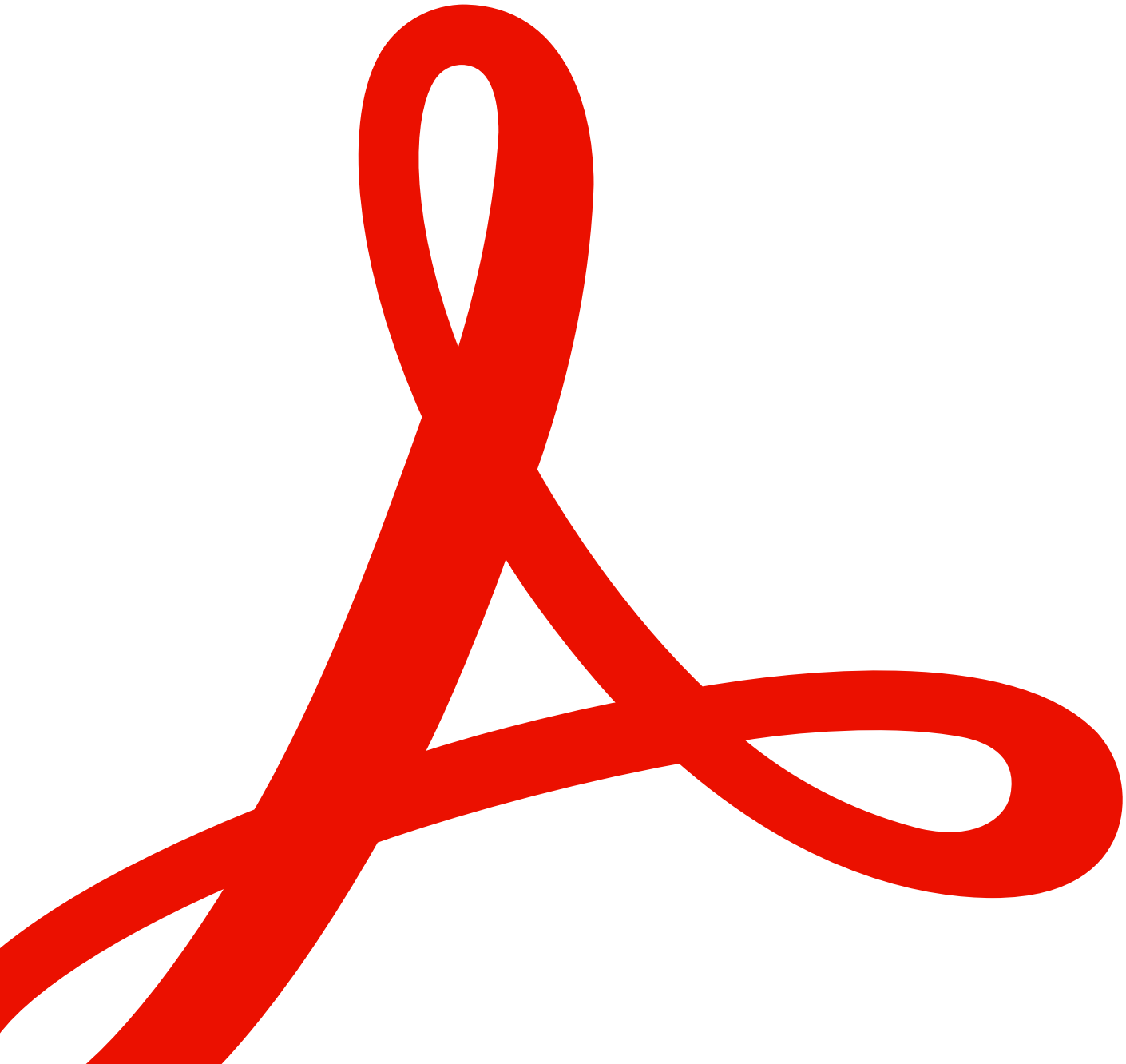
Adobe Document Cloud

Adobe

WHITEPAPER.

Überblick über die Sicherheit von Adobe Acrobat mit Document Cloud-Services.



Inhalt.

Sicherheit bei Adobe.

Adobe nimmt die Sicherheit eurer digitalen Inhalte ernst. Bei Adobe sind Sicherheitsmaßnahmen ein fester Bestandteil der Software-Entwicklung, Prozesse und Programme. Sie werden von interdisziplinären Teams konsequent umgesetzt, um etwaigen Zwischenfällen vorzubeugen, diese aufzudecken und angemessen darauf zu reagieren. Darüber hinaus halten wir uns durch Kooperation mit Partnern, Forschenden und anderen Unternehmen über aktuelle Bedrohungen und Schwachstellen auf dem neuesten Stand und integrieren fortlaufend hochentwickelte Sicherheitstechnologien in unsere Produkte und Services.

In diesem Whitepaper erfahrt ihr, welchen Stellenwert Sicherheit bei Adobe Acrobat mit Document Cloud-Services und den zugehörigen Daten hat.

Überblick über Acrobat mit Document Cloud-Services.

Acrobat mit Document Cloud-Services ist die PDF-Komplettlösung für die moderne, vernetzte Arbeitswelt mit ihren zahlreichen Geräten. Sie vereint Acrobat für den Desktop und den Zugriff auf Premium-Funktionen der Mobile App Acrobat Reader mit Services von Adobe Document Cloud. Somit erfüllt die Lösung jeden Anspruch an einen mobilen, intelligenten Dokumenten-Workflow mit geräteübergreifendem Schutz für wichtige Daten.

Mit Acrobat mit Document Cloud-Services können Kunden und Kundinnen nahezu alle Inhalte in elektronische Dateien umwandeln und weitergeben. Darüber hinaus können sie über Cloud-Services, Desktop-Software oder Mobile Apps PDF-Dateien erstellen und bearbeiten.

Verfügbarkeit.

Die Services von Document Cloud sind in verschiedene Acrobat-Produkte eingebunden.

- Acrobat Pro – Für Nutzer und Nutzerinnen, die mit dem Laptop oder Desktop-Computer arbeiten
- Online-Services von Acrobat – Web-Anwendung für unterstützte Browser wie Chrome, Microsoft Edge, Firefox und Safari auf dem Desktop, Smartphone und Tablet
- Mobile App Acrobat Reader – Kostenloser Download per Apple App Store und Google Play

Acrobat wurde auch in mehrere Produktivitäts-Tools von Microsoft eingebunden. In diesen Fällen werden Dokumente an anderen Orten gespeichert als im eigenständigen Acrobat-Programm. Die jeweiligen Sicherheitsinformationen werden im Bereich Integration mit Microsoft-Produkten aufgeführt.

Document Cloud-Services.

Zu den Services von Document Cloud gehören:

- PDF-Dateien versenden – PDF-Dokumente über einen E-Mail-Client versenden
- Seiten verwalten – Seiten in einem PDF-Dokument einfügen, löschen, neu anordnen oder drehen
- PDF-Dateien erstellen – Word-, Excel- und PowerPoint-Dokumente sowie Bilder oder Fotos in PDF-Dateien umwandeln
- PDF-Dateien exportieren – PDF-Dokumente in editierbare Microsoft Word-, Excel-, PowerPoint- oder RTF-Dateien umwandeln
- PDF-Dateien bearbeiten – PDF-Dokumente auf dem Desktop, Smartphone oder Tablet bearbeiten
- Dateien kombinieren – Mehrere Dateien zu einem kompakten PDF-Dokument zusammenführen – auf jedem Gerät
- Ausfüllen und unterschreiben – Formulare ausfüllen und eine elektronische Unterschrift hinzufügen
- Adobe Scan – Fotos von Quittungen und anderen Papierdokumenten in editierbare, hochwertige PDF-Dateien umwandeln
- Adobe Acrobat Sign (Whitepaper in englischer Sprache) – Dokumente vorbereiten und versenden, um auf jedem modernen Gerät vertrauenswürdige elektronische Unterschriften einzuholen – von einfachen Unterschriften bis hin zu digitalen Signaturen in der Cloud

Der Umfang der Document Cloud-Services wird kontinuierlich erweitert. Eine aktuelle Liste ist auf Adobe.de verfügbar.

Dokumentensicherheit.

Schwärzung.

Mit den Schwärzungswerkzeugen der Adobe Document Cloud-Services lassen sich vertrauliche Informationen zuverlässig schützen. Sowohl Text als auch Bilder können vor der Weitergabe eines Dokuments unwiderruflich gelöscht werden. Es ist auch möglich, Inhalte zu suchen und zu entfernen, die bestimmten Mustern entsprechen, beispielsweise Telefonnummern, Kreditkartennummern und E-Mail-Adressen. Während andere Tools und Methoden der Schwärzung Inhalte lediglich verdecken, werden bei Acrobat die ausgewählten Informationen vollständig aus der Datei entfernt. Mit der Funktion „Dokument bereinigen“ lassen sich auch verborgene Informationen wie Metadaten aus einem PDF-Dokument entfernen.

Freigabe.

Bei Document Cloud gespeicherte Dateien werden automatisch als privat gekennzeichnet. Ihr Inhalt ist somit nur für die Person sichtbar, die sie hochgeladen hat. Endanwender und -anwenderinnen müssen die Freigabe von Inhalten aktiv veranlassen, ansonsten bleiben sie privat. Die Freigabe erfolgt über den Versand eines Links.

Dateien können über Document Cloud-Services entweder zum Anzeigen oder zur Überprüfung freigegeben werden. Ist „Kommentare zulassen“ bei der Freigabe deaktiviert, können Empfangende über den erhaltenen Link nur eine schreibgeschützte Fassung des Inhalts abrufen. Ist die Option aktiviert, können Empfangende Kommentare anbringen, aber keine Änderungen am Inhalt der PDF-Datei vornehmen. Links können per E-Mail, Textnachricht oder ein beliebiges Programm zur Zusammenarbeit bereitgestellt werden.

Elementeinstellungen und Einschränkungen für Freigaben.

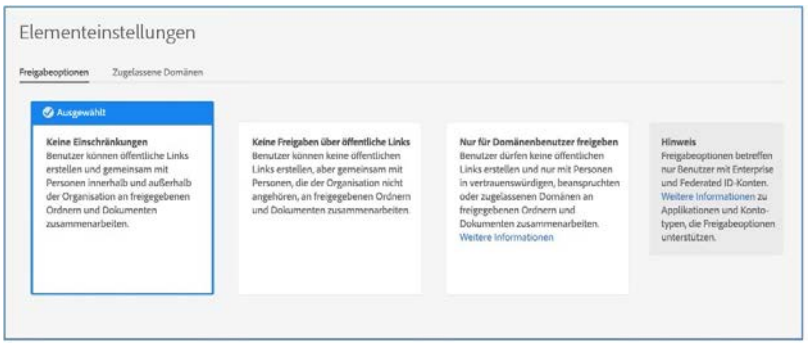


Abb. 1: Einstellungen für Document Cloud-Services

In Document Cloud gespeicherte Inhalte können über die Elementeinstellungen in der Adobe Admin Console mit Freigabeberechtigungen versehen werden. Mit dieser Funktion können IT-Teams die Weitergabe öffentlicher Links deaktivieren und zusätzlich die Zusammenarbeit über Document Cloud auf Domains beschränken, die dem Unternehmen gehören oder für die das Unternehmen den Zugriff zugelassen hat. Wenn Freigabeberechtigungen aktiv sind, müssen sich die Empfangenden anmelden. Mit „Nur für Domänenbenutzer freigeben“ wird festgelegt, dass Inhalte nur innerhalb der Organisation oder mit vertrauenswürdigen anderen Domains ausgetauscht werden können. Die externe Bereitstellung ist nicht möglich.

Microsoft Purview Information Protection.

Microsoft Purview Information Protection (MPIP) ist eine Lösung von Microsoft zur Rechteverwaltung. Anwender und Anwenderinnen von Azure Information Protection und anderen Purview Information Protection-Lösungen von Microsoft können Acrobat oder Acrobat Reader verwenden, um gekennzeichnete und geschützte Inhalte zu lesen. Die neuesten Desktop-Versionen von Acrobat Pro und Acrobat Standard (Version 22.003.20258 und später) wurden mit nativen Funktionen zum Anwenden und Bearbeiten von Information Protection-Vertraulichkeitsbezeichnungen und -richtlinien für ihre PDF-Dateien versehen und erfordern kein Plug-in oder eine separate Installation.

Geschützter Modus.

Um euch vor schädlichem Code zu schützen, der versucht, mithilfe von PDF-Dateien das Dateisystem eurer Computer zu manipulieren, bietet Adobe den geschützten Modus, eine Implementierung der Sandbox-Technologie.

In Acrobat Reader erweitert dieser Modus den Schutz vor Angriffen, die versuchen, Schad-Software zu installieren. So werden das Auslesen und der Abruf vertraulicher Daten und geistigen Eigentums auch im Firmennetzwerk verhindert. Der geschützte Modus wird

standardmäßig beim Starten von Acrobat Reader aktiviert. Insbesondere schränkt dieser Modus die Zugriffsrechte für das Programm ein, sodass Microsoft Windows-Systeme vor böswilligen PDF-Dateien geschützt werden, die gegebenenfalls versuchen, in das Dateisystem des Computers zu schreiben oder Informationen auszulesen, Dateien zu löschen oder auf andere Weise Systemdaten zu verändern.

Der geschützte Modus von Acrobat Reader kann unter Windows 8.1 und höher isoliert in einem AppContainer ausgeführt werden.

Geschützte Ansicht.

Beim Sandboxing handelt sich um eine anerkannte Methode, eine abgegrenzte Umgebung mit eingeschränkten Rechten für die Ausführung von Programmen zu schaffen. Sandboxes tragen zum Schutz der Systeme vor Angriffen mit nicht vertrauenswürdigen Dokumenten bei, die möglicherweise ausführbaren Code enthalten. Im Kontext von Acrobat Reader gelten alle PDF-Dateien und die Prozesse, die sie aufrufen, als nicht vertrauenswürdige Inhalte. Reader behandelt PDF-Dokumente als potenziell schädlich und beschränkt Prozesse, die die PDF-Datei aufruft, auf die Sandbox. Genau wie der geschützte Modus von Acrobat Reader ist die geschützte Ansicht von Acrobat eine Implementierung der Sandbox-Technologie.

Bei Acrobat werden in dieser Ansicht nicht nur das Schreiben von schadhaftem Code auf dem Computer-System mithilfe einer PDF-Datei unterbunden, sondern auch das Auslesen vertraulicher Daten oder geistigen Eigentums. Die geschützte Ansicht beschränkt die Ausführung nicht vertrauenswürdiger Programme (beispielsweise PDF-Dateien mit den von ihr aufgerufenen Prozessen) auf eine isolierte Umgebung – die „Sandbox" –, um zu verhindern, dass schädlicher Code in der Datei den Rechner beeinträchtigt. Bei der geschützten Ansicht wird davon ausgegangen, dass alle PDF-Dateien potenziell schädlich sind. Daher wird jede Ausführung auf die Sandbox beschränkt, es sei denn, eine Datei wurde als vertrauenswürdig gekennzeichnet.

Dieser Schutz beim Öffnen von PDF-Dokumenten steht sowohl in Acrobat als auch im Browser zur Verfügung. Die geschützte Ansicht wird unter Windows 8 und höher in einem AppContainer ausgeführt. Dadurch entsteht eine noch besser abgeschirmte Umgebung. Oben im Anzeigefenster wird eine gelbe Meldungsleiste eingeblendet, sobald eine potenziell schädliche Datei geöffnet wird. Diese Leiste weist darauf hin, dass die Datei nicht vertrauenswürdig ist und in der geschützten Ansicht geöffnet wurde, in der viele Acrobat-Funktionen deaktiviert und die Möglichkeiten der Interaktion mit der Datei eingeschränkt sind. Die Datei ist schreibgeschützt. Eingebettete oder verknüpfte schädliche Inhalte können in das System nicht eindringen.

Um die Datei als vertrauenswürdig zu kennzeichnen und alle Funktionen von Acrobat zu aktivieren, klickt man auf der Meldungsleiste auf „Alle Funktionen aktivieren". Acrobat schaltet daraufhin die geschützte Ansicht aus und fügt die Datei zur Liste vertrauenswürdiger Quellen bzw. Elemente hinzu. Ab dem nächsten Öffnen dieser Datei gelten nicht mehr die Einschränkungen der geschützten Ansicht.

Sicherheit der Adobe Document Cloud-Services.

Authentifizierung.

Das IT-Team gewährt Endanwendern und -anwenderinnen über die Admin Console Zugriff auf die Document Cloud-Services. Die Lizenzen sind anwendergebunden. Acrobat mit Document Cloud-Services unterstützt vier ID-Typen für anwendergebundene Lizenzen: Adobe ID, Business ID, Enterprise ID und Federated ID. Weitere Informationen über diese Identitätstypen und die Adobe Identity Management Services findet ihr im englischsprachigen Überblick über die Sicherheit von Adobe Identity Management Services.

Speicher für Dokumente und andere Inhalte.

Document Cloud-Services nutzen die mehrmandantenfähige Speicherung. Von Anwendern und Anwenderinnen generierte Inhalte und Dokumente werden in mehreren Rechenzentren und in jedem Rechenzentrum auf mehreren Geräten redundant gespeichert. Der gesamte Netzwerkverkehr wird einer systematischen Datenprüfung sowie Prüfsummenberechnungen unterzogen, um Daten zu schützen und ihre Integrität sicherzustellen. Die Inhalte werden schließlich synchron und automatisch in anderen Rechenzentren innerhalb der Region des Kunden bzw. der Kundin repliziert, um auch bei Datenverlust an zwei Standorten die Datenintegrität aufrechtzuerhalten.

In welchem Rechenzentrum die in Document Cloud hochgeladenen Dokumente und anderen Inhalte gespeichert werden, hängt davon ab, welcher Länder-Code den Anwendern bzw. Anwenderinnen zugeordnet ist, die die Daten hochladen. Dies ist unabhängig vom Identitätstyp.

- Die Daten von Anwendern/Anwenderinnen mit einem Länder-Code aus Nord-, Mittel- oder Südamerika werden in Virginia (USA) gespeichert.
- Die Daten von Anwendern/Anwenderinnen mit einem Länder-Code aus Europa oder Afrika werden in Dublin (Irland) gespeichert.
- Die Daten von Anwendern/Anwenderinnen mit einem Länder-Code aus Asien oder dem Nahen Osten werden in Tokio (Japan) gespeichert.

Admins können Enterprise ID- und Federated ID-Accounts über die Adobe Admin Console persönlichen Cloud-Speicher zuteilen. Sie haben aber keinen direkten Zugriff auf die Dokumente oder Inhalte, die Anwenderinnen und Anwender bei Document Cloud speichern. Admins können jedoch den Account übernehmen und dem jeweiligen Anwender bzw. der Anwenderin die Zugriffsrechte entziehen. Nach dem Löschen eines Kontos mit Speicher für Shared Services verlieren die betreffenden Endanwender und Endanwenderinnen den Zugriff auf alle Inhalte, die sie unter dieser ID in der Cloud gespeichert haben. Die Inhalte werden nach 90 Tagen gelöscht.

Admins können auch Adobe ID-Accounts Speicherplatz zuteilen. Sie können diese Art Accounts zwar nicht kontrollieren, aber sie können sie löschen und den Anwendern bzw. Anwenderinnen das Zugriffsrecht für den Cloud-Speicher sowie für Programme und Services entziehen. Auch in diesem Fall werden die Inhalte nach 90 Tagen gelöscht.

Datenverschlüsselung.

Die Document Cloud-Services verschlüsseln Inhalte und Dokumente während der Übertragung standardmäßig mit HTTPS TLS 1.2. Im Ruhezustand werden die Daten mit symmetrischen 256-Bit-AES-Sicherheitsschlüsseln verschlüsselt, die für jeden Kunden/jede Kundin und jede in Anspruch genommene Domain einzeln vergeben werden. Diese Verschlüsselungsmethoden gelten sowohl für die permanente als auch für die vorübergehende Speicherung von Dokumenten.

Dedizierte Verschlüsselungsschlüssel.

Zusätzlich zu den standardmäßigen, integrierten Verschlüsselungsmethoden können Admins für ein höheres Maß an Kontrolle und Sicherheit für einige oder alle Domains der Organisation einen dedizierten Verschlüsselungsschlüssel generieren, mit dem Document Cloud-Inhalte im Ruhezustand verschlüsselt werden. Bei Bedarf kann der Verschlüsselungsschlüssel über die Admin Console deaktiviert werden. Inhalte, die mit diesem Schlüssel verschlüsselt wurden, sind dann nicht mehr zugänglich und können nicht hoch- oder heruntergeladen werden. Dies gilt so lange, bis der Verschlüsselungsschlüssel wieder aktiviert wird.

Hinweis: Nur Document Cloud-Dateien lassen sich mit dem dedizierten Verschlüsselungsschlüssel verschlüsseln, Metadaten nicht.

Weitere Informationen zu Verschlüsselungen mit einem dezidierten Schlüssel findet ihr auf Adobe.de.

Elektronische Unterschriften und digitale Signaturen.

Die Document Cloud-Services umfassen verschiedene Werkzeuge für die Arbeit mit Unterschriften:

- **Ausfüllen und unterschreiben** – Damit können Anwender und Anwenderinnen ein PDF-Dokument öffnen, Formularfelder ausfüllen und das Dokument elektronisch unterschreiben.
- **Zertifikate** – Ermöglicht das elektronische Unterzeichnen in Kombination mit einem digitalen Zertifikat, das kryptografisch an das Unterschriftsfeld gebunden ist. Jedes digitale Zertifikat (digitale ID) ermöglicht die eindeutige Identifizierung des oder der Unterzeichnenden und wird von einem Vertrauensdienst oder einer Zertifizierungsstelle ausgegeben, die auf Vertrauenslisten wie der Adobe Approved Trust List (AATL) und den European Union Trusted Lists (EUTL) aufgeführt sind. Zudem lassen sich mit dem Werkzeug „Zertifikate“ Zeitstempel hinzufügen und die Dokumente mit einem manipulationssicheren Siegel versehen.

Integration mit Microsoft-Produkten.

Adobe und Microsoft haben gemeinsam Integrationen ihrer führenden Produktivität-Tools entwickelt. Acrobat mit Document Cloud-Services ist damit direkt in folgenden Microsoft-Programmen nutzbar:

- Microsoft SharePoint und OneDrive
- Microsoft Teams
- Microsoft Word, Excel und PowerPoint (nur Funktionen zum Erstellen und Schützen von PDF-Dokumenten)

Im Rahmen dieser Integrationen erstellt Adobe lediglich eine temporäre Kopie des PDF-Dokuments. Dabei werden keinerlei kundenspezifische Informationen oder persönliche Daten erfasst, die die Identität von Anwender oder Anwenderin preisgeben.

Acrobat für SharePoint und OneDrive.

Acrobat für SharePoint und OneDrive bietet Zugriff auf PDF-Workflows innerhalb von Microsoft 365 und ermöglicht das Anzeigen, Erstellen und Bearbeiten von PDF-Dokumenten in der Cloud.

Mit dieser integrierten Version von Acrobat werden Dokumente an ihrem ursprünglichen Speicherort auf SharePoint oder OneDrive gespeichert. Aktionen wie das Anzeigen, Kommentieren und Suchen werden lokal auf dem Rechner der Anwender und Anwenderinnen durchgeführt. Geänderte Dokumente werden an ihrem ursprünglichen Speicherort auf SharePoint oder OneDrive gespeichert.

Wenn Anwender oder Anwenderinnen ein Dokument erstellen, organisieren, kombinieren oder exportieren, wird es zur vorübergehenden Verarbeitung an Adobe Document Cloud-Server in der Region gesendet, die dem Länder-Code des Anwenders bzw. der Anwenderin entspricht. Nach 24 Stunden werden die Daten gelöscht. Das Dokument bleibt dabei sowohl bei der Übertragung als auch im Ruhezustand verschlüsselt (siehe Datenverschlüsselung). Das geänderte Dokument wird wieder im SharePoint- oder OneDrive-Account des Anwenders bzw. der Anwenderin gespeichert.

Weitere Informationen zu den Funktionen von Acrobat für SharePoint und OneDrive findet ihr auf Adobe.de.

Acrobat für Microsoft Teams.

Acrobat für Microsoft Teams bietet Zugriff auf PDF-Workflows innerhalb von Microsoft Teams und ermöglicht das Anzeigen, Erstellen und Bearbeiten von PDF-Dokumenten in der Cloud. Kundinnen und Kunden können Acrobat für Microsoft Teams als persönliche Registerkarte, als Bot, als Registerkarte, als Nachrichtenaktion oder als Nachrichtenerweiterung verwenden.

Jedes in einem Chat oder Kanal von Microsoft Teams bereitgestellte PDF-Dokument wird standardmäßig im OneDrive- oder SharePoint-Konto des Anwenders bzw. der Anwenderin gespeichert. Aktionen wie das Anzeigen, Kommentieren und Suchen werden lokal auf dem Rechner der Anwender und Anwenderinnen durchgeführt. Geänderte Dokumente werden an ihrem ursprünglichen Speicherort auf SharePoint oder OneDrive gespeichert.

Wenn Anwender oder Anwenderinnen ein Dokument erstellen, organisieren, kombinieren oder exportieren, wird es zur vorübergehenden Verarbeitung an Adobe Document Cloud-Server in der Region gesendet, die dem Länder-Code des Anwenders bzw. der Anwenderin entspricht. Nach 24 Stunden werden die Daten gelöscht. Das Dokument bleibt dabei sowohl bei der Übertragung als auch im Ruhezustand verschlüsselt (siehe Datenverschlüsselung). Das geänderte Dokument wird wieder im SharePoint- oder OneDrive-Account des Anwenders bzw. der Anwenderin gespeichert.

Weitere Informationen zu den Funktionen von Acrobat für Microsoft Teams findet ihr auf Adobe.de.

Acrobat für Word, Excel und PowerPoint.

Mit dem Add-in „Acrobat PDFMaker“, das über die Registerkarte „Acrobat“ genutzt werden kann, lässt sich ein Microsoft 365-Dokument in eine hochwertige PDF-Datei umwandeln und auf OneDrive speichern oder auf die Festplatte herunterladen. PDF-Dokumente können auch durch Hinzufügen eines Kennworts vor unerlaubtem Zugriff geschützt werden.

Fazit.

Das proaktive Sicherheitskonzept und die strikten Verfahren, die in diesem Dokument beschrieben wurden, dienen dem Schutz von Acrobat mit Document Cloud-Services und euren vertraulichen Daten. Adobe nimmt die Sicherheit eurer digitalen Inhalte sehr ernst. Die weltweiten Bedrohungen werden fortlaufend beobachtet, um kriminellen Aktivitäten stets einen Schritt voraus zu sein und die Sicherheit der Kundendaten zu gewährleisten.

Weitere Informationen zur Sicherheit bei Adobe einschließlich der Prozesse für Unternehmenssicherheit, Programmsicherheit, Betriebssicherheit und Compliance und Zertifizierung sowie zu den Programmen für Sicherheitstests, Problembehandlung und Betriebskontinuität und Disaster Recovery findet ihr im Adobe Trust Center.

Die Informationen in diesem Dokument können ohne vorherige Ankündigung geändert werden. Wenn ihr weitere Informationen zu den Lösungen, Kontrollmechanismen und Lizenzoptionen von Adobe wünscht, wendet euch bitte an den Adobe-Vertrieb.

02/24