

HR performance

entfesseln befähigen verändern



**Weltweit den Bildungsprozess
organisieren
bei MAN DIESEL & TURBO**

Digitale Personalakten sicher speichern und verwalten

„In meinem Aktenschrank sind sensible Daten am sichersten.“ Diese Einschätzung konnte man noch vor wenigen Jahren aus dem Mund so manchen Personalers hören. Inzwischen wissen die meisten nicht nur, dass die Digitalisierung von Personalakten für effizientere Arbeitsabläufe sorgt, sondern auch, dass die Mitarbeiterdaten elektronisch mindestens ebenso sicher aufbewahrt und verwaltet werden wie in der Papiervariante. Grundsätzlich gilt das erst recht beim Betrieb der digitalen Personalakte in der Cloud – vorausgesetzt, man hat bei der Wahl des Outsourcing-Partners alles richtig gemacht.

Eine Lösung für die digitale Personalakte steht bei vielen Personalern weit oben auf der Wunschliste. Schließlich hat sich die Software in diesem Bereich inzwischen zu deutlich mehr als einem elektronischen Abbild der klassischen Personalakte entwickelt. Mit Funktionen, die beispielsweise die Verwaltung von Bewerbungen, den Schriftverkehr mit Mitarbeitern und Behörden oder das Personalcontrolling erleichtern, unterstützen sie die Arbeitsprozesse in der Personalarbeit und entwickeln sich rasch zur zentralen Anwendung in der Abteilung.

Auch in puncto Sicherheit haben sie dem klassischen Aktenschrank einiges voraus: Verschlüsselte Datenübertragung, eine revisionssichere Archivierung sowie ein ausgefeiltes Berechtigungssystem gelten heute als Stand der Technik bei der digitalen Personalakte. Sichere Lösungen erkennt man unter anderem auch daran, dass im Fall eines Falles alle Zugriffe und Änderungen an den Akten in der Bearbeitungshistorie detailliert nachvollzogen werden können.

Überhaupt sollte zunächst einmal die Softwareauswahl im Vordergrund stehen. Aus der Analyse der zu unterstützenden Abläufe ergeben sich funktionale, logistische, aber auch technische Anforderungen: Welche Stammdaten sollen in der digitalen Personalakte geführt werden? Wo müssen Formulare und Prozesse individuell angepasst werden? Wer soll von wo aus Zugriff auf das System erhalten? Wie sehen die einzelnen Rollen und Rechte aus? Soll ein vorhandenes HR-System eingebunden werden, um die Mitarbeiter-Stammdaten direkt in die digitale Personalakte zu übernehmen? Welche Geräte wie Dokumentenscanner oder Belegleser sollen eingebunden werden?

Selbst betreiben oder auslagern?

Ist die passende Software-Lösung gefunden, stellt sich als nächstes die Frage, wie diese betrieben werden soll. In der Regel bieten sich die Optionen, entweder die eigene IT-Abteilung damit zu beauftragen, sich um die Installation der benötigten Technik, der Software und deren Betrieb zu kümmern, oder aber diese Tätigkeiten komplett auszulagern. Sie werden dann entweder vom Rechenzentrum des Herstellers oder einem unabhängigen Outsourcing-Partner übernommen, der die Software über eine Cloud-Infrastruktur betreibt.

Welches Modell letztlich besser passt, hängt von vielen Faktoren ab. Oftmals sind technische und personelle Ressourcen in der unternehmenseigenen IT-Abteilung ausschlaggebend. Ein wichtiges Kriterium ist aber auch, wie stark der Lösungsanbieter seinen Kunden jeweils bei einer möglichst schnellen Einführung unterstützen kann. Unabdingbar ist zudem eine eingehende finanzielle Betrachtung, bei der die genauen Kosten oder Verrechnungspreise der Varianten ermittelt und miteinander verglichen werden. So verteilen sich im Hosting-Modell die Kosten in der Regel als gleichmäßige Betriebsausgaben über die Nutzungszeit, statt bei der eigenen Softwareinstallation das Unternehmen an eine langfristig abzuschreibende Investition zu binden. Andererseits kann der Betrieb durch die eigene IT zumindest vorübergehend kostengünstiger sein, wenn dort etwa freie Ressourcen nach einer ohnehin erfolgten Kapazitätserweiterung mitgenutzt werden können.

Den richtigen Betreiber finden

Schon beim Einholen von Angeboten gilt es, geeignete Rechenzentren, Hosting- oder Cloud-Anbieter zu finden, die den Betrieb der ausgewählten Anwendung übernehmen können. Liegen bereits Erfahrungen mit einem Rechenzentrum vor, das beispielsweise die Entgeltabrechnung erledigt, kann dieses ein erster Anlaufpunkt sein. „Der Betrieb der Personalakte im Rechenzentrum befreit den Kunden ganz vom administrativen Aufwand und den Investitionskosten für die Software. Er bezieht diese einfach als Software as a Service (SaaS) aus der Cloud“, weiß Jürgen Göthling, Leiter Betriebsunterstützung DMS bei der BITMARCK Technik GmbH. „Allerdings müssen höchste Sicherheitsanforderungen eingehalten werden, wie es etwa der Betrieb des Rechenzentrums nach den Bestimmungen des Sozialgesetzbuches (SGB) gewährleistet.“

Dreiviertel der Anwender von Cloud-Computing-Lösungen haben damit gemäß einer aktuellen Marktstudie des Netzwerk- und IT-Dienstleisters BT Germany bereits positive Erfahrungen gemacht. Allerdings zeigt die Studie auch, dass bislang nur wenige Befragte befürworten, Human-Resources-Anwendungen auszulagern. Die Idee, dass sensible Daten außerhalb der eigenen Geschäftsräume abgelegt sind, sorgt offenbar bei so manchem Verantwortlichen für Stirnrunzeln. Tatsächlich sind vertrauliche Daten in der Cloud aber genauso sicher wie im

Unternehmen, wenn einige wichtige Grundregeln beachtet werden.

So muss das Rechenzentrum in der EU, im besten Fall sogar in Deutschland sitzen, um sicherzustellen, dass die strengen Richtlinien aus dem deutschen Bundesdatenschutzgesetz auch dort greifen. Vorsicht ist dagegen bei Niederlassungen von US-Unternehmen geboten. Das amerikanische Antiterrorgesetz Patriot Act verpflichtet nämlich alle Firmen, die ihren Hauptsitz in den Vereinigten Staaten haben, zur Zusammenarbeit mit den dortigen Ermittlungsbehörden und gegebenenfalls auch zur Herausgabe vertraulicher Personaldaten.

Erfolgsfaktoren: Sicherheit und Geschäftsprozesse

Größtmögliche Sicherheit vor Datenpannen versprechen die Bestimmungen des Sicherheitszertifikats ISO 27001 oder der Katalog „IT-Grundschutz“ des Bundesamtes für Datensicherheit in der Informationstechnologie (BSI), der auch weitere Faktoren wie den Schutz vor Diebstahl und unbefugtem Zugang zu den Servern mit einschließt. Seriöse Betreiber garantieren in einem Vertrag zur Auftragsdatenverarbeitung deren Einhaltung und bieten dem Kunden auch in der Praxis die erforderliche Transparenz, was mit seinen Daten geschieht. Für zusätzliches Vertrauen können Prüfungen durch eine unabhängige Stelle, beispielsweise die Zertifizierung als „Secure Data Center“ durch den TÜV, oder regelmäßige Datenschutz-Audits sorgen, wie sie oft im Auftrag großer Kunden durchgeführt werden.

Aber auch der Kunde selbst kann dazu beitragen, die Sicherheit weiter zu erhöhen. So lässt sich etwa bei der Einrichtung der Server festlegen, über welche IP-Adressen oder zu welcher Tageszeit der Zugriff für die unterschiedlichen Personenkreise überhaupt zugelassen wird. Konsequenterweise eingesetzt, geben solche technischen Maßnahmen zusätzliche Sicherheit, dass die vertraulichen Daten nur im vorgesehenen Rahmen genutzt werden.

„Entscheidend ist, dass der Betreiber der Lösung ein gutes Verständnis der Geschäftsprozesse beim Kunden hat“, erläutert Dr. Detlev Noll, Vice President Service Management BUC bei MATERNA. „Nur dann kann er seine Betriebsprozesse so danach ausrichten, dass aus dem reinen Hosting echte Managed Services werden.“ Nach seiner Erfahrung gelingt das umso besser, je enger die Partnerschaft zwischen Betreiber und Hersteller der Lösung ist. „Auf die Empfehlung seines Softwareanbieters zu vertrauen, ist daher nie verkehrt“, lautet sein Rat.

Die Lösung macht den Unterschied

Wer genau hinschaut und sich ausführlich beraten lässt, kann sich bei der Entscheidung über das Betriebsmodell also voll und ganz auf die organisatorischen, technischen und finanziellen Unterschiede konzentrieren. Eine Software für die digitale Personalakte lässt sich in beiden Fällen erfolgreich und verantwortungsvoll einsetzen. So oder so sorgt die Einführung einer solchen Lösung für effiziente Abläufe und mehr Zeit für strate-

Sicherheits-Checkliste

Digitale Personalakte:

- Verschlüsselte Datenübertragung
- Revisions sichere Archivierung, idealerweise TÜV-geprüft
- Granulare Verwaltung von Zugriffsrechten
- Bearbeitungs- und Zugriffshistorie für jedes Dokument

Rechenzentrum:

- Sitz in der EU, idealerweise in Deutschland
- Keine Niederlassung von US-Unternehmen
- Vertrag zur Auftragsdatenverarbeitung, der die Maßnahmen nach § 9 Bundesdatenschutzgesetz garantiert
- Sicherheitsmaßnahmen orientiert an ISO 27001 oder BSI-Katalog
- Regelmäßige Datenschutz-Audits (gern im Auftrag anderer Kunden)
- Enge Zusammenarbeit mit dem Softwareanbieter

Kunde:

- Angebotene Sicherheitsmechanismen konsequent nutzen

gische Aufgaben in der Personalabteilung – und nicht zuletzt für viel Platz in den Aktenschränken.



Autor:

FRANK RÜTTGER, Leiter des Geschäftsfelds IQAkten, IQDoQ GmbH