Mail-Archivierung und Aufbewahrungs-optionen in Microsoft 365 einfach erklärt

von Kent MacMillan
kent@grump-it.pro
grump-it.pro

Inhaltsverzeichnis

Übersicht über die Archivierung und Aufbewahrung von Mails

In Deutschland müssen alle geschäfts- und finanzrelevanten Schreiben und Dokumente wie Rechnungen, Kontoauszüge, Angebote usw. gemäß den gesetzlichen und organisatorischen Anforderungen ordnungsgemäß aufbewahrt und archiviert werden. Wenn es um die Archivierung von Mail geht, stehen viele Unternehmen vor der Herausforderung, diese Anforderungen zu erfüllen. Nach Angaben des Bundesfinanzministeriums müssen Dokumente vollständig, in ihrer ursprünglichen Form, so früh wie möglich und unverändert für 10 Jahre (GoBD) archiviert werden.

Jedes finanzrelevante Dokument darf erst nach Ablauf der gesetzlich vorgeschriebenen Frist vernichtet werden, und jeder Vorgang, der zu einer Veränderung dieser Dokumente im elektronischen Archivierungssystem führen kann, muss nachvollziehbar protokolliert werden. Darüber hinaus sollte der Archivierungsprozess jederzeit von Dritten auf seine Richtigkeit überprüft werden können, so dass die Archivierung und Speicherung stets nachvollziehbar sein muss. Mit dem Übergang der Unternehmen zum Cloud Computing als vorherrschendem Nutzungsmodell ergeben sich neue Möglichkeiten für die Dokumentenarchivierung.

Wie ein solcher Schutz vor Änderungen und Löschungen in Microsoft 365 aussehen kann, welche Voraussetzungen ein Microsoft 365-Administrator erfüllen muss, um die gesetzlichen Anforderungen an die Mailarchivierung zu erfüllen, und welche Microsoft 365-Lösungen für unterschiedliche Anforderungen geeignet sind, werde ich im folgenden Dokument klären. Dabei konzentriere ich mich auf die Cloud-basierten Lösungen von Microsoft 365 und nicht auf On-Prem-Lösungen.

Um die rechtskonforme und organisatorisch komplexe Sicherung und Protokollierung von Mails im Unternehmen gewährleisten zu können, ist es zunächst wichtig zu verstehen, wie elektronische Archivierung funktioniert und welche Arten von Archivierungsmöglichkeiten es generell und in Microsoft 365 gibt.

Gängige Lösungen zur Mail-Archivierung

Es gibt in der Regel zwei Arten von Mail-Archivierungslösungen:

1. Archivpostfächer

2. Journalregeln

Die erste und gängigste Option ist die Verwendung eines Archivpostfachs. Bei dieser Art der Sicherung verfügt der Endnutzer über ein persönliches Mail-Archiv, in das er Nachrichten manuell verschieben kann oder in das Nachrichten automatisch verschoben werden. Diese Archiv-Postfächer können sich vor Ort oder in der Cloud befinden. Durch die Erstellung einer Archivierungsrichtlinie dient diese Methode in erster Linie dazu, das Wachstum von Postfächern einzudämmen, indem nicht benötigte oder alte Nachrichten verschoben werden. So werden beispielsweise Mails nach einem bestimmten Zeitraum von einem Jahr automatisch in ein entsprechendes Online-Archiv-Postfach verschoben.

Diese Art der Mailarchivierung entspricht jedoch nicht den gesetzlichen Anforderungen, die in Deutschland an eine Archivierungslösung gestellt werden, da nicht zwangsläufig alle Nachrichten archiviert werden, da der Benutzer in der Regel auch die automatischen

Mailarchivierungsrichtlinien außer Kraft setzen kann. Zwischen der Erstellung/dem Eintreffen einer Mail im Postfach und dem Verschieben in das Archivpostfach liegt immer ein Zeitraum. Während dieses Zeitraums können Mails von Endbenutzern gelöscht oder geändert werden. Mails sind auch im Archivpostfach nicht vor dem Löschen geschützt.

Die zweite Möglichkeit ist die Journal-Archivierung. Diese stellt sicher, dass jede empfangene/gesendete Mail archiviert wird, was häufig durch sogenannte Journalregeln erreicht wird, bei denen von jeder ein- und ausgehenden Mail eine Kopie an ein externes Journal-Postfach gesendet wird. Normalerweise ist das Journal-Postfach vor Änderungen und Löschungen geschützt und auch die Mail-Administratoren haben nur Leserechte auf das Postfach. Die Art und Weise, wie die Archivdaten gesichert werden, unterscheidet sich je nach Lösungsanbieter. Häufig wird das Journal-Postfach auf einem speziellen WORM (Write-Once-Read-Many)-Speichermedium gespeichert. Wird sichergestellt, dass die archivierten Daten für einen definierten Zeitraum unveränderbar aufbewahrt werden können, spricht man von einer revisionssicheren Archivierung.

Welche dieser Möglichkeiten gibt es in Microsoft 365 und wie werden sie konfiguriert? In den nächsten Abschnitten werden wir diese Lösungen im Kontext von Microsoft 365 untersuchen.

Mail-Archivierung und Aufbewahrungsoptionen in MS365

MRM-Richtlinien und ihre zugehörigen Aufbewahrungstags

https://docs.microsoft.com/de-de/exchange/security-and-compliance/messaging-records-management/messaging-records-management

Microsoft 365 über Exchange Online bietet die Möglichkeit, Messaging Records Management (MRM)-Tags und zugehörige Richtlinien einzurichten, um Mails automatisch in ein Online-Archivpostfach zu verschieben, das neben den Postfächern der Endbenutzer in Exchange Online gehostet wird. Persönliche Archive (In-Situ-Archive) werden über das Microsoft Purview (Compliance)-Portal eingerichtet, und dann können im alten Exchange Online Admin-Portal die entsprechenden Archivierungs-/Aufbewahrungsrichtlinien definiert und dem Postfach des Endbenutzers zugewiesen werden. Die Aufbewahrungsrichtlinien setzen sich aus MRM-Aufbewahrungstags zusammen. Diese definieren, was mit den im primären Postfach vorhandenen Nachrichten geschehen soll. So werden beispielsweise alle Nachrichten, die älter als ein Jahr sind, in das Archiv-Postfach verschoben oder alle als privat eingestuften Nachrichten verbleiben im primären Postfach. MRM-Aufbewahrungstags werden in persönliche und Standardtags unterteilt. Persönliche Tags können vom Endbenutzer nach Bedarf aktiviert und auf das Postfach oder einzelne Ordner angewendet werden. Standardkennzeichnungen werden immer automatisch angewendet. Zusätzlich zu den MRM-Aufbewahrungsrichtlinien stehen dem Endbenutzer drei weitere Optionen zur Verfügung, um Nachrichten in ein Online-Archiv (auch als In-Place-Archiv bezeichnet) zu übertragen:

1. Manuelles Verschieben oder Kopieren von Mails

2. Verschieben oder Kopieren von Nachrichten mit Hilfe von Regeln für den Postausgang

3. Importieren von Nachrichten aus PST-Dateien

Durch das Anwenden einer Aufbewahrungsrichtlinie (die Funktion Messaging Records Management (MRM) in Exchange Online) wird kein inaktives Postfach erstellt, wenn das

Benutzerkonto gelöscht wird. Dies steht im Gegensatz zu der unten beschriebenen Compliance-Archivierungsmethode, bei der die Mails gelöschter Benutzer aufbewahrt werden, sobald ihrem Postfach eine Compliance-Aufbewahrungsrichtlinie zugewiesen wird. Ein weiterer Nachteil dieser älteren Methode zur Archivierung/Aufbewahrung von Mails besteht darin, dass die Endbenutzer auch die Kontrolle über die MRM-Tags haben und die für Ordner und Mails festgelegten Standardrichtlinien außer Kraft setzen können. Um dieses Problem zu beheben, bietet Microsoft zentralisierte Archivierungs- und Aufbewahrungsrichtlinien für Mails über das Compliance-Portal in Microsoft 365.

Compliance-Archivierung

Die zweite in Microsoft 365 verfügbare Option ist die Compliance-Archivierung. Sie ermöglicht die vollständige Aufbewahrung von Postfachelemente. Sowohl gelöschte Elemente als auch Änderungen an Elementen werden (für den Benutzer unsichtbar) in einem separaten Bereich des Postfachs aufbewahrt, der von der Postfachsynchronisierung mit Endgeräten oder Outlook ausgeschlossen ist. Die Compliance-Archivierung erfordert kein Archivpostfach, sondern verwendet für die Aufbewahrung spezielle Unterordner im Ordner "Wiederherstellbare Elemente", die für das Postfach und ein vorhandenes Archivpostfach gelten. Online-Archiv-Postfächer können somit zur Erweiterung des nutzbaren Volumens sowie zur Vereinfachung der Benutzererfahrung verwendet werden, aber die Mails werden weiterhin in den versteckten Unterordnern aufbewahrt. Microsoft 365 bietet Compliance-Archivierung in verschiedenen Formen für unterschiedliche Anforderungen:

- Beweissicherungsverfahren (Aufbewahrung für rechtliche Zwecke)

- In-Situ-Speicher, d. h. durch Aufbewahrungsrichtlinien im Compliance-Portal erstellte Aufbewahrungsfristen, die auf der Grundlage des Erstellungsdatums oder des Betreffs aufbewahrt werden können

Wie funktioniert die Compliance-Archivierung in MS365?

Um die Funktion der Compliance-Archivierung in Microsoft 365 zu verstehen, ist es notwendig, sowohl den Löschvorgang eines Postfachelements als auch die Struktur des Ordners "Wiederherstellbare Elemente" zu erklären:

Löschvorgang ohne Compliance-Archivierung

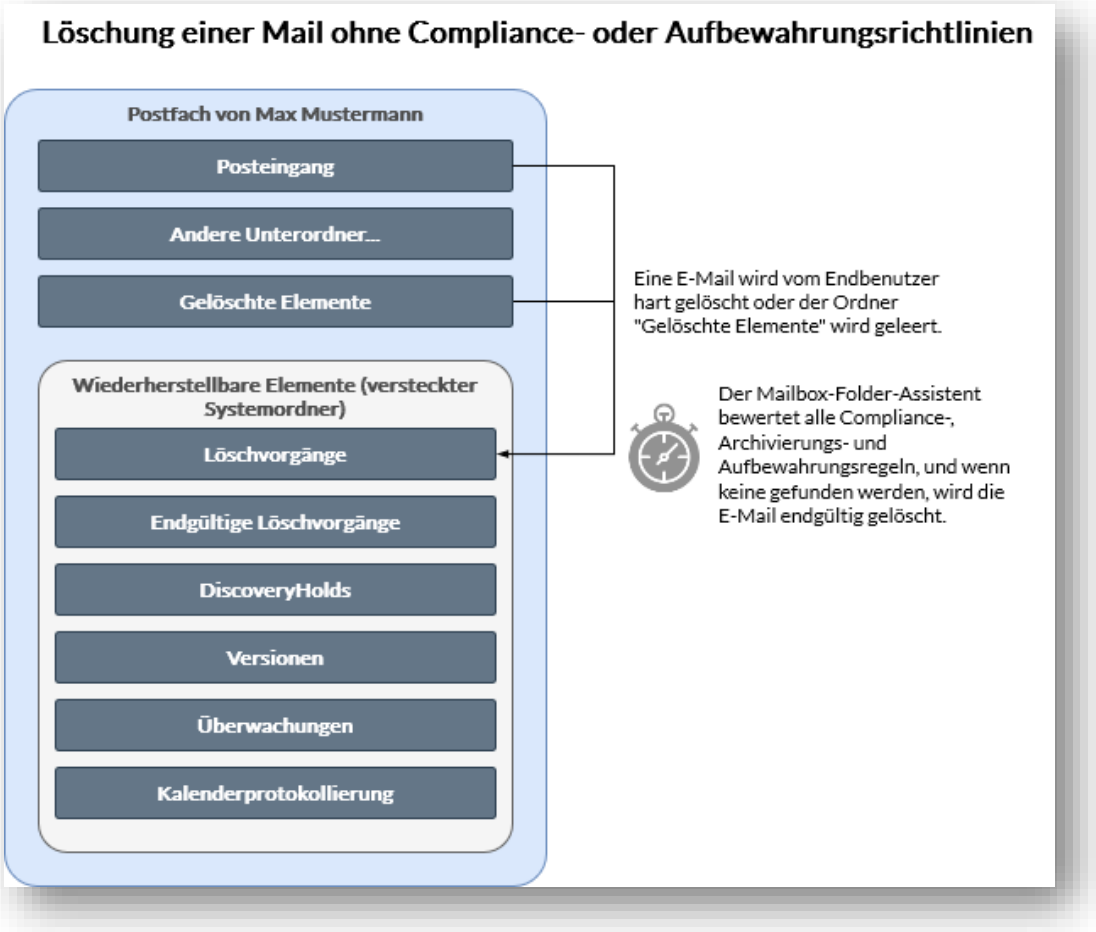
Ein Endbenutzer, Max Mustermann, empfängt oder sendet eine Mail. Die Mail befindet sich entsprechend in seinem Posteingangsordner oder im Ordner Gesendete Elemente in seinem persönlichen Postfach.

Max Mustermann löscht diese Mail und die Nachricht wird in seinen Ordner Gelöschte Elemente verschoben. Dort hat er weiterhin vollen Zugriff auf die Mail, kann sie öffnen, bearbeiten und erneut verschieben.

Alternativ löscht Max Mustermann die Nachricht mit der Tastenkombination UMSCHALT/ENTF. Die Nachricht verschwindet aus der Mailbox und landet unterhalb des Ordners "Wiederherstellbare Elemente" im Unterordner "Löschungen".

Max Mustermann leert seinen Ordner "Gelöschte Elemente". Alle Nachrichten, die sich in diesem Ordner befinden, landen unterhalb des Ordners "Wiederherstellbare Elemente" im Unterordner "Löschungen".

Die Nachricht befindet sich nun im Unterordner "Löschungen". Mustermann kann über die Aktion "Gelöschte Elemente wiederherstellen" in Outlook auf diesen Ordner zugreifen. Er markiert die Nachricht erneut zum Löschen, woraufhin die Mail aufgrund fehlender Compliance-Archivierungsrichtlinien vollständig gelöscht (bereinigt) wird.



Löschvorgang mit aktiver Compliance-Archivierung

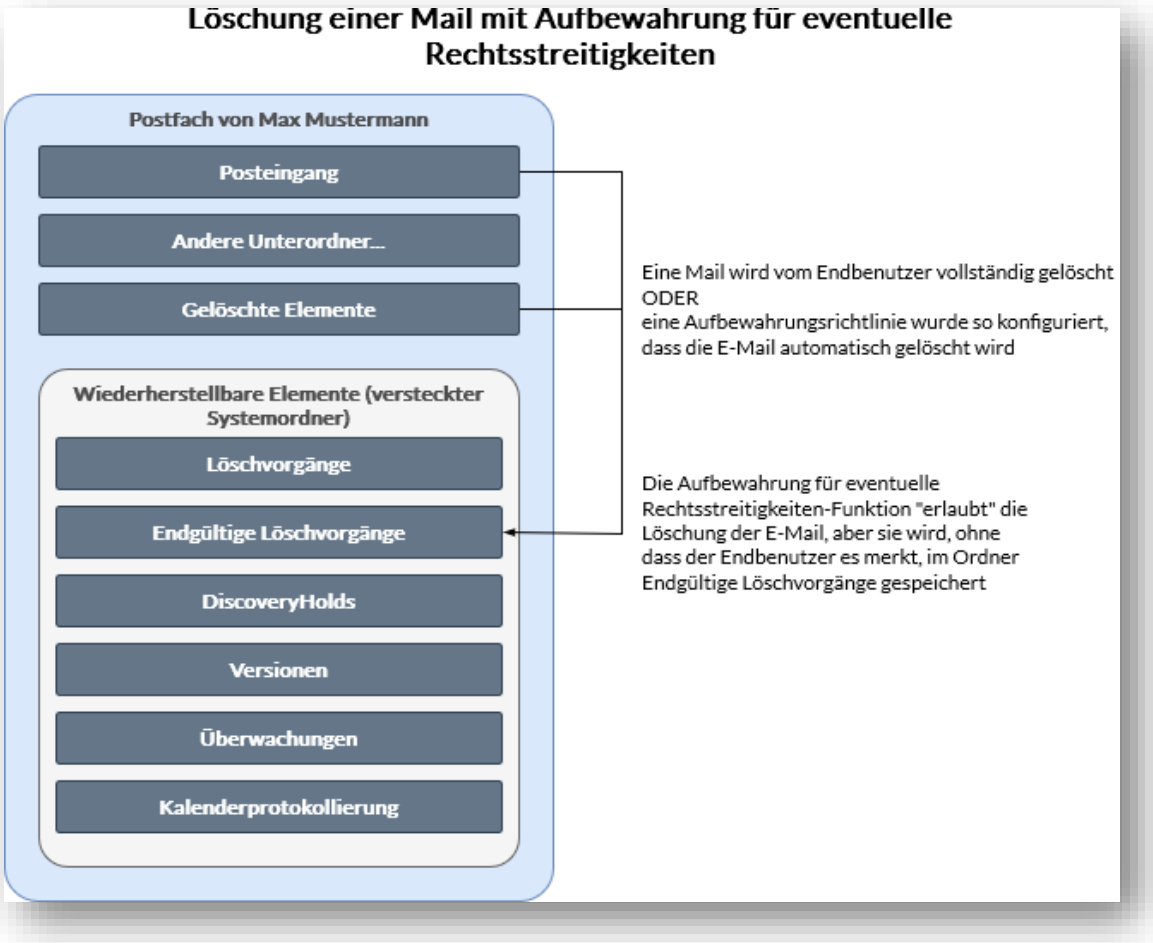
Mit einem Beweissicherungsverfahren eingestellt auf dem Postfach

Die Compliance-Archivierung beginnt mit dem endgültigen Löschen (UMSCHALT+ENTF oder beim Leeren des Ordners Gelöschte Elemente) oder dem Ablauf der Aufbewahrungsfrist für das gelöschte Element.

Die Nachricht befindet sich nun im Unterordner "Löschungen". Auf diesen Ordner kann Mustermann über die Aktion "Gelöschte Elemente wiederherstellen" in Outlook zugreifen. Er markiert die Nachricht erneut zum Löschen, woraufhin die Nachricht aufgrund der Aufbewahrungsfrist für Rechtsstreitigkeiten in den Ordner "Endgültige Löschvorgänge" verschoben wird.

ODER wenn die Nachricht in den Ordner "Löschungen" verschoben wird, wird automatisch ein Zeitstempel erstellt. Dies hängt von der für das Postfach definierten Aufbewahrungsfrist für gelöschte Mails ab. Nach Ablauf der Aufbewahrungsfrist wird die Nachricht automatisch in den Ordner "Endgültige Löschvorgänge" verschoben.

Die Mail verbleibt im Ordner "Endgültige Löschvorgänge", bis der "Aufbewahrung für eventuelle Rechtsstreitigkeiten-Funktion" aus dem Postfach entfernt wurde. Der Inhalt des Ordners " Endgültige Löschvorgänge" kann über eine eDiscovery-Suche, die ebenfalls im Compliance-Portal zu finden ist, abgerufen oder gesucht werden. Der Ordner "Endgültige Löschvorgänge" und der "Aufbewahrung für eventuelle Rechtsstreitigkeiten-Funktion" selbst sind für den Endbenutzer vollständig verborgen. Da die Nachrichten weiterhin wie erwartet gelöscht werden, bemerken die Benutzer möglicherweise nicht, dass sie in der Warteschleife sind. Wenn Ihr Unternehmen verlangt, dass Benutzer in der Warteschleife informiert werden, können Sie der -RetentionComment Eigenschaft des Postfachbenutzers eine Benachrichtigung hinzufügen und die -RetentionUrl Eigenschaft verwenden, um mithilfe von PowerShell einen Link zu einer Webseite für weitere Informationen zu erstellen.

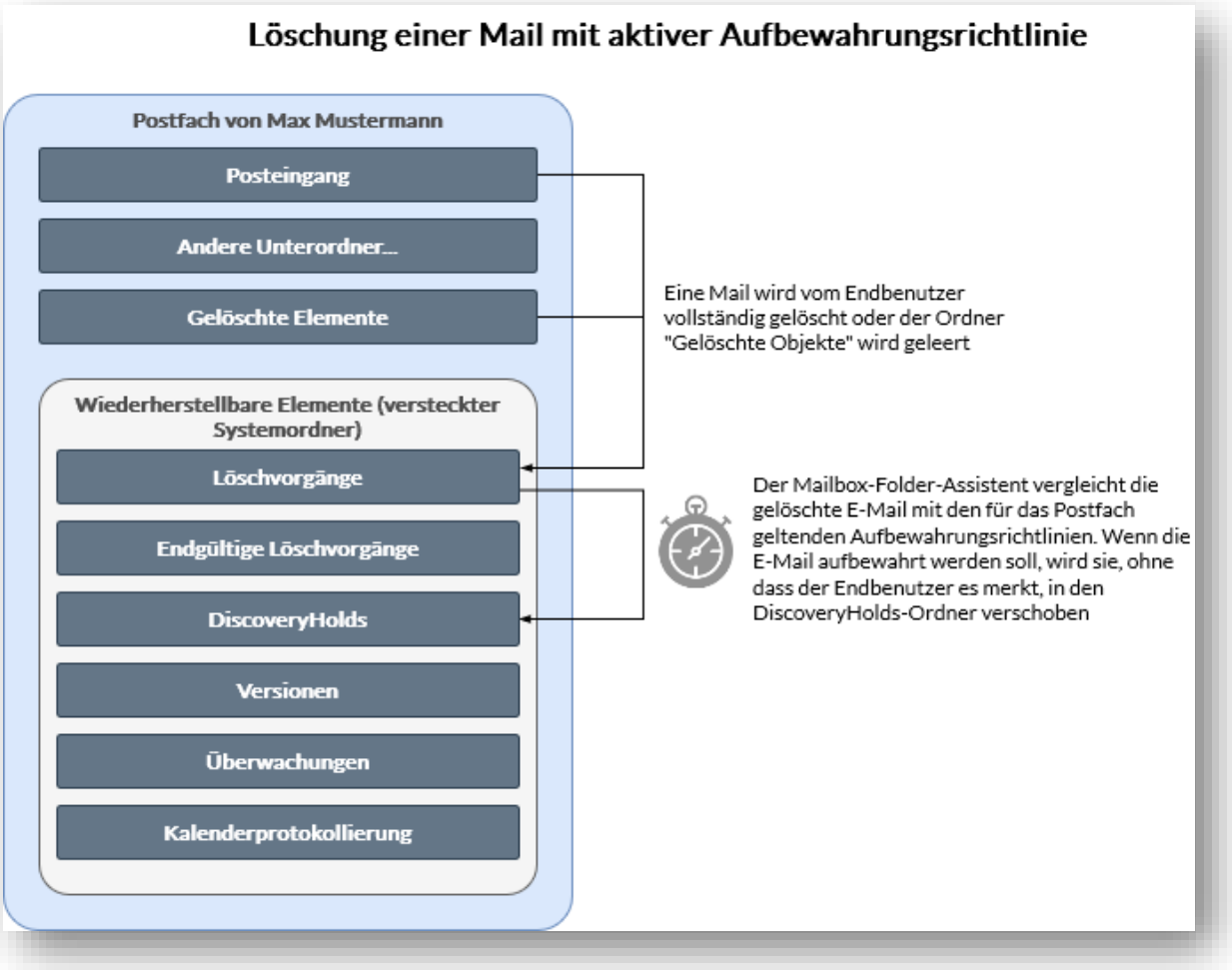


Mit einem eingestellten In-Situ Speicher (Aufbewahrungsrichtlinie)
Die Compliance-Archivierung beginnt mit dem endgültigen Löschen (UMSCHALT+ENTF oder beim Leeren des Ordners „Gelöschte Element“) oder dem Ablauf der Aufbewahrungsfrist für die gelöschte Mail.

Die zum Löschen markierte Nachricht wird aufgrund der aktiven Archivierung in den Ordner "Discovery Hold" verschoben und bleibt dort, bis die Archivierung für das Postfach gestoppt wird. Dies kann darauf zurückzuführen sein, dass die Aufbewahrungsrichtlinie aufgehoben wurde oder dass die Einstellungen in der Aufbewahrungsrichtlinie das Verfallsdatum von Mails/Daten bestimmen.

Der Mailbox-Ordner-Assistent vergleicht den Zeitstempel der Mail täglich mit der verbleibenden Aufbewahrungsfrist für archivierte Elemente. Wenn die Aufbewahrungsfrist abgelaufen ist, wird die Mail zur Löschung markiert und bereinigt.

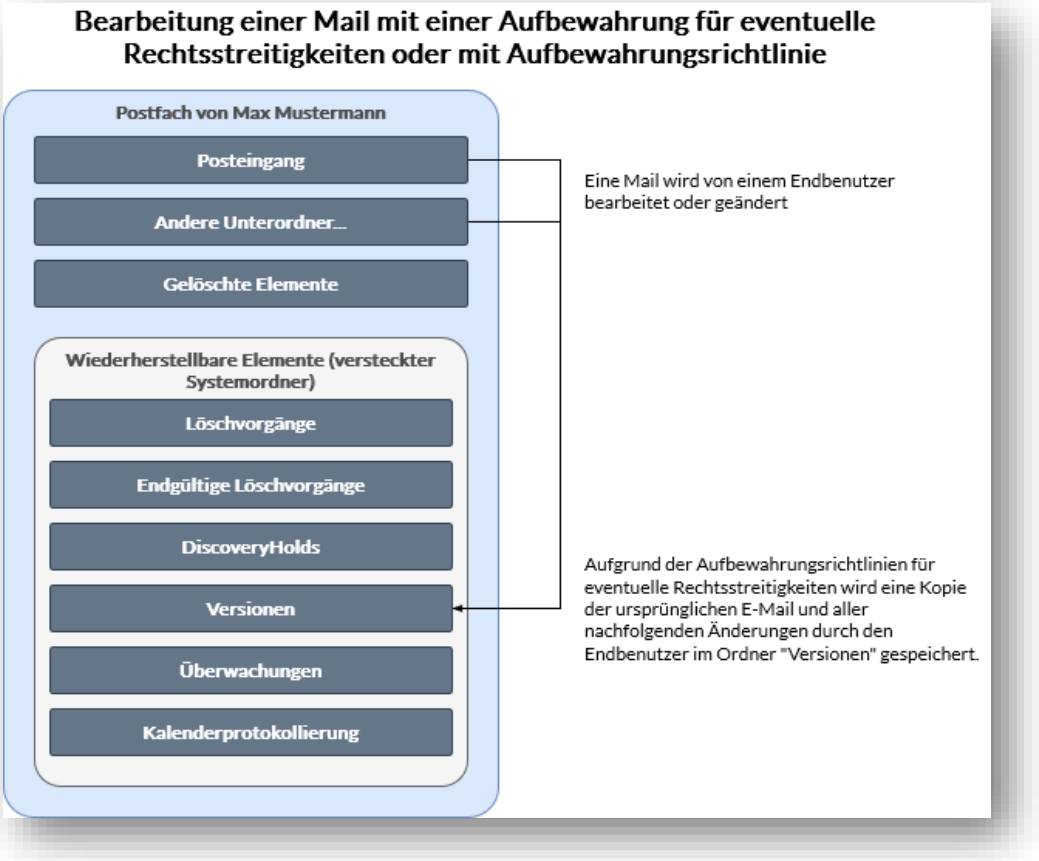
Die Aufbewahrungsfrist und die automatische Löschung von Mails/Daten werden durch Prozesssperren außer Kraft gesetzt. Wenn eine Aufbewahrungsrichtlinie festlegt, dass eine Mail gelöscht werden soll, aber gleichzeitig eine Prozesssperre besteht, wird die Mail "gelöscht", indem es in den Ordner "Endgültige Löschvorgänge" verschoben wird, wo es per eDiscovery-Suche auffindbar ist.



Umgang mit Änderungen bei aktiver Compliance-Archivierung (Versionierung)

Der Ordner "Wiederherstellbare Elemente" enthält einen Unterordner "Versionen". Wenn Max Mustermann bestimmte Eigenschaften der eingehenden Mail ändert (z. B. Betreff, Textkörper, Anhang, Absender und Empfänger, Sende- oder Empfangsdatum), wird eine Kopie des ursprünglichen Elements im Ordner Versionen gespeichert, bevor die geänderte Mail

übertragen wird. Wenn danach weitere Änderungen vorgenommen werden, werden alle Versionen gespeichert. Wird die Aufbewahrung entfernt, werden auch alle Kopien im Ordner "Versionen" vom Mailbox-Assistenten endgültig gelöscht.



Aufbewahrungsfrist

Das Alter der archivierten Elemente richtet sich immer nach dem Datum des Eingangs oder der Erstellung. Ein Element, das in einem zeitbasierten Compliance-Archiv mit einer Aufbewahrungsfrist von 365 Tagen abgelegt wird, verbleibt weitere 65 Tage im Archiv, wenn es 300 Tage nach dem Eingangsdatum gelöscht wird. Zeitbasierte Compliance-Archive können in Verbindung mit einer Aufbewahrungsrichtlinie verwendet werden, um sicherzustellen, dass Mail für den angegebenen Zeitraum aufbewahrt und dann dauerhaft entfernt werden.

Grenzen der Speicherung

Microsoft bietet eine maximale Postfachgröße von 50 GB für die Microsoft 365 Business-Pläne und den Microsoft 365 Enterprise E1-Plan und 100 GB für die Enterprise E3- und E5-Pläne. Ein zusätzliches Archivpostfach bietet weitere 50 GB (Business E1-Tarif) bzw. 100 GB (E3/E5-Tarif) zum Speichern von Postfachinhalten. Endbenutzer, die über eine E3/E5-Lizenz oder eine Exchange Online Plan 2-Lizenz verfügen, können dieses Limit mit der Exchange Online-Funktion zum automatischen Erweitern in Microsoft 365 außer Kraft setzen, um unbegrenzten Speicherplatz für Archivpostfächer zu ermöglichen. Wenn die automatische Erweiterung der Archivierung aktiviert ist, wird dem Archivpostfach eines Benutzers

automatisch zusätzlicher Speicherplatz hinzugefügt, wenn es sich dem Speicherlimit nähert. Dadurch wird dem ursprünglichen Archiv ein sogenanntes „automatisch erweiterte Archivierung“ hinzugefügt. Beispiel: Wenn sich das Archivpostfach der 100-GB-Grenze nähert, wird ein neues expandierendes Archiv bereitgestellt und etwa 50 GB in dieses expandierende Archiv verschoben. Es werden also nur 50% der Daten verschoben, um das zusätzliche Wachstum der Ordner im verschobenen Ordner zu gewährleisten. Die automatische Erweiterung kann für alle Mitarbeiter eines Unternehmens oder nur für bestimmte Benutzer aktiviert werden.

Vergleich der beiden Archivierungsstrategien in Microsoft 365

Unbefristete Archivierung durch Aufbewahrung für rechtliche Zwecke (Beweissicherungsverfahren)

https://docs.microsoft.com/de-de/exchange/security-and-compliance/in-place-and-litigation-holds

Beweissicherungsverfahren wird verwendet, um Elemente in einem Postfach ohne großen Konfigurationsaufwand vor dem Löschen und Ändern zu schützen. Er wird direkt in den Postfacheinstellungen per PowerShell oder im Exchange Admin Portal konfiguriert und kann sowohl für freigegebene als auch für Benutzerpostfächer aktiviert werden. Ab dem Zeitpunkt der Aktivierung werden alle NachrichtenElemente für einen definierbaren Zeitraum oder bis zum Zeitpunkt der Deaktivierung aufbewahrt. Wenn Beweissicherungsverfahren für das Postfach von Max Mustermann aktiviert ist, verbleiben alle gelöschten Elemente im Unterordner Purges des Ordners Recoverable Items, und wenn Änderungen vorgenommen werden, werden die ursprünglichen Elemente im Ordner Versions aufbewahrt. Beweissicherungsverfahren bietet keine Filtermöglichkeiten für die zu archivierenden Elemente.

Beweissicherungsverfahren wird nach wie vor als alternative Methode unterstützt, um Inhalte in einem Postfach aufzubewahren und nach dem Löschen eines Benutzerkontos zu inaktivieren. Da es sich jedoch um eine ältere Technologie handelt, wird empfohlen, stattdessen die Microsoft 365-Aufbewahrung zu verwenden.

Unbefristete Archivierung mit Aufbewahrungsrichtlinien

https://docs.microsoft.com/de-de/microsoft-365/compliance/get-started-with-data-lifecycle-management

Aufbewahrungsrichtlinien ermöglichen - wie der Name schon sagt - die Aufbewahrung von Nachrichten in Postfächern. Sie sind, grob vereinfacht, eine Erweiterung der In-Situ-Aufbewahrung, da definierbare Filter und Schlüsselwörter verwendet werden, um Mails vor dem Löschen zu bewahren und sie für den Benutzer im Ordner „Wiederherstellbare Elemente“ unsichtbar zu halten.

Zusätzlich kann für Aufbewahrungsrichtlinien eine allgemeine Aufbewahrungsfrist definiert werden. Darüber hinaus bieten Aufbewahrungsrichtlinien einen optionalen Schutz gegen nachträgliche Änderungen an der Richtlinie selbst sowie gegen die Deaktivierung der Archivierung von eingeschlossenen Postfächern, einschließlich so genannte „Erhaltungssperre für Richtlinien,“ so dass selbst Administratoren diese nicht entfernen oder ändern können. Aufbewahrungsrichtlinien gibt es auch für andere Datenspeicherorte und Systeme in

Microsoft 365, wie Teams, SharePoint und OneDrive. Sie stellen die empfohlene Lösung von Microsoft für die Aufbewahrung von Daten aus rechtlichen und Compliance-Gründen dar.

Zugriff auf archivierte Daten in Microsoft 365

Der Zugriff auf die Daten der archivierten Postfächer wird über eine rollenbasierte Zugriffskontrolle (RBAC) realisiert. Zu diesem Zweck steht die Rollengruppe eDiscovery Manager zur Verfügung, um Suchaufgaben an nicht-technische Mitarbeiter zu delegieren, ohne dass erhöhte Berechtigungen vergeben werden müssen. Mitglieder dieser Gruppe können eDiscovery-Suchen nach Compliance durchführen, indem sie Postfächer auswählen und dann Suchkriterien wie Schlüsselwörter, Start- und Enddatum, Absender- und Empfängeradressen und Nachrichtentypen angeben. Die Suchergebnisse können dann in der Vorschau angezeigt, kopiert oder exportiert werden.

Besonderheit der archivierten Postfächer in Microsoft 365

Postfächer, auf die die Aufbewahrung zu rechtlichen Zwecken oder die Vor-Ort-Aufbewahrung angewendet wird, sind vor versehentlichem Löschen geschützt, auch wenn sie nicht in einer Aufbewahrungsrichtlinie enthalten sind. Wenn also das zugehörige Benutzerkonto zur Löschung markiert oder die Microsoft 365-Lizenz versehentlich entfernt wird, wird das Postfach zu einem inaktiven Postfach, auf das weiterhin über Compliance eDiscovery-Suchen zugegriffen werden kann. Inaktive Postfächer können alternativ einem neuen Benutzerkonto zugewiesen werden (Wiederherstellung), oder ihr Inhalt kann anderen Postfächern hinzugefügt werden (Wiederherstellung). Das Postfach kann nur gelöscht werden, wenn das Archivierungstag entfernt wird. Damit eignet sich die Mailarchivierung in Microsoft 365 auch als Backup-Schritt im Offboarding-Prozess (Identitätsmanagement).

Vorteile der Mailarchivierung in Microsoft 365

In Kombination mit traditionellen Exchange Online-Postfächern bietet die Mailarchivierung in Microsoft 365 viele Vorteile: Zum einen können Dokumente dauerhaft archiviert werden, so dass keine Daten verloren gehen. Im Falle von Aufbewahrungsrichtlinien werden zudem die strengen Anforderungen an eine revisionssichere Archivierung erfüllt. Zu archivierende Daten werden nicht wie bisher in separate Archive verschoben, sondern verbleiben im Postfach und werden auch bei einer Änderung oder Löschung nur innerhalb des Postfachs verschoben. Durch die Kombination von persönlichen Postfächern ist das Datenvolumen des primären Postfachs gering und kann daher problemlos mit mobilen Geräten abgerufen werden.

Erfolgt die Archivierung in einer Cloud-Lösung (Microsoft 365), gibt es zusätzlich keine Datenvolumenbegrenzung bei der Sicherung, da die Postfachbegrenzung für ein Postfach mit aktivem Archiv-Flag aufgehoben wird. Im Falle eines möglichen Audits können Dritte über das Filtersystem einfach und schnell auf benötigte Daten zugreifen. Durch das Setzen von Filtern kann der Inhalt auch für andere Zwecke gefiltert werden.

Die Handhabung, Verwaltung und Einrichtung der Mailarchivierung in Microsoft 365 ist einfach und transparent. Die Compliance-Archivierung kann darüber hinaus auch als Single-Item-Backup/Restore-Lösung gesehen werden, da archivierte Inhalte vor Löschung geschützt sind und somit jederzeit wiederhergestellt werden können.