Mail Archiving and Retention Options in Microsoft 365 explained simply

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

Contents

E-Mail archiving and retention overview

In Germany, all business and financially relevant mail and documents such as invoices, bank statements, bills and so on must be properly stored and archived in accordance with legal and organizational requirements. When it comes to archiving mail, many companies face challenges in meeting these requirements. According to the German Federal Ministry of Finance, documents must be archived in their entirety, in their original form, as early as possible and unmodified.

Each financially relevant document must be destroyed only after the legally specified period has expired, and every action which may result in changes to these documents in the electronic archiving system must be logged in a way that can be traced. In addition, the archiving process should be available for auditing for accuracy at any time by a third party, so archiving and storage must always be a traceable process. As businesses move towards cloud computing as the dominant usage model, new possibilities for document archiving are becoming available.

In the following document, I will clarify how such protection against changes and deletions can look in Microsoft 365, what requirements a Microsoft 365 administrator must meet to comply with the legal requirements for mail archiving, and which Microsoft 365 solutions are suitable for different requirements. I will focus here on cloud-based solutions offered by Microsoft 365, rather than on-premises solutions.

To be able to ensure the legally compliant and organizationally complex securing and logging of e-mails in the company, it is first important to understand how electronic archiving works and what types of archiving options there are, in general and in Microsoft 365.

Common email archiving solutions

There are usually two types of email archiving solutions:

1. Archive Mailboxes

2. Journal Archiving

The first and most common option is to use an archive mailbox. In this type of backup, the end user has a personal mail archive to which she or he can move messages manually or to which messages are moved automatically. These archive mailboxes can be found on-premises or in the cloud. By creating an archiving policy, this method is primarily used to contain the growth of mailboxes by moving unneeded or old messages. For example, e-mails are automatically moved to a corresponding online archive mailbox after a specified period of one year. However, this type of mail archiving does not meet the legal requirements placed on an archiving solution in Germany, as not all messages are necessarily archived, since the user can generally override even the automatic mail archiving policies. There is always a period between the creation/arrival of a mail in the mailbox and its moving to the archive mailbox. During this period, e-mails can be deleted or modified by end users. E-mails are not protected from deletion even in the archive mailbox.

The second option is journal archiving. This ensures that every received/sent mail is archived, as it often achieved by using so-called journal rules, to which a copy of each incoming/outgoing mail is sent to an external journal mailbox. Normally, the journal mailbox is protected from modification and deletion and even the mail administrators have read-only rights to the mailbox. The way archive data is secured differs depending on the solution provider. The journaling mailbox is often stored on a special WORM (Write-Once-Read-Many) storage medium. If it is ensured that the archived data can be kept unchangeable for a defined period, this is generally referred to as audit-proof archiving.

Which of these options are available in Microsoft 365 and how are they configured? In the next sections, we will examine these solutions in the context of Microsoft 365.

E-Mail Archiving and Retention options in Microsoft 365

MRM policies and their associated retention tags

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

Microsoft 365 via Exchange Online provides the ability to set up Messaging Records Management (MRM) tags and associated policies to automatically move e-mails into an online archive mailbox hosted alongside end-user mailboxes in Exchange Online. Personal archives (in-place archives) are set up via the Microsoft Purview (Compliance) Portal, and then in the old Exchange Online Admin Portal the appropriate archiving/retention policies can be defined and assigned to the end user's mailbox. The retention policies are composed of MRM retention tags. These define what should be done with messages that exist in the primary mailbox. For example, all messages older than one year are moved to the archive mailbox or all messages classified as private remain in the primary mailbox. MRM retention tags are divided into personal and default tags. Personal tags can be enabled by the end-user as needed and applied to the mailbox or individual folders. Default tags are always applied automatically. In addition to MRM retention policies, there are three other options available to the end user to transfer messages to an online (aka in-place) archive:

1. Manually moving or copying messages

2. Move or copy messages using outgoing mail rules

3. Import messages from PST files

Applying a retention policy (the Messaging Records Management (MRM) feature in Exchange Online) does not create an inactive mailbox when the user account is deleted. This is as opposed to the below Compliance archiving method, which will retain deleted users e-mails once a compliance retention policy is assigned to their mailbox. A further unfortunate feature of this older method of archiving/retaining e-mails is that end users also have control over the MRM tags and can override the default policies set for folders and e-mails. To address this issue, Microsoft provides centralized archiving and retention policies for email through the Compliance dashboard in Microsoft 365.

Compliance archiving

The second option available in Microsoft 365 is compliance archiving. It allows the complete retention of mailbox objects. Both deleted items and changes to items are kept (invisible to the user) in a separate area of the mailbox that is excluded from mailbox synchronization to end devices or Outlook. Compliance archiving does not require an archive mailbox but uses special subfolders in the "Recoverable Items" folder for retention that apply to the mailbox and an existing archive mailbox. Online Archive mailboxes can thus be used to expand the usable volume as well as to streamline the user experience, but mail is still retained in the hidden subfolders. Microsoft 365 offers compliance archiving in different forms for different requirements:

- Litigation Hold (retention for legal purposes)
- In-place Hold (in-situ retention) aka holds created by Retention Policies in the Compliance Portal, which can retain based on creation date or subject matter

How does compliance archiving work in Microsoft 365?

To understand the function of compliance archiving in Microsoft 365, it is necessary to explain both the deletion process of a mailbox object and the structure of the "Recoverable Items" folder:

Deletion process without compliance archiving

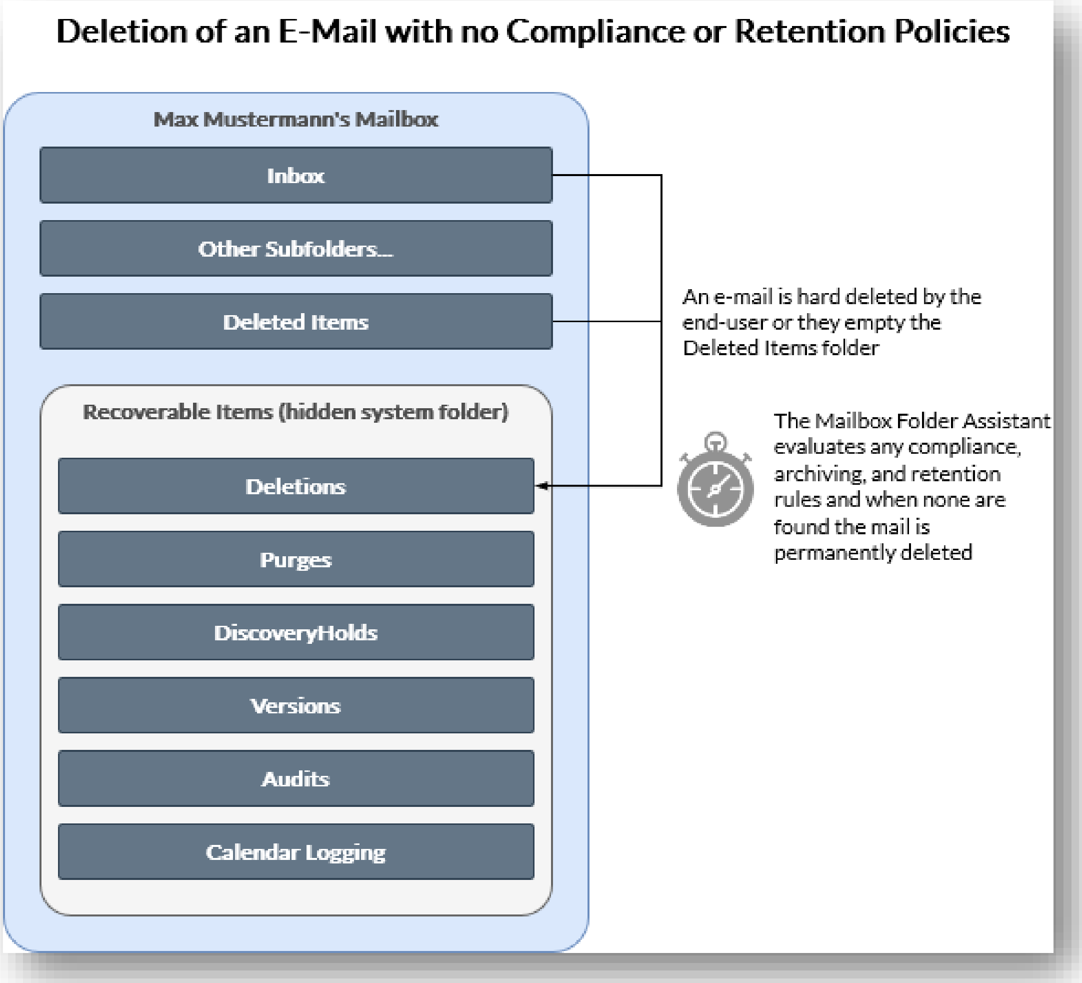
An end-user, Max Mustermann, receives or sends an e-mail. The mail is located accordingly in his Inbox folder or in the Sent Items folder in his personal mailbox.

Max Mustermann deletes this mail, and the message is moved to his Deleted Items folder. There he still has full access to the mail, can open it, edit it and move it again.

Alternatively, Max Mustermann deletes the message with the Shift/Delete key combination. The message disappears from the mailbox and lands below the "Recoverable Items" folder in the Deletions subfolder.

Max Mustermann empties his Deleted Items folder. All messages that are in the folder end up below the "Recoverable Items" folder in the Deletions subfolder.

The message is now in the Deletions subfolder. Mustermann can access this folder via the action "Restore deleted items" in Outlook. He marks the message for deletion again, at which point, due to no compliance archiving policy being in place, the e-mail is fully deleted (purged).


Deletion of an E-Mail with no Compliance or Retention Policies
Max Mustermann's Mailbox
Inbox
Other Subfolders...
Deleted Items
Recoverable Items (hidden system folder)
Deletions
Purges
DiscoveryHolds
Versions
Audits
Calendar Logging
An e-mail is hard deleted by the end-user or they empty the Deleted Items folder
The Mailbox Folder Assistant evaluates any compliance, archiving, and retention rules and when none are found the mail is permanently deleted

Deletion process with active compliance archiving

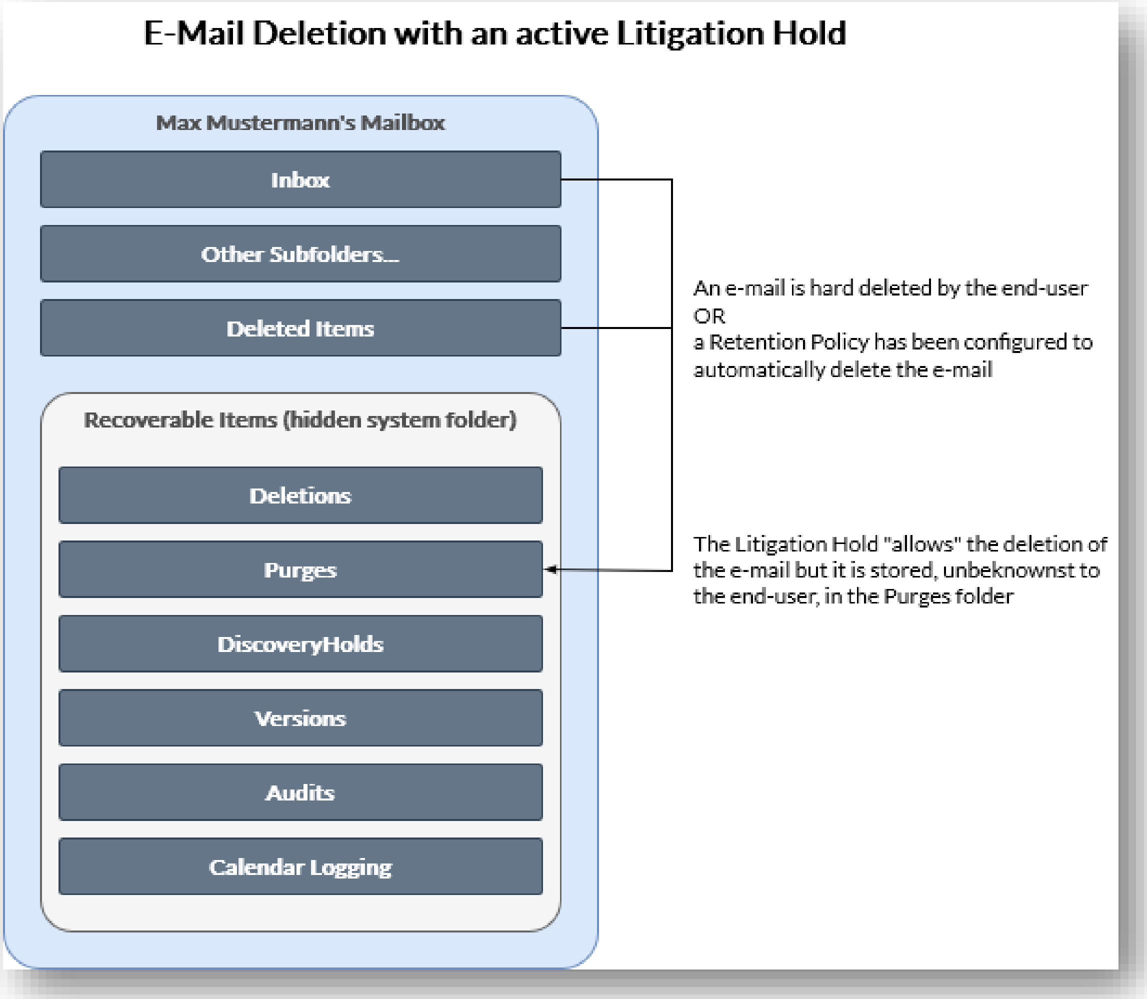
With a Ligation Hold on the mailbox
Compliance archiving starts with the final deletion (SHIFT+DEL or upon emptying of the Deleted Items folder), or the expiration of the retention period for the deleted object.

The message is now in the Deletions subfolder. Mustermann can access this folder via the action "Restore deleted items" in Outlook. He marks the message for deletion again, at which point, due to the presence of a litigation hold, the mail is moved to the Purges folder.

OR when the message is moved to the Deletions folder, an automatic timestamp is generated. This depends on the retention period defined for the mailbox for deleted items. After the retention period expires, the message is automatically moved to the Purges folder.

The e-mail will remain in the Purges folder until the Litigation Hold has been removed from the mailbox. The contents of the Purges folder can be called up or searched for via an eDiscovery search, also found in the Compliance Portal. The Purges folder and the Litigation Hold itself are completely hidden from the end-user. Because messages continue to be deleted as expected, users may not notice they're on hold. If your company requires that users on hold be informed, you can add a notification message to the mailbox user's

RetentionComment property and use the RetentionUrl property to link to a web page for more information using PowerShell.

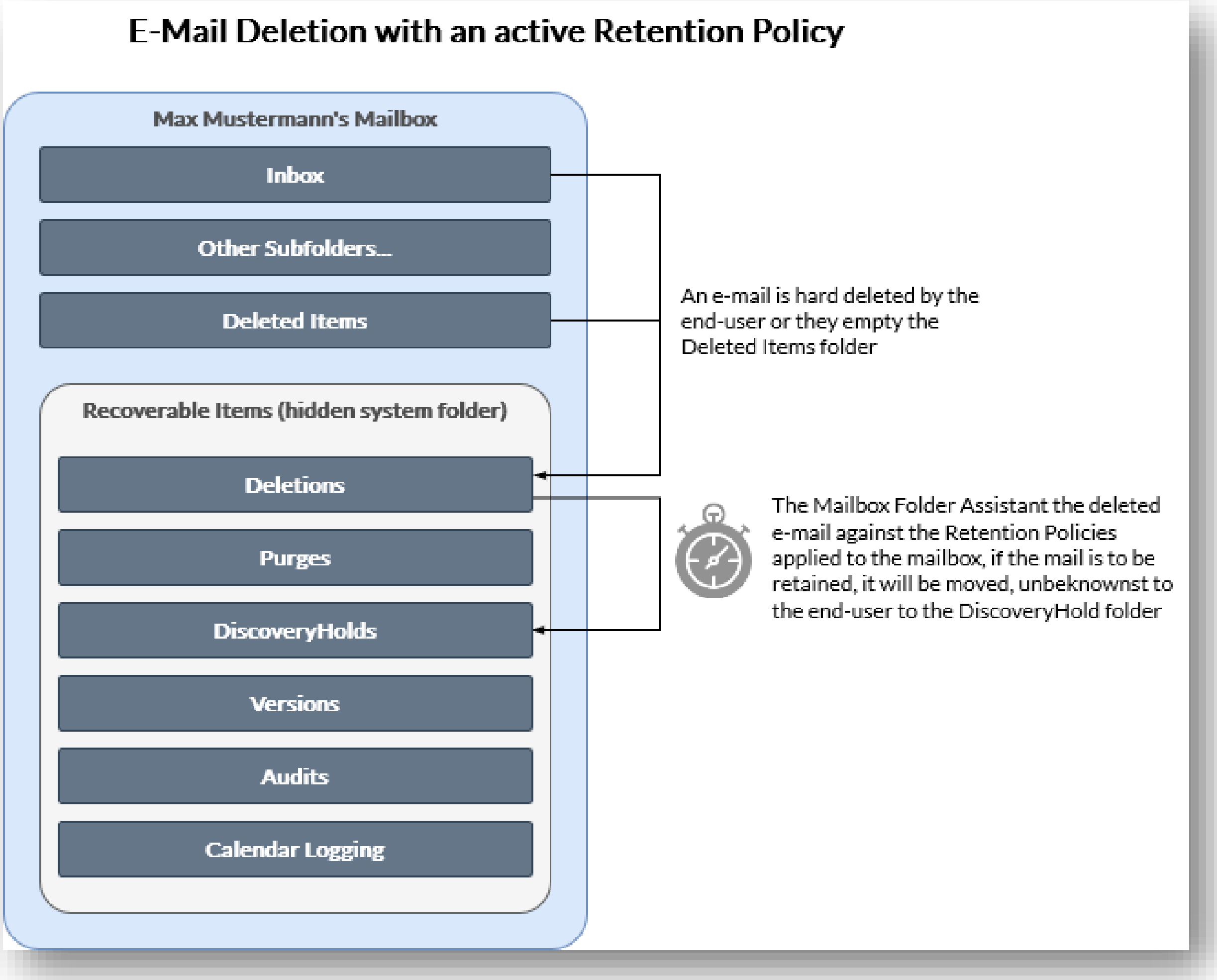

E-Mail Deletion with an active Litigation Hold
Max Mustermann's Mailbox
Inbox
Other Subfolders...
Deleted Items
Recoverable Items (hidden system folder)
Deletions
Purges
DiscoveryHolds
Versions
Audits
Calendar Logging
An e-mail is hard deleted by the end-user
OR
a Retention Policy has been configured to automatically delete the e-mail
The Litigation Hold "allows" the deletion of the e-mail but it is stored, unbeknownst to the end-user, in the Purges folder

With an In-Place Hold (Retention Policy)
Compliance archiving starts with the final deletion (SHIFT+DEL or upon emptying of the Deleted Items folder), or the expiration of the retention period for the deleted object.

The message marked for deletion is moved to the Discovery Hold folder due to active archiving and remains there until archiving is stopped for the mailbox. This can be due to the Retention Policy being lifted or due to the settings in the Retention Policy determining the expiration date of e-mails/data.

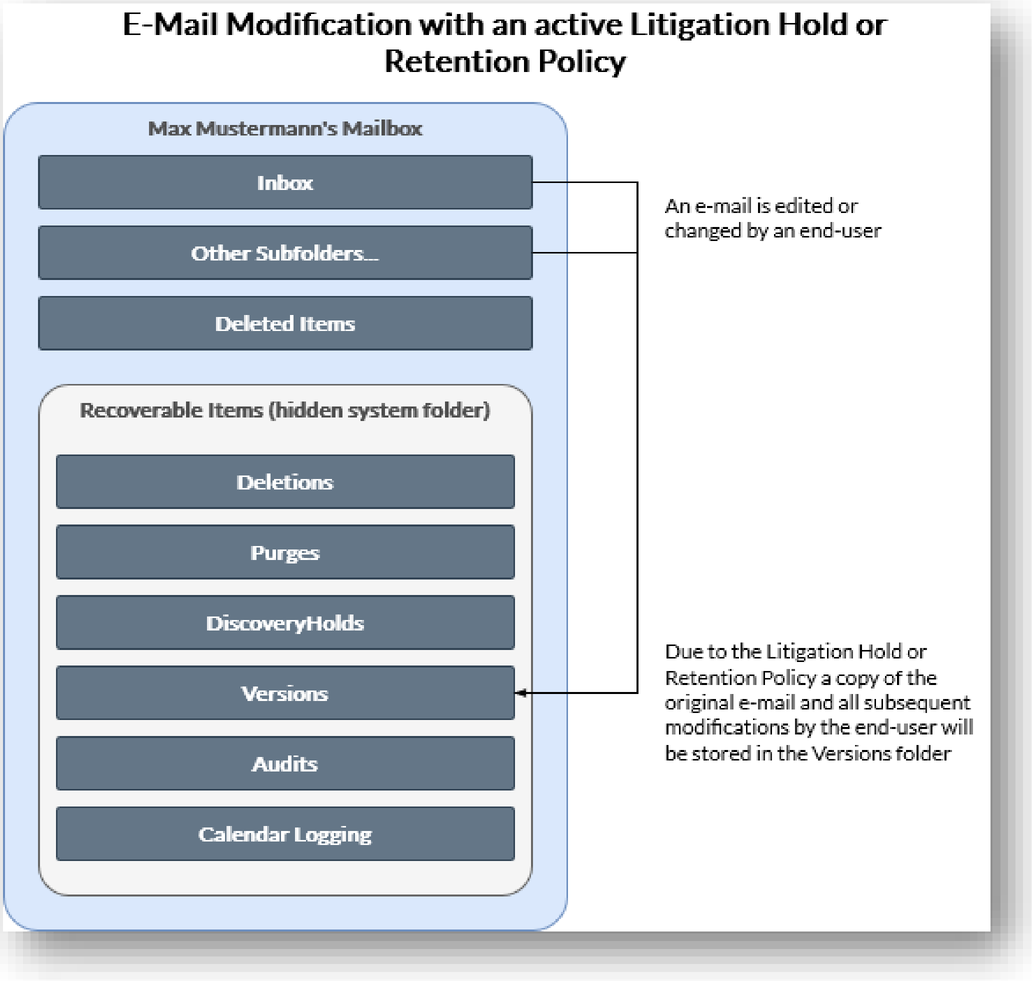
The Mailbox Folder Assistant checks the object's timestamp daily against the remaining retention period for archived items. If the retention period has expired, the item is marked for deletion and purged.

Litigation Holds will override the retention period and the automatic deletion of e-mails/data. Should a Retention Policy determine that an item is to be deleted but a Litigation Hold is also in place, the item will be "deleted" by moving it to the Purges folder, where it is discoverable per eDiscovery Search.


E-Mail Deletion with an active Retention Policy
Max Mustermann's Mailbox
Inbox
Other Subfolders...
Deleted Items
Recoverable Items (hidden system folder)
Deletions
Purges
DiscoveryHolds
Versions
Audits
Calendar Logging
An e-mail is hard deleted by the end-user or they empty the Deleted Items folder
The Mailbox Folder Assistant the deleted e-mail against the Retention Policies applied to the mailbox, if the mail is to be retained, it will be moved, unbeknownst to the end-user to the DiscoveryHold folder

How modifications are handled with active compliance archiving (aka Versioning)

The Recoverable Items folder contains a Versions subfolder. If Max Mustermann changes certain properties of the incoming mail (for example, subject, body, attachment, sender and recipient, send or receive date), a copy of the original item is saved in the Versions folder before the modified mail is transmitted. If further changes are made afterwards, all versions will be saved. If the preservation is removed, all copies in the Versions folder will also be permanently deleted by the mailbox wizard.


E-Mail Modification with an active Litigation Hold or Retention Policy
Max Mustermann's Mailbox
Inbox
Other Subfolders...
Deleted Items
Recoverable Items (hidden system folder)
Deletions
Purges
DiscoveryHolds
Versions
Audits
Calendar Logging
An e-mail is edited or changed by an end-user
Due to the Litigation Hold or Retention Policy a copy of the original e-mail and all subsequent modifications by the end-user will be stored in the Versions folder

Retention period

The age of archived items is always based on the date of receipt or creation. The item placed in a time-based compliance archive with a retention period of 365 days will remain in the archive for another 65 days if it is deleted 300 days after the date of receipt. Time-based compliance archives can be used in conjunction with a retention policy to ensure that items are retained for the specified period and then permanently removed.

Storage limits

Microsoft offers a maximum mailbox size of 50 GB for the Microsoft 365 Business plans and Microsoft 365 Enterprise E1 plan, and 100 GB with the Enterprise E3 and E5 plans. An additional archive mailbox provides an additional 50 GB (Business E1 plan) or 100 GB (E3/E5 plan) to store mailbox content. End users who have an E3/E5 license, or an Exchange Online Plan 2 license, can override this limit with the Exchange Online auto-expand feature in Microsoft 365 to allow unlimited storage for archive mailboxes. When auto-expand archiving is turned on, additional storage is automatically added to a user's archive mailbox as it approaches the storage limit. This adds a so-called expanding archive to the original archive. Example: When the archive mailbox approaches the 100 GB limit, a new expanding archive is provided and about 50 GB is moved to this expanding archive. So, only 50% of the data is moved to ensure the additional growth of the folders in the moved folder. Automatic expansion can be enabled for all employees of a company or only for specific users.

Comparison of the two archiving strategies in Microsoft 365

Indefinite archiving by means of retention for legal purposes (Litigation Hold)

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

Litigation hold is used to preserve items in a mailbox from deletion and modification without much configuration effort. It is configured directly in the mailbox settings per PowerShell or the Exchange Admin Portal and can be enabled for shared as well as user mailboxes. From the moment of activation, all message objects are kept for a definable period or until the time of deactivation. If Litigation Hold is enabled for Max Mustermann's mailbox, all deleted items remain in the Purges subfolder of the Recoverable Items folder, and if changes are made, the original items are kept in the Versions folder. Litigation Hold does not provide filtering options for the items to be archived.

Litigation hold is still supported as an alternative method to keep content in a mailbox and make it inactive after a user account is deleted. However, as an older technology, it is recommended to use Microsoft 365 retention instead.

Indefinite archiving with retention policies

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

Retention policies enable - as the name suggests – the retention messages in mailboxes. They are, roughly simplified, an extension of in-situ retention, as definable filters and keywords are used to keep items from being deleted and to keep them invisible to the user in the Recoverable Items folder.

Additionally, a general retention period can be defined for retention policies. Furthermore, retention policies offer optional protection against subsequent changes to the policy itself as well as against the deactivation of archiving of included mailboxes, including so-called Preservation Locks on policies so that even admins cannot remove or change them. Retention Policies are available for other data storage locations and systems in Microsoft 365, such as Teams, SharePoint, and OneDrive. They represent the recommended solution from Microsoft for retaining data for legal and compliance purposes.

Access to archived data in Microsoft 365

Access to the data of archived mailboxes is realized via role-based access control (RBAC). For this purpose, the eDiscovery Manager role group is available to delegate search tasks to non-technical employees without the need to grant elevated privileges. Members of this group can perform compliance eDiscovery searches by selecting mailboxes and then specifying search criteria such as keywords, start and end dates, sender and recipient addresses, and message types. The search results can then be previewed, copied or exported.

Special feature of archived mailboxes in Microsoft 365

Mailboxes to which retention for legal purposes or in-place retention is applied are protected from accidental deletion, even if they are not included in a retention policy. Therefore, if the associated user account is marked for deletion or the Microsoft 365 license is accidentally removed, the mailbox becomes an inactive mailbox that can still be accessed through Compliance eDiscovery searches. Inactive mailboxes can alternatively be assigned to a new user account (recovery), or their contents can be added to other mailboxes (restore). The mailbox can only be deleted when the archive flag is removed from it. Thus, mail archiving in Microsoft 365 is also suitable as a backup step in the offboarding process (identity management).

Advantages of mail archiving in Microsoft 365

In combination with traditional Exchange Online mailboxes, mail archiving in Microsoft 365 offers many advantages: First, documents can be archived permanently, so no data is lost. In the case of preservation guidelines, the strict requirements for audit-proof archiving are also met. Data to be archived is not moved to separate archives as before but remains in the mailbox and is only moved within the mailbox even in the event of a change, or deletion. Due to the combination of personal mailboxes, the data volume of the primary mailbox is low and can therefore be accessed with mobile devices without any problems.

If archiving takes place in a cloud solution (Microsoft 365), there is additionally no data volume limit when backing up, as the mailbox cap is lifted for a mailbox with an active archive flag. In the event of a possible audit, third parties can easily and quickly access required data through the filter system. Content can also be filtered for other purposes by setting filters.

Handling, managing and setting up mail archiving in Microsoft 365 is simple and transparent. Compliance archiving can additionally also be seen as a single-item backup/restore solution, as archived content is protected against deletion and can therefore be restored at any time.