

SP1

Rechtliche Anforderungen
bei der elektronischen Speicherung
und Archivierung von E-Mails
unter Microsoft Exchange Server 2010
(Stand Service Pack 1)

Inhaltsverzeichnis

1. Zu diesem Whitepaper	3
2. Einleitung	4
3. Neuerungen im Bereich Archivierung in Microsoft Exchange Server 2010 SP1	4
4. Rechtlich relevante Neuerungen von SP1 auf einen Blick	6
5. Historie und Point of no excuse.....	6
6. Die drei Grundprinzipien der Archivierung.....	7
7. Zwischen Herausforderung und Wissensdefizit.....	7
8. Die private Nutzung des betrieblichen/geschäftlichen E-Mail-Accounts.....	7
9. Steuer- und Handelsrechtliche Belange	8
10. Rechtsichere oder revisionssichere Archivierung? Die Irrtümer.	8
11. Suchen und Finden	10
12. Aufbewahrung und Archivierung	10
13. Aufbewahrungspflicht.....	10
14. Handelsbriefe.....	10
15. Geschäftsbriefe	11
16. Elektronische Rechnungen	11
17. Art der Aufbewahrung.....	11
18. Ort der Aufbewahrung	12
19. Herausgabe aufbewahrungspflichtiger Daten.....	13
20. Datenschutz.....	14
21. FAQ Fragenkatalog – Alle Antworten in Kurzform	15
22. FAQ Fragenkatalog – lange Fassung.....	16
 Factsheet/Kontaktdaten	 26

1. Zu diesem Whitepaper

PRW Rechtsanwälte publizieren regelmäßig zu rechtlichen Themen im IT-Umfeld. Dieses Whitepaper wurde von uns für Microsoft Partner erstellt. Es befasst sich mit dem Thema IT-Compliance anhand der Archivierungsfunktionen von Microsoft Exchange Server 2010 mit Service Pack (SP) 1. Die nachfolgenden Ausführungen erheben keinen Anspruch auf Vollständigkeit. Sie geben lediglich einen ersten Einblick in eine sich noch entwickelnde Rechtsthematik und sollen der allgemeinen Information dienen. Berücksichtigt wurde hier ausschließlich die Rechtslage in Deutschland. Dieser Leitfaden gibt einen Überblick über eine Reihe von einzuhaltenden gesetzlichen Vorgaben sowie Tipps zu ihrer Umsetzung und erläutert die dabei zu beachtenden Fallstricke. **Die Rechtsberatung im Einzelfall kann hierdurch jedoch nicht ersetzt werden.** Insbesondere können im hier gewählten Umfang keine branchenmäßigen Besonderheiten, wie etwa das Thema Verschwiegenheit/Geheimhaltung im Berufs- oder Bankenrecht, abgebildet werden. Speziell im Bereich der Archivierung haben viele Sparten eine ganze Reihe von Spezialvorschriften, beispielsweise im Bereich der Archivierungsfristen. Dieses Whitepaper greift einige der Rechtsthemen im Zusammenhang mit der E-Mail Archivierung auf und zeigt Lösungen für eine rechtskonforme Archivierung. Um die angebotenen Lösungen an konkreten Beispielen und Einstellungen aufzuzeigen, wurden die rechtlichen Anforderungen an den Möglichkeiten von Microsoft Exchange Server 2010 und Microsoft Outlook 2010 gespiegelt.

Für die Klärung von technischen Fragen standen uns Mitarbeiterinnen und Mitarbeiter aus dem Hause infoWAN Datenkommunikation GmbH beratend zur Verfügung. Hierfür möchten wir uns ausdrücklich bedanken.

Die Autoren dieses Papers bedanken sich für die vielen positiven Zuschriften und auch für die kritischen Anmerkungen zur ersten Version dieses Papiers. Dieses Feedback und die technischen Weiterentwicklungen im Service Pack 1 sind in dieser zweiten Version berücksichtigt.

Markenrechtlicher Hinweis: Die in diesem Dokument wiedergegebenen Bezeichnungen können Marken, insbesondere aus dem Microsoft Markenportfolio sein. Die unberechtigte Benutzung durch Dritte für eigene Zwecke können die Rechte der Inhaber verletzen.

PRW Rechtsanwälte

München, im November 2010

2. Einleitung

Archivierung ist vom Grundsatz her etwas **Natürliches**. Die Natur macht es uns an vielen Stellen vor. Denken wir nur an die Jahresringe des Baumes. Sie erzählen seine Geschichte. Der Mensch hat ursprünglich Dinge aufbewahrt, weil er es wollte, um Wissen oder Werte zu bewahren. Wir bewahren immer noch auf, weil wir es wollen, jedoch zunehmend auch, weil wir es müssen. Noch häufiger jedoch bewahren wir Dinge auf, von denen wir gar nicht mehr wissen, dass wir sie aufbewahren. Das nennen Spötter dann „Storage in Vollendung“.

Wird die Aufbewahrung systematisiert, bewegen wir uns mit ersten Schritten in Richtung Archivierung. Die moderne Archivierung ist digital und vielschichtig. Sie ist nicht einfach, aber mit Hilfe dieses Whitepapers wird sie für die Microsoft Partner bei der Umsetzung einfacher.

Die wichtigste rechtliche Frage zuerst.

„Kann mit den Archivierungsmöglichkeiten von Microsoft Exchange Server 2010 eine rechtskonforme Archivierung sichergestellt werden“.

Die eindeutige Antwort ist: *„Ja“*.

Microsoft Exchange Server 2010 kann jedoch nicht alle Funktionen bieten, wie sie von im Markt erhältlichen digitalen Archivsystemen teilweise bereitgestellt werden. Und das ist gut so, weil dort gelegentlich Funktionalitäten angeboten werden, die rechtlich nicht gefordert sind oder sogar aus rechtlicher Sicht bedenklich sind. Dazu später im Detail mehr.

3. Neuerungen im Bereich Archivierung in Microsoft Exchange Server 2010 SP1

Im folgenden Abschnitt werden die technischen Neuerungen vorgestellt, die mit Service Pack 1 für Microsoft Exchange Server 2010 im Bereich Archivierung zur Verfügung stehen.

• Vorschau bei der Multimapboxsuche

Die neue Vorschaufunktion der Multimapboxsuche ermöglicht es, die ungefähre Anzahl der zur Suche passenden Elemente zu sehen, bevor die Nachrichten in die Discovery Mailbox kopiert werden. Diese Funktionalität ermöglicht es der mit der Suche betrauten Person die Suchanfrage bei Bedarf anzupassen. So können zum Beispiel langlaufende Suchvorgänge, die sehr viele Treffer produzieren würden, gar nicht erst gestartet werden, um so diese Zeit zu sparen. Umgekehrt kann in Fällen mit ungewöhnlich wenigen Treffern die Suche unmittelbar erweitert werden.

Anmerkungen bei der Multimapboxsuche

Mit der Suche betraute Personen können Nachrichten, die von der Suche zurückgeliefert werden, mit Anmerkungen versehen. Dieses ist eine wichtige Funktion im Rahmen des Discovery-Prozesses.

De-Duplizierung bei der Multimapboxsuche

Die Multimapboxsuche beinhaltet eine Daten De-Duplizierungsfunktionalität. Wenn die Funktion aktiviert ist, wird bei der Suche nur eine Instanz eines gefundenen Objekts in die Discovery Mailbox kopiert, auch wenn dieses Objekt zum Beispiel in mehreren Postfächern enthalten ist. Dadurch werden die Suchresultate übersichtlicher und die Suche läuft schneller.

• Stellvertreterzugriff auf das persönliche Archiv

Sobald die Berechtigung für einen Stellvertreter auf ein Postfach gesetzt wurde, hat der Stellvertreter automatisch auch Zugriff auf das Archiv. Das Archiv wird zusammen mit dem Postfach in Outlook 2010 angezeigt. Dank dieser Verbesserung kann die Archivfunktion auch dann sinnvoll genutzt werden, wenn ein Benutzer einen oder mehrere Stellvertreter eingerichtet hat. Gleiches gilt für die Nutzung der Archivierung bei Funktionspostfächern.

- **Speicherung/Auslagerung des Archivpostfachs auf anderen Exchange Datenbanken und in der Cloud**

Das persönliche Archiv eines Anwenders muss nicht mehr im gleichen Postfachspeicher liegen wie das eigentliche Postfach, sondern kann nun auch auf andere Exchange Datenbanken verschoben werden. Entsprechend ist es nun möglich, die Archivdaten auf anderen Servern oder anderen Speichereinheiten abzulegen. So kann das Archiv zum Beispiel auf einen Exchange Server mit geringerer Ausfallsicherheit ausgelagert werden oder das Archiv auf kostengünstigere Speichermedien gelegt werden.

Auch kann das Archiv für ein Postfach in die Cloud gelegt werden. Mit Microsoft Office 365 (Nachfolger von Microsoft BPOS) kann dann für einen Benutzer ein Postfach auf einem Exchange Server im eigenen Rechenzentrum eingerichtet werden, für das das Archiv in der Cloud bei Microsoft im Rechenzentrum liegt.

Die Exchange 2010 SP1 Version der grafischen Oberfläche ermöglicht es Ihnen das Archivpostfach unabhängig vom persönlichen Postfach zu verschieben. Exchange 2010 SP1 unterstützt folgende Kombinationen:

- Postfach und Archiv „On-Premises“ in der selben Datenbank
- Postfach und Archiv „On-Premises“ auf unterschiedlichen Datenbanken
- Postfach und Archiv „in the Cloud“
- Postfach „On-Premises“ und Archiv „in the Cloud“
- Vereinfachter Import in das Archiv und Export aus dem Archiv

Administratoren haben nun über die Exchange Management Shell die Möglichkeit, PST-Dateien direkt in das persönliche Archivpostfach der Anwender zu importieren. Dies erspart beim Import der Daten den Umweg über das persönliche Postfach in das Archiv. Alternativ kann eine PST-Datei aber auch in das primäre Postfach importiert werden. Generell kann der Administrator den Anwender somit beim Import seiner Altdaten besser unterstützen. Außerdem ist nun der Export sowohl des Postfachs als auch des Archivs in eine PST-Datei mittels eines Powershell Cmdlets möglich.

- **Verbesserungen der grafischen Oberfläche für den Administrator**

Exchange Server 2010 SP1 bietet die Möglichkeit, Verwaltungsaufgaben über die Exchange Verwaltungskonsole oder das Exchange Control Panel zu erledigen. Funktionen, die bereits über die Exchange Management Shell verfügbar waren, können nun auch über die grafische Oberfläche erreicht werden.

Im Bereich Archivierung ist es nun möglich, Beibehaltungsrichtlinien und die dazugehörigen Flags/Tags über die Exchange Verwaltungskonsole anzulegen und zu verwalten. Außerdem ist es nun möglich Berechtigungen für öffentliche Ordner, DAG Einstellungen und Mittel zur Beweissicherung (Litigation Hold) über die grafische Oberfläche zu erreichen.

- **Richtlinien für Kalender und Aufgaben**

Exchange 2010 SP1 bringt nun die Unterstützung für die Erstellung von Aufbewahrungsrichtlinien für die Standardordner Kalender und Aufgaben.

- **Änderungen bei benutzerspezifischen Flags/Tags**

Anwender können nun auch persönliche Flags/Tags auswählen, die in ihrer vom Administrator zugewiesenen Aufbewahrungsrichtlinie nicht enthalten sind. Dazu müssen die Benutzer vom Administrator jedoch entsprechend berechtigt werden und sie können nach wie vor keine eigenen Flags/Tags erstellen, so dass die Kontrolle über die verwendeten Flags/Tags weiterhin beim Unternehmen liegt.

- **Audit-Funktion für Postfachzugriffe**

Der Service Pack 1 liefert auf Wunsch ein umfassendes Protokoll aller Postfachzugriffe durch den Anwender aber auch durch Stellvertreter oder Administratoren. Diese Funktion kann für jedes Postfach individuell aktiviert werden. Die Logdateien liegen in dem Postfach des Anwenders in einem versteckten Bereich und werden standardmäßig für 90 Tage aufbewahrt.

- **Entfernung einiger Aktionen bei den Flags/Tags**

Die Flags/Tags „Als abgelaufen markieren“, „In den Ordner gelöschte Objekte verschieben“ und „In Managed Folder verschieben“ wurden in SP1 abgeschafft. In Englisch sind das die drei Punkte „Mark as Past Retention Limit“, „Move to Deleted Items Folder“ und „Move to a Managed Custom Folder“.

4. Rechtlich relevante Neuerungen von SP1 auf einen Blick

Dieser Abschnitt beschreibt die rechtlich relevanten Neuerungen von SP1 auf einen Blick.

Zum einen sind hier die im vorherigen Abschnitt dargestellten Neuerungen im Bereich Archivierung und Multimapboxsuche zu nennen.

Zum anderen können Anwender ihren Kalender nun auch für anonyme Nutzer freigeben. Diese Funktion muss zwar zuvor von einem Administrator freigeschaltet werden, aber sie legt das Thema Datenschutz und Privatsphäre damit ein Stück weit mehr in die Hände der Unternehmen und Ihrer Mitarbeiterinnen und Mitarbeiter.

5. Historie und Point of no excuse

Im Jahre 1996 wurde Microsoft Exchange breit in den Markt eingeführt. Dem Thema E-Mail-Sicherheit im Sinne von Virenabwehr widmeten sich zunächst andere Hersteller. Erst 10 Jahre später (2006) brachte Microsoft mit der Forefront Suite ihr eigenes hochwertiges und maßgeschneidertes Security Produkt in den Markt. Forefront hat in vielen Tests seine Qualität bewiesen. Niemand wird ernsthaft bezweifeln, dass auch zwischen 1996 und 2006 Antivirusprogramme notwendig waren. Das ist die berechtigte Sicht der IT-Spezialisten. Aus juristischer Sicht wird anders argumentiert. Wenn der Originärhersteller (Microsoft mit Forefront) selbst ein Security Produkt anbietet, dann setzt er damit wohl den Mindeststandard. Aus einem Urteil des Landgerichts Hamburg wurde verschiedentlich abgeleitet, dass jeweils mindestens drei aktuelle unterschiedliche Virenprogramme einzusetzen sind. Das hier benannte Urteil¹ ist zwar nicht unumstritten. Mit Microsoft Forefront sind die Anwender – nach der derzeitigen Rechtsprechung – auf jeden Fall auf der juristisch sicheren Seite, da Forefront mit drei oder mehr Engines scannt.

Im Jahre 2002 wurden die Vorschriften zur digitalen Steuerprüfung (GDPdU) eingeführt. Diese Vorschriften befassen sich auch mit der Aufbewahrung von E-Mails. Digitale Archivhersteller haben dies erkannt und sehr zeitnah Lösungen angeboten. Microsoft bietet mit Exchange Server 2010 nun auch Archivierungsmöglichkeiten für E-Mails an. Die Sicht der IT-Spezialisten auf das Thema Archivierung ist eher technisch getrieben und war bisher stark auf den Begriff der Revisionssicherheit ausgerichtet. Aber auch hier gilt: Wenn der Originärhersteller (Microsoft mit Exchange Server 2010) selbst ein Archivierungstool anbietet, mit dem eine rechtlich einwandfreie Archivierung möglich ist, dann ist für eine unterlassene Archivierung kein argumentativer Platz mehr. Aus der Sicht der Steuerbehörden gelten die Vorschriften bereits rückwirkend seit 2002. Spätestens seit Microsoft Exchange Server 2010 ist E-Mail-Archivierung nun auch technischer Standard.

¹ LG Hamburg, Urteil vom 18.07.2001, 401 O 63/00, NJW 2001, 3486, 3487.

6. Die drei Grundprinzipien der Archivierung

Ein digitales Archivsystem sollte drei Grundprinzipien bedienen können. Es sollte im Stande sein, dass zu archivieren, was der Archivierende archivieren möchte, es sollte das archivieren können, was der Archivierende archivieren muss und es sollte auf keinen Fall das dauerhaft archivieren, was der Archivierende nicht archivieren darf (Stichwort Datenschutz). Das klingt einfach, ist es aber nicht.

7. Zwischen Herausforderung und Wissensdefizit

Ein kleiner Ausschnitt aus dem Bereich der Herausforderungen, die Unternehmen und Institutionen annehmen müssen. Im Bereich der zwingenden gesetzlichen Archivierungsvorschriften gibt es keine Einheitlichkeit zwischen den staatlichen Regelungen (nicht mal innerhalb der EU). Multinationale Unternehmen müssen sich somit nach den jeweils geltenden nationalen Vorschriften richten. Dies ist keine leichte Aufgabe.

Ein anderes Beispiel: Darf ein Unternehmen / eine Institution private E-Mails archivieren, wenn die private E-Mail erlaubt ist? Die Antworten der IT-Verantwortlichen darauf lauten von: „Auf keinen Fall“ über „selbstverständlich“ bis „weiß nicht“. Der Jurist antwortet: „Es kommt darauf an“. Alle Antworten sind unbefriedigend und können doch alle richtig sein. Sicher ist, es herrscht Unsicherheit über viele Rechtsfragen. Dazu trägt auch die Werbung bei:

Mögliche Werbung eines Archivherstellers:

„E-Mails enthalten zum Teil Unterlagen, wie Angebote, Verträge oder Rechnungen. Daraus ergibt sich die Notwendigkeit, geschäftsrelevante E-Mails rechtssicher zu archivieren. Wir haben die Lösung, in dem wir die E-Mails bereits vor Zustellung archivieren. Eine mögliche Manipulation wird damit von Beginn an ausgeschlossen. Durch diesen Automatismus sorgt unsere Lösung für die notwendige Rechtssicherheit.“

Es wird eine rechtssichere und manipulationssichere Archivierung versprochen und weil keine Aktion durch die Endanwender notwendig ist, wird die Lösung rechtssicher.

Beides ist falsch, wie später beschrieben wird.

8. Die private Nutzung des betrieblichen/geschäftlichen E-Mail-Accounts

Kaum ein Thema hat die juristische Diskussion in Deutschland im Zusammenhang mit der E-Mail-Nutzung so sehr entfacht wie die Frage nach der privaten Nutzung². Das Betreiben einer sicheren E-Mail-Infrastruktur wird ohne Filtertechniken nicht praxisgerecht zu realisieren sein. Unabhängig davon, wo die eingesetzte Filtertechnologie jeweils ansetzt – am Client, Server oder vorgelagert auf Internetebene – können sich jedoch rechtliche Probleme ergeben, sobald private Internet- und E-Mail-Nutzung erlaubt oder geduldet wird. Das Ergebnis kann in Kurzform zusammengefasst werden: Deutschland hat gegenüber anderen Staaten eine besondere rechtliche Konstellation mit der Folge, dass dort, wo die private Nutzung des betrieblichen E-Mail-Accounts gestattet oder geduldet ist, die Einhaltung der gesetzlichen Vorgaben nur mit wesentlich mehr regulatorischem Aufwand zu erreichen ist. Der überwiegende Rat der mit dem Thema enger befassten Juristen geht heute daher zunehmend in die Richtung, die private Nutzung zu untersagen, denn damit können viele – wenn auch nicht alle – der rechtlichen Schwierigkeiten auf einfachere Weise geregelt werden. Zum Teil wird auch argumentiert, eine geordnete IT-Sicherheitsstruktur als Bestandteil der IT-Compliance sei nur erreichbar, wenn die Interessen des Einzelnen an einer privaten Nutzung hinter dem Interesse der Gemeinschaft aller Nutzerinnen und Nutzer an einer sicheren IT-Infrastruktur zurückstehen würden. Nur so könnten die zuständigen Abteilungen in der IT die angezeigten Scan- und Sicherungsmaßnahmen durchführen, ohne in Sorge sein zu müssen, dass sie die Rechte ihrer Kolleginnen und Kollegen verletzen würden. Jedem Unternehmen / jeder Institution kann nur geraten werden, seinen Weg zu finden. Nichts tun und das Thema ignorieren ist in jedem Fall ein Fehler. Die Autoren dieses Whitepapers haben sehr viele betriebliche Policies für die Nutzung der E-Mail-Strukturen gemeinsam mit den Unternehmen erarbeitet. Keine war gleich. Einen Standard, der für alle passt, haben wir nicht gefunden.

² Hierzu gibt es umfassende Literatur. PRW stellt auch gerne sein Whitepaper zu privaten E-Mail-Nutzung bereit.

Vielfach wird die betriebliche Diskussion noch dadurch angeheizt, dass unsere Sichtweise von ausländischen Kommunikationspartnern oder Unternehmen nicht geteilt wird, da dort die rechtliche Ausgangssituation wieder eine andere ist

Praxis-Tipp: Bei einer zulässigen privaten Nutzung des betrieblichen Accounts, sollte genau geprüft werden, ob die privaten E-Mails archiviert werden. Dazu besteht keine gesetzliche Pflicht. Es ist zu beachten, dass, wenn es private E-Mails sind, der/die E-Mail-Nutzer(in) auch einen jederzeitigen Anspruch auf Herausgabe seiner privaten E-Mails aus dem E-Mail-Archiv hat. Das ist bei Microsoft Exchange Server 2010 zum Beispiel möglich. Bei sogenannten unveränderbaren und revisionssicheren Archiven ist dies nicht nur nicht möglich, sondern sogar ein rechtliches Problem, denn dort kann der Herausgabeanspruch nicht erfüllt werden.

Sofern Unternehmen nicht rechtzeitig vor Prüfungsbeginn eine Abgrenzung ihrer steuerlich relevanten Datenbestände vornehmen, müssen sie den Datenzugriff auf die gesamten vorgehaltenen Informationen hinnehmen.

Dies gilt selbst dann, wenn aus den angeforderten Daten Rückschlüsse auf sensible oder schutzwürdige Informationen möglich sind.³

Hier bietet Exchange die Möglichkeit, Inhalte aus dezentralen PST-Dateien in Exchange zu importieren, sodass Outlook-Anwender persönliche Daten lokal verwalten können und zugleich notwendige Daten für die Archivierung in den Exchange-Datenbestand integrieren können.

9. Steuer- und Handelsrechtliche Belange

E-Mails stellen keine eigene Kategorie von aufzubewahrenden Unterlagen dar⁴. Demzufolge gibt es auch keine rechtlichen Vorgaben, welche Metainformationen zu speichern sind. Dies dürfte sich nach Praktikabilitäts Gesichtspunkten richten. In Betracht kommt somit die Speicherung solcher Informationen, die die Verschlagwortung beziehungsweise das Wiederauffinden der E-Mails ermöglichen beziehungsweise erleichtern. Sofern in den Metainformationen datenschutzrechtlich relevante Informationen enthalten sind, sollte ihre Speicherung dagegen nach den Grundsätzen der Datensparsamkeit möglichst vermieden beziehungsweise auf das zulässige Maß beschränkt werden.

10. Rechtsichere oder revisionssichere Archivierung? Die Irrtümer.

In der Fachöffentlichkeit ist neben dem Thema der Revisionssicherheit, das Thema der rechtlichen Absicherung oder gar der Rechtsicherheit im Bereich der Langzeitspeicherung mehr und mehr in die Diskussion mit einbezogen worden. Tatsache ist jedenfalls, dass eine rechtssichere Archivierung ein Ziel ist, dessen Realisierung sehr schwierig ist. Das ist aber nicht weiter schlimm. Die historische Archivierung von Papier in Ordnern war auch nicht rechtsicher, weil auch die beste Buchhaltungskraft von allen, irgendwann mal einen Beleg falsch abgelegt hat. Wir gehen also von dem Ziel aus, rechtskonform archivieren zu wollen. Dies ist durch die Parametrisierung eines Automatismus in der Regel nicht zu erreichen. Vielmehr bedarf es zunächst einer Archivierungsplanung und dann deren Umsetzung.

Der Begriff der Revisionssicherheit hat sich in der Diskussion weit verbreitet. Er gilt in Bezug auf die Archivierung gleichsam als Qualitätskriterium. Der Ausdruck „revisionssicher“ steht synonym für „nachprüfbar“, „unveränderbar“, „nachvollziehbar“ und hat angeblich vor allem für die steuerliche Betriebsprüfung große Bedeutung. Nach der Definition des Verbands Information und Organisation e. V. gilt ein digitales Archivierungssystem dann als revisionssicher, wenn mit ihm elektronische Daten gemäß den gesetzlichen Vorgaben und den GoBS sicher, unverändert, vollständig, ordnungsgemäß, verlustfrei reproduzierbar und datenbankgestützt recherchierbar verwaltet werden können. Auf welche Weise insbesondere die Unveränderbarkeit der Daten sichergestellt werden kann beziehungsweise muss, ist wiederum nicht gesetzlich vorgeschrieben, sondern richtet sich nach dem Stand der Technik.

³ FG Rheinland-Pfalz vom 20. Januar 2005 - 4 K 2167/04 -: Zugriffsschutz bei mangelhafter Abgrenzung

⁴ „E-Mails sind aufzubewahren, wenn sie dem Begriff des Handelsbriefs entsprechen.“

(Beck'scher Bilanzkommentar 1999, § 257, Rn 15; Adler/Düring/Schmaltz 1995, § 257, Rn 34)

Die ganze Diskussion hat das Handicap, dass sie Marketing getrieben ist. Wäre sie juristisch getrieben, wäre zunächst aufgezeigt worden, dass der Begriff der Revisionssicherheit im Gesetz nicht vorkommt. Wer beim Bundesamt für Steuern⁵ nachfragt, ob dieses Amt Wert legt auf eine revisionssichere Archivierung, wird ein Nein als Antwort erhalten. Die Steuerbehörden legen Wert auf die Einhaltung der steuerrechtlichen Vorschriften. Eine Aussage zu Revisionssicherheit findet sich darin nicht. Wenn in der Diskussion die Begriffe Revisionssicherheit oder Rechtssicherheit dennoch diskutiert werden, sollte dies lediglich dazu dienen, aufzuzeigen, dass es neben der Revisionssicherheit noch andere rechtliche Themenbereiche gibt, die zu beachten sind. So ist etwa das Thema Datenschutz erst in der jüngeren Zeit aufgrund aktueller Entwicklungen stärker in die rechtlichen Betrachtungen mit einbezogen worden.

Der Begriff der „Rechtssicherheit“ hat rechtsdogmatisch eine andere Bedeutung als das, was tatsächlich angeboten werden kann. Rechtssicherheit ist, nach der deutschen Auffassung, die Klarheit, Bestimmtheit und die Beständigkeit staatlicher Entscheidungen sowie die Klärung von umstrittenen Rechtsfragen oder -verhältnissen in angemessener Zeit. Rechtssicherheit ist Element des Rechtsstaatsprinzips. Verfassungsrang kommt der Rechtssicherheit in Deutschland mit Art. 20 GG⁶ zu.

Rechtssicherheit ist der Schutz des Vertrauens des einzelnen Staatsbürgers in eine durch Rechtsordnung und Rechtspflege garantierte Rechtmäßigkeit der äußeren Erscheinung der ihn umgebenden und ihm begegnenden rechtlich bedeutsamen Verhältnisse und Dinge. Der Grundsatz der Rechtssicherheit, formal besonders ausgeprägt in den verschiedenen Prozessordnungen, garantiert dem Einzelnen die gleiche rechtliche Wertung gleichartiger Einzelfälle, die Voraussehbarkeit von Rechtsfolgen sowie das Vertrauen darauf, dass eine von den Gerichten getroffene Entscheidung durchgesetzt wird. Die Rechtssicherheit ist ein wesentliches Kennzeichen eines Rechtsstaates⁷.

Daran wird deutlich, dass Rechtssicherheit hier begrifflich nicht passt.

Sicherlich wird man rechtlich rasch zu einem Konsens kommen, wenn die Empfehlung ausgegeben wird, dass eine rechtskonforme Langzeitspeicherung mit den relevanten Systemen möglich sein muss. Mit anderen Worten, ein Speichersystem muss sich so parametrisieren lassen, dass die notwendigen gesetzlichen und rechtlichen Bestimmungen erfüllt werden. Nur das kann das Ziel sein. Es darf nicht Ziel sein, Unmögliches zu verlangen. Denn es gilt immer noch der Grundsatz: Impossibilia nulla est obligatio (Es darf nichts Unmögliches verlangt werden).

Für die rechtskonforme Archivierung ist eine vorgeschaltete Analyse der im jeweiligen Einzelfall rechtlich relevanten Vorschriften unumgänglich. Die finanzrechtlich maßgeblichen Rechtsvorschriften ergeben sich aus dem Handelsgesetzbuch (§§ 239, 257 HGB) und der Abgabenordnung (§§ 146, 147 AO) und werden präzisiert durch die Grundsätze der ordnungsgemäßen Buchführung (GoB), die Grundsätze ordnungsgemäßer datenverarbeitungsgestützter Buchführungssysteme (GoBS) sowie die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) des Bundesfinanzministeriums. Bestimmte Techniken oder Verfahren für die Aufzeichnung und Speicherung von Daten schreibt das Gesetz ausdrücklich nicht vor.

Auch digitale Signierung und Verschlüsselung können zur Absicherung gegen nachträgliche Manipulationen geeignet sein. In steuerrechtlicher Hinsicht ist dann allerdings zu beachten, dass E-Mails, die in maschinell auswertbarer Form aufzubewahren sind, zusätzlich auch im Originalzustand einschließlich der verwendeten Schlüssel aufbewahrt werden müssen. Weiterhin fordern die GDPdU, dass der Eingang, die Archivierung und gegebenenfalls Konvertierung sowie die weitere Verarbeitung von aufbewahrungspflichtigen Unterlagen zu protokollieren sind. Der bloße Zugriff auf eine archivierte E-Mail ist damit nicht protokollierungspflichtig. Besteht allerdings das Risiko, dass eine archivierte E-Mail nachträglich verändert, gelöscht, verschoben etc. wird, dürfte bereits aus unternehmensinternen Gründen ein Interesse daran bestehen, eventuelle Zugriffe nachvollziehen und auch die betreffende Person ausfindig machen zu können.

Die zuvor beschriebenen gesetzlichen Anforderungen können mit Microsoft Exchange Server 2010 in vollem Umfang umgesetzt werden.

Zu den Details siehe FAQ Fragenkatalog

⁵ <http://www.bzst.bund.de> ⁶ GG bedeutet Grundgesetz

⁷ Quelle: Duden Recht A-Z. Fachlexikon für Studium, Ausbildung und Beruf. 1. Aufl. Mannheim: Bibliographisches Institut & F.A. Brockhaus 2007. Lizenzausgabe Bonn: Bundeszentrale für politische Bildung 2007.

11. Suchen und Finden

Wenn von der Steuerbehörde zu Recht geforderte Informationen nicht rechtzeitig vorgelegt werden können, droht ein sogenanntes Verzögerungsentgelt.

Das Verzögerungsentgelt dient dazu, den Steuerpflichtigen zur Erfüllung seiner Mitwirkungspflichten zeitnah anzuhalten, insbesondere Anordnungen der Finanzbehörde Folge zu leisten. Das Verzögerungsentgelt kann festgesetzt werden, wenn der Steuerpflichtige seiner Pflicht zur Mitteilung der unter § 146 Abs. 2a Satz 4 AO genannten Umstände nicht unverzüglich nachkommt oder den Datenzugriff nach § 147 Abs. 6 AO nicht, nicht zeitnah oder nicht in vollem Umfang einräumt, oder Auskünfte im Rahmen einer Außenprüfung nicht, erteilt.

Bei der Beschaffung und Suche von und nach Informationen kann die Funktionalität von Exchange 2010, über mehrere Mailboxen nach geschäftlich relevanten Daten zu suchen deshalb sehr hilfreich sein. Hier bietet der Service Pack 1 sinnvolle Verbesserungen, um solche Suchen schneller durchführen zu können. Auch das Anbringen von Kommentaren zu einzelnen Mails, die im Rahmen der Suche gefunden wurden, kann den weiteren Umgang mit den Suchergebnissen erleichtern.

12. Aufbewahrung und Archivierung

E-Mails eine Zeitlang aufzubewahren, empfiehlt sich schon aus unternehmensinternen Gründen, etwa um einen bestimmten Vorgang zu dokumentieren oder um auf den E-Mail-Verkehr Bezug nehmen zu können. Einige E-Mails sind jedoch aufgrund gesetzlicher Vorschriften langfristig aufzubewahren beziehungsweise zu archivieren. Die Aufbewahrungspflicht gilt für Kaufleute und ihnen gleichgestellte Handelsgesellschaften.

13. Aufbewahrungspflicht

Archiviert werden müssen alle E-Mails, die Handelsbriefe (§ 257 HGB) oder Geschäftsbriefe (§ 147 Abgabenordnung – AO) sind, sowie elektronische Rechnungen (§ 14b Umsatzsteuergesetz – UStG). Für Handels- und Geschäftsbriefe gilt eine Mindestaufbewahrungsfrist von sechs Jahren (§ 257, Absatz 4, HGB; § 147, Absatz 3 AO), gerechnet ab dem Schluss des Kalenderjahres, in dem der Brief empfangen oder abgesandt wurde (§ 257, Absatz 5 HGB; § 147, Absatz 4 AO), bzw. bis zum Ende einer laufenden Steuerprüfung. Rechnungen sind zehn Jahre lang aufzubewahren, gerechnet ab dem Schluss des Kalenderjahres, in dem die Rechnung ausgestellt wurde (§ 14b, Absatz 1 UStG).

14. Handelsbriefe

Aufzubewahren sind empfangene Handelsbriefe und Wiedergaben versendeter Handelsbriefe (§ 257, Absatz 1 HGB). Handelsbriefe definiert das Gesetz zwar als „Schriftstücke, die ein Handelsgeschäft betreffen“ (§ 257, Absatz 2 HGB), erfasst werden damit aber auch die modernen schriftlichen Kommunikationsformen wie Faxe und E-Mails (§ 238, Absatz 2 HGB).

Zu den Handelsgeschäften gehören wiederum alle Geschäfte, die dem Interesse des Unternehmens, der Erhaltung seiner Substanz und der Erzielung von Gewinn dienen sollen, wobei ein entfernter, lockerer Zusammenhang genügt. Ein weit verbreiteter Irrtum ist, zu glauben, es genüge, das finale Ergebnis (also nur die Rechnung) in der betriebswirtschaftlichen Software aufzuheben. Aufzubewahren sind Unterlagen wie Angebote, Auftragsbestätigungen, Lieferscheine, Mängelrügen, Reklamationsschreiben etc. Nicht dazu gehören Werbeschreiben, die erst der allgemeinen Bewerbung und Kontaktaufnahme mit potenziellen Kunden, nicht aber bereits der Anbahnung eines konkreten Geschäfts dienen.

15. Geschäftsbriefe

Das Steuerrecht verwendet den Begriff der Geschäftsbriefe (§ 147, Absatz 1 AO). Dieser umfasst zwar auch Handelsbriefe, gilt aber darüber hinaus für alle in irgendeiner Weise schriftlich fixierten Mitteilungen eines Unternehmers über geschäftliche Angelegenheiten an Dritte außerhalb des Unternehmens. Als Adressaten kommen etwa andere Konzernunternehmen, Geschäftspartner oder Behörden in Betracht. Eine bestehende Geschäftsbeziehung zu diesen ist nicht erforderlich.

Als Geschäftsbriefe aufzubewahren sind somit auch Preislisten, Auftragszettel, Bestellscheine, Lieferscheine, Frachtbriefe, Kostenvoranschläge, Bestätigungsschreiben, Verträge, Rücktrittserklärungen, Rechnungen, Quittungen und Mahnungen. Nicht dazu gehören nicht an einen bestimmten Empfänger gerichtete Mitteilungen wie allgemeine Rundschreiben an Kunden und Werbeschreiben. Auch an Mitarbeiter gerichtete Schriftstücke sind aufbewahrungspflichtig, soweit ein Mitarbeiter als Vertragspartner betroffen ist, wie dies etwa bei arbeitsvertraglichen Angelegenheiten der Fall ist.

16. Elektronische Rechnungen

Weiterhin hat ein Unternehmer erhaltene Rechnungen sowie Kopien von Rechnungen, die er selbst ausgestellt hat, aufzubewahren (§ 14b, Absatz 1 UStG). Zusätzliche Anforderungen gelten für elektronische Rechnungen. Diese berechtigen den Unternehmer nur dann zum Vorsteuerabzug, wenn sie mit einer qualifizierten, elektronischen Signatur mit Anbieterakkreditierung nach dem Signaturgesetz (§ 15, Absatz 1 SigG) versehen sind, da nur dann die Echtheit der Herkunft und die Unversehrtheit des Inhalts gewährleistet sind (§ 14, Absatz 3 UStG).

Dies hat auch Auswirkungen auf die Anforderungen an die Aufbewahrung, da der Originalzustand des übermittelten und gegebenenfalls noch verschlüsselten Dokuments jederzeit überprüfbar sein muss. Dementsprechend sind auch die Dokumentation der Signaturprüfung, der Signaturprüfchlüssel und das qualifizierte Zertifikat des Empfängers aufzubewahren. Bei Einsatz von Kryptografiertechniken sind zudem die verschlüsselte und entschlüsselte Rechnung sowie der Schlüssel zur Entschlüsselung der elektronischen Rechnung aufzubewahren.

17. Art der Aufbewahrung

Die Anforderungen an die Aufbewahrung stimmen im Handelsrecht und Steuerrecht weitgehend überein. Sofern eine E-Mail im Zweifel auch steuerrechtlich relevant sein kann, sollten jedoch die strengeren steuerrechtlichen Vorgaben eingehalten werden. Steuerrechtlich relevant sind nach Maßgabe der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) des Bundesfinanzministeriums⁸ in erster Linie die Daten der Finanzbuchhaltung, der Anlagenbuchhaltung und der Lohnbuchhaltung. Für die Dauer der Aufbewahrung muss sichergestellt sein, dass die Daten mit den Originalen bildlich oder inhaltlich übereinstimmen, wenn sie lesbar gemacht werden, dass sie während der gesamten Dauer der Aufbewahrungsfrist verfügbar sind und dass sie jederzeit lesbar gemacht werden können (§ 257, Absatz 3 HGB; § 147, Absatz 2 AO).

Das Steuerrecht fordert zusätzlich, dass steuerrechtlich relevante Daten maschinell ausgewertet werden können (§ 147, Absatz 2, Nummer 2 AO). Ausweislich der GDPdU gilt dies allerdings nicht für Unterlagen, die zwar datenverarbeitungsgestützt erstellt wurden, aber nicht zur Weiterverarbeitung in einem datenverarbeitungsgestützten Buchführungssystem geeignet sind. Als Beispiel werden Textdokumente angeführt. Die strengen Anforderungen an die maschinelle Auswertbarkeit dürften damit nur einen Bruchteil der E-Mail-Korrespondenz eines Unternehmens erfassen. Für die E-Mails, die diesen Vorschriften unterliegen, bedeutet dies, dass sie nicht ausschließlich in ausgedruckter Form oder beispielsweise als PDF-Dateien aufbewahrt werden dürfen. Eine Konvertierung in PDF- oder TIFF-Formate ist damit nicht unzulässig, eine Konvertierung in ein unternehmenseigenes Format (Inhouse-Format) ist nach den GDPdU sogar ausdrücklich erlaubt. Allerdings sind parallel dazu auch die Originale aufzubewahren.

⁸ Zu finden beispielsweise unter www.bundesfinanzministerium.de/cln_06/nn_3792/DE/Steuern/Veroeffentlichungen__zu__Steuerarten/Abgabenordnung/003.html

Für verschlüsselte E-Mails gilt dementsprechend, dass sie auch in entschlüsselter Form aufbewahrt werden müssen, da ihr Originalzustand erkennbar sein muss (§ 146 Absatz 4 AO). Zusätzlich sind die Schlüssel aufzubewahren.

Zu der Frage, ob E-Mail und Anhang voneinander getrennt aufbewahrt werden dürfen, ergibt sich nichts aus den gesetzlichen Regelungen des Handelsrechts oder Steuerrechts. Es wird lediglich darauf abgestellt, dass die aufzubewahrenden Unterlagen inhaltlich beziehungsweise von ihrer bildlichen Darstellung her nicht verändert werden dürfen und jederzeit lesbar gemacht werden können. Das Trennen von E-Mail und Anhang ist daher eher unter praktischen Gesichtspunkten zu beurteilen. Sofern Inhalte einer E-Mail auf den Anhang Bezug nehmen beziehungsweise umgekehrt, sollte die Zuordenbarkeit gewährleistet sein.

18. Ort der Aufbewahrung

Wo elektronische Daten genau aufzubewahren sind, ist im Gesetz nicht geregelt. Lediglich für steuerrechtlich relevante Daten war vorgeschrieben, dass sie im Geltungsbereich der Abgabenordnung, also auf dem Hoheitsgebiet der Bundesrepublik Deutschland aufzubewahren sind (§ 146, Absatz 2 AO – alte Fassung). Daraus kann geschlossen werden, dass die Aufbewahrung nicht unmittelbar beim Aufbewahrungspflichtigen, sondern auch bei einem Dritten erfolgen kann, etwa einem Hostprovider. Dies setzt allerdings voraus, dass dieser jedenfalls in technischer Hinsicht die Anforderungen an die ordnungsgemäße Aufbewahrung in gleicher Weise erfüllt wie der Aufbewahrungspflichtige, dass der Aufbewahrungspflichtige zu keiner Zeit den Zugriff und damit die Herrschaft über die Daten verliert.

Die Konsequenz in beiden Fällen war, dass alle (aufbewahrungspflichtigen) Unterlagen jederzeit im Inland aufzubewahren waren. Ausnahmen gab es lediglich für Betriebsstätten und Organgesellschaften im Ausland.

Die Rechtslage hat sich durch das Steuerbürokratieabbaugesetz mit Wirkung zum 01.01.2009 geändert. Nun gilt § 146 Abs. 2a AO: „Abweichend von Absatz 2 Satz 1 kann die zuständige Finanzbehörde auf schriftlichen Antrag des Steuerpflichtigen bewilligen, dass elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen in einem Mitgliedstaat der Europäischen Union geführt und aufbewahrt werden. Dasselbe gilt für einen anderen Staat, auf den das Abkommen über den Europäischen Wirtschaftsraum vom 3. Januar 1994 (ABl. EG Nr. L 1 S. 3) in der jeweils geltenden Fassung Anwendung findet.“

Die Zustimmung zur Durchführung eines Zugriffs auf elektronische Bücher und sonstige erforderliche elektronische Aufzeichnungen wird der zuständigen Stelle des Staates vorgelegt, in den die elektronischen Bücher und Aufzeichnungen verlagert werden sollen.

Aber Achtung, neu ist das Verzögerungsentgelt nach § 146 Abs. 2b AO: „Kommt der Steuerpflichtige der Aufforderung zur Rückverlagerung seiner elektronischen Buchführung oder seinen Pflichten nach Absatz 2a Satz 4, zur Einräumung des Datenzugriffs nach § 147 Abs. 6, zur Erteilung von Auskünften oder zur Vorlage angeforderter Unterlagen im Sinne des § 200 Abs. 1 im Rahmen einer Außenprüfung innerhalb einer ihm bestimmten, angemessenen Frist nach Bekanntgabe durch die zuständige Finanzbehörde nicht nach oder hat er seine elektronische Buchführung ohne Bewilligung der zuständigen Finanzbehörde ins Ausland verlagert, kann ein Verzögerungsentgelt von 2.500,00 Euro bis 250.000,00 Euro festgesetzt werden. Die Multimapboxsuche von Exchange 2010 kann hier ein gute Hilfestellung bei der schnellen Auffindung von Informationen sein.“

Werden personenbezogene Daten übertragen, ergeben sich zusätzliche datenschutzrechtliche Einschränkungen. So erlaubt das Bundesdatenschutzgesetz die Übermittlung personenbezogener Daten innerhalb des europäischen Wirtschaftsraums (§ 4b, Absatz 1 BDSG). Eine Übermittlung an andere ausländische Stellen ist beispielsweise dann zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist (§ 4b, Absatz 2 BDSG), der Betroffene eingewilligt hat (§ 4c, Absatz 1, Nummer 1 BDSG) oder die Aufsichtsbehörde die Übermittlung genehmigt (§ 4c, Absatz 2 BDSG). Insbesondere eine Übermittlung in die USA ist nur zulässig, wenn sich der Empfänger den Safe-Harbor-Regeln unterworfen hat (was zum Beispiel Microsoft getan hat) oder die Standardvertragsklauseln der EG-Kommission für die Übermittlung personenbezogener Daten in Drittländer verwendet werden.

Tipp: Vor der Parametrisierung sollte über die zuvor genannten Hintergründe Klarheit geschaffen werden. Also kurzum. Serverstandort Deutschland ist kein Problem. Serverstandort Europa ist nach Genehmigung möglich. Außerhalb von Europa erfordert besondere Voraussetzungen, die im Einzelfall zu prüfen sind.

19. Herausgabe aufbewahrungspflichtiger Daten

Im Rahmen der steuerlichen Außenprüfung hat die Finanzbehörde das Recht, Zugriff auf gespeicherte steuerrechtlich relevante Daten zu nehmen. Hierzu kann sie zum einen verlangen, dass der Steuerpflichtige die Daten nach ihren Vorgaben maschinell auswertet und ihr zur Verfügung stellt oder dass ihr gespeicherte Unterlagen und Aufzeichnungen auf einem maschinell verwertbaren Datenträger zur Auswertung überlassen werden (§ 147, Absatz 6 AO). Die neuen technischen Möglichkeiten von SP1 für den vereinfachten Export von primären Postfächern und Archivpostfächern sind hierbei sehr hilfreich.

Im Zusammenhang mit einem Gerichtsverfahren kann sich ebenfalls eine Pflicht zur Herausgabe von Urkunden und anderen Unterlagen (in Papierform) an das Gericht ergeben (§ 142, Absatz 1 Zivilprozessordnung – ZPO). Ein Pre-Trial-Discovery-Verfahren wie in den USA, nach dem der Beklagte im Vorfeld eines Gerichtsverfahrens sämtliche Unterlagen, die in irgendeiner Weise für den Anspruch des Klägers relevant sein können, an diesen herausgeben muss, ist dem deutschen Recht allerdings fremd und würde dem Verbot des Ausforschungsbeweises widersprechen. Allenfalls im Strafverfahren kann es eine vergleichbare Pflicht zur Herausgabe von Unterlagen an die Staatsanwaltschaft geben. Ist jedoch ein deutsches Unternehmen in den USA tätig und wird es dort in Rechtsstreitigkeiten verwickelt, unterliegt es auch den amerikanischen Prozessregeln und damit auch dem Pre-Trial-Discovery-Verfahren.

Nach der seit dem 1. Dezember 2006 in den USA existierenden Electronic Discovery sind in den USA in einen Rechtsstreit verwickelte Unternehmen zudem zur Vorlage elektronisch gespeicherter Informationen (Electronically Stored Information) verpflichtet. Hierzu gehören alle elektronischen Daten, die im Zusammenhang mit der Erstellung eines Dokuments gespeichert werden, einschließlich Entwurfsfassungen, unterschiedlicher Bearbeitungsversionen und so genannter Metadaten, also Zusatzinformationen wie zum Beispiel Angaben über den Bearbeiter des Dokuments, das Datum der Erstellung und der letzten Änderungen sowie die verschiedenen Speicherorte. Die Bundesrepublik Deutschland hat der Einführung einer Electronic Discovery auf der Grundlage des Haager Beweisübereinkommens widersprochen.

Hinweis: Auch die in Deutschland nicht vorgeschriebenen Regeln des US-Rechts können durch die sogenannte **legal hold** Funktion mit Microsoft Exchange 2010 abgebildet werden.

20. Datenschutz

Im Datenschutzrecht gilt der Grundsatz der Datenvermeidung und Datensparsamkeit⁹. Dies bedeutet, dass personenbezogene Daten nur unter strengen Voraussetzungen erhoben, verarbeitet und eben auch gespeichert werden dürfen. Daten, die für den Zweck, zu dem sie erhoben wurden, nicht mehr benötigt werden, sind zu löschen oder zu sperren¹⁰.

E-Mails enthalten bereits im so genannten Header typischerweise personenbezogene Daten (Name, E-Mail-Adresse), aber gegebenenfalls auch im Text der E-Mail selbst (Body) sowie in der Regel in der E-Mail-Signatur (Name, Position, Kontaktdaten des Versenders). Die gesetzlichen Bestimmungen zum Datenschutz greifen somit in jedem Fall, wenn die E-Mail komplett gespeichert wird. Wird nur der Text der E-Mail gespeichert, kommt es darauf an, ob dieser im Einzelfall personenbezogene Daten enthält. Fraglich ist aber, inwieweit die Speicherung einer E-Mail ohne Header und Signatur sinnvoll ist, um sie einem bestimmten Vorgang zuordnen zu können.

Treffen datenschutzrechtliche Lösungs- beziehungsweise Sperrpflichten und handels- und steuerrechtliche Aufbewahrungspflichten aufeinander, ist grundsätzlich anzunehmen, dass nur die personenbezogenen Daten aufbewahrt werden dürfen, die noch benötigt werden. Können diese nicht oder nur mit unverhältnismäßigem Aufwand vorab gelöscht werden, kann wohl vom Vorrang der handels- und steuerrechtlichen Aufbewahrungspflichten ausgegangen werden. Hierbei dürfte unter anderem zu berücksichtigen sein, dass die Nichteinhaltung der handels- und steuerrechtlichen Aufbewahrungspflichten im Gegensatz zu den datenschutzrechtlichen Lösungs- und Sperrpflichten insofern straf- und bußgeldbewehrt ist, als die nicht ordnungsgemäße Aufbewahrung steuerlich relevanter E-Mails dazu führen kann, dass diese nicht oder nicht rechtzeitig vorgelegt werden können. Dies kann wiederum als Steuerhinterziehung (§ 370 AO), Steuerverkürzung (§ 378 AO) oder Steuervergünstigung (§ 379 AO) verfolgt werden.

Aber Achtung, dort wo eine Datentrennung möglich ist, sollte diese unbedingt beachtet und umgesetzt werden¹¹.

Die Einführung technischer Einrichtungen wie eines Datenverarbeitungssystems, die das Verhalten oder die Leistung der Arbeitnehmer überwachen können, unterliegt zwingend der Mitbestimmung des Betriebsrats (§ 87, Absatz 1, Nummer 6 BetrVG)¹². Die weitere Einschaltung des Betriebsrats bezüglich der Archivierung von E-Mails ist jedenfalls vom Bundesdatenschutzgesetz nicht vorgesehen. Betriebsvereinbarungen können aber nach Auffassung des Bundesarbeitsgerichts, die in der Literatur kritisch gesehen wird, die Zulässigkeit der Verarbeitung personenbezogener Daten abweichend von den gesetzlichen Vorschriften regeln. Die Grenze wird dann aber dort zu ziehen sein, wo die Personaldatenverarbeitung nach dem Bundesdatenschutzgesetz unzulässig ist.¹³

⁹ § 3a BDSG ¹⁰ § 35 BDSG

¹¹ S.o. FG Rheinland-Pfalz vom 20. Januar 2005 - 4 K 2167/04 - Zugriffsschutz bei mangelhafter Abgrenzung

¹² Analoge Vorschriften existieren auch für den öffentlichen oder kirchlichen Rechtsraum

¹³ Vergleiche Gola/Schomerus BDSG § 4, Rd. 6.

21. FAQ Fragenkatalog – Alle Antworten in Kurzform

Auf alle nachfolgenden Fragen lautet die einfache und kurze Antwort: **Ja**

- Unterstützt Microsoft Exchange Server 2010 das Archivkonzept des Kunden?
- Ist eine kundenindividuell angepasste Archivierung möglich?
- Sind unterschiedliche Einstellungen zur Archivierung vorhanden?
- Werden alle gesetzlichen Zeiträume bei der Archivierung unterstützt?
- Sind automatische Löschroutinen für nicht mehr archivierungspflichtige Daten vorhanden?
- Ist eine spezielle Kennzeichnung steuer- und handelsrechtlicher Daten vorhanden?
- Werden E-Mails mit digitaler Signatur unterstützt und archiviert? (Hinweis: Berechtigung zum Vorsteuerabzug)
- Sind Vorkehrungen für den Einsatz von Kryptographietechniken hinsichtlich der Archivierung getroffen?
- Sind Maßnahmen zur Sicherstellung der maschinellen Auswertbarkeit steuerlich relevanter Daten vorhanden?
- Ist die Unveränderbarkeit der archivierten Daten sichergestellt?
- Können Maßnahmen zur geordneten Aufbewahrung getroffen werden?
- Können die Anforderungen der GoBS und GDPdU eingehalten werden?
- Ist die nachträgliche Manipulation der Archivdaten ausgeschlossen?
- Werden die Zugriffe protokolliert?
- Ist eine Veränderung des Protokolls ausgeschlossen?
- Ist die Einhaltung von speziellen Anforderungen (z. B. RöntVO, Heimgesetz, Sozialgesetzbuch) möglich?
- Bestehen ausreichende Analysemöglichkeiten für die digitalen Betriebsprüfung?
- Gibt es Möglichkeiten der Datentrennung und -sortierung für unterschiedliche Zwecke?
- Sind Maßnahmen zur Einhaltung des Datenschutzes getroffen?
- Werden die datenschutzrechtlichen Anforderungen hinsichtlich der Datenspeicherung von Microsoft Exchange Server 2010 unterstützt?
- Kann mit personenbezogenen Daten datenschutzkonform verfahren werden?
- Wird die endgültige und restlose Löschung personenbezogener Daten sichergestellt?

22. FAQ Fragenkatalog – lange Fassung

Frage: Unterstützt Microsoft Exchange Server 2010 SP1 das Archivkonzept des Kunden?

Antwort

Persönliches Archiv: Hierbei handelt es sich um ein spezielles Postfach, das mit dem primären Postfach des Anwenders verknüpft ist. Elemente können manuell oder automatisiert durch Beibehaltungsrichtlinien dorthin verschoben werden. Ein Zugriff ist über Outlook 2010 und Outlook Web App (OWA) möglich. Die Inhalte werden vollständig indiziert.

Das persönliche Archiv ist Bestandteil einer Exchange Server 2010 Datenbank, wobei das Archiv sowohl in der gleichen Datenbank wie das Postfach als auch in einer anderen Datenbank (auch auf einem anderen Exchange Server) liegen kann. Es handelt sich hierbei nicht um Outlook Datendateien (.PST) auf dem Rechner des Benutzers. Das persönliche Archiv ist somit automatisch in der Datensicherung der Exchange Server 2010 Datenbanken enthalten.

Bitte beachten: Für die Verwendung des persönlichen Archives ist der Erwerb der Exchange Server 2010 Enterprise Client Zugriffslizenz notwendig.

Beibehaltungsrichtlinien: Es sind zwei Richtlinien zu unterscheiden – Löschrichtlinien und Archivierungsrichtlinien. Mit Löschrichtlinien lassen sich Elemente (z. B. E-Mails oder Kalendereinträge) nach einer festgelegten Zeit automatisch aus dem Postfach entfernen. Archivierungsrichtlinien bewegen Objekte in das persönliche Archiv des Anwenders. Beide Richtlinien können kombiniert eingesetzt werden.

In der englischen Dokumentation werden Beibehaltungsrichtlinien als „Retention Policy“ bezeichnet.

Lösch- und Beibehaltungsrichtlinien beziehen sich immer auf das Alter einer Nachricht. Andere Kriterien können nicht angesetzt werden. Sind an dieser Stelle aber auch nicht erforderlich.

Bitte beachten: Eine Anpassung der Standardkonfiguration für Richtlinien erfordert die Exchange Server 2010 Enterprise Client Zugriffslizenz.

(Vorrats)datenspeicherung:¹⁴ Mit dieser Funktion werden alle gelöschten Objekte weiterhin so aufbewahrt, dass sie über die Multimapboxsuche gefunden werden können. In der englischen Dokumentation wird diese Funktion als „Legal Hold“ bezeichnet. Damit diese Sicherungskopien erstellt werden, muss ein Administrator zuerst den Legal Hold Modus für das entsprechende Postfach aktivieren. Dieser Modus greift immer sowohl für das primäre Postfach als auch für das persönliche Archiv.

Bitte beachten: Für die Verwendung der (Vorrats)datenspeicherung ist der Erwerb der Enterprise Client Zugriffslizenz erforderlich.

Wiederherstellung einzelner Nachrichten: Über Exchange Server 2010 können Administratoren festlegen, wie lange gelöschte und geänderte E-Mails im Wiederherstellungsordner verbleiben. Diese Funktion dient vor allem der Datensicherung und gab es in ähnlicher Version auch schon in älteren Versionen von Exchange Server.

Multimapboxsuche: Durch eine Web-basierte Suche kann ein spezieller Benutzer Mailboxinhalte von primären Postfächern und persönlichen Archiven durchsuchen, die sich über mehrere Anwender erstrecken. Aus Sicherheitsgründen werden alle Suchergebnisse an ein bestimmtes Postfach weitergeleitet. Als Filtermöglichkeiten stehen unter anderem zur Verfügung: Absender, Empfänger, Nachrichtenart, Sende-/Empfangsdatum und cc/bcc.

Standardmäßig kann ein Benutzer nur in seinem eigenen Postfach suchen. Für die eDiscovery Mailbox-Suche über mehrere Postfächer ist es erforderlich, dass ein Administrator der entsprechenden Person die notwendigen Rechte erteilt, indem er das Benutzerkonto dieser Person in eine besondere Gruppe aufnimmt. Standardmäßig ist kein Benutzer und auch kein Administrator berechtigt, eine Suche über mehrere Postfächer durchzuführen.

Bitte beachten: Für die Verwendung der Multimapboxsuche ist der Erwerb der Enterprise Client Zugriffslizenz erforderlich.

¹⁴ Klarstellung: Der Begriff ist nicht deckungsgleich mit dem Begriff im Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Rollenbasierte Zugriffskontrolle: Administratoren können Anwendern Sonderrechte zuweisen. Dadurch können beispielsweise Berichts-, Compliance- und Rechtsbeauftragte für ihre jeweiligen legitimen Aufgaben Multimailboxen durchsuchen und sonstige positionsabhängige Aufgaben durchführen.

Journaling: Die Journaling-Funktion aus den Vorgängerversionen von Exchange steht auch für Exchange Server 2010 weiter zur Verfügung. Über diese Funktion können Nachrichten selektiv oder auch komplett in eine Journal Mailbox kopiert werden, bevor sie in das Postfach des Benutzers zugestellt werden. Die Mails werden dabei in einem oder wenigen speziellen Postfächern abgelegt. Für diese Journaling-Postfächer kann zur weiteren Archivierung auch eine Archiv-Mailbox eingerichtet werden. In der Regel wird Journaling jedoch in Kombination mit einem Archiv eines Drittherstellers eingesetzt. Nutzer der Standard Client Zugriffslizenz können das „Standard Journaling“ pro Mailbox Datenbank ein- oder ausschalten. Das Journaling greift dann für alle Postfächer, die in Datenbanken liegen, für die das Journaling aktiviert wurde. Der Erwerb der Enterprise Client Zugriffslizenz gestattet mit dem „Premium Journaling“ eine höhere Granularität. Hier kann das Journaling gezielt für einzelne Postfächer oder Verteilerlisten aktiviert werden.

Transportregeln: Exchange Server 2010 bietet wie auch schon Exchange 2007 die Möglichkeit, über sogenannte Transportregeln Mails selektiv an ein gesondertes Postfach zu schicken. Für die Verarbeitung der Mails in diesem Postfach gelten die gleichen Anmerkungen wie zum Thema „Journaling“.

Bitte beachten: Die entsprechenden Transportregeln stehen auch zur Verfügung, wenn die Enterprise Zugriffslizenz nicht erworben wurde.

Managed Folder: Auch in Exchange Server 2010 gibt es die aus Exchange Server 2007 bekannten „Managed Folder“. Diese bieten aber keine Archivierung im eigentlichen Sinne.

Teilweise stehen die oben beschriebenen Funktionen nur innerhalb von Outlook 2010 und Outlook Web App zur Verfügung. In älteren Outlook Versionen sind diese Funktionen nicht sichtbar.

Bitte beachten: Nach den Lizenzbedingungen ist für die Verwendung der Funktionen in der Regel die Exchange Server 2010 Standard Client Zugriffslizenz nicht ausreichend. Es muss zusätzlich die Enterprise Zugriffslizenz erworben werden.

Frage: Ist eine kundenindividuell angepasste Archivierung möglich?

Antwort

Ja, die Richtlinien für das Archivieren und Löschen von Elementen ist bis auf Anwenderebene individuell einstellbar. Neue Richtlinien mit unterschiedlichsten Einstellungen können vom Administrator selbst erstellt werden.

Bitte beachten: Für diese Anpassungen durch den Administrator ist die Enterprise Zugriffslizenz erforderlich.

Frage: Sind unterschiedlichen Einstellungen zur Archivierung vorhanden?**Antwort**

Nachrichten können mit einem Ablaufdatum versehen werden.

Dies ist möglich auf Ebene:

- eines gesamten Postfaches,
- für einzelne Ordner,
- für einzelne Nachrichten.

Nach dem Erreichen des Ablaufdatums sind folgende Aktionen durchführbar:

- löschen, mit der Möglichkeit der Wiederherstellung aus dem Exchange Wiederherstellungsordner,
- endgültiges Löschen,
- verschieben in das persönliche Archiv.

Anmerkung: Wenn für ein Postfach/Archiv „Legal Hold“ aktiviert wurde, so kann jedes Element auch dann über die Multimapboxsuche gefunden werden, wenn die Aktion „endgültiges Löschen“ ausgewählt wurde. Wirklich endgültig gelöscht wird ein Objekt in solchen Fällen erst dann, wenn „Legal Hold“ wieder deaktiviert wird.

Frage: Werden alle gesetzlichen Zeiträume bei der Archivierung unterstützt?**Antwort**

Es werden 1 Tag bis unendliche Zeiträume unterstützt.

Frage: Sind automatische Löschroutinen für nicht mehr archivierungspflichtige Daten vorhanden?**Antwort**

Ja, Elemente können automatisch über Löschrichtlinien gelöscht werden. Diese Richtlinien können auf:

- gesamte Postfächer,
 - einzelne Ordner,
 - einzelne Nachrichten
- angewendet werden.

Frage: Ist eine spezielle Kennzeichnung steuer- und handelsrechtlicher Daten möglich?**Antwort**

Eine besondere Kennzeichnung dieser Daten ist über Anpassungen möglich. Es können für das Unternehmen eigene Flags/Tags erstellt werden, die die gewünschte Kennzeichnung und Aktionen enthalten. Die Zuweisung dieser Flags für die einzelnen E-Mails kann durch den Benutzer selbstständig erfolgen. Zuvor sollten entsprechende organisatorische Richtlinien verabschiedet werden.

Alternativ kann eine Kennzeichnung auch über Outlook Kategorien erfolgen. Da diese jedoch nicht zentral verwaltet werden können, ist der Einsatz von Flags/Tags in diesem Fall sinnvoller.

**Frage: Werden E-Mails mit digitaler Signatur unterstützt und archiviert?
(Hinweis: Berechtigung zum Vorsteuerabzug)**

Antwort

Da alle Archiv-Aktionen innerhalb des Exchange-Systems passieren, werden E-Mails mit digitaler Signatur genauso behandelt wie E-Mails ohne digitale Signatur. Der volle Funktionsumfang wird mit Outlook 2010 und Outlook Web App unterstützt, da nur diese Clients Zugang auf das persönliche Archiv haben. Der Umgang mit digital signierten E-Mails ist somit im Archiv nicht anders als beim Einsatz von Exchange 2010 ohne Archiv.

Frage: Sind Vorkehrungen für den Einsatz von Kryptographietechniken hinsichtlich der Archivierung getroffen?

Antwort

Hier verhält es sich ähnlich, wie bei E-Mails mit digitaler Signatur. Alle Archivierungsvorgänge spielen sich innerhalb des Exchange-Systems ab, die Funktionalität von verschlüsselten E-Mails ändert sich daher nicht bei der Archivierung.

Zusätzlich besteht die Möglichkeit E-Mails, die mit Active Directory Rights Management geschützt wurden, auf dem Exchange Server automatisiert zu entschlüsseln und eine entschlüsselte Kopie der Nachricht im Nachrichten-Journal abzuspeichern.

Frage: Sind Maßnahmen zur Sicherstellung der maschinellen Auswertbarkeit steuerlich relevanter Daten vorhanden?

Antwort

Die Trennung und Kennzeichnung von Informationen, die steuerlich relevant sind, ist eine organisatorische Aufgabe des Unternehmers / der Institution.

Die Auswertbarkeit der Daten wird durch folgende Technologien sichergestellt:

Der Endanwender markiert die steuerlich relevanten E-Mails entsprechend der organisatorischen Vorgaben. Dies kann z. B. die Ablage dieser E-Mails in einem bestimmten Ordner, oder das Einfügen eines Schlüsselworts in den Nachrichtentext sein. Die automatisierte Auswertung nutzt die entsprechende Markierung dann aus.

- Verschlagwortung und Indizierung des gesamten Exchange-Systems,
- Nutzung der Funktion der Multimapboxsuche,
- Exportfunktion in der Multimapboxsuche in der PST-Datei, um einen einfachen Datenaustausch an Dritte zu weiteren Untersuchungen zu gewährleisten sowie die generelle Möglichkeit, ein Postfach oder ein Archiv in eine PST zu exportieren,
- Hochverfügbarkeitsmechanismen, um die Verfügbarkeit der Daten sicher zu stellen,
- Automatische Reparaturfunktionen für Festplatten, um häufige Fehler wie „Bad Blocks“ selbstständig ohne administrativen Eingriff zu beheben.

Frage: Ist die Unveränderbarkeit der archivierten Daten sichergestellt?

Antwort

Ein Postfach kann in den Zustand „Legal Hold“ versetzt werden. Hierdurch werden die folgenden Maßnahmen erreicht:

- Objekte innerhalb des Postfaches bleiben unverändert erhalten,
- Objekte, die durch den Anwender gelöscht hätten werden können bleiben erhalten,
- Objekte, die durch Exchange Lösungs-Richtlinien gelöscht worden wären, bleiben erhalten.

Der Zustand „Legal Hold“ ist für den Anwender transparent, die Exchange Richtlinien müssen daher nicht ausgesetzt werden.

Objekte unter „Legal Hold“ können mit E-Discovery Methoden gefunden werden (Multimailboxsuche).

„Legal Hold“ wird über den Wiederherstellungsordner in Exchange umgesetzt, dessen Verhalten in Exchange 2010 gegenüber Vorgängerversionen angepasst wurde. Objekte unter „Legal Hold“ werden in diesem Speicher von Exchange nicht gelöscht und sind für die Multimailboxsuche indiziert.

Löscht der Anwender Daten in einem Postfach unter „Legal Hold“, kommt es zu einer Datenspeicherung im Wiederherstellungsordner. Dieses gilt auch beim „endgültigen Löschen“.

Ändert der Anwender Objekte in einem Postfach unter „Legal Hold“, wird die Version des Originals im Wiederherstellungsordner gespeichert. Falls mehrere Änderungen erfolgen, werden alle Versionen der Mail gespeichert. Damit wird den gesetzlichen Regelungen Rechnung getragen.

Bitte beachten: Ein böswilliger Administrator kann sämtliche Daten vernichten. Dies bedarf aber enormer krimineller Energie, denn sämtliche Instanzen einer Exchange Datenbank und deren Datensicherungen müssten vernichtet werden. Ein solcher Fall ist dem gleich zusetzen, dass ein Mensch ein klassisches Archiv in Brand setzt und es zerstört.

Frage: Können die Anforderungen der GoBS und GDPdU eingehalten werden?**Antwort**

Ja, wobei eine Verfahrensdokumentation und das IKS (Internes Kontroll-System) vom Unternehmen / der Institution erstellt werden muss. Dies ist nicht Aufgabe des Herstellers oder des IT-Dienstleisters.

Während des Übertragungs- / Scanvorgangs darf keine Bearbeitung möglich sein

Die Übertragung von Nachrichten innerhalb einer Exchange-Organisation erfolgt standardmäßig verschlüsselt und somit von außen nicht manipulierbar. Das gilt sowohl für die Übertragung zwischen Client und Server als auch zwischen Servern. Das Kopieren einer Nachricht in eine Archivmailbox funktioniert innerhalb des Systems und nicht über externe Schnittstellen. Der Austausch von Nachrichten mit externen Kommunikationspartnern unterliegt selbstverständlich den üblichen Beschränkungen des Internets und erfolgt in den meisten Fällen unverschlüsselt. Eine solche Übertragung ist in diesem Kontext aber nicht gemeint. Ein Scanvorgang erfolgt nicht.

Indexierung / Risiko der Unauffindbarkeit ist zu reduzieren

Alle Daten in Exchange Server 2010 werden automatisch indiziert.

Durch die Funktion der Multimapboxsuche können berechtigte Administratoren ein Suchen im gesamten System anstoßen.

Die Verwendung der benutzerindividuellen Suche ist mit Outlook Web App und Outlook 2003/2007/2010 effektiv möglich.

Das Risiko der Unauffindbarkeit muss durch den Einsatz der Hochverfügbarkeitsfunktionen von Exchange und gegebenenfalls einer Datensicherung mit der entsprechenden Richtlinie reduziert werden.

Ein Datensicherheitskonzept muss von Unternehmen / der Institution erstellt werden.

Schutz vor Verlust / Veränderung

Exchange Server 2010 bringt Sicherungsmechanismen für das Backup der Exchange-Daten mit.

Die Erzeugung mehrerer Datenbank Kopien ist über Database Availability Groups möglich. Bei Ausfall einer Datenbank auf einem Server, wird die Datenbank eines anderen, bereitgestellten Servers automatisch zur Datenverwendung herangezogen, die Daten sind redundant vorhanden und gehen nicht verloren.

Ein Postfach kann in den Zustand „Legal Hold“ versetzt werden. Hierdurch wird die Originalversion einer Nachricht in der Exchange Datenbank auch bei Veränderung oder Löschung gespeichert.

Die Lesbarkeit der Datenträger ist regelmäßig zu prüfen

Exchange überwacht die Integrität der Datenbanken an verschiedenen Stellen selbstständig. Entsprechende Fehlermeldungen werden im Event Log protokolliert.

Bitte beachten: Zusätzlich ist der Einsatz einer Monitoring Lösung wie Microsoft System Center Operations Manager ratsam.

Frage: Ist die nachträgliche Manipulation der Archivdaten ausgeschlossen?**Antwort**

Ja, zum Beispiel durch die Journalingarchivierung und durch Zugangskontrollen zum Journal.

Die Funktion „Legal Hold“ bewirkt die unveränderliche Datenspeicherung aller Elemente innerhalb eines Postfaches. Alle Änderungen und Löschungen sind hiermit eingeschlossen. Durch die Multimapboxsuche können diese Informationen eingesehen werden. Das entsprechende Postfach muss zuerst von einem berechtigten Administrator in den Legal Hold Modus versetzt werden.

Bitte beachten: Archivdaten von Postfächern, die nicht im Legal Hold Modus sind, können vom Benutzer manipuliert werden. Das war in der klassischen Papierwelt auch so. Hier ist Selbstverantwortung gefragt. Das Archivpostfach liegt in einer normalen Exchange Datenbank. Exchange Datenbanken können nur auf einem Schreib/Lese Medium angelegt werden. Die Verwendung von einem Medium, das nur einmal beschrieben und anschließend nur gelesen aber nicht mehr verändert werden kann, ist bei Exchange Server nicht möglich. Dies ist gesetzlich auch nicht gefordert.

Frage: Werden die Zugriffe protokolliert?**Antwort**

Exchange besitzt die Möglichkeit mit Hilfe des Features der Administrator-Überwachungsrichtlinien, alle Befehle innerhalb der Exchange-Verwaltung zu protokollieren.

Somit können alle administrativen Vorgänge in

die Exchange Verwaltungskonsole

die Exchange Verwaltungsshell

das Exchange Control Panel

aufgezeichnet werden.

Service Pack 1 bietet zusätzlich umfassende Protokollmöglichkeiten für den Zugriff auf Postfächer bis hin zur Überwachung des Zugriffs auf einzelne Objekte in einem Postfach.

Frage: Ist eine Veränderung des Protokolls ausgeschlossen?**Antwort**

Überwachungsprotokolle werden als E-Mail-Nachrichten in dem zu überwachenden Postfach gespeichert. So bleibt das Protokoll auch beim Verschieben des Postfachs enthalten. Ist „Legal Hold“ für ein solches Postfach aktiviert, wird das Protokoll unabhängig von der dafür eingestellten Aufbewahrungszeit solange aufbewahrt, wie „Legal Hold“ aktiv ist.

Frage: Ist die Einhaltung von speziellen Anforderungen (z. B. RöntVO, Heimgesetz, Sozialgesetzbuch) möglich?**Antwort**

Alle Gesetze und Vorgaben, bei denen es um Aufbewahrungsfristen geht, können durch die Exchange Archivierungsrichtlinien und das Feature „Legal Hold“ implementiert werden.

Erforderliche Daten können im persönlichen Archiv für eine festgelegte Zeit abgelegt werden. Auch eine Speicherung der Daten mittels Exchange Journaling ist möglich.

Frage: Bestehen ausreichende Analysemöglichkeiten für die digitale Betriebsprüfung?**Antwort**

Eine Analyse ist durch die Möglichkeit der Indizierung und Verschlagwortung gegeben. Alle Daten können durch eine Suche, entweder innerhalb von Postfächern oder mailboxübergreifend über die Multimapboxsuche eingesehen und analysiert werden.

Ein Export in das PST Dateiformat in der Multimapboxsuche oder mittels Powershell ermöglicht den einfachen Datenaustausch mit Dritten, um zum Beispiel die weitere Analyse durch einen Wirtschafts- oder Steuerprüfer zu ermöglichen.

Frage: Gibt es Möglichkeiten der Datentrennung und -sortierung für unterschiedliche Zwecke?**Antwort**

Für die Datentrennung und -sortierung ist das Unternehmen die Institution selbst verantwortlich.

Microsoft Exchange Server 2010 bietet die Funktionalität der Transportregeln, die dabei helfen sollen, den Fluss von E-Mail-Nachrichten durch die Organisation zu steuern. Eine Transportregel enthält Bedingungen, bei deren Erfüllung diese Regel ausgelöst wird, sowie einen geordneten Satz von Aktionen, die bei Auslösung der Regel auszuführen sind. Zusätzlich kann jede Transportregel Ausnahmen enthalten, die angeben, was aus der Bedingung auszuschließen ist. Bei Verwendung von Transportregeln können Sie z. B. festlegen, welche Daten von der Organisation mit einem bestimmten Begriff im Betreff einer Nachricht in welches Postfach als Kopie weitergeleitet werden soll, oder welche Personen und Gruppen nicht miteinander kommunizieren sollen, wie Nachrichten basierend auf ihrer Klassifizierung durch den Absender verarbeitet werden sollen und vieles mehr.

Mit der Funktion der Managed Folder lassen sich Nachrichten nach einer gewissen Zeit automatisch in vorgegebene Ordner verschieben.

Soweit dies gewollt ist, kann auch der Endanwender E-Mails entsprechend dem vorgesehenen Zweck der Nachricht in unterschiedlichen Ordnern in seinem Postfach ablegen.

Frage: Sind Maßnahmen zur Einhaltung des Datenschutzes getroffen?**Antwort**

Das persönliche Archiv ist nur vom Anwender des primären Postfaches einsehbar. Weitere Berechtigungen müssen explizit vom Administrator vergeben werden.

Über das Rollenmodell der Exchange-Administration kann klar geregelt werden, welche Personen im Exchange-System Zugriff haben. Standardmäßig sind die Elemente der Anwender innerhalb der Postfächer von Dritten nicht einsehbar, auch nicht über die Discovery-Funktion, der Multimapboxsuche. Für derartige Funktionen sind immer Mitgliedschaften in Gruppen notwendig, die nur von berechtigten Exchange-Administratoren vergeben werden können.

Die Kommunikation zwischen Outlook Clients und Exchange 2010 Systemen erfolgt standardmäßig verschlüsselt. Achtung: Dieses gilt nicht für neu installierte Exchange Server (SP1) im Zusammenhang mit Outlook 2003. Hier muss der Zwang zur Verschlüsselung auf dem Server explizit wieder eingeschaltet werden.

Outlook Web App ist nur über eine verschlüsselte Verbindung erreichbar.

Die Multimapboxsuche kann so konfiguriert werden, dass alle Suchanfragen und Ergebnisse umfassend protokolliert werden.

Über Active Directory Rights Management und sogenannte Outlook Protection Rules kann erreicht werden, dass die E-Mails schon auf dem Client verschlüsselt werden und der E-Mail-Inhalt geschützt vom Client zum Server transportiert wird.

Frage: Werden die datenschutzrechtlichen Anforderungen hinsichtlich der Speicherung von Daten von Microsoft Exchange Server 2010 unterstützt?

Antwort

Zahlreiche technische Möglichkeiten der Datenhaltung sind in diesem Dokument beschrieben. Zusätzlich müssen organisatorische Vorschriften, Prozesse und Kontrollmechanismen durch Policies etabliert, überwacht und umgesetzt werden, um ein schlüssiges Gesamtkonzept zu erhalten. Diese liegen zunächst außerhalb der Exchange-Umgebung.

Schutz vor Veränderung und Verfälschung wird dadurch erreicht, dass ein Postfach in den Zustand „Legal Hold“ versetzt werden kann. Hierdurch wird die Originalversion einer Nachricht in der Exchange Datenbank auch bei Veränderung oder Löschung gespeichert.

Sicherung vor Verlust wird durch mehrere Möglichkeiten erreicht:

Der Exchange Server 2010 bringt Sicherungsmechanismen für das Backup der Exchange-Daten mit. Die Erzeugung mehrerer Datenbankkopien ist über Database Availability Groups möglich. Bei Ausfall einer Datenbank auf einem gewissen Server, wird die Datenbank eines anderen, bereitgestellten Servers automatisch zur Datenverwendung herangezogen, die Daten sind redundant vorhanden und gehen nicht verloren.

Für die Sicherung der Kopien z. B. auf Bändern müssen analog zu anderen Sicherungen entsprechende Prozesse und Verfahren im Unternehmen etabliert werden.

Nutzung nur durch Berechtigte

Durch Rechtevergabe im Active Directory oder direkt in der Exchange Datenbank lassen sich alle Zugänge zu den Archiv-Daten exakt steuern.

Mithilfe der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) können sowohl auf allgemeiner als auch auf detaillierter Ebene Aktionen von Administratoren und Endbenutzern gesteuert werden. RBAC ermöglicht außerdem eine genauere Anpassung der den Benutzern und Administratoren zugewiesenen Rollen an ihre tatsächlichen Positionen, die innerhalb der Organisation eingenommen werden. In Exchange Server 2010 steuert RBAC sowohl die durchführbaren administrativen Aufgaben als auch den Grad, zu dem Benutzer ihr eigenes Postfach und ihre Verteilergruppen selbst verwalten können.

Einhaltung der Aufbewahrungsfristen

Die Einhaltung von Aufbewahrungsrichtlinien wird durch die Aufbewahrungsfrist im Exchange Wiederherstellungsordner und die Funktion Legal Hold sichergestellt. Nur Administratoren mit den entsprechenden Rechten im Exchange Server 2010 können diese Einstellungen ändern.

Dokumentation des Verfahrens

Die Dokumentation des Archivverfahrens muss jede(s) Unternehmer / Institution selbst erstellen. Die grundlegenden Funktionen sind in der Basisdokumentation von Exchange Server 2010 verankert. Eine Verfahrensdokumentation sollte zusammen mit dem implementierenden Dienstleister erstellt werden.

Frage: Kann mit personenbezogenen Daten datenschutzkonform verfahren werden?**Antwort**

E-Mails als solche sind personenbezogenen Daten. Diese werden durch die Exchange Löschungs- oder Archivierungsrichtlinien verarbeitet. Der Anwender muss die Daten entsprechend den geltenden Vorgaben behandeln und kennzeichnen.

Frage: Wird die endgültige und restlose Löschung personenbezogener Daten sichergestellt?**Antwort**

Die Löschung bestimmter personenbezogener Daten kann im Rahmen von Postfächern vorgenommen werden.

Gelöschte Daten und Postfächer werden in Exchange Server 2010 immer im sogenannten Wiederherstellungsordner vorgehalten, bevor es zu einer endgültigen Löschung kommt. Die Aufbewahrungsfrist für Objekte im Wiederherstellungsordner kann frei konfiguriert werden. Standard sind 14 Tage, eine angepasste Einstellung muss hier für jeden Kunden gefunden werden.

Zur Erhöhung der Sicherheit kann Exchange so konfiguriert werden, dass beim endgültigen Löschen einer Mail nicht nur eine Tabelle in der Datenbank verändert wird, sondern dass der Bereich der Datenbank, in dem die Mail gespeichert war, unmittelbar überschrieben wird. Somit ist eine Wiederherstellung dieser Daten auch unmittelbar nach der Löschung mit forensischen Tools nicht mehr möglich. Das bieten viele Archivierungsmöglichkeiten nicht an. Wichtig ist zu wissen, dass das Einschalten dieser Funktion die Performance etwas belastet. Der Kunde kann entscheiden, was für ihn Vorrang hat.

Factsheet/Kontaktdaten

Wenn Sie Fragen, Anregungen oder Kritik zu dieser Broschüre haben, können Sie uns gern kontaktieren.
Wir freuen uns darauf.

Kontaktdaten:

PRW Rechtsanwälte

Steinsdorfstraße 14

80538 München

Telefon: +49 89 210977-0

Telefax: +49 89 210977-77

E-Mail: office@prw.de

Für die technische Unterstützung:

infoWAN Datenkommunikation GmbH

Neuhofweg 5

85716 Unterschleißheim

Telefon: +49 89 324756-0

Telefax: +49 89 324756-99

E-Mail: info@infoWAN.de