Die Experten für
E-Mail-Archivierung

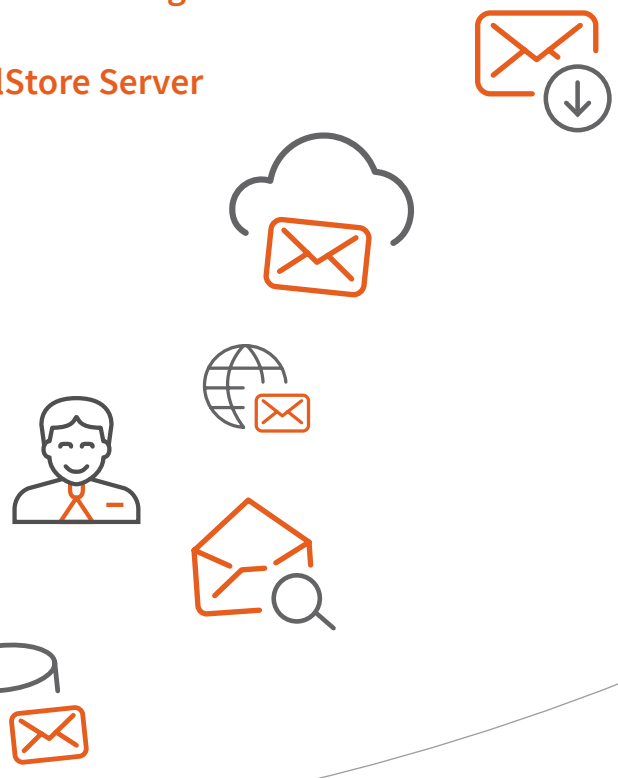
MAIL STORE™

Der Leitfaden für Deutschland

Rechtssichere E-Mail-Archivierung nach GoBD

Inhaltsverzeichnis

Wissen wie & warum



Vorwort

Vorwort

Wissen wie & warum

E-Mail-Archivierung bietet nicht nur zahlreiche technische und wirtschaftliche Vorteile, sie kann für viele Unternehmen zudem eine zwingende Notwendigkeit darstellen. Geltende rechtliche Anforderungen können grundsätzlich nicht ohne eine technische Lösung erfüllt werden. Besonders der rechtliche Aspekt der Archivierung ist sehr vielschichtig. Darüber hinaus fehlt es an zwingend vorgeschriebenen Methoden, die rechtlichen Anforderungen einzuhalten.

Dieser Leitfaden führt durch die wichtigsten Fragestellungen im Hinblick auf die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“ sowie die damit zusammenhängenden handels- und steuerrechtlichen Vorschriften.

Stand: Januar 2020

Wissen wie & warum

Die wichtigsten Fragestellungen

Was muss archiviert werden?

Gemäß § 147 der Abgabenordnung (AO)[1] sind folgende Unterlagen geordnet aufzubewahren:

- 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,
- Buchungsbelege,
- Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union[2],
- sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.

Dazu gehört insbesondere jegliche nach außen gerichtete Korrespondenz, durch die ein Geschäft vorbereitet, abgeschlossen, abgewickelt oder rückgängig gemacht wird. Beispiele sind Rechnungen, Angebote und Auftragsbestätigungen, Mängelrügen und Reklamationsschreiben, Zahlungsbelege und Verträge. Ebenfalls erfasst sind Mitteilungen zwischen Unternehmen desselben Konzerns oder solche, die nur eine einmalige Kontaktaufnahme bezwecken. All dies gilt auch dann, wenn diese Korrespondenz per E-Mail versendet wird.

Daneben existieren jedoch noch weitere Vorschriften, die eine Aufbewahrung von Unterlagen verlangen. Sie sind z. B. in § 257 des Handelsgesetzbuchs (HGB)[3], § 8 des Geldwäschegesetzes[4] und § 50 der Bundesrechtsanwaltsordnung[5] geregelt.

Archivierung von Dateianhängen

E-Mail-Anhänge müssen ebenfalls archiviert werden, sollte die E-Mail ohne diese Anlagen unverständlich oder unvollständig sein. Im umgekehrten Fall, wenn also die E-Mail nur zur Übertragung eines Anhangs dient, ist die E-Mail selbst zwar nicht aufbewahrungspflichtig – wohl aber der jeweilige Anhang.

In der Praxis

Angesichts der Masse täglich empfangener und versendeter E-Mails ist eine Kategorisierung in archivierungspflichtige und nicht archivierungspflichtige E-Mails üblicherweise nur mit erheblichem Aufwand 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 10 „Konflikte zwischen Datenschutz und E-Mail-Archivierung vermeiden“).

---

[1] http://www.gesetze-im-internet.de/ao_1977/__147.html
[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0952&from=DE
[3] https://www.gesetze-im-internet.de/hgb/__257.html
[4] https://www.gesetze-im-internet.de/gwg_2017/__8.html
[5] https://www.gesetze-im-internet.de/brao/__50.html

MAIL STORE

Wissen wie & warum

Wie lange müssen E-Mails aufbewahrt werden?

Die Aufbewahrungsfristen ergeben sich u. a. aus § 257 Abs. 4, 5 HGB[6] und § 147 Abs. 3, 4 AO[7]. Auszugsweise gilt das Folgende:

- Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen, die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen sowie Buchungsbelege und Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union[8] müssen grundsätzlich 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 grundsätzlich sechs Jahre lang aufbewahrt werden.
- Die Fristen beginnen mit Schluss des Kalenderjahres, in dem die Handels- oder Geschäftsbriefe versendet oder empfangen wurden oder die sonstigen Unterlagen entstanden sind, aufgestellt wurden bzw. die letzte Eintragung gemacht oder eine Aufzeichnung vorgenommen wurde.

Die Aufbewahrungsfrist läuft jedoch nicht ab, soweit und solange die Unterlagen für Steuern von Bedeutung sind, für die die Festsetzungsfrist noch nicht abgelaufen ist. In der Praxis wird daher häufig eine regelmäßige Aufbewahrungsfrist von elf Jahren angenommen.

Wer trägt die Verantwortung und welche Konsequenzen drohen?

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

- § 162 AO[9]: steuerliche Konsequenzen, wie Schätzung durch das Finanzamt oder Festsetzung von Zuschlägen
- § 283 StGB[10]: Eine Freiheitsstrafe von bis zu fünf Jahren oder eine Geldstrafe erhält, wer – neben weiteren Voraussetzungen – bei Überschuldung oder Zahlungsunfähigkeit aufbewahrungspflichtige Unterlagen beiseiteschafft, verheimlicht, zerstört oder beschädigt
- § 280 ff. BGB[11] und § 241 Abs. 2 BGB[12]: Schadensersatzansprüche aufgrund schuldhafter Pflichtverletzungen
- § 35 GewO[13], z. B. in Verbindung mit § 6 GmbHG[14]: verwaltungsrechtliche Konsequenzen wie der Verlust der Zuverlässigkeit bzw. die Gewerbeuntersagung, sodass eine Person etwa nicht mehr als Geschäftsführer einer GmbH tätig sein darf

[6] https://www.gesetze-im-internet.de/hgb/__257.html
[7] http://www.gesetze-im-internet.de/ao_1977/__147.html
[8] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0952&from=DE
[9] https://www.gesetze-im-internet.de/ao_1977/__162.html
[10] https://www.gesetze-im-internet.de/stgb/__283.html
[11] https://www.gesetze-im-internet.de/bgb/__280.html
[12] https://www.gesetze-im-internet.de/bgb/__241.html
[13] https://www.gesetze-im-internet.de/gewo/__35.html
[14] https://www.gesetze-im-internet.de/gmbhg/__6.html

Kann eine E-Mail als Beweis genutzt werden?

In Deutschland gilt die Formfreiheit von Verträgen, sofern Gesetze oder Parteivereinbarungen dem nicht entgegenstehen. Verträge können somit mittels E-Mail abgeschlossen werden. Auch wenn im Zivilrecht keine Pflicht zur systematischen Ablage und Aufbewahrung besteht, ist die Archivierung für Unternehmen aus Gründen der Beweisführung empfehlenswert.

Abgesehen von den bereits genannten gesetzlichen Pflichten, ist es ratsam, E-Mails zu archivieren, um bei gerichtlichen Auseinandersetzungen auf diese Dokumente zurückzugreifen. Die Beweiskraft elektronischer Dokumente ist im gesamten europäischen Rechtsraum durch die so genannte eIDAS-Verordnung[15] gestärkt worden. In Deutschland sind auf E-Mails mit qualifizierter elektronischer Signatur zudem nach § 371 a Abs. 1 S. 1 ZPO[16] die Vorschriften über die Beweiskraft privater Urkunden entsprechend anzuwenden. Eine solche Signatur ersetzt also die Unterschrift des Ausstellers. Im Rahmen der freien richterlichen Beweiswürdigung genießen E-Mails ohne qualifizierte elektronische Signatur zwar nicht den gleichen Status wie eine Urkunde, jedoch kann nach § 371 Abs. 1 S. 2 ZPO[17] der Beweis mit einer E-Mail als elektronischem Dokument grundsätzlich aber in Form des Augenscheinbeweises angetreten werden.

Oft sind E-Mails der einzige Nachweis für Absprachen zwischen den Streitparteien. So liefern sie in diesem Zusammenhang wichtige Indizien zu Aussteller, Empfänger, Absende- und Zugangsdatum sowie zu vereinbarten Vertragsinhalten, sofern sie in nicht manipulierter Form und mit dem ursprünglichen Inhalt vorliegen.

[15] Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[16] http://www.gesetze-im-internet.de/zpo/__371a.html

[17] http://www.gesetze-im-internet.de/zpo/__371a.html

Wissen wie & warum

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 (§ 145 ff. AO[18]) sowie den Vorgaben zur Führung der Handelsbücher (§ 238 ff. HGB[19]), die die

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

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

Das Bundesfinanzministerium hat am 28. November 2019 das Schreiben zu den „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“[20] aktualisiert. Diese so genannte Verwaltungsvorschrift konkretisiert die Normen aus der Abgabenordnung und dem Umsatzsteuergesetz (UStG) und bestimmt, wie digitale Unterlagen aufbewahrt werden sollen, u. a. damit das jeweils zuständige Finanzamt bei einer Betriebsprüfung auf diese Informationen zugreifen kann. Die GoBD haben die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“, das „FAQ zum Datenzugriffsrecht der Finanzverwaltung“ sowie die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ abgelöst. 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. Weiterhin 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. Wenn Rechnungen oder Buchungsbelege auf elektronischem Wege eingegangen sind, genügt die Aufbewahrung der tatsächlich weiterverarbeiteten Formate, soweit diese über die höchste maschinelle Auswertbarkeit verfügen. Diese Formate alleine erfüllen die Belegfunktion, wenn sie mit dem vollständigen, originalen Inhalt gespeichert werden.

Eine Umwandlung in ein anderes Format (z. B. Inhouse-Format) zum Zwecke der Archivierung ist nur

[18] https://www.gesetze-im-internet.de/ao_1977/__145.html

[19] https://www.gesetze-im-internet.de/hgb/__238.html

[20] https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf;jsessionid=627CE0137E8E6292120E17384FF3E431.delivery2-master?__blob=publicationFile&v=9

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.

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. Es gelten also dieselben steuerrechtlichen Anforderungen wie für die Aufbewahrung elektronischer Rechnungen, die sich bekanntlich aus der AO, dem UStG und der Umsatzsteuer-Durchführungsverordnung (UStDV) ergeben.

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 nicht 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. Es ist dabei auch nicht relevant, ob es sich bei dem betreffenden DV-System um eigene Hard- oder Software oder eine Cloud-Lösung handelt.[21] 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, die 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, berücksichtigt werden. Die „Merksätze des Verbandes Organisations- und Informationssysteme e. V. zur revisionssicheren elektronischen Archivierung“[22] 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.

[21] Vgl. Rn 20 https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf;jsessionid=627CE0137E8E6292120E17384FF3E431.delivery2-master?__blob=publicationFile&v=9

[22] https://www.voi.de/downloads/top-10-downloads/

- 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.

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“.[23]

Dürfen E-Mails aus dem Archiv gelöscht werden?

Ja, grundsätzlich ist es möglich und nicht zwingend unzulässig, 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, zwischen archivierungspflichtigen und nicht archivierungspflichtigen E-Mails zu unterscheiden, weswegen die meisten Systeme wohl standardmäßig so konfiguriert sein dürften, dass sie alle E-Mails archivieren.

Datensicherheit bei der E-Mail-Archivierung

Die GoBD betonen ferner die Wichtigkeit der Datensicherheit, um eine formell ordnungsmäßige Buchführung sicherzustellen. Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen sind demzufolge ausreichend zu schützen und gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) sowie unberechtigte Eingaben und Veränderungen (z. B. durch Zugangs- und Zugriffskontrollen) zu sichern. Dies dürfte 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) erfordern. Insbesondere sind bei der Einbettung der E-Mail-Archivierung die allgemeinen IT-Schutzziele Vertraulichkeit (autorisierter Zugriff), Integrität (Schutz vor Veränderungen) und Verfügbarkeit zu beachten.

[23] https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf;jsessionid=627CE0137E8E6292120E17384FF3E431.delivery2-master?__blob=publicationFile&v=9

Wissen wie & warum

Konflikte zwischen Datenschutz und E-Mail-Archivierung vermeiden

Durch die Umsetzung einer Compliance-Strategie, mit deren Hilfe u. a. die gesetzlichen Anforderungen zur Aufbewahrung von E-Mails umgesetzt werden sollen, kann ein Unternehmen unter gewissen Umständen in Konflikt mit anderen rechtlichen Vorschriften geraten. So müssten insbesondere die EU-Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG)[24], das Telekommunikationsgesetz (TKG)[25], das Telemediengesetz (TMG)[26] und das jeweilige Landesdatenschutzgesetz beachtet werden.

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 wohl nur mit unverhältnismäßigem Aufwand möglich.

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 Vorschriften zum Datenschutz stehen. Ist den Arbeitnehmern beispielsweise die private E-Mail-Nutzung gestattet, wird der Arbeitgeber sogar als Telekommunikationsanbieter angesehen, sodass ihn besondere Pflichten treffen.

Untersagung der privaten E-Mail-Nutzung

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

Die schriftliche Fixierung kann z. B. in Richtlinien zur 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, das regelmäßig kontrolliert werden sollte, da aus einer Duldung wiederum eventuell eine stillschweigende Erlaubnis abgeleitet werden könnte,

[24] http://www.gesetze-im-internet.de/bdsg_2018/index.html
[25] http://www.gesetze-im-internet.de/tkg_2004/index.html
[26] https://www.gesetze-im-internet.de/tmg/index.html

die die ursprüngliche Weisung möglicherweise aufhebt (Stichwort „betriebliche Übung“). Dies hätte direkte Auswirkungen auf die Zulässigkeit der automatischen Archivierung von E-Mails.

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 die E-Mail-Archivierung dann nicht in Konflikt miteinander stehen, wenn die Mitarbeiter – gegebenenfalls mittels einer Betriebsvereinbarung durch den Betriebsrat – der Archivierung explizit zugestimmt bzw. in sie eingewilligt haben. Allgemein betrachtet ist dies auch zutreffend, wie u. a. Erwägungsgrund 155 zur DSGVO[27] klarstellt. Im Detail ist dies jedoch kompliziert. Gibt der Arbeitgeber in einer eigens dafür formulierten Weisung 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. 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. Tut er dies nicht, wird sein Unterlassen als konkludente Zustimmung gewertet. Problematisch hierbei ist, dass der Mitarbeiter eine Einwilligung nur in Bezug auf seine eigenen durch das Fernmeldegeheimnis geschützten Rechte erklären 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 würde, erscheint dieses Vorgehen nicht als zielführende Alternative. Darüber hinaus würde eine solche konkludente Zustimmung keine Rechtsgrundlage für die Archivierung von sensiblen Daten darstellen, welche regelmäßig in privaten E-Mails enthalten sind (vgl. Art. 9 Abs. 2 lit. a DSGVO, welcher eine ausdrückliche Einwilligung voraussetzt). Ferner müsste die Einwilligung freiwillig erfolgen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Schließlich muss die Einwilligung grundsätzlich auch noch in Schriftform, also mit eigenhändiger Originalunterschrift des Beschäftigten, erfolgen.[28]

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 beinhalten dienstliche E-Mails durchaus häufig datenschutzrechtlich relevante, personenbezogene Inhalte. 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.[29]

---

[27] https://dsgvo-gesetz.de/erwaegungsgruende/nr-155/

[28] Vgl. § 26 Abs. 2 S. 2 und 3 BDSG, https://dsgvo-gesetz.de/bdsg/26-bdsg/; vgl. im Übrigen auch Art. 7 DSGVO, https://dsgvo-gesetz.de/art-7-dsgvo/

[29] Auch Gesundheitsdaten sind Daten einer besonderen Kategorie und somit gemäß Art. 9 DSGVO und § 22 BDSG besonders schützenswert, vgl. https://dsgvo-gesetz.de/art-9-dsgvo/ und https://dsgvo-gesetz.de/bdsg/22-bdsg/

Sonderfall „Bewerbungsunterlagen“

Ein weiteres Beispiel sind Bewerbungsunterlagen. Gemäß dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO[30], § 47 Nr. 5 BDSG[31]) dürfen personenbezogene Daten nur so lange gespeichert werden, wie es erforderlich ist, um den jeweiligen Zweck zu erreichen. Die Speicherung muss in einer Form erfolgen, die die Identifizierung der betroffenen Personen ermöglicht.[32] Dementsprechend ist eine langfristige Aufbewahrung von Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens nicht gestattet. Der Bundesbeauftragte für Datenschutz vertritt sogar die Auffassung, dass Bewerberdaten schon nach zwei Monaten zu löschen sind.[33] Andere Stimmen halten eine Aufbewahrung für maximal sechs Monate für zulässig. Man könnte sogar andenken, ob das Bewerbungsschreiben selbst nicht vielleicht ein aufbewahrungspflichtiger Geschäfts- oder Handelsbrief ist und somit gemäß § 147 Abs. 3 AO[34] grundsätzlich sogar sechs Jahre lang aufbewahrt werden müsste.

Sonderfall „E-Mails an den Betriebsrat“

E-Mails an den Betriebsrat stellen ebenfalls besonders schutzwürdige Informationen dar und unterliegen einem besonderen Schutz.

In der Praxis

Um Konflikte mit dem Datenschutz zu vermeiden, könnten E-Mails mit besonders schutzwürdigen personenbezogenen Inhalten wie Bewerbungsunterlagen oder E-Mails an den Betriebs- oder Personalrat an eine entsprechend eingerichtete E-Mail-Adresse wie zum Beispiel betriebsrat@firma.de gesendet werden. Dieses Postfach kann dann z. B. von der Archivierung ausgeschlossen werden. Gleiches kann für den elektronischen Briefverkehr mit dem Datenschutzbeauftragten oder dem Betriebsarzt gelten.

---

[30] https://dsgvo-gesetz.de/art-5-dsgvo/
[31] https://www.gesetze-im-internet.de/bdsg_2018/__47.html
[32] https://dsgvo-gesetz.de/bdsg/47-bdsg/
[33] https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/BeschaeftigungArbeitArtikel/Bewerbungsunterlagen.html
[34] http://www.gesetze-im-internet.de/ao_1977/__147.html

Wissen wie & warum

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 höhere 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 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.

Wissen wie & warum

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.

Wissen wie & warum

Rechtssichere Archivierung mit MailStore Server

MailStore Server ermöglicht die zuverlässige Einhaltung aller relevanten rechtlichen Vorgaben bei der Archivierung von E-Mails. Dies wird einerseits durch regelmäßige Zertifizierungen, andererseits durch ein umfassendes Technologiekonzept gewährleistet.

Regelmäßige Zertifizierung

MailStore Server wird regelmäßig durch einen unabhängigen IT-Revisor zertifiziert. Die Prüfungen basieren zum einen auf der Grundlage der Prüfungsstandards des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW) „Die Prüfung von Softwareprodukten (IDW PS 880)“ und berücksichtigen alle Teilaspekte der Grundsätze ordnungsgemäßer Buchführung, die die Archivierung betreffen. Im Einzelnen werden u. a. folgende gesetzliche Vorgaben beachtet:

- Vorschriften des Handels- und Steuerrechts über die Ordnungsmäßigkeit der Buchführung (§ 238 ff.[35] und § 257 HGB sowie § 140 ff. AO[36])
- „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)“
- „IDW Prüfungsstandard: Die Prüfung von Softwareprodukten (IDW PS 880)“
- Deutsches Umsatzsteuergesetz (UStG)

Zum anderen wird MailStore Server von einem unabhängigen IT-Revisor ebenfalls regelmäßig auf die Möglichkeit der Einhaltung der Betroffenenrechte und Dokumentationspflichten nach der Datenschutz-Grundverordnung (DSGVO) geprüft, wobei auch das Bundesdatenschutzgesetz Grundlage der Analyse ist.

[35] http://www.gesetze-im-internet.de/hgb/__238.html
[36] https://www.gesetze-im-internet.de/ao_1977/__140.html

Wissen wie & warum

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 Aktienrecht, Banken- und Versicherungsrecht, Beamtenrecht, Produkthaftungsrecht, Medizinrecht usw. ergeben. Hier werden unter Umständen abweichende Aufbewahrungsfristen vorgeschrieben. Auch der Kreis der aufzubewahrenden Unterlagen und Informationen ändert sich gegebenenfalls. Dies ist, wie auch nach Handels- und Steuerrecht, im Einzelfall zu prüfen.

Der Einsatz von MailStore Server kann technisch dabei unterstützen, diese E-Mail-Aufbewahrungspflichten zu erfüllen.

Wissen wie & warum

Umfassendes Technologiekonzept

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

Vollständigkeit der Archivierung durch Journaling	▪ 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 hilft MailStore Server die archivierten Daten vor Manipulationen zu schützen. ▪ 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. ▪ Exportierten E-Mails kann eine kryptografische Signatur hinzugefügt werden, um sie auch außerhalb des Archivs vor Manipulationen zu schützen.
Aufbewahrungsrichtlinien	▪ Administratoren können durch individuelle Aufbewahrungsrichtlinien vollständige Kontrolle darüber behalten, wie lange unterschiedliche Arten von E-Mails archiviert werden. ▪ Sie können selbst definieren, ob und wann E-Mails automatisch aus dem Archiv gelöscht werden und somit unterschiedlichen rechtlich vorgegebenen Aufbewahrungsfristen gerecht werden.
Legal Hold	▪ Ist Legal Hold aktiviert, können ungeachtet aller anderen möglichen Konfigurationen, wie der Benutzerrechte und der Aufbewahrungsrichtlinien, keine E-Mails aus dem Archiv gelöscht werden.

Wissen wie & warum

Protokollierung	▪ MailStore Server protokolliert Änderungen und Ereignisse, die vom Administrator definiert werden können, über eine integrierte Auditing-Funktion.
Auditor-Zugriff und Standardkonformität	▪ Über den 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 exportiert und für eine Betriebsprüfung übermittelt werden.

Informationen

Wissen wie & warum

Über MailStore Server

Mit MailStore Server können Unternehmen alle 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 beispielsweise über eine nahtlose Integration in Microsoft Outlook oder über Web Access auf ihre E-Mails zugreifen und diese schnell mit Hilfe einer Volltextsuche durchsuchen.

MailStore Server, mittlerweile in Version 12 verfügbar, hat sich über viele Jahre hinweg und durch den erfolgreichen Einsatz bei über 60.000 Kunden zu einem weltweiten Standard für die E-Mail-Archivierung in Unternehmen entwickelt. Einfach zu installieren, zuverlässig und wartungsarm.

Über die MailStore Software GmbH

Die MailStore Software GmbH aus Viersen bei Düsseldorf, ein Tochterunternehmen von Carbonite (NASDAQ: CARB), einem führenden Anbieter von Data-Protection-Lösungen, zählt zu den weltweit führenden Herstellern von E-Mail-Archivierungslösungen. Über 60.000 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 Service-Provider an, die auf dieser Basis ihren Kunden 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.

Quellenverzeichnis

Wissen wie & warum

- **Seite 4**

[1]http://www.gesetze-im-internet.de/ao_1977/__147.html *
[2]https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0952&from=DE *
[3]https://www.gesetze-im-internet.de/hgb/__257.html *
[4]https://www.gesetze-im-internet.de/gwg_2017/__8.html *
[5]https://www.gesetze-im-internet.de/brao/__50.html *

- **Seite 5**

[6]https://www.gesetze-im-internet.de/hgb/__257.html *
[7]http://www.gesetze-im-internet.de/ao_1977/__147.html *
[8]https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013R0952&from=DE *
[9]https://www.gesetze-im-internet.de/ao_1977/__162.html *
[10]https://www.gesetze-im-internet.de/stgb/__283.html *
[11]https://www.gesetze-im-internet.de/bgb/__280.html *
[12]https://www.gesetze-im-internet.de/bgb/__241.html *
[13]https://www.gesetze-im-internet.de/gewo/__35.html *
[14]https://www.gesetze-im-internet.de/gmbhg/__6.html *

- **Seite 6**

[15]Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=EN *
[16]http://www.gesetze-im-internet.de/zpo/__371a.html *
[17]http://www.gesetze-im-internet.de/zpo/__371a.html *

- **Seite 7**

[18]https://www.gesetze-im-internet.de/ao_1977/__145.html *
[19]https://www.gesetze-im-internet.de/hgb/__238.html *
[20]https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf;jsessionid=627CE0137E8E6292120E17384FF3E431.delivery2-master?__blob=publicationFile&v=9 *

- **Seite 8**

[21]https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf;jsessionid=627CE0137E8E6292120E17384FF3E431.delivery2-master?__blob=publicationFile&v=9 *
[22]https://www.voi.de/downloads/top-10-downloads/ *

- **Seite 9**

[23]https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.pdf;jsessionid=627CE0137E8E6292120E17384FF3E431.delivery2-master?__blob=publicationFile&v=9 *

Quellenverzeichnis

- **Seite 10**

[24]http://www.gesetze-im-internet.de/bdsg_2018/index.html *

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

[26]https://www.gesetze-im-internet.de/tmg/index.html *

- **Seite 11**

[27]https://dsgvo-gesetz.de/erwaegungsgruende/nr-155/ *

[28]Vgl. § 26 Abs. 2 S. 2 und 3 BDSG, https://dsgvo-gesetz.de/bdsg/26-bdsg/; vgl. im Übrigen auch Art. 7 DSGVO, https://dsgvo-gesetz.de/art-7-dsgvo/ *

[29]Auch Gesundheitsdaten sind Daten einer besonderen Kategorie und somit gemäß Art. 9 DSGVO und § 22 BDSG besonders schützenswert, vgl. https://dsgvo-gesetz.de/art-9-dsgvo/ und https://dsgvo-gesetz.de/bdsg/22-bdsg/ *

- **Seite 12**

[30]https://dsgvo-gesetz.de/art-5-dsgvo/ *

[31]https://www.gesetze-im-internet.de/bdsg_2018/__47.html *

[32]https://dsgvo-gesetz.de/bdsg/47-bdsg/ *

[33]https://www.bfdi.bund.de/DE/Datenschutz/Themen/Arbeit_Bildung/BeschaeftigungArbeitArtikel/Bewerbungsunterlagen.html, abgerufen am 30.04.2019 *

[34]hhttp://www.gesetze-im-internet.de/ao_1977/__147.html *

- **Seite 15**

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

[36]https://www.gesetze-im-internet.de/ao_1977/__140.html *

* aufgerufen am 08. Januar 2020

Kontakt

Sprechen Sie uns an!

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

§

Rechtlicher Hinweis

Dieses Dokument dient lediglich der Information und stellt keine Rechtsberatung dar. Es handelt sich lediglich um eine allgemeine Einführung ohne Anspruch auf Vollständigkeit. Im konkreten Einzelfall wenden Sie sich bitte an einen spezialisierten Rechtsanwalt. Eine Gewähr und Haftung für die Richtigkeit aller Angaben wird nicht übernommen.

MailStore Software GmbH
Clörather Str. 1-3
41748 Viersen, Deutschland
Tel.: +49 (0) 2162 50299-0
Fax: +49 (0) 2162 50299-29
E-Mail: sales@mailstore.com
www.mailstore.com