLS 1.2 (frühere Versionen sind nicht zulässig), sichere Cipher Suites, HSTS und PFS. Weitere Informationen finden Sie unter:
Sicherheitsaspekte von DocuWare Cloud

How is customer data encrypted at rest?
All documents saved in file cabinets are automatically encrypted using the AES (Advanced Encryption Standard) encryption process. AES is the successor to DES (Data Encryption Standard). AES is currently one of the most secure symmetric encryption processes. It is approved for use by the US government as the US encryption standard for documents with the highest security clearance level (Top secret) and meets the strictest security requirements.
An asymmetric key pair is generated for each file cabinet. The private key is used to encrypt the symmetric keys which are created when the documents in a file cabinet are encrypted. The private key for a file cabinet is, in turn, encrypted using a master key.
DocuWare relies on the use of AES with a key length of 256 bits for maximum protection when encrypting. A key length of 4096 bits is used for the encryption of symmetric keys. A new symmetric key is generated for each document.
'Bring your own key' (BYOK) scenarios are not supported.

What options are available in DocuWare to check the integrity of documents with a checksum?

Depending on their performance and security requirements, customers can choose between SHA-256 and SHA-512 for file cabinet configurations.

1.2.2 Access control

How do you handle role provisioning and deprovisioning?

Workflows for onboarding, department move and offboarding of Cloud Operatores are in place and they are reviewed regularly in the SOC 2 Type 2 audit.

Wie werden die Kundendaten im Ruhezustand verschlüsselt?
Alle in Archiven gespeicherten Dokumente werden automatisch mit dem AES-Verfahren (Advanced Encryption Standard) verschlüsselt.
AES ist der Nachfolger von DES (Data Encryption Standard). AES ist derzeit eines der sichersten symmetrischen Verschlüsselungsverfahren. Es ist von der US-Regierung als US-Verschlüsselungsstandard für Dokumente mit der höchsten Sicherheitsstufe (Top Secret) zugelassen und erfüllt die strengsten Sicherheitsanforderungen.
Für jedes Archiv wird ein asymmetrisches Schlüsselpaar generiert. Der private Schlüssel wird zur Verschlüsselung der symmetrischen Schlüssel verwendet, die bei der Verschlüsselung der Dokumente in einem Archiv erstellt werden. Der private Schlüssel für ein Archiv wird wiederum mit einem Hauptschlüssel verschlüsselt. DocuWare setzt bei der Verschlüsselung auf AES mit einer Schlüssellänge von 256 Bit für maximalen Schutz. Für die Verschlüsselung der symmetrischen Schlüssel wird eine Schlüssellänge von 4096 Bit verwendet. Für jedes Dokument wird ein neuer symmetrischer Schlüssel generiert.
„Bring your own key” (BYOK)-Szenarien werden nicht unterstützt.

Welche Optionen bietet DocuWare, um die Integrität von Dokumenten mit einer Prüfsumme zu checken?

Ihren Performance- und Sicherheitsanforderungen entsprechend können Kunden bei der Konfiguration ihrer Archive zwischen SHA-256 und SHA-512 wählen.

1.2.2 Zugangskontrolle

Wie handhaben Sie die Bereitstellung und Aufhebung von Rollen?

Es sind Workflows eingerichtet für die Einarbeitung, den Wechsel in eine andere Abteilung und das Ausscheiden von Cloud-Operatoren. Diese werden regelmäßig im Rahmen des SOC-2-Typ-2-Audits überprüft.

Do you regularly conduct auditing of user access and privileged access accounts? Yes. We set up controls and these are checked during every SOC 2 Type 2 audit.	**Führen Sie regelmäßig Audits des Benutzerzugangs und der Konten mit privilegiertem Zugang durch?** Ja. Wir haben Kontrollen eingerichtet, die bei jedem SOC 2 Typ 2-Audit überprüft werden.
How do you ensure that data is accessed only by those with absolute 'need to know' requirements? Regular audits and review processes are conducted. Cloud Operator's scope of access is determined by the requirements of their job function. SOC 2-controls specify and monitor the frequency of audits and reviews.	**Wie stellen Sie sicher, dass nur diejenigen auf die Daten zugreifen können, die sie unbedingt kennen müssen?** Es werden regelmäßig Audits und Überprüfungsprozesse durchgeführt. Der Umfang des Zugriffs des Cloud-Betreibers richtet sich nach den Anforderungen seiner Funktion. Die SOC-2-Kontrollen legen die Häufigkeit von Audits und Überprüfungen fest und überwachen sie.
Does DocuWare Cloud apply IP filtering ("whitelisting") or are there other security measures in place instead? Yes, you can opt for IP filtering. An organization admin can add specific IP addresses to an allow list via the central gateway settings.	**Wendet DocuWare Cloud IP-Filtering ("Whitelisting") an oder gibt es an dessen Stelle andere Sicherheitsmaßnahmen?** Ja, Sie können sich für IP-Filtering entscheiden. Ein Organisationsadministrator kann bestimmte IP-Adressen über die zentralen Gateway-Einstellungen zu einer Zulassungsliste hinzufügen.
What password management policy does DocuWare Cloud offer? Each DocuWare Cloud customer can define the password complexity in the DocuWare user administration: long and complex passwords, minimum number of 3 different character sets, minimum length of passwords, maximum number of logon failures. Lock duration and maximum password age can be defined. In addition, with combination of an SSO provider, usage of multi-factor-authentication (MFA) is also supported. For the complete recommendation on the password policy, refer to: White Paper DocuWare Cloud	**Welche Passwortverwaltungsrichtlinie bietet DocuWare Cloud?** Jeder DocuWare Cloud Kunde kann in der DocuWare Benutzerverwaltung die Komplexität der Passwörter festlegen: lange und komplexe Passwörter, mindestens 3 verschiedene Zeichensätze, Mindestlänge der Passwörter, maximale Anzahl fehlgeschlagener Anmeldeversuche. Die Sperrdauer und die maximale Gültigkeitsdauer von Passwörtern können ebenfalls festgelegt werden. In Kombination mit einem SSO-Anbieter wird außerdem die Verwendung einer Multi-Faktor-Authentifizierung (MFA) unterstützt. Die vollständigen Empfehlungen zur Passwortrichtlinie finden Sie unter: White Paper DocuWare Cloud

Do you enforce unique username and password? Yes. All logins to productive systems are performed by uniquely identifiable user accounts.	**Sind eindeutige Benutzernamen und Passwörter vorgeschrieben?** Ja. Alle Anmeldungen an Produktivsystemen erfolgen über eindeutig identifizierbare Benutzerkonten.
Which authentication mechanisms are in place for access to secure areas? The authentication mechanisms are explained here: Microsoft Azure Security documentation	**Welche Authentifizierungsmechanismen gibt es für den Zugang zu Sicherheitsbereichen?** Die Authentifizierungsmechanismen werden hier erläutert: Microsoft Azure-Sicherheitsdokumentation
Are group shared or generic accounts and passwords used? No.	**Werden gemeinsame oder generische Konten und Passwörter verwendet?** Nein.
Are passwords protected using hashing algorithms? Yes. PBKDF2 with salt and many thousands of iterations.	**Sind Passwörter durch Hash-Algorithmen geschützt?** Ja. PBKDF2 mit Salt und vielen tausend Iterationen.
What is the retention period for audit logs? At least 90 days for critical (internet facing or data reading or data changing) operations.	**Welche Aufbewahrungsfrist gilt für Audit-Protokolle?** Mindestens 90 Tage für kritische Operationen (internetexponiert oder Daten lesend oder Daten ändernd).
Are removable storage devices permitted in the data centers? No. See for example: Azure facilities, premises, and physical security	**Sind Wechseldatenträger in den Rechenzentren erlaubt?** Nein. Siehe zum Beispiel: Azure-Einrichtungen, Räumlichkeiten und physische Sicherheit
1.2.3 Intrusion detection	**1.2.3 Erkennung von unbefugtem Eindringen**
What are your solutions for intrusion detection (IDS) or intrusion prevention (IPS)? Cloud-ready IDS and IPS are in place. In addition to the existing Microsoft security alerts, DocuWare has added its own security alerts.	**Was sind Ihre Lösungen für Intrusion Detection (IDS) oder Intrusion Prevention (IPS)?** Cloud-fähige IDS und IPS sind vorhanden. Zusätzlich zu den bestehenden Microsoft-Sicherheitsalarmen hat DocuWare seine eigenen Sicherheitsalarme hinzugefügt.

How do you manage and monitor security alerts from IDS/IPS? Active alerting of two separate 24x7 standby teams. Urgency handling process is in place.	**Wie können Sie Sicherheitswarnungen von IDS/IPS verwalten und überwachen?** Zwei separate 24/7-Bereitschaftsdienste werden aktiv alarmiert. Es gibt ein Verfahren zur Behandlung von Dringlichkeitsfällen.
How are system configuration checking tools utilized and maintained? DocuWare uses cloud security tools to measure infrastructure security. This is tracked and measured as an enterprise-level KPI. Desired State Configuration (DSC) is used for critical resources. Alerting about deviations is in place.	**Wie werden die Werkzeuge zur Überprüfung der Systemkonfiguration eingesetzt und gewartet?** DocuWare nutzt Cloud-Sicherheitstools, um die Sicherheit der Infrastruktur zu messen. Dies wird als KPI auf Unternehmensebene verfolgt und gemessen. Für kritische Ressourcen wird die Desired State Configuration (DSC) verwendet. Es gibt ein Verfahren zu Warnmeldungen über Abweichungen.
What is the process in place to update the antivirus signatures? Automated and very timely rollout of anti-virus signatures is in place. DocuWare has added custom alerts for virus alerts in customer documents to the 24x7 standby teams.	**Nach welchem Verfahren werden die Antivirensignaturen aktualisiert?** Die Antiviren-Signaturen werden automatisch und sehr zeitnah bereitgestellt. DocuWare hat den 24/7-Bereitschaftsdienst um benutzerdefinierte Warnungen für Virenwarnungen in Kundendokumenten erweitert.
1.2.4 Distributed Denial of Service (DDOS) attacks	**1.2.4 Verteilte Denial-of-Service-Angriffe (DDOS)**
What is the protection against Distributed Denial of Service (DDOS) attacks? It is Microsoft Azure DDoS protection, see the documentation: Microsoft Azure DDoS protection	**Welchen Schutz gibt es gegen Distributed Denial of Service (DDOS)-Angriffe?** Es handelt sich dabei um den Microsoft Azure DDoS-Schutz, siehe die Dokumentation: Microsoft Azure DDoS-Schutz

1.2.5 Network access control
How is the DocuWare Cloud network protected and traffic limited to what is required to deliver the service? Services provided to the customer are routed through Application Gateways with Web Application Firewall (WAF) and activated OWASP rules. TLS 1.2 is enforced. Internal Azure resources are limited to internal protected networks (e.g., using virtual networks, network security groups and firewalls) and are not accessible from the internet.
Is the firewall configured to hide internal IP addresses, using network address translation? Yes. Cloud-internal IP addresses are not exposed.
Are firewalls or security technology in place to separate the cloud network from other parts of public cloud environment or from the internet? Yes. DocuWare is using virtual networks, network security groups, and/or IP address restrictions.
How are changes to the firewall handled? Changes are tracked and confirmed internally using so-called "Operational Issues" according to SOC 2 Type 2. Desired state configuration is verified by automated tools to quickly detect deviations.

1.2.5 Netzwerkzugangskontrolle
Wie wird das DocuWare Cloud Netzwerk geschützt und der Datenverkehr auf das für die Bereitstellung des Dienstes erforderliche Maß beschränkt? Die dem Kunden zur Verfügung gestellten Dienste werden über Application Gateways mit Web Application Firewall (WAF) und aktivierten OWASP-Regeln geroutet. TLS 1.2 wird erzwungen. Interne Azure-Ressourcen sind auf interne geschützte Netzwerke beschränkt (z. B. unter Verwendung von virtuellen Netzwerken, Netzwerksicherheitsgruppen und Firewalls) und sind nicht über das Internet zugänglich.
Ist die Firewall so konfiguriert, dass sie interne IP-Adressen mithilfe von Netzwerkadressübersetzung verbirgt? Ja. Cloud-interne IP-Adressen werden nicht offengelegt.
Sind Firewalls oder Sicherheitstechnologien vorhanden, um das Cloud-Netz von anderen Teilen der öffentlichen Cloud-Umgebung oder vom Internet zu trennen? Ja. DocuWare verwendet virtuelle Netzwerke, Netzwerksicherheitsgruppen und/oder IP-Adressbeschränkungen.
Wie werden Änderungen an der Firewall gehandhabt? Änderungen werden intern anhand so genannter „Operational Issues“ gemäß SOC-2-Typ-2 nachverfolgt und bestätigt. Die Konfiguration des Soll-Zustands wird durch automatisierte Tools überprüft, um Abweichungen schnell zu erkennen.

What is DocuWare's patch management policy? DocuWare uses staged rolling updates of virtual machine scale sets, one after another without downtime for the customers for minor updates. The operating system is also updated frequently and transparently for the customer.	**Wie sieht die Patch-Management-Richtlinie von DocuWare aus?** DocuWare verwendet stufenweise rollierende Updates für virtuelle Maschinenverbünde, ohne Ausfallzeiten für die Kunden bei kleineren Updates. Auch das Betriebssystem wird häufig und für den Kunden transparent aktualisiert.
Do you permit remote access to your network? Yes, but only for selected Cloud Operations team members from dedicated secured networks. Access is protected by VPN.	**Gestatten Sie den Fernzugriff auf Ihr Netzwerk?** Ja, aber nur für ausgewählte Mitglieder des Cloud-Operations-Teams aus speziell gesicherten Netzen. Der Zugang ist durch VPN geschützt.
Are remote access user activities captured in activity logs? Yes. All remote access actions are recorded in audit logfiles.	**Werden die Aktivitäten von Fernzugriffsbenutzern in Aktivitätsprotokollen erfasst?** Ja. Alle Fernzugriffsaktionen werden in Audit-Protokolldateien aufgezeichnet.
What kind of anti-virus/anti-malware software is used? Microsoft cloud-ready security solutions are installed and updated in an automated and timely manner.	**Welche Art von Antiviren-/Antimalware-Software wird verwendet?** Cloud-fähige Sicherheitslösungen von Microsoft werden automatisch und zeitnah installiert und aktualisiert.
Do you review remote access users? Yes. According to SOC 2 Type 2 controls in place. Remote access users are reviewed periodically to ensure access is still authorized.	**Überprüfen Sie Benutzer mit Fernzugriff?** Ja. Gemäß SOC-2-Typ-2 sind Kontrollen vorhanden. Fernzugriffsbenutzer werden regelmäßig überprüft, um sicherzustellen, dass der Zugriff weiterhin zulässig ist.

1.2.6 Physical security	1.2.6 Physische Sicherheit
How does your company address social engineering attempts and thwarting? We counteract these threats by regularly conducting security awareness trainings. Phishing simulations are run about 12 times a year.	**Wie geht Ihr Unternehmen mit Social-Engineering-Versuchen und deren Vereitelung um?** Wir wirken diesen Bedrohungen entgegen, indem wir regelmäßig Schulungen zum Thema Sicherheit durchführen. Phishing-Simulationen werden etwa zwölfmal pro Jahr durchgeführt.
Do you secure access to your productive computing centers? The Microsoft Azure data centers have a very high security level and have received many certifications. Access for Cloud Operations (DevOps) teams to cloud resources is secured by IP restrictions, VPN access, MFA and auditing. For more information, see: https://learn.microsoft.com/en-us/azure/compliance/	**Sichern Sie den Zugang zu Ihren produktiven Rechenzentren?** Die Microsoft Azure-Rechenzentren verfügen über ein sehr hohes Sicherheitsniveau und haben zahlreiche Zertifizierungen erhalten. Der Zugriff von Cloud Operations (DevOps)-Teams auf Cloud-Ressourcen wird durch IP-Beschränkungen, VPN-Zugang, MFA und Auditing gesichert. Weitere Informationen: https://learn.microsoft.com/de-de/azure/compliance/
What is the visitor policy in the Microsoft Azure data centers? Microsoft Azure data centers have a very high physical access security, you can find more information here: Datacenter physical access security	**Was ist die Besucherrichtlinie in den Microsoft Azure-Rechenzentren?** Die Microsoft Azure-Rechenzentren haben eine sehr hohe physische Zugangssicherheit, weitere Informationen finden Sie hier: Datacenter physical access security
What controls are in place to prevent an unauthorized access or damage to network, power or telecommunications cabling? In the Microsoft Azure data centers, there is full protection by Microsoft, see their Datacenter security overview	**Welche Kontrollen gibt es, um unbefugten Zugriff auf oder Schäden an Netzwerk-, Strom- oder Telekommunikationskabeln zu verhindern?** In den Microsoft Azure-Rechenzentren besteht ein vollständiger Schutz durch Microsoft, siehe deren Datencenter-Sicherheitsüberblick
What is your screen lockout policy and how is it enforced? After 15 minutes of inactivity, the screen of any device that has entered a DocuWare domain is locked automatically. This is enforced by the Microsoft group policy.	**Wie lautet Ihre Richtlinie zur Bildschirmsperre und wie wird sie durchgesetzt?** Nach 15 Minuten Inaktivität wird der Bildschirm eines Gerätes, das sich in einer DocuWare Domäne angemeldet hat, automatisch gesperrt. Dies wird durch die Microsoft-Gruppenrichtlinie erzwungen.

1.3 Cloud processes

1.3.1 Policies and procedures

Do you maintain policies and procedures for the services provided by DocuWare Cloud?
Yes. SOC 2 Type 2 controls for securely operating cloud services are in place and audited.

How is the review and update process set up?

The review process is in accordance with the requirements of SOC 2 Type 2 controls: it consists of a yearly review by the author of the policies, processes and working instructions and a supervisor. The policies, processes and working instructions are signed into effect by management.

How are policies published to relevant users?

The policies are published using notifications in the DocuWare inhouse system and in the inhouse Atlassian Confluence system, trainings for relevant policies, processes, working instructions and Microsoft Teams posts.
Acknowledgement of policies, processes, working instructions is confirmed in a DocuWare workflow via electronic signature.

1.3 Cloud-Prozesse

1.3.1 Richtlinien und Verfahren

Haben Sie Richtlinien und Verfahren für die von DocuWare Cloud bereitgestellten Dienste?
Ja. SOC-2-Typ-2-Kontrollen für den sicheren Betrieb von Cloud-Diensten sind vorhanden und werden geprüft.

Wie ist das Überprüfungs- und Aktualisierungsverfahren aufgebaut?

Das Prüfverfahren entspricht den Anforderungen der SOC 2 Typ 2-Kontrollen: Es besteht aus einer jährlichen Überprüfung der Richtlinien, Prozesse und Arbeitsanweisungen durch den/die Verfasser/in und eine/n Vorgesetzten. Die Richtlinien, Prozesse und Arbeitsanweisungen werden von der Geschäftsleitung per Unterzeichnung in Kraft gesetzt.

Wie werden die Richtlinien für die betroffenen Nutzer veröffentlicht?

Die Veröffentlichung der Richtlinien erfolgt über Benachrichtigungen im DocuWare Inhouse-System und im hauseigenen Atlassian Confluence-System, Schulungen für relevante SOPs und Microsoft Teams-Posts.
Die Anerkennung von SOPs wird in einem DocuWare Workflow per elektronischer Unterschrift bestätigt.

1.3.2 Software development process	1.3.2 Software-Entwicklungsprozess
What is your Quality Assurance (QA) process? Our software development manual describes our SDLC (Software Development Lifecycle) in detail on more than 50 pages and must be signed and followed by every developer. A variety of tests are performed for single units, integrations and the system, using automation and other tools to detect new issues, prevent regressions and hence contribute to a quality product. Release pipelines include automatic quality checks and rollout to production requires a personal release decision by QA. QA reports to management once a month. DocuWare is certified for ISO 9001.	**Wie sieht Ihr Verfahren zur Qualitätssicherung (QA) aus?** Unser Handbuch zur Softwareentwicklung beschreibt unseren SDLC (Software Development Lifecycle) ausführlich auf mehr als 50 Seiten und muss von jedem Entwickler und jeder Entwicklerin unterschrieben und befolgt werden. Es werden unterschiedlichste Tests für einzelne Einheiten, Integrationen und das System durchgeführt. Dabei kommen Automatisierungen und andere Tools zum Einsatz, um neue Probleme zu erkennen, Rückschritte zu verhindern und somit zu einem qualitativ hochwertigen Produkt beizutragen. Die Release-Pipelines umfassen automatische Qualitätsprüfungen, und die Übergabe an die Produktion erfordert eine persönliche Freigabeentscheidung durch die QA. Die QA erstattet der Geschäftsleitung einmal im Monat Bericht. DocuWare ist nach ISO 9001 zertifiziert.
How do you train developers? The Engineering department has a dedicated architecture guild, a DevOps guild and many more. Technical knowledge is shared in technical presentations with other teams. Security trainings take place once a year.	**Wie schulen Sie Entwickler?** Die technische Abteilung hat eine eigene Architektengilde, eine DevOps-Gilde und viele mehr. Technisches Wissen wird in technischen Präsentationen mit anderen Teams geteilt. Es finden jährliche Sicherheitsschulungen statt.
Is a staging / pre-production system used to validate build artifacts before promotion to production? Yes, fully automated CI/CD pipelines are used to deploy and test new versions of containers in test systems automatically. Only versions tested and approved by QA are marked as release candidates to production systems.	**Wird ein Staging-/Vorproduktionssystem verwendet, um Build-Artefakte vor der Übergabe an die Produktion zu validieren?** Ja, vollautomatische CI/CD-Pipelines werden verwendet, um neue Versionen von Containern in Testsystemen automatisch bereitzustellen und zu testen. Nur von der Qualitätssicherung getestete und genehmigte Versionen werden als Freigabekandidaten für Produktionssysteme gekennzeichnet.

What types of security reviews do you perform on third party / open source software (OSS)?
We use a third-party security tool, which is scanning and alerting (about new vulnerabilities).
Policies are in place for allowed licenses and vulnerability levels.
We have a third-party software-approval process that needs to be passed before using new third-party software.

1.3.3 Vulnerability management

How does DocuWare ensure that product vulnerabilities are properly identified, tracked, and remediated?
We use a special solution to detect vulnerabilities in third-party and open source software, which alerts us to existing vulnerabilities in external software libraries that developers may wish to use. The solution also alerts us to newly discovered vulnerabilities in libraries already in use.
We run threat models, static analysis and security reviews. Penetration tests are performed regularly by external security companies. We are monitoring our productive systems and alert on new vulnerabilities detected.
Furthermore, we use a variety of information sources to keep us informed about current CVEs. Based on this and on internal and external audits, we perform regular risk analyses to ensure that vulnerabilities are properly identified, tracked, and remediated.

Welche Arten von Sicherheitsüberprüfungen führen Sie bei Drittanbieter-/Open-Source-Software (OSS) durch?
Wir verwenden ein Sicherheitstool eines Drittanbieters namens Mend, das Scans und Warnungen (über neue Sicherheitslücken) ausgibt.
Es gibt Richtlinien für zulässige Lizenzen und Schwachstellengrade.
Wir haben ein Genehmigungsverfahren für Software von Drittanbietern, das vor der Verwendung neuer Software von Drittanbietern durchlaufen werden muss.

1.3.3 Schwachstellen-Management

Wie stellt DocuWare sicher, dass Sicherheitslücken in Produkten korrekt identifiziert, verfolgt und behoben werden?
Wir verwenden eine spezielle Lösung zum Aufspüren von Schwachstellen in Drittanbieter- und Open-Source-Software. Diese weist uns auf bestehende Schwachstellen in externen Softwarebibliotheken hin, die Entwickler möglicherweise verwenden möchten. Die Lösung warnt uns auch vor neu entdeckten Schwachstellen in bereits genutzten Bibliotheken. Darüber hinaus warnt die Lösung vor neu entdeckten Sicherheitslücken in bereits verwendeten Bibliotheken.
Wir nutzen Bedrohungsmodelle und nehmen statische Analysen und Sicherheitsüberprüfungen vor. Penetrationstests werden regelmäßig von externen Sicherheitsunternehmen durchgeführt. Wir überwachen unsere produktiven Systeme und melden neu entdeckte Schwachstellen.
Zudem nutzen wir eine Vielzahl von Informationsquellen, um uns über aktuelle CVEs zu informieren. Auf dieser Grundlage sowie auf der von internen und externen Prüfungen führen wir regelmäßig Risikoanalysen durch, um sicherzustellen, dass Schwachstellen ordnungsgemäß ermittelt, verfolgt und behoben werden.

How often do you perform penetration tests, security reviews, and vulnerability assessments? Penetration tests are performed by external companies at least once a year. SOC 2 Type 2 and ISO 27001 auditors review the two latest reports during their audits every year and are thus reviewing DocuWare's reaction to and handling of potential findings. Vulnerability assessments: once per month Security reviews: before going live of new services or major features.	**Wie oft führen Sie Penetrationstests, Sicherheitsüberprüfungen und Schwachstellenanalysen durch?** Penetrationstests werden von externen Unternehmen mindestens einmal im Jahr durchgeführt. Die SOC-2-Typ-2-Auditoren und die ISO-27001-Auditoren überprüfen jedes Jahr die beiden letzten Berichte im Rahmen ihrer Audits und überprüfen damit die Reaktion von DocuWare auf potenzielle Feststellungen und deren Bearbeitung. Schwachstellenanalysen: einmal pro Monat Sicherheitsüberprüfungen: vor der Inbetriebnahme neuer Dienste oder wichtiger Funktionen.
Is it possible to view the penetration test results? Redacted penetration test reports can be obtained after signing an NDA.	**Ist es möglich, die Ergebnisse des Penetrationstests einzusehen?** Redigierte Penetrationstest-Berichte können nach Unterzeichnung einer Vertraulichkeitsvereinbarung angefordert werden.
Can we perform penetration testing on systems owned or operated by DocuWare? No, DocuWare does not allow penetration testing to be performed on those systems. It could influence the performance for other customers.	**Können wir Penetrationstests auf Systemen durchführen, die DocuWare gehören oder von ihr betrieben werden?** Nein, DocuWare erlaubt keine Penetrationstests auf diesen Systemen. Dies könnte die Leistung für andere Kunden beeinträchtigen.

How do you resolve critical findings in security tests?
Security bugs get a prioritization according to CVSS 3.1. The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of software and hardware security vulnerabilities.
When priority is greater or equal to 7.0 (High or Critical), a security bug of priority 1 will be created.
Any priority 1 bug (normal or security) will be handled very fast: start fixing this finding within an escalation process.
“Meantime to repair” for such bugs is tracked as a KPI with top management visibility.
Rollout of such fixes as minor hotfix patch to DocuWare Cloud can be performed without any downtime for any customer.

Wie beheben Sie kritische Befunde bei Sicherheitstests?
Sicherheitslücken werden nach CVSS 3.1 priorisiert. Das Common Vulnerability Scoring System (CVSS) bietet einen offenen Rahmen für die Kommunikation der Merkmale und Auswirkungen von Sicherheitslücken in Software und Hardware.
Wenn die Priorität größer oder gleich 7.0 (Hoch oder Kritisch) ist, wird ein Sicherheitsfehler der Priorität 1 erstellt.
Jeder Fehler der Priorität 1 (normal oder Sicherheit) wird sehr schnell behandelt: Beginnen Sie mit der Behebung dieses Fehlers im Rahmen eines Eskalationsprozesses.
Die „durchschnittliche Reparaturzeit" für solche Fehler wird als KPI mit Sichtbarkeit für das Top-Management verfolgt.
Der Rollout von Korrekturen wie Minor-Hotfix-Patches auf DocuWare Cloud kann ohne Ausfallzeiten für den Kunden durchgeführt werden.

1.3.4 Protection from malware

Antivirus and anti-malware protection
Microsoft cloud-ready security solutions are installed and updated in an automated and timely manner.

Cloud security measures
Microsoft Defender for Cloud alerts about cyber security issues or configuration problems out of the box.
DocuWare has added its own alerts to the 24x7 standby teams.
In critical cases, DocuWare customer support is actively informing about infected documents the customer was trying to upload (to prevent damage on customer side). More information:

Microsoft Defender for Cloud

1.3.4 Schutz vor Malware

Antivirus- und Anti-Malware-Schutz
Cloud-fähige Sicherheitslösungen von Microsoft werden automatisch und zeitnah installiert und aktualisiert.

Sicherheitsmaßnahmen in der Cloud
Microsoft Defender for Cloud warnt standardmäßig vor Cyber-Sicherheitsproblemen oder Konfigurationsproblemen.
DocuWare hat den 24/7-Bereitschaftsdienst um spezielle Sicherheitsalarme erweitert.
In kritischen Fällen informiert der DocuWare Kundensupport aktiv über infizierte Dokumente, die der Kunde hochzuladen versucht hat (um Schaden auf Kundenseite zu verhindern). Weitere Informationen:

Microsoft Defender for Cloud

Behavioral analysis alerting
Microsoft Defender for Cloud is leveraging AI mechanisms and behavioral analysis to e.g.,
– warn about users acting from new locations
– warn about users accessing cloud resources not accessed previously
– warn about “impossible travel” situations
(e.g., a user logs on from Berlin and 5 minutes later from Buenos Aires)

1.3.5 Backup and Restore

What is DocuWare’s general backup and restore policy?

DocuWare Cloud always stores 6 copies of the data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters.
For more information, see:
Cloud storage – you get more than what you see

Verhaltensanalyse-Warnung
Microsoft Defender for Cloud nutzt KI-Mechanismen und Verhaltensanalysen, um z. B.:
– vor Benutzern zu warnen, die von neuen Standorten aus agieren
– vor Benutzern zu warnen, die auf Cloud-Ressourcen zugreifen, auf die sie zuvor nicht zugegriffen haben
– vor „Impossible Travel”-Situationen zu warnen
(z. B. meldet sich ein Nutzer aus Berlin und 5 Minuten später aus Buenos Aires an)

1.3.5 Backup und Wiederherstellen

Wie sieht die allgemeine Sicherungs- und Backup-Richtlinie von DocuWare aus?
DocuWare Cloud speichert immer 6 Kopien der Daten, sodass sie vor geplanten und ungeplanten Ereignissen wie vorübergehenden Hardware-Ausfällen, Netzwerk- oder Stromausfällen und massiven Naturkatastrophen geschützt sind.
Weitere Informationen finden Sie hier:
Cloud-Speicher – Sie bekommen mehr als das, was Sie sehen

What is the backup and restore policy regarding documents and data?

With the backup strategy included in DocuWare Cloud, DocuWare enables recovery of documents and metadata to protect the customer's business now and in the future.

Documents: Deleted documents can be restored independently by the customer via the trash bin within 30 days. If this period has elapsed, the procedure outlined below for restoring from backups is used.

In addition to the redundant copies of the encrypted productive data mentioned in the data security section, an additional copy is made and stored in a continuous backup. This happens shortly after the document has been stored or modified in DocuWare. The backup after document modification creates a new copy of the document. This is saved in addition to existing backups of the document. This always applies, regardless of whether document versioning is enabled or disabled in DocuWare. The advantage of enabled document versioning is that the customer can access older document versions directly in DocuWare. Restoring a previous document version follows the same rules as document recovery, see below.

Wie sieht die Sicherungs- und Backup-Richtlinie für Dokumente und Daten aus?

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

Dokumente: Gelöschte Dokumente können vom Kunden innerhalb von 30 Tagen selbständig über den Papierkorb wiederhergestellt werden. Ist diese Zeitspanne verstrichen, wird das unten beschriebene Verfahren zur Wiederherstellung aus Backups angewendet.

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. Beim Backup nach Dokumentveränderung wird eine neue Kopie des Dokuments erstellt. Diese wird zusätzlich zu bereits vorhandenen Backups des Dokuments gespeichert. Dies gilt immer, also sowohl bei aktivierter als auch bei nicht aktivierter Dokumentversionierung in DocuWare. Der Vorteil der aktivierten Dokumentenversionierung ist, dass der Kunde direkt in DocuWare auf ältere Dokumentenversionen zugreifen kann. Die Wiederherstellung einer früheren Version eines Dokuments erfolgt nach denselben Regeln wie die Wiederherstellung von Dokumenten, siehe unten.

Metadata: Full database backups of the metadata happen every week, differential backups every 12 to 24 hours, and transaction log backups every 5 to 10 minutes. The frequency of transaction log backups is based on the compute size and the amount of database activity. You can find more information on https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview	**Metadaten:** Vollständige Datenbanksicherungen der Metadaten erfolgen jede Woche, differenzielle Sicherungen alle 12 bis 24 Stunden und Transaktionsprotokollsicherungen alle 5 bis 10 Minuten. Die Häufigkeit der Backups des Transaktionsprotokolls hängt von der Größe des Rechners und der Menge der Datenbankaktivitäten ab. Mehr Informationen finden Sie hier: https://docs.microsoft.com/en-us/azure/azure-sql/database/automated-backups-overview
Cold Storage: To enable a recovery, DocuWare backs up both the metadata and the documents in a separate cold storage. This cold storage is located in a Microsoft data center within the respective region, currently in Amsterdam (Netherlands) for the EU, in Virginia (USA) for the Americas, in Osaka for Japan and in Victoria (Australia) for Australia and New Zealand. It is physically completely separated from the DocuWare domain(s) and is subject to extended security regulations, so that the data is also protected against possible damaging events in a DocuWare domain (e.g., cyberattacks). The full database backups of the metadata are carried out in the cold storage at weekends, usually during regional nighttime. The documents are backed up directly to cold storage. The generation of backups in the cold storage is automatically monitored continuously. Restore is tested according to SOC 2 Type 2 controls.	**Cold Storage:** Um eine Wiederherstellung zu ermöglichen, sichert DocuWare sowohl die Metadaten als auch die Dokumente in einem separaten Cold Storage. Der Cold Storage befindet sich in einem Microsoft-Rechenzentrum in der jeweiligen Region, derzeit in Amsterdam (Niederlande) für die EU, in Virginia (USA) für den amerikanischen Kontinent, in Osaka für Japan und in Victoria (Australien) für Australien und Neuseeland. Dieser ist physikalisch vollständig von der/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, in der Regel in der regionalen Nachtzeit, im Cold Storage durchgeführt. Die Dokumente werden direkt in einem Cold Storage gesichert. Das Generieren der Backups im Cold Storage wird durchgängig automatisch überwacht. Die Wiederherstellung wird gemäß den Kontrollen von SOC-2-Typ-2 getestet.

Recovery: Point in time restoration of documents is possible to any time within the retention period of 7 days. DocuWare requires the customer to provide information about when the document to be recovered was still accessible. The customer must send the request to DocuWare Support (https://support.docuware.com) no later than 5 days after deleting or modifying the document. Restoration of documents after 7 days must be checked in cooperation with DocuWare Support.
Documents and metadata can be restored to the state of any weekend within the retention period of 3 months or to the state of the first weekend of a month within the retention period of 12 months. After 12 months, documents and metadata can be restored to the state of the first weekend of any calendar year until contract termination.

Retention Period	Recovery	Inform DocuWare Support
Within 7 days	Point-in-time	No later than 5 days
Within 3 months	To state of any weekend	No later than 80 days
Within 12 months	To state of the 1st weekend of a month	No later than 350 days
Until contract termination	To state of the 1st weekend of a calendar year	No limitation or restriction

Wiederherstellung: Die Wiederherstellung von Dokumenten zu einem beliebigen Zeitpunkt innerhalb der Aufbewahrungsfrist von 7 Tagen ist möglich. DocuWare verlangt vom Kunden Angaben darüber, wann das wiederherzustellende Dokument noch zugänglich war. Der Kunde muss den Antrag spätestens 5 Tage nach dem Löschen oder Ändern des Dokuments an 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 auf den Stand eines beliebigen Wochenendes innerhalb der Aufbewahrungsfrist von 3 Monaten oder auf den Stand des ersten Wochenendes eines Monats innerhalb der Aufbewahrungsfrist von 12 Monaten wiederhergestellt werden. Nach 12 Monaten können die Dokumente und Metadaten bis zur Vertragsbeendigung auf den Stand des ersten Wochenendes eines jeden Kalenderjahres zurückgesetzt 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

What Recovery Time Objective (RTO) and Recovery Point Objective (RPO) does DocuWare Cloud provide in the event of a disaster recovery?
For the Recovery Time Objective (RTO) and Recovery Point Objective (RPO), see the
Microsoft Azure documentation

1.3.6 Logs and monitoring

How do you handle logs and monitoring?
All internet facing resources, data reading resources and data changing resources are configured to have audit logs enabled. The retention period for those log files is set to 90 days.

1.3.7 Incident response

Is a security incident response plan formally documented and published?
Yes. The process is documented and tested quarterly with relevant teams.

What is your security incident reporting procedure?

Our security incident reporting follows the SOC 2 Type 2 controls and guidelines.
Our so-called urgency handling process is open to every employee upon suspected incident and will alert our two 24x7 standby teams immediately.
Confirmed findings will be reported without undue delay to customers.

Welche Recovery Time Objective (RTO) und Recovery Point Objective (RPO) bietet DocuWare Cloud im Falle einer Wiederherstellung im Katastrophenfall?
Informationen zum Recovery Time Objective (RTO) und Recovery Point Objective (RPO) finden Sie in der
Microsoft Azure-Dokumentation

1.3.6 Protokolle und Überwachung

Wie gehen Sie mit Protokollen und Überwachung um?
Alle Ressourcen, die mit dem Internet verbunden sind, Ressourcen, die Daten lesen, und Ressourcen, die Daten ändern, sind so konfiguriert, dass Audit-Protokolle aktiviert sind. Die Aufbewahrungsfrist für diese Protokolldateien ist auf 90 Tage festgelegt.

1.3.7 Reaktion auf Vorfälle

Ist ein Plan zur Reaktion auf Sicherheitsvorfälle förmlich dokumentiert und veröffentlicht?
Ja. Der Prozess wird dokumentiert und vierteljährlich mit den zuständigen Teams getestet.

Wie sieht Ihr Verfahren zur Meldung von Sicherheitsvorfällen aus?

Unsere Berichterstattung über Sicherheitsvorfälle folgt den Kontrollen und Richtlinien der SOC 2 Typ 2.
Unser so genanntes Dringlichkeitsverfahren steht jedem Mitarbeiter bei einem vermuteten Vorfall offen und alarmiert sofort unsere beiden 24/7-Bereitschaftsdienste.
Bestätigte Vorfälle werden den Kunden unverzüglich mitgeteilt.

Has there been a data security breach at DocuWare? We had a few minor cases. We resolved the issues, tightened our IT security, and reported to the Data Protection Authority and the police – if required. We tend to report also minor cases to properly address the security needs of our customers.	**Gab es bei DocuWare eine Verletzung der Datensicherheit?** Wir hatten ein paar kleinere Fälle. Wir haben die Probleme gelöst, unsere IT-Sicherheit verschärft und die Datenschutzbehörde und die Polizei informiert – sofern erforderlich. Wir neigen dazu, auch kleinere Fälle zu melden, um den Sicherheitsbedürfnissen unserer Kunden gerecht zu werden.
How and when do you notify clients of a security incident? In case their data is affected, we inform customers via their email address without undue delay. For indirect sales where our customer is an Authorized DocuWare Partner (ADP), we will inform the ADP and it is the ADP's responsibility to inform the end customer.	**Wie und wann benachrichtigen Sie Ihre Kunden über einen Sicherheitsvorfall?** Falls ihre Daten betroffen sind, informieren wir die Kunden unverzüglich über ihre E-Mail-Adresse. Bei indirekten Verkäufen, bei denen unser Kunde ein Authorized DocuWare Partner (ADP) ist, informieren wir den ADP und es liegt in der Verantwortung des ADP, den Endkunden zu informieren.
Is the execution of Security Incident Response (SIR) responsibilities tested or practiced at least periodically? Yes. We are testing our critical incident process at least once every quarter with all relevant teams. This includes testing the 24x7 on call response.	**Wird die Ausführung der Verantwortlichkeiten für die Reaktion auf Sicherheitsvorfälle (Security Incident Response, SIR) zumindest regelmäßig getestet oder geübt?** Ja. Wir testen unseren Prozess für kritische Vorfälle mindestens einmal pro Quartal mit allen relevanten Teams. Dazu gehört auch die Prüfung der 24/7-Rufbereitschaft.
1.3.8 Asset management	**1.3.8 Asset-Management**
Do you have a company-wide asset management policy and procedures? Yes, according to SOC 2 Type 2 controls.	**Verfügen Sie über eine unternehmensweite Vermögensverwaltungsrichtlinie und -verfahren?** Ja, gemäß den Kontrollen nach SOC 2 Typ 2.
What procedures are in place for disposal of assets? Secure hardware handling is part of offboarding and cross-boarding workflows. Secure wiping of hard disks or SSDs is handled.	**Welche Verfahren gibt es für die Entsorgung von Assets?** Die sichere Handhabung von Hardware ist Teil der Offboarding- und Crossboarding-Workflows. Es erfolgt ein sicheres Löschen von Festplatten oder SSDs.

Is a routine assessment performed to detect unauthorized hardware / software? Yes. Automated alerting about new network devices is in place. Furthermore, a software inventory solution for corporate workstations and laptops is in place.	**Wird eine routinemäßige Bewertung durchgeführt, um nicht autorisierte Hardware/Software zu erkennen?** Ja. Es gibt eine automatische Warnung über neue Netzwerkgeräte. Darüber hinaus gibt es eine Software-Inventarisierungslösung für Unternehmens-Workstations und Laptops.
What additional procedures are applied when disposing of customer or client data? A deletion process is applied. The customer can export data as long as the contract is active. DocuWare Professional Services offers paid assistance to customers. Our team supports customers as they migrate live documents and documents integrated into current processes to a new system, which minimizes workflow interruptions. We develop solutions that are specifically tailored to customers' workflows and document types.	**Welche zusätzlichen Verfahren werden bei der Beseitigung von Kunden- oder Klientendaten angewandt?** Es wird ein Löschverfahren angewendet. Der Kunde kann Daten exportieren, solange der Vertrag aktiv ist. DocuWare Professional Services bietet Kunden kostenpflichtige Unterstützung dabei. Unser Team hilft Kunden bei der Migration von Live-Dokumenten und Dokumenten, die in aktuelle Prozesse integriert sind, in ein neues System, wodurch Unterbrechungen des Arbeitsablaufs minimiert werden. Wir entwickeln Lösungen, die speziell auf die Arbeitsabläufe und Dokumenttypen der Kunden zugeschnitten sind.

2 DocuWare – the organization

2.1 General

What is the background of your company?
You can find information on DocuWare's background at:
Digital Document Management Software | Workflow Automation | DocuWare

In what countries do you have offices?
All our offices can be found at:
DocuWare offices and locations

2 DocuWare – die Organisation

2.1 Allgemeine Informationen

Was ist der Hintergrund Ihres Unternehmens?
Informationen zum Hintergrund von DocuWare finden Sie unter:
Digitale Dokumentenmanagement-Software | Workflow-Automatisierung | DocuWare

In welchen Ländern haben Sie Niederlassungen?
Alle unsere Büros finden Sie unter:
DocuWare Büros und Standorte

What work is conducted in your international offices?

DocuWare GmbH is the German parent company providing administration of the cloud, product development, R&D services, marketing and all administrative services to the subsidiaries.
DocuWare Europe GmbH is the German subsidiary providing sales, support and professional services.
DocuWare Ltd. is the British subsidiary providing sales.
DocuWare SARL is the French subsidiary providing sales and professional services in France.
DocuWare SL is the Spanish subsidiary providing sales, professional services and support for Spain, Portugal and LATAM.
DocuWare Corp. is the US subsidiary providing sales, marketing, R&D services, support, professional services and all administrative services to the Americas.
natif.ai is a German subsidiary providing AI services.

Welche Arbeiten werden in Ihren internationalen Niederlassungen durchgeführt?

Die DocuWare GmbH ist die deutsche Muttergesellschaft, die den Tochtergesellschaften die Verwaltung der Cloud, die Produktentwicklung, die Forschungs- und Entwicklungsleistungen, das Marketing und alle administrativen Dienstleistungen zur Verfügung stellt.
Die DocuWare Europe GmbH ist die deutsche Tochtergesellschaft für Vertrieb, Support und Professional Services.
DocuWare Ltd. ist die britische Tochtergesellschaft, die den Vertrieb übernimmt.
DocuWare SARL ist die französische Tochtergesellschaft, die den Vertrieb und Professional Services in Frankreich anbietet.
DocuWare SL ist die spanische Tochtergesellschaft, die Vertrieb, Professional Services und Support für Spanien, Portugal und LATAM anbietet.
DocuWare Corp. ist die US-amerikanische Tochtergesellschaft, die den Vertrieb, das Marketing, die Forschung und Entwicklung, den Support, die Professional Services und alle administrativen Dienstleistungen für den amerikanischen Markt übernimmt.
natif.ai ist eine deutsche Tochtergesellschaft, die KI-Dienstleistungen anbietet.

Has your organization gone through an acquisition or merger in the last years? Yes. 2019: Acquisition of DocuWare by Ricoh. 2024: Acquisition of natif.ai by DocuWare. 2025: Integration of DocuScan into DocuWare Europe GmbH.	**Hat Ihre Organisation in den letzten Jahren eine Übernahme oder Fusion erlebt?** Ja. 2019: Übernahme von DocuWare durch Ricoh. 2024: Übernahme von natif.ai durch DocuWare. 2025: Eingliederung von DocuScan in die DocuWare Europe GmbH.
Does your organization have an appointed board of directors that is responsible for meeting regularly and discussing compliance and legal/regulatory requirements? Yes. The meetings are monthly and of a general nature.	**Verfügt Ihre Organisation über einen ernannten Vorstand, der dafür verantwortlich ist, regelmäßig zu tagen und die Einhaltung von Gesetzen und Vorschriften zu erörtern?** Ja. Die Sitzungen finden monatlich statt und sind allgemeiner Natur.
Does your organization have an internal audit, risk management, compliance department, or similar management oversight unit with responsibility for assessing, identifying and tracking resolution of outstanding regulatory issues? **If yes, please provide a description of the internal teams responsible for this oversight.** Yes, as part of ISO 27001 certification, internal audits are required. We have a compliance department and risk management processes. We do not share this kind of detailed information. Internal audit is conducted on a group level by Ricoh, all other subjects are handled within DocuWare.	**Verfügt Ihr Unternehmen über eine interne Revision, ein Risikomanagement, eine Compliance-Abteilung oder eine ähnliche Managementaufsichtseinheit, die für die Bewertung, Identifizierung und Verfolgung der Lösung offener regulatorischer Fragen zuständig ist?** **Wenn ja, beschreiben Sie bitte, welche internen Teams für diese Aufsicht zuständig sind.** Ja, im Rahmen der ISO-27001-Zertifizierung sind interne Revisionen erforderlich. Wir verfügen über eine Compliance-Abteilung und Risikomanagementverfahren. Wir geben diese Art von Informationen nicht weiter. Die interne Revision wird auf Konzernebene von Ricoh durchgeführt, alle anderen Themen werden innerhalb von DocuWare bearbeitet.

What is a SOC 2 Type 2 certification?
SOC 2 Type 2 is an extensive US IT security certification. A SOC 2 Type 2 report is an internal controls report capturing how a company safeguards customer data and how well those controls are operating. Companies that use cloud service providers use SOC 2 Type 2 reports to assess and address the risks associated with third party technology services.
The auditors are usually on site for two weeks every year and audit our technical and organizational security measures. The audit is conducted according to the latest SOC 2 Type 2 standard published by the AICPA. The audit period is a retrospective (!) of our previous fiscal year that lasts from 1 April to 31 March.
See also:

Information for service organization management published by AICPA

Why do you not share your internal policies?
As all of our internal guidelines contain some type of confidential information, we do not distribute them to partners and customers.

Was ist eine Zertifizierung nach SOC 2 Typ 2?
SOC 2 Typ 2 ist eine umfassende US-amerikanische IT-Sicherheitszertifizierung. Ein SOC-2-Bericht vom Typ 2 ist ein Bericht über die internen Kontrollen, in dem festgehalten wird, wie ein Unternehmen die Kundendaten schützt und wie gut diese Kontrollen funktionieren. Unternehmen, die Cloud-Service-Anbieter nutzen, verwenden Berichte nach SOC 2 Typ 2, um die mit den Technologiedienstleistungen Dritter verbundenen Risiken zu bewerten und anzugehen.
Die Auditoren sind in der Regel jedes Jahr zwei Wochen lang vor Ort und prüfen unsere technischen und organisatorischen Sicherheitsmaßnahmen. Die Prüfung erfolgt gemäß dem neuesten SOC 2 Typ 2-Standard, der vom AICPA veröffentlicht wurde. Der Prüfungszeitraum ist eine rückblickende (!) Prüfung unseres vorangegangenen Geschäftsjahres, das vom 1. April bis zum 31. März dauert.
Siehe auch:

Informationen für das Management von Dienstleistungsunternehmen, veröffentlicht vom AICPA

Warum machen Sie Ihre internen Richtlinien nicht öffentlich?
Da alle unsere internen Richtlinien eine Art von vertraulichen Informationen enthalten, geben wir sie nicht an Partner und Kunden weiter.

2.2 Data privacy compliance

2.2.1 General

Why is DocuWare focusing on GDPR?
GDPR is the most comprehensive data protection law we are aware of. It covers in many cases the requirements of other legislation but we can certainly not ignore them.

Is DocuWare also looking at other data protection legislation?

Of course we do. We are constantly analyzing the differences between the GDPR and the other legislation and if it does not cover necessary items, we additionally install processes that are relevant for other laws, like an additional data privacy website for the CCPA.

How does DocuWare keep up to date on legal developments?

We are member of the Bitkom, the German trade association for digital industry and the BCM, the German trade association of compliance managers. As for the US, we follow the advice of our external legal counsel.
We also constantly evaluate the entire range of specialist media and publications and analyze all relevant information.
We have an internal Data Protection Officer (DPO).
We have an internal Compliance Manager.

Contact details of our Data Protection Officer

2.2 Einhaltung des Datenschutzes

2.2.1 Allgemeines

Warum konzentriert sich DocuWare auf die DSGVO?
Die DSGVO ist das umfassendste Datenschutzgesetz, das uns bekannt ist. Sie deckt in vielen Fällen die Anforderungen anderer Rechtsvorschriften ab, aber wir können sie selbstverständlich nicht ignorieren.

Befasst sich DocuWare auch mit anderen Datenschutzgesetzen?

Selbstverständlich tun wir das. Wir analysieren ständig die Unterschiede zwischen der DSGVO und anderen Gesetzen, und wenn sie notwendige Punkte nicht abdeckt, richten wir zusätzlich Prozesse ein, die für andere Gesetze relevant sind, wie eine zusätzliche Datenschutz-Website für das CCPA.

Wie hält sich DocuWare über rechtliche Entwicklungen auf dem Laufenden?
Wir sind Mitglied im Bitkom, dem Bundesverband der Digitalen Wirtschaft, und im BCM, dem Berufsverband der Compliance Manager.
Was die USA betrifft, so folgen wir dem Rat unseres externen Rechtsberaters.
Darüber hinaus werten wir ständig das gesamte Spektrum der Fachmedien und Publikationen aus und analysieren alle relevanten Informationen.
Wir haben einen internen Datenschutzbeauftragten (DSB).
Wir haben einen internen Compliance Manager.

Kontaktinformationen unseres Datenschutzbeauftragten

How do you ensure your operations are aligned with the regulatory and legal requirements in the countries where you conduct offices as it relates to data handling, processing, and protection? We have local legal advisors.	**Wie stellen Sie sicher, dass Ihre Tätigkeiten mit den rechtlichen und regulatorischen Anforderungen in den Ländern, in denen Sie Niederlassungen betreiben, in Bezug auf die Handhabung, die Verarbeitung und den Schutz von Daten in Einklang stehen?** Wir haben lokale Rechtsberater.
Do you promptly notify customers affected by a security breach? Yes, we do in accordance with applicable law.	**Benachrichtigen Sie die von einer Sicherheitsverletzung betroffenen Kunden umgehend?** Ja, das tun wir in Übereinstimmung mit dem geltenden Recht.
Do you keep a record of personal data breaches? Yes. If there were any, the list is reviewed yearly as part of the SOC 2 Type 2 controls.	**Führen Sie Aufzeichnungen über Verletzungen des Schutzes personenbezogener Daten?** Ja. Wenn es solche Verletzungen gab, wird die Liste jährlich im Rahmen der SOC-2-Typ-2-Kontrollen überprüft.
2.2.2 Internal organizational measures for data protection	**2.2.2 Interne organisatorische Maßnahmen für den Datenschutz**
What are DocuWare's internal organizational measures? DocuWare takes the following internal organizational measures for data protection: – SOP on Data Privacy (see here below) – Information Security Policy for End Users (see 2.5 Security of corporate) – Records of data processing activities – Data protection training – Confidentiality agreements for employees – Privacy and cookie policy	**Was sind die internen organisatorischen Maßnahmen von DocuWare?** DocuWare ergreift die folgenden internen organisatorischen Maßnahmen zum Datenschutz: – SOP zum Datenschutz (siehe weiter unten) – Informationssicherheitsrichtlinien für Endnutzer (siehe 2.5 Security of corporate) – Verzeichnis von Verarbeitungstätigkeiten – Schulung zum Datenschutz – Vertraulichkeitsvereinbarungen für Mitarbeiter – Datenschutz und Cookie-Richtlinie

What does the SOP on Data Privacy cover?
The SOP on Data Privacy includes all the requirements of the European General Data Protection Regulation (GDPR) and the resulting processes and measures, as well as those of the new Swiss Federal Act on Data Protection (FADP).
Main subjects in the field of data protection are:
Theoretical background of applicable law:
– Handling of personal data
– Rights of data subjects/California residents
– Concepts of data processing
– Data breaches
– Sanctioning
– International data transfers
DocuWare implementation:
– Reporting processes
– Data processing agreements
– Trainings
– Internal responsibilities and the data protection officer
– International data transfers

As all of our internal guidelines contain some type of confidential information, we do not distribute them to partners and customers. For general information on DocuWare Cloud Services security, you can refer to the other chapters of this document covering this subject in greater detail.
All our SOPs are subject to a regular review and update, at least on a yearly basis as required by SOC 2 Type 2 certification.

What do the penetration tests cover?
See chapter "DocuWare - the product", section 1.3.3 Vulnerability management.

Was deckt das SOP zum Datenschutz ab?
Die SOP zum Datenschutz umfasst alle Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) und die daraus resultierenden Prozesse und Maßnahmen sowie diejenigen des neuen Schweizer Datenschutzgesetzes (FADP).
Die wichtigsten Themen im Bereich des Datenschutzes sind:
Theoretischer Hintergrund des geltenden Rechts:
– Umgang mit personenbezogenen Daten
– Rechte der betroffenen Personen / in Kalifornien ansässigen Personen
– Konzepte der Datenverarbeitung
– Datenschutzverletzungen
– Sanktionierung
– Internationale Datenübermittlung
DocuWare Implementierung:
– Verfahren zur Berichterstattung
– Vereinbarungen zur Datenverarbeitung
– Schulungen
– Interne Zuständigkeiten und der Datenschutzbeauftragte
– Internationale Datenübermittlung

Da alle unsere internen Richtlinien eine Art von vertraulichen Informationen enthalten, geben wir sie nicht an Partner und Kunden weiter. Allgemeine Informationen zur Sicherheit der DocuWare Cloud Services finden Sie in den anderen Kapiteln dieses Dokuments, in denen dieses Thema ausführlicher behandelt wird.
Alle unsere SOPs werden regelmäßig überprüft und aktualisiert, mindestens einmal im Jahr, wie es die SOC-2-Typ-2-Zertifizierung verlangt.

Worauf beziehen sich die Penetrationstests?
Siehe Kapitel "DocuWare - das Produkt", Abschnitt 1.3.3 Schwachstellen-Management.

What are the Records of Data processing Activities (RPA)? GDPR requires companies to create so-called records of data processing activities to document how data flows through the company. These records include, e.g., a description of the IT systems used, the departments and external companies that receive the data, the legal basis for date processing and information about data processing agreements in place. We have created records of data processing activities for all our internal processing operations. Like our SOPs, the records of data processing activities are updated on an annual basis. For DocuWare Cloud Services, we do not offer a standardized template for customers, because the configurations are individually tailored to each customer's needs. Furthermore, there might be additional process steps taken outside DocuWare Cloud which we cannot know of.	**Was ist das "Verzeichnis von Verarbeitungstätigkeiten"?** Die DSGVO verlangt von Unternehmen, dass sie ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten erstellen, um zu dokumentieren, wie die Daten durch das Unternehmen fließen. Diese Aufzeichnungen enthalten z. B. eine Beschreibung der verwendeten IT-Systeme, der Abteilungen und externen Unternehmen, die die Daten erhalten, die Rechtsgrundlage für die Datenverarbeitung und Informationen über bestehende Datenverarbeitungsverträge. Für alle unsere internen Verarbeitungen haben wir ein Verzeichnis von Verarbeitungstätigkeiten erstellt. Wie unsere SOPs wird auch das Verzeichnis von Verarbeitungstätigkeiten jährlich aktualisiert. Für die DocuWare Cloud Services bieten wir kein standardisiertes Template für Kunden an, da die Konfigurationen individuell auf die Bedürfnisse des Kunden zugeschnitten sind. Darüber hinaus kann es weitere Prozessschritte außerhalb der DocuWare Cloud geben, die wir nicht kennen können.
What does the data protection training cover? The privacy trainings cover GDPR day-to-day cases and situations as well as the CCPA and will cover future applicable law.	**Was beinhaltet die Schulung zum Datenschutz?** Die Schulungen zum Datenschutz decken alltägliche Fälle und Situationen der DSGVO sowie des CCPA ab und werden sich mit dem künftig geltenden Recht befassen.
Do all DocuWare employees participate in data privacy trainings? Yes. All DocuWare employees (worldwide) participate in an annual data protection training and test. Evidence exists but is treated confidentially for data protection reasons.	**Nehmen alle DocuWare Mitarbeiter an Schulungen zum Datenschutz teil?** Ja. Alle DocuWare Mitarbeiterinnen und Mitarbeiter (weltweit) nehmen jährlich an einer Schulung und Prüfung zum Datenschutz teil. Nachweise liegen vor, werden aber aus Datenschutzgründen vertraulich behandelt.

Do you require employees who access client data to sign a confidentiality agreement that access client data? Yes. All employees sign a general confidentiality agreement confidentiality agreement or non-disclosure agreement (NDA) upon hire that extends beyond the term of the employment contract. All system administrators sign a specific confidentiality agreement tailored to the security-related aspects of the positions.	**Verlangen Sie von Mitarbeitern, die Zugang zu Kundendaten haben, die Unterzeichnung einer Vertraulichkeitserklärung, die den Zugang zu Kundendaten regelt?** Ja. Alle Mitarbeiter unterzeichnen bei ihrer Einstellung eine allgemeine Vertraulichkeitsvereinbarung bzw. eine Geheimhaltungsvereinbarung, die über die Dauer des Arbeitsvertrags hinaus gilt. Alle Systemadministratoren unterzeichnen eine spezielle Vertraulichkeitsvereinbarung, die auf die sicherheitsrelevanten Aspekte ihrer Position zugeschnitten ist.
What is DocuWare's privacy and cookie policy? We provide detailed information about our privacy policy, please see Our general GDPR-based privacy policy Our CCPA policy Our cookie policy All sites are checked and adapted at regular intervals to ensure that they are up to date.	**Wie lautet die Datenschutz- und Cookie-Richtlinie von DocuWare?** Ausführliche Informationen über unsere Datenschutzpolitik finden Sie hier: Unsere allgemeinen DSGVO-basierten Datenschutzrichtlinien Unsere CCPA-Richtlinie Unsere Cookie-Richtlinie Alle Websites werden in regelmäßigen Abständen überprüft und angepasst, um sicherzustellen, dass sie auf dem neuesten Stand sind.

2.2.3 Data protection officer

Who is DocuWare's data protection officer?
Contact details of our data protection officer:

Catherina Schneider-Nissen
DocuWare GmbH
Planegger Str. 1
82110 Germering
Tel.: +49 89 894433-0
dataprotection@docuware.com

She is registered with the relevant supervisory body, the Bavarian State Office for Data Protection Supervision.

In addition, there are native-speaking data protection coordinators.

2.2.4 Technical and Organizational Measures (TOMs)

Where does DocuWare provide information on its TOMs?
Our current TOMs within the DocuWare Group can be found on our website:
TOMs
They are subject to an annual review.

2.2.5 Rights of data subjects

How does DocuWare handle rights of data subjects in general?

For information on data handling in relation to applications, our websites and other issues, please refer to our data privacy site. In our data privacy statement, we explain how we handle the rights of data subjects:
Data privacy

2.2.3 Datenschutzbeauftragter

Wer ist der oder die Datenschutzbeauftragte von DocuWare?
Kontaktangaben unserer Datenschutzbeauftragten:

Catherina Schneider-Nissen
DocuWare GmbH
Planegger Str. 1
82110 Germering
Tel.: +49 89 894433-0
dataprotection@docuware.com

Sie ist bei der zuständigen Aufsichtsbehörde, dem Bayerischen Landesamt für Datenschutzaufsicht, registriert.

Darüber hinaus gibt es muttersprachliche Datenschutzkoordinatoren.

2.2.4 Technische und organisatorische Maßnahmen (TOMs)

Wo informiert DocuWare über seine TOMs?
Unsere aktuellen TOMs innerhalb der DocuWare Gruppe finden Sie auf unserer Website:
TOMs
Sie werden jährlich überprüft.

2.2.5 Rechte der betroffenen Personen

Wie geht DocuWare mit den Rechten der Betroffenen im Allgemeinen um?
Informationen zum Umgang mit Daten im Zusammenhang mit Bewerbungen, unseren Websites und anderen Themen finden Sie auf unserer Datenschutzseite. In unserer Datenschutzerklärung erläutern wir, wie wir mit den Rechten der Betroffenen umgehen:
Datenschutz

How does DocuWare handle requests from data subjects?
On our website, we provide a form for requests from data subjects. In addition, all other contact options such as telephone or email can of course also be used.
If we are able to assign a data subject to a customer, we will pass on the inquiry without delay. The likelihood of this is very low because we do not have access to customer data.
Form on website:

Information Request from DocuWare

How does DocuWare handle the deletion process for customer-related data at contract termination?
After termination of a customer cloud contract, the customer has time to download its data from the cloud until to the effective date of the termination. One can either use the DocuWare Request feature for smaller amounts of data or book our Professional Services Team subject to a fee. After this date, the customer will no longer have access to the data in the cloud.
Data is deleted from the productive system after approximately 60–90 days, and from the cold storage after a further 30 days at the latest.

2.2.6 International data transfers

One major subject in the GDPR are international data transfers. GDPR requires that personal data travels around the globe with its European protection. That requires transfer mechanisms that provide for this.

An overview can be found at:
International dimension of data protection | European Commission (europa.eu)

Wie geht DocuWare mit Anfragen von Betroffenen um?
Auf unserer Website stellen wir ein Formular für Anfragen von betroffenen Personen zur Verfügung. Darüber hinaus können natürlich auch alle anderen Kontaktmöglichkeiten wie Telefon oder E-Mail genutzt werden.
Wenn wir eine betroffene Person einem Kunden zuordnen können, werden wir die Anfrage unverzüglich weiterleiten. Die Wahrscheinlichkeit dafür ist sehr gering, da wir keinen Zugang zu Kundendaten haben.
Formular auf der Website:

Informationsanforderung von DocuWare

Wie handhabt DocuWare die Löschung von kundenbezogenen Daten bei Vertragsende?
Nach Beendigung eines Cloud-Vertrags hat der Kunde Zeit, seine Daten aus der Cloud herunterzuladen, und zwar bis zum Datum des Wirksamwerdens der Kündigung. Für kleinere Datenmengen kann man entweder die DocuWare Request Funktion nutzen oder unser Professional Services Team kostenpflichtig buchen. Nach diesem Zeitpunkt hat der Kunde keinen Zugriff mehr auf die Daten in der Cloud.
Die Daten werden nach etwa 60–90 Tagen aus dem Produktivsystem und spätestens nach weiteren 30 Tagen aus dem Cold Storage gelöscht.

2.2.6 Internationale Datenübermittlung

Ein wichtiges Thema der DSGVO ist die internationale Datenübermittlung. Die Datenschutz-Grundverordnung schreibt vor, dass personenbezogene Daten mit ihrem europäischen Schutz rund um den Globus reisen. Das erfordert Transfermechanismen, die dies vorsehen.

Eine Übersicht finden Sie hier:
Internationale Dimension des Datenschutzes | Europäische Kommission (europa.eu)

How does DocuWare deal with the ECJ's decision on the EU-U.S. Privacy Shield and the EU-U.S. Data Privacy Framework?

Due to the general political situation, we rely on providers with European data centers in relation to software we use internally. Customers' data will stay in their current region.
If we have to transfer data out of the EEA we will continue to use the Standard Contractual Clauses (SCC).

Supplementary measures to the SCC
The Data Protection Conference (Datenschutzkonferenz, DSK) as the joint decision-making body of the German state data protection supervisory authorities, has already determined that the data protection level of the GDPR cannot be guaranteed in the USA, which is why additional measures are necessary.

DocuWare has made an encryption method available to all employees involved in data transfers out of the EEA. We consider encryption as a highly effective measure. Other measures are under development for data transfers within the DocuWare Group along the lines of the Microsoft measures mentioned below.

Wie geht DocuWare mit der Entscheidung des EuGH zum EU-US Privacy Shield und zum EU-U.S. Data Privacy Framework um?

Aufgrund der allgemeinen politischen Lage setzen wir bei der von uns intern verwendeten Software auf Anbieter mit Rechenzentren in Europa. Die Daten unserer Kunden verbleiben in ihrer aktuellen Region.
Sollten wir Daten außerhalb des Europäischen Wirtschaftsraums (EWR) übertragen müssen, werden wir weiterhin die Standardvertragsklauseln (SCC) verwenden.

Ergänzende Maßnahmen zum SCC
Die Datenschutzkonferenz (DSK) als gemeinsames Entscheidungsgremium der deutschen Landesdatenschutzaufsichtsbehörden hat bereits festgestellt, dass das Datenschutzniveau der DSGVO in den USA nicht gewährleistet werden kann, weshalb zusätzliche Maßnahmen notwendig sind.

DocuWare hat allen Mitarbeitern, die mit Datenübertragungen außerhalb des EWR zu tun haben, ein Verschlüsselungsverfahren zur Verfügung gestellt. Wir halten die Verschlüsselung für eine sehr wirksame Maßnahme. Für den Datentransfer innerhalb der DocuWare Gruppe sind weitere Maßnahmen in Vorbereitung, die sich an den unten genannten Microsoft-Maßnahmen orientieren.

Microsoft measures
In addition, it should be noted that Microsoft has developed contractual guarantees for all European customers. These guarantees consist of the following measures:
- informing the data subject if Microsoft has been legally required by a government order to release data to US security authorities;
- Microsoft's obligation to seek legal recourse in the US courts to challenge the government order to release the data;
- the right to compensation for a data subject whose data has been unlawfully processed and who has suffered material or non-material damage as a result.
This is relevant because DocuWare Cloud Services is hosted in Microsoft Azure data centers.
You can find the latest Microsoft DPA including SCCs at:

Licensing Documents (microsoft.com)

Microsoft-Maßnahmen
Darüber hinaus hat Microsoft vertragliche Garantien für alle europäischen Kunden entwickelt. Diese Garantien bestehen aus den folgenden Maßnahmen:
– Unterrichtung der betroffenen Person, wenn Microsoft aufgrund einer behördlichen Anordnung gesetzlich verpflichtet ist, Daten an US-Sicherheitsbehörden weiterzugeben;
– Verpflichtung von Microsoft, die behördliche Anordnung zur Herausgabe der Daten vor den US-Gerichten anzufechten;
– das Recht auf Schadenersatz für eine betroffene Person, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat.
Dies ist relevant, da die DocuWare Cloud Services in Microsoft Azure-Rechenzentren gehostet werden.
Die aktuelle Microsoft DPA einschließlich SCCs finden Sie unter:

Lizenzierungsdokumente (microsoft.com)

How does DocuWare process customer data in third countries?
Our European customers' data resides in the Microsoft Azure data center in Ireland, with data mirroring to the Netherlands. There are the two following exceptional cases – which can be influenced by you as a customer – when your data may be processed in our subsidiary in the US:

1) Third level support by the development department
The DocuWare Support Team in Europe might not be able to solve a case on its own and might have to involve the DocuWare development department in US, which is responsible for several software features, e.g., the API for the signature services. It is worth mentioning that DocuWare employees in the US also work on our inhouse system, which is hosted in Ireland. The data is viewed from the US, which turns it into an international data transfer from a GDPR point of view.

Wie verarbeitet DocuWare Kundendaten in Drittländern?

Die Daten unserer europäischen Kunden befinden sich im Microsoft Azure-Rechenzentrum in Irland, mit Datenspiegelung in den Niederlanden. In den beiden folgenden Ausnahmefällen – die Sie als Kunde beeinflussen können – können Ihre Daten in unserer Tochtergesellschaft in den USA verarbeitet werden:

1) Third-Level-Unterstützung durch die Entwicklungsabteilung
Das DocuWare Support-Team in Europa ist unter Umständen nicht in der Lage, einen Fall allein zu lösen, und muss die DocuWare Entwicklungsabteilung in den USA einschalten, die für einige Software-Funktionen verantwortlich ist, z. B. für die API für die Signaturdienste. Erwähnenswert ist, dass die DocuWare Mitarbeiterinnen und Mitarbeiter in den USA auch auf unserem Inhouse-System arbeiten, das in Irland gehostet wird. Die Daten werden von den USA aus eingesehen, was sie aus Sicht der Datenschutzgrundverordnung (DSGVO) zu einer internationalen Datenübermittlung macht.

2) Support 24 hours/5 days
DocuWare offers 24/5-support for severe support cases. This is only possible through the involvement of our DocuWare colleagues in the US. You can find out what that looks like at:
24/5 Support · DocuWare Support Portal

Which subcontractors DocuWare works with?
All subcontractor relationships can be found at:
Subcontractors of DocuWare
Purpose of subcontractor assignments: The purposes for each service provider can be seen in the detailed subcontractor list on our webpage linked above.
Contracts with subcontractors: In addition to the main contract, a data processing agreement and SCC, if applicable, have been entered into with all subcontractors.

DocuWare works with the following subcontractors:

1. DocuWare GmbH
The parent company DocuWare GmbH is a subcontractor of the sales units (DocuWare Europe GmbH, DocuWare S.L., DocuWare SARL, and DocuWare Ltd.), as it is the administrator of the cloud application. DocuWare Corp. in the USA is connected to DocuWare GmbH for the above-mentioned support cases with standard contractual clauses or a data processing agreement. DocuWare GmbH acts also as the Corp.'s representative in accordance with Art. 27 GDPR. Furthermore, Microsoft is a processor because the DocuWare Cloud solution is hosted there.

2) Support 24 Stunden/5 Tage
DocuWare bietet 24/5-Support für schwerwiegende Supportfälle. Dies ist nur durch das Einbeziehen unserer DocuWare Kolleginnen und Kollegen in den USA möglich. Wie das aussieht, erfahren Sie hier:
24/5 Support · DocuWare Support Portal

Mit welchen Subunternehmern arbeitet DocuWare zusammen?
Alle Beziehungen zu Unterauftragnehmern finden Sie hier:
Unterauftragnehmer von DocuWare
Zweck der Beauftragung von Unterauftragnehmern: Die Zwecke für jeden Dienstleister sind in der detaillierten Liste der Unterauftragnehmer auf der oben verlinkten Webseite aufgeführt.
Verträge mit Unterauftragnehmern: Zusätzlich zum Hauptvertrag wurden mit allen Unterauftragnehmern eine Datenverarbeitungsvereinbarung und ggf. ein SCC abgeschlossen.

DocuWare arbeitet mit den folgenden Unterauftragnehmern zusammen:

1. DocuWare GmbH
Die Muttergesellschaft DocuWare GmbH ist Unterauftragnehmerin der Vertriebseinheiten (DocuWare Europe GmbH, DocuWare S.L., DocuWare SARL und DocuWare Ltd.), da sie Administratorin der Cloud-Anwendung ist. Die DocuWare Corp. in den USA ist für die oben genannten Supportfälle mit Standardvertragsklauseln oder einem Datenverarbeitungsvertrag mit der DocuWare GmbH verbunden. Die DocuWare GmbH handelt auch als Vertreter der Gesellschaft gemäß Art. 27 GDPR. Zudem ist Microsoft ein Verarbeiter, da die DocuWare Cloud-Lösung dort gehostet wird.

2. Microsoft
Information about data protection at Microsoft can be found here:
General Data Protection Regulation, GDPR Overview (microsoft.com)
Microsoft's subcontractors can be found here (registration with Microsoft required):
My Library (microsoft.com)
Microsoft's DPA:
Licensing Resources and Documents (microsoft.com)

3. DocuWare Corporation
To provide 24h/5d support, the team at DocuWare Corporation (USA) is involved.

4. Nemetschek OOD
Nemetschek OOD (Bulgaria), to which DocuWare GmbH is a shareholder, is involved in the
European Level 1 Support as well as in Product Development and Quality Assurance (QA).

5. Sendgrid/Twilio
The Sendgrid API from Twilio is used to send emails through DocuWare Cloud. This applies to:
– System messages, such as messages about updates or downtime.
– Emails initiated by notifications or workflows, unless a customer's own SMTP server is used.

6. Additional subcontractors
If you have booked additional cloud services, other subcontractors may be used on a case-by-case basis. These can be seen under the above link. The data will not be transmitted to companies other than those mentioned. This includes that the data will not be sold within the meaning of the CCPA.

2. Microsoft
Informationen zum Datenschutz bei Microsoft finden Sie hier:
Datenschutz-Grundverordnung, Übersicht (microsoft.com)

Microsofts Unterauftragnehmer finden Sie hier (Registrierung bei Microsoft erforderlich):
Meine Bibliothek (microsoft.com)
Microsofts DPA:
Ressourcen und Dokumente zur Lizenzierung (microsoft.com)

3. DocuWare Corporation
Für den 24/5-Support ist das Team der DocuWare Corporation (USA) zuständig.

4. Nemetschek OOD
Die Nemetschek OOD (Bulgarien), an der die DocuWare GmbH beteiligt ist, ist sowohl im
europäischen Level-1-Support als auch in der Produktentwicklung und Qualitätssicherung (QA) tätig.

5. Sendgrid/Twilio
Für den Versand von E-Mails über DocuWare Cloud wird die Sendgrid API von Twilio verwendet. Dies gilt für:
– Systemmeldungen, z. B. Meldungen über Updates oder Ausfallzeiten.
– E-Mails, die durch Benachrichtigungen oder Workflows ausgelöst werden, es sei denn, es wird ein kundeneigener SMTP-Server verwendet.

6. Zusätzliche Unterauftragnehmer
Wenn Sie zusätzliche Cloud-Dienste gebucht haben, können von Fall zu Fall weitere Unterauftragnehmer eingesetzt werden. Diese können unter dem obigen Link eingesehen werden. Die Daten werden nicht an andere als die genannten Unternehmen weitergegeben. Dies schließt ein, dass die Daten nicht im Sinne des CCPA verkauft werden.

7. Second-level support from manufacturers of software components
From time to time, we need to involve the manufacturers of software components that have been integrated in the DocuWare software in the handling of support cases. We concluded a data processing agreement and, if applicable, the SCC with these manufacturers as standard.
The data is transmitted in an encrypted form.

2.3 Certifications and standards

Does your organization review service auditor reports on controls?
If yes, is this done on an annual basis?
If yes, are exceptions noted and reviewed by leadership and action taken to mitigate risk?
Yes. We do and we follow up on their requests.
Yes, this is done on an annual basis.
Yes, exceptions are noted and reviewed by leadership and action taken to mitigate risk.

Does your organization have a governance structure in place in order to clearly outline compliance standards and communicate standards to employees?
Yes. DocuWare has a compliance management team. As for certifications: We have another team handling SOC 2 Type 2 and ISO standards.

7. Second-Level-Support von Herstellern von Softwarekomponenten
Von Zeit zu Zeit müssen wir die Hersteller von Software-Komponenten, die in die DocuWare Software integriert wurden, in die Bearbeitung von Supportfällen einbeziehen. Mit diesen Herstellern haben wir standardmäßig einen Datenverarbeitungsvertrag und ggf. den SCC abgeschlossen.

Die Daten werden in verschlüsselter Form übertragen.

2.3 Zertifizierungen und Standards

Überprüft Ihre Organisation die Berichte der Prüfer über die Kontrollen?
Wenn ja, wird dies jährlich durchgeführt?
Wenn ja, werden Ausnahmen vermerkt, von der Leitung überprüft und Maßnahmen zur Risikominderung ergriffen?
Ja. Das tun wir, und wir gehen auf ihre Anfragen ein.
Ja, dies wird jährlich durchgeführt.
Ja, Ausnahmen werden vermerkt, von der Leitung überprüft und es werden Maßnahmen zur Risikominderung ergriffen.

Verfügt Ihr Unternehmen über eine Governance-Struktur, um die Compliance-Standards klar zu umreißen und den Mitarbeitern zu vermitteln?
Ja. DocuWare verfügt über ein Compliance-Management-Team. Was die Zertifizierungen betrifft: Wir haben ein weiteres Team, das sich mit SOC-2-Typ-2 und ISO-Normen befasst.

What certifications does DocuWare hold?
DocuWare has numerous certifications. For example, it has been SOC 2 Type 2 certified since 2021 (SOC 2 Type 1 until 2020).
All current DocuWare certifications and standards can be found here:

Compliance and certifications
A selection of the certificates can also be found in the appendix.

Does DocuWare comply with the European Union's NIS 2 directive?
DocuWare has successfully achieved ISO 27001 certification, which underscores our commitment to the highest standards of information security and management practices. Regarding NIS 2 compliance, we are actively working to meet all requirements. We are currently aligning our processes and systems to ensure full compliance with NIS 2 regulations.

2.4 Information Security Management

Does your organization have an Information Security Management Policy?
Yes.
Our Information Security Management Policy describes DocuWare's Information Security Management System (ISMS). It defines for example the ISMS's scope, the roles and responsibilities, a legal contractual requirements register, a risk management planning as well as implementation notes.

Welche Zertifizierungen hat DocuWare?
DocuWare verfügt über zahlreiche Zertifizierungen. Beispielsweise ist es seit 2021 nach SOC 2 Typ 2 zertifiziert (bis 2020 nach SOC 2 Typ 1).
Alle aktuellen DocuWare-Zertifizierungen und Standards finden Sie hier:

Compliance und Zertifizierungen
Eine Auswahl der Zertifikate ist auch im Anhang zu finden.

Erfüllt DocuWare die NIS 2-Richtlinie der EU?

DocuWare wurde erfolgreich nach ISO 27001 zertifiziert, was unser Engagement für höchste Standards in den Bereichen Informationssicherheit und Managementpraktiken unterstreicht. Im Hinblick auf die NIS 2-Konformität arbeiten wir aktiv daran, alle Anforderungen zu erfüllen. Derzeit passen wir unsere Prozesse und Systeme an, um die vollständige Einhaltung der NIS 2-Vorschriften sicherzustellen.

2.4 Informationssicherheitsmanagement

Verfügt Ihr Unternehmen über eine Richtlinie zum Management der Informationssicherheit?
Ja.
Unsere Richtlinie zum Management der Informationssicherheit beschreibt das Informationssicherheits-Managementsystem (ISMS) von DocuWare. Es definiert beispielsweise den Geltungsbereich des ISMS, die Rollen und Verantwortlichkeiten, ein rechtliches und vertragliches Anforderungsregister, eine Risikomanagementplanung sowie Umsetzungshinweise.

2.5 Security of corporate IT

2.5.1 General

Does DocuWare have an implemented security policy?
If yes, what does it cover?
Yes. We do have several internal policies that on one hand regulate how end users are to handle IT provided services and equipment and on the other hand, how administrators must configure and manage IT services and equipment.
Furthermore, we maintain policies and instructions regarding disaster recovery and risk assessment.
The policies are confidential.
The Information Security Policy for end users deals with IT security and topics such as password lengths and similar issues. DocuWare proves the efficiency of these procedures through its annual SOC 2 Type 2 controls.
As all of our internal guidelines contain some type of confidential information, we do not distribute them to partners and customers.

Does DocuWare have an information security risk management program that ensures threats are assessed and mitigated on a periodic basis?

Yes. In the risk assessment, each risk is evaluated according to severity and potential impact. Risk assessments are carried out quarterly together with top management and other responsible employees.

2.5 Sicherheit der Unternehmens-IT

2.5.1 Allgemeines

Verfügt DocuWare über eine implementierte Sicherheitsrichtlinie?
Wenn ja, was deckt sie ab?
Ja. Wir haben mehrere interne Richtlinien, die einerseits regeln, wie die Endbenutzer mit den von der IT bereitgestellten Diensten und Geräten umgehen sollen, und andererseits, wie die Administratoren die IT-Dienste und Geräte konfigurieren und verwalten müssen.
Darüber hinaus verfügen wir über Richtlinien und Anweisungen zum Desaster-Recovery und zur Risikobewertung.
Die Richtlinien sind vertraulich.
Die Informationssicherheitsrichtlinie für Endnutzer befasst sich mit IT-Sicherheit und Themen wie der Länge von Passwörtern und ähnlichen Fragen. Die Effizienz dieser Verfahren beweist DocuWare durch die jährlichen SOC-2-Typ-2-Kontrollen.
Da alle unsere internen Richtlinien eine Art von vertraulichen Informationen enthalten, geben wir sie nicht an Partner und Kunden weiter.

Verfügt DocuWare über ein Informationssicherheits-Risikomanagementprogramm, das sicherstellt, dass Bedrohungen in regelmäßigen Abständen bewertet und entschärft werden?

Ja. Bei der Risikobewertung wird jedes Risiko nach seinem Schweregrad und seinen möglichen Auswirkungen beurteilt. Die Risikobewertungen werden vierteljährlich zusammen mit der Unternehmensleitung und anderen verantwortlichen Mitarbeitern durchgeführt.

How does DocuWare handle user provisioning and deprovisioning? We have a highly automated process in place that efficiently handles on-boarding/side-boarding/offboarding. Notifications and tasks will be sent out to the relevant persons to complete workflow steps.	**Wie handhabt DocuWare das Provisioning und Deprovisioning von Benutzern?** Wir verfügen über einen hochautomatisierten Prozess, der Onboarding, Sideboarding und Offboarding effizient abwickelt. Es werden Benachrichtigungen und Aufgaben an die entsprechenden Personen gesendet, um die Arbeitsschritte zu erledigen.
Is a security awareness training program established for all employees? Every employee starting at DocuWare receives a basic security training. Additionally, every employee must partake in annual information security (and data protection) trainings. The content varies depending on the current threat landscape. Training participation is mandatory and enforced.	**Wurde für alle Mitarbeiter ein Schulungsprogramm zum Thema Sicherheit eingerichtet?** Jede/r neue Mitarbeiter/in bei DocuWare erhält eine grundlegende Sicherheitsschulung. Darüber hinaus müssen alle Mitarbeiter und Mitarbeiterinnen an jährlichen Schulungen zum Thema Informationssicherheit (und Datenschutz) teilnehmen. Die Inhalte variieren je nach aktueller Bedrohungslage. Die Teilnahme an den Schulungen ist obligatorisch und wird durchgesetzt.
Do external entities receive access to internal systems? Access from outside the organization is only granted to contractors and other third parties via a dedicated process after each individual case has been examined. Only the minimum necessary permissions are granted.	**Erhalten externe Stellen Zugang zu internen Systemen?** Der Zugriff von außerhalb der Organisation wird Auftragnehmern und anderen Dritten nur nach einer Einzelfallprüfung mit einem speziellen Prozess gewährt. Es werden nur die unbedingt erforderlichen Berechtigungen erteilt.
2.5.2 Server and client security	**2.5.2 Server- und Client-Sicherheit**
Does DocuWare allow transferring customer data from company computers to portable media? We utilize third party software that blocks USB ports on all devices. This also protects against malicious or modified USB sticks. In addition, Microsoft Defender for Endpoint is in place.	**Erlaubt DocuWare die Übertragung von Kundendaten von Firmenrechnern auf mobile Medien?** Wir verwenden Software von Drittanbietern, die USB-Anschlüsse auf allen Geräten blockiert. Dies schützt auch vor bösartigen oder modifizierten USB-Sticks. Darüber hinaus ist Microsoft Defender für Endpoint installiert.

Is an anti-malware solution installed on servers and workstations? Yes. Anti-malware software is installed on every client and server. Additionally, it is blocking scripts and Office macros. The software is automatically updating itself. In addition, Microsoft Defender for Endpoint is in place.	**Ist eine Anti-Malware-Lösung auf Servern und Computer-Arbeitsplätzen installiert?** Ja. Auf jedem Client und Server ist eine Anti-Malware-Software installiert. Diese blockiert zudem Skripte und Office-Makros. Die Software aktualisiert sich automatisch. Zusätzlich ist Microsoft Defender for Endpoint installiert.
Are workstations data storages encrypted? Yes, we require encryption for all portable devices and their drives. Encryption health is checked and workstations are required to have Bitlocker activated.	**Sind die Datenspeicher der Computer-Arbeitsplätze verschlüsselt?** Ja, wir bestehen auf Verschlüsselung für alle tragbaren Geräte und deren Laufwerke. Der Verschlüsselungsstatus wird überprüft und Workstations müssen Bitlocker aktiviert haben.
How are workstations kept up to date? We use tools to automatically and regularly patch third-party software installed on all devices. Furthermore, updates to the operating systems are deployed automatically and reboots are enforced in a timely manner. Automations are checked on a regular basis.	**Wie werden die Computer-Arbeitsplätze auf dem neuesten Stand gehalten?** Wir verwenden Tools, um die auf allen Geräten installierte Software von Drittanbietern automatisch und regelmäßig zu patchen. Darüber hinaus werden Aktualisierungen der Betriebssysteme automatisch eingespielt und Neustarts rechtzeitig erzwungen. Die Automatisierungen werden regelmäßig überprüft.
How are data drives being disposed of? We follow documented procedures to securely erase data drives irrecoverably. Appropriate methods are used for HDDs and SSDs respectively. When a device which includes a data drive is passed from one employee to another, the same process is followed.	**Wie werden die Datenlaufwerke entsorgt?** Wir befolgen dokumentierte Verfahren zur sicheren und unwiederbringlichen Löschung von Datenlaufwerken. Entsprechende Methoden werden für HDDs und SSDs verwendet. Wenn ein Gerät, zu dem auch ein Datenlaufwerk gehört, von einem Mitarbeiter zum nächsten gegeben wird, kommt das gleiche Verfahren zur Anwendung.

Does DocuWare use Mobile Device Management (MDM) technology to manage mobile BYOD devices?
When used in the office, BYOD* mobile devices can only connect to a separate WiFi network.
Furthermore, a Microsoft Solution ensures that corporate data is only stored on mobile BYOD devices in encrypted form. We control the container and are able to set requirements for the device (minimum patch level, lock screen). If the company requirements are not met, company data cannot be accessed. This solution applies to all mobile Microsoft business applications (like OneDrive, Teams, etc.) and automatically isolates the data from other apps. This also prevents the transfer to non-business apps.
**Bring Your Own Device*

2.5.3 Network security

Is data encrypted in transfer between the DocuWare network and data center?
Yes. For more information, see chapter "DocuWare - the Product", section 1.2.1 Encryption.

Are secure remote access procedures in place?
Access to the company network: The DocuWare company network is protected by various security measures to ensure data confidentiality and integrity. We use established security protocols and multi-factor authentication methods to access various solutions, depending on the required security level.
The security level is regularly audited to ensure continuous security and compliance.

Setzt DocuWare Mobile Device Management (MDM) ein, um mobile BYOD-Geräte zu verwalten?
Bei Verwendung im Büro können BYOD*-Mobilgeräte nur mit einem separaten WLAN-Netzwerk verbunden werden.
Darüber hinaus stellt eine Microsoft-Lösung sicher, dass Unternehmensdaten auf mobilen BYOD-Geräten nur in verschlüsselter Form gespeichert werden. Wir kontrollieren den Container und können Anforderungen an das Gerät festlegen (minimaler-Patch-Level, Sperrbildschirm). Werden die Unternehmensanforderungen nicht erfüllt, kann nicht auf Unternehmensdaten zugegriffen werden. Diese Lösung gilt für alle mobilen Microsoft-Geschäftsanwendungen (wie OneDrive, Teams usw.) und isoliert die Daten automatisch von anderen Apps. Dadurch wird auch die Übertragung an geschäftsfremde Apps verhindert.
**Bring Your Own Device*

2.5.3 Netzsicherheit

Werden die Daten zwischen dem DocuWare Netzwerk und dem Rechenzentrum verschlüsselt übertragen?
Ja. Weitere Informationen finden Sie im Kapitel „DocuWare - das Produkt“, Abschnitt 1.2.1 Verschlüsselung.

Gibt es sichere Verfahren für den Fernzugriff?
Zugriff auf das Unternehmensnetzwerk: Das DocuWare Unternehmensnetzwerk ist durch zahlreiche Sicherheitsmaßnahmen geschützt, um die Vertraulichkeit und Integrität der Daten zu gewährleisten. Wir verwenden etablierte Sicherheitsprotokolle und Multi-Faktor-Authentifizierungsmethoden für den Zugriff auf verschiedene Lösungen, je nach erforderlicher Sicherheitsstufe.
Die Sicherheitsstufe wird regelmäßig überprüft, um kontinuierliche Sicherheit und Compliance zu gewährleisten.

What is your firewall management process?
In accordance with the SOC 2 controls, changes and exceptions have to be approved prior to implementation.

At which interval do you review firewall rules?
Firewall rules and exceptions are reviewed quarterly.

Is a network segmentation in place?
Yes.

Can you provide internal network maps?
Due to the sensitive nature of the information, we can't provide any insight here.

2.5.4 Backups

Is online storage encrypted?
Yes.

How is DocuWare handling backups of IT systems?
(See above for DocuWare Cloud Service Backup for customers)
Backup frequency: Systems are backed up daily, weekly or monthly depending on the criticality.
Backup retention: Depending on the frequency, backups are kept ranging from 2 weeks (10 snap-shots at a time) to 1 year (2 snapshots at a time).
Backup restore tests: Restore tests are done on a monthly basis.
Backup encryption: All backups are encrypted using current security standards and in accordance with the SOC 2 Type 2 certification.

Wie sieht Ihr Firewall-Management-Prozess aus?
In Übereinstimmung mit den SOC-2-Typ-2-Kontrollen müssen Änderungen und Ausnahmen vor ihrer Umsetzung genehmigt werden.

In welchen Abständen überprüfen Sie die Firewall-Regeln?
Die Firewall-Regeln und -Ausnahmen werden vierteljährlich überprüft.

Gibt es eine Netzwerksegmentierung?
Ja.

Können Sie interne Netzpläne zur Verfügung stellen?
Aufgrund des sensiblen Charakters der Informationen können wir hier keinen Einblick gewähren.

2.5.4 Backups

Ist die Online-Speicherung verschlüsselt?
Ja.

Wie geht DocuWare mit Backups von IT-Systemen um?
(Siehe oben für DocuWare Cloud Service Backup für Kunden)
Backup-Häufigkeit: Die Systeme werden abhängig von ihrer Relevanz täglich, wöchentlich oder monatlich gesichert.
Aufbewahrungsdauer der Backups: Je nach Häufigkeit werden die Backups zwischen 2 Wochen (je 10 Snapshots) und 1 Jahr (je 2 Snapshots) aufbewahrt.
Tests zur Backup-Wiederherstellung: Die Wiederherstellungstests werden monatlich durchgeführt.
Backup-Verschlüsselung: Alle Backups werden nach aktuellen Sicherheitsstandards und gemäß SOC-2-Typ-2-Zertifizierung verschlüsselt.

2.5.5 Identity protection
Is Multi-Factor Authentication (MFA) for employee accounts in place? Yes. It is mandatory for every employee to register a secondary authentication factor. This is enforced from the start and cannot be circumvented. Service accounts are subject to this policy, too. In rare cases where an exception is granted, it is configured in a way that is as secure as possible. Exceptions are documented and reviewed regularly.
What is DocuWare's password policy? Password requirements (length, complexity, rotation, password storage) are in accordance with the SOC 2 Type 2 controls.
How does DocuWare protect against malicious login attempts? We use a logon protection system which is based on artificial intelligence. It can detect logins from malicious actors (for example, atypical travel, new device, authentication protocol, MFA method used). As soon as such a login is detected, the user account in question is automatically blocked and an alert is sent to IT. The case will then be investigated manually, and the user will be unblocked once the account was secured and the impact assessed. Logins are also blocked after a certain number of failed attempts.

2.5.5 Schutz der Identität
Gibt es eine Multi-Faktor-Authentifizierung (MFA) für Mitarbeiterkonten? Ja. Jeder Mitarbeiter ist verpflichtet, einen zweiten Authentifizierungsfaktor zu registrieren. Dies wird von Anfang an durchgesetzt und kann nicht umgangen werden. Auch für Servicekonten gilt diese Richtlinie. In den seltenen Fällen, in denen eine Ausnahme gewährt wird, wird diese so sicher wie möglich konfiguriert. Ausnahmen werden dokumentiert und regelmäßig überprüft.
Was ist die Passwortrichtlinie von DocuWare? Die Anforderungen an Passwörter (Länge, Komplexität, Rotation, Speicherung von Passwörtern) entsprechen den SOC-2-Typ-2-Kontrollen.
Wie schützt sich DocuWare vor bösartigen Anmeldeversuchen? Wir verwenden ein Anmeldeschutzsystem, das auf künstlicher Intelligenz basiert. Es kann Anmeldungen von böswilligen Akteuren erkennen (z. B. „atypical travel", neues Gerät, Authentifizierungsprotokoll, verwendete MFA-Methode). Sobald eine solche Anmeldung entdeckt wird, wird das betreffende Benutzerkonto automatisch gesperrt und eine Warnung an die IT-Abteilung gesendet. Der Fall wird dann manuell untersucht, und der Nutzer wird entsperrt, sobald das Konto gesichert und die Auswirkungen bewertet wurden. Außerdem werden Anmeldungen nach einer bestimmten Anzahl von Fehlversuchen gesperrt.

Do you have controls in place that restrict access to information and uniquely identify users?
Yes. We operate on least privilege principles. That means, each employee starts out with only the most basic permissions to access corporate resources that concern the entire company. Then, additional permissions are granted in line with their activity. If employees change departments, the permissions are reevaluated and revoked accordingly. Permissions are directly tied to the personal user account that each employee receives.

Does DocuWare evaluate their user directory as well as granted permissions?
To ensure that the access rights of offboarded employees have been revoked as planned, monthly user access audits are performed. Critical changes to permissions, such as domain privileges, are alerted to IT staff and are reviewed immediately. Anomalies are documented and checked, too.

2.5.6 Threat & vulnerability management

How is risk assessment done?
Every month, risk assessments with top-level management are scheduled.
Special teams conduct weekly risk assessments to keep risks under control; these teams are not integrated into top-level management. Risk mitigation measures are planned, their progress is monitored, and newly identified risks are discussed.

Verfügen Sie über Kontrollen, die den Zugang zu Informationen einschränken und die Benutzer eindeutig identifizieren?
Ja. Wir arbeiten nach dem Prinzip der geringsten Privilegien. Das bedeutet, dass jeder Mitarbeiter zu Beginn nur die grundlegendsten Berechtigungen für den Zugriff auf Unternehmensressourcen, die das gesamte Unternehmen betreffen, erhält. Je nach Tätigkeit werden dann zusätzliche Genehmigungen erteilt. Wenn Mitarbeiter die Abteilung wechseln, werden die Berechtigungen neu bewertet und entsprechend entzogen. Die Berechtigungen sind direkt an das persönliche Benutzerkonto gebunden, das jeder Mitarbeiter erhält.

Wertet DocuWare das eigene Benutzerverzeichnis sowie die vergebenen Berechtigungen aus?
Um sicherzustellen, dass die Zugriffsrechte ausgeschiedener Mitarbeiterinnen und Mitarbeiter wie geplant entzogen wurden, werden monatlich Zugriffsüberprüfungen durchgeführt. Kritische Änderungen von Berechtigungen, wie z. B. Domänenprivilegien, werden den IT-Mitarbeitern gemeldet und sofort überprüft. Auch Anomalien werden dokumentiert und überprüft.

2.5.6 Bedrohung & Schwachstellenmanagement

Wie erfolgt die Risikobewertung?
Monatlich finden Risikobewertungen unter Einbeziehung der obersten Führungsebene statt.
Wöchentlich führen spezielle Teams Risikobewertungen durch, um Risiken unter Kontrolle zu halten; diese Teams sind nicht in die oberste Führungsebene eingebunden. Es werden Maßnahmen zur Risikominderung geplant, deren Fortschritt verfolgt wird, und neu identifizierte Risiken werden besprochen.

What is DocuWare doing to protect against personal data breaches? In accordance with the SOC 2 Type 2 controls, we have mechanisms of identification, assessment and notification of personal data breaches implemented.	**Was unternimmt DocuWare zum Schutz vor Datenschutzverletzungen?** In Übereinstimmung mit den SOC 2 Typ 2-Kontrollen verfügen wir über Mechanismen zur Identifizierung, Bewertung und Benachrichtigung bei Verletzungen des Schutzes personenbezogener Daten.
Do you promptly notify customers affected by a security breach? Yes, in accordance with our internal controls and applicable law.	**Benachrichtigen Sie die von einer Sicherheitsverletzung betroffenen Kunden umgehend?** Ja, gemäß unseren internen Kontrollen und geltendem Recht.
How does DocuWare ensure that vulnerabilities are properly identified, tracked and remediated? We use a variety of information sources to keep us informed about current CVEs. Based on this and on internal and external audits, we use an endpoint detection and response tool to properly identify vulnerabilities. As part of the risk management process, the CVEs are qualified and transferred to the mitigation process based on their criticality.	**Wie stellt DocuWare sicher, dass Schwachstellen richtig erkannt, verfolgt und behoben werden?** Wir verwenden eine Vielzahl von Informationsquellen, um uns über aktuelle CVEs zu informieren. Auf dieser Grundlage sowie auf der Grundlage interner und externer Audits verwenden wir ein Endpunkt-Erkennungs- und Reaktionstool, um Schwachstellen einwandfrei zu ermitteln. Im Rahmen des Risikomanagement-Prozesses werden die CVEs qualifiziert und je nach ihrer Kritikalität in den Abhilfeprozess überführt.
Do you have an incident management process for handling urgent security incidents in your company? Yes, in accordance with the SOC 2 Type 2 controls. The urgency handling process is also tested quarterly, to make sure that the automations work and staff is trained for the worst case. We have an on-call response team which is available 24x7 and ready to respond to reported incidents.	**Gibt es in Ihrem Unternehmen einen Prozess für die Behandlung dringender Sicherheitsvorfälle?** Ja, in Übereinstimmung mit den SOC-2-Typ-2-Kontrollen. Der Prozess der Dringlichkeitsbearbeitung wird außerdem vierteljährlich getestet, um sicherzustellen, dass die Automatisierungen funktionieren und die Mitarbeiter für den schlimmsten Fall geschult sind. Wir haben ein Bereitschaftsteam, das rund um die Uhr verfügbar ist und auf gemeldete Vorfälle reagieren kann.

Do you have a formal Disaster Recovery Plan (DRP)?
Yes. We have a documented disaster recovery plan with detailed instructions on how to recover from disasters. We can't give further insights here due to its sensitive nature.

2.6 Human Resources security

Does your organization conduct background checks on your employees and contractors during onboarding?

Yes.
Europe: For the ones that will receive elevated permissions, such as the staff administrating the DocuWare Cloud, and as permitted by law in the country of hiring.
United States: Everyone.

Does your organization conduct education verification of new employees and contractors?
Yes. As permitted by law in the country of hiring.

Upon hire, are the employees and contractors required to complete a series of compliance training to ensure they are meeting and understanding various company security policies?
If yes, do your active employees and contractors complete security awareness training on an annual basis?

The answer to both questions is yes.

Verfügen Sie über einen formellen Disaster Recovery Plan (DRP)?
Ja. Wir verfügen über einen dokumentierten Disaster Recovery Plan mit detaillierten Anweisungen für die Disaster Recovery. Wir können hier aus Vertraulichkeitsgründen keine weiteren Einblicke geben.

2.6 Sicherheit des Personals

Führt Ihr Unternehmen bei der Einstellung von Mitarbeiterinnen und Mitarbeitern sowie Auftragnehmern Hintergrundprüfungen durch?

Ja.
Europa: Für diejenigen, die erhöhte Berechtigungen erhalten, wie z. B. die Mitarbeiter, die die DocuWare Cloud administrieren, und im Rahmen der gesetzlichen Bestimmungen des Landes, in dem sie eingestellt werden.
Vereinigte Staaten: Alle.

Führt Ihre Organisation eine Überprüfung der Ausbildung von neuen Mitarbeitern und Auftragnehmern durch?
Ja. Soweit dies im Land der Einstellung gesetzlich zulässig ist.

Müssen Mitarbeiter und Auftragnehmer bei ihrer Einstellung eine Reihe von Schulungen zur Einhaltung der Vorschriften absolvieren, um sicherzustellen, dass sie die verschiedenen Sicherheitsrichtlinien des Unternehmens einhalten und verstehen?
Wenn ja, absolvieren Ihre aktiven Mitarbeiter und Auftragnehmer jährlich eine Schulung zum Sicherheitsbewusstsein?

Die Antwort auf beide Fragen lautet ja.

Is there an employee handbook that is reviewed, updated, and approved by executive management and also communicated to employees? Yes. For Europe and APAC, there is a list of SOPs instead of an employee handbook. For the US and LATAM, we have an employee handbook.	**Gibt es ein Mitarbeiterhandbuch, das von der Geschäftsleitung geprüft, aktualisiert und genehmigt sowie an die Mitarbeiterinnen und Mitarbeiter weitergegeben wird?** Ja. Für Europa und APAC gibt es eine Liste von SOPs anstelle eines Mitarbeiterhandbuchs. Für die USA und LATAM haben wir ein Mitarbeiterhandbuch.
If there is such a handbook, is it reviewed and approved at least annually? Yes. SOPs and the handbook are reviewed on an annual basis. This is required by the SOC certification.	**Wenn ja, wird es mindestens einmal jährlich überprüft und freigegeben?** Ja. Die SOPs und das Handbuch werden jährlich überprüft. Dies ist für die SOC-Zertifizierung erforderlich.
If If there is such a handbook, are employees required to read and sign it annually? Yes. Employees must read the SOPs and re-sign them if there have been changes to the SOPs.	**Wenn ja, sind die Mitarbeiter verpflichtet, es jährlich zu lesen und zu unterzeichnen?** Ja. Die Mitarbeiterinnen und Mitarbeiter müssen die SOPs lesen und erneut unterzeichnen, wenn diese sich geändert haben.
Do you require employees to sign off on an information technology security policy upon hire? Yes.	**Verlangen Sie von Ihren Mitarbeitern, dass sie bei ihrer Einstellung eine Richtlinie zur IT-Sicherheit unterzeichnen?** Ja.
Does your organization require targeted staff to complete additional training based on their roles and responsibilities? Yes.	**Verlangt Ihre Organisation von bestimmten Mitarbeiterinnen oder Mitarbeitern, dass sie je nach Aufgaben und Zuständigkeiten zusätzliche Schulungen absolvieren?** Ja.

2.7 Environmental, Social and Governance (ESG) / Corporate Social Responsibility (CSR)

What are DocuWare's contributions to ESG and CSR?
DocuWare places great emphasis on environmental and social management, as well as corporate social responsibility. We are therefore dedicated to our ecological and social responsibilities.

Sustainability & supply chain laws around the world are intended to improve the human rights and environmental situation by setting out requirements for a responsible management of supply chains. Due to its current size, DocuWare is not covered by these laws, but shares the values and supports the necessitiy of this legal regulation (e.g., Lieferkettensorgfaltspflichtengesetz, LkSG; Corporate Sustainability Due Diligence Directive, CSDDD).

Global compact: In September 2015, all 193 Member States of the United Nations adopted a plan for achieving a better future for all – laying out a path over the next 15 years to end extreme poverty, fight inequality and injustice, and protect our planet. At the heart of “Agenda 2030” are the 17 Sustainable Development Goals (SDGs) which clearly define the world we want – applying to all nations and leaving no one behind. As a member of the Ricoh Group, DocuWare participates in the agenda and actively shares and supports its goals.

2.7 Environmental, Social and Governance (ESG) / Corporate Social Responsibility (CSR)

Was trägt DocuWare in den Bereichen ESG und CSR bei?
DocuWare misst dem Umwelt- und Sozialmanagement sowie der Corporate Social Responsibility einen hohen Stellenwert bei. Damit bekennen wir uns zu unserer ökologischen und sozialen Verantwortung.

Nachhaltigkeits- und Lieferkettengesetze weltweit sollen die Menschenrechts- und Umweltsituation verbessern, indem sie Anforderungen an ein verantwortungsbewusstes Management von Lieferketten festlegen. Aufgrund seiner aktuellen Größe fällt DocuWare nicht unter diese Gesetze, teilt jedoch die Werte und unterstützt die Notwendigkeit dieser gesetzlichen Regulierung (z. B. Lieferkettensorgfaltspflichtengesetz, LkSG; Corporate Sustainability Due Diligence Directive, CSDDD).

Global Compact: Im September 2015 haben alle 193 Mitgliedstaaten der Vereinten Nationen einen Plan für eine bessere Zukunft für alle angenommen, der einen Weg für die nächsten 15 Jahre aufzeigt, um extreme Armut zu beenden, Ungleichheit und Ungerechtigkeit zu bekämpfen und unseren Planeten zu schützen. Das Herzstück der „Agenda 2030“ sind die 17 Ziele für nachhaltige Entwicklung (Sustainable Development Goals, SDGs), die klar die Welt definieren, die wir wollen – und die für alle Nationen gelten und niemanden zurücklassen. Als Mitglied der Ricoh-Gruppe beteiligt sich DocuWare an der Agenda und unterstützt aktiv deren Ziele.

2.8 Securing offices, rooms, and facilities

Are the facilities shared with any other organizations?
No.

Are facilities only accessible by people within your organization with a smart card system?
Yes.

Are visitors allowed in your facilities?
If yes, is there a check-in system in place to ensure their entry and exit?
The answer to both questions is yes.

Which authentication mechanisms are in place for all access to secure areas?
Corporate buildings: NFC-tags to open doors to other floors.

What is DocuWare's visitor policy?
A visitor policy is in effect for DocuWare buildings. Visitors need to register with time of arrival and check out upon leaving the buildings. The area for meetings with visitors and customers is separated from the rest of the buildings and secured with additional solutions.
Information on the high physical access security of Microsoft Azure data centers can be found at:
Datacenter physical access security information

2.8 Sicherung von Büros, Räumen und Anlagen

Werden die Einrichtungen mit anderen Organisationen geteilt?
Nein.

Sind die Einrichtungen nur für Personen innerhalb Ihrer Organisation mit einem Smartcard-System zugänglich?
Ja.

Sind Besucher in Ihren Einrichtungen erlaubt?
Wenn ja, gibt es ein Check-in-System, um sicherzustellen, dass sie das Gebäude betreten und verlassen?
Die Antwort auf beide Fragen lautet ja.

Welche Authentifizierungsmechanismen gibt es für den Zugang zu Sicherheitsbereichen?
Unternehmensgebäude: NFC-Tags zum Öffnen von Türen zu anderen Stockwerken.

Was ist die Besucherregelung von DocuWare?
Für die DocuWare Unternehmensgebäude ist eine Besucherrichtlinie in Kraft. Besucher müssen sich unter Angabe ihrere Ankunftszeit anmelden und beim Verlassen der Gebäude abmelden. Der Bereich für Besucher- und Kundengespräche ist vom übrigen Gebäude abgetrennt und mit weiteren Lösungen gesichert.
Informationen über die hohe physische Zugangssicherheit der Microsoft Azure Rechenzentren finden Sie hier:
Datacenter physical access security information

2.9 Business relations and vendor management

Does DocuWare have a third-party supplier security policy?

Yes.
Our third-party supplier security policy ensures that suppliers meet DocuWare's requirements and the applicable legislation for information security. We evaluate all suppliers in terms of their criticality to DocuWare's operations.

ll suppliers that are critical for DocuWare's business are registered and recorded in our Third-Party Supplier Register with the following information:
– Supplier name and contact details of the owner of the relationship
– Services provided to DocuWare
– Executed table on criticality

Criticality of business is derived in the following four categories. Suppliers are classified high, medium, or low depending on the highest rating they receive in one category:
– Service availability
– Impact on the quality of our services
– Impact on our revenue, either by losing revenue or by having to pay penalties
– Regulatory risks, e.g., by not complying with legal requirements

The entries in the supplier register are checked annually and on an ad hoc basis for up-to-dateness and quality of service provision.

2.9 Geschäftsbeziehungen und Lieferantenmanagement

Verfügt DocuWare über eine Sicherheitsrichtlinie für Drittanbieter?

Ja.
Unsere Sicherheitsrichtlinien für Drittanbieter stellen sicher, dass die Lieferanten die Anforderungen von DocuWare und die geltenden Gesetze zur Informationssicherheit erfüllen. Wir bewerten alle Lieferanten nach ihrer Kritikalität für den Betrieb von DocuWare.

Alle Lieferanten, die für DocuWare geschäftskritisch sind, werden in unserem Drittlieferantenregister mit den folgenden Informationen registriert und erfasst:
– Name des Lieferanten und Kontaktdaten des Inhabers der Beziehung
– Für DocuWare erbrachte Dienstleistungen
– Ausgeführte Tabelle zur Kritikalität

Die Kritikalität von Unternehmen wird in die folgenden vier Kategorien eingeteilt. Die Lieferanten werden je nach der höchsten Bewertung, die sie in einer Kategorie erhalten, als hoch, mittel oder niedrig eingestuft:
– Verfügbarkeit des Dienstes
– Auswirkungen auf die Qualität unserer Dienstleistungen
– Auswirkungen auf unsere Einnahmen, entweder durch Einnahmeverluste oder durch die Zahlung von Strafgeldern
– Regulatorische Risiken, z. B. durch Nichteinhaltung gesetzlicher Vorschriften

Die Einträge im Lieferantenregister werden jährlich und anlassbezogen auf Aktualität und Qualität der Leistungserbringung überprüft.

Does your organization have a third party risk assessment process in place in order to review vendors for services in DocuWare Cloud? Yes. We check their credit rating and we do an export control check. It is a DocuWare process that requires input from all relevant departments.	**Verfügt Ihr Unternehmen über einen Prozess zur Risikobewertung von Drittanbietern, um Anbieter von Diensten in DocuWare Cloud zu prüfen?** Ja. Wir prüfen ihre Kreditwürdigkeit und führen eine Exportkontrollprüfung durch. Es handelt sich um einen DocuWare Prozess, der die Mitarbeit aller relevanten Abteilungen erfordert. Das Verfahren wird zur Zeit überarbeitet und erweitert.
Does your organization outsource any IT or security functions to a third party service provider? Yes. Our information security management ensures that data and information are secured by means of principles and procedures.	**Lagert Ihr Unternehmen IT- oder Sicherheitsfunktionen an einen Drittanbieter aus?** Ja. Unser Informationssicherheitsmanagement gewährleistet, dass Daten und Informationen durch Richtlinien und Verfahren gesichert sind.
What is DocuWare's position regarding Artificial Intelligence (AI)? We are leveraging AI in our product, organization, and innovations to maximize customer and operational value. We are committed to a set of Trusted AI Principles, ensuring accuracy, reliability, security, privacy and compliancy, transparency, and human centricity in our usage.	**Wie steht DocuWare zum Thema Künstliche Intelligenz (KI)?** Wir nutzen KI in unseren Produkten, unserer Organisation und unseren Innovationen, um den Nutzwert für unsere Kunden und unseren Betrieb zu maximieren. Wir verpflichten uns zu einer Reihe von Grundsätzen für vertrauenswürdige KI, die Genauigkeit, Zuverlässigkeit, Sicherheit, Datenschutz und Compliance, Transparenz und einen menschenzentrierten Ansatz bei der Nutzung gewährleisten.
What measures have been taken around the AI Act of the European Union? So far, we rolled out an AI literacy training to all colleagues and we created a risk assessment of the internally used AI. As for the customer-facing AI we are having those assessed by external legal counsel (as of July 2025).	**Welche Maßnahmen wurden im Zusammenhang mit dem KI-Gesetz (AI Act) der Europäischen Union ergriffen?** Bislang haben wir eine KI-Schulung für alle Mitarbeiterinnen und Mitarbeiter durchgeführt und eine Risikobewertung der intern verwendeten KI erstellt. Die kundenorientierten KI-Anwendungen werden derzeit von einem externen Rechtsberater geprüft (Stand Juli 2025).

Is there any more information about AI at DocuWare?
Yes, there is. Under this link our White Paper about "AI-based data processing with DocuWare" can be found:
White Paper AI-based data processing with DocuWare

Gibt es weitere Informationen zu KI bei DocuWare?
Unter diesem Link finden Sie unser White Paper zum Thema „KI-basierte Datenverarbeitung mit DocuWare“:
White Paper KI-basierte Dokumentenverarbeitung mit DocuWare

Abkürzungen

AI	Artificial Intelligence
AES	Advanced Encryption Standard
BCP	Business Continuity Plan
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Cyber Security Authority)
BYOD	Bring Your Own Device
BYOK	Bring Your Own Key
C5	Cloud computing compliance criteria catalogue of BSI in
CCPA	California Consumer Privacy Act
CI/CD	Continuous Integration/Continuous Delivery or Deployment
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DES	Data Encryption Standard
DLP	Data Loss Prevention
DPA	Microsoft Data Protection Addendum
DR	Disaster Recovery
DSC	Desired State Configuration
DSK	Datenschutzkonferenz (Data privacy conference)
ECJ	European Court of Justice
FADP	Federal Act on Data Protection (Switzerland)
GDPR	General Data Protection Regulation (EU)
HIPAA	Health Insurance Portability and Accountability Act
HSTS	HTTP Strict Transport Security
IDS	Intrusion detection system
IPS	Intrusion prevention system

KPI	Key Performance Indicator
MFA	Multi-factor authentication
NDA	Non-disclosure agreement
OSS	Open-source software
OWASP	Open Web Application Security Project
PFS	Perfect Forward Secrecy
QA	Quality Assurance
R&D	Research and Development
RPA	Records of Processing Activities (GDPR)
SCC	Standard Contractual Clauses
SDLC	Software Development Life Cycle
SHA	Secure Hash Algorithm
SOC	System and Organization Controls (AICPA)
SOP	Standard Operating Procedure
VLAN	Virtual Local Area Network
WAF	Web Application Firewall

OCG CERTIFICATION
ISO/IEC 27001

CERTIFICATE

Information Security Management System
ISO/IEC 27001:2013

The Austrian Computer Society (OCG) certifies that the implementation and continuous improvement of an Information Security Management System (ISMS) of the Certified Organisation (stated below) complies with the requirements of ISO/IEC 27001:2013.

Certified Organisation:

DocuWare **DocuWare GmbH**
Planegger Straße 1, 82110 Germering, Germany

Certified location, products, processes, services and scope:
Location in Germering Setup and operation of the document management SaaS solution **DocuWare Cloud** hosted in the cloud environment.
This includes all related significant internal services and processes of the company teams Cloud Operations and Platform Services, Cloud Customer Lifecycle, Cloud Security, Customer Support, Compliance Assurance and Security and Compliance.

Date of initial certification: 18.07.2023

Expiry Date: 17.07.2026

Certificate No: 023/1_2023

For and on behalf of the Austrian Computer Society (OCG)

Vienna, 19 July 2023
Place, Date

Thomas Mück
OCG President

OCG has been accredited as certification body for management systems according to ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 standards for certifications to the ISO/IEC 27001 standard by the National Accreditation Body „Akkreditierung Austria" since 5 July 2013 (ID-number: 0948).

Austrian Computer Society I Wollzeile 1 I 1010 Vienna, Austria I Phone: + 43 1 5120235-0 I info@ocg.at | www.ocg.at

CERTIFICATE

dqs

This is to certify that

DocuWare

DocuWare GmbH

Planegger Straße 1
82110 Germering
Germany

has implemented and maintains a **Quality Management System**.

Scope:
Development, sales and support of software for document management and workflow automation

Through an audit, documented in a report, it was verified that the management system fulfills the requirements of the following standard:

ISO 9001 : 2015

Certificate registration no.	31617252 QM15
Valid from	2023-12-29
Valid until	2026-12-28
Date of certification	2023-12-29

IAF

DAkkS Deutsche Akkreditierungsstelle D-ZM-16074-01-00

DQS GmbH

Christian Gerling
Managing Director

DQS IS A MEMBER OF IQNET

Accredited Body: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
The validity of this certificate can only be verified by the QR-code.

SWISS INFORMATION GOVERNANCE COMPETENCE CENTER

ZERTIFIKAT

Das krm Kompetenzzentrum Records Management bestätigt, dass
der Service „DocuWare Cloud" der Firma DocuWare GmbH, Germering (DE) die Anforderungen der Geschäftsbücherverordnung GeBüV (Schweiz) erfüllt.

DocuWare Cloud

UNTERSUCHTE VERFAHREN UND SYSTEME
DocuWare Cloud Base / Pro / Enterprise / Large Enterprise

GESETZLICHE GRUNDLAGEN UND NORMEN
OR 958f, Geschäftsbücherverordnung, MWSTG Archivierungsteil,
Ordnungsmässigkeitskatalog krm.

ANALYSEVERFAHREN
Im Oktober 2023 wurde das Verfahren geprüft. Die Resultate wurden in einem Prüfbericht dokumentiert und dem Geprüften übergeben.

RESULTAT
Die Lösung erfüllt die gesetzlichen Anforderungen der erwähnten Rechtsgrundlagen.

ZERTIFIZIERUNGS-ID
2023-V016, 01.11.2023
Zertifikat gültig bis 31.12.2025.
Status, Nutzungsbedingungen und Vorgabekonfiguration einsehbar unter:
www.digitalkonform.ch/zertifizierte-produkte-und-anwender

DIE GESCHÄFTSFÜHRER

Bruno Wildhaber

Digital signiert von Bruno Wildhaber
DN: cn=Bruno Wildhaber, c=CH, o=Kompetenzzentrum Records Management, ou=KRM, email=bruno.wildhaber@krm.swiss
Grund: Ich bestätige die Genauigkeit und Richtigkeit des Dokuments
Ort: Schwerzenbach
Datum: 2023.11.25 13:07:33 +01'00'

SWISS INFORMATION GOVERNANCE COMPETENCE CENTER

ZERTIFIKAT

Das krm Kompetenzzentrum Records Management bestätigt, dass
die Software DocuWare Version 7.x On-Premises der Firma DocuWare GmbH, Germering (DE) die Anforderungen der Geschäftsbücherverordnung GeBüV (Schweiz) erfüllt.

DocuWare 7.x On-Premises

PROFESSIONAL / ENTERPRISE SERVER

UNTERSUCHTE VERFAHREN UND SYSTEME
DocuWare 7.3 bis 7.9 On-Premises Professional / Enterprise Server

GESETZLICHE GRUNDLAGEN UND NORMEN
OR 958f, Geschäftsbücherverordnung, MWSTG Archivierungsteil,
Ordnungsmässigkeitskatalog krm.

ANALYSEVERFAHREN
Im Oktober 2023 wurde das Verfahren untersucht und vor Ort geprüft. Die Resultate wurden in einem Prüfbericht dokumentiert und dem Geprüften übergeben.

RESULTAT
Die Lösung erfüllt die gesetzlichen Anforderungen der erwähnten Rechtsgrundlagen.

ZERTIFIZIERUNGS-ID
2023-V016, 01.11.2023
Zertifikat gültig bis 31.12.2025
Status, Nutzungsbedingungen und Vorgabekonfiguration einsehbar unter:
www.digitalkonform.ch/zertifizierte-produkte-und-anwender

DIE GESCHÄFTSFÜHRER

Bruno Wildhaber

Digital signiert von Bruno Wildhaber
DN: cn=Bruno Wildhaber, c=CH, o=Kompetenzzentrum Records Management, ou=KRM, email=bruno.wildhaber@krm.swiss
Grund: Ich bestätige die Genauigkeit und Richtigkeit des Dokuments
Ort: Schwerzenbach
Datum: 2023.11.25 13:08:39 +01'00'

LOGICIEL

www.marque-nf.com

Certificat

Certificate

No 203/437-7

Date d'émission *(issuedate)* **: 02/04/25**

Date de renouvellement *(renewal date)* **: 02/04/26**

Numéro de version 7.12 certifiée le 02/04/25 conforme aux règles NF203 V6.0

Issue number 7.12 certified on 02/04/25 according to NF203 V6.0 rules

Première admission le 22/09/21 pour la version 7

First admission on 22/09/21 according to issue 7

DOCUWARE

17 RUE DU COLISEE - 75008 PARIS

Est autorisée à apposer la marque NF en application des règles générales de la marque NF et du référentiel de certification de l'application NF Logiciel (NF203) pour le produit :

Is authorized to affix the NF mark on the product, in accordance with the general rules of the NF mark and the NF Logiciel (NF203) rules.

DocuWare, version 7.12,
WEB / WINDOWS - CCFN

Le produit désigné est certifié conformément aux Règles de certification (parties 1 à 9) NF Logiciel et à la norme ISO/CEI 25051 : 2014. *The designated product is certified in accordance with the Certification rules NF Logiciel (parts 1 to 9) and the ISO/IEC 25051 : 2014 standard.*

Le produit est conforme aux exigences spécifiques concernant les Composants Coffre-Fort Numérique (CCFN) de la Partie 10 des règles de certification NF Logiciel et à la NFZ42020. *The product conforms to the requirements conceming the Digital vault storage (CCFN) defined in part 10 of the NF Logiciel rules and NFZ42020.*

Le présent certificat, renouvelable, est valable jusqu'au 02/04/26, sous réserve des contrôles effectués par INFOCERT et/ou AFNOR Certification et sauf retrait, suspension ou modification. *This certificate, renewable, is valid until 02/04/26, subject to the controls carried out by INFOCERT and/or AFNOR Certification and except withdrawal, suspension or modification.*

Ce certificat annule et remplace tout certificat antérieur. *This certificate supersedes all previous certificates*

La validité de ce certificat peut être vérifiée sur le site internet d'AFNOR Certification www.marque-nf.com
The validity of the certificate can be checked on the AFNOR Web site www.marque-nf.com.

Julien NIZRI
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

CERTI F 1332.4 11/2014

Secrétariat technique assuré par
Technical secretariat provided by
INFOCERT
http://www.infocert.org
admin@infocert.org