White Paper DocuWare Cloud

For DocuWare version 7.10 and higher

May 2024

This document was created using AuthorIT™.

Disclaimer

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by DocuWare GmbH. DocuWare GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

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

Contents

1 Introduction

1.1 Objectives of this White Paper

DocuWare Cloud is a multi-client cloud solution for document management and workflow automation. This White Paper describes the technical features of DocuWare Cloud, focusing mainly on the technical and organizational measures implemented by DocuWare in the areas of security (IT security and data protection) and scalability. Further topics include support, for example in the event of data migration, as well as compliance and certifications. The White Paper is primarily aimed at technical employees of prospects, customers, and sales partners as well as consulting companies or specialist media.

1.2 Introducing DocuWare Cloud

DocuWare Cloud is a "software as a service" (SaaS) solution. DocuWare in turn relies on the services of Microsoft Azure as a "platform as a service" (PaaS) for its own offering. All customer documents, files, and metadata are stored on Azure Storage. The databases are hosted by Azure SQL (managed service).

The scope of this White Paper is limited to the direct services of DocuWare. On its own website, Microsoft describes the services provided by Microsoft Azure and the associated IT security and data protection measures on which DocuWare is based.

2 Security

Customer data in DocuWare Cloud is protected in accordance with generally accepted technical rules and standards. This is ensured by the IT infrastructure and technologies from Microsoft Azure Security Services and DocuWare, as well as their compliance with current data protection guidelines.

2.1 IT Security

DocuWare Cloud ensures the security of your data through encryption of documents and communication, a sophisticated rights concept, access restrictions, and security audits.

Document encryption

All documents archived in DocuWare Cloud are automatically encrypted using the Advanced Encryption Standard (AES). Documents migrated from DocuWare on-premises systems can be encrypted subsequently. AES is a symmetric encryption method that meets the highest security requirements. For example, it is approved for use by the US government as the encryption standard for documents with the highest security clearance level (top secret).

In the AES procedure, an asymmetric key pair is generated for each file cabinet. The private key is used in turn to encrypt the symmetric keys which are created when the documents in a file cabinet are encrypted. The private key of the file cabinet is then encrypted again with a master key.

For maximum protection, DocuWare uses a 256-bit key length for encryption with AES. A key length of 1024 bits is used to encrypt the symmetric keys. A new symmetric key is generated for each document. This means that even during cryptanalysis, no patterns can be detected and no keys can be calculated.

Encrypting communication

Within a data center used by DocuWare, all customer data is secured via a VPN (virtual private network). In addition, the network infrastructure is virtualized and the virtual network is isolated from the outside.

The current TLS protocol (successor protocol to SSL) is used to encrypt data traffic between users and the data center, provided it is supported by the browser used. TLS is used for all traffic based on HTTP (HTTPS) and TCP. This means that users can immediately see in their browser whether their connection is secure and validated: When the connection is secure, the URL address turns green (except in Google Chrome).

For further protection against external attacks, there are additional security layers and functions, such as HSTS for protection against protocol downgrade attacks and cookie hijacking.

Authentication

For secure and convenient authentication, you can use Single Sign-On (SSO) to use the credentials of just one account for all DocuWare applications. To do this, you need to connect your organization to an identity provider. DocuWare supports Microsoft Azure Active Directory und Microsoft Active Directory Federation Services (4.0) as identity providers.

By clicking on the single sign-on button in the DocuWare login dialog, the user is redirected to the identity provider. After successful authentication, login in DocuWare is automatic, regardless of whether the user logs in via DocuWare Client, DocuWare Mobile, the Desktop Apps, in configuration or administration.

DocuWare also supports Microsoft Active Directory Federation Services (ADFS) for SSO. DocuWare uses OpenID Connect for this, so the ADFS version in Windows Server 2016 or higher is required, since OpenID Connect is only supported there.

It should be noted that in Azure Active Directory, Microsoft makes some default settings for logout in single sign-on, specifically persistence of browser settings and validity period of tokens. Detailed documentation is available on the Microsoft website:

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

Rights concept

DocuWare Cloud has a sophisticated rights system. An essential element of rights administration in DocuWare is the distinction between functional rights and file cabinet rights.

Functional rights are assigned per DocuWare organization and refer to specific functions. These include, for example:

- Manage users
- Configure file cabinets and document trays
- Design workflows
- Use stamps
- Create and edit configurations of DocuWare components, such as Connect to Outlook, Smart Connect, or DocuWare Forms

File cabinet rights refer to a specific file cabinet and the documents stored in it. File cabinet rights include:

- Administrative permissions, e.g. manage rights or dialogs, or migrate documents
- General permissions relating to documents in the file cabinet, e.g. store, search, edit, or delete documents
- Overlay permissions, e.g. stamp documents, add annotations or graphical elements to documents, or delete annotations
- Index field permissions, e.g. change field contents or use field entries that are not in a select list

Rights for users and administrators

For all configurations of DocuWare Cloud, for example document trays, file cabinets, or forms, you assign permissions – either directly to users or via roles. There are two different types of permissions: User rights allow you to use the object in question. Administrator rights allow you to change the object or the associated configuration.

Access limitation through data separation

DocuWare Cloud strictly separates customer data – one DocuWare organization per customer – from system data.

Administrators of DocuWare Cloud systems only have access to the system data that is urgently needed for operation. See also the section "System Support with 24/7 Availability> Maintenance."

The DocuWare administrators of the customers have full access to their respective organization settings, but not the settings of the DocuWare system.

Security audit

Regular external and internal penetration tests help to maintain the security of the systems at the level of the generally accepted technical rules of technology. The results of the penetration tests are critically scrutinized by the external auditors during regular certification for the SOC2 standard.

In addition, Azure Security Services provides detailed risk reporting so that any problems that arise with Microsoft Azure can be resolved immediately.

Customers can create document, archive, and organization-level audit reports within their organization and export them to universal CSV format for easy analysis. For example, this makes it clear who changed which settings, or stored or deleted which documents, and when. For example, the records can be used to document compliance with legal guidelines.

Analysis of telemetry data

Real-time security analyses of telemetry data are carried out to check whether unusual events are occurring within DocuWare systems in comparison to normal operation. If such events are detected, appropriate action shall be taken. The investigations include:

- Database accesses (access location and command semantics)
- Error rate
- Performance changes
- Login attempts
- Critical system updates
- Network traffic

2.2 Data Security and Data Protection

Data security and data protection are business-critical functions that require continuous monitoring and management. DocuWare reliably guarantees the security, protection, and recoverability of customer data when configured and handled correctly. DocuWare supports the customer in their compliance with the applicable regional data protection law. Data protection through technology design (privacy by design) has been a key principle for DocuWare since the company was founded in 1988. The technical and organizational measures (TOMs) can be found here.

Data security

DocuWare Cloud always stores multiple 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. All documents that customers work with (productive data) are encrypted (see section Document encryption) and stored in a Microsoft Azure data center (main location). This applies both to the documents in file cabinets and to those in document trays.
In addition, two copies of each individual document are stored in this data center immediately after it enters or is modified in DocuWare.

Furthermore, to secure the entire live data inventory against major incidents such as earthquakes or aircraft crashes, three copies of each document are copied to a second data center located at another location in the same region (georedundant storage, GRS). Both locations always have the current version of each document.

Data protection

The operation of customer systems is subject to the applicable regional data protection laws.

Data center locations: Customer data is hosted in Microsoft Azure data centers in the following regions: EU, US, Japan, and Australia/New Zealand.

Region	Main location	GRS location
EU	North Europe, Ireland	West Europe, Netherlands
US	Central US, state of Iowa	East US 2, state of Virginia
Japan	Japan East, Tokio/Saitama	Japan West, Osaka
Australia/New Zealand	Australia East, New South Wales	Australia Southeast, Victoria

Country-specific mapping to data centers: A detailed list with the country-specific mapping of DocuWare Cloud customers to Microsoft Azure regional data centers can be found here.

Using Microsoft Office Online: When a customer uses Microsoft Office Online, the document is transferred to a Microsoft Azure data center, usually one near the user's geographic location. Since DocuWare has no influence on the data center used, it cannot be guaranteed that documents will not leave the respective region of the data center used by DocuWare – EU, USA, Japan, Australia/New Zealand.

Backup

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.

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.

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, 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 predominantly 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.

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

Recovery is possible only in cooperation with DocuWare Support. If recovery is necessary due to incorrect operation on the part of the customer (e.g., due to accidental deletion or modification of documents), the costs for recovering will be additionally charged.

3 Scalability

Both DocuWare itself and Microsoft Azure, as part of its platform as a service (PaaS) infrastructure, offer extensive methods and technologies for scalability.

Scalability per customer

DocuWare Cloud supports teams of all types and sizes. Its storage volume and number of user licenses can be flexibly adapted to the relevant company size and document volume.

When certain storage limits are reached or exceeded, DocuWare automatically sends email notifications to the organization administrator and the ADP contact. This applies in each case when 85%, 90%, 95%, 99%, and 100% of the storage limit is reached or exceeded. The storage volume is calculated according to the formula *1 GB = 1000*1024*1024*.

- When 85% of the storage limit is reached or exceeded, these notifications go to the ADP contact in the case of an indirect customer, and to the organization administrator in the case of a direct customer.
- When 90%, 95%, 99%, and 100% of the storage limit is reached or exceeded, the notifications go to the organization administrator and ADP contact in the case of an indirect customer, and only to the organization administrator in the case of a direct customer.

Notifications are sent when the remaining storage volume is less than 100 days. The calculation is based on the storage behavior of the last 30 days.

Scaling the Cloud system

The DocuWare Cloud System is automatically scaled according to the number of users, the number of requests from these users and the resulting load on the system. In the time slots in which a particularly large number of users are working with DocuWare simultaneously, additional servers are automatically started to handle the higher load. Since DocuWare Cloud is a so-called public cloud, scaling takes place per system and not per customer organization.

4 Integration Capability

DocuWare Cloud can be connected to almost any other enterprise application to maximize the benefits of document management and workflow automation. This works regardless of whether this application is operated as an on-premises system or is cloud-based. More information can be found in the DocuWare White Paper Integration.

5 System Support with 24/7 Availability

Monitoring

Continuous automatic monitoring of all processes takes place at the Microsoft Azure data center. Any conspicuous incidents are automatically reported to DocuWare's system support. Monitoring includes:

- Constant performance controls
- Regular complete tests of the DocuWare basic functions
- Statistical surveys of customer usage behavior, for example on how many actions customers perform in a particular time window (e.g. document search and storage, login), in order to enable performance improvements

In the event of irregularities, DocuWare's system support team intervenes immediately with 24/7 availability.

Hotfixes and upgrades

Once or twice a year, the new version of DocuWare is installed in customer organizations. To do this, the corresponding organization is taken offline, the upgrade is performed, and the organization is then brought back online with the new DocuWare version.

DocuWare will inform customers about the planned update four weeks in advance. In the event of an error, the organization is brought back online with the previous DocuWare version to ensure that no longer downtimes occur.

Customers should always keep the locally installed components (Desktop Apps) up to date. Users can easily perform the corresponding updates themselves, as long as they are authorized to install software locally. Otherwise, the IT administrator can perform the update as a silent install using a software management solution.

Maintenance

Full or extensive administration rights for DocuWare Cloud systems are required for certain maintenance activities. In order to guarantee data security that complies with the generally accepted technical rules and standards, access by maintenance administrators is subject to logging.

In addition, the following security mechanisms apply:

- Any access to DocuWare Cloud systems takes place in an RDP session.
- To be able to start an RDP session, an administrator must use defined, specially protected IP addresses to log in to a VPN that is secured by certificates and is only available to the administrators.
- Every DocuWare Cloud administrator has an own ID. It is therefore always possible to determine who logged in to which system.
- All administrators are trained and, in particular, have been instructed regarding the highly sensitive, protected handling of data such as certificates and passwords.

6 Data Handover upon Termination of the Contract

Customer data belongs to the customer – always

If a customer decides to terminate the contractual relationship, DocuWare will, upon request, assist the customer in downloading their documents from the DocuWare Cloud system and/or migrating them to another system. There are two ways of doing this:

1. Smaller quantities of documents that do not need to be processed quickly, or no longer need processing at all, can be exported and used as stand-alone archives with DocuWare Request. This option is limited to a maximum of 50,000 documents or 10 GB storage volume.
2. For larger amounts of data and many documents that are integrated into current processes, the specialists from DocuWare Processional Services can help. Their fee-based services offer the following benefits:
   -- After consultation with the customer, the documents are accessed directly in the data center and in such a way that large amounts of data are transferred in the shortest possible time.
   -- Live documents as well as documents integrated into current processes are migrated promptly into the processes of a new system, thus minimizing interruptions to workflows.
   -- Solutions specially tailored to the workflows and document types used by the customer are developed.

Following termination of the contractual relationship, all customer data within the DocuWare Cloud system and all backup data will be securely and irrevocably deleted: Data is deleted from the productive system after 60–90 days, and from the cold storage after a further 30 days at the latest.

It is no longer possible to restore the data after this point.

7 Compliance and Legal

Certifications of DocuWare and DocuWare Cloud

DocuWare is certified and helps your business to be compliant. Product, company and platform meet the requirements of standards and regulations to ensure your information and data security, for example HIPAA, CCPA, GDPR, APPI, SOC 2 Type 2, ISO 27001 and many more.

The certifications relating to a software version are not renewed for each new version, but instead at regular intervals. More information on DocuWare certifications.

Microsoft Azure certifications

Microsoft leads the industry in establishing clear security and privacy requirements and then consistently meeting these requirements. Azure meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. Learn more about Microsoft Azure certifications.

Changes to the Cloud White Paper

DocuWare reserves the right to adapt the content of the Cloud White Paper, in particular with regard to the described services and standards, for legitimate reasons, provided that this is reasonable for the customer. In particular, a justified reason may exist in the event of further technical development, the introduction of new services or standards, changes in the range of services offered by service providers used (in particular Microsoft), or changed legal or official requirements.