Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **February 2023**
Commissioned by **MailStore**

The Benefits of Third-Party Email Archiving for Businesses Using Microsoft 365

Executive Summary

Email continues to be the primary method of communication and collaboration for most users, despite the increased use of new solutions such as Microsoft Teams and Slack. Email contains a wealth of critical information which must be protected through robust email backup and archiving capabilities so that businesses and users have ready access to their data at all times.

Businesses moving to Microsoft 365 must continue to employ best practices for email backup and archiving to protect, preserve, and keep available their corporate data. Backup and archiving don't happen automatically in Microsoft 365. In addition, email backup and archiving capabilities must accommodate scenarios that Microsoft 365 does not handle as well as some third-party solutions, such as hybrid environments and those that include non-Microsoft data.

This white paper discusses why small and mid-sized businesses (SMBs) should deploy an email archiving solution, and why they should consider the use of a third-party solution instead of the native email archiving solutions within Microsoft 365.

KEY TAKEAWAYS

Here are the key takeaways discussed in this white paper:

- **Microsoft 365 is being widely adopted by SMBs**
  Microsoft 365 offers a wide range of communication and collaboration capabilities at a reasonable price. Further, it requires only minimal IT involvement to maintain and is offered by a trusted and reliable vendor.
- **Decision makers are obligated to take good care of their data**
  Using a single vendor in the cloud for email, collaboration, email backup, email archiving, and more makes everything simpler for IT. However, this does not release decision makers from their obligation to take good care of their data.
- **SMBs need robust email backup and archiving capabilities**
  To take good care of their data, SMBs should have robust email backup and archiving capabilities to protect and preserve their critical data assets, many of which are stored in their email systems. Email backup and archiving address complementary use cases, and both are needed.
- **Microsoft is not responsible for protecting and preserving its customers' data**
  Under the "shared responsibility model" in Microsoft 365, customers must take proactive steps to ensure that their data is appropriately backed up and archived.
- **The consequences of not proactively protecting data can be significant**
  Consequences include accidental or malicious deletion of important data, ransomware that renders data inaccessible, and an inability to respond to legal or regulatory demands for data, among others.
- **Deploy and maintain a robust email archiving solution**
  Every organization should deploy and maintain a robust email archiving solution to preserve its business records in email and ensure that these records can be searched and produced efficiently. Decision makers should consider the use of third-party solutions to preserve and archive their data.

SMBs should have robust backup and archiving capabilities in place to protect, preserve, and keep available their critical data assets.

ABOUT THIS WHITE PAPER

This white paper was commissioned by MailStore. Information about MailStore is provided at the end of the paper.

The Growing Importance of Microsoft 365 for Businesses

Microsoft 365 is of growing importance to businesses across the world. In this section, we look at the growing installed base and penetration into the business email and collaboration market.

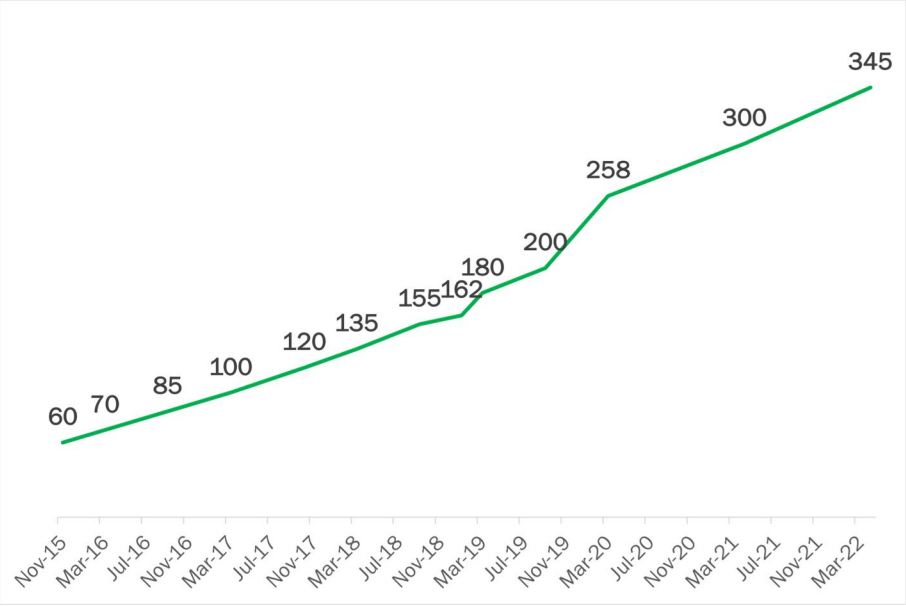
A GROWING NUMBER OF ORGANIZATIONS ARE DEPLOYING MICROSOFT 365

Microsoft 365 is a robust and capable platform that provides a wide range of capabilities, including email, desktop productivity applications, collaboration, security, archiving, encryption, voice, and other services. Microsoft offers a variety of Microsoft 365 plans for small businesses, enterprises, government entities, educational institutions, and home users.

Although Microsoft has been providing hosted solutions in one form or another since the late 1990s, Microsoft 365 represents the most successful iteration of the company's not-on-premises email and collaboration offering. Based on the most recently released data from Microsoft, the company had nearly 345 million users at the end of the first quarter in 2022, as shown in Figure 1.[1] This is nearly six times higher than the number of users in November 2015.

Microsoft 365 is a robust and capable platform.

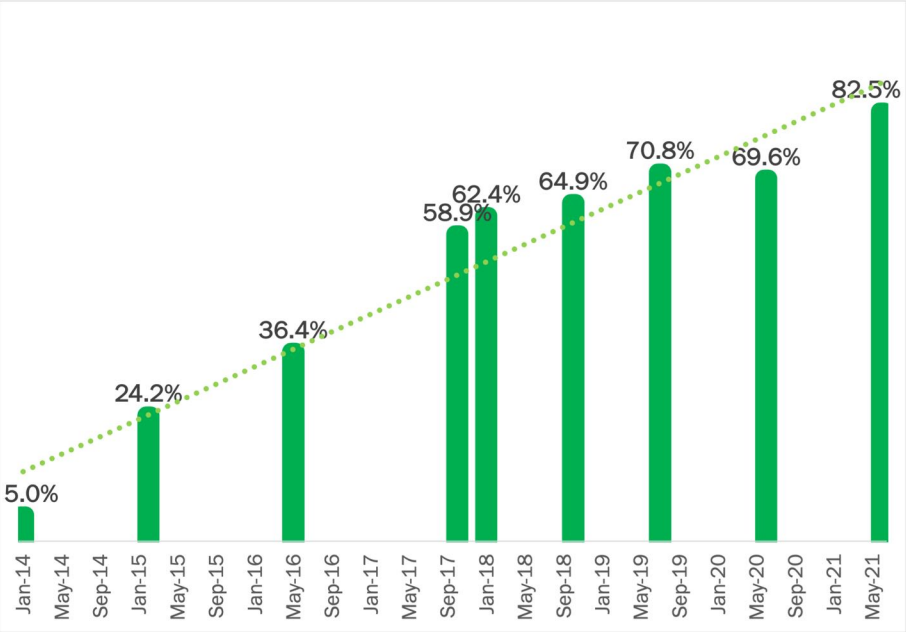
Figure 1
Global Users of Microsoft 365 Commercial Plans
Millions of users



Source: Osterman Research (2023) based on data published by Microsoft Corporation

Coincident with the growth of the installed base of Microsoft 365 is the increasing penetration of Microsoft 365 into the business-grade email and collaboration market. Market tracking by Osterman Research through multiple surveys in recent years has witnessed ongoing and significant growth in the usage of Microsoft 365 for email among businesses in North America—with over 80% penetration in less than a decade in market (see Figure 2).

Figure 2
Penetration of Microsoft 365
Percentage of business-grade email users in North America equipped with Microsoft 365



Source: Osterman Research (2023)

MICROSOFT 365 FREES ORGANIZATIONS FROM STORAGE-DRIVEN CONCERNS, BUT THERE IS A DOWNSIDE

One of Microsoft's fundamental value propositions of Microsoft 365's email component, Exchange Online, is its very large mailboxes. As a rule, Microsoft 365 offers a 50-gigabyte mailbox for the Business plans and 100-gigabyte mailboxes for the more expensive Microsoft 365 and Office 365 Enterprise plans.[2]

Very large mailboxes can be a boon to user productivity because they don't limit users' ability to store information, and they absolve organizations from storage-driven email concerns. However, there are downsides to having such an enormous quantity of storage available to each user, such as:

- **More significant data breach when an account is compromised**
  If a user's Microsoft 365 account credentials are compromised through a phishing attack, the threat actor gains access to a significant trove of valuable business data. If data had been moved to a separate archive, the scope of the data breach would be significantly less.
- **Longer restoration timeframes**
  If a 50-GB or 100-GB mailbox needs to be restored from backup, the user will be offline much longer than if information is continuously migrated to an archive.
- **Reduced responsiveness and performance in Outlook**
  Responsiveness and performance in Outlook decrease if there are too many items in a folder,[3] and Outlook has a history of an increasing number of application pauses as the size of the mailbox grows beyond 10 gigabytes.[4]

Organizations relying on massive user mailboxes face downsides including a greater data breach scope, longer restoration timeframes, and reduced application performance.

The Need for Email Archiving

Organizations using email for business communications need assurance of accuracy and completeness in their email records. In this section, we look at business drivers for email archiving, and why backup is not email archiving.

BUSINESS DRIVERS FOR EMAIL ARCHIVING

Email continues to be the primary method of communication and collaboration in the vast majority of organizations, including SMBs. Consequentially, email systems contain a wide variety of data types, such as contracts, purchase orders, marketing plans, shipping records, communications with clients and prospects, responses to technical support inquiries, HR records, evidence of sexual harassment and unfair treatment of employees, and many other types of information—all of which are business records. Purely from the perspective of knowing what has been offered, stated, agreed, or disputed, having an accurate and complete record of email is essential to an organization meeting its business, administrative, or governmental requirements. For example, there are day-to-day situations in which having ready access to email data is useful:

- **An order is disputed**
  A salesperson needs to find all information when a customer has a dispute about an order.
- **A commitment is questioned**
  A supplier asks about a commitment that was made to them.
- **An email is accidentally deleted**
  A user accidentally deleted or removed an email from his mailbox.
- **Email services are unavailable**
  An email is unavailable on the mail server or service, and also not present in the latest backup.
- **A legal investigation is launched**
  Competitors, customers, business partners, and disgruntled employees can all initiate legal proceedings against an organization to gain redress or compensation for an alleged wrongdoing.
- **An internal investigations seeks evidence**
  Allegations of sexual harassment, unfair treatment, racial discrimination, and other employment-related charges can only be addressed if full and accurate records are available.

Email continues to be the primary method of communication and collaboration in the vast majority of organizations, including SMBs.

COMPLIANCE DRIVERS FOR EMAIL ARCHIVING

Efficient organizational operations and navigating day-to-day situations are only the beginning of why an accurate and complete record of email is essential. An increasing number of organizations face a growing collection of stringent regulatory obligations, industry requirements, and legal decisions. For example:

- **GDPR in Europe**
  There is a need to determine if the company is complying with the European Union's General Data Protection Regulation (GDPR), including data collection, processing, and storage.
- **Privacy obligations in the United States**
  State-level data privacy obligations in the United States impose GDPR-like

requirements on organizations collecting and processing data on the people covered by these new regulations.

- **Data retention obligations**
  Regulations specific to the healthcare, financial services, manufacturing, energy, and aviation industries, among others, commonly impose data retention obligations on email messages. While the specifics vary by country and industry, email messages usually have to be retained for multiple years.

As a result, because business records must be retained for the appropriate length of time as determined by court decisions, regulatory obligations, industry best practices, or the advice of legal counsel, every organization should maintain an archive of its emails and attachments to retain and preserve these records.

A failure to retain records carries a number of consequences. These include the inability for an organization to adequately defend itself in a legal action, a court fine or sanction for a failure to retain required records, regulatory fines, and the inability to fully retain a record of information that can be crucial in the normal operation of a business.

IS EMAIL ARCHIVING UNNECESSARY WHEN USING BACKUP?

Businesses relying on email should be doing both email archiving and backup. These are complementary best practices that address different strategic use cases, not competing ones:

- **Backup meets the strategic use case of disaster recovery**
  Email backups are intended for the strategic use case of enabling business continuity and disaster recovery, including issues that cause data loss. These range from a software upgrade that goes awry to a rogue administrator or other employee that deletes data. Backups have a short-term focus, they contain unindexed data, they are typically retained for no more than 30 to 90 days, and they are intended to snapshot data at a given point in time.
- **Email archiving meets the strategic use case of information protection, availability, and discovery**
  Email archives are intended for strategic purposes to preserve business records in response to legal, regulatory and best practice requirements. Email archiving is essential to preserve data in its original form, to index email data for purposes of search and retrieval, and to keep it available and retrievable at any time. While email backups have a short-term focus, email archives are designed for data that must be retained for longer periods—sometimes one year, but more often three to seven years, or for an indefinite period of time. Moreover, while email backups are designed to capture snapshots of data at one point in time, email archiving captures all business records on a continual basis and is there to work with for browsing, restoring records when necessary, and complying with retention requirements.

UNDERSTAND THE ADVANTAGES AND DISADVANTAGES OF NATIVE MICROSOFT 365 EMAIL ARCHIVING

It is essential for decision makers considering or using any email system with bundled archiving capabilities—including Microsoft 365—to understand what the native email archiving capabilities within the platform can and cannot do. Based on this understanding, decision makers must determine if those capabilities will meet their organization's email archiving requirements.

It is essential for decision makers considering or using Microsoft 365 to understand what the native archiving capabilities within the platform can—and cannot—do.

The Native Archiving Options in Microsoft 365

While Microsoft offers a robust and capable communication and collaboration solution in Microsoft 365, email is not automatically archived. Organizations that have deployed Microsoft 365 must either invest the time and effort to fully understand how to reliably apply combinations of information governance and compliance features, such as retention policies and legal holds, or use a third-party email archiving solution that may be more intuitive to use, especially for SMBs with limited or no dedicated IT department. In this section, we look at what is available in Microsoft 365.

CONCEPTUAL PILLARS OF EMAIL ARCHIVING IN MICROSOFT 365

Microsoft's conceptual approach and architecture for email archiving in Microsoft 365 rests on four interrelated pillars:

1. **Messages are "archived" where they are in Exchange Online, not in a secondary archive**
   Email messages can be protected from deletion wherever they are located in Exchange Online—which in essence creates an archive of protected content. Creating a secondary archive copy of email messages in Microsoft 365 is not done. In Microsoft's view, as long as suitable deletion protections are established over every email and email attachment, a secondary archive copy is not required. There is a clear risk of failure in this approach, in that if the protections are circumvented or fail, authoritative data is likely to be lost.
2. **Retention policies specify what is and isn't kept—and for how long**
   Retention policies can specify how long messages are retained—that is, not able to be deleted—and when they must be deleted, across both the user's primary and archive mailboxes.
3. **Archive policies specify movement of messages to a user's archive mailbox**
   Archive policies specify which messages are moved to a user's archive mailbox when email archiving is enabled or Exchange Online Archiving is used. These policies move messages out of the user's primary mailbox to their archive mailbox, generally based on time. Retention policies apply to the user's primary and archive mailboxes, and messages are protected wherever they are located. The size of the user's primary mailbox is dictated by the plan they are assigned and can never grow larger than this allocated quota.
4. **Archive, legal, and eDiscovery capabilities depend on the Office 365 or Microsoft 365 plan assigned to each and every user**
   The capabilities available for archiving, legal hold, and eDiscovery are determined at the level of each individual user, not the organization as a whole. While Microsoft 365 enables the mix-and-match of plans within a given organization, the higher-priced plans are needed for full capabilities.

What this conceptual architecture means, therefore, is that the "archiving" options in Microsoft 365 address where a message is stored. None of the native archiving options by themselves include special protections to prevent alteration or deletion—that requires the complementary use of retention policies. In the case of Exchange Online Archiving, the archive mailbox reduces the volume of mailbox items stored in the user's primary mailbox, which can never grow larger than the 50-GB or 100-GB size limit (which is dictated by the plan assigned to the individual).

While Microsoft offers a robust and capable communication and collaboration solution in Microsoft 365, email is not automatically archived in the platform.

An essential point to note is that Microsoft's conceptual approach of in-place archiving (i.e., retention policies can be applied wherever the message is located) means that all data received by, created within, or saved to a workload in Microsoft 365 is already considered part of the data set—irrespective of where it is stored. A newly received email in Exchange Online is already in the Microsoft 365 storage universe, and whether it remains in the user's primary mailbox or is moved to the user's archive mailbox, its storage location is irrelevant. If compliance and information governance capabilities are included in the plan assigned to an individual, they work across the individual's primary and archive mailboxes.

There are four options for archiving email messages and other mailbox items in Microsoft 365: archive to PST, archive to a folder in Outlook using the archive button, archive to a separate mailbox, and archive to a separate mailbox using Exchange Online Archiving. We look at these options below.

OPTION 1: ARCHIVE TO PST

Any user can "archive" their email content to PST files that are stored locally or in the cloud. This content is not indexed and so is difficult to search and produce when needed for internal investigations, early case assessment, and other legal situations. Archiving to PST is not a recommended option for meeting compliance and information governance requirements for email archiving. Moreover, PST files are intended only for archiving in an Outlook context, since the initial Outlook archiving feature (called AutoArchive) is based on PST files. While Microsoft calls this feature "archiving," it is not a true archive. The feature is designed only to relieve mailboxes of less-used and older emails.

How it works: users can choose folders or individual emails to archive and these can be manually or automatically moved out of the primary mailbox. This content will be stored as a PST file in a location of the user's choosing.

PST files can be deleted at will by anyone with access to them, and can be irretrievably lost if the user's computer storing the PST file is corrupted, lost, or stolen. If PST files are stored in OneDrive, they will be lost when the user leaves the organization and their Office 365 account is deactivated (unless special action is taken to retain OneDrive contents).

The "Archive" button in Outlook merely moves messages to a folder called "Archive" in the user's primary mailbox. Microsoft says to think about it as just another file folder.

OPTION 2: MOVE MESSAGES TO THE ARCHIVE FOLDER IN OUTLOOK USING THE ARCHIVE BUTTON

The Outlook client includes a button for "archiving" messages, although this merely moves messages to a folder called "Archive" in the user's primary mailbox (accessible via Outlook). This capability changes where a message is stored in the user's mailbox, but has nothing to do with archiving from a compliance and information governance point of view unless retention policies are in force on the user's Exchange Online mailbox. Without retention policies, the user can delete and modify messages in the "Archive" folder.

Microsoft's recommendation on the use of the Archive button in Outlook echoes this reality: "*We recommend that you use the Archive feature to keep your Inbox clear of messages that you've already answered or acted on. Think of the Archive like a file folder. You can store items in the Archive folder and still access them easily. You can also delete messages or move them to specific folders, if that's more your style*."[5]

Microsoft targets the Archive button in Outlook at organizations where users will not exceed the 50-GB size limit of an Exchange Online mailbox in the lower-priced Microsoft 365 and Office 365 plans, which in Microsoft's approach avoids the need for archiving content in a separate mailbox. Since the size of the user's mailbox on these plans cannot be increased above 50 GB, if more storage is required, an archive mailbox is Microsoft's solution.

OPTION 3: ARCHIVE TO AN ARCHIVE MAILBOX WITHOUT USING EXCHANGE ONLINE ARCHIVING

The less expensive Office 365 Enterprise E1 plan and two of the Microsoft 365 Business plans include the option of an archive mailbox, with a 50 GB initial and maximum size to complement the user's primary 50 GB mailbox. The archive mailbox capability must be established by an administrator using the Exchange Admin Center or PowerShell. The Office 365 and Microsoft 365 plans above do not include capabilities for eDiscovery or legal hold, and rules-based application of retention policies is not supported.

Microsoft previously called this option In-Place Archiving in Office 365.

OPTION 4: ARCHIVE TO AN ARCHIVE MAILBOX USING EXCHANGE ONLINE ARCHIVING

Exchange Online Archiving (EOA) is positioned as Microsoft's enterprise-class email archiving solution. EOA enables users to copy or move email content between their primary mailbox and their archive mailbox, and administrators can establish both archive and retention policies to move, manage, retain, and delete email contents across the primary and archive mailboxes. EOA offers the same basic archiving capabilities as Option 3 above but increases the archive mailbox size to 100 GB initially, with the option of automatically increasing archive storage per user to a maximum of 1.5 TB.[6] EOA must be established by an administrator, and retention policies must be used to avoid ad hoc deletion of email messages by users. Administrators can enable and disable archive mailboxes using the Exchange Admin Center or PowerShell.

EOA must be established by an administrator, and retention policies must be used to avoid ad hoc deletion of email messages by users.

Whether a user has access to Exchange Online Archiving or not is dependent on the plan they are assigned. It is bundled with Office 365 and Microsoft 365 plans that include Exchange Online Plan 2 or can be separately licensed for plans that only include Exchange Online Plan 1. The Office 365 Enterprise and Microsoft 365 Enterprise plans that include Exchange Online Plan 2 also feature capabilities for eDiscovery, legal hold, and retention. Users assigned the Microsoft 365 Business Premium plan are excluded from eDiscovery searches, holds, and exports.

Microsoft's eDiscovery tools work seamlessly with both a user's primary and archive mailboxes, and legal holds can be put in place on responsive content. Given the architectural design of in-place archiving and retention policies, however, eDiscovery can only ever find content that has been pre-selected for retention. Unless everything is kept by policy—and nothing can be deleted by an ad hoc user action—the corpus of data available for eDiscovery searches will be incomplete.

There are certain limitations to be aware of with EOA:

- **Transport rules, journaling, and auto-forwarding not allowed**
  EOA is positioned as a per-user archiving solution for their email only. EOA does not permit the use of transport rules, journaling, or auto-forwarding to move content into a user's EOA archive.[7] These approaches also cannot be used with other mail-enabled applications for the purpose of creating an immutable archive.
- **Only supports Microsoft**
  EOA is positioned for exclusive use with Microsoft 365 and the latest versions of Microsoft Exchange Server. It does not offer platform independence or support multiple email platforms, meaning that organizations also using other cloud-based email services (e.g., Google Workspace) or on-premises email servers (e.g., MDaemon, IceWarp, or IMAP4 and POP3 email servers) cannot use EOA as an email archive.
- **Archive mailboxes can be turned off … and irretrievably deleted**
  If an administrator disables a user's archive mailbox in the Exchange Admin Center or by PowerShell, it will be permanently deleted after 30 days. If the administrator reactivates a user's archive mailbox within 30 days, the connection with the previous archive mailbox will be restored. If this happens after more than 30 days, a new and empty archive mailbox will be instantiated for the user.[8] When an easy configuration change is all it takes to delete content that should have been archived, the business and compliance risks to organizations are significant.

Exchange Online Archiving is for exclusive use with Microsoft 365—it does not offer platform independence or support multiple email platforms.

COMPARISON OF MICROSOFT'S OPTIONS FOR ARCHIVING

Figure 3 summarizes the capabilities of Microsoft's archiving options in Microsoft 365.

Figure 3
Comparison of Options for Archiving Email in Microsoft 365

Archiving option	**Archive to PST (option 1)**	**Archive Folder (option 2)**	**Archive Mailbox (option 3)**			**Exchange Online Archiving (option 4)**		
Plan assigned to the individual	**Any plan**	**Any plan**	**Microsoft 365 Business Basic and Standard**	**Office 365 Enterprise E1**	**Office 365 Enterprise F3**	**Microsoft 365 Business Premium**	**Microsoft 365 Enterprise E3 or E5**	**Office 365 Enterprise E3 or E5**
Maximum mailbox size	Not applicable	Not applicable	50 GB	50 GB	2 GB	50 GB	100 GB	100 GB
Archive mailbox	Not applicable	Not applicable	50 GB	50 GB	Not available	100 GB	100 GB	100 GB
Auto-expanding archiving	Not applicable	Not applicable	No	No	No	Yes, to 1.5 TB	Yes, to 1.5 TB	Yes, to 1.5 TB
Content indexing and search	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
eDiscovery, including hold and export	No	Depends on the plan	No	No	No	No	Yes	Yes
Litigation hold to meet legal requirements	No	Depends on the plan	No	No	No	Yes	Yes	Yes
Retention labels	No	Depends on the plan	No	Manual only	Manual only	Manual only	E3 (manual only) vs E5 (manual and rules-based)	E3 (manual only) vs E5 (manual and rules-based)
Archives email from non-Microsoft sources	No	No	No	No	No	No	No[9]	No[10]
Provides platform independence	No	No	No	No	No	No	No	No

Source: Osterman Research (2023)

Limitations in the Native Archiving Options in Microsoft 365

Microsoft's email "archive" in Microsoft 365 is called by the same name as true email archiving solutions, but the terminology used by Microsoft obfuscates the reality. The two types of solutions are not the same, and the native archiving options in Microsoft 365 are hampered by several important limitations. Decision makers must ensure their organization can abide with the differences and downsides.

THE ARCHIVE IS NOT INDEPENDENT

Archived data is held in place by virtue of retention policies, meaning that it exists on the Microsoft tenant along with all other Microsoft 365 data in the tenant. Problems like ransomware, account takeovers, retention policy failures, and service outages affect all data in Microsoft 365, including email archives. Attempting to move from Microsoft 365 to another solution (e.g., Google Workspace) or to a different tenant—a situation that organizations are continually exposed to with merger and acquisition activity—comes with a high degree of technical challenge to ensure all current and archived data, inclusive of active legal holds, are moved without compromising chain of custody.

In contrast, a third-party email archiving solution is not tied to Microsoft 365, and thus is fully independent with no vendor lock-in to Microsoft. Using a third-party archive provides the flexibility for the organization to move to another email solution at any point with no effect on the archive, and likewise to migrate to a new Microsoft 365 tenant without the technical overhead, elongated business disruption, and compliance and legal risk.

A third-party email archiving solution is not tied to Microsoft 365, and thus is fully independent with no vendor lock-in to Microsoft.

COMPLEXITY DRIVES ELEVATED DATA RISK

True email archiving solutions collect a full history of all email messages sent and received by an organization. This is normally accomplished by journaling of email traffic, which has a long history and requires only a one-time setting to establish. The archive provides a physically separate repository of email messages to meet business, legal, supervisory, and regulatory requirements. This separate repository is completely different from the day-to-day messaging system used by employees to send and receive email.

The native archiving approaches in Microsoft 365 do not use journaling. Given the in-place ethos, they rely on a coordinated approach covering one or more mailboxes per user, retention policies, and often Messaging Records Management. To achieve the same outcome in Microsoft 365 as with a journaling-based email archive, all these approaches must be used correctly, consistently, and without error. To always capture a full complement of email messages, which journaling allows, every user must also be on full legal hold in perpetuity. This represents a very heavy-handed approach to archiving email.

RETENTION POLICIES DO NOT PROTECT AGAINST ADMINISTRATOR ERROR

Retention policies in Microsoft 365 are the key mechanism for ensuring email messages are retained and not deleted. However, retention policies have failed organizations before, because they are not immune to error by IT administrators. For example, editing retention policies is the approach recommended by Microsoft for removing coverage for departed employees so that their Exchange mailbox can be deleted, instead of being converted to an inactive mailbox. But things have gone wrong when policies are edited. For example, an administrator at KPMG made a mistake when updating a retention policy for personal chat in Microsoft Teams (which is stored in the user's Exchange mailbox), which resulted in the unintentional but permanent deletion of retained chat histories for 145,000 users. If an error that simple in Microsoft 365 can permanently erase data that was supposed to be retained, organizations relying on Microsoft 365 face a continual and significant risk of non-compliance due to Microsoft's insistence that a separate and secondary archive is not required.

RETENTION POLICIES DO NOT PROTECT AGAINST ROGUE ADMINISTRATORS OR MALICIOUS BAD ACTORS

Retention policies do not offer protection against rogue administrators who maliciously delete data by modifying retention policies, or against malicious bad actors, such as hackers, who might disable these policies. Microsoft 365 enables the use of the Preservation Lock capability to prevent malicious users and hackers from modifying or disabling retention policies. However, the downside is that a Preservation Lock cannot be undone, which has two important implications:[10]

- If the storage allocation for an account gets full, additional storage will have to be purchased given that data under lock cannot be deleted.
- If, under a privacy regulation like the GDPR or CCPA/CPRA, a data subject requests their data to be deleted and there is no obligation for the data controller or processor to retain that data, or you no longer have a legal basis to keep the data, the data under lock cannot be deleted in compliance with the privacy regulation. This could lead to a compliance violation.

Organizations relying on Microsoft 365 face a continual and significant risk of non-compliance due to Microsoft's insistence that a separate and secondary archive is not required.

RETENTION POLICIES RESULT IN A SIGNIFICANT INCREASE IN STORAGE

The use of retention policies to retain content in a mailbox counts against the storage allocation for each user's primary and archive mailbox in Exchange Online. This leads to significant increases in storage volumes compared to the approach taken by third-party email archiving solutions.

Microsoft's approach does not optimize the storage volume across multiple users by using single-instance storage, as is done in third-party email archiving solutions. Organizations using third-party email archiving solutions are able to reduce overall storage requirements on the email server by securely archiving content to a secondary archive, applying single-instance storage, and deleting the original from the email server.

AUDIT RECORDS ARE ONLY STORED FOR A LIMITED DURATION

Audit records for mailbox activities are created by default in Microsoft 365. They capture events such as when a user reads or accesses a message in their mailbox, deletes a message, or purges an email from their mailbox (i.e., a "hard delete" which permanently deletes a message). Access to audit records is critical for

Microsoft 365 given its in-place ethos, because without auditing, a user could delete messages to cover their tracks.

However, records in the audit log are only stored for a maximum of 90 days for users without an E5 (Office 365 or Microsoft 365) license, and for a default of one year for users that do have an E5 license assigned to them.[11] The duration of storing audit records is dictated by the license assigned to every user individually; it is not an organization-wide setting. In other words, to have the ability to retain audit records for a year or longer, every user in the organization must have one of the higher-priced E5 (or equivalent academic or government) or add-on licenses assigned to them. Even if audit records are stored for a year, however, an internal investigation that is looking for malicious mailbox activities after three years will fail to find the requisite evidence.

HEIGHTENED CYBERSECURITY RISK AND BREACH FOOTPRINT

Microsoft offers 50-GB and 100-GB mailboxes to licensed users of Microsoft 365, along with up to 1.5 TB of additional email storage when the user's primary mailbox is full or nearing quota. This represents a massive amount of data that is readily available across the user's mailboxes, accessible through the user's credentials. With so many organizations using Microsoft 365, and so much data accessible through the in-place ethos, Microsoft 365 is a very attractive target for cyberthreat actors. All it takes is for credentials to be compromised through phishing, credential stuffing, or some other type of attack for threat actors to gain access to a massive collection of data across the user's mailbox and associated archives. The breach footprint is significant.

With so many organizations using Microsoft 365, and so much data accessible through the in-place ethos, Microsoft 365 is a very attractive target for cyberthreat actors.

With third-party email archiving solutions that capture a full email record in a secondary system, the size of the user's mailbox can be proactively managed downward, curtailing the data breach footprint.

PROTECTION AGAINST ACCIDENTAL AND INTENTIONAL DELETION

Microsoft 365 includes the ability to recover accidentally or intentionally deleted content in a user's primary and archive mailboxes, although there is a time-limited window of opportunity for doing so. Content that has been deleted by a user is placed into the Recycle Bin (aka the Deleted Items folder) and is available for a default of 30 days. If it has not been emptied, it's a simple matter to recover this content from the Recycle Bin by dragging it back out to the desktop or a folder. If discarded content is more than 30 days old, it will still be recoverable from the Recoverable Items folder for a default of 14 days, meaning that accidentally deleted content is available for a maximum of 44 days by default.[12] Since "archive" mailboxes in Microsoft 365 are only about storage (unless retention policies are used), users can delete emails from their archive at will.

There are several important limitations to consider in the context of accidental deletion protection:

- If a user purges their Recycle Bin or the Recoverable Items folder, content will not be recoverable.
- Content can be recovered only to the original user and is not accessible by others unless it is first recovered and then transferred to someone else.
- Content in the Recycle Bin counts as part of each user's storage quota.

If organizations want to use Microsoft's email archiving solution and have policy-based protection against accidental and intentional deletion, either retention policies or a litigation hold must be used. Configuring retention policies and retention labels is an involved and complicated process—and must be completed very early in the lifecycle of using Exchange so that all email is captured and retained.[13] A litigation hold can also be implemented that will take precedence over retention policies.[14] However, litigation holds cannot hold data retroactively and will not protect data for any content that has been altered or deleted prior to the implementation of the hold.

U.S. CLOUD ACT GIVES THE U.S. GOVERNMENT ACCESS TO ANY USER'S DATA, EVEN IN EUROPE

The U.S. CLOUD Act of 2018 enables the United States government and its agencies to access any data stored anywhere in the world on servers belonging to U.S. companies. This includes data in Microsoft 365 for organizations not doing any business in the United States, and data on users who are not U.S. citizens.

European authorities have not taken kindly to the provisions in the U.S. CLOUD Act since it conflicts with the provisions of GDPR. For organizations that want to continue to use Microsoft 365 for communication and collaboration, buying into the in-place archiving approach creates an ever-expanding collection of email data that can be accessed under the U.S. CLOUD Act. If the data is in Microsoft 365, the U.S. government and its agencies have mechanisms for gaining access to it.

The U.S. CLOUD Act does not grant access to data that is stored in data systems that were created by non-U.S. companies. Data in email archiving solutions built by European companies, for example, is safe from the reaches of the U.S. government and its agencies.

German data protection authorities continue to assess Microsoft 365 as having multiple significant shortcomings against the GDPR.

SIGNIFICANT DOUBT ON GDPR COMPLIANCE IN MICROSOFT 365

As of late 2022, German data protection authorities continue to assess Microsoft 365 as having multiple significant shortcomings against the GDPR—based on a two-year investigation into multiple data privacy concerns.[15] One result has been to ban educational institutions in Germany from using Microsoft 365,[16] and to raise concerns about its use by other public sector organizations. The various data protection authorities in Germany concluded that the lack of transparency regarding the processing of personal data by Microsoft for its own purposes means Microsoft 365 is not operated in compliance with GDPR, even in light of Microsoft's September 2022 data protection addendum.[17] Microsoft, obviously, disagrees with the characterization, and the differences between the two parties remain unsolved.[18]

Organizations subject to GDPR that embrace Microsoft 365 for long-term storage of email archives need to be aware that as of early 2023, significant areas of dispute on GDPR compliance remain between European data processing authorities and Microsoft. If continued non-compliance of Microsoft 365 remains, organizations in Europe subject to GDPR may be forced to find alternative email, collaboration, and productivity tools. This potential outcome highlights the risk of using email archiving and retention policies in Microsoft 365 versus using a third-party email archiving solution. The latter enables long-term storage and processing that is already GDPR compliant by design and enables easier migration to another email solution should that be required for GDPR compliance.

DATA RESIDENCY CHALLENGES

Organizations using a third-party archiving solution have absolute certainty on where their data is stored. Since the organization has full control over server and data center locations, the choice of managed service providers with data residency guarantees, and the storage location of backup media, they achieve certainty in complying with internal policies and external regulations on data residency.

It's not that simple with Microsoft 365. Organizations using Microsoft 365 only have assurances as to where their data is stored, which is a much lower standard than certainty. Unpicking what is and isn't done in Microsoft 365 from a data residency viewpoint is multi-faceted, and includes:

- **The original tenant architecture was "one and done"**
  From the beginning of Microsoft 365, the design of the tenant architecture was that each organization used one and only one tenant, homed in one geographical region, and to which all out-of-region traffic would route for access to the organization's data. This design works perfectly for organizations that are solely active in one geographical region but can cause significant data sovereignty and data residency challenges for multi-national and cross-regional organizations. The sole tenant location for the organization is set when the organization first signs up for Microsoft 365, and even then, some content types in Microsoft 365 have historically only been served out of the North American region, regardless of the organization's master region, although Microsoft is slowly changing this over time for most (not all) data types.
- **Multi-Geo allows splitting a tenant into logical regions**
  Microsoft's Multi-Geo add-on enables an organization with users in multiple geographical regions to split their tenant across multiple logical regions—with a primary region and one or more satellite regions. Users can be assigned to satellite regions and have their primary and archive mailbox reside in the assigned satellite region,[19] along with data for other Microsoft 365 workloads which are beyond the scope of this white paper. Multi-Geo is targeted at larger and more complex organizations and carries an additional per-user price tag. Multi-Geo has been enabled by Microsoft's build-out of local data centers in more countries, including Germany.[20]
- **Advanced Data Residency for operating workloads and storing data in specifically defined locations**
  The Advanced Data Residency add-on for enterprise customers of Microsoft 365 is designed to address requirements for comprehensive data residency.[21] It ensures Microsoft 365 workloads are operated in specifically defined locations, as well as storing customer data in defined locations. The Advanced Data Residency add-on incurs an additional per-user fee for all licensed users (i.e., 100% of licensed users in the tenant). Advanced Data Residency was initially released in November 2022,[22] hence it is a new offering and how subsequent versions will change remains to be seen.
- **EU Data Boundary for the Microsoft Cloud**
  Microsoft's latest data residency commitment for Europe is called the EU Data Boundary, and applies to Azure, Microsoft 365, and Dynamics 365.[23] It is a commitment to store and process more personal data in Europe and limit the data being transferred to the United States.

What remains unclear, however, is the degree to which these new approaches resolve the data residency issue. With each new add-on offering, Microsoft repeats the claim that it has addressed data residency, calling into question the validity of all previous assertions.

Microsoft keeps adding new options in Microsoft 365 to solve the data residency challenge, despite claiming it has previously addressed all the issues.

LACK OF LEGAL CERTAINTY OVER DATA TRANSFERS BETWEEN EUROPE AND THE UNITED STATES

Two previous legal frameworks covering the transfer of data between the European Union and the United States have been struck down by the Court of Justice of the European Union (CJEU):

- **Safe Harbor struck down in October 2015**
  The Safe Harbor framework enabled the exchange of personal data for commercial purposes between the European Union and the United States, but after revelations of surreptitious access to such data by the U.S. National Security Agency (NSA) and other similar agencies, it was ruled invalid by the CJEU in October 2015.
- **EU-U.S. Privacy Shield struck down in July 2020**
  After U.S. privacy laws received criticism from European privacy advocates for not providing the same level of privacy protection as those in the European Union and not satisfying the requirements of the GDPR, the CJEU struck down the revised Privacy Shield in July 2020. The dissolution of Privacy Shield has a significant impact, since around 5,000 companies in the United States and 250 companies in Europe were enrolled in the agreement.[24] What this means for customers that must transfer personal data on residents of the European Union to the U.S. is that they can no longer do so under the protection of Privacy Shield and must find other ways to transfer data. While this can still be accomplished, the process is more cumbersome, potentially slower, and often more expensive.

Without the protections of the Privacy Shield, one alternative has been the use of Standard Contractual Clauses (SCCs), although reliance on these is not a panacea. SCCs may be more difficult because the European Court of Justice has required data protection authorities in the European Union to scrutinize these transfers more carefully and block them if needed. Another alternative has been Binding Corporate Rules, but these are difficult to implement and thus an unreasonable burden for smaller organizations. Without the protection of the Privacy Shield, organizations have had to rely on potentially risky SCCs or find alternative ways of transferring data.

A legal resolution in 2023 is looking increasingly likely (rated as a 70% to 80% chance).[25] The new EU-U.S. Data Privacy Framework (originally called the Trans-Atlantic Data Privacy Framework) was announced in March 2022.[26] Following an Executive Order by President Biden in October 2022 committing to several significant safeguards to address the reasons the Privacy Shield was invalidated,[27] the European Commission ruled in December 2022 that the new framework meets European requirements.[28] This is only a draft decision, however, as several further European groups must ratify the framework before it is fully embraced. It remains to be seen how or if European privacy advocates will challenge the new framework.

While the new EU-U.S. Data Privacy Framework is expected to be ratified in 2023, it remains to be seen how or if European privacy advocates will challenge the new framework.

In summary, issues pertaining to data residency and data transfer for Microsoft 365 are a complex and evolving affair, with multiple moving parts as different commercial, government, and regulatory organizations jockey for position. How long it takes to find a data residency and data transfer approach that works for all parties—if this ever happens—remains to be seen. Organizations that need immediate certainty should tread carefully when adopting Microsoft 365.

Recommendations and Next Steps

Osterman Research recommends SMB decision makers to take several steps to evaluate their needs for email archiving and which archiving solution to implement.

STEP 1. DEFINE YOUR REASONS AND DRIVERS FOR EMAIL ARCHIVING

Determine why email archiving is important for your organization. IT managers and others charged with making decisions about email archiving and Microsoft 365 should consult with their legal, compliance and/or Data Privacy Officer to determine wider legal, compliance, and business requirements beyond what is important to IT. Making this determination is likely to include the following core ideas:

- **Understand your need to archive email**
  Many organizations do not yet appreciate the importance of properly archiving emails and attachments, and this issue is not limited to SMBs. Many large enterprises do not archive their emails and attachments. As discussed in this paper, a failure to archive email and attachments will prevent organizations from satisfying their legal, regulatory, and other obligations to find and produce data when needed. The consequences of being unable to do so include fines, sanctions, loss of corporate reputation, and other serious problems that almost always are more expensive than an archiving solution.
- **Determine your risk tolerance for GDPR compliance**
  German data protection authorities continue to challenge GDPR compliance in Microsoft 365. Continued machinations between German and wider European data protection agencies and Microsoft is expected. Can you tolerate the uncertainty, or do you want to know where you stand immediately? Significant issues remain in the areas of undeclared data processing, data residency, and data transfers out of the European Union.

Why is email archiving important for your organization?

STEP 2. DETERMINE THE IMPORTANCE OF KEY ATTRIBUTES OF EMAIL ARCHIVING SOLUTIONS

True email archiving solutions have several common attributes. These include:

- **Certainty of authentic and unchanged email messages**
  A true email archiving solution enables organizations to maintain authentic copies of emails, and hence meet legal, regulatory, and best practice obligations. For example, the ability to retain all relevant business records means there are no holes in the data record that provides a complete picture of a company's operations. Since all emails are accounted for in their original form, there are no nasty surprises when facing legal and regulatory demands. Employees who have access to their old emails in the archive do not need to spend time recreating content—which would negatively affect productivity.
- **Create an independent copy of email in a secondary location**
  The "3-2-1 rule" is a well-accepted best practice that dictates that an organization should retain three copies of its data: two of them locally and one that is remote and separate from the primary system that created and stores the data. For example, satisfying this best practice can be achieved by having a copy of email and attachments on the email server, a second copy in email backup and email archiving solutions, and the backups and archived content stored in a separate location (either on-premises or in the cloud). Solutions

such as Microsoft 365 that use the platform itself to provide data protection violate the 3-2-1 rule.

- **Self-service access to email archives**
  The ability for end users to search for and find their own emails in an archive alleviates the burden on IT staff members. The ability makes employees more efficient because they gain access to their emails and files more quickly. The result is a win for both IT and employees, ensuring that information is as accessible as possible with a minimum of effort.
- **Future-proof the archive and ensure its portability**
  An email archiving solution should future-proof the organization from lock-in to a particular email platform. Archiving solutions that are independent of the email platform enable an organization to move fluidly to new email platforms as the market changes—and in response to merger and acquisition activity—and to move to a new email archiving solution when required. It is important to provide as much flexibility as possible in this area.
- **Integrate with multiple email platforms to offer a unified archive**
  Organizations that operate multiple email platforms, such as Microsoft 365, Google Workspace, and on-premises email servers (e.g., MDaemon, IceWarp) need to archive email for all platforms. Using native capabilities in these platforms creates data siloes that are more difficult to manage, administer, and search over time. The use of a unified email archiving solution that accommodates all email platforms eliminates the need for separate and disjointed solutions. More importantly, a unified approach greatly reduces IT administrative requirements and streamlines ongoing legal, regulatory, and eDiscovery processes for searching and producing information.
- **Take data protection regulations into account**
  True email archiving solutions take data protection regulations into account so that they can meet the requirements of applicable regulations. For example, email archiving solutions created within the European Union by European vendors have a much higher alignment with GDPR by design, since there is no clash of data protection regimes as is evident with vendors from the United States. While vendors in other jurisdictions are taking steps to address GDPR and other emerging data privacy regulations in their own jurisdictions, European vendors have the advantage.

Email archiving solutions created within the European Union by European vendors have a much higher alignment with GDPR by design, since there is no clash of data protection regimes.

STEP 3. EVALUATE THE ADVANTAGES OF USING THIRD-PARTY TOOLS

Third-party email archiving solutions offer several advantages over the native offerings in Microsoft 365. These include:

- **Independent archive**
  A third-party email archiving solution offers the advantage of creating an archive independent of the Microsoft 365 platform, which enacts the 3-2-1 rule. This is particularly important when using a cloud service like Microsoft 365, since the primary infrastructure supporting email should not be the same one supporting email archiving.
- **Support for multiple email platforms in a unified archive**
  The use of a third-party email archiving solution delivers the advantage of archiving content from non-Microsoft email platforms within a unified archive. While multiple archiving solutions can be maintained, this adds to the cost and complication of retaining business records. Using a single archive reduces the number of siloes that IT must maintain and that must be searched.

- **Shared email archive and group access to archived content**
  Third-party email archiving solutions support new use cases for accessing email content, such as shared and group access to email archives—subject to data protection and data privacy requirements. Microsoft 365 does not provide this option, because Exchange Online Archiving is designed for only a single user.[29]
- **Wider indexing support**
  Third-party email archiving solutions often include the ability to index a greater number of file types, which leads to easier search and retrieval of content.
- **Deletion prevention**
  Third-party email archiving solutions prevent users from deleting content from their own archive. This is a "by design and by default" capability, removing the need to configure and maintain retention policies.
- **Deduplication to optimize storage and search**
  Many third-party archiving solutions will enable deduplication, which can significantly reduce storage requirements and speed searching.

STEP 4. DO A THOROUGH COST ANALYSIS

Do a thorough cost analysis to determine the difference between what is offered in Microsoft 365 and via third-party email archiving solutions. Areas of cost to examine include:

- **Administering the email archiving solution versus configuring retention policies and litigation holds**
  If a third-party email archiving solution is selected, configuration and administration is required. If Microsoft 365 for email archiving is pursued, ensuring the correct mix of retention policies and/or litigation holds will be essential. It is likely that the annual time and cost to administer the email archiving solution is less than the Microsoft 365 alternative.
- **Changing the mix of Microsoft 365 plans**
  The full Exchange Online Archiving service requires licensing the most expensive Office 365 and Microsoft 365 Enterprise plans for every user. By using a third-party archiving solution, organizations can subscribe to less expensive plans for some users, reducing the total cost of ownership for both Microsoft 365 and overall communication and collaboration capabilities.
- **Paying the additional licensing costs for data residency add-ons**
  Several add-on options are available in Microsoft 365 to increase the assurance of where data is stored. If strict data residency requirements apply to your organization, determine the added cost for embracing these add-ons.

The use of third-party archiving solutions can enable organizations to deploy less expensive Microsoft 365 plans for some users, reducing the total cost of ownership.

While the use of third-party solutions in conjunction with Microsoft 365 can add a degree of complexity for IT in terms of solution and licensing management, the cost benefits of doing so almost always outweigh these additional complexities.

Summary

Microsoft 365 is a robust and capable platform for email, productivity, and collaboration, but it has various limitations in its email archiving capabilities that SMB decision makers need to consider. This puts uninformed business owners at unnecessary risk, and so these owners should seriously consider the use of third-party email archiving solutions.

About MailStore

MailStore, an OpenText company, is specialized in the development of innovative email archiving solutions for small and medium-sized businesses. With tens of thousands of customers in over 100 countries, MailStore is one of the global leaders in their field. Their products and solutions are used by small and medium-sized businesses from all sectors, as well as by public and educational institutions. Millions of private users are also using the free MailStore Home software.

MailStore's goal is to apply the best available technologies to support their customers in making efficient and sustainable use of email as one of the most valuable and comprehensive information resources of our time and to help them to meet a growing number of compliance requirements.

www.mailstore.com

sales@mailstore.com

+49 (0) 2162 502990 (Intl.)

+1 800 747 2915 (US)

[1] Microsoft, Microsoft FY22 Third Quarter Earnings Conference Call, April 2022, at https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/TranscriptFY22Q3.docx?version=52d815b6-1a9f-0c49-d0ab-5cd077ae469d

[2] Microsoft Learn, Exchange Online limits, December 2022, at https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#mailbox-storage-limits

[3] Microsoft Learn, Outlook performance issues in a Cached Exchange Mode .ost or .pst file, September 2022, at https://learn.microsoft.com/en-US/outlook/troubleshoot/performance/performance-issues-if-too-many-items-or-folders

[4] Microsoft Learn, You may experience application pauses if you have a large Outlook data file, March 2022, at https://learn.microsoft.com/en-US/outlook/troubleshoot/performance/application-pauses-if-you-have-large-data-file

[5] Microsoft Support, Archive in Outlook for Windows, December 2022, at https://support.microsoft.com/en-us/office/archive-in-outlook-for-windows-25f75777-3cdc-4c77-9783-5929c7b47028

[6] Microsoft Learn, Learn about archive mailboxes, October 2022, at https://learn.microsoft.com/en-us/microsoft-365/compliance/archive-mailboxes?view=o365-worldwide

[7] Microsoft Learn, Learn about auto-expanding archiving, December 2022, at https://learn.microsoft.com/en-us/microsoft-365/compliance/autoexpanding-archiving?view=o365-worldwide

[8] Microsoft Learn, Enable archive mailboxes for Microsoft 365, November 2022, at https://learn.microsoft.com/en-us/microsoft-365/compliance/enable-archive-mailboxes?view=o365-worldwide

[9] Using third-party data connectors, content from various non-email sources can be archived

[10] Microsoft Learn, Data immutability in Microsoft 365, September 2022, at https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-immutability?view=o365-worldwide

[11] Microsoft Learn, Search the audit log in the compliance portal, September 2022, at https://learn.microsoft.com/en-au/microsoft-365/compliance/audit-log-search?view=o365-worldwide

[12] Microsoft Learn, Recoverable Items Folder in Exchange Online, June 2022, at https://learn.microsoft.com/en-us/exchange/security-and-compliance/recoverable-items-folder/recoverable-items-folder

[13] Microsoft Learn, Learn about retention policies and retention labels, December 2022, at https://learn.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

[14] Microsoft Learn, Create a Litigation Hold, December 2022, at https://learn.microsoft.com/en-us/microsoft-365/compliance/ediscovery-create-a-litigation-hold?view=o365-worldwide

[15] Natasha Lomas, Microsoft 365 faces darkening GDPR compliance clouds after German report, November 2022, at https://techcrunch.com/2022/11/28/microsoft-365-faces-darkening-gdpr-compliance-clouds-after-german-report/

[16] Vuk Mujovic, Germany Forces a Microsoft 365 Ban Due to Privacy Concerns, September 2022, at https://techgenix.com/microsoft-365-ban-in-germany/

[17] DSK, Definition of the conference of the independent data protection supervisory authorities of the federal and state governments, November 2022, at https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

[18] Microsoft, Our Continued Commitment to Meet and Exceed EU Data Privacy Laws, November 2022, at https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/DSK-Blog-Post_25NOV2022_ENG_FINAL.pdf

[19] Microsoft Learn, Data Residency for Exchange Online, November 2022, at https://learn.microsoft.com/en-us/microsoft-365/enterprise/m365-dr-workload-exo?source=recommendations&view=o365-worldwide

[20] Paul Lorimer, Microsoft Office 365 and Dynamics 365 now available from new German datacenter regions, February 2020, at https://www.microsoft.com/en-us/microsoft-

365/blog/2020/02/20/microsoft-office-365-dynamics-365-now-available-from-new-german-datacenter-regions/

[21] Microsoft Learn, Advanced Data Residency in Microsoft 365, November 2022, at https://learn.microsoft.com/en-us/microsoft-365/enterprise/advanced-data-residency?view=o365-worldwide

[22] Paul Lorimer, Microsoft 365 expands data residency commitments and capabilities, October 2022, at https://www.microsoft.com/en-us/microsoft-365/blog/2022/10/20/microsoft-365-expands-data-residency-commitments-and-capabilities/

[23] Microsoft, The EU Data Boundary for the Microsoft Cloud, December 2022, at https://www.microsoft.com/en-us/trust-center/privacy/european-data-boundary-eudb

[24] Dan Swinhoe, EU court invalidates Privacy Shield data transfer agreement, July 2020, at https://www.csoonline.com/article/3567061/eu-court-invalidates-privacy-shield-data-transfer-agreement.html

[25] Natasha Lomas, EU confirms draft decision on replacement US data transfer pact, December 2022, at https://techcrunch.com/2022/12/13/eu-us-data-privacy-framework-draft-decision/

[26] The White House, United States and European Commission Announce Trans-Atlantic Data Privacy Framework, March 2022, at https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

[27] The White House, President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, October 2022, at https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

[28] European Commission, COMMISSION IMPLEMENTING DECISION of XXX pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, December 2022, at https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf

[29] Microsoft Learn, Exchange Online Archiving service description, December 2022, at https://learn.microsoft.com/en-us/office365/servicedescriptions/exchange-online-archiving-service-description/exchange-online-archiving-service-description