Leitfaden zur E-Mail-Archivierung in Deutschland

IT-Security made in Germany

Stand: 01.10.2015

Leitfaden für den Einsatz von E-Mail-Archivierungsprodukten, der Ihnen technische, wirtschaftliche und gesetzliche Fragestellungen umfassend beantwortet.

Warum Email-Archivierung?

Zum einen aufgrund der Vielzahl an technischen und wirtschaftlichen Vorteilen, zum anderen aufgrund der rechtlichen Notwendigkeit.

Fragen und Antworten zur gesetzeskonformen Email-Archivierung:

1. Warum ist es sinnvoll Emails zu archivieren?
2. Was muss archiviert werden?
3. Wie lange müssen Daten aufbewahrt werden?
4. Wer trägt die Verantwortung und was kann passieren, wenn nicht archiviert wird?
5. Welche Richtlinien gibt es dafür?
6. Gesetzliche Konflikte: Datenschutz versus E-Mail-Archivierung

1. Warum ist es sinnvoll Emails gesetzeskonform zu archivieren?

Geschäftliche Kommunikation in Form von E-Mails und die darin enthaltenen enthalten einen großen Wissens- und Datenpool. Diese Daten dürfen nicht verloren gehen, bzw. sollte doch Verlust vorkommen, müssen sie schnell wieder herzustellen sein.

Der Verlust von Daten – durch Soft- oder Hardwarefehler oder auch durch absichtliche Löschung – kann geschäftskritisch und teuer werden, sollten die Daten wiederhergestellt werden müssen. Manchmal ist ein Wiederherstellen aber auch gar nicht mehr möglich, bzw. oft reicht eine für IT-Systeme übliche Datensicherung/Backup nicht aus.

Außerdem ist der Zeitraum, auf den Sie zurückgreifen können, häufig viel zu gering. Wenn Sie sich beispielsweise am Ende eines zwei Jahre umfassenden Projektes mit dem Kunden über den Projektumfang streiten, wird es keine passende Datensicherung mehr geben. Eine E-Mail-Archivierung hat dieses Problem nicht – E-Mails können direkt und ohne Umwege gesucht, darauf zugegriffen und wiederhergestellt werden. Die Gründe für eine Wiederherstellung sind vielfältig: Im einfachsten Fall geht es um versehentlich gelöschte E-Mails und Dokumente, oftmals soll jedoch etwas im Nachhinein verstanden, bearbeitet oder bewiesen werden. Oder aber: Ein Mitarbeiter verlässt das Unternehmen und sein Nachfolger muss sich in Projekte einarbeiten, Aufträge nachvollziehen, Fehler oder Tätigkeiten Verantwortlichen zuordnen oder dem Finanzamt oder dem Gericht Sachverhalte beweisen.

Zudem sorgen die wachsenden Datenmengen für große Probleme auf Mailservern. Speicherkosten und Lizenzkosten steigen, da nicht mehr genutzte E-Mail-Konten weiter vorgehalten werden müssen und der E-Mail-Verkehr auf diese Weise stetig zunimmt. In der Folge werden Server und Clients immer langsamer, entsprechend schwerer ist es, Informationen in riesigen E-Mail-Beständen (wieder) zu finden. Die Praxis zeigt: Um ihre E-Mail-Konten übersichtlich zu halten, löschen Anwender E-Mails oft vorzeitig oder unüberlegt, und vernichten damit wichtige Daten und Dokumente. Auch ein absichtliches Löschen von E-Mails - evtl. aus kriminellen Gründen – kommt immer wieder vor. Die geltenden gesetzlichen Anforderungen schreiben den Einsatz einer revisionssicheren E-Mail-Archivierung zwingend und umfassend vor. Im Gegensatz zu einem normalen Backup muss somit eine GoBD konforme Archivierungslösung nachweislich dafür sorgen, dass keine Manipulation der archivierten Daten stattgefunden hat. Verschiedene technische Einstellungen beim Archivierungsvorgang sorgen hier für die Beweiswerterhaltung. Dies garantiert im Zweifel vor Gericht oder dem Finanzamt, dass keine Manipulation von archivierten Datenbeständen stattgefunden hat. Rechtskonforme E-Mail-Archivierung erfordert gesetzlich unveränderte und unveränderbare Speicherung über sehr lange Zeiten – z.T. sogar für immer. Viele Archivierungsprodukte entsprechen jedoch nicht den Richtlinien des Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Revisionssicherheit im Sinne der Beweiswerterhaltung vor Gericht, Finanzamt etc. geht damit verloren.

2. Was muss archiviert werden?

Mailen ist eine rechtsrelevante Kommunikationsform geworden. So können z. B. Rechnungen, Angebote, Geschäftsbriefe und sonstige Dokumente sehr viel besser, schneller und kostengünstiger verschickt werden als per Post. So ist der klassische Postversand durch den E-Mail-Verkehr heute zu fast 75% ersetzt worden. Die Kommunikation mit Kunden oder Lieferanten, Buchführung, Personalthemen, medizinische Dokumentation, Akten der Verwaltung etc. unterliegen inzwischen jedoch einer gesetzeskonformen Archivierungspflicht.

Welche Emails müssen GoBD konform archiviert werden und gemäß welcher rechtlichen Grundlage?

Anwendungsgebiete	Aufzubewahrende Dokumente	Rechtsgrundlage
Buchführung	– Elektronische Rechnungen – Handelsbücher – Handelsbriefe – Inventarverzeichnisse – Eröffnungsbilanzen – Jahresabschluss – Lagebericht – Konzernabschluss – Konzernlagebericht – Arbeitsanweisungen – Organisationsunterlagen – Buchungsbelege	§ 238 ff. HGB § 140 AO § 14b UStG
Personalsachen	– Kündigung, Auflösungsvertrag – Befristungsvereinbarung – Arbeitszeitnachweise – Lohn– und Berechnungsnachweis – Beschäftigungsverzeichnis – Ärztliche Bescheinigung, Verzeichnis der Jugendlichen – Integrationsverzeichnis – Beschäftigungsverzeichnis – IOS-, EN-ISO-Normen, ASTM–Methoden – Zulassungsschein, Prüfbefunde – Wahlakten – Befristungsvereinbarung	§ 623 BGB § 2 Abs. 1 Satz 3 NachwG § 16 Abs. 2 ArbZG § 165 Abs. 4 Satz 2 SGB VII § 22 Abs. 3 LadenSchlussG § 41 Abs. 1, 50 Abs. 2 JArbSchG § 80 SGB IX § 13 Abs. 4 Satz 1 und Satz 2 BiostoffVO § 7 der 3. BImSchV § 27 StrlSchVO § 19 WO § 14 Abs. 4 TzBfG
Medizinische Dokumentation	– Ärztliche Dokumentation: z. B. Arztbrief, Patientenkartei; Medikamentenverschreibung – Aufzeichnungen über Röntgenbehandlung: z. B. Röntgenaufzeichnungen, Röntgenbilder	Landesrechtliche Berufsordnungen für Ärzte, z. B. § 10 Abs. 3 BerufsO Ärzte Hessen § 28 Abs. 4 RöntgV
Bankunterlagen	– Vollständige Geschäftsdokumentation: vgl. HGB; z. B. Risikohandbücher – Identifizierungsunterlagen – Dokumente der Wertpapierdienstleistung: z. B. Aufträge	§ 25a Abs. 5 KWG § 9 GWG § 34 WpHG
Akten der Verwaltung	– Haushaltsplan – Haushaltsrechnung – Akten – Öffentlich-rechtliche Verträge – Unterlagen der öffentlich-rechtlichen Verwaltungstätigkeit	§ 33, 33a HGrG § 29 VwVfG § 57 VwVfG § 56 SGB X i.V.m § 3a Abs. 2 VwVfG § 110a SGB IV
Gerichtsakten	– Vollständige Prozessakten – Schriftgut der Bundesgerichte und der Generalstaatsanwaltschaft: z. B. Aktenregister, Namensverzeichnis, Karteien (§ 1 Abs. 2 SchrAG)	§ 298a ZPO SchriftgutaufbewahrungsG

3. Wie lange müssen Daten aufbewahrt werden?

Gängige gesetzliche Aufbewahrungspflichten und -zeiten reichen je nach Dokumentenart von zwei Jahren bis „unbegrenzt“. Die Kommunikation mit Geschäftspartnern – dazu gehört jegliche Korrespondenz, durch die ein Geschäft vorbereitet, abgewickelt, abgeschlossen oder rückgängig gemacht wird – verlangt beispielsweise eine sechsjährige Archivierung. Rechnungen oder Personalakten dagegen müssen 10 Jahre archiviert werden. Gerichtsurteile und Baupläne müssen sogar dauerhaft aufbewahrt werden.

Wie sieht die Praxis aus?

In der Regel sollten E-Mails so archiviert werden, dass das Mindestaufbewahrungsdatum 10 Jahre beträgt. Im normalen Geschäftsbetrieb reicht das meist aus. Das Archivierungssystem sollte es aber zulassen, dass unterschiedliche Archivierungszeiträume gleichzeitig festgelegt werden können und E-Mails automatisch, durch von Ihnen festgelegte Regeln abgelegt bzw. kategorisiert werden können.

Achtung: In bestimmten Berufsgruppen muss beachtet werden, dass andere Aufbewahrungspflichten gelten und das verwendete Archivierungssystem eventuell entsprechend konfiguriert werden muss. Insbesondere Ärzte und Anwälte sind hiervon vermehrt betroffen.

4. Wer trägt die Verantwortung und was kann passieren, wenn nicht archiviert wird?
Betriebe müssen den Zugriff seitens der Steuerbehörden auf die oben angegebenen Emails langfristig sicherstellen. Dies ist gesetzlich zwingend vorgeschrieben. Die Verantwortung liegt daher in jedem Fall beim zuständigen EDV-Leiter und schlussendlich natürlich auch beim Geschäftsführer. Kommen Geschäftsführer den gesetzlichen Pflichten nicht nach, drohen in schweren Fällen Geldbußen oder sogar Freiheitsstrafen.

5. Welche Richtlinien gibt es dafür?
Eine Reihe von Gesetzen und Verordnungen stellen E-Mails bereits Briefen gleich. Verträge können per E-Mail geschlossen werden und die elektronische Post hat vor Gericht volle Beweiskraft erlangt. In Deutschland gibt es eine Reihe von Compliance-Anforderungen:

- HGB (Handelsgesetzbuch)
- AO (Abgabenordnung)
- GDPdU (Grundsatze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
- Basel II
- die TR 03125 des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

All diese Gesetze und Verordnungen beeinflussen die Verwaltung von E-Mails. Wenn eine E-Mail eine elektronische Signatur mit qualifizierten Zeitstempeln entsprechend dem Signaturgesetz trägt, wird sie als ein rechtsverbindliches Original betrachtet. Dementsprechend muss der Anwender sie zentral verwalten und langfristig sichern. Qualifizierte Zeitstempel von einem Trustcenter sind deshalb für die Beweiswerterhaltung von archivierten Dokumenten unabdingbar. Da Verschlüsselungen mit der Zeit jedoch unsicher werden und gehackt werden können und damit eine Manipulation von Daten in Zukunft möglich würde, ist es äußerst wichtig, auch bereits signierte Dokumente von Zeit zu Zeit wieder mit anderen, besseren kryptografischen Algorithmen neu zu signieren. Idealerweise und zur Sicherheit sollte dies in einer Archivierungslösung täglich und automatisch geschehen.

Wie sieht die Praxis aus?
Grundsätzlich müssen alle relevanten E-Mails inkl. ihrer Anhänge vollständig, manipulationssicher und jederzeit verfügbar archiviert werden. Die Daten müssen in dem Format vorliegen, in dem sie ursprünglich waren, d. h. ein Formatwechsel darf nicht stattgefunden haben. Gleichzeitig müssen sie maschinell auswertbar sein.

Anforderungen an eine revisionssichere E-Mail-Archivierung
Einen Leitfaden* stellen die Informationen 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 muss von einem sachverständigen Dritten jederzeit überprüfbar sein
- Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein

BSI-Richtlinie TR 03125
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat hierzu die technische BSI-Richtlinie TR 03125 zur Beweiswerterhaltung kryptographisch signierter Dokumente bereitgestellt. Diese beschreibt genau, wie E-Mails und andere elektronische Dokumente archiviert werden müssen, um den jetzigen und zukünftigen Erfordernissen des Gesetzgebers und der Beweiswerterhaltung zu genügen. Weiterführende Informationen zur Aufbewahrung elektronisch signierter Dokumente sind im Handlungsleitfaden des Bundesministeriums für Wirtschaft und Technologie beschrieben.

BSI-Richtlinie TR 03125
Siehe auch: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

Handlungsleitfaden zur Aufbewahrung elektronisch signierter Dokumente Im Verwaltungs- und Unternehmensbereich wird das Aufkommen elektronischer und elektronisch signierter Dokumente in den kommenden Jahren drastisch zunehmen. Die rechtsichere Behandlung dieser Dokumente wird hier näher erläutert: http://www.securepoint.de/fileadmin/securepoint/downloads/uma/bmwi-leitfaden.pdf

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

6. Gesetzliche Konflikte: Datenschutz versus E-Mail-Archivierung

Die Einführung der GoBD konformen Aufbewahrung von E-Mails, kollidiert häufig mit anderen Gesetzen oder Richtlinien.

Fallstrick Betriebsvereinbarung zur privaten E-Mail-Nutzung

Vielfach wird davon ausgegangen, dass eine private Nutzung des beruflichen E-Mail-Kontos nicht mit der Archivierung in Konflikt steht, wenn der Mitarbeiter mittels einer Betriebsvereinbarung zugestimmt hat. Theoretisch ist das auch zutreffend. In der Praxis tauchen dann jedoch Fallstricke auf, da Mitarbeiter zwar ihre eigenen, durch das Fernmeldegeheimnis geschützten Rechte abtreten können, jedoch nicht das Recht ihrer externen Kommunikationspartner, deren Kommunikation ja ebenfalls archiviert werden würde.

Private Inhalte in berufliche E-Mails

Auch berufliche E-Mails können datenschutzrechtlich relevante, personenbezogene Inhalte besitzen, denn eine berufliche E-Mail ist beispielsweise auch die Kommunikation eines Mitarbeiters mit einem Betriebsarzt. Einige deutsche IT-Rechtler vertreten jedoch 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 Archivierungslösung informieren.

Automatische Archivierung aller E-Mails und private Nutzung

Es wäre praxisfremd alle ein- und ausgehenden E-Mails dahingehend zu überprüfen, ob es sich um archivierungspflichtige oder nicht archivierungspflichtige E-Mails handelt. Da die Archivierung jedoch in jedem Fall vollständig sein soll, muss die sofortige und automatische Archivierung bei Ein- und Ausgang gewährleistet sein, um mögliche Manipulationen zu unterbinden. Diese Archivierungsstrategie kann aber wie bereits erwähnt in Konflikt mit den Datenschutzrichtlinien stehen. Ist Mitarbeitern z. B. die private E-Mail-Nutzung gestattet, unterliegt der Arbeitgeber als Telekommunikationsanbieter dem Bundesdatenschutzgesetz (BDSG) und dem Telekommunikationsgesetz (TKG).

Untersagung der privaten E-Mail-Nutzung

Die beste und – streng genommen – einzige Lösung ist daher, dem Mitarbeiter aus vorgenannten Gründen die Nutzung des beruflichen E-Mail-Kontos für private Zwecke explizit zu untersagen.
Dies muss mit dem Mitarbeiter besprochen und schriftlich fixiert werden. Die regelmäßige Überprüfung dieser Maßnahme ist ebenfalls notwendig, um rechtlichen Bestand zu haben.

Best Practice/Lösung:

In Anbetracht der gesetzlichen Richtlinien ist das Verbot der privaten Nutzung beruflicher E-Mail-Konten der einzige Weg, um Konflikte zwischen Datenschutz und der gesetzlich vorgeschriebenen Archivierung von E-Mails zu vermeiden. Da die meisten Mitarbeiter heutzutage Smartphones und Tablets besitzen, können sie ohnehin jederzeit problemlos privat kommunizieren.

Die Christo.Net GoBD konforme Email Archivierungs-Lösung

Die komplexen Anforderungen des Gesetzgebers werden in vollem Umfang erfüllt. Die Archivierung erfolgt gesetzeskonform, revisionssicher und automatisch.

Übersicht:

- 100-prozentige Archivierung aller ein-/ausgehenden und internen E-Mails für beliebig lange Zeiträume
- Indizierung von E-Mails (Volltextsuche)
- Nur für autorisierte Personen
- Gesetzeskonforme, revisionssichere und automatische Archivierung des E-Mail-Verkehrs
- Sicherer Schutz vor Rechtsnachteilen wie z.B. steuerlichen Schätzungen, Beweisverlusten, Gutachten, Prozessen etc.
- Einfaches Wiederfinden und Wiederherstellung von versehentlich oder absichtlich gelöschten E-Mails
- Keine Anpassung oder Konfiguration erforderlich
- Entlastung Ihres bestehenden E-Mailservers
- Kostengünstiger, vollautomatischer Betrieb – Sie müssen nichts tun!

! Dieses Dokument dient der unverbindlichen Information und ist keine Rechtsberatung. Alle Angaben sind ohne jede Gewähr. Bitte lassen Sie sich in jedem Fall von einem Anwalt beraten!