Foto: Voßbein

Foto: Hoffmann

Autor
**Jörn Voßbein**
Geschäftsführer
und Seniorberater,
UIMC Dr. Voßbein
GmbH & Co. KG

consultants@uimc.at

Autor
**Tim Hoffmann**
Geschäftsstellenleiter und
Datenschutzbeauftragter,
UIMC.austria

thoffmann@uimc.at

# IT im Personalbereich: Was der Datenschutz fordert

Personalarbeit wird heutzutage in all ihren Phasen maßgeblich technisch unterstützt. Doch wenn Sie personenbezogene Daten verarbeiten, müssen Sie auch datenschutzrechtliche Aspekte beachten.

Es existieren Softwareprodukte zur Bewerberauswahl, zur Personalverwaltung, zur Zeiterfassung, zur Personalentwicklung bis hin zu vollintegrierten Systemen inklusive elektronischer Personalakte. Deshalb sind in den Personalabteilungen viele Fragen zu klären – angefangen von „Dürfen diese Daten überhaupt erfasst werden?" über „Wer darf auf die Informationen zugreifen?" oder „Welche Datensicherheitsmaßnahmen sind zu ergreifen?" bis hin zu „Was geschieht mit den Daten, wenn der Mitarbeiter ausscheidet?".

Bei einer Grobeinteilung der Personaladministration in die Teilprozesse Bewerbungsverfahren, Personalverwaltung und Personalaustritt unterscheiden wir im Hinblick auf die entsprechenden Datenschutzkernaspekte deutliche Schwerpunkte, wie Abbildung 1 zeigt. Beim Teilprozess Bewerbung beispielsweise sind die Anforderungen des Datenschutzes im Bereich Datensicherheit sehr hoch, in der Protokollierung aber niedrig.

| Datenschutz-anforderungen | Teilprozess Bewerbung | Teilprozess Verwaltung | Teilprozess Austritt |
|---|---|---|---|
| **Zulässigkeit der Datenerhebung** | hoch | hoch | niedrig |
| **Sicherstellung der Datensicherheit** | hoch | hoch | niedrig |
| **Protokollierung & Transparenz** | niedrig | hoch | niedrig |
| **Daten-Löschung** | mittel | mittel | hoch |

*Abbildung 1:*
*Bedeutung der Datenschutzanforderungen in Teilprozessen der Personaladministration*

## Teilprozess Bewerbungsverfahren

Bei einem Bewerbungsverfahren mittels teilautomatisiertem Workflow gehen heutzutage viele Bewerbungen per E-Mail ein; zum Teil fördern die Personalabteilungen dies auch gezielt. Im weiteren Verlauf des Prozesses verteilen diese dann, meist mittels eines simplen elektronischen Workflows, die Unterlagen intern – in der Regel – an jene Mitarbeiter per Mail, die an der Personalauswahl beteiligt sind (zum Beispiel Personalbereich und Leiter der Personal einstellenden Abteilung). Da aber E-Mails ohne besondere Schutzmaßnahmen als unsicher zu betrachten sind, da sie „mitgelesen", fehladressiert oder unberechtigt weitergeleitet werden können, ist stets zu empfehlen, dem Bewerber beide Wege der Bewerbung zu ermöglichen (E-Mail oder Postweg), um ihm so selbst die Entscheidung zu überlassen.

Immer beliebter werden integrierte Softwarelösungen für Bewerbungsprozesse zum Beispiel in Form von (firmeneigenen) Online-Plattformen. Hierbei fragen die Unternehmen in der Regel fest vorgegebene Daten ab und geben dem Bewerber die Möglichkeit, Foto, Anschreiben und Le-

benslauf als Datei hochzuladen. Die Online-Plattform sollte verschlüsselt sein, was als eine Verbesserung der Sicherheit gegenüber der E-Mail anzusehen ist. Die abgefragten Datenfelder sind so zu gestalten, dass die Personalisten nur Daten erfragen, die im konkreten Fall der Stellenausschreibung für eine fundierte Personalentscheidung erforderlich sind. Die Kennzeichnung als freiwillig ist in der Regel problematisch, weil sich der Bewerber gegebenenfalls genötigt fühlt, Daten preiszugeben, um seine „Bewerbungschancen" nicht zu gefährden. Ferner ist eine Recherche im Internet oder in sozialen Netzwerken nur in Ausnahmefällen zulässig. Dies sollten Sie zuvor im Einzelfall rechtlich prüfen lassen.

Bei ausschließlich elektronischen Bewerbungsunterlagen sind die Daten nach Ablauf des Bewerbungsverfahrens sicher zu löschen. Innerhalb des beschriebenen automatisierten Bewerbungsverfahrens kann eine integrierte Softwarelösung eine solche Datenlöschung zum Teil auch teilautomatisiert umsetzen. Natürlich sollten Sie hierbei entsprechende Klagefristen – beispielsweise gemäß den Antidiskriminierungsgesetzen – berücksichtigen.

Bei einem E-Mail-basierten Workflow ist das Löschen oftmals nicht trivial: E-Mails befinden sich nicht nur sowohl im Ein- und Ausgangsordner des E-Mail-Programms, sondern werden oftmals noch lokal oder in einem persönlichen Verzeichnis gespeichert. Somit liegt eine „Bewerbungsmappe" vielfach vor. Empfehlenswert ist in diesem Kontext, die Daten zentral abzuspeichern, das Verzeichnis mit entsprechenden Zugriffsrechten zu versehen und den Beteiligten nur den Speicherort per Mail mitzuteilen.

## Teilprozess Personalverwaltung

Im Rahmen der Personalverwaltung sind die Personalunterlagen und -daten sicher zu verwahren. Hierzu sind Schränke zu verschließen, Arbeitsplätze aufzuräumen und PCs zu sperren. Ferner haben Sie Personalakten regelmäßig zu „bereinigen", indem Sie jene Unterlagen/Dokumente entnehmen und (sicher) vernichten, deren Aufbewahrung nicht mehr erforderlich ist.

Viele Softwareprogramme zur Personalverwaltung bieten mittlerweile auch die Möglichkeit, eine elektronische Personalakte zu integrieren. So sind die wichtigen Unterlagen der Personalakte über das Programm

abrufbar und zielgruppenorientiert auch dezentral zur Verfügung zu stellen, wie zum Beispiel dem Vorgesetzten oder dem Mitarbeiter selbst. Hierbei ist auf eine gewissenhafte und restriktive Zugriffsberechtigungsvergabe zu achten, eine Unterscheidung zwischen Lese-, Schreib- und Änderungsrechten vorzunehmen und möglichst der Download zu unterbinden. Ferner sollten Sie veranlassen, eine Protokollierung jeglicher Änderungen vorzunehmen; unter Umständen ist auch die Protokollierung von Lesevorgängen sinnvoll.

Im Rahmen der Personalentwicklung speichern Unternehmen weitere Daten über die Mitarbeiter, die über die bloße Abwicklung des Arbeitsverhältnisses hinausgehen. So verarbeiten sie Informationen über die Qualifikationen, aber zum Teil auch weitere Informationen im Rahmen von Zielvereinbarungsgesprächen. Neben einer gegenüber dem Mitarbeiter transparenten Verarbeitung sollten Sie auch auf ein sehr restriktives Zugriffsrechtemodell achten und Regeln für den Umgang mit besonders vertraulichen Informationen aufstellen, beispielsweise wenn es um private oder finanzielle Probleme geht.

## Teilprozess Mitarbeiteraustritt

Bei Austritt eines Mitarbeiters aus dem Unternehmen informieren Sie die erforderlichen Stellen schnellstmöglich (IT-Abteilung und gegebenenfalls Werksschutz/Portier zur Sperrung der entsprechenden Rechte). Des Weiteren sind jene Daten und Unterlagen nach dem Austritt zu vernichten beziehungsweise zu löschen, die Sie nach Ablauf des Beschäftigungsverhältnisses nicht mehr benötigen. Daten, die Ihr Unternehmen aus steuerlichen Gründen noch aufbewahren muss, sollten Sie technisch sperren lassen.

Viele Unternehmen sind mittlerweile Teil eines Unternehmens- oder Konzernverbunds. So übertragen die Unternehmen im Rahmen von sogenannten Shared Services beispielsweise die Personalverwaltung/-abrechnung oder den IT-Support an die Muttergesellschaft. Hierbei handelt es sich um den gleichen Sachverhalt wie bei einer Auslagerung an einen Externen („Erbringung von Dienstleistungen" gemäß § 10 f. DSG) und es ist keine rechtliche Privilegierung von Konzernunternehmen möglich.

Ferner setzen Unternehmensgruppen Mitarbeiter oftmals unternehmensübergreifend ein, um ihre Kenntnisse und Fähigkeiten (Skills)

gewinnbringend für die gesamte Gruppe zu nutzen. Dabei teilen sie Personalinformationen konzernweit, was datensparsam geschehen sollte. Rechtlich liegt eine Datenübermittlung vor, bei der verschiedene formale und arbeits-, aber eben auch datenschutzrechtliche Anforderungen zu beachten sind. Sobald die Konzerngesellschaften außerhalb der EU beheimatet sind, ist die Hürde noch höher. Unter Umständen sind auch die besonderen Anforderungen zu einem Informationsverbundsystem gemäß § 50 DSG 2000 zu beachten. Ein Informationsverbundsystem ist nach § 18 Absatz 2 DSG 2000 vorabkontrollpflichtig.

## Anforderungen an die IT-Anwendungen

Im Rahmen der Softwareauswahl sollten die Personalabteilungen zunächst ein Pflichtenheft erstellen, in das auch die datenschutzrechtlichen Anforderungen einfließen. Hierzu kann die Checkliste auf Seite 35 als Anregung dienen. Darüber hinaus sollten Sie Maßnahmen treffen, um die Informationssicherheit zu gewährleisten. Neben Anforderungen, welche die Software bereits abbilden sollte, sind weitere Maßnahmen der Infrastruktur (wie zum Beispiel Datensicherungen, Update-/Patch-Management oder Virenscanner und Firewalls) und organisatorische Regelungen erforderlich (zum Beispiel Pflicht der PC-Sperrung, Passwortrichtlinie oder Rechtevergabe-Workflow). Die Datensicherheitsmaßnahmen unterliegen dem technischen Fortschritt und sind kontinuierlich anzupassen.

Sehr oft übernehmen externe Dienstleister Aufgaben bei der Einführung oder der späteren Wartung und Fehlerbehebung. Dabei ist die rechtmäßige und sichere Datenverwendung besonders sicherzustellen. Hierzu sollten die Auftraggeber zwingend einen Vertrag abschließen. Auch sollten Sie entsprechende Informationen vom Dienstleister einholen, um dessen Arbeit überprüfen zu können. Halten Sie schriftlich fest, dass Subdienstleister nur mit Billigung des Auftraggebers herangezogen werden dürfen. Hierzu hat der Dienstleister Sie so rechtzeitig zu informieren, dass Sie dies gegebenenfalls untersagen können. Sofern der (Sub-)Dienstleister außerhalb der EU/EWR sitzt, müssen Unternehmen die Standardvertragsklauseln der EU-Kommission nutzen sowie die Genehmigung der Datenschutzkommission einzuholen.

Vor Aufnahme einer Datenanwendung hat grundsätzlich eine Meldung im Datenverarbeitungsregister stattzufinden. Eine Meldepflicht besteht

nicht, wenn die eingesetzte Software einer sogenannten Standardanwendung entspricht. Hierzu gehört unter anderem die Personalverwaltung, wobei Sie aber stets im Einzelfall prüfen sollten, ob eine Meldung aufgrund einer Abweichung vom Standard dennoch erforderlich ist.

## Fazit

In allen Phasen der Personaladministration spielen heute zunehmend integrierte Softwaresysteme eine immer größere Rolle. Doch diese Technisierung macht die Anforderungen an den Datenschutz sowohl auf der technischen als auch auf der organisatorischen Seite erheblich komplexer. Deshalb ist es besonders wichtig, in einem frühen Stadium die Datenschutzaspekte in die Überlegungen zur Softwareauswahl und -implementierung einzubeziehen. Sinnvoll ist es, wenn hierfür ein kompetenter Ansprechpartner im Unternehmen zur Verfügung steht, der die Datenschutzaspekte sowohl von der juristischen als auch von der informationstechnischen Seite zu beleuchten in der Lage ist. Als praktikabel hat es sich hier gezeigt, für diese Rolle die Position des Datenschutzbeauftragten zu nutzen.

### Checkliste

**Datenschutz-Anforderungen**

- Umsetzung eines dedizierten Berechtigungskonzepts
- Anpassung der Datenmasken und Passwortregeln/-konventionen
- Verschlüsselte Datenübermittlung/-speicherung
- Möglichkeiten zur Anonymisierung/Pseudonymisierung
- Datensicherung/Back-up
- Sicherstellung von regelmäßigen (Sicherheits-)Updates/Patches
- Protokollierung von Veränderungen und Zugriffen
- Möglichkeiten zur Löschung und Sperrung von Daten
- Bei Wartung durch Dienstleister: Abschluss eines Datenschutzvertrags und Auditierung

*Abbildung 2: Datenschutz-Anforderungen an Personalsoftware*