

Ist die Zustimmung zur Archivierung durch eine Betriebsvereinbarung eine Alternative?

Bisweilen wird die Auffassung vertreten, dass die private Nutzung des geschäftlichen eMail-Accounts und eMail-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 eMails von Außenstehenden archiviert würden und deren Recht auf Datenschutz verletzt würde, erscheint dieses Vorgehen nicht als zielführende Alternative.

Konflikte bei dienstlichen eMails mit personenbezogenen Inhalten

Es existieren darüber hinaus noch gewisse Unsicherheiten, selbst wenn die private Nutzung der geschäftlichen eMail-Accounts explizit untersagt ist: Beispielsweise können auch dienstliche eMails 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 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).

Sonderfall „E-Mails an den Betriebsrat“

eMails an den Betriebsrat stellen ebenfalls sensible Informationen dar und unterliegen einem gesteigerten Persönlichkeitsrecht.

In der Praxis

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

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) und dem Schutz des eingerichteten und ausgeübten Gewerbebetriebes des Arbeitgebers (Art. 14 Abs. 1 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 eMail-Archivierung gemäß § 4 Abs. 3 BDSG nachkommen und alle Mitarbeiter vor der Implementation einer entsprechenden Lösung informieren.

Grauzone: Spam-Filterung vor der Archivierung

Die Spam-Filterung vor der Archivierung birgt grundsätzlich das Risiko, dass archivierungspflichtige eMails 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) eMail-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 eMails 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 eMails nicht zu 100% sichergestellt werden. Diese eMails können fälschlicherweise vom Spam-Filter abgewiesen werden. Das Verfahren geht demnach mit einem gewissen rechtlichen Risiko einher. Daher sollten die als Spam identifizierten eMails – soweit möglich – in regelmäßigen Abständen kontrolliert werden. Geschäftsrelevante eMails, die fälschlicherweise als Spam aussortiert wurden, können in diesem Fall nachträglich archiviert werden.
Als Spam identifizierte eMails werden noch vor Annahme durch den eigenen eMail-Server abgewiesen	Solange als Spam identifizierte eMails nicht angenommen werden, besteht auch keine Pflicht zur Verarbeitung oder zur Archivierung dieser eMails. Technisch gesehen darf die Annahme der eMail nicht mittels Statuscode 250 vom SMTP-Server „quittiert“ werden. In diesem Fall ist nicht der eigene, sondern der zustellende eMail-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 eMails 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:

- Vorschriften des Handels- und Steuerrechts über die Ordnungsmäßigkeit der Buchführung (§§ 238 ff. und § 257 HGB sowie §§ 140 ff. AO)
- IDW Stellungnahme zur Rechnungslegung „Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)“
- Die „Grundsätze zur ordnungsgemäßen 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.

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 eMails) 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 eMails im Unternehmen. eMails können beispielsweise noch vor der Zustellung in die Postfächer der Mitarbeiter archiviert werden.
Originalgetreue Archivierung	Archivierte eMails stimmen in jeder Hinsicht mit dem Original überein und können bei Bedarf ohne Informationsverlust aus dem Archiv heraus wiederhergestellt werden.
Manipulationssicherheit	<ul style="list-style-type: none"> - Durch Bildung von SHA-Hashwerten über die Inhalte der eMails 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 eMail-Inhalte ist weder in der grafischen Oberfläche noch programmintern vorgesehen. - Eine kryptografische Signatur, die man exportierten eMails hinzufügen kann, stellt sicher, dass exportierte eMails selbst außerhalb des Archivs vor Manipulationen geschützt bleiben.
Aufbewahrungsfristen	<ul style="list-style-type: none"> - Grundsätzlich kann kein Benutzer, solange die Standard-Benutzerrechte nicht aktiv vom Administrator geändert werden, eMails 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 eMails 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	<ul style="list-style-type: none"> - 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 eMails 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 alle Vorteile moderner eMail-Archivierung einfach und sicher für sich nutzbar machen. Dazu legt MailStore Server Kopien aller eMails in einem zentralen eMail-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 eMails zugreifen und diese in höchster Geschwindigkeit durchsuchen.

