DATATREE
YOUR COMPLIANCE PROVIDER

Minenfeld Archivierung

Ansätze. Rechtsfragen. Verantwortlichkeiten.

Minenfeld Archivierung - Theorie und Praxis
Schloß Eicherhof, Leichlingen
Donnerstag, 19. April 2012

Hohe Speicherkosten, zeitraubende Backups und nicht genau zuordenbare elektronische Beweisführung, wenn beispielsweise Auskünfte über die gespeicherten Daten von Betroffenen nach § 34 Bundesdatenschutzgesetz (BDSG) verlangt werden, stellen Unternehmen vor vielfältige Probleme.

Konflikte mit bestehenden Gesetzen wie dem Datenschutz sind vorprogrammiert. Nicht nur teure Abmahnungen von Konkurrenten, Verbraucherschutzorganisationen und anderen Berechtigten drohen. Auch die Aufsichtsbehörden der Bundesländer drängen auf Nachweise einer rechtskonformen Datenspeicherung, da sie Beschwerden nachgehen müssen.

Folge ist ein Minenfeld an Unwägbarkeiten, die Unternehmen teuer zu stehen kommen können - sowohl im betriebswirtschaftlichen als auch rechtlichen Sinne!

Wer als Unternehmer bei Beschwerden, Datenmissbrauch oder -diebstahl gegenüber Aufsichtsbehörden und vor Gericht auf der sicheren Seite sein will, muss nachweisen, dass er alle Gesetze berücksichtigt hat.

Das Problem: Ein eigenes Gesetz, das zum Beispiel alle Verpflichtungen zur Archivierung digitaler Speicherung, so auch von E-Mails, zusammenfasst, gibt es nicht. Stattdessen finden sich vereinzelte Regelungen an unterschiedlichsten Stellen wie beispielsweise:

- der Abgabenordnung (AO)
- dem Handelsgesetzbuch (HGB)
- dem Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- dem Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr (KonTraG)
- das Telemediengesetz (TMG)
- dem Bundesdatenschutzgesetz (BDSG)
- dem Telekommunikationsgesetz (TKG)
- dem Strafgesetzbuch (StGB) .

Das BDSG verbietet **grundsätzlich** die **Erhebung, Verarbeitung und Nutzung** personenbezogener Daten, erlaubt diese aber unter bestimmten Voraussetzungen **(Verbot mit Erlaubnisvorbehalt / lex generalis).**

Datenerhebung ist somit zulässig, wenn sie ...

durch das BDSG selbst ...
Beispiel: öffentlich zugängliche Daten

oder durch eine andere Rechtsvorschrift ...
Beispiel: Steuern, Abgaben

gesetzliche Grundlage

oder durch die Einwilligung des Betroffenen ...
Beispiel: Einverständniserklärung zur Datennutzung

... erlaubt wird.

DATATREE
YOUR COMPLIANCE PROVIDER

E-Mail- und Internetzugang sind Betriebsmittel zur Erbringung der Arbeitsleistung. Aber mit Bereitstellung privater Nutzung wird der Arbeitgeber zum geschäftsmäßigen TK-Anbieter (E-Mail - § 3 Nr. 10 TKG); Telemedienanbieter (Internet - § 2 (1) TMG)

► Das Fernmeldegeheimnis „infiziert“ damit das Mailpostfach und die Internetlogfiles!

Bei Duldung oder **Erlaubnis** der privaten Nutzung **ohne** spezifische **rechtliche Regelung** ergeben sich technische, rechtliche und betriebliche Probleme:

Aufgrund § 88 TKG und § 206 StGB generell:

- Spamfilterung unzulässig

- Logfilespeicherung und Auswertung unzulässig
  beides sind unabdingbare technische Sicherheitsmaßnahmen zum Schutz der IT-Systeme eines Unternehmens

- Kontrolle der Nutzungsvorgaben unzulässig!
  hierzu ist ein Arbeitgeber aber aufgrund gesetzlicher Vorgaben verpflichtet

Bei Abwesenheit des Arbeitnehmer:

- Einsichtnahme in Maileingang durch Arbeitgeber stets unzulässig!
- Wichtige Geschäftsmails nicht einsehbar

Welche Aufbewahrungsfristen im jeweiligen Einzelfall bei verschiedenen Datenkategorien zu berücksichtigen sind, bedarf allerdings einer Recherche. So sind die wichtigsten Aufbewahrungsvorschriften für den nicht-öffentlichen Bereich beispielsweise in folgenden Gesetzen und Vorschriften festgelegt:

- Handels- und Steuerrecht § 257 HGB Handelsgesetzbuch
- Arbeitszeitordnung AZO (Arbeitszeitnachweis)
- Bundesrechtsanwaltsordnung BRAO (Handakten von Rechtsanwälten)
- Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (Jahresrechnung)
- Aufbewahrungsvorschriften in der Datenverarbeitung nach BDSG und HGB (z.B. Systemnachrichten, Protokolle über Datenträgertransporte, Standardsoftware, Anwenderprogramme)

Nach Ablauf der jeweiligen Aufbewahrungsfristen greift die Verpflichtung zur Löschung oder Sperrung der personenbezogenen Daten nach dem Bundesdatenschutzgesetz (§ 35 Abs. 2 Nr. 3 und 4 BDSG). Personenbezogene Daten müssen gelöscht werden, wenn sie für den Zweck ihrer Erhebung nicht mehr erforderlich sind und gesetzliche Aufbewahrungspflichten einer Löschung nicht widersprechen.

Bestehen Aufbewahrungspflichten, so tritt eine Sperrung an die Stelle der Löschung der Daten. Zudem werden die Daten auch dann gesperrt und nicht gelöscht, wenn die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigen würde oder wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohen Aufwand möglich wäre.

Das Problem: Oft geben Unternehmen keine genauen Löschfristen an. Viele Betriebe beschränken sich auf die Aussage, eine Löschung der Daten vornehmen zu wollen, sobald die Daten für die Erfüllung des Zwecks ihrer Erhebung nicht mehr erforderlich sind.

Ohne konkrete Termine für die Datenlöschung aber ist Überwachung unmöglich. Es muss also zunächst eine Festlegung der Löschfristen her. Ein Unternehmen braucht also nicht nur ein Archivierungskonzept, sondern auch ein Löschkonzept.

Wichtig: Löschfristen sind vom Unternehmen jeweils selbst zu definieren. Denn während sich die Aufbewahrungsfristen recherchieren lassen, gibt es abgesehen von einigen branchenspezifischen Datenschutzregelungen keine konkreten Löschfristen. So muss die verantwortliche Stelle im Unternehmen ,also die Geschäftsführung - bestimmte Fristen für die Löschung festlegen. In der Praxis fällt dies der Unternehmensleitung oft nicht leicht. Gründe dafür sind meist:

- die Furcht, Daten löschen zu lassen, die später noch gebraucht werden
- die fehlende Motivation für eine Datenlöschung, abgesehen von dem frei werdenden Speicherplatz
- die Schwierigkeit, die Löschfristen sinnvoll zu bemessen

Wie wichtig ein durchstrukturiertes Archivsystem zum Wissens- und Knowhow-Erhalt ist, zeigt sich beispielsweise,

wenn ein wichtiger Mitarbeiter die Firma verlässt, er zwar Aktenordner oder Festplatten voll mit Dateien hinterlässt, der Inhalt aber schlecht strukturiert ist und nur unter hohem Zeitaufwand wieder nutzbar gemacht werden kann.

Zudem muss gesichert sein, dass vorhandenes Wissen bei einer Mitarbeiterfluktuation nicht kopiert und mitgenommen werden kann.

Sanktionen bei nicht ordnungsgemäßer Archivierung

Neben diesen unternehmenspolitisch weichen Faktoren drohen teilweise massive Sanktionen, wenn ein Unternehmen nicht ordnungsgemäß archiviert.

Stichwort: Organisationsverschulden

- Werden steuerrelevante E-Mails nicht archiviert, kann die Steuerbehörde z.B. den Gewinn und damit die Steuerschuld schätzen (vgl. § 162 Abs. 2 AO)

- Die Unternehmensleitung muss gemäß § 13 Abs. 1 StGB sicherstellen, dass aus dem Unternehmen heraus keine Straftaten begangen werden. Strafrechtliche Maßnahmen drohen beispielsweise, wenn das Unternehmen durch eine unzureichende oder gar manipulative E-Mail-Archivierung vorsätzlich die Übersicht über das Vermögen erschwert, um Vermögensteile aus der Insolvenzmasse beiseite zu schaffen oder zu verheimlichen (vgl. § 283 ff. StGB)

- Aus der gesellschaftsrechtlichen Haftung von Vorständen einer Aktiengesellschaft oder Geschäftsführern einer GmbH können sich auch zivilrechtliche Schadensersatzansprüche ergeben. Insbesondere im Bereich der unternehmerischen Risikovorsorge – zu der auch die ordnungsgemäße Archivierung zählt – haftet die Unternehmensleitung persönlich für unterlassene Risikomanagement-Maßnahmen, wenn dadurch ein finanzieller Schaden für das Unternehmen entsteht (vgl. §§ 93 Abs. 2 AktG, 43 Abs. 2 GmbHG).

Vorstände

Geschäftsführer

Sonstige explizit Verantwortliche

sind dazu verpflichtet, geeignete Maßnahmen zu implementieren,

zu **überwachen** und ständig zu **aktualisieren**, damit die Einhaltung aller gesetzlichen Vorschriften im Unternehmen gewährleistet ist.

Oberbegriffe:

Organisationsverschulden / Auswahlverschulden

Der Anspruch einer revisionssicheren Archivierung lautet : Niemandem – wie beispielsweise auch System-Administratoren, Geschäftsführern sowie externen Dritten wie Hackern – soll es möglich sein, Unternehmensdaten zu manipulieren.

Der Verband Organisations- und Informationssysteme hat dazu Grundsätze zur Revisionssicherheit von elektronischen Archiven definiert:

- Jedes Dokument wird unveränderbar archiviert,
- es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen,
- jedes Dokument muss mit geeigneten Retrievaltechniken (zum Beispiel durch das Indexieren mit Metadaten) wieder auffindbar sein,
- es muss genau das Dokument wiedergefunden werden, das gesucht worden ist,
- kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können,
- jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können,
- alle Inhalte müssen zeitnah wiedergefunden werden können,
- alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist,
- elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist,
- das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen (BDSG, HGB, AO etc.) sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

DATATREE
YOUR COMPLIANCE PROVIDER

Folge:

Nach den Regelungen der Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) reicht es nicht aus,
relevante E-Mails auszudrucken und abzuheften.
Sie müssen digital und revisionssicher (siehe Folie 10) innerhalb individueller Fristen gespeichert werden!

Vielen Dank für Ihre Aufmerksamkeit!

DATATREE AG
Bernd Fuhlert
Heubesstraße 10
40597 Düsseldorf
Tel: +49 211 5989471
Fax: +49 211 59894780
Mobil: +49 176 62960098
E-Mail: bernd.fuhlert@datatree.eu
Web:www.datatree.eu