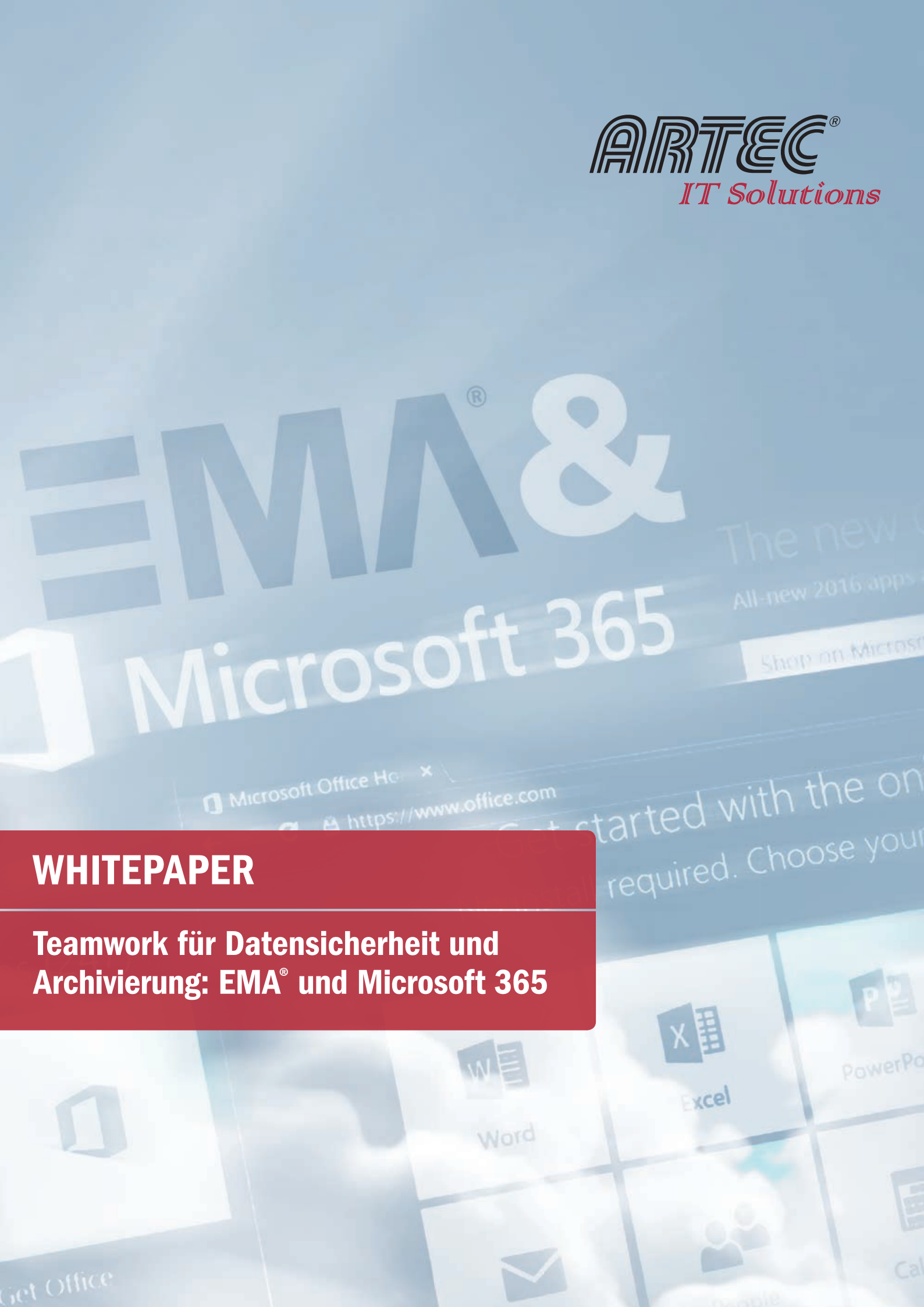
ARTEC IT Solutions



WHITEPAPER

Teamwork für Datensicherheit und Archivierung: EMA® und Microsoft 365

INHALTSVERZEICHNIS

EDITORIAL

Microsoft bietet Funktionen zur Archivierung von E-Mails als Zusatzprodukt zu Microsoft 365 an. In diesem Whitepaper werden grundlegende Funktionen und Eigenschaften der E-Mail Archivierung von Microsoft 365 zusammengefasst und im Hinblick auf Aufwände, Sicherheit und mögliche Risiken analysiert. Dem gegenüber stellen wir mit EMA® ein hoch sicheres Unified Archive System für alle relevanten Datenquellen, das auf dem Prinzip redundanter Datenhaltung für kritische Unternehmensdaten beruht. Für den Spezialfall der Archivierung von E-Mails ermöglicht der Einsatz von EMA® zusammen mit Microsoft 365 die Implementierung von Best Practices zur Datensicherheit und Einhaltung von Compliance-Vorgaben und zugleich die produktive Nutzung archivierter Daten.

DIE E-MAIL ARCHIVIERUNG VON MICROSOFT 365

Technische Grundlagen

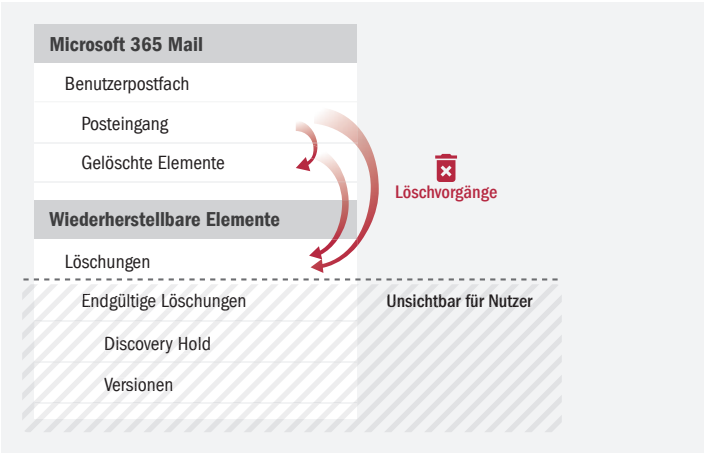
Die E-Mail Archivierung in Microsoft 365 und Outlook im Allgemeinen ist zu einem wesentlichen Teil dazu gedacht, die Eingangspostfächer der Anwender zu entlasten, indem sie in einem mehrstufigen Prozess E-Mails für gewisse Zeiträume wiederherstellbar hält. Man unterscheidet dabei die Archivierung unter der Kontrolle der Nutzer, bei der E-Mails nach einem festgelegten Zeitraum in ein dem Nutzer zugewiesenes Archivpostfach verschoben werden, von der sogenannten Compliance Archivierung, mit der höhere rechtlich-organisatorische Anforderungen erfüllt werden sollen.

Prinzipiell ist bei der Compliance Archivierung die Aufbewahrung von E-Mails auf die einzelnen Postfächer der Benutzer bezogen. Diese werden in einen für den Nutzer sicht- und bearbeitbaren und einen verborgenen Bereich unterteilt. Der Vorgang der E-Mail Archivierung ist nun bei Microsoft 365 immer eng gebunden an die Ausführung von Löschungen von E-Mails in den Postfächern und Ordnern der Nutzer, entweder manuell durch die Nutzer selbst, oder durch andere Prozesse. Gelöschte E-Mails werden normalerweise zunächst in den sichtbaren Unterordner **Gelöschte Elemente** im Nutzer-Postfach verschoben, von wo aus der Nutzer sie einfach wiederherstellen kann. Prozesse der dauerhaften Aufbewahrung von E-Mails mit Wiederherstellungsmöglichkeiten beginnen erst, wenn E-Mails aus dem Unterordner **Gelöschte Elemente** entfernt und damit zum endgültigen Löschen vorgesehen werden. Dies kann automatisch geschehen oder vom Nutzer veranlasst werden, indem er den Unterordner **Gelöschte Elemente** löscht. Alternativ können Nutzer E-Mails auch unter Umgehung von **Gelöschte Elemente** direkt zum endgültigen Löschen markieren durch die Tastenkombination **Shift+Delete**.

Aus **Gelöschte Elemente** entfernte E-Mails landen nun zunächst in einem speziellen Unterordner im Ordner **Wiederherstellbare Elemente**. Der Ordner **Wiederherstellbare Elemente** ist unterteilt in einen für den Nutzer sicht- und zugreifbaren Bereich und einen nicht sichtbaren Bereich, der nur für die Administratoren zugänglich ist. Der für den Nutzer sichtbare Bereich enthält den Unterordner **Löschungen**, der im Wesentlichen ein Sicherheitsanker gegen das versehentliche endgültige Löschen von Elementen ist. Die Elemente im Unterordner **Löschungen** erhalten beim Eintritt in diesen einen Zeitstempel. Nach Ablauf einer gesetzten Aufbewahrungsfrist in Bezug auf die generierten Zeitstempel werden Elemente weiter verschoben in den nicht sichtbaren Bereich des Ordners **Wiederherstellbare Elemente** und dort in den Unterordner **Endgültige Löschungen (purges)**. Auch diese Verschiebung kann der Nutzer selbst erzwingen durch Markieren von Elementen im Unterordner **Löschungen** zum endgültigen Löschen. Für den Nutzer sind Elemente in endgültige Löschungen nicht mehr sicht- oder zugreifbar. Was und wann mit ihnen weiter geschieht, hängt von den Systemparametern und Einstellungen der speziellen Microsoft 365-Instanz ab.

Microsoft 365 bietet nun verschiedene Verfahren zur Archivierung im Rahmen einer Beweissicherung – der sogenannten Compliance Archivierung – an, von denen **Litigation Hold** und **In-Place-Hold** die wichtigsten sind. Beim **Litigation Hold** Verfahren wird für jedes dafür konfigurierte Postfach ab dem Zeitpunkt der Einrichtung alle Nachrichten vor Löschungen oder Änderungen bewahrt, indem gelöschte bzw. geänderte Elemente in Unterordnern von **Wiederherstellbare Elemente** verschoben werden. Diese Unterordner sind einerseits **Discovery Hold** bei Löschungen und andererseits **Versionen** bei Änderungen von Nachrichten. In letzteren Unterordner wird bei jeder Änderung eine Kopie des geänderten Elements gespeichert. Die Aufbewahrung all dieser Nachrichten dauert bis zur Deaktivierung von **Litigation Hold** oder bis zu einem vorher bestimmten Zeitraum an. Diese Methode stellt also eine Art Überwachung der Nutzeraktivitäten für ein bestimmtes Benutzerpostfach und einen bestimmten Zeitraum dar.

In-Place-Hold erlaubt es, sogenannte **eDiscovery** Fälle zu definieren, die bestimmte Postfächer umfassen und Nachrichten darin bis zur Aufhebung des eDiscovery-Falls (ohne bestimmten Aufbewahrungszeitraum) vor Löschung und Veränderung schützen. Dies geschieht im Prinzip auf die gleiche Weise wie bei **Litigation Hold**. Bei **In-Place-Hold** können zusätzlich Filter und Schlüsselwörter für die Archivierung definiert werden.



▲ Vereinfachte Ordnerstrukturen in Microsoft 365 und normale Löschungen

Produkteigenschaften

Die technische Funktionalität der E-Mail-Archivierung in Microsoft 365 ist darauf ausgelegt, die Postfächer bestimmter Benutzer für einen bestimmten Zeitraum nach festen Regeln zu überwachen, indem Elemente in für die Nutzer nicht zugängliche Bereiche verschoben werden. Sie ist dagegen nicht für kontinuierliche Archivierung der gesamten Kommunikation innerhalb und außerhalb eines Unternehmens gedacht.

Dies erklärt sich neben der technischen Auslegung auch aus wirtschaftlichen Gründen. Die E-Mail Archivierung ist ein Zusatzprodukt, das für jedes Postfach mit einer monatlichen Rate hinzugebucht werden muss. Bei der Microsoft 365 Archivierung ist die Volumenobergrenze für die überwachten Postfächer aufgehoben, was notwendig ist, damit unter keinen Umständen zu archivierende E-Mails verloren gehen können. Folglich muss der Anbieter schon für die dynamische Bereitstellung des zusätzlichen Speichers Kosten geltend machen. Andererseits spart der Nutzer durch die rein intra-systemische Datenhaltung die Kosten für die Unterhaltung oder Anmietung eines dedizierten Archivspeichers.

Microsoft 365 vermeidet bei der Aufbewahrung von E-Mails jede redundante Datenhaltung. E-Mails sind demnach bei aktivierter Archivierung teils in den speziell dafür gedachten Unterordnern oder aber in den Nutzerpostfächern zu finden, je nachdem, ob sie gelöscht wurden oder nicht.

Die Aufbewahrung von archivierten E-Mails in den Unterordnern **Discovery Hold** und **Versionen** erlaubt die Konstruktion vielfältiger Richtlinien für die Archivierung. Ihre Einrichtung und Administration erfordert hohe Vertrautheit mit dem System und stellt zugleich eine nicht ganz triviale Aufgabe bei der Umsetzung organisatorischer Zielvorgaben dar. Die beschriebenen Standard-Methoden von Microsoft 365 sind zwar für viele Anwendungsfälle ausreichend, jedoch ist nicht klar ob mit alle Anforderungen eines Unternehmens an eine bestimmte Archivierungsaufgabe erfüllt werden können. Somit ist besondere Sorgfalt nötig, um mit der Microsoft 365 Archivierung alle organisationsrelevanten Ziele (Compliance) zu erreichen und Risiken auszuschließen. Vor Beginn der Archivierung müssen die Archivierungsrichtlinien so geplant werden, dass alle relevanten Daten erfasst werden. Im Nachgang der Archivierung müssen die für einen bestimmten Fall wichtigen Elemente herausgesucht und gefiltert werden. Dem Administrator kommt in diesem Systemaufbau eine besonders wichtige Rolle und hohe Verantwortung zu.

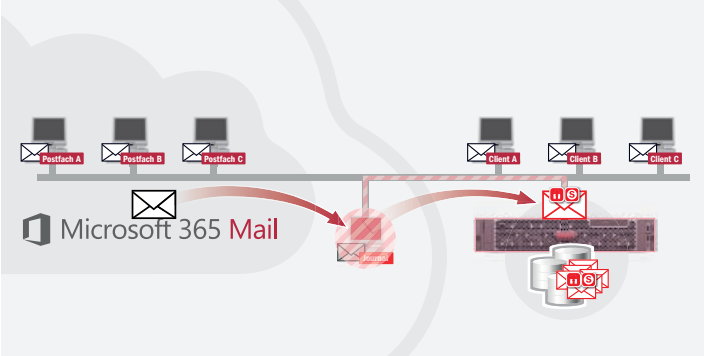
Grundsätzlich sichern die Archivierungsfunktionen von Microsoft 365 Daten zu bestimmten Zeitpunkten, die nichts mit der Historie der Daten, zum Beispiel ihrer Entstehung, dem Empfang oder dem Versenden einer E-Mail, zu tun haben. Insbesondere bezüglich E-Mails handelt es sich hier also um eine Archivierung von Daten, nicht aber der zugehörigen Kommunikationsvorgänge. Konkret drückt sich dies darin aus, dass E-Mails im Zeitraum von ihrer Entstehung (Empfang oder Versenden) bis zu ihrer Archivierung in den Nutzer-Postfächern nicht manipulations- und revisionssicher gespeichert sind.

MICROSOFT 365 ARCHIVIERUNG MIT EMA®

Die hochsichere Unified Archiving Lösung EMA® eignet sich zum Management und Compliance Archiving von Unternehmensdaten aus vielen unterschiedlichen Quellen. Neben den Modulen Mail, File, Print, Scan und Voice für die Erfassung aller wesentlichen Daten- und Kommunikationsformate, bietet EMA® Anbindungen an Cloud Speicher wie die Synchronisierung mit OneDrive, oder mit Anwendungen wie Sharepoint und SAP. Im vorliegenden Whitepaper fokussieren wir uns auf die Compliance Archivierung von E-Mails mit EMA® aus Microsoft 365 Mail.

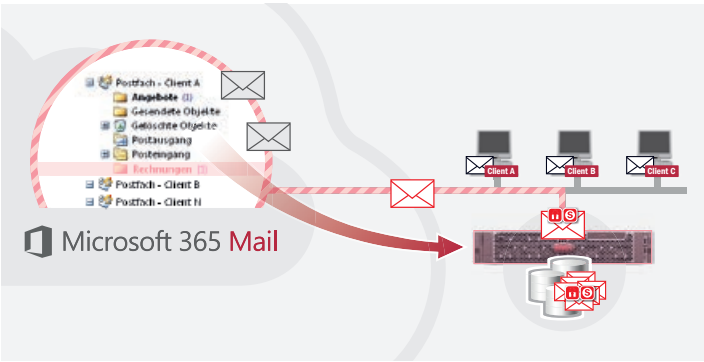
Technische Grundlagen und Eigenschaften

Die Archivierung von E-Mails aus Microsoft 365 mit EMA® ist denkbar einfach und flexibel einsetzbar, sowohl als Cloud-Lösung oder auch innerhalb der eigenen IT-Infrastruktur. Die optimale Anbindung des Archivs erfolgt über ein Journaling-Postfach mit der Journaling-Funktion, die in vielen Microsoft 365 Paketen enthalten ist. Dabei werden sowohl Kopien ein- und ausgehender E-Mails sowie Journalberichte über E-Mail Kommunikationsprozesse unmittelbar an ein Journal-Postfach gesendet **[10]**. Das Journal-Postfach, das sich außerhalb der Microsoft 365 Infrastrukturen befinden muss, wird von ARTEC in der EMA®-Infrastruktur bereitgestellt und passend zur Exchange-Online Instanz des Kunden konfiguriert. EMA® holt sich regelmäßig die im Journal-Postfach liegenden E-Mails und Journalberichte ab. Alle Daten werden dann von EMA® mit Zeitstempeln versehen, signiert und verschlüsselt abgelegt.



Der wesentliche Vorteil der Journaling-Lösung für die Archivierung mit EMA® liegt in ihrer Unmittelbarkeit und lückenlosen Sicherheit. Bereits das Journaling-Postfach befindet sich in der hochsicheren ARTEC-Infrastruktur. EMA® erlaubt zur Archivierung die Anbindung beliebiger Speichersysteme beim Nutzer oder auch in der Cloud.

Herausforderung Zukunftssicherheit:
Die zweitbeste Option zur Archivierung von Microsoft 365 E-Mail mit EMA® ist die der Ordner-Synchronisierung. Sie kann angewendet werden, wenn die Journaling-Lösung aus technischen, organisatorischen oder vertraglichen Gründen nicht möglich ist. In dieser Variante scannt EMA® die überwachten Postfächer regelmäßig auf Veränderungen. Hierbei wird ein Vergleich mit dem Bestand der bereits in EMA® archivierten Daten vorgenommen. Alle neu hinzugekommenen E-Mails werden an EMA® übertragen und unmittelbar mit Zeitstempeln und elektronischen Signaturen versehen und verschlüsselt im Archiv abgelegt. Wie bei der Archivierung durch Microsoft 365 selbst ist bei der Archivierung über die reine Ordnersynchronisierung zu beachten, dass Latenzzeiten zwischen Ein- oder Ausgang einer E-Mail und der Archivierung entstehen können, während derer zum Beispiel Nutzer Daten verändern oder E-Mails löschen können.



Vom Anschluss an das Microsoft 365 System an ist die Archivierung mit EMA® prinzipiell konfigurationslos. Alle anfallenden Daten werden kontinuierlich und dauerhaft archiviert, zudem ist aber auch die Einrichtung persistenter Filterregeln einfach möglich. In EMA® eingehende E-Mails und gegebenenfalls auch Journaling-Metadaten werden unmittelbar Volltext-indiziert und sind damit sofort für die inhaltsbasierte Suche verfügbar. EMA® ist also ein Live-Archiv, das im laufenden Betrieb ohne weiteres für beliebige Extraktionen oder Analysen von Daten genutzt werden kann. Für die Nutzer stehen bei EMA® neben der umfassenden Suchfunktion verschiedene Anwendungsmodule wie E-Discovery und Case Management ohne zusätzlichen administrativen Aufwand zur Verfügung.

EMA® verfolgt weiterhin einen umfassenden Unified Archive Ansatz bei dem viele weitere Quellen von Unternehmensdaten ebenso direkt archiviert werden können. Dies umfasst Dateien in überwachten Speicherorten über die EMA® File Funktion, gescannte Dokumente und Ausdrucke (EMA® Scan und Print), Telefonie (EMA® Voice) und Anwendungsdaten DMS oder ECM Systemen wie SAP Dokumente oder Sharepoint Folder.

Vergleich:
EMA® setzt auf planmäßige, globale Redundanz während die Microsoft 365 E-Mail Archivierung postfachzentrisch sparsame Datenhaltung praktiziert. Die unterschiedlichen Ansätze der Microsoft 365 Archivierung gegenüber der Archivierung mit EMA® zeigen sich am deutlichsten bei der Erfüllung von Compliance Aufgaben wie E-Discovery. Bei der Microsoft 365 Archivierung sind dies Aufgaben, die direkt mit der Einrichtung und dem Management der Archivierungsfunktion selbst verknüpft sind. Das heißt, diese für ein Unternehmen hoch relevanten und risikobehafteten Vorgänge involvieren stets die IT-Administration. EMA® als Unified Live Archiv trennt die Archivierung als Aufgabe von der nachfolgenden, im Prinzip beliebigen Nutzung der Daten. Die Anwendungsmodule E-Discovery und Case Management zum Beispiel stehen damit nutzerseitig direkt den zuständigen Fachabteilungen, etwa dem CIO, zur Verfügung.

Die beschriebenen Unterschiede wirken sich gravierend in den Bereichen IT-Sicherheit, Compliance, und Risikomanagement aus. Zu allererst sind Daten in den Nutzerpostfächern vor der Archivierung nicht manipulationssicher der Schutz vor Löschung oder Veränderung (durch Versionierung) muss bei Microsoft 365 jeweils gesondert eingerichtet werden.

Entsprechend ist auch die Wiederherstellung von gelöschten E-Mails aus dem Archiv bei Microsoft 365 eine aufwändige Administrationsaufgabe. Bezüglich der Erfüllung von Compliance-Anforderungen zieht dies zusätzliche Dokumentationspflichten (was wird von wann bis wann unter welchen Richtlinien archiviert und wer ist hierfür verantwortlich). Die herausgehobene Rolle des Administrators in der Verwaltung der Microsoft 365 E-Mail Archivierung birgt zusätzliche Risiken, da das System prinzipiell nicht umfassend gegen durch Administratoren hervorgerufene, gewollte oder versehentliche Manipulationen oder Datenverluste geschützt ist. Hier bietet EMA® prinzipbedingte Vorteile:

- Vollständige, revisionssichere Archivierung aller relevanten Daten
- Auditierbarkeit aller Prozesse durch umfassende, integritätsgeschützte Logs
- Granulare Zugriffsrechte und erweiterte Zugriffsschutzfunktionen zum Beispiel nach dem 4-Augen Prinzip

Etliche Aufgaben können nur mit einem umfassenden Live-Archiv wie EMA® überhaupt angegangen werden. Dies betrifft zum Beispiel die Möglichkeiten des Disaster Recovery und der Business Continuity im Fall eines unwiederbringlichen Datenverlustes. Hier bietet EMA® weitgehende Optionen, um Unternehmensdaten schnell wiederherzustellen und zugleich das Live-Archiv im Produktivbetrieb als Interimslösung zu nutzen.

Zusammenfassend erfüllen die Archivfunktionen von Microsoft 365 nicht von vornherein (Out-of-the-Box) die Anforderungen an Revisionssicherheit, Compliance, Risikomanagement und Rechtssicherheit. Vielmehr erfordert jede dieser Einzelaufgaben zumindest administrativen Aufwand und gegebenenfalls sogar zusätzliche interne Prozesse. Zugleich ist die Microsoft 365 E-Mail Archivierung nicht kostenfrei und es sollten zumindest im Einzelfall Kosten und Nutzen im Vergleich mit einer umfänglicheren und dedizierten Archivierungslösung abgewogen werden.

Schließlich stellt das Microsoft 365 E-Mail Archiv eine Insellösung dar, die ausschließlich für die Nutzung innerhalb der jeweiligen Microsoft 365 Anwendungen tragfähig ist. Eine Zusammenschau von E-Mails mit anderen archivierten Daten und die Verwendung in anderen Anwendungen ist nicht möglich.

SPEZIALANWENDUNG: MIGRATION ZU MICROSOFT 365

EMA® kann Organisationen zudem bei der Migration von Altsystemen, z.B. On-Premise Exchange Server, Lotus Notes u.ä., in die Cloud zu Microsoft 365 Mail unterstützen. Dies funktioniert nach einem einfachen Schema:

- EMA® wird als E-Mail Archiv an das Altsystem angebunden und importiert alle bestehenden Daten. Zugleich startet die Archivierung neuer Daten automatisch ab dem Installationszeitpunkt.
- Ist der aktuelle Datenbestand in EMA® übernommen kann das Altsystem abgeschaltet und die Microsoft 365 Cloud in Betrieb genommen bzw. »bezogen« werden.
- Dabei wird die Journaling-Funktion aktiviert und die EMA®-Archivierung für die Microsoft 365 Installation etabliert. EMA® ist damit als Archivspeicher für Microsoft 365 Mail aktiv.
- Die Bestandsdaten vor dem Umzug in die Cloud können nun von EMA® über die Wiederherstellungsfunktion zurückgespielt werden und sind dann in den Nutzerpostfächern in Microsoft 365 verfügbar.

Interessant ist hier, dass Schritt 4 in gewisser Weise optional ist. Im Zuge der Migration können hier einfach Policies zur Datensparsamkeit in Microsoft 365 Mail implementiert werden, etwa indem nur Mails wiederhergestellt werden, die nicht älter als 10 Tage sind und von da ab alle älteren Mails aus Microsoft 365 entfernt werden.

MICROSOFT 365 UND EMA® – FAZIT UND EMPFEHLUNGEN

Vor dem Einsatz von Microsoft 365 mit der von Microsoft angebotenen E-Mail Archivierung sollte eine kritische und vergleichende Kosten-Nutzen Analyse erfolgen und die Erreichbarkeit von Zielen hinsichtlich Datensicherheit, -verfügbarkeit, Compliance, Risikominimierung und Datenmanagement geprüft werden. Pragmatisch scheint aber der kombinierte Einsatz von Microsoft 365 mit einer dedizierten Archivierungslösung, die sich wie EMA® ohne viel Aufwand anbinden und verwalten lässt, am sinnvollsten. In der Zusammenschau ergeben sich einige Best-Practice Empfehlungen für den effizienten und sicheren Umgang mit Microsoft 365:

- Setzen Sie Microsoft 365 zusammen mit einer unabhängigen, sicheren Archivierungslösung ein, die produktives Arbeiten mit archivierten Daten für die Endanwender ermöglicht
- Daten sollten mit geringstem möglichen zeitlichen Verzug aus Microsoft 365 in das Archivsystem übertragen werden, am besten über die Journaling Funktion. Achten Sie bei der Auswahl des Microsoft 365-Pakets auf diese Funktion
- Definieren Sie Richtlinien, um Daten nach möglichst kurzen Fristen aus Microsoft 365 zu entfernen – Mailverdrängung
- Prüfen Sie mögliche Einsparungen durch Mailverdrängung (kleinere Benutzer-Postfächer)
- Etablieren Sie klare Zugriffsrichtlinien zum Archiv
- Sichern Sie Microsoft Produkte technisch ab, soweit möglich etwa nach der Handreichung **[4]**. Verhindern Sie insbesondere die automatische Übertragung von Diagnose-Daten
- Passen Sie Ihre Datenschutzerklärung an die Nutzung von Microsoft 365 an
- Bleiben Sie auf dem Laufenden, was Microsoft 365 und Datenschutz angeht!

Arbeitsprozesse kosteneffizient mit cloudbasierten Anwendungslösungen abzubilden ist für viele Unternehmen aller Größen das Gebot der Stunde. Ein dediziertes, umfassendes Datenmanagement für die kontrollierte, langfristige Aufbewahrung aller wichtigen Unternehmensdaten bietet hierbei zusätzliche Potenziale für die Organisation effizienterer Arbeitsprozesse. Dedizierte Unified Archiving Lösungen wie EMA® bieten hier eine skalierbare Lösung, die nahtlos und ohne zusätzlichen Arbeits- und Organisationsaufwand die Anforderungen an Compliance, Datensicherheit und Datenschutz zu erfüllen helfen.

MICROSOFT 365 – HINTERGRÜNDE ZU SICHERHEIT UND DATENSCHUTZ

Cloud-Anwendungen stellen kein grundsätzliches Problem für den Datenschutz dar, sofern die Verantwortlichkeiten und Prozesse bei der Verarbeitung personenbezogener Daten geklärt und nachvollziehbar sind. Insofern sind für praktisch alle Cloud-Anwendungen Einordnungen als Auftragsverarbeitungen im Sinne von Art. 28 DSGVO anzustreben. Dies setzt die Einhaltung von zwei Prinzipien voraus: Erstens müssen alle verantwortlichen Empfänger personenbezogener Daten bekannt und vertraglich – direkt oder indirekt – zur Einhaltung und Offenlegung von Datenschutzregeln verpflichtet sein. Zweitens dürfen Auftragsverarbeiter nicht eigenständig und mit eigenen Interessen Prozesse auf den Daten durchführen.

Die Befolgung beider Prinzipien ist für Microsoft 365 zunächst grundsätzlich möglich. Microsoft und seine bekannten sogenannten »Sub-Processors« **[8]** sichern vertraglich die Einhaltung von Datenschutzgrundsätzen zu. Zudem erfolgt die Verarbeitung von Daten bei Cloud-basierten Microsoft-Anwendungen zunächst in jedem einzelnen Fall anscheinend nur auf Veranlassung des Auftraggebers beziehungsweise des einzelnen Nutzers. Wenngleich solche Operationen auch in der Cloud an einem dem Nutzer unbekannten Ort stattfinden, sollten sie doch einheitlich in der Verantwortlichkeit des Auftragsverarbeiters liegen.

Die Verwendung von Microsoft 365 birgt dennoch nach übereinstimmender Expertenmeinung besondere Risiken für den Datenschutz. Zwei wesentliche Eigenschaften von Microsoft 365 stehen hier im Fokus der Kritik und bereiten Anwendern konkrete Probleme bei dem Versuch, Microsoft 365 in Übereinstimmung mit den Regeln des Datenschutzes einzusetzen, da sie die tatsächliche Einhaltung der oben genannten Prinzipien infrage stellen.

Verarbeitung von Personenbezogenen Daten in fremden Rechtsgebieten

Die Verarbeitung von Daten erfolgt bei Microsoft 365 und ähnlichen Cloud-Anwendungen weltweit operierender Konzerne in global verteilten Rechenzentren, von denen viele außerhalb der Europäischen Union und damit des direkten Geltungsbereichs der DSGVO liegen. Die DSGVO fordert in diesem Fall besondere Sorgfalt von dem ursprünglich Verantwortlichen für die Datenverarbeitung, um sicher zu stellen, dass den Europäischen entsprechende Regeln auch am Verarbeitungs- und Speicherort der Daten eingehalten werden (Kapitel 5, DSGVO). Dies wird nun insbesondere für die USA in Zweifel gezogen. Die dortige Sicherheitsgesetzgebung, insbesondere durch den »Clarifying Lawful Overseas Use of Data Act« (CLOUD Act **[6]**) erlaubt US-Sicherheitsbehörden weitgehenden Zugriff auf personenbezogene Daten, die US-Firmen speichern oder Verarbeiten, bei Vorliegen von Verdachtstatbeständen oder vermuteten Gefahren aus einem weiten Spektrum. Im Zweifelsfall erstreckt sich diese amerikanische Gesetzgebung auch auf ausländische Töchter und Standorte amerikanischer Firmen. Die Firmen sind außerdem in jedem Fall zur Verschwiegenheit über die Datenherausgabe verpflichtet.

Eine US-amerikanische Firma kann also schwerlich die Sicherheit und Einhaltung von europäischen Datenschutzgrundsätzen garantieren. Microsoft sichert aktuell jedenfalls nicht vertraglich zu, dass Daten nicht in den USA gespeichert, verarbeitet oder in die USA transferiert, oder weiterhin amerikanischen Sicherheitsbehörden übergeben werden. Eine zwischenzeitlich bestehende Lösung durch die mit der Deutschen Telekom als Treuhänder betriebene Microsoft Cloud Deutschland, wurde inzwischen abgekündigt. Zugleich kündigt Microsoft an **[5]**, ab 2020 Microsoft 365 aus in Europa (in Deutschland an den Standorten Berlin und Frankfurt) betriebenen Rechenzentren anzubieten. In wie weit dies bei der gegebenen Rechtslage zu einer positiven datenschutzrechtlichen Bewertung führt, bliebt abzuwarten.

Unkontrollierte Datenübertragung und Verarbeitung durch Microsoft

Institutionen und Unternehmen sind nach Art. 35 DSGVO verpflichtet, bei Vorliegen besonderer Risiken, zum Beispiel der Verarbeitung besonders sensibler Daten, vorab eine Datenschutz-Folgenabschätzung durchzuführen. Vor diesem Hintergrund hat das Niederländische Justizministerium eine entsprechende Studie zum Einsatz von Microsoft 365 durchführen lassen, die als »Data Protection Impact Assessment« (DPIA) **[1]** veröffentlicht wurde. Fokus der Studie ist die automatische Übertragung diagnostischer Daten im Sinne der Studie, das heißt Daten die durch die Nutzung von Microsoft 365 oder der verbunden Dienste in Cortana **[7]** entstehen. Als ein Ergebnis der Studie hat Microsoft anerkannt, dass solche Daten personenbezogene Daten im Sinne der DSGVO darstellen.

Die Schlussfolgerungen aus dieser Studie sind für den praktischen Einsatz von Microsoft 365 besonders relevant, weil sie die Grundlagen des Datenschutzes berühren. Microsoft ist nach diesen Erkenntnissen nicht mehr nur Auftragsverarbeiter sondern eigentlich Verantwortlicher im Sinne der DSGVO. Dies würde im Prinzip zwingend den Abschluss einer Vereinbarung zur gemeinsamen Verantwortlichkeit (Joint Controllership Agreement) zwischen den Anwendern und Microsoft nötig machen. Als praktische Maßgabe empfiehlt die Studie, die Übertragung diagnostischer Daten so weit als möglich zu unterbinden und gibt hierzu praktische Hinweise:

»In the interim, Microsoft has helped the Dutch government to implement settings to minimise the processing of telemetry data, based on the blocking of traffic from certain ports that send information to the telemetry end-point in the USA. The effectivity of this solution still has to be tested in combination with a data viewer tool.«

Weiterhin sichert Microsoft selbst hier Verbesserungen zu, um Nutzern bessere Kontrolle über die eventuell gesammelten Daten zu geben, zum Beispiel ein Tool das Einblick in diese Daten erlaubt. Anwendern kann zwischenzeitlich nur geraten werden, die automatisierte Datenübertragung aus Microsoft 365 so weit als möglich zu unterbinden. Generelle Hinweise zum allgemeinen Vorgehen hierfür im Kontext von Microsoft Produkten finden sich in einer Handreichung des BSI **[4]**.

Die beschriebenen Umstände stellen die nach der DSGVO nötigen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten infrage. Ein berechtigtes Interesse, Daten in den fremden Rechtsraum zu übertragen, kann nicht angenommen werden, weil die Sicherheit der Verarbeitung der Daten dort untergraben wird durch die unklaren Zugriffsmöglichkeiten Dritter. Eine gültige Einwilligung der von der Datenverarbeitung Betroffenen einzuholen ist hier ebenfalls schwierig und risikobehaftet, da es schon nicht einfach möglich ist, ihnen die Verarbeitungsprozesse nachvollziehbar zu erklären (eine notwendige Voraussetzung für die gültige Einwilligung). Da das Bestehen bestimmter Rechtsgrundlagen nach der DSGVO Bedingung für die Datenverarbeitung ist, kommen Datenschutzbeauftragte und Experten zu dem Schluss, dass der Einsatz von Microsoft 365 eigentlich nur im Rahmen von sogenannten »On Premise« Lösungen in abgeschotteten Bereichen unter der eigenen Kontrolle des Unternehmens erlaubt sei **[9]**. Dies stellt natürlich die wesentlichen Vorteile von Microsoft 365 als Cloud-Lösung infrage.

Hilfreich für Unternehmen kann die Bewertung des Einsatzes von Microsoft 365 in öffentlichen Einrichtungen durch die Datenschutz-Aufsichtsbehörden sein, da diese verpflichtet sind hier eingehende Prüfungen vorzunehmen. In einer ersten Stellungnahme **[2]** hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) den Einsatz von Microsoft 365 in Schulen als zuständige Aufsichtsbehörde untersagt, wobei insbesondere auf die schon beschriebene Problematik der unkontrollierten Übertragung von diagnostischen Daten abgehoben wurde. Weiterhin sieht der HBDI die Sicherheit und Nachvollziehbarkeit insbesondere vor dem Hintergrund der Möglichkeit eines unkontrollierten Zugriffs ausländischer Behörden als gefährdet an. Interessant ist hierbei, dass Schulen nicht ohne weiteres durch Einwilligungen (zum Beispiel der Eltern) eine eigene Rechtsgrundlage für die Datenverarbeitung mit Microsoft 365 schaffen können, da dies durch die unabdingbaren Schutzrechte von Minderjährigen zum Beispiel nach Art. 8 DSGVO ausgeschlossen ist:

»Ob die Einwilligung der Betroffenen in bestimmten Situationen die digitale, personenbezogene Datenverarbeitung rechtfertigt, kann dahin gestellt bleiben. Im Zusammenhang mit der Nutzung von Microsoft 365 in der Cloud bietet die Einwilligung jedenfalls keine Lösung, weil die Sicherheit und Nachvollziehbarkeit der Datenverarbeitungsprozesse nicht gewährleistet sind.«

In einer weiteren Stellungnahme **[3]** hat der HBDI seine Haltung weitgehend revidiert, ohne inhaltlich zu wesentlich anderen Bewertungen zu kommen und »duldet« nun »bis auf weiteres« den Einsatz von Microsoft 365 in Schulen unter der Maßgabe, die Übertragung von Diagnosedaten zu unterbinden. Ohne Inhalte zu nennen, sei die Neubewertung nach intensiven Gesprächen mit Microsoft zustande gekommen »die einen erheblichen Anteil der Bedenken entkräfteten«. Für den Außenstehenden bleibt abzuwarten, was die weitere Prüfung durch den HBDI und andere Stellen ergibt.

REFERENZEN

[1] Privacy Company. DPIA DIAGNOSTIC DATA IN MICROSOFT OFFICE PROPLUS. 2. November 2018.

→ https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf

[2] Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen. 09.07.2019

→ https://datenschutz.hessen.de/pressemitteilungen/stellungnahme-des-hessischen-beauftragten-f%C3%BCr-datenschutz-und

[3] Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen. 02.08.2019

[4] BSI: EMPFEHLUNG: IT IN UNTERNEHMEN Sichere Konfiguration von Microsoft Office 2013/2016/2019. BSI-CS 135 | Version 1.00 vom 29.05.2019

[5] Microsoft Deutschland: Microsoft stellt seine Cloud-Dienste ab 2019 aus neuen Rechenzentren in Deutschland bereit und reagiert damit auf veränderte Kundenanforderungen. 31.08.2018

→ https://news.microsoft.com/de-de/microsoft-cloud-2019-rechenzentren-deutschland/

[6] H.R.4943 – Cloud Act

→ https://www.congress.gov/bill/115th-congress/house-bill/4943

[7] Verbundene Dienste für Microsoft Outlook und Office 365: Häufig gestellte Fragen.

→ https://support.microsoft.com/de-de/help/4482715/microsoft-outlook-and-office-365-connected-services-faq

[8] Microsoft Online Services Subprocessors List.

[9] Bewertung des LfDI Rheinland-Pfalz. (Ralf Kamnitzer, personal communication)

[10] Journale in Exchange Online.

→ https://docs.microsoft.com/de-de/exchange/security-and-compliance/journaling/journaling

Disclaimer

Dieses Whitepaper dient lediglich der Information und stellt keine Rechtsberatung dar. Die Inhalte dieses Dokuments wurden mit größtmöglicher Sorgfalt erstellt. Irrtümer und Änderungen sind vorbehalten. Der Anbieter übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Inhalte. Die Nutzung der Inhalte erfolgt auf eigene Gefahr des Nutzers. Mit der reinen Nutzung des Dokuments kommt keinerlei Vertragsverhältnis zwischen dem Nutzer und dem Anbieter zustande. Die in diesem Dokument veröffentlichten Inhalte unterliegen dem deutschen Urheber- und Leistungsschutzrecht. Jede vom deutschen Urheber- und Leistungsschutzrecht nicht zugelassene Verwertung bedarf der vorherigen schriftlichen Zustimmung des Anbieters oder jeweiligen Rechteinhabers.

Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Übersetzung, Einspeicherung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien und Systemen. Inhalte und Rechte Dritter sind dabei als solche gekennzeichnet. Die unerlaubte Vervielfältigung oder Weitergabe einzelner oder kompletter Inhalte ist nicht gestattet und strafbar. Lediglich die Herstellung von Kopien und Downloads für den persönlichen Gebrauch ist erlaubt.

Rechtliche Hinweise

Autor

Dr. Andreas Schmidt, Chief Information Officer (CIO), ARTEC IT Solutions AG

Haftungshinweis

Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung oder Garantie für Vollständigkeit, Richtigkeit und Aktualität aller zur Verfügung gestellten Texte und Daten.