Sieben Grundsätze zum Datenschutz

Sicherheit von Digitalen Personalakten

Seit den Anfängen der Digitalen Personalakte Mitte der 1990er Jahre[1] wurden die Rechts- und Revisionsvorschriften nach und nach konkretisiert, so dass heute die Digitale Personalakte als rechtssicher gilt, wenn bestimmte Rahmenbedingungen eingehalten sind, die im Folgenden in den ‚Sieben Grundsätzen zum Datenschutz' erläutert werden sollen.

Spätestens seit Bekanntgabe der Abschaffung der papiergebundenen Lohnsteuerkarte ab nächstem Jahr – der Papierphalanx im Personalumfeld – verstummen auch die letzten Kritiker der Digitalen Personalakte und nehmen zur Kenntnis, dass heute in Gerichtsurteilen sogar explizit Bezug auf Dokumente aus der Digitalen Personalakte genommen wird (z.B. VG Sigmaringen, Aktenzeichen 1 K 1235/04).

Allerdings müssen einige Voraussetzungen geschaffen sein, um die Sicherheit von Digitalen Personalakten zu gewährleisten:

1. Detailliertes Berechtigungskonzept

Über einen differenzierten Zugriffsschutz muss gewährleistet sein, dass nur Berechtigte genau die Dokumente der Akte sehen oder bearbeiten können, für die sie zugelassen sind. Hierbei ist auf die Ausgestaltung der bekannten Fragestellung „Wer darf Was bei Wem?" zu achten: Hierbei sind die Berechtigten (Wer) zu definieren (Personalaschbearbeiter, Führungskräfte, Mitarbeiter…), die Rollen mit den zulässigen Funktionen (Was), die von diesen ausgeführt werden dürfen (nur lesen, drucken, attribuieren, löschen…) sowie auf welche Gruppen von Akten (Wen) zugegriffen werden darf (standortbezogen, abteilungs-/kostenstellenweise…)[2].

2. Einsichtsbeschränkung

Aus dem Berechtigungskonzept leiten sich entsprechend die Einsichtsbeschränkungen ab, die der Frage nachgehen, welche Teile, d.h. welche Dokumente der Akte für wen zur Verfügung stehen sollen. Eine datenschutzkonforme Gestaltung muss hier die unterschiedlichen Benutzergruppen entsprechend berücksichtigen. So sollte z. B. der Personalabrechner nur auf die abrechungsrelevanten Dokumente Zugriff haben.

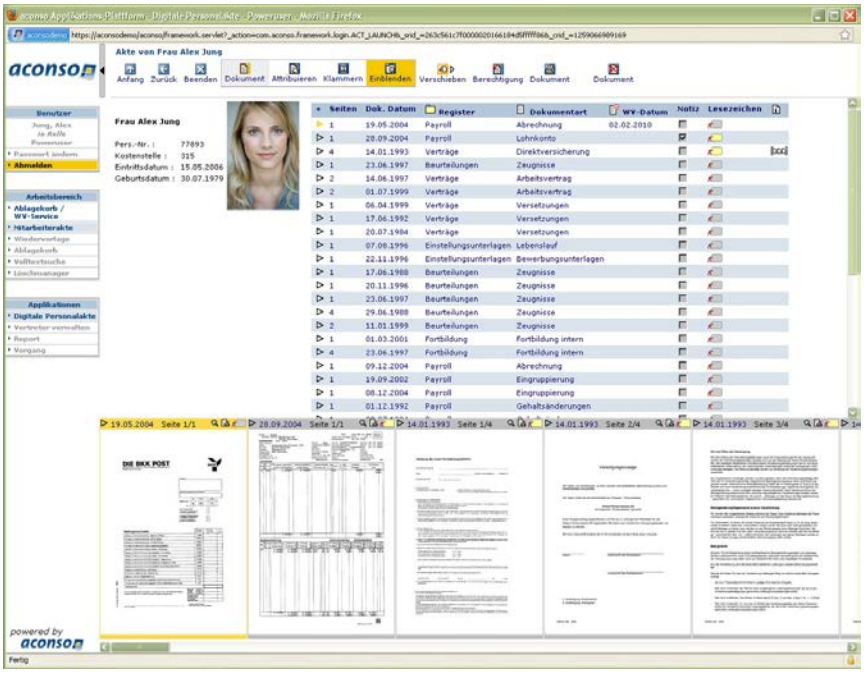
3. Protokollierung

Die sekundengenaue Protokollierung stellt die Grundlage der Nachvollziehbarkeit aller Änderungen von Metadaten (z. B. Registerzuordnung) sowie des Dokumenten-Check-in und -out (z.B. Einscannung, Löschung) innerhalb der Digitalen Personalakte dar. Diese kann – unter Beachtung der Einschränkungen des Betriebsverfassungsgesetzes – auch bis hin zur Protokollierung von reiner Recherchetätigkeit reichen.

Unbedingt zu beachten ist, dass nicht alle Tätigkeiten in der Digitalen Personalakte protokolliert werden dürfen, insbesondere bei rückstandsfreier Löschung, da das Löschprotokoll Rückschlüsse auf ein Vorhandensein eines Dokumentes zulässt. Etliche Systeme – gerade aus dem fiskalpolitisch geprägten Abrechungsumfeld – können dies bis heute nicht umsetzen.

4. Mehrere ineinandergreifende Sicherheitsmechanismen

Hierbei werden i.d.R. folgende vier Aspekte verstanden: (a) persönliche Authentifizierung und Autorisation des Benutzers, (b) Verschlüsselung der Kommunikation zwischen Server und Client, (c) sichere Übernahme von Daten und Berechtigungen aus HR-Systemen, insbesondere dem Abrechnungssystem und schließlich (d) das nicht-Speichern von Informationen im lokalen Cache.



Look and Feel der Digitalen Personalakte mit aconso FastView©

5. Rechts- und revisionssichere Archivierung

Um die Unveränderbarkeit der Dokumentinhalte sicherzustellen, muss eine vollständige Übertragung des Originals – nicht einer Kopie [sic!] – auf das Speichermedium erfolgen und dort ordnungsmäßig in einem unveränderbaren, rechtssicheren Format wie TIFF G4 oder PDF/A gespeichert werden, um dann jederzeit unverzüglich mit unverändertem Inhalt und Index mittels eindeutiger Dokument-ID retrievalt (wiedergegeben) werden zu können[3]. Dass auch beim Einscannen von Papier die Einhaltung des Datenschutzgesetzes berücksichtigt werden muss, sei hier eigens hingewiesen: Insofern scheitert die kostengünstigere Erstverscannung im nicht-deutschen Rechtsraum[4].

6. Trennung von Datenbank und Archivbereich

Heute werden zurecht insbesondere auf Seite des technischen Designs hohe Ansprüche an die Sicherheit gestellt: Die bewusste Trennung von Datenbank, in der die Metadaten zum Dokument gespeichert werden, und Archivbereich, auf dem die eigentlichen Dokumente gespeichert werden, führt dazu, dass unterschiedliche Personen administrieren können: Während der Datenbankspezialist nur Zugriff auf die Datenbank hat – und damit höchstens Metadaten sehen könnte –, kann ein anderer IT-Spezialist für den Archivbereich dort nur unsortierte Dokumentmengen sehen, d. h. ein gezieltes Suchen nach einem bestimmten Dokument ist nicht möglich. Damit ist die auf Personalseite oft berechtigt geäußerte Sorge, nun könnten auch Personen der IT gezielten (wenn auch nicht legalen) Zugriff auf Personendaten bekommen, unbegründet.

7. Verfahrensdokumentation

Die Umsetzung der Dokumentation des vollständigen Prozessablaufes – zu dem nicht nur der ITtechnische , sondern auch der organisatorische Prozess zählt – wird nicht selten gescheut, obgleich in Tz. 6 der GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme) eine solche Verfahrensdokumentation eindeutig vorgeschrieben ist. Sie gilt als umfangreich, ressourcen- und damit kostenintensiv, aber auch – nicht zu Unrecht – als Garant für Rechtssicherheit. In ihr wird nicht nur das interne Kontrollsystem (IKS) dokumentiert, das die Gesamtheit aller aufeinander abgestimmten Kontrollen, Maßnahmen und Regelungen der Personal-Organisation umfasst, sondern auch die Beschreibung der sachlogischen Lösung (z. B. Beschreibung von Datenbeständen, Verarbeitungsregeln, Datenaustausch…) wie auch deren technische Umsetzung in der sogenannten programmtechnischen Lösung sowie der Beschreibung zur Programmidentität und Datenintegrität. Darüber hinaus hat sie Arbeitsanweisungen für den Anwender zu enthalten. Sind diese ‚Sieben Grundsätze zum Datenschutz' eingehalten, so darf von einer rechts- und revisionssicheren Personalakte ausgegangen werden, die vor dem Hintergrund der Novellierung des Bundesdatenschutzgesetzes (BDSG) neue Brisanz bekommt.

Ausblick

Mit der Novellierung des BDSG vom 1.9.2009 wird in § 32 BDSG zum einen erstmals explizit auf Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses eingegangen, zum anderen auf die nicht automatisierte Verarbeitung ausgedehnt, d. h. auf die althergebrachte Papiersammlung von Personendaten, wie sie häufig noch in Unternehmen in der papiergebundenen Personalakte vorzufinden ist. Damit wird sich künftig eine Papierakte immer schwerer als eine Digitale Personalakte tun, alle Rechtsvorschriften einhalten zu können. Kurz: Die Digitale Personalakte ist heute sicherer als ihre papiergeführte Schwester – vorausgesetzt alle Datenschutzvorschriften werden gemäß BDSG exakt eingehalten.

[1] Grentzer: Räumlich-strukturelle Auswirkungen von IuK-Technologien in transnationalen Unternehmen, Münster 1999, S. 131-147

[2] Grentzer: Die Einführung einer digitalen Personalakte – Leitfaden für den Praktiker, Lohn + Gehalt Ausgabe 02/2005, März 2005

[3] Geis, Grentzer, Jänicke: Rechtliche Betrachtung eines digitalen Personalakten-Systems, Lohn + Gehalt Ausgabe 02/2003, März 2003

[4] Zur Bestandsaktendigitalisierung siehe: Bartosch: Digitale Personalakte, Frechen 2008, S.160-172; Rauchenecker, Grentzer: Die Digitale Personalakte – Perfekt Scannen, Lohn + Gehalt Ausgabe

04/2007, Juni 2007

Autorenkontakt

aconso AG
Dr. Martin Grentzer
Bavariaring 26 | 80336 München
Tel +49-89-516186-0 | Tel +49-89-516186-29
E-Mail: grentzer@aconso.com | www.aconso.com