Rechtssichere E-Mail-Archivierung

Der Leitfaden für die Schweiz

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. Besonders der rechtliche Aspekt der Archivierung ist sehr vielschichtig und von zahlreichen Grauzonen geprägt.

Dieser Leitfaden führt durch die wichtigsten Fragestellungen.

Stand: 01. Januar 2017

Übersicht der wichtigsten Fragestellungen

Was muss archiviert werden?

- Buchungsbelege, Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, 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)[1].

Bei mehrwertsteuerrelevanten Belegen kommt darüber hinaus die „Verordnung des EFD vom 11. Dezember 2009 über elektronische Daten und Informationen (ElDI-V)“[2] zum Tragen, die aber in ihren Forderungen nicht über das oben Geschilderte hinausgeht.

Archivierung von Dateianhängen

E-Mail-Anhänge müssen ebenfalls archiviert werden, sollte die E-Mail ohne diese Anlagen unverständlich oder unvollständig sein.

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 (vgl. Seite 5 „Konflikte zwischen Datenschutz und E-Mail-Archivierung vermeiden“).

Wie lange müssen E-Mails aufbewahrt werden?

Nach dem Obligationenrecht 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 Art. 70 Ziff. 3).3

[1] http://www.admin.ch/opc/de/classified-compilation/19110009/index.html
[2] http://www.admin.ch/opc/de/classified-compilation/20092054/index.html

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.

Kann eine E-Mail als Beweis genutzt werden?

Seit dem Jahre 2010 gilt die vereinheitlichte schweizerische Zivilprozessordnung. Demnach sind E-Mails und andere digitale Dokumente, nach neuesten Rechtsprechungen, unter geltendem kantonalem Zivilprozessrecht als (Computer-)Urkunden zu betrachten.

Zu beachten ist hierbei, dass dies auch ausdrücklich ohne elektronische Signatur gilt, da die Beweiseignung nicht von dieser abhängt. Soll jedoch die Beweiskraft und –dienlichkeit gegeben sein, ist eine elektronische Signatur, die gem. Art. 14 Abs. 2 Obligationenrecht (OR) der Handunterschrift gleichgestellt ist, zwingend erforderlich.

Folglich liegt die Problematik der Nutzung von E-Mails als Beweismittel nicht in der Eignung der E-Mail als Beweismittel, sondern in der Beweiskraft.

In der Praxis

Gemäß Art. 957 Abs. 4 Obligationenrecht (OR) haben die in elektronischer Form archivierten Dokumente, sofern sie die Anforderungen der Geschäftsbücherverordnung (GeBüV) erfüllen, dieselbe Beweiskraft wie solche die ohne Hilfsmittel lesbar sind.

[3] http://www.admin.ch/opc/de/classified-compilation/20081110/index.html

Anforderungen an eine revisionssichere E-Mail-Archivierung

Die entsprechenden Vorgaben werden in der Geschäftsbücherverordnung (GeBüV)[4] 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 jederzeit 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.
- Eine physische oder logische Trennung von archivierten E-Mails nach aktiven und abgeschlossenen Geschäftsvorfällen muss stets gegeben sein (Artikel 7).
- Der Zugriff auf archivierte E-Mails ist regelungs- und aufzeichnungspflichtig (Artikel 8).

Einen allgemeinen Leitfaden stellen 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.

[4] http://www.admin.ch/opc/de/classified-compilation/20001467/index.html

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 vorgebeugt, 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 Post- und Fernmeldegeheimnis.[5].

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.

Die schriftliche Fixierung kann z.B. in Richtlinien betreffend der Nutzung der firmeneigenen IT-Infrastruktur, in einer Betriebsvereinbarung, einer Einverständniserklärung der Belegschaft oder im individuellen Anstellungsvertrag erfolgen.

Ist die Zustimmung zur Archivierung durch Personalreglemente eine Alternative?

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 der Archivierung explizit zugestimmt haben. Allgemein betrachtet ist dies auch zutreffend, im Detail jedoch kompliziert. Gibt der Arbeitgeber in einer eigens dafür formuliertes Personalregelement bekannt, dass grundsätzlich alle über den dienstlichen E-Mail-Account empfangenen und versendeten E-Mails archiviert werden, schließt das folglich auch alle privaten, über diesen E-Mail-Account versendeten E-Mails mit ein. Dies

[5] Fernmeldegesetz (FMG) Kapitel 7 Art. 43, 46

hat die Abtretung der durch das Fernmeldegeheimnis geschützten Rechte durch den Mitarbeiter zur Folge. Will der Arbeitnehmer nun verhindern, dass private E-Mails archiviert werden, steht es ihm frei, auf den Versand von privaten E-Mails über den dienstlichen E-Mail-Account zu verzichten.[6] Problematisch hierbei bleibt, dass der Mitarbeiter durch das Versenden von privaten E-Mails über den dienstlichen E-Mail-Account auf diese Weise nur seine eigenen durch das Fernmeldegeheimnis geschützten Rechte abtritt. Dies gilt jedoch nicht für einen eventuellen „externen Kommunikationspartner“, dessen Nachrichten unwissentlich und unwillentlich mitgesichert würden. Da also die E-Mails von Außenstehenden archiviert würden und deren Recht auf Datenschutz verletzt, erscheint dieses Vorgehen als nicht zielführende Alternative.

Konflikte bei dienstlichen E-Mails mit personenbezogenen Inhalten

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.

Ist die private Nutzung des dienstlichen E-Mail-Accounts erlaubt, sind Mitarbeiterschulungen und ausführliche Informationen über die Konsequenzen der Nutzung der automatischen Archivierung voranzustellen. Darüber hinaus sollte Mitarbeitern die Möglichkeit gegeben werden diese automatische Archivierung mittels privater Kennzeichnung von E-Mails zu unterbinden.

[6] http://www.swlegal.ch/CMSPages/GetFile.aspx?disposition=attachment&nodeguid=3dd34b9c-405f-476b-8618-81ba7141181f.

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:

Verfahren	Konsequenzen
Es wird auf die Spam-Filterung vor der Archivierung verzichtet	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.
Empfangene E-Mails werden von einer Anti-Spam-Lösung gefiltert und danach archiviert	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. Daher sollten die als Spam identifizierten E-Mails – soweit möglich – in regelmäßigen Abständen kontrolliert werden. Geschäftsrelevante E-Mails, die fälschlicherweise als Spam aussortiert wurden, können in diesem Fall nachträglich archiviert werden.
Als Spam identifizierte E-Mails werden noch vor Annahme durch den eigenen E-Mail-Server abgewiesen	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 Archivierung mit MailStore Server

Unternehmen können mit MailStore Server alle relevanten rechtlichen Anforderungen bei der Archivierung von E-Mails erfüllen. Dies wird einerseits durch regelmäßige Zertifizierungen, andererseits durch ein umfassendes Technologiekonzept gewährleistet.

Regelmäßige Zertifizierung

MailStore Server wird regelmäßig durch eine unabhängige Wirtschaftsprüfungsgesellschaft zertifiziert. Die Prüfung basiert auf der Grundlage der Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e.V. (IDW) "Die Prüfung von Softwareprodukten" (IDW PS 880) und berücksichtigt alle Teilaspekte der Grundsätze ordnungsgemäßer Buchführung, welche die Archivierung betreffen. Im Einzelnen werden folgende gesetzliche Vorgaben beachtet:

Schweiz

- Vorschriften zur Buchführung, Aufbewahrung und Edition des schweizerischen Obligationenrechts (OR)[7]
- 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 (MWSTG) und die Wegleitung für Mehrwertsteuerpflichtige
- Geschäftsbücherverordnung (GeBüV)[8]

Erfüllung sonstiger Aufbewahrungspflichten (z.B. aus dem Gesundheitswesen)

Neben den Vorschriften in der Abgabenordnung und dem Handelsgesetzbuch existieren weitere branchen- oder anwendungsspezifische Aufbewahrungspflichten, die sich aus dem Aktiengesetz, Banken- und Versicherungsgesetz, Beamtenrecht, Produkthaftungsgesetz, Röntgenverordnung usw. ergeben. Hier werden unterschiedliche Aufbewahrungsfristen vorgeschrieben. Diese Aufbewahrungspflichten definieren gegenüber den handels- und steuerrechtlichen Regelungen keine zusätzlichen materiellen Anforderungen an die revisionssichere Aufbewahrung von 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 diese Aufbewahrungspflichten (hinsichtlich E-Mails) technisch erfüllt werden.

[7] http://www.admin.ch/opc/de/classified-compilation/19110009/index.html

[8] http://www.admin.ch/opc/de/classified-compilation/20001467/index.html

Umfassendes Technologiekonzept

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

Vollständigkeit	▪ MailStore Server ermöglicht die vollständige Archivierung aller E-Mails im Unternehmen. E-Mails können beispielsweise noch vor der Zustellung in die Postfächer der Mitarbeiter archiviert werden.
Originalgetreue Archivierung	▪ Archivierte E-Mails stimmen in jeder Hinsicht mit dem Original überein und können bei Bedarf ohne Informationsverlust aus dem Archiv heraus wiederhergestellt werden.
Manipulationssicherheit	▪ Durch Bildung von SHA-Hashwerten über die Inhalte der E-Mails und eine interne AES256-Verschlüsselung schützt MailStore Server die archivierten Daten vor Manipulationen. ▪ Es erfolgt kein direkter Zugriff der MailStore Client-Komponenten auf die Archivdateien. ▪ Die Änderung der E-Mail-Inhalte ist weder in der grafischen Oberfläche noch programmintern vorgesehen.
Aufbewahrungsfristen	▪ Grundsätzlich kann kein Benutzer, solange die Standard-Benutzerrechte nicht aktiv vom Administrator geändert werden, E-Mails aus dem Archiv löschen. ▪ Darüber hinaus können globale und über allen Benutzerrechten stehende Aufbewahrungsfristen definiert werden.
Legal Hold	▪ Ist Legal Hold aktiviert, können ungeachtet aller anderen möglichen Konfigurationen wie der Benutzerrechte und der Aufbewahrungsfristen, keine E-Mails aus dem Archiv gelöscht werden.
Protokollierung	▪ MailStore Server protokolliert Änderungen und Ereignisse, die vom Administrator definiert werden können, über eine integrierte Auditing-Funktion lückenlos.
Datenzugriff	▪ Über einen speziellen Benutzertyp „Auditor“ kann für externe Prüfer der Zugriff auf das Archiv realisiert werden. Alle Aktionen dieses Benutzertyps werden grundsätzlich protokolliert. ▪ Zudem können alle E-Mails jederzeit im Standardformat nach RFC822/RFC2822 aus dem Archiv heraus exportiert und für eine Betriebsprüfung übermittelt werden.

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 Kopien aller E-Mails in einem zentralen E-Mail-Archiv ab und stellt so die Unveränderbarkeit, 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 höchstmöglicher Geschwindigkeit durchsuchen. MailStore Server kombiniert eine leistungsstarke Technologie mit niedrigen Kosten und intuitiver Bedienbarkeit.

Über die MailStore Software GmbH

Die MailStore Software GmbH mit Hauptsitz in Viersen bei Düsseldorf, ein Tochterunternehmen des US-amerikanischen Backup-Spezialisten Carbonite (NASDAQ: CARB), zählt zu den weltweit führenden Herstellern von E-Mail-Archivierungslösungen. Über 35.000 Unternehmen, öffentliche Institutionen und Bildungseinrichtungen in mehr als 100 Ländern vertrauen auf die Produkte des deutschen Spezialisten.

Zudem bietet MailStore mit der MailStore Service Provider Edition (SPE) eine Lösung speziell für Provider an, die auf dieser Basis ihren Kunden rechtssichere E-Mail-Archivierung als Managed Service anbieten können.

Mit MailStore Home befindet sich ein weiteres Produkt im Portfolio, das Einzelanwendern die kostenlose Archivierung ihrer privaten E-Mails ermöglicht. MailStore Home wird derzeit weltweit von über 1.000.000 Anwendern genutzt.

Sprechen Sie uns an!

MailStore Software GmbH

Cloerather Str. 1-3
41748 Viersen
Deutschland

E-Mail: sales@mailstore.com
Telefon: +49-(0)2162-502990
Fax: +49 (0)2162 - 50299-29

Rechtlicher Hinweis