White Paper
DocuWare Cloud

For DocuWare Version 7 and higher

January 2019

This document was created using AuthorIT™, Total Document Creation.

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
Therese-Giehse-Platz 2
D-82110 Germering
www.docuware.com

DocuWare

Contents

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.

2 Introduction

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.

3 Security

Customer data in DocuWare Cloud is protected in accordance with the generally accepted rules of technology. 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.

3.1 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 documents

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.

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 the customers' 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 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 is taken. The investigations include:

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

3.2 Data Security and Data Protection

DocuWare Cloud reliably guarantees the security, protection, and recoverability of customer data when configured and handled correctly. In this way, it 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

All documents that customers work with (productive data) are 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 productive 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 the systems is subject in each case to the regionally applicable data protection law. Data from customers in the EMEA region is hosted in data centers in the European Union (EU). The current main location is Dublin (Ireland); the GRS location is Amsterdam (Netherlands). The data is subject to the EU General Data Protection Regulation (GDPR).

Data from our customers in the North and South America regions is hosted in data centers in the United States. The current main location is in the state of Iowa; the GRS location is in Virginia. The data of American customers is subject to US data protection guidelines.

Backup

If the customer has accidentally deleted documents, these can be restored if necessary. Also if documents were changed erroneously, any previous version can be restored. In both cases, the restrictions below apply.

To enable a recovery, DocuWare backs up both the databases 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 and in the state of Washington (USA) for the Americas.

A copy of each document is made and stored in a continuous backup. This happens shortly after the document has been saved or modified in DocuWare. The backup after document modification creates a new copy of the document. This is saved in addition to already existing backups of the document. This always applies, regardless of whether document versioning is enabled or disabled in DocuWare.

The cold storage is physically completely separate from the DocuWare domain, which means that the database is also protected against possible damage events in the DocuWare domain. The generation of backups in the cold storage is automatically monitored continuously. The backups in the cold storage are stored for at least one year.

By manually importing the backup data into the live system, a DocuWare organization can be completely restored in cooperation with DocuWare Support. If the import of backup data is necessary due to incorrect operation on the part of the customer (e.g., due to accidental deletion or modification of documents), the support costs for the recovery will be charged to the customer.

A document can only be recovered if it has not been modified or deleted during its backup. The backup of a new or modified document is initiated in the file cabinet no earlier than five seconds after the document has been written.

To make sure that the correct database version is used for the recovery, DocuWare requires the customer to provide information about when the document to be recovered was still visible in the file cabinet. In order for the associated database entries to be restored, the customer must send the request to DocuWare Support no later than 30 days after deleting or modifying the document.

In addition to the documents, full backups for the SQL databases are carried out in the cold storage at weekends, usually during regional nighttime.

File share snapshots

In addition to document backup, Microsoft's Azure Files service generates file share snapshots once a week for each organization. These include the changes from the respective previous status. The snapshots are stored for at least one year.

All of a customer's documents are thus protected against damage risks at different storage locations and in compliance with the respective regional data protection laws.

DocuWare reserves the right to change the locations of the productive, GRS, and backup data (especially if the locations offered by Microsoft Azure are changed) or to add further locations as long as they remain within the respective economic territory (EU or USA).

4 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.

Scaling the Cloud system

DocuWare Cloud is automatically scaled according to the number of users, the amount of data, and the size of the workload. Since DocuWare Cloud is a public cloud, the scaling takes place per system and not per customer organization.

Performance and load balancing

The balancing of loads across all available services ensures a consistently high performance of the entire DocuWare system. DocuWare Cloud responds quickly and dynamically to fluctuating load conditions with load balancing, by scaling existing services higher or lower and/or adding complete services.

5 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.

6 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 rules of technology, 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.

7 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: after 60 to 90 days at the main location and GRS location, and then in the following quarter in the cold storage.

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

8 Compliance and Legal

Certifications of DocuWare and DocuWare Cloud

The certifications relating to a software version are not renewed for each new version, but instead at regular intervals. For more information on DocuWare certifications, please go to https://start.docuware.com/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.