Checkliste zur Rechtssicherheit

Was sollten Sie für einen rechtskonformen Umgang mit Personalakten beachten?

Personalakten, ob digital oder analog, beinhalten personenbezogene und damit besonders schützenswerte Daten. Für den Umgang mit ihnen formulieren das Bundesdatenschutzgesetz (BDSG) sowie das Betriebsverfassungsgesetz (BetrVG) einige Richtlinien und Vorschriften. Darüber hinaus gilt es eventuelle Betriebsvereinbarungen und technische wie organisatorische Schutzmaßnahmen (TOM) einzuhalten. Damit Sie auf der sicheren Seite sind, fasst diese Checkliste die zentralen rechtlichen Anforderungen im Umgang mit elektronischen Personalakten für Sie zusammen. Erläuterungen zu den Einzelpunkten finden Sie im Anhang.

Folgendes müssen Sie beachten:

- ☐ Erlaubnis: Achten Sie darauf, dass von allen Ihren Mitarbeitern eine Einwilligung zur Datenerhebung vorliegt.

- ☐ Transparenz: Informieren Sie Ihre Mitarbeiter über die Art, Umfang und Grund der Datenerhebung. Stellen Sie jederzeit sicher, dass Ihre Arbeitnehmer die Möglichkeit haben, in die über sie geführten Personalakten Einsicht zu nehmen.

- ☐ Integrität: Stellen Sie sicher, dass die personenbezogenen Daten korrekt sind und es auch bleiben.

- ☐ Zweckbindung: Gewährleisten Sie, dass die Daten nur für den vorher definierten Zweck erhoben werden.

- ☐ Datensparsamkeit& Datenvermeidung: Sammeln Sie nicht wahllos Daten, sondern erheben Sie nur die tatsächlich geschäftsrelevanten und notwendigen personenbezogenen Daten

- ☐ TOM: Achten Sie auf die Einhaltung aller technischen und organisatorischen Schutzmaßnahmen (TOM) nach Anlage zu §9 des BDSG. (Näheres unter Erläuterungen.)

- ☐ Vorabkontrolle: Vor der Einführung einer elektronischen Personalaktenlösung müssen Sie das System durch Ihren betrieblichen Datenschutzbeauftragten kontrollieren und freigeben lassen.

Erläuterungen

Personenbezogene Daten werden in besonderer Weise durch das Bundesdatenschutzgesetz (BDSG) geschützt. Es erlaubt die Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten jedoch nur in einem begrenzten Umfang (§ 28 und § 32). Das heißt, der elektronische Umgang mit den personenbezogenen Daten ist an unterschiedliche Bedingungen geknüpft.

- ○ Ein wichtiges Forderungsbündel sind **Datensparsamkeit und Datenvermeidung** (§ 3a BDSG). Das heißt, Arbeitgeber dürfen nur die zwingend notwendigen Daten erheben und verarbeiten. Diese Forderung dient vor allem der Prävention von Datenschutzverletzungen. Je weniger Daten erhoben werden, umso weniger Datenpannen können auftreten. Was zwingend notwendig ist, muss auch vor der Datenerhebung geklärt sein. Ein wahlloses Sammeln von Daten und eine spätere Auswertung nach ad-hoc Fragestellungen ist nicht zulässig.

- ○ Das Prinzip der **Richtigkeit** oder, im Kontext von Datenhaltung und Verarbeitung etwas konkretisiert, die **Integrität** der Daten ist eine zentrale Anforderung. Arbeitgeber müssen sicherstellen, dass die personenbezogenen Daten korrekt sind und es auch bleiben. Durch die automatisierte Übernahme von Mitarbeiterstammdaten aus dem führenden HR-System lassen sich etwa die Veränderungen der Arbeitnehmerdaten durch eine fehlerhafte manuelle Eingabe vermeiden. Dazu muss natürlich der verlustfreie und korrekte Datentransfer zwischen den Applikationen gesichert sein. Integrität betrifft zudem Punkte wie das ordnungsgemäße Scannen und lesbar machen von Dokumenten sowie den Schutz vor Veränderungen durch eine langfristig revisionssichere Archivierung.

- **Transparenz** bei der Datenerhebung und Datenverarbeitung ist eine weitere gesetzliche Verpflichtung. Hieraus ergeben sich etwa das Einsichtsrecht des betroffenen Mitarbeiters in seine Akte (§ 34 BDSG) und die Möglichkeit zur Kontrolle des Systems durch den Datenschutzbeauftragten eines Unternehmens. Systemseitig muss es also möglich sein, Dritten jederzeit einen Zugriff auf Personalakten zu gewähren, beispielsweise dem Betriebsrat (nach § 83 BetrVG).

Technische und organisatorische Schutzmaßnahmen (TOM)

Die **Anlage zu §9 des BDSG** beschreibt, welche technischen und organisatorischen Schutzmaßnahmen (TOM) Sie als Arbeitgeber im Umgang mit elektronischen Akten treffen müssen. Die elektronische Personalakte unterstützt sie dabei in fast allen Belangen. Dennoch gilt es einige Dinge zu beachten.

1. Zutrittskontrolle

Stellen Sie sicher, dass nur befugte Mitarbeiter Zutritt zu den Räumlichkeiten haben, in denen die Verarbeitung personenbezogener Daten stattfindet.

2. Zugangskontrolle

Gewährleisten Sie, dass nur befugtes Personal über die nötigen Login-Daten für die Nutzung der elektronischen Personalaktenlösung verfügt.

3. Zugriffskontrolle

Erstens dürfen Ihre Mitarbeiter nur auf die Inhalte zugreifen können, für die sie berechtigt sind. Zweitens muss sichergestellt sein, dass die Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Hier leistet die elektronische Personalakten-Anwendung schon sehr viel. Sie müssen nur dafür Sorge tragen, dass auch niemand über Umwege und Hintertüren in Ihrer IT auf die Daten zugreifen kann, etwa durch ungesicherte Netzwerke.

4. Weitergabekontrolle

Ähnlich wie bei dem vorherigen Punkt geht es um die Vermeidung unberechtigter Zugriffe und Veränderungen durch die eine physische oder digitale Weitergabe der Daten. Sie müssen protokollieren, wem Sie die Daten wofür zur Verfügung stellen. Beim physischen Transport, etwa zu einem Dienstleister, müssen Ihre Personalakten in verschließbaren Behältern aufbewahrt werden. Ebenso muss sich der Dienstleister dem Datenschutz verpflichten (Auftragsdatenvereinbarung).

5. Eingabekontrolle

Sie müssen nachträglich überprüfen können, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. Die elektronische Personalakten-Lösung macht diese Nachvollziehbarkeit möglich. Stellen Sie aber sicher, dass sich nur berechtigtes Personal einloggen kann.

6. Auftragskontrolle

Als Auftraggeber müssen Sie dafür sorgen, dass die von Ihnen an Dritte, etwa einen Scandienstleister, übergebenen Daten, nur so verarbeitet werden, wie Sie es beabsichtigt haben. Nehmen Sie unbedingt Ihre Kontrollrechte war.

7. Verfügbarkeitskontrolle

Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Themen sind etwa:

- ☐ Brandschutzmaßnahmen
- ☐ Überspannungsschutz
- ☐ Unterbrechungsfreie Stromversorgung
- ☐ Klimaanlage
- ☐ Festplattenspiegelung
- ☐ Backupkonzept
- ☐ Virenschutzkonzept
- ☐ Schutz vor Diebstahl

Diese Checkliste und auch die Erläuterungen können natürlich nur eine Hilfestellung für die zentralen Kriterien eines rechtskonformen Umgangs mit personenbezogenen Daten und elektronischen Personalakten sein. Sollten Sie bei einigen Punkten im Zweifel sein, ob und wie sie sich in Ihrem Unternehmen umsetzen lassen, ziehen Sie bitte eine professionelle Rechtsberatung hinzu.

Über forcont

Die forcont business technology gmbh (www.forcont.de) ist ein auf Enterprise Content Management (ECM) spezialisiertes Softwarehaus mit Hauptsitz in Leipzig und einer Geschäftsstelle in Berlin. Das 1990 als IXOS Anwendungs-Software GmbH gegründete Unternehmen bietet standardisierte Anwendungsprodukte und individuelle Projektlösungen zur Steuerung dokumentenlastiger Geschäftsprozesse – alternativ auch als Software-as-a-Service (SaaS) aus der Cloud. Die technologische Basis ist die Software forcont factory FX. forcont leistet zudem den kompletten Service im ECM-Umfeld von SAP. Zu den mehr als 200 Kunden (http://www.forcont.de/unternehmen/referenzen) zählen so namhafte Unternehmen und Einrichtungen wie ALBA Group plc & Co. KG, Deutsche Solar GmbH, Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR), GASAG Berliner Gaswerke AG, Radeberger Gruppe KG, Total Deutschland GmbH und TRW Airbag Systems GmbH.

Ansprechpartner

Gunther Ebert, Manager ECM Products, forcont business technology gmbh
E-Mail: gunther.ebert@forcont.de