2/2014

PRAXISPROJEKT
Konzernweite Personaldaten
Rainer Knyrim, Bernhard Horn

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Personaldatenverarbeitung: Vom Papierakt zum ePersonalakt

Markus Oman, Rainer Knyrim

Checkliste: E-Recruiting

Hans-Jürgen Pollirer

Datenschutz beim Einsatz mobiler „smarter" Endgeräte

Wolfgang Goricnik, Thomas Riesenecker-Caba

Datenschutz am Arbeitsplatz: Was darf der Arbeitgeber kontrollieren?

Viktoria Haidinger

Interview mit Andrea Dillenz

Katharina Schmidt

ISSN 2313-5409

dako.manz.at

MANZ

P.b.b. Verlag Manz 1230 Wien, Gutheil Schoder Gasse 17

Markus Oman
Geschäftsführender Gesellschafter O.P.P.-Beratungsgruppe

Rainer Knyrim
Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte

Vom Papierakt zum ePersonalakt in der Praxis

eArchiv; Betriebsvereinbarungspflicht; Aufbewahrung und Löschung. Immer mehr Firmen und öffentliche Organisationen digitalisieren ihre Archive, inklusive der in Papierform vorhandenen Personalakten. Was ist bei der Umsetzung in der Praxis zu beachten?

eArchiv & Workflowsysteme

Die derzeit am häufigsten eingesetzten elektronischen Anwendungen liegen im Bereich der Verarbeitung und Archivierung von Eingangsrechnungen, Ausgangsrechnungen, eRechnungen, Eingangspost, ePersonalakten und Vertrags- bzw Dokumentenverwaltung. Bei all diesen Anwendungsgebieten sind Anforderungen aus dem Steuer- und Unternehmensrecht sowie die Beschränkungen des DSG 2000 zu beachten.

Generell ist es empfehlenswert, sich an den Anforderungen für die rein elektronische Aufbewahrung von Finanzdokumenten zu orientieren,[1] dabei stehen zumeist die Nachvollziehbarkeitskriterien im Zentrum der Betrachtungen: § 132 Abs 2 BAO besagt, dass die Aufbewahrung von Belegen, Geschäftspapieren und sonstigen Unterlagen auf Datenträger möglich ist, wenn gewährleistet ist, dass die Ablage vollständig, geordnet und inhaltsgleich erfolgt und eine urschriftgetreue Wiedergabe somit sicherstellt ist.

Des Weiteren entstehen für **den Unternehmer folgende Verpflichtungen:** Die Wiedergabe muss auf Kosten des Unternehmens, in angemessener Frist und mit zur Verfügung gestellten Hilfsmitteln zur Lesbarmachung erfolgen und der Unternehmer muss – soweit erforderlich – dauerhafte Wiedergaben beibringen. Alle Merkmale, die Beweiskraft haben (urschriftsgetreue Wiedergabe iSd § 132 BAO, § 190 UGB), müssen erhalten bleiben. Überdies ist ua auch die Normierung durch § 212 UGB (Aufbewahrungspflicht) und § 216 UGB (Vorlage von Unterlagen auf Datenträgern) zu beachten.[2]

Ein zusätzlicher sinnvoller **Orientierungsansatz** sind die **10 Goldenen Regeln**[3] zur elektronischen Archivierung:

- **1.** Jedes Dokument muss unveränderbar archiviert werden können.
- **2.** Es darf kein Dokument auf dem Weg in das Archiv oder im Archiv selbst verloren gehen.
- **3.** Jedes Dokument muss mit geeigneten Retrievaltechniken und Retrievalprozessen wieder auffindbar sein.
- **4.** Es muss genau das Dokument bzw File wieder gefunden werden können, das gesucht worden ist (zu beachten ist: dies ist auch ein organisatorisches Thema).
- **5.** Kein Dokument darf während seiner definierten Lebenszeit zerstört werden können.
- **6.** Jedes Dokument muss in genau der gleichen (gewünschten) Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
- **7.** Jedes Dokument muss zeitnah wieder gefunden werden können.
- **8.** Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustands möglich ist.
- **9.** Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informations- und Revisionssicherheitsverlust möglich ist.
- **10.** Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen sowie die betrieblichen Vorgaben aller Anwender hinsichtlich Datensicherheit, Datenschutz und aller sonstigen relevanten Normen über die Lebensdauer des Archivs sicherzustellen.

Vernichtung von Originalunterlagen

Die Vernichtung von zB papierenen Originalunterlagen[4] ist zulässig, sobald Belege revisionssicher und unlöschbar, also auf nicht wiederbeschreibbaren Medien archiviert sind. So darf etwa eine Original-Papierrechnung (zB ein Spesenbeleg eines Mitarbeiters) vernichtet werden, wenn das vom Original gescannte Abbild (inhaltsgleich und für den Menschen lesbar) auf einem „wormfähigen Medium“[5] über die gesetzliche Aufbewahrungsfrist unlöschbar gespeichert ist.

Digitale Personalakten

Bei der gänzlichen Digitalisierung der Personalverwaltung und insb beim Einscannen bestehen einerseits arbeits- und betriebsverfassungsrechtliche Rahmenbedingungen, andererseits öffentlich-rechtliche Verpflichtungen des Arbeitsgebers, zB aus dem DSG 2000.

Mögliche Betriebsvereinbarungspflicht

Für elektronische Personalakten könnte die Mitwirkung des Betriebsrats notwendig sein. 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 nehmen. Zur Einsicht des Betriebsrats in die Daten einzelner Arbeitnehmer ist regelmäßig deren Zustimmung erforderlich.[6]

Je nach konkreter Ausgestaltung, Funktionalität und Inhalt der ePersonalakten (etwa wenn in diesen Personalfragebögen enthalten sind), zu denen es noch keine Betriebsvereinbarung gibt, könnte diese nach § 96 Abs 1 Z 2 ArbVG erforderlich sein. Ebenso könnte iSv § 96 Abs 1 Z 3 ArbVG eine Betriebsvereinbarung erforderlich sein, wenn der ePersonalakt Kontrollmaßnahmen zur Kontrolle der Arbeitnehmer ermöglicht. Der ePersonalakt könnte auch als System zur automatisierungsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers eingestuft werden, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen (§ 96 a Abs 1 Z 1 ArbVG). Dies, da beim kompletten elektronischen Erfassen bzw Verarbeiten des Personalakts eine

[1] *Oman/Groschedl*, eRechnung² (2013). [2] Mehr zu eArchiven siehe *Knyrim/Oman*, Archivsysteme mit Fokus auf ePersonalakten aus betriebswirtschaftlicher, technologischer und rechtlicher Sicht, in *Jahnel*, Jahrbuch Datenschutzrecht 2012 (2012) 177 ff. [3] Vgl VOI – Verband Organisations- und Informationssysteme e.V., www.voi.de. [4] *Oman/Groschedl*, eRechnung² 2013 [5] „worm“ ist die Abkürzung für write once read multiple. [6] *Sacherer*, Der digitale Personalakt – Ist das „papierlose Personalbüro“ zulässig? RdW 2008, 96.

Vielzahl unterschiedlicher Daten erfasst wird, bei denen uU nicht mehr argumentiert werden kann, dass es sich um ein nicht betriebsvereinbarungspflichtiges „Basissystem" handelt.[7]

Der ePersonalakt könnte auch ein System zur Beurteilung von Arbeitnehmern des Betriebs (§ 96 a Abs 1 Z 2 ArbVG) sein, wenn Zielvereinbarungen oder Jahresgespräche im ePersonalakt erfasst werden und man deren betriebliche Notwendigkeit nicht argumentieren kann.

Darüber hinausgehende Betriebsvereinbarungen sind nicht verpflichtend und wären dann etwa im Hinblick auf IKT sog Betriebsvereinbarungen über Maßnahmen zur zweckentsprechenden Benützung von Betriebseinrichtungen und Betriebsmitteln iSd § 97 Abs 1 Z 6 ArbVG.

Für die Betriebsvereinbarungspflicht kommt es nicht darauf an, welche Daten tatsächlich verarbeitet werden, sondern darauf, welche Daten aufgrund der technisch möglichen Funktionen des Systems verarbeitet werden **könnten**.[8]

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 unterschiedlich lange Aufbewahrungsfristen, die auf verschiedenen gesetzlichen Grundlagen beruhen.

Es gibt für Personaldaten keine allgemeine, einfache Aufbewahrungsfrist oder -regel, sondern es greifen verschiedene, komplizierte Rechtsgrundlagen und Aufbewahrungsfristen ineinander. So müssen etwa Mitarbeiterdaten, die **finanzielle Ansprüche** aus dem Arbeitsverhältnis enthalten, drei Jahre 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 für Daten, die für die Ausstellung eines Dienstzeugnisses erforderlich sind. Da die allgemeine Verjährungsfrist für Ansprüche in Österreich laut ABGB 30 Jahre ist, können Daten bis 30 Jahre nach ihrem Entstehen oder sogar nach Ende eines Dienstverhältnisses noch relevant sein.[9]

Auch wenn das DSG 2000 keine Legaldefinition des Löschbegriffs enthält, ist unter Löschen von Daten iSd DSG 2000 das „physische Löschen"[10] gemeint und nicht das bloß „logische Löschen".[11] Um das Löschungsgebot zu erfüllen, genügt es daher nicht, die Datenorganisation nur so zu verändern, dass ein „gezielter Zugriff" auf die betreffenden Daten ausgeschlossen ist.

Wesentlich ist daher, dass das System, mit dem die eingescannten Daten verwaltet werden, die Definition **individueller Löschregeln** für verschiedene Datenkategorien und einzelne Dateien zulässt und diese auch für die Zukunft wieder adaptiert werden können.

Dokumenttypen

Typische Arten von **Dokumenten**, die sich in Personalakten befinden, sind bspw folgende: Bewerbungen, Zeugnisse, Dienstverträge, Vereinbarungen, Ausweise, Meldezettel, Kursbestätigungen/Zertifikate, Pendlerpauschale, AV/AE-Formulare, (Versicherungs-)Polizzen, Pensionskassa, Protokolle (Mitarbeitergespräch, Personalmeetings), Lohnzettel (L16), Arbeitsbescheinigungen, Nettozettel, Lohnkonto, Reisekostenabrechnungen.

Festzustellen ist, dass in der Praxis oft viele Dokumente in Personalakten archiviert sind, die in diesen gar nicht aufgehoben werden sollten, etwa veraltete Strafregisterauszüge, Gesundheitszeugnisse, Dokumente über familiäre Anlässe, sogar alte Pläne über private Bauvorhaben von Arbeitnehmern wurde in der Praxis von den Autoren schon gesichtet. Daher sollten die Akten vor der Weiterbehandlung und insb 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.

Nicht benötigte Dokumente sollten aus dem Personalakt entfernt werden.

Grundsätzlich könnte man die **Register** des Aktes (auch in elektronischer Form) zB 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 notwendige Kategorien sind natürlich denkbar.

Mitarbeiterinformation über Scanvorgang

Um die Mitarbeiter darüber zu informieren, dass ihre in Papierform vorgelegten Unterlagen, nämlich der gesamte Personalakt, elektronisch eingescannt werden, ist zu empfehlen, in die Dienstverträge eine Information entsprechend § 24 DSG 2000 aufzunehmen und die bestehende Belegschaft darüber zu informieren.[12]

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. Insb ist auch sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind.[13] Die Regelungen des § 14 Abs 2 DSG 2000 sind, soweit möglich und wirtschaftlich vertretbar, einzuhalten.

Zugriffsberechtigungen

Nach § 14 Abs 2 Z 5 DSG 2000 sind die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln (Zugriffsbeschränkungsprinzip). Ein ausgereiftes Zugriffsberechtigungskonzept, das die Zugriffsberechtigungen nach dem üblichen und richtigerweise angewandten **„Need to know"-Prinzip** vergibt, ist jedenfalls notwendig. Zugriffe innerhalb des Konzerns sind, wenn sie nicht reinen Dienstleisterzwecken dienen, meist beim DVR meldepflichtige Datenübermittlungen und können, wenn die EU-Grenzen dabei überschritten werden, eine Vorabgenehmigung durch die Datenschutzbehörde erforderlich machen.

[7] Weil etwa auch Daten über frühere Ausbildungen bei anderen Arbeitgebern oder zu Gehaltsvorschüssen erfasst werden; diese fallen streng genommen nicht unter die für die Erfüllung der gesetzlichen, kollektivvertragsrechtlichen und arbeitsvertraglichen Verpflichtungen erforderlichen Daten. Betriebsvereinbarungen nach § 96 a Abs 1 Z 1 ArbVG sind erzwingbare Betriebsvereinbarungen: Sie können von beiden Seiten bei der gerichtlichen Schlichtungsstelle zwangsweise durchgesetzt werden. Siehe dazu auch *Knyrim/Oman*, Archivsysteme aaO.
[8] *Dohr/Pollirer/Weiss/Knyrim*, DSG² Anh V 17. [9] *Sacherer*, Der digitale Personalakt – Ist das „papierlose Personalbüro" zulässig? RdW 2008, 98. [10] Das ist eine Maßnahme mit der Wirkung, dass der Auftraggeber nicht mehr über die Daten verfügt; OGH 15. 4. 2010, 6 Ob 41/10 p. [11] Das ist 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. [12] *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 24 Anm 4.
[13] *Knyrim*, Datenschutzrecht² (2012) 267.

Protokollierung

Die Datensicherheitsmaßnahmen in § 14 DSG 2000 sehen ua vor, dass ein Protokoll über die erfolgten Datenzugriffe geführt werden soll. Welche Informationen müssen dabei gesammelt werden? Nach § 14 Abs 2 Z 7 DSG 2000 ist, soweit im Hinblick auf Abs 1 erforderlich, Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insb Änderungen, Abfragen (optimal auch bloße Bildschirmabfragen) und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können.

Auch über die erfolgten Datenzugriffe muss ein Protokoll geführt werden.

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 (weil zB die Unrichtigkeit der Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist; § 27 Abs 1 DSG 2000). Längere Aufbewahrungsfristen sehen zB die Steuergesetze vor (§ 132 BAO). Wenn die Protokoll- und Dokumentationsdaten unbedingt notwendig sind, um die Unveränderheit von Daten nachzuweisen (zB in der Buchhaltung), und wenn dies nicht anders gewährleistet ist (durch ein sonst revisionssicheres System), teilen sie das Schicksal des ihnen zugrunde liegenden Datenbestands und sollten so lange aufbewahrt werden wie die ihnen zugrunde liegenden Daten.[14]

Texterkennung und Volltextsuche

Es ist naheliegend, dass die als Bilddateien eingescannten Seiten oder bereits elektronisch existierenden Dokumente einer automatischen Volltexterkennung unterzogen werden, damit der Inhalt der Bilddateien mittels Volltextsuche gefunden werden kann. Bei einer derartigen Volltextsuche sollte darauf geachtet werden, dass sie 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 diesem einzelnen Mitarbeiter eine Scandatei ausgewählt wurde, in der die Volltextsuche durchgeführt werden soll.

Eine **Volltextsuche** über den **gesamten Datenbestand** sollte technisch unbedingt eingeschränkt werden und nur unter besonderen Umständen[15] durchgeführt werden, da damit Auswertungen „quer" über alle Mitarbeiter durchgeführt werden könnten, die über das für das Arbeitsverhältnis erforderliche Ausmaß hinausgehen und uU weder arbeitsverfassungsrechtlich noch datenschutzrechtlich zu rechtfertigen wären.

PRAXISTIPP

Bei der Einführung von ePersonalakten hat sich in der Praxis folgender Prozess bewährt:[16]

- **Personalakt (Papier) aufbereiten und „entrümpeln":**
  Es ist wichtig, im ersten Schritt die Personalakten so aufzubereiten, dass einerseits 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 andererseits ein Register erstellt wird. Entsprechend der Registerordnung sollte am Beginn jedes neuen Registerabschnitts ein Trennblatt (zB mit Barcode) eingefügt werden (Bewerbungsunterlagen, Vertragsunterlagen, Beurteilungen, Verrechnungen etc). Dies hilft, dass schon während des Scanprozesses und der nachfolgenden Ablage im eArchiv automatisch eine passende Klassifizierung bzw Zuordnung erfolgt.
- **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.
- **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- und Visualisierungswerkzeug geschehen.
- **Dokumenttypen definieren:**
  Um den verschiedenen normativen und betriebswirtschaftlichen Anforderungen gerecht zu werden, empfiehlt es sich, das eArchiv und ebenso die ePersonalakte mit Hilfe von Dokumenttypen (Bewerbungsschreiben, Dienstverträge, Mitarbeiterbeteiligungen, Stock Options, Verwarnungen, Zeugnisse, Dokumente zu Arbeitsunfällen, Arbeitserlaubnis, An-/Abmeldungen Krankenkasse, Jahreslohnzettel L16 etc) zu verwalten bzw zu nutzen. Nur so ist ein ordnungsgemäßer Einsatz bei gleichzeitig maximierter Effizienz möglich.
- **Aufbewahrungsfristen der Dokumenttypen und Zugriffe festlegen:**
  Jedem Dokumenttyp werden Aufbewahrungsfristen (sog Retention Times) zugewiesen, welche an die entsprechenden Gesetze (EStG, BAO, AngG, UrlG, EO, AbgEO, VVG, AuslBG, ABGB) und an die begrenzenden Regelungen des DSG 2000 anzupassen sind; man nennt dies auch „document lifecycle". 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[17] Zugriff hat.
- **Abstimmung mit dem Implementierungspartner und Review des Soll-Prozesses:**
  Nachdem alle organisatorischen Maßnahmen durchgeführt wurden, muss eine kritische Abstimmung mit dem Implementierungspartner durchgeführt werden, um die Soll-Vorgehensweise abzusichern bzw nötigenfalls anzupassen.
- **eArchive implementieren:**
  Die technische Implementierung erfolgt zumeist durch einen externen Partner in enger Abstimmung mit den hauseigenen Technologieexperten.

[14] *Jahnel,* Datenschutzrecht (2010) Rz 5/24; *Oman/Groschedl,* eRechnung² (2013). [15] ZB Verdachtsfall auf strafbare Handlung oder Verletzung von Dienstpflichten im Einzelfall. [16] Siehe schon *Knyrim/Oman,* Archivsysteme, aaO. [17] § 14 Abs 2 Z 7 DSG 2000: Es ist Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insb Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Siehe dazu näher *Dohr/Pollirer/Weiss/Knyrim,* DSG² § 14 Anm 12.

- Altdaten und 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.
- Tests durchführen:
  Der gesamte Prozess ist mittels eines mehrstufigen Tests (auf technischer Ebene, aus Sicht der Anwender und auf Basis der internen und externen Normen, wie zB IKS[18] Controlling; weitere unternehmensrelevante gesetzliche Anforderungen) auf Fehlerfreiheit zu prüfen.
- Ordnungsgemäße Dokumentation erstellen:
  Das gesamte Verfahren (Planung, Implementierung, Migrationen, Test, Schulungen etc) ist so zu dokumentieren,[19] 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.

Dako 2014/14

[18] ISd § 22 Abs 1 GmbHG bzw § 82 AktG. [19] Die Dokumentationspflicht ergibt sich auch aus den Datensicherheitsmaßnahmen des DSG 2000, siehe § 14 Abs 2 Z 8 DSG 2000. Eine Anleitung zum Aufbau einer Dokumentation ergibt sich aus dem IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informatik (BSI).

Zum Thema

Über die Autoren

Mag. Ing. Markus Oman, CSE, ist geschäftsführender Gesellschafter der O.P.P.-Beratungsgruppe. Tel: +43 (0)699 125 180 89, E-Mail: markus.oman@opp-beratung.com, Internet: www.opp-beratung.com

Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte in Wien. Tel: +43 (0)1 533 16 95, E-Mail: knyrim@preslmayr.at, Internet: www.preslmayr.at

Literatur

Knyrim/Oman, Archivsysteme mit Fokus auf ePersonalakten aus betriebswirtschaftlicher, technologischer und rechtlicher Sicht, in *Jahnel,* Jahrbuch Datenschutzrecht 2012 (2012) 177 ff;

Oman/Groschedl, eRechnung[2] (2013);

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