comdatis
it-consulting
d.velop

Whitepaper

Archivierung mit SharePoint Online – GoBD konform

Was ist SharePoint Online?

SharePoint Online ist eine Webanwendung in der Microsoft-365- bzw. Office-365-Umgebung, die das Zusammenarbeiten beispielsweise an Projekten vereinfacht. Darüber hinaus bietet die Software diverse Kommunikationskanäle an, um mit internen sowie externen Geschäftspartnern zu interagieren. Microsoft bietet die Software als ein Dokumentenmanagementsystem und Content-Management-Plattform an. Ein Dokumentenmanagementsystem (DMS) bezeichnet die Verwaltung elektronischer Dokumente mit der Nutzdatei, sowie beschreibenden Eigenschaften/Metainformationen, die die Wiederauffindbarkeit der Informationen sicherstellen und eine virtuelle Aktenbildung ermöglichen. SharePoint Online kann somit als vollwertige Lösung für das Enterpreise-Information-Management (EIM) eingesetzt werden.

Die Software basiert auf Webseiten (Sites), die individuell angepasst werden können. Die Webseiten sind das zentrale Element in SharePoint Online, um Inhalte strukturiert darzustellen. Die Seiten können als Dokumentenbibliotheken, Wiki- oder Bildbibliotheken, aber auch als Listen erstellt werden.

Rechtliches

In der neuen Fassung der „Grundsätze ordnungsmäßiger Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD), die im November 2019 veröffentlicht wurden, ist unter Randziffer 20 die explizite Nutzung von Cloud-Systemen ergänzt worden. Aus Datenschutzsicht besteht eine Verarbeitung im Auftrag eines Verantwortlichen gemäß Art. 28 bzw. Art. 4 Abs. 1 Nr. 8 der DS-GVO. Rechtlich legitimiert wird diese Verarbeitung im Auftrag durch die Standardvertragsklauseln, die Bestandteil der Microsoft Online Services Terms sind. Rechtlich bestimmte Maßnahmen zur Datensicherheit werden durch bestehende Zertifikate von Microsoft erfüllt. Dokumente zur Beweissicherung in Rechtsstreitigkeiten können mittels Legal Hold Beweissicherungsverfahrens vor Löschung gesperrt werden. Eine Protokollierung kann je nach Anforderung in verschiedenen Umfängen implementiert werden.

Welche Voraussetzungen müssen erfüllt werden?

- Microsoft Office 365-Tarif, der eine Anwendung von Aufbewahrungsbezeichnungen („Retention Labels“) und/oder Aufbewahrungsrichtlinien unterstützt
- Es werden keine Server o.ä. gebraucht
- Internetverbindung
- Benutzerlizenzen
- Keine Aktualisierungen oder Change-Management

Ist SharePoint Online ein DMS (Dokumentenmanagement System)?

SharePoint Online umfasst die Aufgaben eines DMS. Mittels Bibliotheken und Listen lassen sich Inhalte verwalten und organisieren. Über die Aufbewahrungsrichtlinien werden Löschungen oder Veränderungen von Dokumenten unterbunden.

Was ist der Unterschied zwischen DMS & ECM?

Ein DMS (Dokumentenmanagementsystem) ist ein System zur elektronischen Verwaltung von Dokumenten. Die Software dient zur Aufbewahrung, Verwaltung und Nachverfolgung elektronischer Dokumente. Unter elektronischen Dokumenten versteht man auch papierbasierte Dokumente, die mit Hilfe eines Scanners digitalisiert wurden. Ein ECM (Enterprise-Content-Management) geht ein Schritt weiter. Ein ECM löst zwar ähnliche Aufgabenstellungen wie ein DMS, diese sind jedoch nicht auf die Verwaltung elektronischer Dokumente beschränkt. Ziel eines ECM ist die Speicherung, Bereitstellung und Verwaltung von Informationen. Darüber hinaus bietet ein ECM die Möglichkeit zur Zusammenführung von unstrukturierten und strukturierten Informationen. Kurz gesagt, ist ein DMS ein untergeordneter Teil eines ECM-Systems.

Aufbewahrungsrichtlinien

Aufbewahrungsrichtlinien lassen sich so einstellen, dass Dokumente nicht während der Aufbewahrungsfrist gelöscht oder geändert werden. Aufbewahrungsrichtlinien – die als Datensatz klassifiziert wurden – lassen sich zentral im Admin Center nur von einem Administrator erstellen und verändern. Die Anpassung oder Entfernung von bereits auf Dokumente und Dateiordner angewandten Aufbewahrungsrichtlinien können nur von einem Administrator verändert oder entfernt werden.

Standort, welche Unterschiede gibt es dort?

Der genaue Standort der Daten ist im Admin-Center aufgelistet. Die bei Microsoft abgelegten Dokumente befinden sich in der Europäischen Union (EU), wenn das Unternehmen seinen Sitz in der EU hat. In der Abgabenordnung (AO) müssen die Vorgaben des § 146 beachtet und eingehalten werden. Demnach sind die Bücher und die sonst erforderlichen Aufzeichnungen im Geltungsbereich des Gesetzes zu führen und aufzubewahren. Mit dem Jahressteuergesetz 2020 wurde die Möglichkeit geschaffen, elektronische Bücher und Aufzeichnungen innerhalb der EU ohne schriftlichen Ausnahmeantrag aufzubewahren. Der Datenzugriff muss in vollem Umfang möglich sein und die Besteuerung darf durch die Auslagerung nicht beeinträchtigt werden. Die genannten Anforderungen sind ebenfalls Bestandteile der zu erstellenden Verfahrensdokumentation.

Ein schriftlicher oder elektronischer Antrag an die zuständige Finanzbehörde ist nur noch erforderlich, wenn eine Aufbewahrung in einem Drittstaat erfolgt. Für Neukunden bietet Microsoft auch eine Datenhaltung in Deutschland an. Bestandskunden von Microsoft können einen Umzug der Daten in ein Rechenzentrum mit Standort Deutschland beantragen.

Art der Aufbewahrung

Es können folgende Varianten der Archivierung ausgewählt werden:

- Zentrales Datenarchiv (Records Center): Dokumente werden dabei in ein extra geschaffenes Datenarchiv verschoben (z. B. alle Ein- und Ausgangsdokumente befinden sich in einem Datenarchiv)
- In-Place-Archivierung (in-Place-Records Management bzw. Retention Labels): Dokumente verbleiben an Ort und Stelle und werden nur mittels Aufbewahrungsrichtlinien klassifiziert (z. B. alle Ein- und Ausgangsdokumente befinden sich kontextbezogen in einem Projekt-/oder Kundenordner)

Benutzer, Rechte und Rollen

Folgende Benutzerrollen müssen angelegt werden:

- Globaler Administrator. Dieser kann Aufbewahrungsrichtlinien erstellen und verändern, um Benutzer zu Administratoren in Teilbereichen (Helpdesk-Administrator) ernennen.
- Benutzer mit entsprechenden Berechtigungen, d. h. Ausschluss der Änderung an Aufbewahrungsrichtlinien

Zertifikate von Microsoft

Folgende Zertifikate sind seitens Microsofts vorhanden, die ein hohes Maß an Informationssicherheit garantieren.

- ISO 27001
- ISO 27018
- FedRAM
- FERPA
- HIPAA/HITECH
- SOC 1 und SOC 2 Typ 2
- Cloud Computing Compliance Controls Catalogue (C5) (für "Office 365 Deutschland" in Planung)
- IDW PS 951 (Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen) (für "Office 365 Deutschland" in Planung)

Weitere Zertifikate von Microsoft können im Compliance Center unter folgender URL eingesehen werden: https://www.microsoft.com/de-de/trustcenter/compliance/complianceofferings

Datenbereitstellung für Prüfer

Im Rahmen einer digitalen Betriebsprüfung müssen dem Betriebsprüfer Zugriffsrechte auf die Daten gewährleistet werden. Dabei steht es dem Prüfer frei, welche Zugriffsart er auf die Daten bekommen möchte. Die Finanzbehörde unterscheidet drei Zugriffsarten:

Z1: Unmittelbarer Datenzugriff
Z2: Mittelbarer Datenzugriff
Z3: Datenträgerüberlassung

Alle drei Zugriffsarten lassen sich in SharePoint Online abbilden.

Microsoft Dienste

Microsoft gewährleistet eine Betriebszeit von 99,9%. Darüber hinaus ist Microsoft für das Change-Management zuständig, dementsprechend ist die Software stetig auf dem neusten Stand der Technik. Dadurch ist eine erhöhte Sicherheit möglich, da durch die Updates Sicherheitslücken geschlossen werden. Microsoft bietet den Kunden die gleiche Sicherheit auf Basis der Microsoft Security Development Lifecycle-Richtline an. Ein Datenschutzkonzept muss separat erstellt werden.

eDiscovery Funktionalität

Die eDiscovery-Suche ermöglicht es Benutzern, nach elektronisch gespeicherten Informationen zu suchen, die als Compliance-Nachweis oder als Beweis in Rechtsstreitigkeiten verwendet werden können. Zu den durchsuchbaren Inhalten zählen strukturierte Inhalte wie Dokumente und Listenelemente sowie Blogs, Wikis, Newsfeeds und Inhalte in Exchange-Postfächern.

Durch das eDiscovery Hold lassen sich Informationen sperren. Das Sperren bedeutet, dass eine Kopie des ursprünglichen Inhalts für den Fall aufbewahrt wird, dass diese durch einen Benutzer später geändert oder gelöscht wird. Sperrungen sind möglich bei Inhalten auf SharePoint-Websites (einschließlich OneDrive for Business-Websites) und in Exchange-Postfächern (einschließlich archivierter Skype for Business-Unterhaltungen). Eine Sperre wird verwendet, um den Inhalt in der Form aufzubewahren, die er zum Zeitpunkt der Festlegung der Sperre hatte. Wenn Benutzer eine Sperre auf eine Website oder ein Postfach anwenden, verbleiben die Inhalte an ihrem ursprünglichen Speicherort.

GoBD und Verfahrensdokumentation

Die Kernkriterien der GoBD sind nachfolgend in der Spalte „Prinzip“ aufgelistet. Die Prinzipien basieren auf den Grundsätzen ordnungsmäßiger Buchführung (GoB), die GoBD präzisieren die Grundsätze auf IT-gestützte Systeme.

Ordnungsprinzip, d.h. es müssen geordnete und ausreichende Indexstrukturen vorhanden sein:
Für die Ablage der Dokumente werden gleichartige Dokumente (Dokumentarten) in einer Dokumentenbibliothek abgelegt und archiviert. Für jede Dokumentenbibliothek kann eine andere Aufbewahrungsdauer festgelegt werden. Die Einstellungen werden auf die Unterverzeichnisse vererbt.

Vollständigkeit, d.h. eine lückenlose Belegarchivierung muss sichergestellt sein:
Soweit technisch möglich werden Dokumente automatisiert abgelegt. Die manuellen Prozesse werden den zuständigen Mitarbeitern mittels Arbeitsanweisungen bekannt gemacht. Die Vollständigkeit wird im Rahmen des internen Kontrollsystems regelmäßig geprüft.

Richtigkeit, d.h. für die archivierten Dokumente ist die Übereinstimmung mit dem Original sicherzustellen; Manipulationen an Dokumenten müssen ausgeschlossen werden können:
Dokumente werden in der Form archiviert, wie diese empfangen oder versendet werden. Papierbasierte Dokumente, die mittels Scannung in das Archiv übermittelt werden, müssen einer unmittelbaren Sichtkontrolle unterliegen.

Unveränderbarkeit, d.h. es dürfen keine Änderungen an Dokumenten durchgeführt werden bzw. Änderungen müssen nachvollziehbar sein (Versionierung):
Durch die Aufbewahrungsrichtlinien kann eine Unveränderbarkeit der Dokumente im Archiv sichergestellt werden. Für Veränderbare Dokumente kann eine Versionierung stattfinden.

Nachvollziehbarkeit, d.h. die angewendeten Verfahren müssen in der Verfahrensdokumentation für einen sachverständigen Dritten nachvollziehbar dokumentiert sein:
Um die Anforderung einer Nachvollziehbarkeit nachzukommen, ist eine Verfahrensdokumentation von Nöten. In der Verfahrensdokumentation sind neben den Arbeitsprozessen auch die technischen Prozesse und Einstellungen zu beschreiben.

Zeitgerecht, d.h. es erfolgt eine zeitnahe Erfassung und die Einhaltung gesetzlicher Aufbewahrungsfristen ist sichergestellt:
Die gesetzlichen Aufbewahrungsfristen werden durch die definierte Dokumentlebensdauer in den Richtlinien abgebildet. Nach GoBD ist die zeitnahe Verarbeitung von Belegen vorgeschrieben.

Eine GoBD-konforme Archivierung mittels SharePoint Online kann durchgeführt werden, wenn das Archiv ordnungsgemäß eingestellt ist, sodass eine Löschung oder Veränderung der Dokumente nicht stattfinden kann und eine Verfahrensdokumentation vorhanden ist. Eine Genehmigung des zuständigen Finanzamtes ist, bedingt durch das Jahressteuergesetz 2020, nur dann notwendig, wenn die Datenhaltung außerhalb Europas stattfindet.

Die Ausführungen stellen die Meinung des/der Autoren wieder und haben keine bindende Wirkung. Insofern verstehen sich alle angebotenen Informationen ohne Gewähr auf Richtigkeit und Vollständigkeit. Für eine Umsetzung ist stets eine Beratung im Einzelfall notwendig.

d.velop

Das Unternehmen d.velop AG

Die 1992 gegründete d.velop AG mit Hauptsitz in Gescher entwickelt und vermarktet Software zur durchgängigen Digitalisierung von Geschäftsprozessen und branchenspezifischen Fachverfahren und berät Unternehmen in allen Fragen der Digitalisierung. Mit der Ausweitung des etablierten ECM-Portfolios rund um Dokumentenmanagement, Archivierung und Workflows auf mobile Apps sowie standardisierte und Custom-SaaS-Lösungen bietet der Software-Hersteller auch Managed Services an. Dabei sind die Rechtssicherheit und die Einhaltung gesetzlicher Vorgaben dank eines ausgereiften Compliance Managements gewährleistet.

d.velop stellt digitale Dienste bereit, die Menschen miteinander verbinden, sowie Abläufe und Vorgänge umfassend vereinfachen und neugestalten. So hilft der ECM-Spezialist Unternehmen und Organisationen dabei, ihr ganzes Potenzial zu entfalten.

Ein starkes, international agierendes Netzwerk aus rund 350 spezialisierten Partnern macht d.velop Enterprise Content Services weltweit verfügbar.

d.velop-Produkte – on Premises, in der Cloud oder im hybriden Betrieb – sind branchenübergreifend bislang bei mehr als 11.900 Kunden mit über 2,8 Millionen Anwendern im Einsatz; darunter Tupperware Deutschland, eismann Tiefkühl-Heimservice GmbH, Parker Hannifin GmbH, Nobilia, Schmitz Cargobull, FingerHaus GmbH, die Stadt Wuppertal, die Basler Versicherung, DZ Bank AG, das Universitätsklinikum des Saarlands oder das Universitätsklinikum Greifswald.

d.velop AG
Schildarpstraße 6–8
48712 Gescher, Deutschland
Fon +49 2542 9307-0

d-velop.de
info@d-velop.de

comdatis
it-consulting

Das Unternehmen comdatis

Die Mitarbeiter der comdatis sind als IT-Berater und als IT-Sachverständige tätig und auf Themen der IT-Compliance spezialisiert. Hervorgegangen ist die comdatis aus der Service-Line ambiFOX(audit) der d.velop ambiFOX GmbH. Ein Beratungsschwerpunkt ist die Erstellung von Verfahrensdokumentationen nach GoBD oder TR-RESISCAN für ein ersetzendes Scannen. Die hochgradige Spezialisierung auf Lösungen der d.velop garantiert ein umfassendes Know-How bei gleichzeitig angemessenen Beratungsaufwänden.

Die comdatis ist Ihr Beratungsspezialist für:

- ECM-Compliance & Verfahrensdokumentaton: Erstellung von Verfahrensdokumentationen (GoBD, TR-RESISCAN), Beratung bzgl. revisionssicherer Archivierung (z. B. TR-RESISCAN, Mailarchivierung), Schulungen
- IT-Prüfung: Unterstützung von Wirtschaftsprüfungsgesellschaften, Steuerberatern und Unternehmen bei der Durchführung von IT-Prüfungen
- Datenschutz & Informationssicherheit: Einführung von Datenschutzmanagementsystemen und/oder Informationssicherheitsmanagementsystemen (ISO 27001), Durchführung von Datenschutzaudits, Externer Datenschutzbeauftragter, Datenschutzberatung

comdatis it-consulting GmbH & Co. KG
Deventer Weg 8
48683 Ahaus, Deutschland
Fon +49 2567 82 90 000

comdatis.de
info@comdatis.de

Version: Archivierung mit SharePoint Online – GoBD konform | Stand: März 2021 | Alle Rechte und Änderungen vorbehalten.
Die tatsächliche Realisierung der Lösung ist unternehmensspezifisch und kann von den beschriebenen Funktionen abweichen.