Leitfaden E-Mail-Management

Rechtliche Grundlagen
und praktische Umsetzung

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner und Projektleitung:

Frank Früh | Bitkom e. V.
T +49 030 27576-201 | f.frueh@bitkom.org

Verantwortliches Bitkom-Gremium

AK Input- & E-Mail-Management

Autoren

- Gesa Diekmann, Bitkom e.V.
- Marc Drögsler, inovoo GmbH
- Steffen Ewald, ELO Digital Office GmbH
- Frank Früh, Bitkom e.V.
- Stephan Gehling, H &S Heilig und Schubert InformationsManagement GmbH
- Sven Gelzhäuser, 1&1 De-Mail GmbH
- Stefan Groß, PSP Peters Schönberger GmbH Wirtschaftsprüfungsgesellschaft
- Daniel Mikeleit, ELO Digital Office GmbH
- Julia Schubert, Bitkom e.V.
- Andreas Schulz, Bitkom Servicegesellschaft mbH
- Antje Sommer, Retarus GmbH
- Jürgen Vogler, Mentana Claimsoft GmbH

Die Autoren bedanken sich beim Bitkom Arbeitskreis Input & E-Mail-Management und insbesondere bei Klaus Gettwart, Mail ConsultGmbH, sowie Tobias Kühn, Bitkom Consult, für die zahlreichen Hinweise und das Feedback im Rahmen der Erarbeitung dieser Publikation.

Inhaltsverzeichnis

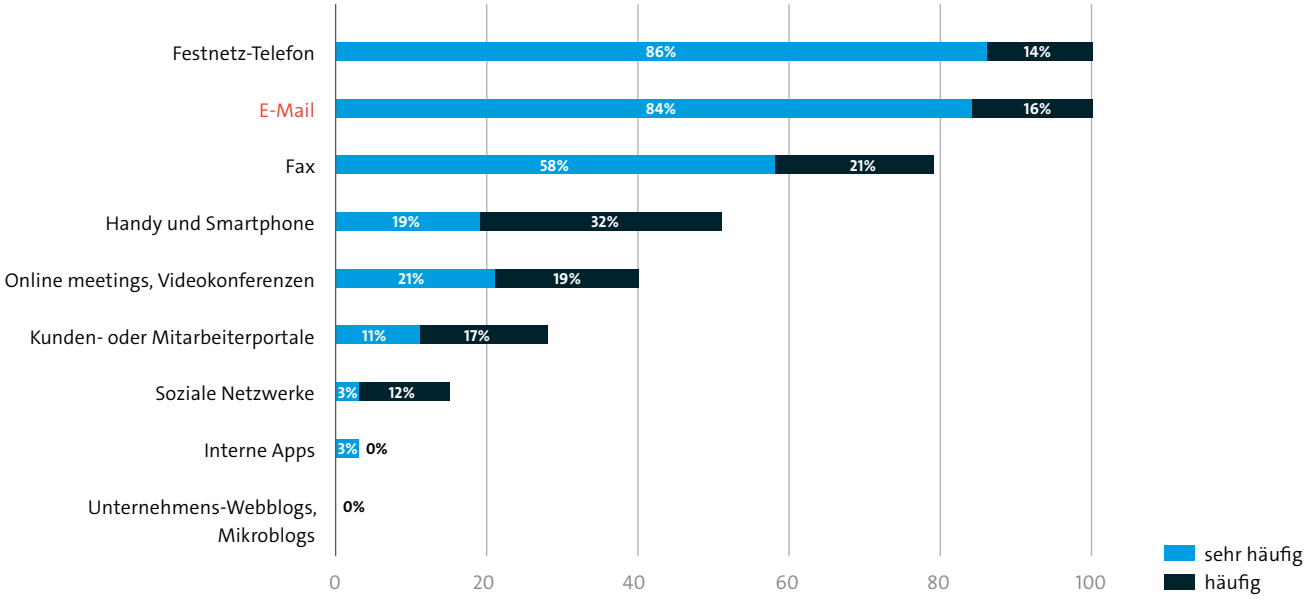
1 Einleitung

1 Einleitung

Die E-Mail ist aus dem Geschäftsleben kaum wegzudenken. Es gibt in Deutschland faktisch kein Unternehmen mehr, welches sich nicht der E-Mail als Kommunikationskanal bedient. Neben Telefonie ist E-Mail das wichtigste Medium, um mit Geschäftspartnern, Kunden und Kollegen zu kommunizieren. Gemäß einer Bitkom-Untersuchung erhält jeder Mitarbeiter eines deutschen Unternehmens im Schnitt 18 geschäftliche E-Mails am Tag[1]. Da wundert es nicht, dass sich Unternehmen Gedanken darüber machen, wie Sie mit ihren E-Mails optimal umgehen. E-Mail-Management-Systeme, die oftmals Teil einer Enterprise-Content-Management-Lösung (ECM- Lösung) sind, helfen hier den Überblick zu bewahren, Kommunikation zu verfolgen und zu optimieren.

Die E-Mail ist Standard in der Unternehmenskommunikation

Wie häufig kommen die folgenden Kommunikationskanäle für die interne und externe Kommunikation in Ihrem Unternehmen zum Einsatz?



Quelle: Bitkom, Digital Office Index, 2016
Basis: Unternehmen ab 20 Mitarbeiter (n=1.108)

Abbildung 1: Digital Office Index (Repräsentative Untersuchung zum Digitalisierungsgrad von Büro- und Verwaltungsprozessen in deutschen Unternehmen)

Natürlich gibt es auch noch eine ganze Reihe weiterer Kanäle, über die geschäftsrelevante Informationen ins Unternehmen fließen. So werden bspw. immer mehr Absprachen über Social Media und Kollaborationsplattformen getroffen. Dies gilt sowohl bei der Kommunikation des Unternehmens mit dem Konsumenten (der Kunde bestellt einen Servicetechniker per Facebook) als auch in der Business-to-Business-Kommunikation (Verträge werden gemeinsam

1 Vgl. ↗Bitkom-Presseinformation

online erarbeitet). Eine zentrale Betrachtung aller Kommunikationskanäle in einem Omni-Channel-Input-Managementsystem wird für den reibungslosen Kommunikationsprozess immer wichtiger. In dieser Publikation wird nur das Thema E-Mail fokussiert, wenngleich die getätigten Aussagen oftmals auch für andere Kanäle gelten.[2]

Während es beim **E-Mail-Management**[3] um die optimale Verarbeitung und Beantwortung der Kommunikation geht, handelt es sich bei der **E-Mail-Archivierung** um ein Konzept bzw. System, welches der langfristigen, unveränderlichen und sicheren Aufbewahrung elektronischer Nachrichten dient.

Die Verantwortung für die Einführung einer vorschriftsgemäßen E-Mail-Archivierung liegt grundsätzlich in den Händen des Vorstands bzw. Geschäftsführung eines jeden Unternehmens.[4] Der Treiber der Einführung von E-Mail-Management und -Archivierung sollte ohnehin im Idealfall die Geschäftsführung oder Organisationsleitung sein, da eine ganzheitliche Prozessbetrachtung erforderlich ist und die eingesetzte Technik nur ein Mittel zum Zweck darstellt. Da alle betrieblichen Bereiche tangiert werden, ist es – das zeigt die Erfahrung – sehr wichtig, einen erweiterten Lenkungsausschuss für das Einführungsprojekt mit folgendem Teilnehmerkreis zu besetzen:

- IT-Leitung und -Administration für alle technischen Belange
- Datenschutzbeauftragter zur Klärung und Absicherung datenschutzrechtlicher Fragen
- Vertreter des Betriebsrats[5]
- Key-User aus den Fachabteilungen nach Bedarf.

In dieser Publikation werden zunächst die rechtlichen Grundlagen und Beweggründe für die Einführung eines E-Mail-Managements dargelegt. Dann wird auf die verschiedenen zur Verfügung stehenden Möglichkeiten der Archivierung eingegangen und die rechtlichen Vorschriften eingehend untersucht. Ein gesondertes Kapitel haben die Autoren den Risiken und Sonderfällen in der Praxis gewidmet. Zum Abschluss werden dem Leser zehn Praxistipps mit auf den Weg gegeben, die er bei der Einführung von E-Mail-Management beherzigen sollte.

2 Hinweis: Die Anbindung von Social Media erfolgt zum einen über Konnektoren, die eine native Anbindung der Quelle erlauben, zum anderen über die Übermittlung der relevanten Informationen von der Quelle an das Archivsystem. So bieten zum Beispiel diverse Sofortnachrichtendienste die Option, die erzeugten Chatnachrichten im Mailclient abzulegen, um diese von dort über E-Mail-Management-Systeme zu verarbeiten.

3 In der Fachliteratur wird synonym auch oft die Bezeichnung E-Mail Response Management System (ERMS) verwendet.

4 Vgl. hierzu auch die weiteren Ausführungen zu den Rechtsfolgen der Verletzung der gesetzlichen Vorgaben in Kapitel 2.

5 Es gibt zwar nur bei manchen Aspekten des E-Mail-Managements ein Mitbestimmungsrecht des Betriebsrats, dieser stellt jedoch auch ohne ein solches einen wichtigen Partner im Projekt dar, um die Anwenderakzeptanz zu erhöhen.

2 Rechtliche Grundlagen

2 Rechtliche Grundlagen

Abhängig vom Land, in dem ein Unternehmen tätig ist, muss es unterschiedliche Gesetze, Vorschriften und Normen beachten, die teilweise gravierend von den in Deutschland gültigen Regelungen zum Umgang mit E-Mails abweichen. In diesem Leitfaden wird nur auf die in Deutschland gültigen rechtlichen Vorschriften eingegangen.

Allgemeine rechtliche Vorschriften

Geschäftliche Unterlagen werden bzw. müssen über einen bestimmten Zeitraum archiviert und aufbewahrt werden. Diese Verpflichtung zur Archivierung folgt nicht aus einem einzigen Gesetz, sondern ergibt sich national aus einer Vielzahl von Vorschriften. Insbesondere ergeben sich Aufbewahrungs- bzw. Archivierungsfristen aus der Abgabenordnung (AO) und dem Handelsgesetzbuch (HGB) und damit aus dem Steuer- sowie Handelsrecht. Nach § 146 Abs. 2 AO sind »Bücher und die sonst erforderlichen Aufzeichnungen (...) im Geltungsbereich dieses Gesetzes (...) aufzubewahren«. Zudem ist in § 257 Abs. 1 HGB verankert, dass die dort erwähnten »Unterlagen« geordnet aufbewahrt werden müssen.

Eine wesentliche Vorschrift im Kontext der Aufbewahrung elektronischer Unterlagen und mithin E-Mails bilden die »Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« (GoBD). Demnach sind aufzeichnungs- und aufbewahrungspflichtige Daten, Datensätze, elektronische Dokumente und elektronische Unterlagen, welche im Unternehmen entstanden oder dort eingegangen sind, auch in dieser Form aufzubewahren und dürfen vor Ablauf der Aufbewahrungsfrist nicht gelöscht werden. E-Mails mit der Funktion eines Handels- oder Geschäftsbriefs oder eines Buchungsbelegs sind entsprechend den GoBD in elektronischer Form aufbewahrungspflichtig.

Neben den bereits erwähnten Bestimmungen können sich Aufzeichnungspflichten bspw. auch aus dem Telekommunikationsgesetz (TKG), dem Bundesdatenschutzgesetz (BDSG) oder dem Sarbanes-Oxley Act (SOX) ergeben, aber auch aus den §§ 91 ff. Aktiengesetz (AktG), den §§ 41 ff. GmbH-Gesetz, Umsatzsteuergesetz (§ 14 b Abs. 1 UStG) und Genossenschaftsgesetz (§ 33 GenG). Branchenabhängige Regelungen wie die Röntgenverordnung, REACH Chemikalienverordnung oder das Wertpapierhandelsgesetz sowie die Apothekenbetriebsordnung, Gewerbeordnung, das Kreditwesengesetz oder Versicherungsaufsichtsgesetz enthalten ebenfalls Aufzeichnungspflichten.

Was muss archiviert werden?

Ein Steuerpflichtiger muss nach § 147 AO »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 (...)« und »(...) sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung« sind, aufbewahren.

Kaufleute werden aufgrund § 257 Abs. 1 HGB verpflichtet, folgende Unterlagen geordnet aufzubewahren:

- Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, Einzelabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
- die empfangenen Handelsbriefe,
- Wiedergaben der abgesandten Handelsbriefe und
- Belege für Buchungen in den zu führenden Büchern (Buchungsbelege).

Handelsbriefe sind nach § 257 Abs. 2 HGB Schriftstücke, die ein Handelsgeschäft betreffen und dienen damit der Vorbereitung, dem Abschluss, der Durchführung, der Änderung oder der Rückgängigmachung eines Handelsgeschäftes. Nicht nur »Geschäftsbriefe« in Papierform fallen hierunter, sondern auch elektronische Nachrichten wie E-Mails, De-Mails[6], Faxe, Telegramme etc.

Nicht nur die als Handels- oder Geschäftsbrief einzustufenden empfangenen E-Mails bzw. eingehende elektronische Post müssen geordnet aufbewahrt werden (vgl. § 257 Abs. 1 Nr. 2 HGB), sondern es sind auch Kopien der abgesandten E-Mails (Handelsbrief) zurückzubehalten und aufzubewahren, §§ 238 Abs. 2, 257 Abs. 1 Nr. 3 HGB. E-Mails mit der Funktion eines Handels- oder Geschäftsbriefs oder eines Buchungsbelegs sind damit in elektronischer Form aufbewahrungspflichtig. Deshalb sind E-Mails, welche nur als »Transportmittel« dienen und darüber hinaus keine aufbewahrungspflichtigen Informationen enthalten, nicht aufbewahrungspflichtig (vgl. Rdnr. 121 GoBD).[7] Eine E-Mail mit beigefügter elektronischer Rechnung ist also wie ein Papierbriefumschlag anzusehen, sofern keine aufbewahrungspflichtigen Informationen enthalten sind.

»E-Mails sind Handelsbriefe, sofern sie der Vorbereitung, dem Abschluss, der Durchführung, der Änderung oder der Rückgängigmachung eines Handelsgeschäftes dienen.«

Beginn und Dauer der Aufbewahrungsfrist

Die Aufbewahrungsfrist[8] aus steuerlicher Sicht beginnt mit Ablauf des Kalenderjahres, in dem die letzte Eintragung in die Bücher vorgenommen wurde, der letzte Beleg entstanden ist oder beim Empfang oder Versand des letzten Handels- oder Geschäftsbriefs. Regelmäßig handelt es sich dabei um das Jahr der Bilanzaufstellung (§ 147 Abs. 4 AO). Steuerlich maßgebend für den Beginn des Fristablaufs ist demgemäß der Zeitpunkt, in dem die letzte Buchung vorgenommen wurde. Es wird nicht auf den Geschäftsvorfall sondern auf den Buchungsvorgang selbst bzw. die Schaffung des Belegs abgestellt. Rechnungen sind auf der Grundlage von § 14b Abs. 1 UStG zehn Jahre aufzubewahren. Die Aufbewahrungsfrist beginnt dabei nach § 14b Abs. 1 S. 3 UStG mit Ablauf des Kalenderjahres, in dem die Rechnung ausgestellt wurde.

6 Soweit in diesem Dokument keine anderen Angaben gemacht werden, gelten die Ausführungen zur E-Mail gleichermaßen für De-Mail und weitere gesonderte Verfahren wie EGVP und beA.

7 Hinweis: Der Bitkom Arbeitskreis ECM-Compliance hat sich ausführlich mit dem Thema E-Mail und GoBD auseinandergesetzt. Auf der ↗Webseite finden sich eine Reihe von Publikationen zur Vertiefung des Themas.

8 Wenn signierte Anhänge in einer E-Mail vorhanden sind, die eine Willensbekundung/Vertragsschluss im Sinne des Schriftformersatzes beinhalten oder die Mail als solche einen signierten Vertragsschluss darstellt, so können andere Fristen gelten.

Dabei müssen die empfangenen Handels- oder Geschäftsbriefe, die Wiedergabe der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, für sechs Jahre aufbewahrt werden (vgl. § 147 Abs. 3 AO). Handelsrechtlich sind die empfangen sowie die Wiedergabe der abgesandten Handelsbriefe ebenfalls über einen Zeitraum von sechs Jahren aufzubewahren (§ 257 Abs. 4 HGB).

Dagegen müssen Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen, die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen, Buchungsbelege etc. grundsätzlich zehn Jahre lang aufbewahrt werden (vgl. § 147 Abs. 3 AO sowie § 257 Abs. 4 HGB).

Da die Abgrenzung zwischen »Handelsbrief« (6 Jahre) und »steuerlich relevant« (10 Jahre) oftmals nicht eindeutig oder nur mit erheblichem Aufwand machbar ist, wird in der Praxis meistens generell die längere Aufbewahrungsfrist angewandt.

»In der Praxis wird zumeist für alle Dokumente eine einheitliche Aufbewahrungsfrist festgelegt, nämlich die längste relevante.«

Besonderheiten der GoBD

Die GoBD enthalten zahlreiche Besonderheiten, die es in Bezug auf die Behandlung von E-Mails zu beachten gilt. Diese sollen nachfolgend kurz dargestellt werden.

Von besonderer Bedeutung im E-Mail-Kontext ist das Kriterium der Ordnung, dessen Erfüllung zumeist größerer Anstrengungen bedarf, als dies beispielsweise bei gescannten Papierdokumenten oder automatisiert erzeugten Ausgangsrechnungen der Fall ist. Für E-Mails bedeutet dies, dass diese mittels einer Indexstruktur identifizierbar und klassifizierbar sein müssen sowie insbesondere eine eindeutige Zuordnung zum jeweiligen Geschäftsvorfall möglich sein muss. Dazu sind auch die weiteren innerhalb der GoBD benannten Anforderungen (Vollständigkeit, Unveränderbarkeit, keine Einschränkung der maschinellen Auswertbarkeit) zu gewährleisten.

E-Mails mit der Funktion eines Handels- bzw. eines Geschäftsbriefs oder eines Buchungsbelegs sind entsprechend den GoBD in elektronischer Form aufbewahrungspflichtig. Dabei gilt, dass diese als im DV-System empfangene Daten im Ursprungsformat aufzubewahren sind. Die mit den GoBD einhergehenden Anforderungen an die Konvertierung bedürfen im Hinblick auf E-Mails damit stets einer gesonderten Würdigung.[9]

Zu beachten gilt, dass die Außenprüfung grundsätzlich auch auf E-Mails des täglichen Geschäftsverkehrs (Handels- und Geschäftsbriefe) mit steuerrelevanten Inhalten zugreifen darf. Rechtswirksame elektronische Nachrichten sind nach § 257 HGB als empfangene Handelsbriefe (§ 257 Abs. 1 Nr. HGB), als Wiedergabe abgesandter Handelsbriefe (§ 257 Abs. 1 Nr. 3 HGB) und als Buchungsbelege (§ 257 Abs. 1 Nr. 4 HGB) aufzubewahren. Daher sind diese originär elektronischen Unterlagen im Rahmen der Aufbewahrungspflicht getrennt von nicht steuerrelevanten oder gar privaten E-Mails zu konservieren. Eine vernachlässigte Trennung steuerlich relevanter

9 Vgl. hierzu ausführlich Groß/Lindgens/Zöller/Brand/Heinrichshofen, ↗Was bedeutet Konvertierung?

E-Mails könnte hingegen dazu führen, dass der gesamte Mailverkehr inklusive sensiblem oder datenschutzrechtlich bedenklichem elektronischen Schriftverkehr einer Prüfung mit Einsatz moderner Suchfunktionen unterzogen wird.

Mögliche Rechtsfolgen bei Verletzung der gesetzlichen Vorgaben

Im Falle eines Verstoßes gegen die steuerlichen Vorschriften könnte die Finanzbehörde den steuerlichen Gewinn nach § 162 Abs. 2 AO schätzen und zudem ein Zwangsgeld nach § 328 Abs. 1 AO durchsetzen. Des Weiteren kann nach § 379 AO eine Ordnungswidrigkeit vorliegen, sofern vorsätzlich oder leichtfertig die Buchführungspflicht verletzt worden ist. Soweit das Unternehmen bestimmten Pflichten (insbesondere die Einräumung des Datenzugriffs oder zur Vorlage angeforderter Unterlagen im Rahmen einer Außenprüfung) nicht nachkommt, kann auf der Grundlage das § 146 Abs. 2b AO zudem ein Verzögerungsgeld festgesetzt werden.

Neben den steuerrechtlichen Sanktionen kann eine Verletzung der Buchführungspflichten strafrechtlich relevant sein und mit einer Freiheitsstrafe von bis zu 2 Jahren oder einer Geldstrafen belegt werden, §§ 283 ff. StGB. Ebenso kann eine Strafbarkeit aus § 274 Abs. 1 Nr. 2 StGB wegen Beseitigung beweiserheblicher Daten mit einer Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe in Betracht kommen.

Wie bereits in Kapitel 1 erwähnt, liegt die Verantwortung für die Einführung einer vorschriftsgemäßen E-Mail-Archivierung und für die technischen sowie organisatorischen Maßnahmen zu sorgen, in den Händen des Vorstands bzw. Geschäftsführung eines jeden Unternehmens. Es ist damit möglich, dass Vorstandsmitglieder, die ihre »Buchführungs-« Pflichten verletzen und damit archivierungspflichtige E-Mails nicht speichern, der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet sind, § 93 Abs. 2 AktG (persönliche Haftung). Nach § 91 Abs. 2 AktG hat der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, um den Fortbestand der die Gesellschaft gefährdenden Entwicklungen früh zu erkennen und damit zu überwachen.

Dasselbe gilt grundsätzlich auch für die GmbH-Geschäftsführer. Die Geschäftsführer einer GmbH haben für eine ordnungsgemäße Buchführung der Gesellschaft und damit auch Aufbewahrung von Unterlagen zu sorgen. Liegt sodann eine Obliegenheitsverletzung i.S.d. § 43 Abs. 2 GmbHG vor, so haben diese der Gesellschaft solidarisch den entstandenen Schaden zu ersetzen.

Im Falle einer fehlerhaften Archivierung von als Handels- oder Geschäftsbrief einzustufenden E-Mails kann sich zudem ein Schadensersatzanspruch aus den §§ 280 ff. BGB i.V.m. § 241 BGB ergeben.

Datenschutz

E-Mails sind in der Regel der Träger von personenbezogenen Daten. Schon die E-Mail-Adresse allein kann ein personenbezogenes Datum gemäß § 3 Abs. 1 BDSG sein, insbesondere wenn diese den Namen des Versenders bzw. Empfängers enthält. Auch der Inhalt der E-Mail, bspw. die Signatur des Versenders und Anhänge können sensible Informationen beinhalten. Neben personenbezogenen Daten können zudem hier auch Geschäftsgeheimnisse enthalten sein. Daher müssen die entsprechenden Aufbewahrungsfristen eingehalten werden, um einerseits den Datenschutz und andererseits die Datensicherheit zu gewährleisten.

Gemäß § 35 BDSG müssen personenbezogene Daten gelöscht werden, sollte der Zweck für die Verarbeitung bzw. Speicherung entfallen sein. Allerdings gilt dies nur, soweit es keine Aufbewahrungsfristen gibt, die dem entgegenstehen. Diese können neben den gesetzlichen auch vertragliche Aufbewahrungsfristen sein. Ist ein Löschen der E-Mails aus technischen, vertraglichen oder gesetzlichen Vorgaben nicht möglich, müssen diese gesperrt werden. Mit der Sperrung muss die Nutzbarkeit der E-Mails eingeschränkt werden. Eine Sperrung muss eintreten:

- wenn eine gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfrist dem Löschen entgegensteht,
- wenn der Grund zur Annahme besteht, dass das Löschen der E-Mails das schutzwürdige Interesse des Betroffenen verletzten würde, oder
- wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

Nicht mehr benötigte E-Mails müssen also unverzüglich, spätestens jedoch nach Ablauf einer Aufbewahrungsfrist, gelöscht oder wenigstens für die weitergehende Verwendung gesperrt werden.

Eine weitere Besonderheit ist die Trennung von privaten und geschäftlichen E-Mails. Ob eine private Nutzung des geschäftlichen E-Mail-Accounts erlaubt ist, sollte jedes Unternehmen regeln. Zum einen fordert eine vermehrte private Nutzung der geschäftlichen E-Mails-Accounts mehr Speicherplatz ein und zum anderen könnten private E-Mails mit archiviert werden, für deren Archivierung es keine gesetzliche Grundlage gibt. Dies wird besonders schwierig, wenn das Postfach (oder ein Teil des Inhalts) eines ausgeschiedenen Mitarbeiters einem Nachfolger zugänglich gemacht werden muss. Ein Unternehmen, welches einen geschäftlichen E-Mail-Account für die private Nutzung anbietet, gilt grundsätzlich als Diensteanbieter gemäß § 3 Abs. 6 TKG und muss damit das Fernmeldegeheimnis gemäß § 88 TKG wahren. Dies erschwert zum Beispiel auch eine automatisierte Analyse der E-Mails auf Schadcode. Unternehmer sind gut beraten, die private Nutzung des geschäftlichen E-Mail-Accounts entweder komplett zu verbieten oder zumindest die Nutzung in einer Betriebsvereinbarung, im Arbeitsvertrag oder einer Nutzungs-Richtlinie zu regeln, bspw. die Kennzeichnung von privaten E-Mails als »privat« oder die Speicherung von privaten E-Mails in einem separaten Aufbewahrungsort. Alternativ könnte die gelegentliche Nutzung des dienstlichen Internetanschlusses für die Nutzung der

»Praxistipp: Untersagen Sie die Nutzung des dienstlichen E-Mail Accounts für das Versenden von privaten Nachrichten. Erlauben Sie Ihren Mitarbeitern stattdessen, hin und wieder über eine Webanwendung einen Blick in ihre privaten E-Mails zu werfen. «

privaten Webmailer erlaubt werden. So kann auf bequemem Weg die gesetzliche Archivierung mit der privaten Nutzung gesetzeskonform in Einklang gebracht werden. Selbstverständlich ist es auch möglich die private Nutzung zuzulassen, jedoch erfordert dies zusätzlichen Aufwand bei der Prüfung des schutzwürdigen Interesses der Betroffenen sowie detaillierte Analysen der technischen Voraussetzungen. Es gibt Lösungen in welchen definierte E-Mails von einer automatischen Archivierung ausgeschlossen werden können. Damit wäre die Übertragung des Postfachs an einen Nachfolger datenschutzgerecht möglich. Die Pflicht zur Wahrung des Fernmeldegeheimnisses besteht hier allerdings weiterhin.

Mitbestimmung des Betriebsrats

In manchen Aspekten des E-Mail-Managements gibt es ein Mitbestimmungsrecht des Betriebsrates. Ein solches Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG kann sich bspw. mit der Aufbewahrung von Daten ergeben, insbesondere dann, wenn eine technische Einrichtung wie eine elektronische Archivierung eingeführt und/oder eingesetzt wird, die auch dazu benutzt werden kann, das Leistungsverhalten der Mitarbeiter zu überwachen. »Eine technische Einrichtung i.S. des § 87 I Nr. 6 BetrVG ist dann dazu bestimmt, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, wenn die Einrichtung zur Überwachung objektiv und unmittelbar geeignet ist, ohne Rücksicht darauf, ob der Arbeitgeber dieses Ziel verfolgt und die durch die Überwachung gewonnenen Daten auch auswertet.« (BAG, Beschluss vom 9. 9. 1975 - 1 ABR 20/74 (Mannheim)). Auch wenn der Betriebsrat keine Befugnisse aus dem Betriebsverfassungsgesetz herleiten kann, so stellt er dennoch einen wichtigen Partner im Projekt dar. Bereits durch dessen Einbeziehung kann die Anwenderakzeptanz erhöht werden.

Pflichtangaben für E-Mails nach § 37a HGB

Um die Sicherheit des Geschäftsverkehrs zu schützen, müssen Geschäftsbriefe gemäß§ 37 a HGB zwingend bestimmte Grundinformationen über den Kaufmann und sein Handelsgeschäft enthalten. Die Vorschrift wird entsprechend ihres Schutzzwecks weit ausgelegt und erstreckt sich auf Geschäftsbriefe jeder Form. Damit sind alle schriftlichen Äußerungen über geschäftliche Angelegenheiten erfasst und insbesondere auch Emails, die an Geschäftspartner, andere Konzernunternehmen oder Behörden gerichtet sind.

Gemäß § 37 a Absatz 1 HGB umfassen diese Angaben grundsätzlich folgende Punkte:

- Firmenname,
- Bezeichnung der Rechtsform (§ 19 Abs. 1 Nr. 1 HGB),
- der Ort seiner Handelsniederlassung und
- das Registergericht die Nummer, unter der die Firma in das Handelsregister eingetragen ist.

Zusätzlich müssen bei Kapitalgesellschaften noch Angaben über die Geschäftsführer gemacht werden. Diese Vorgaben folgen aus der jeweiligen Rechtsform der Gesellschaft. So müssen zum Beispiel bei der GmbH gemäß § 35a GmbHG die Geschäftsführer genannt und – sofern

ein Aufsichtsrat gegründet wurde – dessen Vorsitzende mit Vor- und Nachname angegeben werden.

Urteile zum Thema E-Mail Management und Archivierung

Einige Grundsatzurteile rund um den Themenbereich finden sich im Anhang dieser Publikation. So wurde unter anderem geurteilt, dass ein betriebliches Verbot über die private E-Mail-Nutzung nicht dem Mitbestimmungsrecht des Betriebsrats unterliegt, die Kündigung eines Arbeitnehmers, der die dienstliche E-Mail exzessiv privat nutzt, wurde für rechtens befunden und dass der Zugriff auf ein E-Mail-Postfach während der Krankheit eines Mitarbeiters bei Einhaltung der formellen Anforderungen nicht die Persönlichkeitsrechte des Mitarbeiters verletzten.

Exkurs zu österreichischen Regelungen[10]

Im Wesentlichen gelten im Ausland ähnliche Regelungen wie in Deutschland. Am Beispiel Österreich erkennt man, dass der Unterschied meist nur in der geforderten Aufbewahrungsfrist liegt. So beträgt die Aufbewahrungspflicht für alle Buchhaltungsunterlagen und Aufzeichnungen sieben Jahre. Auch hier startet der Fristenlauf mit Schluss des Kalenderjahres, für das die Verbuchung vorgenommen wurde bzw. auf das sich der Beleg bezieht.

Bei EDV-Buchführung oder EDV-Aufzeichnungen sind die Daten in entsprechender elektronischer Form auf Datenträgern aufzubewahren und im Fall einer Prüfung zur Verfügung zu stellen (§§ 131,132 BAO). Die Aufbewahrungszeiten können auch zwölf Jahre betragen, wenn es sich z. B. um Unterlagen und Aufzeichnungen handelt, die Grundstücke betreffen – für bestimmte Grundstücke sogar 23 Jahre (§ 18 Abs. 10 UStG). Die rechtlichen Grundlagen werden u. a. in der Bundesabgabenordnung (BAO) und dem Unternehmergesetzbuch (UGB) geregelt.

Hinsichtlich der technischen Methoden zur Digitalisierung von aufbewahrungspflichtigen Dokumenten und Belegen machen die österreichischen Finanzbehörden bewusst keine konkreten Vorgaben.

10 Für weitere Informationen empfehlen wir den Besuch der Webseite des österreichischen Bundesministerium für Finanzen.

3 Beweggründe von Unternehmen für E-Mail-Management

3 Beweggründe von Unternehmen für E-Mail-Management

Im vorangegangenen Kapitel wurde auf die rechtlichen Aspekte des E-Mail-Managements eingegangen. Dies stellt aber nur einen möglichen Beweggrund für die Einführung eines E-Mail-Management-Systems dar. Ein weiterer betrachtet das Thema aus einem eher technisch orientierten Ansatz, um die Mailserver zu entlasten und Daten auf kostengünstigeren Speichermedien auszulagern. Ein in Zukunft immer bedeutenderer Grund wird die Orientierung an Geschäftsprozessen sein. Das bedeutet eine zielgerichtete Verarbeitung von E-Mails durch die Verknüpfung mit Vorgängen und damit eine nicht unerhebliche Qualitätssteigerung der Informationen sowie eine beachtliche Zeitersparnis bei der Suche nach relevanten Daten, was einen positiven Einfluss auf die Unternehmensproduktivität hat.

3.1 Der technokratische Ansatz

Als in Deutschland am 03.08.1984 die erste E-Mail eintraf, die als Grußbotschaft von Wissenschaftlern der US-amerikanischen Plattform CSNET aus Cambridge (Massachusetts) an ihre Kollegen von der Universität Karlsruhe gesendet wurde, hat wohl keiner damit gerechnet, dass sich diese Form der Kommunikation zu einem der wichtigsten Dienste im Internet entwickelt.

Laut einer Studie aus dem Jahr 2015 geht das Technologie-Marktforschungsunternehmen The Radicati Group davon aus, dass im Jahr 2016 jeden Tag über 215 Milliarden E-Mails verschickt werden. Gut 116 Milliarden E-Mails entfallen laut diesem Report auf geschäftlich gesendete und empfangene E-Mails. Der aktuelle Anteil an Spam-Mails wird je nach Quelle auf ca. 50 Prozent geschätzt. Die Radicati Group schätzt, dass aktuell bereits mehr als 2/3 der gesamten Kommunikation eines Unternehmens über E-Mail abgewickelt wird.

Täglicher E-Mail Verkehr (in Mrd.)	2015	2016	2017	2018	2019
Weltweit gesendet / empfange E-Mails pro Tag	205,6	215,3	225,3	235,6	246,6
Weltweit gesendet / empfange Geschäfts-E-Mails pro Tag	112,5	116,4	120,4	124,5	128,8

Tabelle 1: Weltweiter E-Mail Verkehr im Zeitverlauf[11]

Dies hat zur Folge, dass die E-Mail das Kommunikationsmittel Nummer 1 geworden ist, welches immer mehr den klassischen Schriftverkehr im Alltag ersetzt. Neben der tatsächlichen Anzahl von E-Mails steigt auch die Anzahl der Adressaten täglich permanent an. Der zunehmende Ausbau schneller Internetanbindungen, sowohl im mobilen Bereich über LTE als auch im Festnetzbereich durch DSL / VDSL / Kabel, lässt nun auch den Versand von E-Mails mit größeren Anhängen zu.

11 Quelle: ↗ E-Mail Statistics Report, 2015 - 2019, RADICATI GROUP, INC, abgerufen am 5.2.2016

All die vorgenannten Gründe ziehen aus technischer Sicht eine große Herausforderung mit sich, denn durch den Anstieg des E-Mail-Aufkommens werden die E-Mail Datenbanken, in denen die E-Mails inklusive Ihrer Anhänge gespeichert werden, immer größer. Gab es zu Beginn der ersten Generationen von E-Mail-Servern auf Seiten der Hersteller Restriktionen in Bezug auf Datenbankgrößen, die eine Auslagerung von E-Mails von Nöten machten, um die Datenbanken zu verschlanken, so sind diese mittlerweile gefallen. Dennoch verursachen große Datenbanken auf performanten Speichersystemen entsprechend hohe Speicherkosten, die durch die Auslagerung auf kostengünstigeren Medien gesenkt werden könnten. Ein weiterer negativer Aspekt großer E-Mail-Datenbanken ist das zeitintensive Backup und die langen Wiederherstellzeiten im Desaster Recovery-Fall.

Ohne ein E-Mail-Management-System begegnet die IT Abteilung häufig dieser Herausforderung mit unterschiedlichen Postfachlimits für die Anwender. Das veranlasst diese unter Umständen dazu, Mails einfach zu löschen - im schlimmsten Fall ohne zu verifizieren, ob die Mail zu einem Kundenvorgang gehört und damit eigentlich aufbewahrt werden muss. Eine weitere von Anwendern häufig gewählte Option ist die Auslagerung von E-Mails, z. B. in PST-Dateien oder NSF-Dateien auf der lokalen Festplatte und/oder auf Netzlaufwerken. Liegt auf der einen Seite bei der Auslagerung auf lokalen Festplatten das größte Problem in der dezentralen und unsicheren Datenhaltung, unterstützt mancher Hersteller auf der anderen Seite keine Auslagerung auf Netzwerklaufwerken. Keine dieser Optionen stellt eine Lösung des Problems dar, da auch die Erfahrung zeigt, dass das Postfachlimit schnell wieder erreicht ist. Sie bedeuten in der Regel einen enormen Aufwand für den Benutzer wie auch für den Administrator.

»Ein E-Mail–Managementsystem spart Speicherkosten.«

Ein E-Mail-Management-System unterstützt hier effektiv bei der Entlastung von E-Mail-Servern durch Auslagern und Langzeitaufbewahrung auf wirtschaftlichen und/oder revisionssicheren Medien. Dies wird erreicht, indem Original-E-Mails mit Anhängen durch eine Verknüpfung – den sogenannten Shortcuts oder Links - ausgetauscht werden. Durch die Nutzung von Verknüpfungen bleibt der Anwender in seiner gewohnten E-Mail-Anwendung und kann wie gewohnt auf seine E-Mails zugreifen. Nach der Archivierung reduziert sich je nach Archivierungs-Regel der Speicherbedarf im E-Mail-Datenbank-Speicher um bis zu 70 Prozent. Da die meisten E-Mail-Management-Systeme bei der Speicherung und Auslagerung auch auf Single-Instance-Speichertechnologien[12] zurückgreifen, können bis zu 50 Prozent kürzere Sicherungszeiten erreicht werden. In der Regel werden hier auch Web Access-, WebApp-Integrationen oder Offline-Verfügbarkeit angeboten.

12 Single-Instance Storage (SIS) ist die Fähigkeit eines Systems, nur eine Kopie der Inhalte vorzuhalten, die mehrere Benutzer oder Computer teilen. Somit ist es ein Mittel zur Beseitigung von Datenduplikaten mit Ziel der Effizienzerhöhung.

3.2 Der Compliance Ansatz

Wie bereits in Kapitel 2 beschrieben, gibt es eine Vielzahl von Anforderungen, die definieren, was Unternehmen bei der Aufbewahrung von E-Mails einschließlich Anhängen zu beachten haben.

Steuerlich relevanter, elektronischer Schriftverkehr ist wie ein Papierdokument urschriftlich gemäß der Aufbewahrungsfristen aufzubewahren und prüfbar bereitzustellen. Allerdings reicht es nicht aus, einfach einen reinen Ausdruck bereit zu stellen. Während der gesamten Laufzeit der Archivierung müssen für den Betriebsprüfer die elektronischen Dokumente durch deren Prüfsoftware maschinell auswertbar sein. Auch die Unveränderbarkeit der Dokumente muss das Unternehmen sicherstellen.

Bei der Erfüllung rechtlicher Anforderungen (Compliance) und der Einhaltung von Aufbewahrungsfristen und bei der Gewährleistung der Unveränderbarkeit von gespeicherten Objekten erwartet der Anwender Unterstützung durch den Einsatz eines E-Mail-Management-Systems. Diese Anforderung muss durch die eingesetzte E-Mail-Managementlösung und das dort verwendete Verfahren zur Ablage abgedeckt werden. Die zur Ablage und ggf. langfristigen Verwaltung von E-Mail-Objekten zu verwendenden Speichertechnologien werden i.d.R. nicht vom Gesetzgeber oder anderen relevanten Behörden vorgeschrieben. In diesem Zusammenhang können aber sogenannte Hierarchische Speicher Management-Lösungen (HSM)[13] den Anwender technologisch unterstützen – dies auch im Zusammenhang mit einer Unveränderbarkeit von Objekten. Die Konzeption der Archivinfrastruktur hängt in erster Linie von den Anforderungen des Unternehmens ab. Selbst wenn Anwender versehentlich E-Mails löschen, bleiben diese bis zum Erreichen der vorgesehenen Lebenszeit im Archiv erhalten. Wird auf die Journal-Funktion[14] von E-Mail-Servern zurückgegriffen, die eine Kopie aller ein- und ausgehenden E-Mails in ein Journal-Postfach schreibt, unterstützt diese im Zusammenspiel mit einem E-Mail-Management-System den lückenlosen Nachweis der gesamten E-Mail-Kommunikation.

»Ein E-Mail-Managementsystem ermöglicht Compliance.«

3.3 Der Prozessmanagement Ansatz

Betrachtet man E-Mail-Management ganzheitlich, ist es als Bestandteil der Kommunikationsstrategie in einem Unternehmen anzusehen. Auch wenn jede Kommunikationsform und jeder Kommunikationskanal seine Besonderheiten aufweist, so ist grundsätzlich das Ziel immer dasselbe, nämlich eingehende Kundenanliegen zentral, einheitlich und schnell, gleichzeitig jedoch individuell zu bearbeiten und zu beantworten. Leider schwächelt in vielen Unternehmen derzeit die Kundenkommunikationsstrategie in diesem Punkt. Das beginnt bei einem fehlenden Vorgehensmodell bei zentralen Postfächern (Funktions-Postfächern), geht über den fehlenden

13 Unter HSM versteht man eine Kombination aus Hard- und Software mit klar definierten Funktionen und Schnittstellen für die Objektspeicherung sowie für die Administration.

14 Vgl. hierzu auch Kapitel 4.6

Bezug zu existierenden Geschäftsvorfällen bis dahin, dass zwar zeitnahe und adäquate Antworten auf Anfragen erwartet werden, dies aber nur selten eingehalten wird. Daher besteht in vielen Unternehmen zunehmend die Herausforderung, E-Mails und Dokumente so abzulegen, bzw. einem Vorgang oder Prozess zuzuordnen, dass abteilungsübergreifend auf Informationen zugegriffen werden kann, ohne lange suchen zu müssen.

»Ein E-Mail-Managementsystem steigert die Effizienz und verbessert die Kommunikation.«

Nach einer Studie von McKinsey & Company[15] verbringt der durchschnittliche Arbeitnehmer gut 19 Prozent seiner Arbeitszeit pro Woche mit dem Suchen und Finden von Informationen. Das entspricht fast einem Arbeitstag pro Woche oder 1,5 Stunden am Tag. Ein prozessorientiertes E-Mail-Management-System kann hier effektiv und effizient unterstützen, diese Zeit zu minimieren. Ein kleines Rechenbeispiel: Werden pro Mitarbeiter nur fünf Minuten am Tag für »Suchen & Finden« eingespart und legt man einen Durchschnittlichen Stundensatz von 20 Euro mit 230 Arbeitstagen pro Jahr zugrunde, ergibt sich einer rechnerische Summe von gut 380 Euro im Jahr – pro Mitarbeiter.

Natürlich darf dabei das Ablegen der Informationen die Anwender nicht zusätzlich belasten. Zu diesem Zweck bieten E-Mail-Management-Systeme durchaus geeignete Mittel an. Dazu gehört es, automatisiert das Anliegen des Versenders zu identifizieren (Klassifizierung), weitere Informationen aus den eingehenden Dokumenten zu generieren (Extraktion und Anreicherung), daraus dann den jeweiligen internen Prozess für die Bearbeitung anzustoßen (Routing) und abschließend zu entscheiden, über welchen Kanal die Beantwortung stattfinden soll (Schnittstelle zum Response Management / Output Management).

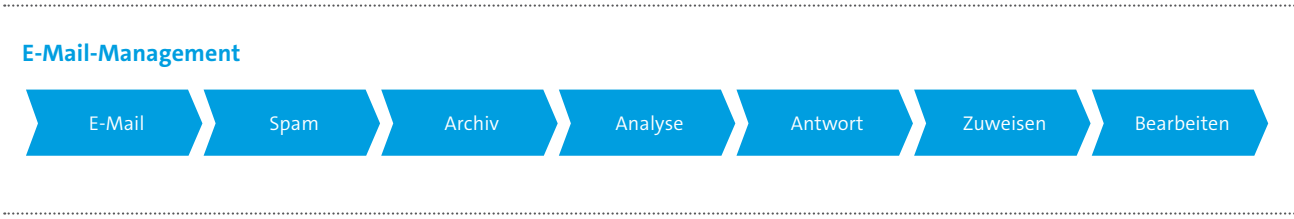


Abbildung 2: Prozesse im E-Mail-Management

Die oben genannten Maßnahmen lassen sich automatisiert oder halb-automatisiert umsetzen, indem z. B. eine Dokumentenverwaltung in der E-Mail-Applikation (z. B. MS Outlook, Lotus Notes, etc.) durch Regeln oder einfaches Drag & Drop zu den Prozessen bzw. in die digitale Akte erfolgt und dabei eine automatische Verschlagwortung vom Element beim Ablegen stattfindet. Diese Informationen können dann durch zentrale Berechtigungssysteme oder individuelle Freigaben mit anderen Personen oder Gruppen geteilt werden. Neben der Zuordnung relevanter Informationen zu Prozessen oder digitalen Akten unterstützt eine intelligente und performante Volltextsuche den Anwender beim Finden relevanter Elemente.

15 Vgl. McKinsey Global Institute, ↗ The social economy: Unlocking value and productivity through social technologies, abgerufen am 05.02.2016

4 Praktische Umsetzung der E-Mail-Archivierung

4 Praktische Umsetzung der E-Mail-Archivierung

Neben der manuellen Archivierung über Plug-Ins oder Apps in der gewohnten E-Mail-Applikation, gibt es im Allgemeinen drei Möglichkeiten der automatischen Archivierung, wobei bei einer die Journaling-Funktion des Mailservers eine wichtige Rolle spielt. Es handelt sich hierbei um die zeitgesteuerte Archivierung, die Schwellwert-basierende Archivierung und die Journal-Archivierung. Die verschiedenen Archivierungsmöglichkeiten bzw. -methoden werden in den nachfolgenden Kapiteln beschrieben, sowie deren Vor- und Nachteile aufgeführt.

4.1 Die manuelle Archivierung

Die manuelle Archivierung sieht die sofortige Archivierung über Plug-Ins oder Apps vor, was zur Folge hat, dass der Anwender die Entscheidung trägt, ob und welche E-Mail er archiviert. Er identifiziert somit für das Unternehmen die archivierungsrelevanten Elemente, was sehr fehleranfällig sein kann. Zudem ist hierbei ein entsprechendes Plug-in im E-Mail-Client bereitzustellen oder Archivsoftware auf den PCs und Notebooks zu installieren.

4.2 Die zeitgesteuerte Archivierung

Bei der zeitgesteuerten Archivierung gibt es zwei unterschiedliche Ansätze:

1. Archivierung aller Dokumente
   - Hierbei werden die zu archivierenden Dokumente nach Ablauf einer festgelegten Zeitspanne archiviert.

2. Regelbasierte Archivierung
   - Beim diesem Ansatz werden die E-Mails nur nach bestimmten Regeln archiviert. Diese Regeln können bspw. auf Basis von Benutzergruppen vergeben werden. Sie können Filter für Absender und Empfänger enthalten oder auch nach Alter und Größe der E-Mail über die Archivierung entscheiden.

4.3 Die zeitgesteuerte Archivierung mit Ausnahmen

Bei der zeitgesteuerten Archivierung mit Ausnahmen werden alle E-Mails mit einem, vom Kunden bestimmten Alter (z. B. 30 Tage), archiviert, es sei denn, sie befindet sich in einem bestimmten Ordner des E-Mail-Clients (z. B. Ordner Privat oder Spam). Die Ausnahmen können oftmals sehr einfach definiert werden. Bei dieser Art der Archivierung wird die Mailbox ohne das Zutun der Benutzer durch die Archivierung entlastet. Wie stark hängt dann vom definierten Zeitpunkt der Archivierung ab.

4.4 Die zeitgesteuerte Archivierung von bestimmten Ordnern

Bei der zeitgesteuerte Archivierung werden die E-Mails mit einem bestimmten Alter nur dann archiviert, wenn Sie sich in einem oder mehreren bestimmten Ordnern befinden. Alle sich in Unterordnern befindende E-Mails werden dabei ebenfalls archiviert. Diese Art der Archivierung setzt voraus, dass der Benutzer die zu archivierenden E-Mails in diesen bestimmten Ordner verschiebt, damit das Postfach des Benutzers durch die Archivierung entlastet und die E-Mail gesetzeskonform aufbewahrt werden kann. Die Entlastung des Mailservers und die Einhaltung der Compliance-Regeln sind also stark vom Benutzerverhalten abhängig.

4.5 Die Schwellwert-basierende Archivierung

Mit Schwellwert wird der Bereich zwischen zwei definierten Grenzwerten bezeichnet, in dessen Grenzen Aktionen ausgelöst werden. Bei der schwellwertbasierenden Archivierung werden die E-Mails eines Benutzers automatisch archiviert, sobald der Maximalwert seiner Postfachbelegung erreicht ist. Es wird dann solange archiviert, bis der untere Grenzwert wieder unterschritten ist.

Hier ein Beispiel:

Der Benutzer hat ein Mailboxlimit am E-Mail-Server von 500 MB und der Administrator hat ein oberes Limit von 90 Prozent und ein unteres Limit von 60 Prozent definiert. Wird sein Postfach nun größer als 450 MB, werden die E-Mails aus seinem Postfach archiviert bis dieses wieder kleiner als 300 MB ist. Dann stoppt die Archivierung. Dabei können auch wieder Ordner definiert werden, die nicht archiviert werden sollen. Außerdem kann diese Regel zusätzlich auf Benutzerebene vergeben werden.

4.6 Die Journal Archivierung

Bei der Journal-Archivierung benutzt man die Journaling-Funktion des E-Mail Servers. Bei dieser Funktion wird von jeder ein- und ausgehenden E-Mail (auch von internen E-Mails, Besprechungsanfragen, etc.) eine Kopie erzeugt und in einem definierten Postfach gespeichert. Dieses Postfach wird dann von der E-Mail-Archivlösung nach einem Zeitplan archiviert.

Ziel dieser Art der Archivierung ist es, von jeder E-Mail der relevanten Postfächer eine Kopie zu haben, falls diese mutwillig oder durch einen Fehler des Benutzers gelöscht wurde. Zu beachten ist aber, dass dadurch die eigentlichen Postfächer nicht entlastet werden. Diese müssen dann zusätzlich, mit einer der oben genannten Archivierungsregeln, archiviert werden. Die Journal-Archivierung dient nur der Sicherung der E-Mail Inhalte und ist für die Compliance maßgeblich, da nur hiermit die Integrität der archivierten Daten sichergestellt werden kann.

»Nur die Journal Archivierung stellt die Einhaltung der Compliance Regeln sicher.«

4.7 Die ereignisgesteuerte Archivierung

Diese Art der Archivierung reagiert auf bestimmte Ereignisse des Systems oder des Benutzers. Entweder können hierfür eigene Regeln definiert oder die selben wie bei der zeitgesteuerten Archivierung angewendet werden.. Sollen E-Mails möglichst zeitnah ins Archiv übernommen werden, bietet sich diese Art ebenfalls an, ersetzt jedoch nicht das Journaling.

Zwei einfache Beispiele sollen dieses Verfahren erläutern:

- **Eine E-Mail trifft ein, die im Betreff das Wort Rechnung enthält:** Das Ereignis wäre in dem Fall das Eingehen der Nachricht. Das Regelwerk prüft den Betreff auf das Schlüsselwort »Rechnung«. Ist es vorhanden, wird die E-Mail in den Rechnungsbereich archiviert.

- **Ein Anwender schiebt eine Datei in einen bestimmten Ordner:** Hier lautet das Ereignis »Nachricht verschoben«. Über das Regelwerk sind nun bestimmte Ordner zur Archivierung bestimmt. Ist das Ziel der Verschiebeaktion ein solcher Ordner, wird der Verarbeitungsprozess angestoßen.

4.8 Filtermöglichkeiten

Sämtliche genannten Methoden bieten i.d.R. eine Vielzahl von unterschiedlichen Filtermöglichkeiten über die Metadaten oder enthaltene Begriffe in Body, Betreff oder Anhang einer Nachricht. Filter können ein- oder ausschließende Wirkung haben und auch miteinander kombiniert werden. Es lohnt sich, die Möglichkeiten der eingesetzten Archivsoftware in diesem Bereich genau zu studieren, um eine bestmögliche Anpassung an die Unternehmensprozesse zu erreichen.

5 Sonderfälle, Praxisrisiken und Fallstricke

5 Sonderfälle, Praxisrisiken und Fallstricke

In der Praxis gibt es eine Reihe von Sonderfällen, auf die in dieser Publikation nicht erschöpfend und im Einzelnen eingegangen werden kann. So bedürfen bspw. E-Mails des Betriebsrats, des Betriebsarztes, der Personalabteilung und/oder des Aufsichtsrats einer gesonderten Betrachtung der einzuhaltenden Vorschriften. Unternehmen, die solche Sonderfälle in Ihrer Organisation identifizieren, wird dringend geraten sich hierzu fachkundige Beratung einzuholen. In diesem Kapitel wird auf einige der Sonderfälle eingegangen, die aus Sicht der Autoren in den meisten Unternehmen Anwendung finden.

5.1 Löschung von E-Mails nach Ablauf der Aufbewahrungsfrist

Sobald E-Mails personenbezogene Daten beinhalten, unterliegen diese den Regelungen des BDSG. Als Konsequenz müssen E-Mails und Anhänge nach Ablauf der Aufbewahrungsfristen gelöscht werden, sobald der Zweck für die Speicherung erloschen ist, bzw. sobald eine Speicherung nicht mehr zulässig ist.

E-Mails und deren Anhänge sollten genauestens geprüft werden, bevor diese gelöscht werden, da es möglich ist, hier andere Gesetzesgrundlagen zu verletzten. So müssen Bewerbungsdaten eines abgelehnten Bewerbers bereits nach kurzer Zeit gelöscht werden. Hier empfiehlt es sich, Sonderregeln zu definieren, um diese Art von E-Mails gar nicht erst in den Archivierungsprozess aufzunehmen. E-Mails mit Rechnungen, Belegen, Angeboten etc. dürfen nicht so schnell gelöscht werden, da hier die Archivierungsfristen anderer Gesetze verletzt werden könnten. Daher müssen Löschfristen, je nach Art und Zweck der E-Mail, definiert werden.

Abhängig vom eingesetzten Archivierungssystem kann das Löschen von E-Mails technische Probleme verursachen. Oft ist das Löschen einer E-Mail aus einem Archivierungssystem oder von einem Datenträger nicht ohne enorme Aufwände möglich. Hier gibt es die Möglichkeit, auf das Löschen zu verzichten und stattdessen ein »sperren« der E-Mails anzuwenden. Geregelt wird diese Alternative in § 35 Abs. 3 BDSG. Sperren meint an dieser Stelle die Weiterverarbeitung der E-Mails einzuschränken (siehe § 3 Abs. 4 BDSG). In der Praxis bedeutet dies, den Zugriff auf das E-Mail-Archiv nachweisbar einzuschränken. Denkbar wären auch Szenarien in denen die E-Mails und Anhänge verschlüsselt abgelegt werden.[16] Zudem empfehlen wir ebenfalls den Ermessensspielraum des »unverhältnismäßig hohen Aufwands« schriftlich zu dokumentieren, um hier ggf. Nachweise gegenüber der Aufsichtsbehörde parat zu haben. Auch ist es ratsam Lösch- und Vernichtungsprotokolle nachzuhalten.

Wie bereits in Kapitel 1 erwähnt, müssen die empfangenen Handels- oder Geschäftsbriefe, die Wiedergabe der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen,

16 Vgl. hierzu Kapitel 5.3

soweit sie für die Besteuerung von Bedeutung, sechs Jahre aufbewahrt werden (vgl. § 147 Abs. 3 AO). In Fällen, in denen der E-Mail bspw. eine Belegfunktion zukommt, gilt die zehnjährige Aufbewahrungsfrist, sofern nicht in anderen Steuergesetzen kürzere Aufbewahrungsfristen zugelassen sind (vgl. § 147 Abs. 3 AO; § 257 Abs. 4 HGB). Auf der anderen Seite kann sich die Aufbewahrungsfrist auch verlängern, sobald steuerrelevante Unterlagen für ein Steuerverfahren erforderlich sind und zugleich die Frist für die Festsetzung eines Steuerbescheids noch nicht verstrichen ist (vgl. § 147 Abs. 3 S. 2). In diesen Fällen dürfen E-Mails auch nach Ablauf der entsprechenden Archivierungsfrist nicht gelöscht werden.

Entscheidet sich das Unternehmen für eine lückenlose Archivierung durch Journaling,[17] sollten die Archivierungsprotokolle/Journale mit entsprechenden Zugriffseinschränkungen versehen werden, sodass hier nur wenige Mitarbeiter Zugriff haben. Notwendige Zugriffe sollten zur Schaffung von Transparenz und Nachweisbarkeit dokumentiert werden und ggf. im Vier-Augen-Prinzip stattfinden. Bei einer vollständigen Archivierung können auch sensible Daten mit archiviert werden, hier müssen Regelungen getroffen werden, um derartige E-Mails im Nachgang zu löschen oder zu sperren.

Es ist ratsam sich bereits bei der Gestaltung des Archivs fachlich qualifiziert beraten zu lassen.

5.2 Sonderfall: Bewerbungsunterlagen

Im digitalen Zeitalter werden Bewerbungsunterlagen größtenteils per E-Mail versandt. Dabei stellt sich die Frage, wie lange solche Unterlagen aufbewahrt werden müssen. Grundsätzlich dürfen Bewerberdaten – welche von Natur aus personenbezogene Daten[18] enthalten – »(...) für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses ... erforderlich ist« (vgl. § 32 Abs. 1 Alt. 1 BDSG). Doch sind diese personenbezogene Daten dann zu löschen, wenn »sie für eigene Zwecke verarbeitet werden (...)« und ihre »(...) Kenntnis für die Erfüllung des Zwecks nicht mehr erforderlich (...)« ist. (vgl. § 35 Abs. 2 Nr. 2 BDSG). Der Wortlaut besagt damit, dass Bewerbungsunterlagen direkt nach Erfüllung des Zwecks und somit mit Absage an den ungeeigneten Bewerber gelöscht werden müssen, denn die eingereichten Bewerbungsunterlagen sowie die Kenntnis über diese personenbezogenen Daten haben ihren Zweck mit der Absage erfüllt und werden grundsätzlich nicht mehr benötigt.

Doch um als Arbeitgeber Diskriminierungsvorwürfe zu entkräften und folglich zum Nachweis der Durchführung und dem Abschluss eines ordnungsgemäßen Bewerbungsverfahrens, kann sich eine darüber hinausgehende Aufbewahrungspflicht bzw. -frist ergeben. § 21 Abs. 5 S. 1 AGG besagt, ein Anspruch aus einem Verstoß gegen das Benachteiligungsverbot kann innerhalb

17 Vgl. Kapitel 4.6.

18 Vgl. hierzu die Ausführungen zum Datenschutz in Kapitel 2.

einer Frist von »zwei Monaten«[19] geltend gemacht werden (vgl. auch § 15 Abs. 4 AGG für Entschädigungs- und/oder Schadensersatzansprüche). Wenn nun die Bewerbungsunterlagen mit der Absage an den Bewerber aufgrund des Bundesdatenschutzgesetzes vernichtet bzw. gelöscht werden, könnten sich Arbeitgeber gegen Ansprüche aufgrund einer unzulässigen Benachteiligung im Bewerberverfahren nicht verteidigen und stünden hilflos da. Aus diesem Grund ist es grundsätzlich legitim, Bewerberdaten einschließlich deren Notizen und Anmerkungen über die Dauer des Bewerbungsverfahrens hinaus – für zwei Monate ab Zugang der Absage – aufzubewahren.

Ebenso sollten mögliche Fristverlängerungen aus §§ 15 Abs. 5, 21 Abs. 5 S. 2 AGG sowie § 224 ZPO nicht außer Acht gelassen werden. Nach § 15 Abs. 5 AGG bleiben Ansprüche gegen den Arbeitgeber, die sich aus anderen Rechtsvorschriften ergeben, unberührt. Zudem kann sich eine Fristverlängerung aus § 21 Abs. 5 S. 2 AGG ergeben, wenn nach Ablauf der Zweimonatsfrist »... der Benachteiligte ohne Verschulden an der Einhaltung der Frist verhindert war.« Aufgrund des § 224 ZPO kann sich die Frist verlängern, wenn das zuständige Gericht eine Fristverlängerung für das Klageverfahren gewährt.[20]

Gesetzlich ist damit keine allgemeingültige Frist für die Aufbewahrung von Bewerbungsunterlagen festgeschrieben, doch um einen möglichen Vorwurf der Diskriminierung abzuwehren und in Bezug auf die bereits erwähnten Vorschriften, ist es aus unserer Sicht gerechtfertigt bzw. ratsam, solche Daten mindestens für drei Monate aufzubewahren. Selbst eine Frist von sechs Monaten kann aus unserer Sicht gerechtfertigt sein.[21] Damit müssen sämtliche Bewerberdaten mit Ablauf der Frist gelöscht werden, sofern kein Rechtsstreit bei Gericht anhängig ist.

Sollten Arbeitgeber den Bewerber trotz der Absage für zukünftige Stellen im Unternehmen für Interessant halten und möchten dessen eingereichte Bewerbungsunterlagen speichern (sog. »Bewerberpool«), so ist hierzu die ausdrückliche Einwilligung des Betroffenen erforderlich.

19 Entscheidend für den Beginn der Zweimonatsfrist ist der Zugang der Absage an den Bewerber sowie der Eingang der Klageschrift beim Arbeitsgericht.

20 Eine solche Fristverlängerung aufgrund § 224 ZPO erfolgt im Ermessen des Gerichts.

21 So auch: 5. Tätigkeitsbericht des Bayrisches Landesamtes für Datenschutzaufsicht für die Jahre 2011 und 2012, S. 62.

5.3 Sonderfall: Verschlüsselte E-Mails

Exkurs: E-Mail-Verschlüsselung

Der Versand einer E-Mail über das Internet ist vergleichbar mit dem Versand einer Postkarte: Jeder, der am Versand oder Transport beteiligt ist, könnte den Inhalt unbemerkt mitlesen oder gar verändern.

Um diesen fehlenden Umschlag für die elektronische Post zu ersetzen, müssen geeignete Schutzmechanismen eingesetzt werden. Nur mithilfe bewährter Verschlüsselungssysteme lassen sich vertrauliche Nachrichten vor unberechtigtem Zugriff geschützt übermitteln. Den umfassendsten Schutz bieten die Ende-zu-Ende-Verschlüsselungsverfahren. Die gängigen Standards sind die sogenannten Public-Key-Verfahren S/MIME und PGP.

Bei diesen Verschlüsselungsverfahren muss ein eindeutiges Schlüsselpaar verwendet werden, um E-Mails auf Senderseite zu verschlüsseln und auf Empfängerseite zu entschlüsseln. Die Ver- und Entschlüsselung, sowie die dazu erforderliche Verwaltung der Schlüssel erfolgt entweder direkt im E-Mail-Client oder auf einer serverbasierten Lösung.

Das Bundesdatenschutzgesetz fordert von Unternehmen bei der Übertragung sensibler Daten per E-Mail eine sichere Methode. Gemäß Anlage (zu § 9 Satz 1) des BDSG[22] müssen Unternehmen sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine geeignete Maßnahme im Sinne der gesetzlichen Regelungen ist die Verwendung von Ende-zu-Ende Verschlüsselungsverfahren. Zahlreiche Unternehmen nutzen daher zur Übermittlung von Angeboten, Rechnungen, Patienten- oder Kundendaten standardisierte Verfahren wie z. B. S/MIME oder PGP.

Bei der Anwendung von Ende-zu-Ende-Verschlüsselung müssen Unternehmen zusätzlich darauf achten, dass die Lesbarkeit der E-Mail über den gesamten Archivierungszeitraum erhalten bleibt. Technisch kann diese Anforderung auf zwei Wegen realisiert werden. Entweder durch direkte Archivierung der E-Mail im verschlüsselten Format oder durch Entschlüsselung der E-Mail vor der Archivierung.

5.3.1 Direkte Archivierung der E-Mail im verschlüsselten Format

Wird eine E-Mail in verschlüsselter Form im Archiv abgelegt, kann sie nur mit dem privaten Schlüssel des Empfängers entschlüsselt werden. Das ist vor allem dann eine Herausforderung, wenn im Recherche-Fall der betreffende Empfänger bereits das Unternehmen verlassen oder zwischenzeitlich einen neuen Private-Key für seine Verschlüsselung erhalten hat. Beide Szenarien sind während der gesetzlichen Aufbewahrungspflicht von bis zu zehn Jahren nicht unwahrscheinlich.

Wird die E-Mail technisch nicht vor der Archivierung, sondern erst auf dem E-Mail-Client des Nutzers entschlüsselt, ist es erforderlich, ein Private-Key-Management in das Archiv zu

22 Vgl. ↗Bundesdatenschutzgesetz Anlage (zu § 9 Satz 1), abgerufen am 05.02.2016

integrieren und kontinuierlich zu pflegen. Das stellt sicher, dass jederzeit alle privaten Schlüssel zu den archivierten E-Mails vorliegen.

5.3.2 Entschlüsselung der E-Mail vor der Archivierung

Das Archivieren und Wiederherstellen von E-Mails wird erheblich erleichtert, wenn eine Ende-zu-Ende verschlüsselte E-Mail bereits vor der physischen Archivierung entschlüsselt wird. Die Entschlüsselung der E-Mail erfolgt in diesen Fällen nicht auf dem Client des Nutzers, sondern zentral auf dem E-Mail Server oder einem vorgeschalteten Gateway. Im Anschluss wird die unverschlüsselte E-Mail im Archiv abgelegt.

Der Vorteil liegt darin, dass für die Archivierung selbst kein Private-Key-Management erforderlich wird. Ein Wiederherstellen der E-Mail ist jederzeit möglich. Es ist unerheblich, ob die jeweiligen privaten Schlüssel noch existieren.

5.4 Sonderfall De-Mail

Neben der klassischen E-Mail-Kommunikation kommt vermehrt auch De-Mail, als standardisiertes elektronisches Pendant zur klassischen Papierpost, zur Anwendung. Dabei gelten für eine De-Mail grundlegend die gleichen Regelungen wie für eine E-Mail.

Eine Besonderheit ist jedoch, dass nicht nur zweifelsfrei identifizierte Kommunikationspartner auf verschlüsselter Art und Weise, sei es mittels Ende-zu-Ende- und/oder Transportverschlüsselung, per De-Mail und über akkreditierte De-Mail-Diensteanbieter (DMDA) kommunizieren, sondern dass diese Kommunikation nach De-Mail Gesetz auch nachhaltig nachweisbar ist. Die rechtsverbindliche Nachweisbarkeit wird durch Versand- und Empfangsbestätigungen, die qualifiziert elektronisch signiert nach SigG23 sind, herbeigeführt. Diese sind, ähnlich einem papierbasierten Einwurfeinschreiben, Bestätigungen des De-Mail versendeten Providers bzw. empfangenden Providers, dass eine De-Mail an eine dezidierte De-Mail-Adresse zu einem bestimmten Zeitpunkt versendet wurde bzw. eigegangen ist. Eine Bestätigung enthält, jeweils für sich entsprechend, folgende Angaben:

- die De-Mail-Adresse des Absenders und des Empfängers;
- das Datum und die Uhrzeit des Versands/Eingang der Nachricht
- den Namen und Vornamen oder die Firma des akkreditierten Diensteanbieters, der die Versand-/Eingangsbestätigung erzeugt und
- die Prüfsumme der zu bestätigenden Nachricht.

Darüber hinaus besteht die Möglichkeit der förmlichen Zustellung nach den Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, per De-Mail. Hierzu ist die öffentliche Verwaltung berechtigt eine sogenannte Abholbestätigung zu verlangen, aus der

sich ergibt, dass sich der Empfänger nach dem Eingang der Nachricht im Postfach an seinem De-Mail-Konto sicher im Sinne des § 4 De-Mail G angemeldet hat und ebenfalls qualifiziert elektronisch signiert ist. Eine Abholbestätigung enthält folgende Angaben:

- die De-Mail-Adresse des Absenders und des Empfängers;
- das Datum und die Uhrzeit des Eingangs der Nachricht im De-Mail-Postfach des Empfängers;
- das Datum und die Uhrzeit der sicheren Anmeldung des Empfängers an seinem De-Mail-Konto im Sinne des § 4;
- den Namen und Vornamen oder die Firma des akkreditierten Diensteanbieters, der die Abholbestätigung erzeugt und
- die Prüfsumme der zu bestätigenden Nachricht.

Alle Bestätigungen sind, begleitend zu jeder De-Mail, ebenfalls gesetzeskonform zu archivieren, insbesondere auch um die Einhaltung einer Frist nachweisen zu können. Des Weiteren muss der DMDA sicherstellen, dass Nachrichten, für die eine Eingangsbestätigung oder eine Abholbestätigung erteilt worden ist, durch den Empfänger ohne eine sichere Anmeldung an seinem De-Mail-Konto erst 90 Tage nach ihrem Eingang gelöscht werden können. Dies muss bei einer automatisierten Archivierung zwingend berücksichtigt werden.

Ein weiterer Sonderfall innerhalb De-Mail ist der Identitätsbetätigungsdienst, gemäß § 6 De-Mail G. Hier kann der DMDA einen Dienst anbieten, mit dem der Nutzer - auf Basis seiner beim DMDA hinterlegten Daten - seine Identität gegenüber einem Dritten sicher elektronisch bestätigen lassen kann. Die Übermittlung der Identitätsdaten erfolgt mittels De-Mail, sodass diese besondere De-Mail, sofern relevant, ebenfalls gesetzeskonform archiviert werden muss.

Als letzter De-Mail-Sonderfall sei der De-Safe, auch Dokumentenablage gemäß § 8 De-Mail G, genannt. Hier kann der DMDA dem Nutzer ein Archiv zur sicheren und verschlüsselten Ablage von Dokumenten anbieten. Sollte diese Möglichkeit zur Archivierung genutzt werden, so ist jedoch im Einzelfall zu prüfen, ob die Anforderungen an eine gesetzeskonforme Archivierung gewahrt werden, da es sich hierbei lediglich um eine Archivierungsmöglichkeit handelt bei der der DMDA nur gewährleistet, dass die Dokumente sicher abgelegt werden und die Vertraulichkeit, die Integrität sowie die ständige Verfügbarkeit der abgelegten Dokumente gewahrt ist.

6 Zehn Praxistipps

6 Zehn Praxistipps

1 Journalarchivierung in Kombination mit Server- und Clientarchivierung

Jede Archivierungsart hat Ihre bestimmten Eigenschaften und unterschiedliche rechtliche Aspekte. So ist die Journalarchivierung eine notwendige Bedingung für Compliance – jedoch unter Umständen alleine nicht hinreichend. Die serverseitige Postfacharchivierung entlastet Datenbanken und Benutzer. Sie kann mit Ihrem normalerweise starren Regelwerk zwar sehr viel zur Prozessintegration beitragen, jedoch nicht alle Fälle der vorgangsbezogenen Ablage abdecken. Damit kann die Clientarchivierung Ihre Stärken in Form des Anwenderwissens ausspielen.

2 Untersagung des Versendens privater E-Mails

Das E-Mail-System ist Betriebsmittel und es besteht kein grundsätzliches Recht auf Privatnutzung. Heutzutage ist durch Smartphones und im Web frei zugängliche Mailprovider ohnehin kein zusätzlicher Mehrwert für Mitarbeiter gegeben, wenn sie die geschäftliche Mailadresse privat nutzen dürften.

3 Mitarbeitereinverständnis zur Archivierung eingehender privater E-Mails

Der Empfang von E-Mails privater Natur kann nicht verboten werden, da er ggf. außerhalb des Einflussbereichs der Mitarbeiter liegt. Wichtig ist, dass deshalb ein rechtsgültiges Einverständnis aller Anwender zustande kommt, dass sämtliche Nachrichten im geschäftlichen Postfach archiviert und – unter Einhaltung von Vertraulichkeitsspielregeln – auch evtl. von Dritten (z. B. Steuerprüfer) eingesehen und ausgewertet werden dürfen. Wird dieses versäumt gibt es evtl. einen Konflikt zwischen Datenschutz und Compliance – letztere kann sonst gefährdet sein!

4 Einbeziehung des Betriebsrats und des Datenschutzbeauftragten

Der Betriebsrat ist – auch wenn er nicht in jedem Szenario ein Mitbestimmungsrecht hat – ein wichtiger Partner im Projekt, um die Anwenderakzeptanz zu erhöhen. Mit Hilfe des Datenschutzbeauftragten können datenschutzrechtliche Bedenken im Vorfeld ausgeräumt werden. Ein zu spätes Einbinden dieser Parteien kann den zeitlichen Projektverlauf bei der Einführung der E-Mail-Archivierung am Ende enorm verlängern.

5 Aufbewahrungsfristen beachten

Für steuerlich relevante E-Mails sind dies laut GOBD >= zehn Jahre (zehn Jahre nach Abschluss des Geschäftsvorfalls+ Rest des laufenden Jahres). Danach ist Löschen erlaubt, aber keine Pflicht! Branchenspezifisch können jedoch noch zusätzliche Regelungen für – insbesondere längere – Aufbewahrungsfristen gelten. Informieren Sie sich daher frühzeitig, welche auf Ihr Unternehmen zutreffen.

6 Löschfristen personenbezogener Daten

Oftmals sind bei personenbezogenen Daten die Löschfristen, also die maximal zulässige Aufbewahrungsdauer, deutlich kürzer als die minimalen Aufbewahrungsfristen aus anderen Regelungen. Zum Beispiel bei Bewerbungen liegt die Löschfrist für personenbezogene Daten bei sechs Monaten. Durch technische und andere Maßnahmen lässt sich dieser Konflikt jedoch lösen (vgl. Kapitel 5.1). Ihr Datenschutzbeauftragter ist hierfür der richtige Ansprechpartner.

7 Archivierungsformat für E-Mails

Hier wird empfohlen eines der gängigen Standardformate zu wählen, wie z. B. das EML-Format oder das MSG-Format. Diese Formate sind genormt, allgemein akzeptiert und weitestgehend kompatibel mit allen gängigen E-Mail Programmen.

8 Anhänge immer im Originalformat aufbewahren

Schon aus kurz- bis mittelfristigen Handhabungsgründen sowie der Integrität archivierter Nachrichten, wurde oben die Empfehlung ausgesprochen, das Originalformat – eingebettet in die ursprüngliche Nachricht – beizubehalten. Des Weiteren wird empfohlen, die Attachments zusätzlich separat in einem Langzeitformat (z. B. PDF/A) zu archivieren, um spätere Lesbarkeit zu gewährleisten.

9 (Halb-)automatisierte, vorgangsbezogene Ablagestruktur im Archiv

Einerseits wird dies u. a. ansatzweise von der GOBD gefordert, andererseits bringt es zusätzlich echte Mehrwerte fürs Unternehmen. Anhand vielerlei Metadaten einer E-Mail sowie einer Analyse des Textes auf z. B. Rechnungs- oder andere Vorgangsnummern, lässt sich diese bereits im Posteingang vorsortieren. Anschließend kann ein Abgleich mit Daten aus CRM- oder ERP-Systemen erfolgen, um den Vorgangsbezug herzustellen. In der Folge sorgt dies für gesteigerte Transparenz aller Geschäftsvorfälle.

10 Aktive Mitwirkung von Key-Usern bei der Ausgestaltung des E-Mail-Managements

Niemand kennt die Prozesse und deren Problemzonen besser als die Anwender, die im Tagesgeschäft häufig mit E-Mails arbeiten. Oftmals entsteht hoher manueller Aufwand, um Informationen per E-Mail an die richtige Stelle weiterzuleiten, ältere Mails zu einem Vorgang zu finden oder Anhänge richtig einzuordnen. Hier liegt viel Potential für eine stark verbesserte Informationslogistik.

Anhang

Urteile und Fälle zum E-Mail-Management

Für die Maßgabe der Rechtsprechung in der E-Mail-Kommunikation sind vier Phasen des E-Mail-Kommunikationsprozesses grundlegend:[23]

1. Übermittlung der E-Mail an den Server des E-Mail-Providers.
2. Die E-Mail liegt auf dem Server des E-Mail-Providers.
3. Übersendung der E-Mail vom Server des E-Mail-Providers an den Herrschaftsbereich des Empfängers.
4. Die E-Mail ist im Herrschaftsbereich des Empfängers angekommen (bspw. im Posteingang des PCs).

Urteile zum E-Mail-Management

Verfassungsgerichtsurteil vom 2. März 2006 – 2 BvR 2099/04

Das BVerfG urteilte, dass eine E-Mail während des Übertragungsvorgangs durch das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) geschützt sei. Dieser Schutz endet, sobald die Übertragung abgeschlossen ist. Ist die E-Mail übertragen und liegt im Herrschaftsbereich des Nutzer greift das Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG.

Dem Urteil liegt eine Klage einer Richterin zugrunde, die sich gegen die gegen sie angeordnete Wohnungsdurchsuchung im Zuge von Ermittlungen über einen Verstoß des Dienstgeheimnisses richtete. Es sollten Kommunikationsverbindungsdaten auf PC und Mobiltelefon (u. a. E-Mails) ermittelt werden, um einen eventuellen Kontakt zu Journalisten nachzuweisen. Die Klägerin klagte gegen den Zugriff auf die privaten Daten gemäß Art. 10 GG. Das Urteil sah aber keine Verletzung des Art. 10 GG, da dieses Grundrecht Daten auf und während des Kommunikationswegs schützt, nicht aber, wenn sich die Daten bereits an einem Ort gespeichert/gelagert befinden. E-Mails, die im POP3-Verfahren auf einer lokalen Festplatte gespeichert wurden, sind deshalb nicht mehr vom Fernmeldegeheimnis geschützt. Ist der Übertragungsvorgang abgeschlossen, greift das Schutzrecht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG. Gleichzeitig erkannten die Richter an, dass Art. 10 GG entwicklungsoffen ist und sich eben nicht auf die von der Deutschen Bundespost angebotenen Fernmeldedienste beschränkt, sondern die Entwicklung der TK-Techniken berücksichtigt. Daten sind in besonderer Weise schützenswert, wenn der Eingriff heimlich und nicht offen stattfindet, wie etwa bei der Erstellung von Bewegungsprofilen. Ist der Zugriff offen und nicht-heimlich, stehen dem Betroffenen Maßnahmen zur Verfügung, dem Zugriff entgegenzuwirken (z. B. mittels anwaltlichem Beistand). Der Zugriff auf Daten und die damit verbundene Einschränkung von Art. 2 (Phase 2+4) bzw. Art. 10 (Phase 1+3) bedarf in jedem Fall einer rechtlichen Grundlage und der Abwägung der Verhältnismäßigkeit, urteilten die Richter.

23 BVerfG: Recht auf informationelle Selbstbestimmung schützt gespeicherte TK-Verbindungsdaten beim Teilnehmer, MMR 2006, 217.

Verfassungsbeschwerde vom 18. Juni 2009

Gemäß dem o.g. Urteil urteilte das BVerfG, dass Daten fernmeldegeschützt gemäß Art. 10 GG sind, solange sie übertragen werden (Phase 1+3).

Die Verfassungsbeschwerde richtete sich gegen die Beschlagnahmung von E-Mails eines Mitarbeiters durch sein Unternehmen. Dieses hatte ein Ermittlungsverfahren gegen einen Dritten angestrengt, im Zuge dessen die E-Mails des Angestellten als Beweismaterial dienen sollten. Das zuständige Amtsgericht ordnete im Zuge der Ermittlungen die Durchsuchung der Wohnung des Mitarbeiters an, gegen den selbst aber nicht ermittelt wurde. Der Mitarbeiter nutzte für den Zugriff auf seine E-Mails das IMAP. Empfangene E-Mails wurden nicht auf seinen lokalen Rechner übertragen, sondern blieben in einem zugangsgesicherten Bereich auf dem Mailserver seines Providers gespeichert. Nach Ansicht des Mitarbeiters unterfielen die gespeicherten E-Mail dem Schutzbereich des Fernmeldegeheimnisses, da die finale Übertragung nicht abgeschlossen war. In einem ersten Urteil, sah das zuständige Landgericht die Übertragung abgeschlossen. Die Speicherung auf einem beim Teilnehmer vorgehaltenen Gerät sei mit der Speicherung auf dem PC vergleichbar und der Übermittlungsvorgang sei demzufolge abgeschlossen. Diesem Urteil entsprachen auch die Richter des BVerfG und ergänzten somit das Urteil aus dem Jahr 2006. Es sei unerheblich, ob die E-Mails auf dem Server zwischen- oder endgespeichert worden sind. Zwar seien die Rechte des Mitarbeiters eingeschränkt worden, dies aber auf einer rechtlichen Grundlage. Zum Zwecke der wirksamen Strafverfolgung, Verbrechensbekämpfung und des öffentlichen Interesses an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren, muss der Gesetzgeber Einschränkungen des Fernmeldegeheimnisses ermöglichen. Andernfalls könnte jeder Nutzer belastende E-Mails durch eine Auslagerung auf den Mailserver seines Providers vor dem Zugriff der Strafverfolgungsbehörden entziehen.

Bundesfinanzhofurteil vom 24. Juni 2009 - IV R 26/06

Der BFH urteilte 2009, dass neben den außersteuerlichen und steuerlichen Büchern, Aufzeichnungen und Unterlagen zu Geschäftsvorfällen auch alle Unterlagen aufzubewahren sind, die zum Verständnis und zur Überprüfung der für die Besteuerung gesetzlich vorgeschriebenen Aufzeichnungen im Einzelfall von Bedeutung sind.

Nach herrschender Meinung ergibt sich aus dem Urteil, dass neben Büchern, Aufzeichnungen, Inventaren etc. die Archivierungspflicht auch sonstige Unterlagen betrifft, soweit sie für die Besteuerung von Bedeutung sind. Das heißt, wenn aufzeichnungspflichtige Unterlagen wie Geschäftsbriefe per E-Mail versendet werden, müssen folglich auch diese archiviert werden. Archivierungspflichtig sind auch die Datenanhänge von E-Mails, wenn sie die Nachricht verständlich machen oder vervollständigen. Aus den GoBD ergeht jedoch, dass die Aufbewahrungspflicht nicht für E-Mails besteht, wenn diese eine archivierungspflichtige Datei lediglich im Anhang transportieren.

Urteile zur privaten E-Mail Nutzung

Landesarbeitsgerichtsurteil vom 7. April 2006 – 10 TaBV 1/06 (ArbG Dortmund)

Das LAG urteilte, dass das betriebliche Verbot über die Privatnutzung des Internet- und E-Mail-Verkehrs nicht dem Mitbestimmungsrecht des Betriebsrats unterliegt. Zudem haben Arbeitnehmer keinen Anspruch auf die Privatnutzung von Betriebsmitteln, auch nicht auf die Privatnutzung des Internet und E-Mail-Systems.

In den Jahren 1997 bis 2005 hatte ein Unternehmen per Dienstanweisung die private Nutzung von Internet und E-Mail ausdrücklich erlaub. 2005 plante das Unternehmen die private Internetnutzung gänzlich zu verbieten und die Privatnutzung des E-Mail-Systems mit Regeln zu belegen. Der Betriebsrat forderte ein Mitbestimmungsrecht. Das Unternehmen lehnte dies ab. Vor dem LAG forderte der Betriebsrat eine einstweilige Verfügung gegen das Inkrafttreten der Dienstanweisung. Das LAG lehnte das Begehren des Betriebsrates ab. Die Gestattung der Privatnutzung von Internet und E-Mail ist eine freiwillige Leistung des Unternehmens, auf die ein Arbeitnehmer keinen Anspruch hat. Bei Internet und E-Mail handelt es sich um Betriebsmittel.
Für den Betriebsrat leitet sich aus § 87 Abs. 1 BetrVG kein Mitbestimmungsrecht ab, da dieser nur Mitbestimmungsrechte hat, sofern es sich um Maßnahmen des sogenannten Ordnungsverhaltens der Arbeitnehmer im Betrieb handelt. Bei der betreffenden Dienstanweisung handele es sich aber um ein Direktionsrecht des Unternehmens. Ein Mitbestimmungsrecht des Betriebsrats könne sich allenfalls dann ergeben, wenn konkrete Regelungen zur Privatnutzung von Internet und E-Mail aufgestellt werden sollten.

Landesarbeitsgerichtsurteil vom 31. Mai 2010 – 12 Sa 875/09

Das LAG urteilte, dass eine Kündigung eines langjährigen Arbeitnehmers gerechtfertigt ist, wenn dieser exzessiv das dienstliche E-Mail-System privat nutzt. Dies kann auch ohne Anmahnung erfolgen.

Für den klagenden Mitarbeiter existierte eine Dienstanweisung aus dem Jahr 1997, die die Unterbrechung der Arbeitszeit zur Erledigung privater Angelegenheiten untersagte. In der Vergangenheit jedoch hat die Gemeinde, bei der der Mitarbeiter angestellt war, die Privatnutzung des E-Mail-Systems in den Pausen geduldet. Der Mitarbeiter hatte während seiner Dienstzeit von seinem dienstlichen PC u. a. private E-Mail-Kommunikation geführt.
Die Gemeinde sprach eine außerordentliche Kündigung mit sozialer Auslauffrist aus.
Der Mitarbeiter klagte vor dem Arbeitsgericht Dortmund auf Kündigungsschutz, da sich aus der Privatnutzung kein Arbeitsrückstand ergeben habe und die Privatnutzung durch die Gemeinde nicht untersagt gewesen sei. Zunächst gab das Arbeitsgericht der Klage statt, da eine außerordentliche Kündigung nicht ohne vorherige Abmahnung auszusprechen sei.
Das Arbeitsgericht hatte die Privatnutzung des E-Mail-Systems als nicht »ausschweifend« gewertet. In einer Berufung vor dem LAG legte die Gemeinde eine Beweislast vor, gemäß der der Mitarbeiter durchschnittlich weit über 100 private E-Mails pro Tag empfangen habe.
Da sich die vorgelegten E-Mails im Sinne eines Dialogs aufbauten, ging das Gericht davon aus,

dass sich der Sendeumfang in ähnlicher Größenordnung bemaß, so dass die Aussage des Mitarbeiters, nicht auf alle E-Mails geantwortet zu haben, für die Richter als widerlegt galt. Die Richter urteilten, dass der Mitarbeiter aufgrund dieser »exzessiven« Privatnutzung seine dienstlichen Aufgaben nicht erfüllen konnte. Das LAG sprach die außerordentliche Kündigung wirksam. Die Richter urteilten, dass das exzessive Privatnutzen von E-Mails eine außerordentliche Kündigung auch ohne vorherige Abmahnung rechtfertigt. Bei dieser exzessiven Privatnutzung und der Vernachlässigung der Dienstaufgaben könne auch die langjährige Betriebszugehörigkeit und das Lebensalter des Mitarbeiters nicht berücksichtigt werden. Die Fortsetzung des Dienstverhältnisses könne dem Betrieb nicht zugemutet werden. Die Richter vertraten die Auffassung, dass nicht einmal die soziale Auslauffrist dem Betrieb zuzumuten gewesen sei.

Landesarbeitsgerichtsurteil Berlin-Brandenburg vom 16. Februar 2011

Das LAG Berlin-Brandenburg urteilte, dass ein Arbeitgeber nicht zum Dienstanbieter wird, weil er seinen Beschäftigten gestattet, den dienstlichen E-Mail-Account auch privat zu nutzen. Das LAG urteilte, dass E-Mails, die im Posteingang bzw. im Postausgang liegen, nicht durch das Fernmeldegeheimnis vor dem Zugriff des Arbeitgebers geschützt sind.

Das Urteil ging auf eine Klage einer Arbeitnehmerin gegen ihren Arbeitgeber zurück, der den Zugriff auf die im elektronischen Postfach vorhandenen E-Mails vollständig verhindern sollte. Die Arbeitnehmerin war arbeitsunfähig erkrankt, so dass sich der Arbeitgeber Zugriff auf den E-Mail-Account verschaffte, um geschäftsrelevante E-Mails abzurufen. Die Angestellte warf dem Arbeitgeber vor, dass dieser mit dem Zugriff ihre Persönlichkeitsrechte verletzt hatte, da durch den Abruf auch private E-Mails lesbar wurden. Das LAG urteilte, dass der Schutz privater E-Mails nur dann gewährleistet werden muss, wenn der Arbeitgeber auch Dienstanbieter ist, d.h. geschäftsmäßig Post- oder Telekommunikationsdienste erbringt. Das LAG schrieb der Angestellten zudem eine Eigenverantwortlichkeit zu, da sie keine Stellvertreterregelung für ihre Abwesenheit vorgenommen hatte, die den Zugriff auf dienstliche E-Mails regelte, obgleich der Arbeitgeber für diesen Fall verpflichtende Regelungen getroffen hatte. Versuche des Arbeitgebers, die Angestellte zu kontaktieren, scheiterten, da die Angestellte auf Anrufe und E-Mails nicht reagierte. So wurde auch der Vorwurf, der Arbeitgeber habe keine Einwilligung erholt, abgewiesen. Das Persönlichkeitsrecht könne zudem eingeschränkt werden, sofern der Zugriff ein schutzwürdiges Interessen des Arbeitsgebers darstellt. Im verhandelten Fall entschied das Gericht, dass die Interessen des Arbeitgebers nach der Aufrechterhaltung eines ungestörten Arbeitsablaufs überwogen. Zudem hatte der Arbeitgeber alle formellen Anforderungen eingehalten: Der Datenschutzbeauftragte wurde kontaktiert, beim Zugriff auf den Account war ein Betriebsratsmitglied als Zeuge anwesend, und bestätigte dem Gericht, dass lediglich dienstliche E-Mails abgerufen worden waren. Bereits am 17. August 2010 wurde die Klage vom Arbeitsgericht abgewiesen. Die Beschäftigte ging in Berufung, das LAG bestätigte das Urteil und wies die Klage ab.

Die Autoren

Gesa Diekmann,
Bitkom e.V.

Gesa Diekmann ist Juristin und leitet seit 2014 den Wissenschaftlicher Dienst im Bitkom. Ihr Tätigkeitsschwerpunkt ist das Datenschutzrecht. Zuvor war sie als Unternehmensjuristin und als Wissenschaftliche Mitarbeiterin im Deutschen Bundestag tätig.

Marc Drögsler,
inovoo GmbH

Marc Drögsler, Dipl.-Ing., ist seit 2007 als CTO bei der inovoo GmbH tätig und verantwortet das Produktmanagement im Bereich Multi Channel Capture und Enterprise Mobile Solutions. Im Rahmen seiner Tätigkeit begleitete er viele große Unternehmen vom klassischen Scanprozess auf dem Weg in die Digitalisierung. Das Know-how hierfür generierte Herr Drögsler während seiner mehrjährigen internationalen Projekterfahrung in unterschiedlichen Branchen, wo er verschiedenste Ansätze zur Digitalisierung erfolgreich umsetzen konnte.

Steffen Ewald,
ELO Digital Office GmbH

Steffen Ewald, (LL.B. Wirtschaftsrecht / LL.M Int. Lizenzrecht) ist seit Ende 2014 bei der ELO Digital Office GmbH tätig. Als Stabstelle für den Bereich »Recht & Compliance« kümmert er sich um die rechtlichen Angelegenheiten der ELO Digital Office GmbH.

Frank Früh,
Bitkom e.V.

Frank Früh, Dipl.-Kaufmann, ist seit 2014 Bereichsleiter für Enterprise Content Management im Bitkom e.V. und fachlich wie organisatorisch für alle Themen rund um Dokumentenmanagement, elektronische Akte sowie Input- und Output-Management verantwortlich. Er hat sich schon während seines Studiums intensiv mit der Wirtschaftsinformatik auseinandergesetzt und war viele Jahre in der Beratung rund um das Thema Records Management in der Pharmaindustrie tätig.

Stephan Gehling,
H&S Heilig und Schubert InformationsManagement GmbH

Stephan Gehling, MBA, ist seit 2007 bei der H&S Heilig und Schubert InformationsManagement GmbH in Schwabach tätig und verantwortet den Geschäftsbereich E-Mail-Management. Als Wirtschaftsinformatiker war er unter anderem bei der Siemens AG für den Lösungsvertrieb im Umfeld IP Networking und Security verantwortlich. Im Rahmen seiner Bitkom-Aktivitäten engagiert sich Herr Gehling im Vorstand des Arbeitskreises Input & E-Mail-Management sowie im ECM-Lenkungsausschuss.

Sven Gelzhäuser,
1&1 De-Mail GmbH

Sven Gelzhäuser, Diplom-Wirtschaftsjurist (FH), befasst sich seit 2006 mit dem Thema der qualifizierten elektronischen Signatur und der rechtssicheren Nachweisbarkeit von digitalen Prozessen. Seit 2008 ist Herr Gelzhäuser in verschiedenen Funktionen innerhalb des Produktmanagements der 1&1 De-Mail GmbH (ein Tochterunternehmen der United Internet AG) verantwortlicher Ansprechpartner im Rahmen der Entwicklung, Implementierung und Weiterentwicklung der De-Mail. Seit 2012 begleitet er diese Themen auch in Funktion des Datenschutzbeauftragten.

Stefan Groß,
Peters, Schönberger & Partner

Stefan Groß ist Steuerberater, Certified Information Systems Auditor und Partner der Kanzlei Peters, Schönberger & Partner. Er berät vornehmlich an der Schnittstelle Steuerrecht und Neue Medien und verfügt über eine ausgeprägte Expertise im europäischen Umsatzsteuerrecht. Stefan Groß gilt als Fachmann im Bereich der steuerrechtlichen Aspekte der E-Rechnung sowie der GoBD und ist ehrenamtlich als Leiter des Arbeitskreises »ECM-Compliance« des Bitkom e.V. sowie als Vorstandsvorsitzender des Verbandes elektronische Rechnung (VeR) tätig. Seine Steuerrechtsexpertise kommt in zahlreichen Veröffentlichungen und Vorträgen zum Ausdruck.

Daniel Mikeleit,
ELO Digital Office GmbH

Daniel Mikeleit, Dipl. Wirt.-Ing. (FH), ist seit 2004 bei der ELO Digital Office GmbH tätig. Er ist Fachexperte für ECM-Produkte im Microsoft- und IBM-Umfeld. Darüber hinaus ist er auch als Berater und Autor spezialisiert auf das wichtige Thema »Effizientes E-Mail-Management«.

Julia Schubert,
Bitkom e.V. (bis September 2015)

Julia Schubert, Politikwissenschaft M.A., war bis September 2015 beim Bitkom beschäftigt. Bevor sie in den Wissenschaftlichen Dienst des Bitkom wechselte, unterstützte sie den Fachbereich Enterprise Content Management. Dort betreute sie vor allem die Branchen-Website und unterstützte den Fachbereich bei der Organisation und Umsetzung diverser Branchenevents.

Andreas Schulz,
Bitkom e.V.

Andreas Schulz ist seit 2014 als Berater im Team von Bitkom Consult für den Bereich Datenschutz zuständig. Darüber hinaus ist er als Referent bei der Bitkom Akademie aktiv und leitet unter anderem zahlreiche Online-Seminare zu Datenschutzthemen. Andreas Schulz hat Informationswissenschaften in Potsdam studiert und ist seit 2010 zertifizierter Datenschutzbeauftragter.

Antje Sommer,
Retarus GmbH

Antje Sommer, Dipl.-Kauffrau, ist seit sechs Jahren für E-Mail-Services tätig. Bei der Telekom Deutschland GmbH war sie bis 2013 als Commercial Managerin für T-Online E-Mail zuständig und betreut seit 2014 als Produktmanagerin das E-Mail Security Portfolio der retarus GmbH. Bei dem globalen Managed-Services-Anbieter verantwortet sie u. a. die rechtskonforme Weiterentwicklung der Angebote für E-Mail-Archivierung und Verschlüsselung.

Jürgen Vogler,
Mentana-Claimsoft GmbH

Jürgen Vogler, Informatiker für Medizinökonomie, war bis Februar 2014 Geschäftsfeldleiter E-Business und Produktmanager De-Mail bei der Francotyp Postalia Vertrieb und Service GmbH, bis er im März 2014 die Geschäftsführung der Mentana-Claimsoft übernahm. Herr Vogler hat seinen fachlichen, vertrieblichen und technischen Hintergrund im Consulting und Vertrieb bei großen nationalen und internationalen Unternehmen erwerben können und ist einer der ersten Teilnehmer der De-Mail-Initiative. Herr Vogler ist ausgewiesener Experte für Consulting, De-Mail, In-/Outbound-Prozesse und ECMS, DMS, ECM und engagiert sich im Vorstand des Bitkom Arbeitskreises »Input- & E-Mail-Management«.

Abkürzungsverzeichnis

Abs.
Absatz

AktG
Aktiengesetz

AO
Abgabenordnung

BGB
Bürgerliches Gesetzbuch

BDS
Bundesdatenschutzgesetz

bspw.
bspw.

bzw.
beziehungsweise

DMDA
De-Mail-Diensteanbieter

ECM
Enterprise Content Management

etc.
et cetera, und andere

ff.
fortfolgende

GenG
Gesetz betreffend die Erwerbs- und Wirtschaftsgenossenschaften

GmbHG
Gesetz betreffend die Gesellschaften mit beschränkter Haftung

GoBD
Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff

HGB
Handelsgesetzbuch

i.d.R.
in der Regel

i.V.m.
in Verbindung mit

IT
Informationstechnik

LTE
Long Term Evolution

NSF
Notes Storage Facility

PC
Personal Computer

PST
Personal Storage Table

SigG
Gesetz über Rahmenbedingungen für elektronische Signaturen

SOX
Sarbanes-Oxley Act

StGB
Strafgesetzbuch

TKG
Telekommunikationsgesetz

u. a.
unter anderem

UStG
Umsatzsteuergesetz

vgl.
vergleiche

z. B.
zum Beispiel

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom