Merkblatt E-Mail-Archivierung

Alle Geschäftsbriefe in elektronischer Form sind gemäß §257 HGB, § 147 AO und den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)[1] aufzubewahren.

I. Allgemeine Grundsätze der E-Mail-Archivierung

Folgende Anforderungen sind an den Prozess der E-Mail-Archivierung zu stellen:

- Die Archivierung hat **vollständig** und zum **frühestmöglichen Zeitpunkt** zu erfolgen.
- Die Dokumente müssen **unverändert (manipulationssicher)** abgelegt werden.
- Die **Zugriffsrechte** müssen eingeschränkt werden.
- Jede Änderung muss **protokolliert** werden.
- Beim Einsatz eines externen Dienstleisters müssen **Kontrollmöglichkeiten** hinsichtlich einer ordnungsgemäßen Archivierung bestehen.

II. Datensicherheit

Die Datensicherheit ist bei der E-Mail-Archivierung ein Qualitätsmerkmal. Kann diese nicht gewährleistet werden, können die Daten nicht als Beweis[2] genutzt werden. Das Bundesamt für Sicherheit in der in der Informatik (BSI) hat dazu wesentliche Richtlinien zur Beweiserhaltung kryptografisch signierter Dokumente[3] aufgestellt.

- **Integrität und Authentizität:** Eine ordnungsgemäße Aufbewahrung muss mittels technischer und organisatorischer Maßnahmen auch über einen längeren Zeitraum sichergestellt werden.[4] Etwaige Anforderungen an den Daten- und Geheimhaltungsschutz müssen auch im Langzeitarchivierungssystem z. B. Verschlüsselung, Pseudonimisierung erhalten bleiben.
- **Manipulationssicherheit:** Es muss sichergestellt werden, dass Manipulationen ausgeschlossen sind, dies kann zum Beispiel mit einem qualifizierten Zeitstempel[5] sichergestellt werden. Kann dies nicht nachgewiesen werden ist die Vertrauenswürdigkeit nicht gegeben.

---

[1] Die GoBD sind ab dem 1. Januar 2017 uneingeschränkt anzuwenden.
[2] Die Zulassung als Beweismittel von elektronischen Dokumenten muss gemäß § 286 ZPO geklärt werden.
[3] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html#doc6617308bodyText1
[4] Die Lesbarkeit und Verfügbarkeit der Speichermedien und Datenformate muss unabhängig von den einzelnen Produkten und Herstellern gewährleistet werden.
[5] Rahmenbedingungen für eine elektronischen Signatur werden in der eIDAS-Verordnung aufgestellt.

- **Suchalgorithmus:** Für den Fall, dass Dokumente wieder aufgerufen werden müssen, ist eine entsprechend verlässliche Indexierung und Verwaltung beim Archivsystems vorzuhalten.
- **Zugriffseinschränkungen:** Der Zugriff muss eingeschränkt werden und auch erhalten bleiben, wenn ein Systemwechsel stattfindet.
- **Schnittstellen und Komponente:** Das Archivsystems sollte neben der Verfügbarkeit und Lesbarkeit der elektronischen Unterlagen auch Funktionen besitzen mit denen die Verkehrsfähigkeit beibehalten wird und nach Ablauf der Aufbewahrungsfrist muss eine datenschutzkonforme Löschung[6] möglich sein.
- **Nachweisbarkeit und Protokollierung:** Jegliche Einstellungsänderungen, Zugriffsvorgänge (auch unberechtigter Weise) und Löschung von Daten müssen nachvollziehbar dokumentiert sein.
- **IT-Infrastruktur:** Weiterhin müssen auch die IT-Systeme oder die eingesetzten IT-Dienstleister den hier aufgezählten Anforderungen gerecht werden. Das bedeutet zum Einen, dass entsprechende Hard- und Software (z. B. redundante Systeme, Notfallplan) eingesetzt wird und zum Anderen angemessene technische und organisatorische Kontrollmöglichkeiten vorliegen.

III. Anforderungen an das Archivierungsverfahren

Das BSI setzt voraus, dass vor dem Einrichten eines elektronischen Archivsystems über die technischen Systeme und relevanten Prozesse ein IT-Sicherheitskonzept erstellt wird.

Folgende Mindestanforderungen sind bei der Auswahl des Archivierungssystems zu berücksichtigen:

1. Langfristig verkehrsfähige und standardisierten Datenformate (z. B. PDF oder XML)
2. Rechtscharakter mit einer elektronischen Signatur, einschließlich der erforderlichen Verifikationsdaten
3. Funktion zum Prüfen von Signaturen
4. Bereitstellung einer vertrauenswürdigen Anzeigemaske (Trusted Viewer)[7]
5. Schnittstellenfunktionalitäten zur Ablage und zum Löschen[8] der zu archivierenden Dokumente und Daten sowie eine Schnittstelle zur Bereitstellung des technischen Nachweises der Authentizität und Integrität[9]

[6] Die Löschung von Daten mittels eines Löschantrags z. B. bei Ablauf der Aufbewahrungsfrist muss eine Begründung beinhalten.
[7] Die Anwendungsumgebung muss durch eine anerkannte Bestätigungsstelle gemäß §18 SigG überprüft worden sein.
[8] Keine Initiierung durch das Archivierungssystem.

6. Protokollierung durchgeführter Archivaktivitäten
7. Verwaltung und Zuordnung der Archivdaten zu den zugehörigen Geschäftsprozessen und den Ablageorten der archivierten Daten
8. Zugriffsschutzmechanismen auf Grundlage eines zuverlässigen und konfigurierbaren Berechtigungssystems

IV. Sonderfälle bei der Archivierung

Besondere personenbezogene Daten wie Daten über Personalangelegenheiten (z. B. Krankenschein, Betriebsratskommunikation) oder Bewerbungsunterlagen unterliegen einem besonderen Schutzniveau und sollten daher nicht in den allgemeinen Sammelordnern archiviert werden, sondern getrennt aufbewahrt werden. Insbesondere Bewerbungsunterlagen sind gemäß § 58 Abs. 2 DSAnpUG-EU/BDSG n.F.; § 35 Abs. 2 BDSG a.F. zu löschen, wenn der Zweck der Speicherung entfallen ist, aufgrund ggf. gerichtlicher Überprüfbarkeit durch das Allgemeine Gleichbehandlungsgesetz (AGG) ist eine entsprechende Zurückbehaltung von max. 6 Monaten angemessen. Es bietet sich an, gerade für Bewerbungen, einen extra E-Mail-Account einzurichten. Dieser sollte zudem die Möglichkeit einer Verschlüsslung bieten und getrennt von der allgemeinen E-Mail-Kommunikation abgelegt werden. Analog sollte auch E-Mail-Verkehr mit der Personalabteilung im Rahmen des Beschäftigtendatenschutzes verwaltet werden.

Problemfelder mit der E-Mail-Archivierung ergeben sich, wenn es den Mitarbeitern gestattet wird den betrieblichen E-Mail-Account zur privaten Kommunikation zu nutzen.

Weiterhin sollte auch die datenschutzrechtliche Transparenz über den Einsatz eines E-Mail-Archivierungs-Systems bei den Kommunikationspartnern gewahrt werden. Es bietet sich daher an Informationen zur E-Mail-Archivierung in die Datenschutzerklärung aufzunehmen.

V. Beispiele für E-Mail-Archivierungs-Programme

Es gibt verschiedene auf dem Markt erhältliche Programme zur E-Mail-Archivierung. Laut eigenen Angaben erfüllen beispielhaft die folgenden E-Mail-Archivierungsprogramme der Firmen: MailStore Software GmbH, Securepoint GmbH und Reddoxx GmbH grundsätzlich die Anforderungen des BSI[10].

Sofern im Rahmen des Einsatzes eines Programms zusätzliche Services (Support- und Fernwartung, Cloud-Dienstleistungen) in Anspruch genommen werden. Kann es im Einzelfall notwendig sein eine

---

[9] Verschlüsselung der Kommunikation über die Schnittstellen (Middleware, externe Anbieter oder Dienstleister).

[10] Laut eigenen Angaben den der Dienstleister/ Hersteller nach Stand: Quartal I 2017.

Datenschutz-Folgenabschätzung (Vorabkontrolle des Bundesdatenschutzgesetzes) durchzuführen bzw. eine vertragliche Grundlage durch Abschluss einer Auftragsdatenverarbeitung zu schaffen.

Gerne unterstützen wir Sie aus datenschutzrechtlicher Sicht bei der Auswahl des E-Mail-Archivierungs-Programms.