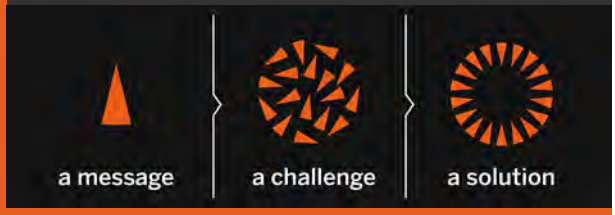
Leitfaden zur rechtssicheren E-Mail-Archivierung in der Schweiz

Stand: 08. März 2012

E-Mail-Archivierung bietet nicht nur zahlreiche technische und wirtschaftliche Vorteile, sie stellt für Unternehmen zudem eine zwingende Notwendigkeit dar. Geltende rechtliche Anforderungen können nicht ohne eine solche Lösung erfüllt werden. Leider ist gerade der rechtliche Aspekt der Archivierung sehr vielschichtig und von zahlreichen Grauzonen geprägt.

Dieser Leitfaden soll durch die wichtigsten Fragestellungen führen.



MAIL STORE™

Übersicht

Was muss archiviert werden?

- Buchungsbelege, Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lage-berichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
- die empfangenen Handels- oder Geschäftsbriefe,
- Wiedergaben der abgesandten Handels- oder Geschäftsbriefe,
- sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.

E-Mails sind im Unternehmen Teil der Geschäftskorrespondenz, für die grundsätzlich eine Aufbewahrungspflicht besteht. Im Besonderen gilt dies für alle Schreiben, durch die ein Geschäft vorbereitet, abgewickelt, abgeschlossen oder rückgängig gemacht wird. Beispiele sind Rechnungen, Aufträge, Auftragsbestätigungen, Zahlungsbelege und Verträge. Dies gilt auch dann, wenn diese per E-Mail versendet werden. Grundlage hierfür ist die Buchführungspflicht nach Art. 957 ff. OR (Obligationenrecht).

Bei mehrwertsteuerrelevanten Belegen kommt darüber hinaus die „Verordnung des EFD vom 11. Dezember 2009 über elektronische Daten und Informationen (EIDI-V)“ zum Tragen, die aber in ihren Forderungen nicht über das oben Geschilderte hinausgeht.

In der Praxis

In Anbetracht der Masse der täglich empfangenen und versendeten E-Mails ist eine Kategorisierung in archivierungspflichtige und nicht-archivierungspflichtige E-Mails fast nicht möglich. Es wird daher oft bevorzugt, einfach alle E-Mails zu archivieren. Dies kann ein Unternehmen jedoch in Konflikt mit anderen Gesetzen bringen.

Wie lange müssen E-Mails aufbewahrt werden?

Nach dem Obligationenrecht (Artikel 962) ergeben sich folgende Aufbewahrungsfristen:

- Sämtlich Geschäftsbücher, die Buchungsbelege und die Geschäftskorrespondenz müssen zehn Jahre lang aufbewahrt werden.
- Bei Korrespondenz, die sich auf Geschäfte mit Immobilien oder Grundstücken bezieht, gilt eine längere Frist von mindestens 20 Jahren (u.a. MwStG 70 Ziff. 3).

In der Praxis

Auch hier ist in Anbetracht der Masse der E-Mails eine zuverlässige Kategorisierung mit vertretbarem Aufwand kaum möglich. Oft werden aus diesem Grund alle E-Mails mindestens zehn Jahre lang aufbewahrt.

Wer trägt die Verantwortung?

Die Verantwortung für die ordnungsgemäße Umsetzung der rechtlichen Anforderungen zur Aufbewahrung von E-Mails liegt bei der Geschäftsleitung eines Unternehmens. Kommt diese ihrer Pflicht nicht nach, drohen empfindliche Strafen.

Anforderungen an eine revisionssichere E-Mail-Archivierung

Die entsprechenden Vorgaben werden in der so genannten Geschäftsbücherverordnung (GeBüV) geregelt:

- Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden. Artikel 3 spricht in diesem Zusammenhang von Integrität (Echtheit und Unverfälschbarkeit).
- Die Prozesse und die ggf. eingesetzte Software und Infrastruktur müssen lückenlos dokumentiert werden (Artikel 4) und können von einem sachverständigen Dritten je-derzeit geprüft werden.
- Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß und dauerhaft sicher (Artikel 5: „...vor schädlichen Einwirkungen geschützt“) aufbewahrt werden (Artikel 6, Verfügbarkeit). Jeder Zugriff auf das Archiv muss protokolliert werden.

Quelle: Verordnung vom 24. April 2002 über die Führung und Aufbewahrung der Geschäftsbücher (Geschäftsbücherverordnung; GeBüV)

Einen allgemeinen Leitfaden stellen zudem die Merksätze des Verbandes Organisations- und Informationssysteme e.V. zur revisionssicheren elektronischen Archivierung dar:

- Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß aufbewahrt werden.
- Die Archivierung hat vollständig zu erfolgen – kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Jedes Dokument ist zum organisatorisch frühestmöglichen Zeitpunkt zu archivieren.
- Jedes Dokument muss mit seinem Original übereinstimmen und unveränderbar archiviert werden.
- Jedes Dokument darf nur von entsprechend berechtigten Benutzern eingesehen werden.
- Jedes Dokument muss in angemessener Zeit wiedergefunden und reproduziert werden können.
- Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist vernichtet, d.h. aus dem Archiv gelöscht werden.
- Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden.
- Das gesamte organisatorische und technische Verfahren der Archivierung kann von einem Sachverständigen Dritten jederzeit geprüft werden.
- Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein.

Quelle: Verband Organisations- und Informationssysteme e.V. (VOI)

Grundsätzlich sollten alle relevanten E-Mails und deren Dateianhänge vollständig, manipulationssicher und jederzeit verfügbar aufbewahrt werden. Weiterhin sollten die Daten maschinell auswertbar sein.

Konflikte zwischen Datenschutz und E-Mail-Archivierung vermeiden

Durch die Umsetzung einer Compliance-Strategie, mit deren Hilfe die gesetzlichen Anforderungen zur Aufbewahrung von E-Mails umgesetzt werden sollen, kann ein Unternehmen unter gewissen Umständen in Konflikt mit anderen rechtlichen Vorschriften geraten.

Automatische Archivierung aller E-Mails sofort bei Ein- und Ausgang

In Anbetracht der Masse der täglich empfangenen und versendeten E-Mails ist eine Kategorisierung in archivierungspflichtige und nicht -archivierungspflichtige E-Mails in der Praxis beinahe unmöglich.

Um die Vollständigkeit der Archivierung zu gewährleisten werden häufig alle E-Mails sofort bei Ein- und Ausgang archiviert. So wird gleichzeitig möglichen Manipulationen vorgebaut, da Mitarbeiter die digitale Post vor der Archivierung weder verändern noch löschen können.

Diese Archivierungsstrategie kann jedoch in Konflikt mit den Datenschutzrichtlinien stehen. Ist den Arbeitnehmern beispielsweise die private E-Mail-Nutzung gestattet, unterliegt der Arbeitgeber als Telekommunikationsanbieter dem Bundesdatenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG).

Untersagung der privaten E-Mail-Nutzung

Zur Lösung dieses Problems kann die private E-Mail-Nutzung untersagt oder die ausschließliche Nutzung externer E-Mail-Dienste vorgeschrieben werden. Um juristisch auf der sicheren Seite zu sein, muss dies schriftlich fixiert, kontrolliert und konsequent durchgesetzt werden.

Vergleichbare Situationen in Deutschland, Österreich und der Schweiz

Die hier für Deutschland geschilderte Problematik und die aufgezeigten Lösungsansätze sind auch für Österreich und die Schweiz relevant. Allerdings besitzen die jeweils zu Grunde liegenden Gesetze und Vorschriften abweichende Bezeichnungen in den jeweiligen Ländern.

Alternative Betriebsvereinbarung?

Bisweilen wird die Auffassung vertreten, dass die private Nutzung des geschäftlichen E-Mail-Accounts und E-Mail-Archivierung dann nicht in einem Konflikt stehen, wenn die Mitarbeiter – gegebenenfalls mittels einer Betriebsvereinbarung durch den Betriebsrat – der Archivierung explizit zugestimmt haben. Allgemein betrachtet ist dies auch zutreffend, im Detail jedoch kompliziert. Denn problematisch hierbei ist, dass der Mitarbeiter auf diese Weise nur seine eigenen durch das Fernmeldegeheimnis geschützten Rechte abtreten kann. Dies gilt jedoch selbstverständlich nicht für einen eventuellen „externen Kommunikationspartner", dessen Nachrichten ja unwissentlich und unwillentlich mitgesichert würden. Da also die E-Mails von Außenstehenden archiviert würden und deren Recht auf Datenschutz verletzt, erscheint dieses Vorgehen nicht als zielführende Alternative.

Personenbezogene Inhalte dienstlicher E-Mails

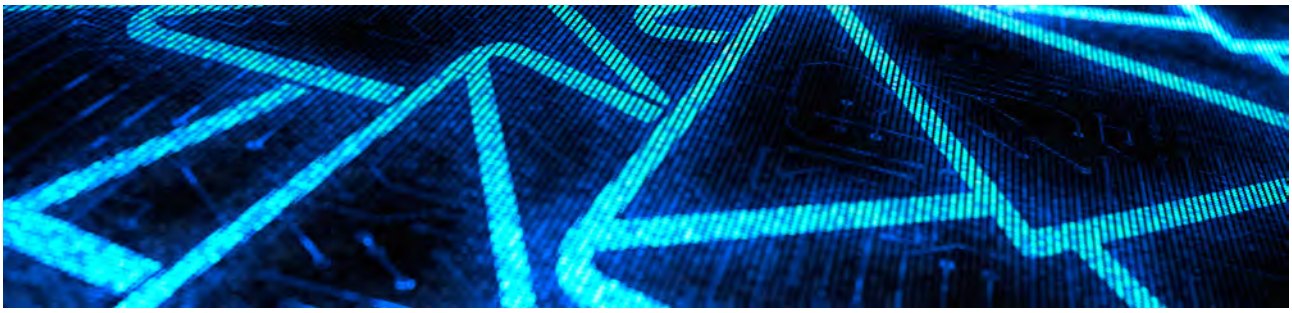
Es existieren darüber hinaus noch gewisse Unsicherheiten, selbst wenn die private Nutzung der geschäftlichen E-Mail-Accounts explizit untersagt ist: Beispielsweise können auch dienstliche E-Mails durchaus datenschutzrechtlich relevante, personenbezogene Inhalte haben. In diesem Zusammenhang wird gegen eine generelle Archivierung aller Mails beispielhaft die mögliche elektronische Post des Betriebsarztes an einen Mitarbeiter angeführt. Selbstverständlich handelt es sich dabei um vertrauliche und somit schützenswerte Inhalte.

Führende deutsche IT-Rechtler vertreten allerdings die Auffassung, dass bei einer Interessenabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 I GG i.V.m. Art.1 I GG) und dem „Schutz des eingerichteten und ausgeübten Gewerbebetriebes des Arbeitgebers" (Art. 14 I GG) letzterer obsiegt. Der Begriff der „Erforderlichkeit" (§ 32 BDSG) spielt hierbei eine wichtige Rolle. Denn aufgrund der zahlreichen Gesetze und Vorschriften besteht eben nicht nur ein Interesse, sondern geradezu die Pflicht zur Archivierung. Allerdings muss der Arbeitgeber unbedingt seiner Informationspflicht über die E-Mail-Archivierung gemäß § 4 III BDSG nachkommen und alle Mitarbeiter vor der Implementation einer entsprechenden Lösung informieren.

Best Practice Tipp

Das Verbot der privaten Nutzung betrieblicher E-Mail-Accounts ist nach Abwägung aller Möglichkeiten der beste Weg, um Konflikte zwischen Datenschutz und E-Mail-Archivierung vermeiden.

Grauzone: Spam-Filterung vor der Archivierung



Die Spam-Filterung vor der Archivierung birgt grundsätzlich das Risiko, dass archivierungspflichtige E-Mails nicht durch den Spam-Filter und somit auch nicht in das Archiv gelangen. Die Archivierung wäre somit nicht vollständig und streng genommen auch nicht rechtssicher. In der Praxis bestehen dazu drei Handlungsmöglichkeiten:

Es wird auf die Spam-Filterung vor der Archivierung verzichtet	Empfangene E-Mails werden von einer Anti-Spam-Lösung gefiltert und danach archiviert	Als Spam identifizierte E-Mails werden noch vor Annahme durch den eigenen E-Mail-Server abgewiesen
Auf diese Weise ist zwar die Vollständigkeit der Archivierung sichergestellt, jedoch geht dies mit technischen Nachteilen einher. So wird durch das extrem hohe (da ungefilterte) E-Mail-Volumen der Speicherbedarf des Archivs stark erhöht. Die Folge sind höherer Aufwand und Kosten beim Speichermanagement und bei der Datensicherung. Zudem nimmt die Qualität der Suchergebnisse bei der Archivsuche durch den hohen Spam-Anteil deutlich ab.	Auf diese Weise wird zwar der Speicherbedarf des Archivs deutlich verringert und die Qualität von Suchabfragen erhöht, jedoch kann eine vollständige Archivierung aller relevanten E-Mails nicht zu 100% sichergestellt werden. Diese E-Mails können fälschlicherweise vom Spam-Filter abgewiesen werden. Das Verfahren geht demnach mit einem gewissen rechtlichen Risiko einher.	Solange als Spam identifizierte E-Mails nicht angenommen werden, besteht auch keine Pflicht zur Verarbeitung oder zur Archivierung dieser E-Mails. Technisch gesehen darf die Annahme der E-Mail nicht mittels Statuscode 250 vom SMTP-Server „quittiert“ werden. In diesem Fall ist nicht der eigene, sondern der zustellende E-Mail-Server für die Versendung des NDR (Non-Delivery Reports) an den Absender verantwortlich.

Rechtssichere E-Mail-Archivierung mit MailStore Server

MailStore Server wird regelmäßig durch eine unabhängige Wirtschaftsprüfungsgesellschaft zertifiziert. Die Prüfung findet auf der Grundlage der Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW) "Erteilung und Verwendung von Softwarebescheinigungen" (IDW PS 880) statt und berücksichtigt alle Teilaspekte der Grundsätze ordnungsgemäßer Buchführung, welche die Archivierung betreffen.

Regelmäßige Zertifizierungen

Schweiz

- Vorschriften zur Buchführung, Aufbewahrung und Edition des schweizerischen Obligationenrechts (OR)
- Richtlinien der Treuhand Kammer bezüglich der Grundsätze ordnungsmäßiger Buchführung (Revisionshandbuch der Schweiz)
- "Richtlinien für die Ordnungsmäßigkeit des Rechnungswesens unter steuerlichen Gesichtspunkten sowie über die Aufzeichnung von Geschäftsunterlagen auf Bild- oder Datenträger und deren Aufbewahrung" der eidgenössischen Steuerverwaltung (EStV)
- Verordnung über die schweizerische Mehrwertsteuer (MWSTV) und die Wegleitung für Mehrwertsteuerpflichtige

Deutschland

- Vorschriften des Handels- und Steuerrechts über die Ordnungsmäßigkeit der Buch-führung (§§ 238 ff. und § 257 HGB sowie §§ 140 ff. AO)
- IDW Stellungnahme zur Rechnungslegung "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)"
- IDW Prüfungsstandard "Erteilung und Verwendung von Softwarebescheinigungen (IDW PS 880)"
- "Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)" der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV) sowie das dazu ergangene Begleitschreiben des Bundesministers der Finanzen vom 07.11.1995
- Schreiben des Bundesministers der Finanzen "Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)" vom 16.07.2001
- Deutsches Umsatzsteuergesetz

Österreich

- Österreichische handels- und steuerrechtliche Vorschriften (§ 189 UGB, §§ 131, 132 BAO)
- Fachgutachten des Fachsenats Datenverarbeitung der österreichischen Kammer der Wirtschaftstreuhänder (KFS DV1, Stand 11/1998)
- Österreichisches Umsatzsteuergesetz

Aufbewahrungspflichten und -fristen von Dokumenten im Gesundheitswesen

Die Aufbewahrungspflichten im Gesundheitswesen, die sich beispielsweise aus dem Sozialgesetzbuch ergeben, definieren gegenüber den handels- und steuerrechtlichen Regelungen keine zusätzlichen materiellen Anforderungen an die revisionssichere Aufbewahrung von Belegen oder Dokumenten. Dies bedeutet, dass keine weiteren technischen Anforderungen an die Informationstechnologie gestellt werden. Es erweitert sich jedoch der Kreis der aufzubewahrenden Unterlagen und Informationen. Diese sind, wie auch nach Handels- und Steuerrecht, im Einzelfall zu prüfen. Letztendlich können mit MailStore Server somit auch die Aufbewahrungspflichten (hinsichtlich E-Mails) im Gesundheitswesen technisch erfüllt werden.

Das MailStore Server-Technologiekonzept

Neben regelmäßigen Zertifizierungen sorgt ein umfassendes Technologiekonzept dafür, dass Unternehmen mit Hilfe von MailStore Server die geltenden gesetzlichen Anforderungen zuverlässig erfüllen können.

- MailStore Server ermöglicht die 100% vollständige Archivierung aller E-Mails im Unternehmen
- Archivierte E-Mails stimmen in jeder Hinsicht mit dem Original überein
- Protokollierung von Änderungen und Ereignissen über eine integrierte Auditing-Funktion im Windows-Ereignisprotokoll
- Zugriff durch Prüfer über Benutzertyp „Auditor“ möglich
- Alle E-Mails können jederzeit im Standardformat nach RFC822 aus dem Archiv heraus exportiert werden
- Bildung von SHA1-Hashwerten über die Inhalte der E-Mails
- Interne AES256-Verschlüsselung
- Kein direkter Zugriff der MailStore Client-Komponenten auf die Archivdateien
- Änderung der E-Mail-Inhalte ist weder in der grafischen Oberfläche noch programmintern vorgesehen
- Automatische Archivierung aller E-Mails sofort bei Ein- und Ausgang verhindert Manipulationen zum Zeitpunkt vor der Archivierung durch MailStore Server

Über MailStore Server

Mit MailStore Server können Unternehmen die rechtlichen, technischen und wirtschaftlichen Vorteile moderner E-Mail-Archivierung einfach und sicher für sich nutzbar machen. Dazu legt MailStore Server perfekte Kopien aller E-Mails in einem zentralen E-Mail-Archiv ab und stellt so die Sicherheit und Verfügbarkeit beliebiger Datenmengen über viele Jahre hinweg sicher.

Anwender können weiterhin über Microsoft Outlook, Web Access oder mobil über Tablets und Smartphones auf ihre E-Mails zugreifen und diese in atemberaubender Geschwindigkeit durchsuchen.

MailStore Server kombiniert eine leistungsstarke Technologie mit niedrigen Kosten und intuitiver Bedienbarkeit. Bereits heute vertrauen über 10.000 Unternehmen aller Größen und Branchen bei der E-Mail-Archivierung auf MailStore Server.

Rechtlicher Hinweis