



Guide to Email Archiving

Basics, Benefits, Business Relevance



Contents

p. 3

Foreword

p. 4

Chapter 1: Introduction to Email Archiving

p. 4 What Is Email Archiving?

p. 4 Why Do You Need an Email Archiving Solution?

p. 5 Email Archiving: A Component of Information Management

p. 6 Backups or Email Archiving? Why Not Use Both?

p. 9

Chapter 2: The Benefits

p. 9 The Benefits of Email Archiving for the IT Department and Your Business

p. 12 Why an Independent Third-Party Solution Is Worthwhile

p. 14

Chapter 3: What Types of Email Archiving Are There?

p. 14 Email Archiving in the Cloud or On-Premises?

p. 15 Mailbox Archiving vs. Journal Archiving

p. 17

Chapter 4: Compliance

p. 17 Email Archiving – A Legal Matter?

p. 18 The General Data Protection Regulation (GDPR) and Its Relevance
Beyond the European Union

p. 20

Chapter 5: Email Archiving in Practice

p. 20 How Indianapolis International Airport Benefits From Email Archiving

p. 22

Check List: Finding the Right Email Archiving Solution

Foreword

Foreword

Dear Reader,

can you remember when you sent your first email? Or how many emails you've sent and received since then? Probably not. And why should you? After all, emails have been part and parcel of our daily lives for years. It's a technical achievement we've long since taken for granted and one we're happy to entrust with important information. We use it, for example, to share important data with business colleagues or clients. Our mailbox (hopefully) keeps a record of all the data we send and receive. We've probably created our own folder structure in our email client of choice so that our mails are stored in a structured manner. Then, suddenly, the term "email archiving" pops up.

If you're reading this guide, it's likely you've already heard about email archiving and are hoping to find more detailed information on the subject. Or perhaps this document is your introduction to email archiving and you're looking for the basic facts. A big question is whether you really need to archive your emails if they're already stored safe and sound in your mailbox? The simple answer is: yes, you do!

But if that's the case, why do we hear so little about the subject, while issues such as cyber-security and the Internet of Things are mentioned all the time in IT circles? Sadly, we can't answer that question either. But we can give you several reasons why you should consider archiving your emails: we can highlight the strategic approaches you might want to follow, and we can show you how your company stands to benefit from a professional email archiving solution.

We hope this document sheds light on the relevance of email archiving in a globally networked business world.



Chapter 1: Introduction to Email Archiving

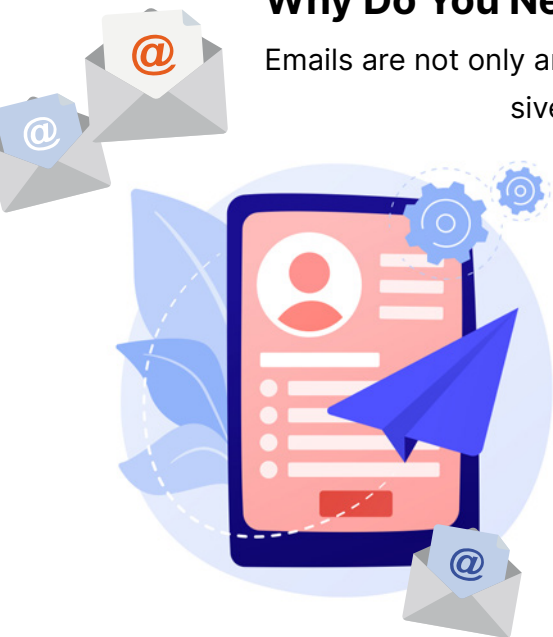
In order to recognize the potential benefits of an email archive, we need to understand how a professional email archiving solution works. In the following, we'll explain what is meant by email archiving, why using an email archiving solution is so important, and how archiving is an integral part of information management and helps your business staying cyber resilient.

What Is Email Archiving?

With email archiving, special software stores copies of all the company's emails in a central archive. The email archive supplements the existing email system, which can, of course, continue to be used as before. The IT administrator is responsible for configuring which emails are transferred automatically to the archive and when, and decides whether the emails, once archived, should be deleted automatically from the mailboxes on the mail server. If the archiving software allows users to access the whole archive (i.e. the archived emails and their file attachments) by themselves, there's no need for an administrator to be involved. Ideally, the software will be able to manage very large volumes of data efficiently.

Why Do You Need an Email Archiving Solution?

Emails are not only an important means of communication, they're also a comprehensive and valuable information resource for any company. Besides business correspondence, they can contain quotes, contracts, invoices and sales data, and even classified company information, such as data on internal work processes or financial data. Managing this information resource efficiently is an elementary component of any successful corporate strategy and one of the prime tasks of information management. As well as supporting the smooth exchange of email data, this entails ensuring that business-critical email data that are so important for the success of the company are preserved in the long-term and made constantly available.



Avoiding Data Silos, Bundling Information, and Keeping It Permanently Available

Often, the data sent in emails remain in workers' mailboxes or reside on their desktops (e.g. in PST files) rather than being stored at a central location. This gives rise to fragmented data silos harboring years of knowledge and expanding on a daily basis: they are hardly fit for purpose. A professional email archiving solution can provide help. Even though some companies still downplay the relevance of email archiving, it is doubtlessly an essential part of information management. By archiving and consolidating email data, an archiving solution not only creates a basis for the effective utilization of this information, but also supports compliance with data retention policies and privacy requirements, which are found in varying degrees in many countries around the globe.

In the following, we'll explain how email archiving can be classified within IT and how it differs from related concepts, such as data backups. We'll also demonstrate how a company stands to benefit from using an email archiving solution, and discuss the different types of email archiving and the legal necessity of having such a solution. Finally, we'll provide a list of the requirements that should be met by any professional email archiving solution.

Email Archiving: A Component of Information Management

While email archiving is about preserving data in emails, its primary objective is ensuring that email data remain available and retrievable over time so that all this data can be put to optimum use. So, email archiving is actually a **component of information management**, the aim of which is to regulate the targeted handling of information. A distinction should, therefore, be drawn between email archiving, data security, and data privacy, even though the demarcation lines can at times be blurred.

Data security is the task of protecting a company's data from the risk of corruption, compromise, and loss arising from both internal and external threats. Measures include protecting the underlying infrastructure with the aid of firewalls and antivirus programs, for example. Email archiving can make a valuable contribution to securing the data contained in emails.

On the other hand, **data privacy** has more to do with personal data and compliance with legal requirements, i.e. under which circumstances may personal data be collected, processed, or used. In this regard, an email archiving solution can provide valuable help (more on this in chapter 4, page 17).

Backups or Email Archiving? Why Not Use Both?

It's often said that if you're backing up your data, you don't really need an email archiving solution as well. This is a misconception.

While, at first glance, there may be similarities between [email archiving and a backup system](#), the two solutions actually pursue quite different objectives. Backups will never be able to do the job of a professional email archiving system, nor can an email archiving solution perform the role of a backup application. So, mindful of business continuity, these two instruments should, ideally, be used in tandem.

The Benefit of Backups

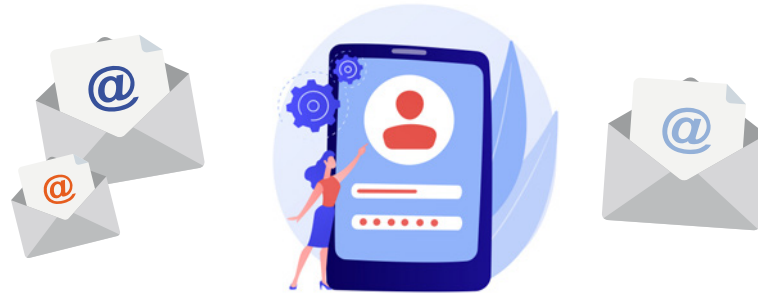
The primary purpose of a backup is to support [disaster recovery \(DR\)](#). Backups protect important data and systems (ideally, including the email archive itself) over, usually, short or medium time frames. An IT administrator can then restore these temporary, backed up data sets from external storage or the cloud. This ensures that business-critical systems and data remain available even in emergencies (e.g. after system failure or a ransomware attack). After being recovered – and, depending on the backup concept in place – the data within the backup can be overwritten respectively deleted (e.g. in the case of incremental backups), or deleted completely according to a fixed schedule if the backup file is no longer needed. Therefore, a backup provides a snapshot of the saved data at a particular point in time. All data processed since the last backup will not be retrievable following a loss event.

The Benefit of Email Archiving

The aim of email archiving is to store emails over time in a form that is faithful to the original, easy to find, and permanently available. Availability is guaranteed even if access to the mail server is interrupted, e.g. due to system failure. The integrity of an email inventory is usually achieved by archiving emails directly upon arrival at and departure from the mail server (“journal archiving” – see chapter 3, page 15).



Ideally, users can access the archive themselves and do not have to rely on the IT team to retrieve email data. However, email archiving only secures data in emails, including file attachments. Data from other sources, services, or entire systems cannot be backed up with an email archiving solution.





















Good to know: **Cyber Resilience, Business Continuity, Disaster Recovery.**




With increasing digitization and steady growth in cyber crime, companies around the world are placing ever more importance on having a sophisticated cyber resilience strategy.

The term [cyber resilience](#) encompasses all the measures and concepts introduced by a company to protect its corporate data and critical IT infrastructure before, during and after a cyber attack. It's not just about having an IT security strategy in place: you also need to plan for how corporate processes and systems must behave in the wake of a successful cyber attack or system failure, so that they can remain at a level capable of sustaining business operations. So, cyber resilience is basically a measure of how "digitally fit" a company's IT-based processes and systems are.

A key element of any cyber resilience strategy is [business continuity management](#), which comprises all the organizational, technical and personnel-related measures designed to prevent business interruption during a cyber attack, or, in the event of an emergency, to bring about a resumption of business activity as soon as possible.

An important part of business continuity management is disaster recovery, which deals with securing and restoring the necessary technical infrastructure, i.e. the business-critical data and all the IT networks and systems. Backups and email archiving provide valuable support here.

Objectives	Email backups	Email archiving
Eliminate mailbox quotas		
Eliminate PST files		
Reduce storage requirements through de-duplication and compression		
Reduce the workload of email servers and simplify backup and restore processes		
Provide complete, tamper-proof and long-term email retention		
Helps to meet compliance requirements		
Assistance with eDiscovery scenarios		
Full-text indexing of emails for fast searches		
End users: restore lost emails quickly and easily		

 Fully applies
  Applies
  Partially applies
  Applies to a lesser extent
  Doesn't apply

The ratings in this table are based on the fundamental concepts of backups and email archiving. The functions of an email archiving solution discussed here are based on the range of functions provided by MailStore Server. The functions of backup and email archiving solutions may vary, depending on the vendor.



Chapter 2: The Benefits

The use of professional email archiving software is critical in terms of a company's information management. Depending on the functionality of the archiving solution, there are other positive effects, and we will examine these in more detail below.

The Benefits of Email Archiving for the IT Department and Your Business

Archiving emails is not only an important tool when it comes to fully exploiting all the information contained in emails, it can, depending on the archiving method, have benefits for the IT department and even your entire business.

Protection Against Data Loss

Time and again, workers will delete emails – by accident, ignorance, sometimes even with malicious intent. A scenario whereby a user deletes the entire contents of a mailbox upon leaving the company is particularly serious. Emails can be manipulated by means of a ransomware attack, too. Critical data are lost in this way around the globe every day. With the aid of an email archiving solution, all future and existing inbound and outbound email traffic can be fully archived and protected against manipulation, with data loss effectively ruled out. What is more, emails distributed across local user systems (e.g. [PST files](#)) can be transferred to the central archive, too.

Support With Business Continuity

In most cases, failure of the IT infrastructure and the unavailability of business-critical data will disrupt business processes. As part of a business continuity strategy, backups can be used to restore important systems and data, such as email servers, along with all the mail data they contain. However, recovery can take several hours or even days. In the worst case, the company will not be able to access business-critical information contained in emails during the downtime. An independent archive can eliminate this problem. If the email server fails or data are lost, all archived emails will ideally remain available for any search and recovery operation. Business-critical data will remain permanently available and business activity can be continued without interruption.

Help With Legal Compliance

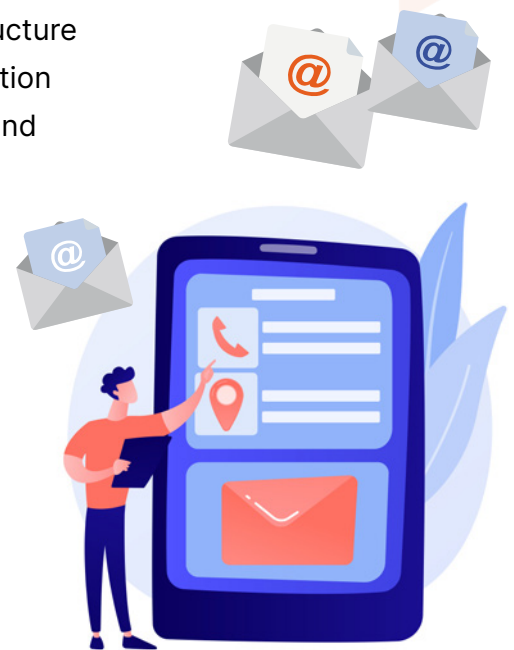
Depending on the country and the sector of industry, the processing of email data can be subject to legal requirements, e.g. where data must be retained for use as evidence and information for audits, legal disputes, or the preparation of annual financial statements and tax returns. And we're not only talking about areas such as finance, health-care, law, or education in which sensitive data are increasingly processed, but also in the majority of companies. Besides data capture, the term data processing relates to aspects of data storage, availability, usage, provision, modification, deletion and transmission. In many countries, the need for data privacy is increasingly coming to the fore. The best-known examples of privacy legislation are the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR), which not only applies within the EU, but must be observed also by companies based outside the EU that process personal data of EU citizens. For most companies, therefore, it makes sense to use an email archiving solution that is capable of archiving all relevant emails and file attachments completely and in a form that is tamper-proof and permanently available.

Increase Productivity in Everyday Business

If a company can access its entire email stocks quickly and comprehensively, this can often augment staff productivity. Onerous searches for information in ancient data silos and extending over many local user systems become a thing of the past. The positive effect can be further enhanced if the email archiving solution is capable of mapping a user's customary folder structure to the archive, and also provides a self-service function for users to access the archive independently and find and restore emails via full-text searches. Regular archiving of emails can also help to reduce the load on mailboxes, avoid issues with mailbox quotas, and boost the performance of the mail client.

Reduction in IT Cost and Effort

Email archiving can help cut the cost of managing emails, including the associated IT effort involved. Storage requirements and, thus, mailbox sizes can often be reduced significantly by



swapping out content from the mail server. And if users can access the email archive autonomously, IT personnel are spared the onerous task of restoring specific emails from backups or email servers in response to a user request. IT experts can invest their new-found capacity in more important projects.

Support With Migration Projects

Consolidating email that has been backed up decentrally, and fully archiving all emails make it easier for an IT department to migrate to another email platform, for example, in the case of a change of email provider or in-house email server. Since all emails are stored in the archive, there's no need to move emails that are still on the old system across to the new platform. The new email system thus remains free of the clutter of old emails. If required, historical emails can be accessed directly via the archive.

Help With eDiscovery

A complete, audit-proof email archive equipped with a [comprehensive search function](#) is not only useful when it comes to collecting information for internal company reporting, it can also be an invaluable aid in eDiscovery scenarios where emails are required as evidence in court in the event of a legal dispute. External auditors can also benefit from the search function if they are given access privileges to the archive.

Fast ROI

Using an archiving solution for emails reduces the workload on the IT department, can significantly cut storage costs, and improve staff productivity. As a rule, the initial cost of an email archiving solution quickly pays for itself. And a pleasing side-effect is that companies can protect themselves against the financial risk of data loss or legal breaches.



Why an Independent Third-Party Solution Is Worthwhile

Today, many companies rely on the collaboration and productivity suites of popular providers such as Microsoft (Microsoft 365) and Google (Google Workspace). The services they contain, such as the email platform or chat and meeting programs, are provided in the cloud. Companies that use cloud services benefit from low investment costs and ease of scalability compared with on-premises systems.

Why Your Emails Are Not Automatically Secure in the Cloud

But there is a downside. Once created and saved, the data in the services remain in the cloud. If the cloud infrastructure fails, business-critical data can be lost. What many users don't realize is that it is their responsibility, not the cloud provider's, to look after their data. Indeed, major cloud providers have long since identified the challenges and risks associated with processing and storing data in the modern era, and this is why their terms and conditions transfer this responsibility to the users of their cloud services. The provider is responsible merely for furnishing and maintaining the underlying infrastructure, something that is referred to as the "[shared responsibility model](#)". This extends also to the areas of backup and archiving. ***You as a customer of a public cloud provider are responsible for your data stored in their services!***

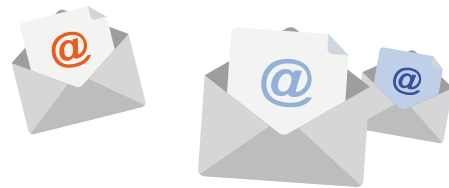
The Advantage of an Independent Third-Party Solution

Some providers do offer native archiving solutions for their email platform, but here too, it is the user who is responsible for backing up data. And if the email archive uses the same cloud platform as the email client, the email archive will also be unavailable if the cloud service fails. A platform-independent, professional email archiving solution can eliminate this risk, while providing access to archived emails even when the cloud infrastructure is down. Moreover, native archiving solutions do not normally meet the requirements of professional email archiving – another reason why users should consider setting up their own professional email archive.



The 3-2-1 Rule – Keeping Independent Copies of Emails

In order to minimize the risk of data loss, what is known as the 3-2-1 rule has proven itself in practice. The 3-2-1 rule states that a company should keep three copies of its data, in our case, emails. Two of these copies should be stored locally, one on the email server and another in a local backup and archiving system. The third data set should be kept remotely, i.e. separate from the other two storage locations (e.g. in the cloud or in another company building).



Chapter 3: What Types of Email Archiving Are There?

Various strategic approaches can be taken to email archiving depending on the IT infrastructure available and the business objectives pursued. Basically, a decision must be made as to whether archiving is to take place locally within the company's own infrastructure ("on-premises"), or whether a cloud platform is to be used. Additionally, the right archiving method must be chosen based on what the company wants to achieve, with a distinction being drawn between mailbox archiving and journal archiving.

Email Archiving in the Cloud or On-Premises?

If a company wishes to run its email archiving operations in a **cloud**, it must ensure that the platform offers maximum security and availability. Because if the cloud infrastructure fails, accessing the archived data may be compromised or even become impossible. In the worst case, the archived data will be lost. Especially when using cloud-based collaboration and productivity suites such as [Microsoft 365](#) or [Google Workspace](#), it can be tempting to dispense an independent professional email archiving solution and use the comparable services of the cloud providers. Managing everything "under one roof" and being able to do without a third-party solution for email archiving sounds comfortable and practical to many companies. As mentioned earlier, however, we recommend using a professional third-party solution to archive emails, and keeping them independent from the email services in use.

With an **on-premises** solution, on the other hand, the software is operated within the company's own server environment. This approach is of interest not only to companies

that have their own IT infrastructure and own in-house mail servers, but also in cases where a company wishes to operate its mail server in the cloud (e.g. Microsoft 365) but wants to keep the archive locally available (a hybrid approach). Locally accessible email archives minimize the risk of denial-of-access or even complete data loss that can occur if the cloud services on which communications and archiving software are operated and used fail. Ideally, users will be able to access the complete email inventory via the archive during the outage and keep their business up and running.



Mailbox Archiving vs. Journal Archiving

As well as deciding whether archiving is to be operated on-premises or in the cloud, a company must define how its emails are to be archived. Essentially, there are two approaches to email archiving: [mailbox archiving and journal archiving](#), and these pursue different goals. In some cases, combining the two methods can make sense.

When ***user mailboxes are archived (mailbox archiving)***, the current folder structure and the users' full email histories are transferred to the archive. You can also transfer locally stored emails, e.g. PST files stored on desktops, to the archive. The advantage is that, rather than adapting to a new environment, workers find that their customary folder structures have been retained and mapped to the archive. In addition, deletion rules can be created to ensure that emails are automatically deleted from the mailbox after a certain length of time, once they have been successfully archived. This means that mailbox quotas can be eliminated and demands on storage capacity reduced; also, since the volume of data on the email server is reduced, backup and restore processes become faster and easier to manage. However, one risk inherent in archiving entire user mailboxes is that crucial emails can go astray if users delete or manipulate emails, or a cyber-attack occurs before archiving is completed. If the primary goal of email archiving is to maintain an archive that is always complete and faithful to the original for optimum compliance with legal and regulatory requirements, then ***journal archiving*** is the better alternative.

By archiving all inbound and outbound emails immediately even before they reach the user, your business can ensure that electronic correspondence is stored in a form that is complete, faithful to the original, tamper-proof, and permanently available. However, with the journaling method, mailbox folder structures are not mapped to the archive. If users need to find archived emails, they need a powerful search function that is easy to use and delivers the desired results quickly. It's also possible to ***combine journal archiving and mailbox archiving*** in order to benefit from the positive aspects of each method.



- **Example 1:**

In order to comply with the ever-increasing number of regulations and to avoid data loss, a company decides to implement a journaling solution. At the same time, mailbox archiving (where all mailboxes are archived) is used to ensure that personal archives have the same folder structure as on the email client. Depending on the archiving solution, and, provided that the archiving software is capable of [internally de-duplicating emails](#), this combination of methods requires only marginally more storage space.

- **Example 2:**

With the introduction of an email archiving solution, the mailbox archiving method is initially used to extract all existing emails from the mailboxes and to transfer any local emails (e.g. PST files stored on a user's desktop) to a central archive and, if necessary, delete the mails from the mailboxes and the decentral storage locations. Thereafter, all future emails are archived using the journaling method.



Chapter 4: Compliance

Companies often use “compliance” to refer to the obligation to adhere not only to existing laws, but also to internal company policies on ethics, integrity and employee behavior. In the following, we’ll explain the role email archiving plays in fulfilling certain legal obligations and email retention requirements.

Email Archiving – A Legal Matter?

As global data volumes continue to grow in the digital age, more and more laws and regulations are being introduced to regulate how data is handled and to establish a legal basis. The examples of the [General Data Protection Regulation \(GDPR\)](#) in the EU, and the [CCPA](#), [HIPAA](#), [FERPA](#), and [Federal Rules of Civil Procedure \(FRCP\)](#) laws in the US show how much importance legislators now attach to the secure handling of personal electronic data. Legal requirements on the retention of business-critical data in electronic format usually also exist, and these can vary depending on country and industry sector.

A comprehensive and well-thought-out approach to information and data management is now essential in order to meet the demands of increasing data privacy laws, retention obligations, and the resulting stricter corporate guidelines. Given that most business-critical data are sent by email or stored in mailboxes, the often-neglected subject of email archiving has suddenly taken on a new and crucial role.

Because, with the aid of an email archiving solution, business-critical data stored in emails can be retained for many years in a form that is faithful to the original and tamper-proof, then automatically and selectively deleted after a certain length of time. Such a solution can, therefore, be a key component when it comes to meeting the challenges of statutory compliance.

Depending on the laws of the land, a failure to provide technical support in implementing legal requirements, or the willful disregard of such laws can attract severe fines and penalties. And this does not only concern large companies in the public eye. Small and mid-sized businesses, too, need to get to grips with data security and accept their



own accountability for compliance with regulations and laws, regardless of whether they are in a highly regulated industry such as healthcare, education or finance, or not. In addition, a complete and tamper-proof email archive can play an important role in civil or criminal proceedings, as in many countries of the world, electronic documents are permitted as evidence in court. These include emails and their file attachments. Ideally, not only a company's own researchers but also external attorneys who, if necessary, can or will have to be granted access to the archive, will be able to gather evidence in the form of email data.

The General Data Protection Regulation (GDPR) and Its Relevance Beyond the European Union

The [European Union's General Data Protection Regulation \(GDPR\)](#) harmonizes data privacy laws in Europe, placing an emphasis on the protection of personal data. However, although the name might suggest that the regulation is applicable only within the European Union, companies based outside the EU may also have to abide by its provisions in some circumstances. Thus, non-EU companies that need to store or process the personal data of EU citizens – a common enough scenario in today's globalized world – will also be subject to the GDPR.

In different areas, therefore, companies must ensure that personal data is handled in a manner that complies with the terms of the GDPR. Breaches can attract fines of up to EUR 20 million or 4 percent of a company's total global turnover of the preceding financial year, whichever is higher. Complying with the data protection rules set down in the GDPR is a corporate-wide challenge involving numerous processes and procedures. So, email archiving tools can help businesses meet several core requirements of the EU regulation, as is the case with the following GDPR articles, for example:

Right of Access (Article 15 GDPR)

Archived emails contain personal data. With a professional email archiving solution, the contents of an email can be fully searched, extracted in a commonly used format, and then made available. This enables companies and organizations to meet their obligation to provide information.

Right to Object (Article 21 GDPR)

When a company processes personal data, it must demonstrate that it has obtained the consent of the data subject to do so. The data subject must also be able to withdraw this consent. With an email archiving solution, the consent and withdrawal of this consent, as issued in emails, as well as the resulting transaction emails – for example opt-ins of email marketing or lead management systems – are reproduced in the email archive.

Right to Erasure (Article 17 GDPR)

For a variety of reasons, individuals have the right to demand that their personal data be deleted (“the right to be forgotten”). When data is deleted, the following requirements must be met:

- Emails must be irretrievably erased
- Statutory retention periods must be safeguarded
- Database conformity must be guaranteed

With the aid of individually configurable [retention policies](#), a professional email archiving software allows you to automate the deletion of emails from an archive, i.e. including the personal data stored on the data subject. Furthermore, delete requests can be recorded by specifying the reason for the deletion as part of a manual delete procedure that is logged.

Right to Data Portability (Article 20 GDPR)

Data subjects have the right to receive personal data stored about them in a structured, commonly used and machine-readable format, and to transfer this data to another controller. Archiving solutions that allow export to common email formats such as EML, MSG, and PST takes this right to data portability into account.



Chapter 5: Email Archiving in Practice

The preceding chapters paint a more complex picture of email archiving than one might at first assume. It should also be remembered, however, that the theory covers all eventualities and options, some of which do not exist in practice or cannot be reproduced due to varying local conditions relating to the industry or the country in question. The use case of Indiana International Airport shows how email archiving can appear in practice.

How Indianapolis International Airport Benefits From Email Archiving

Indianapolis International Airport has been archiving its emails for many years. Mail-Store Server was installed in 2011, replacing another vendor's archiving solution which had been described as unreliable and complicated to run. The airport has been using the email archiving solution on a daily basis for more than ten years now; it is reliable, and provides valuable support when it comes to managing business-relevant projects.

Choosing and Deploying an Archiving Strategy

Over the years, Indianapolis International Airport had employed various **strategic approaches to email archiving**. In the beginning, they opted for mailbox archiving, a few years later switching to journal archiving (journaling).

Initially, with **mailbox archiving**, all the emails were extracted from the users' mailboxes at regular intervals and then archived. Indianapolis International Airport also defined deletion rules for all archived emails in order to reduce the strain on the mail server. This not only allowed backup and restore processes to be optimized, but also eliminated the need for mailbox quotas, which had been the reason why some employees had resorted to using PST files in the past. With the help of the email archiving solution, the decentral, error-prone PST files could be transferred to the central archive. The emails were then accessed directly from the archive.

In the meantime, Indianapolis International Airport has switched to **journal archiving**. In order to prevent data loss and ensure compliance with legal requirements on the availability and security of business-critical data, all emails are now copied straight to the archiving system the moment they arrive at or depart from the server.

Practical Search Function

However, the switch from mailbox archiving to journaling meant that the users' customary folder structures were no longer being mapped to the archive. But this wasn't a problem for the users at Indianapolis International Airport because they could rely on the email archiving solution's powerful search function to retrieve specific emails from the archive whenever necessary.

In this case, the archive is accessed either via [the add-in integrated in Outlook](#), the [Web Access functionality](#), or the installed [MailStore client](#). So far, users have not experienced any problems when running internal archive searches.

Easy Email Migration to Microsoft 365 Thanks to Email Archiving

A few years ago, Indianapolis International Airport decided to [migrate from Microsoft Exchange 2010 to Microsoft 365](#). Thanks to their email archiving solution, the process of migrating emails was greatly simplified. Instead of relocating all the mailboxes and all the emails from the previous Microsoft Exchange 2010 environment to the new email system, the emails were simply moved straight to the central archive. This meant that Microsoft 365 could be rolled out free of ballast from the historical mail inventory. If employees ever need to access historical emails or locate an old email attachment, they can do so using the above-mentioned options directly via the archive.

Takeaway

The example of Indianapolis International Airport shows that a professional email archiving solution can deliver a whole host of benefits for a company for many years, not only in the field of archiving.



Check List: Finding the Right Email Archiving Solution

In order to benefit from all the advantages email archiving has to offer, it is advisable to place corresponding requirements on the functionalities of the archiving solution. All legal, economic and technical requirements should be taken into account.

Below you will find a checklist with all relevant criteria that a professional email archiving solution should fulfill.

- Retention policies:** The archiving solution should enable administrators to define individual retention policies so that they can decide how long certain emails are retained and whether they should be deleted from the archive automatically after a certain time.
- Journal archiving:** The archiving solution should be able to archive emails the moment they are sent or received in order to prevent data from being lost and to maintain the archive's integrity. This helps to ensure legal compliance.
- Archiving existing emails:** When you roll out the new software, it should be no problem to archive current emails stored in individual mailboxes, public folders, shared mailboxes and on a user's desktop, including file attachments.
- Tamper-proof archiving:** The archiving solution should be able to protect archived data from manipulation by using encryption methods so that specific legal requirements are complied with.
- Deletion rules:** The archiving solution should have the means to delete archived emails automatically from users' mailboxes after defined periods of time.
- Self-service for the user:** Not all archiving solutions allow users to access the archive by themselves. But the workload on an IT department can be reduced significantly if the new solution allows users to work productively within the archive.
- Flexibility:** The archiving software should support all conventional email systems and archiving methods. Ideally, it should also be possible to realize customized application scenarios via an integrated API.



- Easy to install and run:** Simple installation makes it easier to get the software up and running, while intuitive handling facilitates rapid implementation of the archiving system. Having all the necessary components, e.g., database systems, integrated during setup helps save time, while reducing costs and administrative effort.
- User-friendly:** Users must be able to access archived emails as usual via Microsoft Outlook, browser, or while on the road with a tablet or smartphone.
- Certification:** For many companies, it's important that the software permits GDPR-compliant working standards and, where required, boasts appropriate certification.
- Flexible storage management:** Choosing an archiving software that uses methods such as de-duplication and compression can help reduce storage requirements by as much as 70 percent. Flexible storage management also means that fast, expensive storage media can be reserved for current emails; a good system will always transfer older, less frequently accessed emails to slower, cheaper storage.
- Fit for purpose:** Your archiving tool must be a good fit for the size and requirements of the business. For example, it is rarely the case that an SMB will need a large enterprise solution, rather software that is tailored to the small or mid-sized company in terms of functional scope and total cost of ownership (TCO).



About MailStore

MailStore, a subsidiary of OpenText, specializes in developing innovative email archiving solutions for small and mid-sized businesses. With tens of thousands of corporate customers in more than 100 countries, MailStore is a global leader in its field. MailStore products and solutions are used by small and medium-sized businesses from all sectors, as well as by public and educational institutions.

MailStore's ambition 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.

Contact your IT service provider for advice on email archiving.



Graphics: Designed by vectorjuice / Freepik