DocuWare

DocuWare Security FAQs

All about DocuWare's security measures in compliance area,
for DocuWare Cloud and IT

June 2022

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. The English version of this paper shall govern for all purposes.

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

DocuWare

Contents

1 Compliance

1.1 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 external Data Protection Officer (DPO). We have an internal Compliance Manager.

1.2 Organizational data protection measures

1.2.1 DocuWare's internal organizational measures

What are DocuWare's internal organizational measures?	DocuWare takes the following internal organizational measures for data protection: – SOP IT Security & Data Protection – Penetration tests – Records of data processing – Data protection training – Confidentiality agreements for employees – Privacy and cookie policy

What does the SOP IT Security & Data Protection cover?	The SOP IT Security & Data Protection contains all the requirements of the GDPR (General Data Protection Regulation) and the resulting processes and measures. Furthermore, it deals with data protection according to US law, e.g., the CCPA (California Consumer Privacy Act) and HIPAA (Health Insurance Portability and Accountability Act). Standard Operating Procedures (SOPs) are our internal regulations for different subjects. 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 The second part of the SOP 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 certification. SOC 2 Type 2 is a very 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. See also Information for service organization management published by AICPA. 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 SOC 2 Type 2 standard. The audit period will be one whole year starting in 2022. 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?	We have external auditors perform penetration tests twice a year. They help to further improve our high security level. The results of these tests are not published but the results are audited for the SOC 2 Type 2 certification. The SOC 2 Type 2 auditors also follow up on findings and the measures taken to remedy them.
What are the Records of Data Processing (RDPs)?	GDPR requires companies to create so-called records of data processing 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 (RDP) for all our internal processing operations. Like our SOPs, the RDP 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.
What does the data protection training cover?	All DocuWare employees (worldwide) participate in an annual data protection training and test. Evidence exists but is treated confidentially for data protection reasons.
What does the confidentiality agreements for employees cover?	All employees sign a general confidentiality agreement 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.
What is DocuWare's privacy and cookie policy?	Our general GDPR-based privacy policy can be found at: EN | DE | ES | FR | JA The CCPA privacy policy can be found here. Our cookie policy can be found at: EN | DE | ES | FR All sites are checked and adapted at regular intervals to ensure that they are up to date.

1.2.2 Data protection officer

Who is DocuWare's data protection officer?	Contact details of our data protection officer: Mr. Stephan Hartinger Coseco GmbH Phone: +49-8232 80988-70 Email: datenschutz@coseco.de He is registered with the relevant supervisory body, the Bavarian State Office for Data Protection Supervision. In addition, there are native-speaking data protection coordinators: EN: Data Protection Officer (docuware.com) DE: Datenschutzbeauftragter (docuware.com)

1.2.3 Certifications

What certifications does DocuWare hold?	DocuWare is certified according to ISO 9001, ISO 27001 and SOC 2 Type 2 as of 2021 (until 2020 SOC 2 Type 1). In addition, the system meets the requirements of the German (GoBD), Swiss (GeBüV) and Spanish tax authorities. DocuWare is HIPAA compliant. All current certifications can be found here: EN | DE | ES | FR

1.2.4 Technical and Organizational Measures (TOMs)

Where can someone find DocuWare's TOMs?	Our current TOMs within the DocuWare Group can be found on our website at: EN | DE They are subject to an annual review.

1.2.5 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: EN | DE

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 backups after a further 60 days at the latest.
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

1.3 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)

1.3.1 The ECJ's decision on the EU-US Privacy Shield

What is the content of the ECJ's decision on the EU-US Privacy Shield?	In its July 2020 decision, the European Court of Justice (ECJ) invalidated the Privacy Shield as a data transfer mechanism for personal data to the US. The then current version of the standard contractual clauses were reviewed and upheld in the same ruling. However, data exporters have to examine their enforceability for each individual data transfer. If they cannot be sufficiently enforced in the destination country, the data exporter must take additional measures to the data processing agreement and the standard contractual clauses.

1.3.2 What does DocuWare do about Standard Contractual Clauses and the additional measures?

Standard Contractual Clauses instead of Privacy Shield	Since the ruling, DocuWare entered into Standard Contractual Clauses (SCCs) with all companies that previously used the Privacy Shield and new incoming suppliers, when applicable. The European DocuWare entities have implemented the SCCs with DocuWare Corporation. The SCCs are also in place with Microsoft. **New SCC 2021** The EU Commission published new SCCs in the Official Journal on June 7, 2021 and grants a transition period of 18 months until December 27, 2022. Currently we are working on concluding the SCC 2021 with all relevant business partners, either existing ones or new ones. We kindly ask for your understanding that this big undertaking will take some time to finish.
Supplementary measures	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. Currently, 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. **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)

1.3.3 How does DocuWare process customer data?

How does DocuWare process customer data in third countries?	Our European customers' data resides in the Microsoft Azure data center in Ireland, with 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: **Second-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. **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 can at: EN: 24/5 Support · DocuWare Support Portal DE: 24/5 Support · DocuWare Support Portal
Where can I find information about DocuWare subcontractors?	All subcontractor relationships can be found at: EN | DE | ES | FR **Purpose of subcontractor assignments** The purpose is to provide the DocuWare Cloud Services at all times. **Contracts with subcontractors** In addition to the main contract, a data processing agreement and SCC, if applicable, have been entered into with all subcontractors.

Which subcontractors DocuWare works with?	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 and 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. **Microsoft** Information about data protection at Microsoft can be found here. EN: General Data Protection Regulation, GDPR Overview (microsoft.com) DE: Datenschutz-Grundverordnung, Übersicht (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. **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. 4. **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 Security for DocuWare Cloud

2.1 General

2.1.1 Cloud provider

Which Cloud provider is used?	DocuWare Cloud uses the Microsoft Azure Public cloud. The datacenter used for all resources is fixed to a dedicated region (US, EU, Japan or Australia/. New Zealand). Customers from other regions will currently be assigned to one of those datacenters. Data of one customer stays in one privacy region. Regional mapping to data centers

2.1.2 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 exact the same version and configuration as the one which was tested. In addition, it enables seamless rollback in rare cases, when updated software shows bugs in production.

2.1.3 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. Thus, only computing or networking resources are shared.

2.1.4 Operating DocuWare Cloud

Who is operating DocuWare Cloud?	DocuWare Cloud is operated and monitored by a dedicated DocuWare team with 24x7 standby: Cloud Operations (DevOps). Automated scale-out 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.
Security first – what does that mean?	Data and database contents of DocuWare Cloud customers is encrypted “at rest” (when stored on disk or in the database) and such not accessible even to DocuWare Cloud operators. Access of Cloud Operations team to cloud resources is performed from a restricted and separated network and secured by VPN connections. Any actions performed by the Cloud Opera¬tions team are recorded in audit logs.
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 suspected incident or problem, any DocuWare employee can immediately alert responsible standby operators at any point in time (24x7).
What is the cloud management portal?	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.
To which degree does the DocuWare Cloud comply to 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).

2.2 Security aspects

2.2.1 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.
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 scenarios (BYOK) are not supported.

2.2.2 Access control

How do you handle role provisioning and deprovisioning?	Role provisioning for Cloud Operators is handled according to SOC 2 Type 2: workflows for onboarding, department move and offboarding are in place and they are reviewed regularly.
Do you regularly conduct auditing of user access and privileged access accounts?	Yes. According to SOC 2 Type 2 controls and audited during every SOC 2 Type 2 audit.
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. SOC2-controls specify and monitor the frequency of audits and reviews.

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, min-imum 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.
Do you enforce unique username and password?	Yes. All logins to productive systems are performed by uniquely identifiable user accounts.
Which authentication mechanisms are in place for all access to secure areas?	Corporate buildings: NFC-tags to open doors to other floors. Cloud data center: See Microsoft Azure Security documentation at: https://docs.microsoft.com/en-us/azure/security/
Are group shared or generic accounts and passwords used?	No
Are passwords protected using hashing algorithms?	Yes. In DocuWare Cloud: PBKDF2 with salt and many thousand iterations.
What is the retention period for audit logs?	At least 90 days for critical (internet facing or data reading or data changing) operations.
Are removable storage devices permitted in the data center?	No. See for example: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

2.2.3 Intrusion detection

What are your intrusion detection (IDS) or intrusion prevention solutions (IPS)?	Cloud-ready IDS and IPS are in place. DocuWare has added custom alerts for additional security alerts to the 24x7 standby teams.
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.
How are system configuration checking tools utilized and maintained?	Cloud security tools for measuring infrastructure security is measured and tracked as a company-level KPI. Desired state configuration is used for critical resources. Alerting about deviations is in place.

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.

2.2.4 Distributed Denial of Service (DDOS) attacks

What is the protection against Distributed Denial of Service (DDOS) attacks?	It is Microsoft Azure DDoS protection.

2.2.5 Network control

How is 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. 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.
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. Operating system is also updated frequently and transparently for the customer.
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 access.

Are remote access user activities captured in activity logs?	Yes. All remote access actions are recorded in audit logfiles.
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.
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.

2.2.6 Physical security

How does your company address Social Engineering attempts and thwarting?	Security awareness trainings, monthly security and data protection awareness competition. Network separation for teams having access to critical systems.
Do you secure access to your productive computing centers?	The Microsoft Azure datacenters have very a 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.
What is your visitor policy?	Visitor policy in DocuWare's corporation buildings is in place. Visitors need to register with time of arrival and sign 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. The Microsoft Azure datacenters have a very high level of physical access policies.
What controls are in place to prevent unauthorized access to or damage to network, power or telecommunications cabling?	In the Microsoft Azure datacenters, there is full protection by Microsoft.
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.

2.3 Cloud processes and compliance

2.3.1 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.
What are the policies and procedures for the review and update process?	The review process is in accordance with the requirements of SOC 2 Type 2: it consists of a yearly review by the author of the SOP and a supervisor. It is signed into effect by management.
How are policies published to all relevant users?	The policies are published using Notifications from the general file cabinet and from the HR file cabinet of the DocuWare inhouse system, trainings for relevant SOPs and Microsoft Teams posts. Acknowledgement of SOPs is confirmed in a DocuWare workflow via electronic signature.

2.3.2 Software development process

How do you ensure code is being developed professionally and in a secure manner?	Our Software Development handbook describing our SDLC is very detailed (> 50 pages) and has to be signed and followed by every developer.
How do you train developers?	The Research & Development department has a dedicated Architecture guild, a Scrum guild and many more. Technical knowledge is shared in technical presentations with other teams. Security training takes place once a year.
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.

What types of security reviews do you perform on 3rd party / open-source software (OSS)?	We use a third-party security tool called WhiteSource. Scanning and alerting (about new vulnerabilities). Policies are in place for allowed licenses and vulnerability levels. We do have a third-party software-approval process (before using new third-party software).
What is your quality assurance process?	SDLC process is documented in an internal and confidential 52-pages internal guide. QA uses unit tests, integration tests and automated tests to control quality of builds and to avoid regression bugs. Release pipelines include automatic quality checks and rollout to production requires a personal release decision by QA. QA reports to management once a month.

2.3.3 Vulnerability management

How often do you perform penetration tests, security reviews, and vulnerability assessments?	Penetration tests: twice a year by an external security company The Penetration test report is not available for customers. However, SOC 2 Type 2 auditors are reviewing the 2 last reports every year during their audit and are thus reviewing our reaction to and handling of potential findings. Vulnerability assessments: once per month Security-reviews: before going live of new services or major features
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.

2.3.4 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 custom alerts for additional security 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).
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)

2.3.5 Backup and Restore

What is DocuWare’s general backup and restore policy?	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.
What is the backup and restore policy regarding documents and data?	In addition to the redundant copies of the encrypted productive data mentioned in the data security section, another 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. If document versioning is disabled, the customer must open a support ticket to access older document versions. (However, this effort will be charged by DocuWare Professional Services team.)

What is the backup and restore policy regarding databases?	Full database backups 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.
Is there a cold storage and how is it used?	To enable a recovery, DocuWare backs up both the full backups of the databases and the continuous backup of the documents in a separate cold storage. This cold storage is located in a Microsoft Azure datacenter within the respective region, currently in Amsterdam (Netherlands) for the EU, in the state of Washington (USA) for America, 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., cyber attacks). The full backups for the SQL databases are carried out in the cold storage at weekends, usually during regional nighttime. The documents are backed up directly to the cold storage. The generation of backups in the cold storage is automatically monitored continuously. Restore is tested according to SOC 2 Type 2 controls.

2.3.6 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. Retention period for those log files is set to 90 days.

2.3.7 Incident response

Is a security incident response plan formally documented and published?	Yes. The process is documented and tested quarterly with appropriate parties.
What is your security incident reporting procedure?	According to SOC 2 Type 2 controls and guidelines. Our so-called Urgency handling process is open to every single employee upon suspected incident and will alert our two 24x7 standby teams immediately. Confirmed findings will be reported without delay to customers.
Has there been a data security breach at your institution?	We had a few minor cases that were reported immediately. We resolved the issues, tightened our IT security, and reported to the Data Protection Authority and the police.

How and when do you notify clients of a security incident?	We inform customers via their email address without undue delay and report if their data was concerned by the security incident.
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 responsible personnel. This includes testing the 24x7 on call response.

2.3.8 Vendor management

Do you utilize subcontractors for the provision of the product or service offering?	Yes. You can find the most current lists at: EN | DE | ES | FR
Are third party vendors vetted prior to engagement?	We check their credit rating and we do an export control check.
Does your organization outsource any IT or security functions to a third party service provider?	Yes, to Microsoft Azure data centers.

2.3.9 Asset management

Do you have a company-wide asset management policy and procedures?	Yes, according to SOC 2 Type 2 controls.
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.
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.
What additional procedures are applied when disposing of customer or client data?	A deletion process is applied. The customer can export data (if requested). Once this has been done and confirmed by the customer, the secure deletion process is initiated.

3 IT Security

3.1 General

Why is DocuWare not providing certain documents and details?	Due to the sensitive nature of the topics discussed in this paper, we can only provide information that does not put our company at risk. Thank you for understanding. You will see us referring to the SOC 2 Type 2 certification wherever it makes sense throughout the paper. This allows us to prove that we operate securely without providing sensitive information. The SOC 2 Type 2 certification status is only awarded to companies who operate on strict security and compliance procedures that are based on current industry standards.
Does DocuWare have an implemented security policy?	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 but were successfully assessed during SOC 2 Type 2 audit.
Does DocuWare perform background checks on individuals you employ?	Yes. Europe: For the ones that will receive elevated permissions, such as the staff administrating the DocuWare Cloud. United States: Everyone.
Does DocuWare rely on any cloud-based service to support company operations and/or provide a product/service to your customers?	Yes, Microsoft Azure public cloud.
How does DocuWare handle user provisioning and deprovisioning?	We have a wide range of automations in place that will handle on-boarding/side-boarding/off-boarding. Notifications and tasks will be sent out to the relevant persons to complete workflow steps.

Is a security awareness training program established for all employees?	Yes, in accordance with the SOC 2 certification. Every employee starting at DocuWare receives adequate security training which greatly limits the risk of threats due to social engineering. Additionally, every employee must partake in another security (and data protection) training at least once a year. The content varies each time and depends on the current threat landscape. The training participation is mandatory and enforced.
Do you have controls in place that restrict access to information and uniquely identify users?	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. We do not grant anonymous access to internal corporate resources.
Can you provide internal network maps?	We can't give insights here due to their sensitive nature. Thank you for understanding.
Do external entities receive access to internal systems?	External access is occasionally granted for contractors and third parties. There is a fixed process that must be followed to grant access with the minimum permissions possible. Through strict documentation and regular reviews, we ensure that external access happens in a most controlled manner.

3.2 Server and client security

Does DocuWare allow transferring customer data from company computers to portable media?	We utilize third party software that locks down devices regarding USB usage. Any portable storage media that is being plugged in will be blocked. This also protects against malicious or modified USB sticks. Data from the DocuWare Cloud is never stored on portable media.
Is an anti-malware solution present on servers and workstations?	Yes. Anti-malware software is present on every client and server. Additionally, it is blocking scripts and Office macros. The software is automatically updating itself.
Are workstations data storages encrypted?	Yes, we enforce encryption for all portable devices and their drives. Encryption health is checked and enforced on a regular basis.

How are workstations kept up to date?	We utilize tools to automatically and regularly patch 3rd party software present on all devices. Furthermore, updates to the operating systems are deployed automatically and reboots are forced in a timely manner. Automations are checked on a regular basis.
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 changes ownership inside the company, the same process is followed.

3.3 Network security

Does DocuWare perform regular penetration testing?	Yes, at least once a year for the corporate IT. The DocuWare product is tested more often. We have an external company perform penetration tests.
Is it possible to view the penetration test results?	We can't give insights here due to their sensitive nature. Thank you for understanding. The test results are analyzed regularly as part of the SOC 2 Type 2 certification. The auditors check these reports very thoroughly and ensure that we are following up on the findings and close vulnerable spots.
Is data encrypted in transfer between the DocuWare network and the data center?	Yes, according to current security standards (e.g., AES 256 encryption).
Are secure remote access procedures in place?	Remote access to the corporate network is only granted through an encrypted VPN tunnel which enforces user authentication.
Do you have a firewall management process?	Yes, in accordance with the SOC 2 Type 2 certification. 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?	We use multiple Virtual Local Area Networks (VLANs) with access control so that critical systems are separated from the workstation network. The IT operates in a separate segment.

3.4 Backups

Are backups kept geo-redundant?	Yes. They are managed by Microsoft. For geo-redundancy, local machines are backed up to a cloud backup provider (IONOS).
Is online storage encrypted?	Corporate data is sometimes stored on Microsoft OneDrive and other Microsoft services, where data is encrypted in transfer and at rest.
How is DocuWare handling backups of IT systems?	(See above for DocuWare Cloud Service Backup for customer) 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 snapshots 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.

3.5 Identity protection

Is Multi-Factor Authentication (MFA) for employee accounts in place?	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 certification.
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.

Does DocuWare evaluate their user directory as well as granted permissions?	The user directory is checked monthly for stale accounts and more. Critical changes to permissions, such as domain privileges, are alerted to IT staff and are reviewed immediately. Anomalies are documented and checked, too.

3.6 Threat & vulnerability management

How is risk assessment done?	Risk assessment meetings are done quarterly, to stay aware of risks. We plan possible mitigations, following up on the mitigation progress and discuss newly discovered risks.
What is DocuWare doing to protect against personal data breaches?	In accordance with the SOC 2 Type 2 certification, we have mechanisms of identification, assessment and notification of personal data breaches implemented.
Do you promptly notify customers affected by a security breach?	Yes, in accordance with the SOC 2 Type 2 certification.
Do you have formal rules for managing security incidents in your company?	Yes, in accordance with the SOC 2 Type 2 certification. The 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.
Do you have a formal business continuity plan (DR/BCP)?	We have a documented and tested disaster recovery plan with detailed instructions on how to recover from disasters. We can’t give further insights here due to their sensitive nature. Thank you for understanding. That being said, the disaster recovery plan is analyzed yearly as part of the SOC 2 Type 2 certification.
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 certification.

DocuWare

4 Appendix: Abbreviations

AES	Advanced Encryption Standard
BCP	Business Continuity Plan
BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Cyber Security Authority)
C5	Cloud computing compliance criteria catalogue of BSI Germany
CCPA	California Consumer Privacy Act
CI/CD	Continuous Integration and either Continuous Delivery or Continuous Deployment
CVSS	Common Vulnerability Scoring System
DES	Data Encryption Standard
DPA	Microsoft Data Protection Addendum
DR	Disaster Recovery
DSK	Datenschutzkonferenz
ECJ	European Court of Justice
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
SCC	Standard Contractual Clauses
SDLC	Systems Development Life Cycle
SOC	System and Organization Controls (AICPA)
SOP	Standard Operating Procedure
RDP	Records of Data Processing
VLAN	Virtual Local Area Network
WAF	Web Application Firewall