Rechtssichere E-Mail-Archivierung

Der Leitfaden für Deutschland

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: 11. November 2015

Übersicht der wichtigsten Fragestellungen

Was muss archiviert werden?

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

Dazu gehört jegliche Korrespondenz, durch die ein Geschäft vorbereitet, abgewickelt, abgeschlossen oder rückgängig gemacht wird. Beispiele sind Rechnungen, Aufträge, Reklamationsschreiben, Zahlungsbelege und Verträge. Dies gilt auch dann, wenn diese per E-Mail versendet werden.

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 7 „Konflikte zwischen Datenschutz und E-Mail-Archivierung vermeiden“).

Wie lange müssen E-Mails aufbewahrt werden?

Die Aufbewahrungsfristen ergeben sich aus dem Handelsgesetzbuch (§ 257 HGB) [1] und der Abgabenordnung (§ 147 AO) [2]:

- Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen, die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen sowie Buchungsbelege müssen zehn Jahre lang aufbewahrt werden.
- Empfangene Handels- oder Geschäftsbriefe, Wiedergaben der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, müssen sechs Jahre lang aufbewahrt werden.
- Die Fristen beginnen mit Schluss des Kalenderjahres, indem die Handels- oder Geschäftsbriefe versendet oder empfangen wurden oder die sonstigen Unterlagen entstanden sind.

[1] http://www.gesetze-im-internet.de/hgb/__257.html

[2] http://www.gesetze-im-internet.de/ao_1977/__147.html

Die Aufbewahrungsfrist läuft jedoch nicht ab, soweit und solange die Unterlagen für Steuern von Bedeutung sind, für welche die Festsetzungsfrist noch nicht abgelaufen ist. In der Praxis geht man daher von einer regelmäßigen Aufbewahrungsfrist von elf Jahren aus.

Wer trägt die Verantwortung und welche Konsequenzen drohen?

Die Verantwortung für die ordnungsgemäße Umsetzung der rechtlichen Anforderungen zur Aufbewahrung von E-Mails liegt bei der Geschäftsführung eines Unternehmens. Kommt diese ihrer Pflicht nicht nach, drohen zivilrechtliche und strafrechtliche Konsequenzen:

- § 162 AO3: Steuerliche Konsequenzen, wie Strafzahlungen an das Finanzamt
- § 283 StGB4: z.B. eine Freiheitsstrafe von bis zu 2 Jahren bei Verletzung der Buchführungspflicht
- § 280ff. BGB5 und § 241 Abs. 2 BGB6: Schadensersatzansprüche

Kann eine E-Mail als Beweis genutzt werden?

Abgesehen von der gesetzlichen Pflicht ist es auch ratsam E-Mails zu archivieren, um bei gerichtlichen Auseinandersetzungen auf diese Dokumente zurückzugreifen. Im Rahmen der freien richterlichen Beweiswürdigung genießen E-Mails zwar nicht den gleichen Status wie eine Urkunde, gelten nach § 371 Abs. 1 Satz 2 ZPO[7] als elektronisches Dokument grundsätzlich aber als Augenscheinbeweis. Zudem sind sie oft der einzige Nachweis für Absprachen zwischen den Streitparteien. So liefern E-Mails in diesem Zusammenhang wichtige Indizien zu Aussteller, Empfänger, Absende- und Zugangsdatum sowie zu vereinbarten Vertragsinhalten. Zusammen mit einer qualifizierten elektronischen Signatur können E-Mails zudem vom Aussteller oder mittels notariell beglaubigter Handzeichen unterzeichneten Privaturkunden gleichgestellt werden (§ 371a ZPO). Dies begründet die formelle Beweiskraft von E-Mails und wird als Beweis gewertet, dass in qualifiziert elektronisch signierten E-Mails enthaltene Erklärungen tatsächlich von den Ausstellern abgegeben wurden.

[3] http://www.gesetze-im-internet.de/ao_1977/__162.html
[4] http://www.gesetze-im-internet.de/stgb/__283b.html
[5] http://www.gesetze-im-internet.de/bgb/__280.html
[6] http://www.gesetze-im-internet.de/bgb/__241.html
[7] http://www.gesetze-im-internet.de/zpo/__371a.html

Anforderungen an eine revisionssichere E-Mail-Archivierung

Allgemeine Anforderungen an eine revisionssichere E-Mail-Archivierung ergeben sich insbesondere aus den Ordnungsvorschriften für die Buchführung und für Aufzeichnungen (§ 146 AO) sowie den Vorgaben zur Führung der Handelsbücher (§ 239 HGB), welche die

- Vollständigkeit
- Richtigkeit,
- Zeitgerechtheit,
- Unveränderbarkeit,
- Ordnung und
- Nachvollziehbarkeit

bei der Führung der Handelsbücher und sonstiger erforderlicher Aufzeichnungen in den Vordergrund stellen.

Das Bundesfinanzministerium hat zudem am 14.11.2014 das Schreiben zu den „Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“[8] veröffentlicht. Das Verwaltungsschreiben konkretisiert die Normen aus der Abgabenordnung (AO) und dem Umsatzsteuergesetz (UStG) und bestimmt, wie digitale Unterlagen aufbewahrt werden sollen, damit das Finanzamt bei einer Betriebsprüfung auf diese Informationen zugreifen kann. Die GoBD gelten seit dem 1.1.2015 und lösen die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“, das „FAQ zum Datenzugriffsrecht der Finanzverwaltung“ sowie die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ ab. Folgende Aspekte der GoBD sind für die revisionssichere Archivierung von E-Mails besonders zu beachten:

Grundsätzlich müssen alle relevanten E-Mails und deren Dateianhänge **vollständig**, **manipulationssicher** und **jederzeit verfügbar** aufbewahrt werden. Weiterhin müssen die Daten **maschinell auswertbar** sein. Eine alleinige Aufzeichnung auf Mikrofilm oder Papier ist nicht ausreichend, da dies den Anforderungen an die (jederzeitige) maschinelle Auswertbarkeit nicht genügt. Weiterhein stellt eine Langzeitarchivierung im verwendeten E-Mail-System keine geeignete Lösung dar, da die Anforderungen an die Ordnungsmäßigkeit (insbesondere Unveränderbarkeit und Nachvollziehbarkeit) schwerlich erfüllt werden können.

Eine Umwandlung in ein anderes Format (z. B. Inhouse-Format) zum Zwecke der Archivierung ist nur zulässig, wenn die maschinelle Auswertbarkeit nicht eingeschränkt und keine inhaltliche Veränderung vorgenommen wird (Grundsatz der Unveränderbarkeit). Wird eine E-Mail beispielsweise als PDF-Datei gespeichert, so gehen dabei gegebenenfalls die Informationen des Headers (z. B. Informationen zum Absender, Zustelldatum etc.) verloren und sind somit nicht mehr ohne weiteres nachvollziehbar.

[8] http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=1

Sofern beispielsweise eine Gelangensbestätigung, als Nachweis der Steuerbefreiung bei innergemeinschaftlichen Lieferungen, per E-Mail übermittelt wird, verlangen die Finanzbehörden für den Nachweis der Herkunft eine sichere Aufbewahrung der kompletten E-Mail samt Anhang im elektronischen Original.

Aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen, die im Unternehmen entstanden oder dort eingegangen sind, sind ebenfalls in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. Eine Aufbewahrung ausschließlich in ausgedruckter Form ist daher nicht mehr zulässig. Die Dokumente müssen für die Dauer der Aufbewahrungsfrist unveränderbar erhalten bleiben. Dies gilt unabhängig davon, ob die Aufbewahrung im Produktivsystem oder durch Auslagerung in ein anderes DV-System erfolgt. Unter Zumutbarkeitsgesichtspunkten ist es jedoch nicht zu beanstanden, wenn der Steuerpflichtige elektronisch erstellte und in Papierform abgesandte Handels- und Geschäftsbriefe nur in Papierform aufbewahrt.

Das Archivierungsverfahren für E-Mails unterliegt nach den GoBD der Verpflichtung zu einer Verfahrensdokumentation, welche auch als Teil der generellen Verfahrensdokumentation des Archivierungs- bzw. Dokumentenmanagementsystems umgesetzt werden kann. Hierbei sollten jedoch die für die E-Mail-Archivierung spezifischen Aspekte, wie beispielsweise Regelungen zu SPAM, Konvertierungseinstellungen, Beschreibung der Maßnahmen zur Sicherung der Vollständigkeit, Nachvollziehbarkeit, Unveränderbarkeit und maschinellen Auswertbarkeit etc. berücksichtigt werden. Die „Merksätze des Verbandes Organisations- und Informationssysteme e.V. zur revisionssicheren elektronischen Archivierung“[9] erläutern, was dies konkret für die Archivierung elektronischer Dokumente bedeutet:

- 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.

[9] http://www.voi.de/publikationen/leitfaeden-whitepaper/view_document/299-merksaetze-des-voi-zur-revisionssicheren-elektronischen-archivierung

Was ist zu beachten, wenn aufbewahrungspflichtige E-Mails verschlüsselt archiviert werden?

Es muss sichergestellt sein, dass der Prüfer bei einer Datenträgerüberlassung auf die Daten zugreifen kann und die maschinelle Auswertbarkeit gewährleistet ist. Die Entschlüsselung der übergebenen steuerlich relevanten Daten muss "spätestens bei der Datenübernahme auf Systeme der Finanzverwaltung erfolgen."[10]

Dürfen E-Mails aus dem Archiv gelöscht werden?

Ja, grundsätzlich ist es möglich, E-Mails aus dem Archiv zu löschen, solange dies nicht mit der gesetzlich geforderten Vollständigkeit und Dauer der Aufbewahrung in Konflikt steht. So dürfen beispielsweise Spam-E-Mails aus dem Archiv entfernt werden. In der Praxis ist es jedoch schwierig in archivierungspflichtige und nicht-archivierungspflichtige E-Mails zu unterscheiden, weswegen die meisten Systeme standardmäßig so konfiguriert sind, dass sie alle E-Mails archivieren.

Datensicherheit bei der E-Mail-Archivierung

Die GoBD betonen ferner die Wichtigkeit der Datensicherheit bei der formellen Ordnungsmäßigkeit der Buchführung. Daten, Datensätze, elektronischen Dokumente und elektronischen Unterlagen sind demzufolge ausreichend zu schützen und gegen Verlust, (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) und unberechtigte Eingaben und Veränderungen (z.B. durch Zugangs- und Zugriffskontrollen) zu sichern. Dies erfordert die Einbettung der E-Mail-Archivierungslösung in das IT-Sicherheitskonzept der Unternehmung sowie die Überwachung der Wirksamkeit und Einhaltung der technischen und organisatorischen Vorgaben durch ein effizientes Internes Kontrollsystem (IKS). Insbesondere sind bei der Einbettung der E-Mail-Archivierung die allgemeinen IT-Schutzziele Vertraulichkeit (autorisierter Zugriff), Integrität (Schutz vor Veränderungen) und Verfügbarkeit zu beachten.

[10] http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=1

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 Bundesdatenschutzgesetz (BDSG)[11] und dem Telekommunikationsgesetz (TKG)[12].

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.

Eine sachgerechte E-Mail-Richtlinie sollte den Verarbeitungsprozess einer E-Mail im E-Mail-System über den gesamten Lebenszyklus und Kommunikationsprozess beschreiben und definieren. Dies schließt das oben aufgeführte Verbot der privaten Nutzung der betrieblichen E-Mail-Kommunikationsstrukturen mit ein, welches regelmäßig kontrolliert werden sollte, da aus einer Duldung wiederum eine stillschweigende Erlaubnis abgeleitet werden könnte, die die ursprüngliche Weisung aufhebt. Dies hätte direkte Auswirkungen auf die Zulässigkeit der automatischen Archivierung von E-Mails.

[11] http://www.gesetze-im-internet.de/bdsg_1990/index.html

[12] http://www.gesetze-im-internet.de/tkg_2004/index.html

Ist die Zustimmung zur Archivierung durch eine Betriebsvereinbarung 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 – 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.

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.

Sonderfall „Bewerbungsunterlagen“

Ein weiteres Beispiel sind Bewerbungsunterlagen. Gemäß § 35 Abs. 2 BDSG[13] sind personenbezogene Daten zu löschen, wenn sie für eigene Zwecke verarbeitet werden, „sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.“ Dementsprechend ist eine langfristige Aufbewahrung von Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens nicht gestattet. Um sich vor einem etwaigen Verstoß gegen das Benachteiligungsverbot nach dem Antidiskriminierungsgesetz (AGG) zu verteidigen, ist lediglich eine Aufbewahrungsfrist von zwei Monaten nach Abschluss des Bewerbungsverfahrens gestattet (§ 15 Abs. 4 AGG) [14].

Sonderfall „E-Mails an den Betriebsrat“

E-Mails an den Betriebsrat stellen ebenfalls sensible Informationen dar und unterliegen einem gesteigerten Persönlichkeitsrecht.

In der Praxis

Um Konflikte mit dem Datenschutz zu vermeiden, sollten E-Mails mit personenbezogenen Inhalten wie Bewerbungsunterlagen oder E-Mails an den Betriebs- oder Personalrat an eine entsprechend eingerichtete E-Mail-Adresse wie z.B. betriebsrat@firma.de gesendet werden. Dieses Postfach kann dann von der Archivierung ausgeschlossen werden.

---

[13] http://www.gesetze-im-internet.de/bdsg_1990/__35.html

[14] http://www.gesetze-im-internet.de/agg/__15.html

Führende deutsche IT-Rechtler vertreten zudem die Auffassung, dass bei einer Interessenabwägung zwischen dem Datenschutz des Arbeitnehmers (Art. 2 Abs. 1 GG[15] i.V.m. Art. 1 Abs. 1 GG[16]) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes des Arbeitgebers (Art. 14 Abs. 1GG)[17] letzterer obsiegt. Der Begriff der „Erforderlichkeit“ (§ 32 BDSG)[18] 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 Abs. 3 BDSG[19] nachkommen und alle Mitarbeiter vor der Implementation einer entsprechenden Lösung informieren.

[15] http://www.gesetze-im-internet.de/gg/art_2.html
[16] http://www.gesetze-im-internet.de/gg/art_1.html
[17] http://www.gesetze-im-internet.de/gg/art_14.html
[18] http://www.gesetze-im-internet.de/bdsg_1990/__32.html
[19] http://www.gesetze-im-internet.de/bdsg_1990/__4.html

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:

Deutschland

- Vorschriften des Handels- und Steuerrechts über die Ordnungsmäßigkeit der Buchführung (§§ 238 ff.[20] und § 257 HGB sowie §§ 140 ff. AO)
- IDW Stellungnahme zur Rechnungslegung "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)"
- Die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“ von 11/2014
- IDW Prüfungsstandard "Die Prüfung von Softwareprodukten (IDW PS 880)"
- Deutsches Umsatzsteuergesetz (UStG)

Hinweis zur GoBD

Bei der Zertifizierung von MailStore Server 9.4.1 wurden bereits die GoBD berücksichtigt.

[20] http://www.gesetze-im-internet.de/hgb/__238.html

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.

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 30.000 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

Dieses Dokument dient lediglich der Information und stellt keine Rechtsberatung dar. Im konkreten Einzelfall wenden Sie sich bitte an einen spezialisierten Rechtsanwalt. Eine Gewähr und Haftung für die Richtigkeit aller Angaben wird nicht übernommen.