Rainer KNYRIM / Markus OMAN

Archivsysteme mit Fokus auf ePersonalakten aus betriebswirtschaftlicher, technologischer und rechtlicher Sicht

Inhaltsübersicht

I. Einleitung / Problemstellung ... 177

II. Allgemeines zum Datenschutz ... 178

A. Aufbewahrungsdauer ... 178
B. Löschung ... 178

III. Die derzeit aktuellen Anwendungsgebiete der eArchive ... 178

A. Vernichtung von Originalunterlagen ... 179
B. Rz 1559 der Umsatzsteuerrichtlinien ... 179

IV. Digitale Personalakten ... 182

A. Mögliche Betriebsvereinbarungspflicht ... 182
B. Aufbewahrungs- und Löschungspflichten ... 184
C. Datenarten ... 184
D. Dokumenttypen ... 185
E. Mitarbeiterinformation über Scanvorgang ... 186

V. Datensicherheitsmaßnahmen ... 186

A. Zugriffsberechtigungen ... 187
B. Protokollierung ... 188
C. Verschlüsselung ... 188
D. Texterkennung und Volltextsuche ... 189

VI. Vorgehen bei der Einführung von ePersonalakten ... 189

VII. Zusammenfassung ... 191

I. Einleitung / Problemstellung

Eine immer größere Zahl an Konzernen beabsichtigt, sämtliche in Papierform vorhandenen Personalakten einzuscannen. Grund dafür ist die bessere Verfügbarkeit der Personalakten, die aufgrund von unterschiedlichen Standorten der Konzernunternehmen erforderlich ist. Die einmal eingescannten Papierakten werden oft weiterhin in Papierform archiviert aufgehoben. Die einzelnen Scanvorgänge hinsichtlich der bestehenden Papierakten werden oft durch ein Dritt-

unternehmen durchgeführt. Sobald der Altbestand an Personalakten eingescannt wurde, werden die Papierakten der neu eingetretenen Mitarbeiter von den Mitarbeitern der Personalabteilung laufend selbst eingescannt.

II. Allgemeines zum Datenschutz

A. Aufbewahrungsdauer

Nach § 6 Abs 1 Z 5 DSG 2000 dürfen Daten nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben. Die zulässige Dauer der Aufbewahrung personenbezogener Daten lässt sich daher primär aus den verschiedenen gesetzlichen Aufbewahrungsfristen ableiten. Es ist daher auch möglich, dass eine einmal rechtmäßige Verarbeitung durch Zeitablauf unzulässig wird. Es ist im Einzelfall sohin stets eine Interessenabwägung vorzunehmen sowie Bedacht auf die gesetzlichen Vorschriften zu nehmen.

B. Löschung

Sobald die Aufbewahrung und Verarbeitung der personenbezogenen Daten nicht mehr unbedingt erforderlich ist, müssten die Daten gelöscht oder anonymisiert werden. Unter „Löschen" ist die Unkenntlichmachung von Daten zu verstehen in der Art, dass sie der Datenanwendung unwiderruflich entzogen werden.[1] Siehe dazu näher bei III. B.

III. Die derzeit aktuellen Anwendungsgebiete der eArchive

Die derzeit am häufigsten eingesetzten eArchivanwendungen liegen im Bereich der Verarbeitung und Archivierung von Eingangsrechnungen, Ausgangsrechnungen, eRechnungen, Eingangspost, ePersonalakten und der Vertragsverwaltung.

Bei all diesen Anwendungsgebieten sind einerseits Anforderungen aus dem Steuer- und Unternehmensrecht und auf der anderen Seite auch zumeist die Beschränkungen des DSG 2000 zu beachten. Wir möchten an diesem Punkt nur einen kleinen Abriss zu diesen Themen geben und uns dann in diesem Artikel auf ePersonalakte konzentrieren.

Generell stehen zumeist die Nachvollziehbarkeitskriterien im Zentrum der Betrachtungen:

§ 132 Abs 2 BAO besagt, dass die Aufbewahrung von Belegen, Geschäftspapieren und sonstigen Unterlagen auf Datenträgern möglich ist, wenn gewährleistet ist, dass die Ablage vollständig, geordnet und inhaltsgleich erfolgt und eine urschriftgetreue Wiedergabe somit sichergestellt ist.

1 *Dohr/Pollirer/Weiss/Knyrim*, DSG[2] § 4 Anm 10

Des Weiteren entstehen **für den Unternehmer folgende Verpflichtungen**:
Die Wiedergabe muss auf Kosten des Unternehmens, in angemessener Frist und mit von diesem zur Verfügung gestellten Hilfsmitteln zur Lesbarmachung erfolgen.

Alle Merkmale, die Beweiskraft haben (Urschriftsgetreue Wiedergabe iSd § 132 BAO, § 190 UGB), müssen erhalten bleiben. Dies gilt für Dokumente, die originär auf Papier erstellt worden sind. Des Weiteren ist u.a. noch die Normierung durch den § 212 UGB (Aufbewahrungspflicht) und § 216 UGB (Vorlage von Unterlagen auf Datenträgern) zu beachten.

Bei der Archivierung von Daten, ist auch eine Orientierung an Bestimmungen[2] der BAO zur Bereitstellung von Daten sinnvoll.

Beim Verarbeiten von Papiereingangsrechnungen ist auf einen sorgfältigen und strukturierten Prozess zu achten und besonders auf die elektronische Aufbewahrung (besonders wenn man die Originale vernichten will), welche der USt-RL 1559 entsprechen muss[3].

A. Vernichtung von Originalunterlagen

Die Vernichtung von Originalunterlagen ist zulässig, sobald Belege revisionssicher und unlöschbar, also auf nicht wiederbeschreibbaren Medien archiviert sind (WORMfähig, siehe USt-RL RZ 1559)

B. Rz 1559 der Umsatzsteuerrichtlinien

- Information des BMF (Steuer- und Zollkoordination, Fachbereich Umsatzsteuer) aus dem Jahr 2005 - Speicherung und Archivierung von Eingangsrechnungen - INFO/0002-FB USt/05 - 9. Februar 2005:

Sachverhalt:

- Nach den Umsatzsteuerrichtlinien 2000 Rz 1559 kann der Beweis, dass dem Unternehmer eine Rechnung zugegangen ist, auch durch mikroverfilmte Rechnungen erbracht werden. Dasselbe gilt für die optischen Speicherplatten, wenn die mittels Scanner erfassten und urschriftgetreu auf der optischen Speicherplatte gespeicherten Rechnungen nicht mehr verändert werden können. In der Praxis werden die Eingangsrechnungen meist bei Einlangen eingescannt und dann auf der Festplatte zwischengespeichert und erst später auf den oben angeführten Medien archiviert.
- Beim Scann- und Verarbeitungsprozess ist zu beachten, dass die Originalrechnungen nicht schon ab der Zwischenspeicherung vernichtet werden kön-

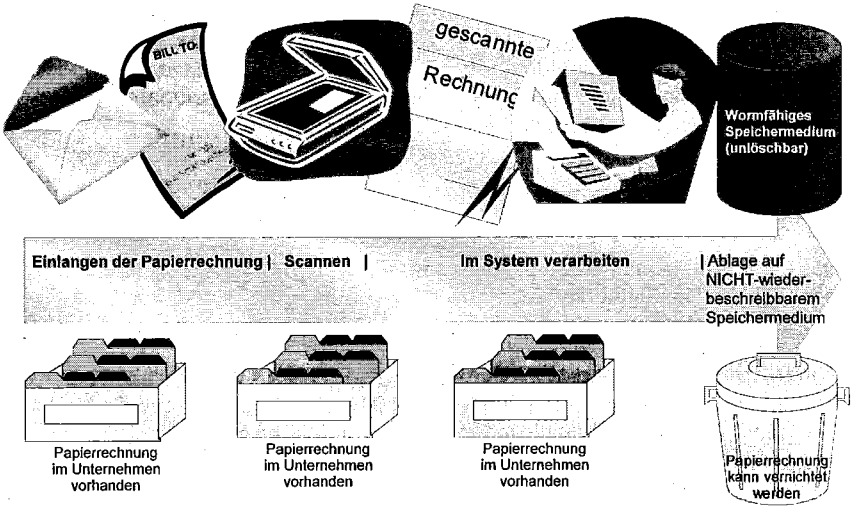
2 Bestimmungen zur Bereitstellung von Daten:
- §§ 131 Abs. 3 und 132 Abs. 3 BAO
- alle Daten, die für die Abgabenerhebung relevant sein können
- insbesondere auch Daten aus vorgelagerten Systemen (Kassen, Lagerbewirtschaftung)
- Grundaufzeichnungen
- Nachweis einzelner Geschäftsfälle

3 *Oman/Groschedl*, eRechnung: Die auf elektronischem Weg übermittelte Rechnung, Seite 119.

nen, sondern erst, wenn sie auf die wormfähigen Archivierungsmedien übertragen werden.

- Der bundesweite Fachbereich Umsatzsteuer vertritt die in den Umsatzsteuerrichtlinien Rz 1559 zum Ausdruck kommende Rechtsansicht, dass den umsatzsteuerrechtlichen Erfordernissen der Aufbewahrung von Originalrechnungen nur dann Genüge getan ist, **wenn die Rechnungen auf solchen EDV Trägern gespeichert werden, die nicht mehr verändert werden können.** Lediglich Abschriften und Durchschriften können auch auf wiederbeschreibbaren Datenträgern gespeichert werden. **Die Originalbelege dürfen erst dann vernichtet werden, wenn sie auf die nicht überschreibbaren Archivierungsmedien übertragen worden sind.**

Die Original-Papierrechnung darf also vernichtet werden, jedoch erst, wenn das vom Original gescannte Abbild (inhaltsgleich, voll leserlich und ausdruckbar) auf einem „wormfähigen Medium" unlöschbar gespeichert ist, wie die Grafik verdeutlicht.



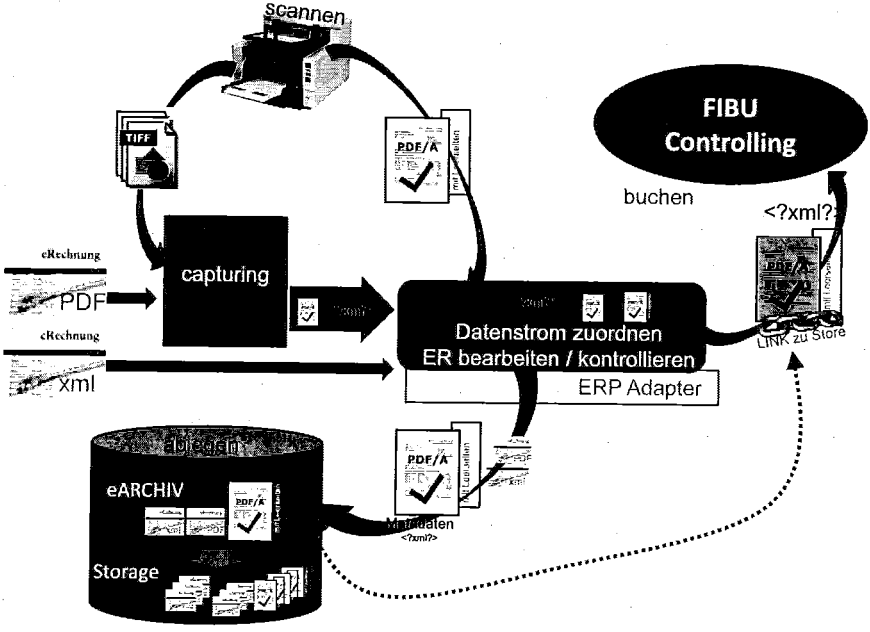
Die am elektronischen Weg übermittelte Rechnung iSd § 11 Abs 2 UStG hat derzeit folgenden Normenrahmen:

Die Anerkennung einer auf elektronischem Weg übermittelten Rechnung kann nur dann erfolgen, wenn die Echtheit der Herkunft und Unversehrtheit des Inhaltes gewährleistet ist. Des Weiteren ist die Zustimmung des Empfängers als Voraussetzung festgelegt, wobei diese Zustimmung keinem Formzwang unterliegt. Der Unternehmer hat eine Durch- oder Abschrift aufzubewahren (Aufbewahrungsfrist von 7 Jahren, wenn nicht andere gesetzliche Regelungen anderes Bestimmen), welche die Echtheit der Herkunft und Unversehrtheit des Inhaltes von auf elektronischem Weg übermittelten Rechnungen über die vorgeschriebene Aufbewahrungsfrist gewährleistet[4] (Verweis auf § 132 BAO und iwF den **Massensignaturerlass AÖF 2005/191 (BMF – 010219/0163 – IV /9/2005)**).

4 Technisch erstellt entsprechend § 2 Z 3 lit a-d SigG

Es bleibt abzuwarten, wie sich die neuen Regelungen bzgl. der eRechnung auf Basis der neuen EU-Richtlinie gestalten[5].

Folgendes Schaubild zeigt ein mögliches Zusammenspiel der verschiedenen Systeme im Bereich der diversen Eingangskanäle von Rechnungen.



Bevor die ePersonalakte detaillierter besprochen wird, möchten wir noch ein paar Gedanken zur Eingangspost und zur Vertragsverwaltung vorstellen:

Bei der Eingangspost ist besonders darauf zu achten, dass die Übernahme höchst sorgfältig (hierzu sind bestimmte Verfahren notwendig, deren Ausführung den Rahmen dieses Artikel sprengen würde) und zeitnah erfolgt. Danach sind ähnliche Verfahren sinnvoll wie bei der Eingangsrechnung.

Bei **Vertragsverwaltungen** sollte man sich primär folgenden Fragen stellen:

Das Verwalten von (schriftlichen) Vereinbarungen umfasst die Führung und Dokumentation der vertraglichen Verhandlungen zwischen Auftraggeber und Auftragnehmer, Vollstreckung von Verträgen und die Dokumentation von Änderungen. Zu beachten ist dabei, dass folgende Eckpunkte der Verwaltung von Verträgen gegeben sind:

- Abbildung von Unternehmensstrukturen, Hierarchien und Kompetenzen
- Alle Verträge im Überblick

5 Nach Artikel 233 Absatz 1 Unterabsatz 2 Mehrwertsteuer-Systemrichtlinie 2006/112/EG in der Fassung der Richtlinie 2010/45/EU des Rates zu den Rechnungsstellungsvorschriften vom 13. Juli 2010 legt jeder Unternehmer fest, in welcher Weise die Echtheit der Herkunft, die Unversehrtheit des Inhalts und die Lesbarkeit der Rechnung gewährleistet werden können. Dies kann durch jegliche innerbetriebliche Steuerungsverfahren erreicht werden, die einen verlässlichen Prüfpfad zwischen einer Rechnung und einer Lieferung oder Dienstleistung schaffen können.

- Benutzerverwaltung
- Eskalationsmöglichkeiten
- Genehmigungsprozesse, sowie transparente Prozesse
- Referenzierungsmöglichkeiten
- Revisionssichere Dokumentation und Revisionssicherheit der Dokumente (ev. unlöschbar über die vorgeschriebene Aufbewahrungsdauer)
- Schnelles Auffinden von Informationen und Dokumenten durch komfortable Such- und Filterfunktionalität
- Verwaltung von Rahmen- und Einzelverträgen
- Überwachung bzw. Auswertung von zB Fristen,
- Vertragsarchivierung
- Vertragscontrolling
- Vertragserstellung und -verhandlungen
- Vertragsvereinbarungen automatisiert erfüllen

Beispiele für Vertragsarten, die in einer Vertragsverwaltung vorhanden sein können:

- Beteiligungsverträge
- Gesellschaftsvereinbarungen
- Kommunikation GF / VST / AR (Corporate Governance)
- Konzernvereinbarungen
- Kreditverträge
- Kunden- und Lieferantenverträge
- Lizenzen und assoziierte Verträge (Wartung, SLA)
- Miet-, Pacht- und Leasingverträge
- Arbeitsverträge
- Rahmenvereinbarungen
- Versicherungspolizzen

IV. Digitale Personalakten

Bei der gänzlichen Digitalisierung der Personalverwaltung bestehen einerseits arbeits- und betriebsverfassungsrechtliche Rahmenbedingungen, andererseits öffentlich-rechtliche Verpflichtungen des Arbeitgebers zB aus dem DSG. Zu beachten ist auch, dass der Arbeitgeber aufgrund der Beweislastverteilung der Zivilprozessordnung mit einem Beweisproblem belastet wird und unter Umständen Ansprüche nicht mehr verfolgen oder abwehren kann, wenn er nicht (mehr) über die erforderlichen Unterlagen verfügt. Für den Fall, dass öffentlich-rechtliche Verpflichtungen zur Aufbewahrung der Originalpapierdokumente neben den eingescannten Dokumenten bestehen, ist ein Verstoß dagegen regelmäßig mit einer Verwaltungsstrafe bedroht.

A. Mögliche Betriebsvereinbarungspflicht

Elektronische Datenverarbeitungssysteme – wie ein digitaler Personalakt – können die Mitwirkungspflicht des Betriebsrates bewirken. Der Betriebsrat hat nach § 91 Abs 2 ArbVG das Recht, auf Verlangen die Grundlagen für die Verarbeitung und Ermittlung zu überprüfen und darf in die verwendeten Daten Einsicht neh-

men. Zur Einsicht des Betriebsrates in die Daten einzelner Arbeitnehmer ist regelmäßig deren Zustimmung erforderlich. [6]

Jene Datenanwendungen, die unbedingt eine Zustimmung des Betriebsrates benötigen, sind in § 96 Abs 1 ArbVG aufgezählt; diese sind im Hinblick auf elektronische Personaldatenbanken:

- Die Einführung von Personalfragebögen, sofern in diesen nicht bloß die allgemeinen Angaben zur Person und Angaben über die fachlichen Voraussetzungen für die beabsichtigte Verwendung des Arbeitnehmers enthalten sind (§ 96 Abs 1 Z 2 ArbVG);
- sowie die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren (§ 96 Abs 1 Z 3 ArbVG).

Zusätzlich regelt § 96a Abs 1 ArbVG weitere Maßnahmen, die zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates bedürfen, wobei diese Zustimmung aber durch eine Entscheidung der Schlichtungsstelle ersetzt werden kann. Es sind dies:

- Die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen. Eine Zustimmung ist aber nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben (§ 96a Abs 1 Z 1 ArbVG);
- sowie die Einführung von Systemen zur Beurteilung von Arbeitnehmern des Betriebes, sofern mit diesen Daten erhoben werden, die nicht durch betriebliche Verwendung gerechtfertigt sind (§ 96a Abs 1 Z 2 ArbVG).

Über diese hinausgehende Betriebsvereinbarungen sind nicht verpflichtend und wären im Hinblick auf EDV sog. Betriebsvereinbarungen über Maßnahmen zur zweckentsprechenden Benützung von Betriebseinrichtungen und Betriebsmitteln iSd § 97 Abs 1 Z 6 ArbVG, der sämtliche Themen beinhaltet, die in einer freiwilligen Betriebsvereinbarung abgeschlossen werden können. Zu beachten ist allerdings, dass, wenn eine derartige Betriebsvereinbarung einmal geschlossen ist, deren Abänderung oder Aufhebung nur mehr gemeinsam mit dem Betriebsrat erfolgen kann, wobei bei Nicht-Einigung mit dem Betriebsrat auf Antrag eines der Streitteile die Schlichtungsstelle entscheidet (§ 97 Abs 2 ArbVG).

Für die Betriebsvereinbarungspflicht kommt es nicht darauf an, welche Daten tatsächlich verarbeitet werden, sondern darauf, welche Daten aufgrund des Systems verarbeitet werden können. [7]

---

6 *Sacherer*, Der digitale Personalakt – Ist das „papierlose Personalbüro" zulässig?, RdW 2008, 96.

7 *Dohr/Pollirer/Weiss/Knyrim*, DSG², Anh V 17

B. Aufbewahrungs- und Löschungspflichten

Personaldaten dürfen aufgrund § 6 Abs 1 Z 5 DSG 2000 nicht unbegrenzt gespeichert werden, sondern sind zu anonymisieren oder zu löschen, wenn sie für das Arbeitsverhältnis oder Ansprüche aus diesem nicht mehr erforderlich sind und allfällige Aufbewahrungspflichten abgelaufen sind.

Es gibt hinsichtlich Personaldaten keine allgemeine, einfache Aufbewahrungsfrist oder -regel, sondern es greifen verschiedene, komplizierte Rechtsgrundlagen und Aufbewahrungsfristen. So müssen etwa Mitarbeiterdaten, die finanzielle Ansprüche aus dem Arbeitsverhältnis enthalten, drei Jahre lang nach deren Entstehen, buchhaltungsrelevante Daten hingegen sieben Jahre ab Jahresende nach deren Entstehen aufbewahrt werden. Sonderfristen gibt es überdies etwa für Daten zur Arbeitskräfteüberlassung oder Daten, die für die Ausstellung eines Dienstzeugnisses erforderlich sind, sodass Daten bis 30 Jahren nach ihrem Entstehen oder sogar nach Ende eines Dienstverhältnisses noch relevant sein könnten.[8]

Auch wenn das DSG 2000 keine Legaldefinition des Löschbegriffs enthält, ist unter Löschen von Daten iSd DSG 2000 das „physische Löschen"[9] gemeint und nicht das bloß „logische Löschen"[10]. Um das Löschungsgebot zu erfüllen, genügt es daher nicht, die Datenorganisation so zu verändern, dass ein „gezielter Zugriff" auf die betreffenden Daten ausgeschlossen ist.

In Hinblick auf die in unterschiedlicher Länge gebotene, höchstzulässige Aufbewahrungsdauer ist es nur sehr schwer möglich, standardisierte „Löschroutinen" zu erstellen. Dies auch deshalb, weil sich die oben genannten Speicherfristen auch wieder ändern können.

Sehr wesentlich ist daher, dass das EDV-System, mit dem die eingescannten Daten verwaltet werden, die Definition individueller Löschregeln für verschiedene Datenkategorien und einzelne Dateien zulässt und diese auch an geänderte Umstände (zB Gesetzesänderungen) adaptiert werden können.

C. Datenarten

Es werden meist Daten des Mitarbeiters betreffend seinen Dienstvertrag sowie etwaige Ergänzungen daraus, zu Aus- und Weiterbildung des Dienstnehmers, zu Abwesenheiten, zu Exekutionen und Pfändungen, zu Darlehen (Entgeltvorschüssen), zu vom Mitarbeiter verlangten Bestätigungen für andere öffentliche Stellen, sowie zum Vorpensionseintritt gesammelt und verarbeitet. Da dies keine über die Erfüllung der mit dem Arbeitsvertrag zusammenhängenden Verpflichtungen des Arbeitgebers sind, könnte man auf den ersten Blick meinen, dass für die Einführung des elektronischen Personalaktes keine Betriebsvereinbarungspflicht besteht, weil die Datenverarbeitung nicht über die Erfüllung von Verpflichtungen hinausgeht, die sich aus Gesetz, Kollektivvertrag oder Arbeitsvertrag

8 *Sacherer*, Der digitale Personalakt – Ist das „papierlose Personalbüro" zulässig?, RdW 2008, 98.

9 = eine Maßnahme mit der Wirkung, dass der Auftraggeber nicht mehr über die Daten verfügt, OGH vom 15.04.2010, 6 Ob 41/10p

10 = eine Maßnahme, mit der erreicht wird, dass Daten innerhalb der EDV-Anlage nicht mehr zur Verfügung stehen, unkenntlich gemacht werden sowie durch das Betriebssystem als nicht mehr vorhanden interpretiert werden

ergibt. Da beim kompletten Einscannen des Personalaktes aber eine Vielzahl unterschiedlicher Daten erfasst wird, bei denen dieses Argument unter Umständen nicht immer greift,[11] könnte dadurch dennoch eine Betriebsvereinbarungspflicht nach § 96a Abs 1 Z 1 ArbVG auslöst werden.[12]

Ebenso könnten verschiedene Varianten von Personalfragebögen enthalten sein, die einer Betriebsvereinbarungspflicht nach § 96 Abs 1 Z 2 ArbVG[13] unterliegen dürften. Siehe dazu schon oben. Zu qualifizierten Fragebögen, die eine Betriebsvereinbarungspflicht auslösen, zählen Fragebögen, die zB Fragen nach Vorstrafen, gesundheitlicher Eignung oder Erkrankung, Religionszugehörigkeit oder dem Beendigungsgrund vorheriger Dienstverhältnisse enthalten, insbesondere wenn sie in Einstellungsfragebögen enthalten sind. Sollten nun derartige Informationen (Fragen) auch in den Personalfragebögen enthalten sein, die wiederum in Personalakten abgelegt sind, würde auch dadurch „indirekt" die Betriebsvereinbarungspflicht des eingescannten Personalaktes ausgelöst.[14]

Ebenso denkmöglich ist, dass Zielvereinbarungen und Jahresergebnisgespräche stattfinden, die im Personalakt erfasst werden. Sollte dies der Fall sein, so könnten derartige Daten für den eingescannten Personalakt ein weiteres Mal eine Betriebsvereinbarungspflicht auslösen, nämlich nach § 96 Abs 1 Z 4 ArbVG als Information über Regelungen von sonstigen leistungsbezogenen Prämien, sofern die Zielvereinbarungen einen Leistungsbezug haben. Ebenso könnten die Zielvereinbarungen und Jahresergebnisgespräche ein „System zur Beurteilung von Arbeitnehmern des Betriebes" sein, mit dem Daten erhoben werden, die nicht durch betriebliche Verwendung gerechtfertigt sind und das daher nach § 96a Abs 1 Z 2 ArbVG betriebsvereinbarungspflichtig ist.

Es ist weiters denkbar, dass Personalstatistiken, die Persönlichkeitsbeurteilungen der Arbeitnehmer zulassen, erstellt werden. Diese können entweder aus den eingescannten Daten erst generiert werden oder anderweitig erstellt werden und bei den eingescannten Daten abgespeichert werden. In diesem Fall wird in der Regel eine zustimmungspflichtige Kontrollmaßnahme nach § 96 Abs 1 Z 3 ArbVG vorliegen.[15]

D. Dokumenttypen

Typische Arten von Dokumenten, die sich in Personalakten befinden, sind folgende (nicht abschließende Aufzählung):

- Bewerbungen
- Zeugnisse
- Dienstverträge

11 Etwa weil auch Daten über frühere Ausbildungen oder zu Gehaltsvorschüssen erfasst werden; diese fallen streng genommen nicht unter die für die Erfüllung der gesetzlichen, kollektivvertragsrechtlichen und arbeitsvertraglichen Verpflichtungen erforderlichen Daten.

12 Es handelt sich bei der Betriebsvereinbarung gemäß § 96a Abs 1 Z 1 ArbVG um eine erzwingbare Betriebsvereinbarung: sollte zwischen Unternehmen und dem Betriebsrat keine Einigung gefunden werden, kann eine entsprechende Regelung von beiden Seiten bei der gerichtlichen Schlichtungsstelle zwangsweise durchgesetzt werden.

13 Diese ist nicht durch die Schlichtungsstelle erzwingbar.

14 Ausführlich *Dohr/Pollirer/Weiss/Knyrim*, DSG[2], Anh V 17 B.

15 Ausführlich *Dohr/Pollirer/Weiss/Knyrim*, DSG[2], Anh V 17 B.

- Vereinbarungen
- Ausweise, Meldezettel
- Kursbestätigungen/Zertifikate
- Div. Unterlagen, etwa
  - Pendlerpauschale
  - AV/AE-Formular
  - (Versicherungs-)Polizzen
  - Pensionskassa,
  - Protokolle (Mitarbeitergespräch, Personalmeetings, ...)
- Lohnzettel (L16)
- Arbeitsbescheinigung
- Nettozettel, Lohnkonto
- Reisekostenabrechnung
- Strafregisterauskunft, soweit zulässig

Festzustellen ist, dass in der Praxis oft viel mehr Dokumente in Personalakten archiviert sind, die in diesen gar nicht aufgehoben werden sollen, etwa veraltete Strafregisteraufzüge, Gesundheitszeugnisse, Dokumente hinsichtlich familiärer Anlässe, sogar 20 Jahre alte Pläne über private Bauvorhaben von Arbeitnehmern (zur Gewährung von Gehaltsvorschüssen oder Firmenkrediten) wurde in der Praxis von den Autoren schon gesichtet. Daher sollten die Akten vor der Weiterbehandlung und insbesondere vor der Digitalisierung durchforstet werden und alle unzulässig aufbewahrten Dokumente (sowohl hinsichtlich Dokumentenart als auch hinsichtlich Speicherdauer) zunächst aus dem Personalakt entfernt und vernichtet werden.

Grundsätzlich könnte man die Register des Aktes (auch in elektronischer Form) in folgende Bereiche gliedern:

Bewerbungsunterlagen, Aus- & Weiterbildung, Vertragsunterlagen, Beurteilungen, (gesetzlich vorgeschriebene) Aufzeichnungen, Kopien von Urkunden, Dokumente (sofern für Entgelt oder arbeitsvertragliche Regelungen von Bedeutung), weitere Unterlagen für Steuer und Sozialversicherung. Weitere jeweils spezifisch notwenige Kategorien sind natürlich denkbar.

E. Mitarbeiterinformation über Scanvorgang

Um die Mitarbeiter darüber zu informieren, dass ihre in Papierform vorgelegten Unterlagen, nämlich der gesamte Personalakt, elektronisch eingescannt wird, ist zu empfehlen, in die Dienstverträge eine Information entsprechend § 24 DSG 2000 aufzunehmen.[16]

V. Datensicherheitsmaßnahmen

Nach § 14 Abs 1 DSG 2000 sind für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, zur Gewährleistung der Datensicherheit Maßnahmen zu treffen. Insbesondere ist auch sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind.

16 *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 24 Anm 4

Dabei ist je nach der Art der verwendeten Daten und je nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt.[17] Insbesondere ist, soweit dies erforderlich ist, nach § 14 Abs 2 DSG 2000

- die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
- die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
- jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
- die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
- die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
- die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
- Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
- eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

A. Zugriffsberechtigungen

Nach § 14 Abs 2 Z 5 DSG 2000 ist die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln (Zugriffsbeschränkungsprinzip). Es soll sichergestellt werden, dass durch technische, organisatorische und personelle Regelungen erreicht wird, dass nur die zur Benutzung des IT-Systems berechtigten Personen auf die Daten zugreifen können.

Ob es ein ausgereiftes Zugriffsberechtigungskonzept gibt, dass die Zugriffsberechtigungen nach dem üblicher und richtiger Weise angewandten Prinzip auf „need to know"-Basis vergibt, sodass nur jene Personen und nur insoweit Zugriff auf Daten erhalten, als diese unbedingt einen Zugriff benötigen, um die ihnen organisatorisch zugeordneten Tätigkeiten ausführen zu können, ist im Einzelfall einer genauen Betrachtung zu unterziehen: Das Zugriffsberechtigungskonzept, insbesondere die Strukturierung der Zugriffsrollen und die Zuteilung der einzelnen Rollen auf die jeweiligen Arbeitsfunktionen und die Korrektheit der Zuteilung der Berechtigungen an die richtigen Personen ist von der internen Revision nachzuprüfen. Zu beachten ist dabei das fehlende datenschutzrechtliche Konzernprivileg, wodurch Zugriffe im Konzern nur unter besonderen Bedingungen zulässig sind.[18]

17 *Knyrim*, Datenschutzrecht² (2012) 267.
18 *Knyrim*, Datenschutzrecht² (2012) 26.

B. Protokollierung

Die Datensicherheitsmaßnahmen in § 14 DSG 2000 sehen ua vor, dass Protokoll über die erfolgten Datenzugriffe geführt werden soll. Zur Frage, welche Informationen dabei gesammelt werden müssen, ist folgendes zu sagen:

Nach § 14 Abs 2 Z 7 DSG 2000 ist, soweit im Hinblick auf Abs 1 erforderlich, Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen (optimal: auch bloße Bildschirmabfragen) und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Eine derartige Protokollierung muss unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewähren, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Grundsätzlich sind derartige Protokoll- und Dokumentationsdaten drei Jahre lang aufzubewahren (§ 14 Abs 5 DSG 2000). Die Aufbewahrungsfrist von drei Jahren kann im Einzelfall aber kürzer oder länger sein. Eine Verkürzung kommt unter anderem dann in Betracht, wenn Daten früher gelöscht werden müssen (dies zB, weil die Unrichtigkeit der Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist – § 27 Abs 1 DSG). Längere Aufbewahrungsfristen sehen zB die Steuergesetze vor (nach § 132 BAO). Dann, wenn die Protokoll- und Dokumentationsdaten unbedingt notwendig sind, um die Unveränderheit von Daten nachzuweisen, zB in der Buchhaltung, wenn dies nicht anders gewährleistet ist (durch ein sonst revisionssicheres System), teilen sie das Schicksal des ihnen zugrunde liegenden Datenbestandes, und sollten dann solange aufbewahrt werden, wie die ihnen zugrunde liegenden Daten.[19]

C. Verschlüsselung

§ 14 Abs 1 DSG 2000 schreibt vor, dass für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen sind. Dabei ist je nach der Art der verwendeten Daten und je nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

In § 14 Abs 2 DSG 2000 sind beispielhaft Datensicherheitsmaßnahmen aufgezählt, die eine Verschlüsselung nicht explizit nennen. Die Verschlüsselung von Daten kann daher eine sinnvolle, flankierende Datensicherheitsmaßnahme sein, es besteht aber kein expliziter und ausdrücklicher gesetzlicher Zwang zu einer Datenverschlüsselung, insbesondere dann nicht, wenn diese technisch nicht oder nur sehr schwer durchführbar und wirtschaftlich nicht vertretbar ist und die Datensicherheit durch andere Maßnahmen ausreichend hergestellt werden kann.

Inwieweit die Verschlüsselung von als Bilddaten eingescannter Personalakten technisch – sowohl in Hinblick auf die Datenmengen und die Zugriffszeiten als

19 *Jahnel*, Datenschutzrecht (2010), Rz 5/24.

auch in Hinblick auf die notwendige lange Speicherdauer (im Fall der Personalakten etwa ein ganzes „Mitarbeiterleben" lang und noch viele Jahre danach) – umsetzbar, sinnvoll und wirtschaftlich vertretbar ist, muss analysiert werden. Sofern das Unternehmen die Scans nicht verschlüsselt auf ihren Servern ablegt, muss jedenfalls durch andere Datensicherheitsmaßnahmen – wie etwa die oben erwähnten Zugriffschranken und Zugriffsberechtigungskonzepte – sichergestellt werden, dass kein Missbrauch der Daten erfolgen kann.

D. Texterkennung und Volltextsuche

Es ist durchaus naheliegend, dass die als Bilddateien eingescannten Seiten (zB aus den Personalakten) einer automatischen Volltexterkennung unterzogen werden, damit der Inhalt der Bilddateien mittels Volltextsuche gefunden werden kann. Bei einer derartigen Volltextsuche sollte darauf geachtet werden, dass diese so gestaltet ist, dass sie nur hinsichtlich einzelner Dokumente bei einem einzelnen Mitarbeiter durchgeführt werden kann, also eine Volltextsuche erst dann möglich ist, wenn zuerst ein einzelner Mitarbeiter angewählt wurde und bei dem einzelnen Mitarbeiter eine Scandatei ausgewählt wurde, in der die Volltextsuche durchgeführt werden soll.

Es sollte technisch unbedingt vorausgesetzt werden, dass eine Volltextsuche über den gesamten eingescannten Datenbestand nur unter besonderen Umständen[20] durchgeführt werden kann, damit nicht Auswertungen „quer" über alle Mitarbeiter durchgeführt werden könnten, die über das für das Arbeitsverhältnis erforderliche Ausmaß hinausgehen und dann uU weder arbeitsverfassungsrechtlich noch datenschutzrechtlich rechtfertigbar wären. Eine derartige Volltextsuche über den gesamten Datenbestand beinhaltet nämlich ein enormes Missbrauchspotential (etwa Suche nach Krankheitsinformationen oder bestimmten Krankheiten oder Kontodaten oder Kreditkartennummern etc.).

VI. Vorgehen bei der Einführung von ePersonalakten

Bei der Einführung von ePersonalakten hat sich in der Praxis folgender Prozess bewährt:

1. Personalakt (Papier) aufbereiten und „entrümpeln"
   Es ist wichtig im ersten Schritt die Personalakte so aufzubereiten, dass nur jene Unterlagen in eine elektronische Form gebracht werden, bei denen dies Sinn macht (aus der Sicht des DSG, wenn ein rechtmäßiger Zweck besteht) und ein Register erstellt wird. Entsprechend der Registerordnung sollte am Beginn jedes neuen Registerabschnitts ein Trennblatt (z.B. mit Barcode) eingefügt werden (Bewerbungsunterlagen, Vertragsunterlagen, Beurteilungen, Verrechnungen, etc.). Dies wiederum verhilft dazu, dass schon während des Scanprozesses und der nachfolgenden Ablage im eArchiv automatisch eine passende Klassifizierung bzw. Zuordnung erfolgt.

20 ZB Verdachtsfall auf strafbare Handlung oder Verletzung von Dienstpflichten im Einzelfall.

2. Ist-Analyse der HR Abläufe
   Die Einführung eines neuen Systems bietet auch die Chance, bestehende Abläufe zu überdenken. Um bessere Abläufe definieren zu können, ist es unabdingbar, den (tatsächlich gelebten) Ist-Ablauf genau zu kennen und transparent zu dokumentieren.
3. Soll - Prozess definieren
   Bevor Entscheidungen bzgl der Technik getroffen werden, sollte jedenfalls der (möglichst optimierte) Soll-Prozess definiert sein und wiederum transparent dokumentiert werden. Dies sollte, wie schon bei der Ist-Erhebung, mit einem prozessmodellierungs- & Visualisierungswerkzeug geschehen.
4. Dokumenttypen definieren
   Um den verschiedenen normativen und betriebswirtschaftlichen Anforderungen gerecht zu werden, empfiehlt es sich, ein eArchiv und ebenso die ePersonalakte mit der Hilfe von Dokumenttypen (Bewerbungsschreiben, Dienstvertrag, Mitarbeiterbeteiligungen, Stock Options, Verwarnungen, Zeugnisse, Dokumente zu Arbeitsunfällen, Arbeitserlaubnis, An-/Abmeldungen GKK, Jahreslohnzettel L16, etc.) zu verwalten bzw. zu nutzen. Nur so ist ein ordnungsgemäßer Einsatz bei gleichzeitig maximierter Effizienz möglich.
5. Aufbewahrungsfristen der Dokumenttypen und Zugriffe festlegen
   Jedem Dokumenttyp werden Aufbewahrungsfristen (sog Retention Times) zugewiesen, welche an zwingende Normen (EStG, BAO, AngG, UrlG, EO, AbgEO, VVG, AuslBG, ABGB, etc. und an die begrenzenden Normen des DSG) anzupassen sind. Des Weiteren ist zu definieren, wer welchen Zugriff auf die Informationen hat, was in welcher Form protokolliert ist und wer unter welchen Bedingungen auf diese Protokolle[21] Zugriff hat.
6. Abstimmung mit dem Implementierungspartner und Review des Sollprozesses
   Nach dem alle organisatorischen Maßnahmen durchgeführt wurden, muss eine kritische Abstimmung mit dem Implementierungspartner durchgeführt werden, um die Soll-Vorgehensweise abzusichern bzw. nötigenfalls anzupassen.
7. eArchive implementieren
   Die technische Implementierung erfolgt zumeist durch den externen Partner in enger Abstimmung mit den hauseigenen Technologieexperten.
8. Altdaten & Dokumente (wenn notwendig) übernehmen
   Wenn Altdaten zu übernehmen sind, so ist dies ebenfalls genau zu planen und nachweislich sicherzustellen, dass die Migration ordnungsgemäß (vollständig, geordnet und nachvollziehbar) durchgeführt wurde.
9. Tests durchführen
   Der gesamte Prozess ist mittels eines mehrstufigen Tests (auf technischer Ebene, aus Sicht der Anwender und auf Basis der internen & externen Normen, wie z.B. IKS, Controlling; gesetzlichen Anforderungen) auf Fehlerfreiheit zu prüfen.
10. Ordnungsgemäße Dokumentation erstellen
    Das gesamte Verfahren (Planung, Implementierung, Migrationen, Test, Schu-

21 § 14 Abs 2 Z7 DSG 2000: Es ist Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Siehe dazu näher *Dohr/Pollirer/Weiss/Knyrim,* DSG[2] § 14 Anm 12.

lungen, etc.) ist so zu dokumentieren,[22] dass das Vorgehen für einen sachverständigen Dritten nachvollziehbar ist und die Ordnungsmäßigkeit aus dieser Unterlage eindeutig hervorgeht. Des Weiteren sollten auch klar nachprüfbare Ansätze für einen externen Auditor geboten werden, damit dieser mittels eigener Prüfhandlungen das ordnungsgemäße Handeln nachprüfen und gegebenenfalls testieren kann.

VII. Zusammenfassung

Eine immer größere Zahl an Konzernen beabsichtigt, sämtliche in Papierform bestehenden Aktenarchive einzuscannen. Zurzeit werden eArchivanwendungen im Bereich der Verarbeitung und Archivierung von Eingangsrechnungen, Ausgangsrechnungen, eRechnungen, Eingangspost, ePersonalakten und der Vertragsverwaltung am häufigsten eingesetzt. Bei all diesen Anwendungsgebieten sind einerseits Anforderungen und Verpflichtungen aus dem Steuer- und Unternehmensrecht und auf der anderen Seite die Beschränkungen des DSG 2000 zu beachten.

Daten dürfen nicht unbegrenzt gespeichert werden, sondern sind zu anonymisieren oder zu löschen, wenn sie für das Rechtsverhältnis oder Ansprüche aus diesem nicht mehr erforderlich sind und allfällige Aufbewahrungspflichten abgelaufen sind. Dabei ist festzuhalten, dass unterschiedliche Datenarten regelmäßig unterschiedlichen Aufbewahrungsfristen unterliegen und im Umkehrschluss entsprechend abweichende Löschungsverpflichtungen auferlegen. Keineswegs lässt sich aus der Rechtsordnung eine generelle Aufbewahrungspflicht von sieben Jahren für alle Datenarten ableiten. Es ist daher vom Auftraggeber auch technisch sicherzustellen, dass die unterschiedlichen Verpflichtungen in Bezug auf Speicherdauer von Datenarten umgesetzt werden können. So wird es beispielsweise den Anforderungen des DSG 2000 und den sich aus anderen Gesetzen ergebenden Aufbewahrungspflichten nicht entsprechend sein, einen gesamten Personalakt im *.tiff/*.PDF/*PDF/A-Format in eine einzige Datei einzuscannen und das gesamte Image „untrennbar" in Bezug auf die einzelnen Datenarten für eine gleich lange Dauer abrufbar zu halten.

Es sind für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, zur Gewährleistung der Datensicherheit Maßnahmen zu treffen. Insbesondere ist auch sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind. Es sollten technische und organisatorische Vorkehrungen getroffen werden, damit eine Volltextsuche über den gesamten eingescannten Datenbestand nur unter besonderen Umständen durchgeführt werden kann.

---

22 Die Dokumentationspflicht ergibt sich auch aus den Datensicherheitsmaßnahmen des DSG, siehe § 14 Abs 2 Z 8 DSG. Anleitung zum Aufbau einer Dokumentation ergeben sich aus dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informatik (BSI).

Bei der Implementierung von eArchivanwendungen sollte technisch unbedingt eingeschränkt werden, dass Daten nicht in einer Art und Weise abrufbar gehalten werden, die über das erforderliche Ausmaß hinausgehen und dies dann uU weder arbeitsverfassungsrechtlich noch datenschutzrechtlich rechtfertigbar wäre. Um solche Problematiken zu minimieren, wird eine Vorgangsweise ähnlich der unter Punkt VI. geschilderten Prozesse empfohlen.