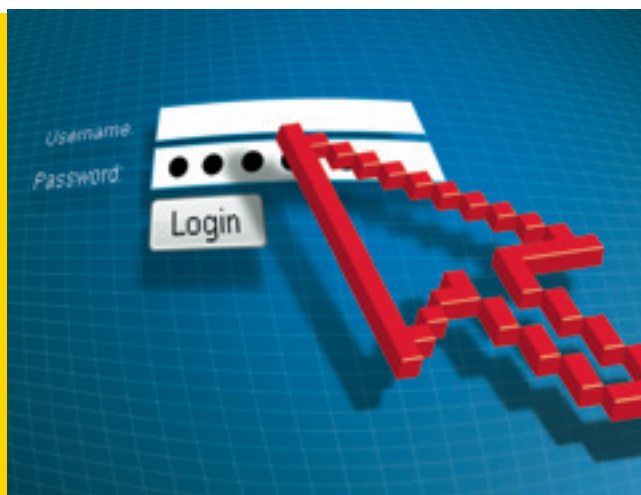


IT ist nicht genug

Wie mit Bewerberdaten zu verfahren ist, schreibt das Bundesdatenschutzgesetz unmissverständlich vor. Doch manche Firma scheint es dabei nicht so genau zu nehmen.



Der Student traute seinen Augen nicht: Bloß weil er sich bei der Eingabe der im Inserat angegebenen Bewerbungskennziffer vertippte, konnte er plötzlich auf seinem Bildschirm wichtige Informationen anderer Bewerber abrufen: Telefonnummern, E-Mail-Adressen und Anschriften, sogar genaue Auskünfte zu bisherigen Arbeitgebern aller Bewerber, die mit der Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur (Unesco) zwischen 2006 und 2011 in Kontakt getreten waren. Klar wurde das klaffende Datenleck inzwischen geschlossen. Aber nicht etwa, weil die UN-Behörde postwendend auf den Hinweis des irritierten Bewerbers reagiert hätte. Nein, erst musste ein Nachrichtenmagazin den Missstand aufgreifen, um die Verantwortlichen aus ihrem Dämmer Schlaf zu reißen. Wer glaubt, dies sei ein Einzelfall, irrt gewaltig. Schluderei in der Datensicherheit und Datenmissbrauch im HR-Umfeld ist häufiger anzutreffen als es Personaler und Bewerber für möglich halten.

Aufrüttelnde Missstände

Was der Hamburger Softwareexperte Josef Kemedner in manchen Betrieben in Erfahrung bringt, sollte jeden Personaler eigentlich aufrütteln. Da ist zunächst der Datenmissbrauch: „Informationen über Bewerber oder Kollegen werden weiterge-

geben und verkauft, teilweise sogar von eigenen Mitarbeitern.“ Aber auch mit der gebotenen Sorgfalt, die der Gesetzgeber zum Schutz von Bewerberdaten an den Tag zu legen vorschreibt, nimmt man es hier und dort Kemedner zufolge nicht so genau. „Hat man erst einmal die Daten erhalten, werden sie oft ausgedruckt oder kopiert, auf irgendeinem Stapel abgelegt und nicht selten vergessen.“ Der Umgang mit herkömmlich auf Papier sowie digital eingereichten Bewerbungen ist äußerst lax, wie Personaler gegenüber dem Marketingleiter der Recall GmbH offen zugeben.

Das Bundesdatenschutzgesetz (BDSG) schreibt vor, mit Daten von Bewerbern vertraulich umzugehen und sie vor dem Zugriff Dritter geschützt unter Verschluss zu halten. Vorbildlich gehen Personaler vor, wenn Datenschutzbeauftragte und Betriebsrat im Sinne des Gesetzgebers das weitere Vorgehen aushandeln und ihren Kollegen bei der praktischen Ausführung zur Seite stehen, wie Ansgar Kinkel, Leiter Personalmarketing und Recruiting der Cirquent GmbH in Frankfurt, erläutert: „Das reicht vom Bildschirmenschutz mit Passwort bis zur Frage, wie wichtige Unterlagen wegzuschließen sind, sobald sie ausgedruckt wurden.“

Wie wichtig es ist, Mitarbeiter anzuleiten, sensibel mit Bewerberdaten umzugehen, weiß auch die Deutsche Telekom,

die regelmäßig Datenschutzschulungen für alle Mitarbeiter des Recruiting & Talent Service durchführt. Rund 40 Mitarbeiter, die in Personalauswahl und Diagnostik tätig sind, sind zusätzlich nach DIN 33430 zertifiziert. Ausführlich wird in dieser Norm beschrieben, wie personenbezogene Daten zu behandeln sind. „Eine technisch realisierte Sicherheit“, so Frank Staffler, Leiter Recruiting & Talent Service Operations im Shared Service Center in Leinfelden-Echterdingen, könne grundsätzlich immer durch Fehlverhalten unterlaufen werden, „indem zum Beispiel Bewerbungsunterlagen ausgedruckt und offen liegengelassen werden.“

Schwachstellen im Prozess

Solche Schwachstellen im Prozess sind auch der Allianz ein Dorn im Auge. Deshalb müssen sich alle Beteiligten strikt an die Vorgaben beim E-Recruiting halten. Bewerben kann man sich beim Versicherungsmulti nur noch online. „Ein großer Vorteil ist dabei von vornherein“, so HR-Sprecherin Sabine Kluge, dass die Unterlagen „nicht mehr physisch anwesend sind, nicht ausgedruckt werden müssen und der Zugriff durch die technische Legitimationsvergabe eindeutig geregelt und damit stark beschränkt ist“. Ganz genau nimmt es die BMW-Tochter Cirquent. Jeder am Bewerbungsprozess Beteiligte, ob Praktikant oder Manager, muss laut

„ Viele Personaler wöhnen sich in Sicherheit, weil sie Datenschutz und Prozessoptimierung einem technischen System überantworten.

Kinkel eine Vertraulichkeitserklärung unterschreiben, „damit das, was technisch nicht abgedeckt wird, organisatorisch geregelt ist.“

Hundertprozentige Sicherheit gibt es freilich nirgends. Juristen zählen das zum „normalen Lebensrisiko“. Gut beraten sind Personaler daher, Risiken durch Einsatz von IT auf ein möglichst geringes Maß zu reduzieren. Je größer ein Unternehmen, zitiert Tobias Neufeld, Fachanwalt für Arbeitsrecht bei Allen & Overy in Düsseldorf, eine Daumenregel, desto professioneller würden auch solche Softwareprogramme eingesetzt. „Die Anforderungen von HR, Datenschutz und Compliance werden zuvor abgeklopft und in die IT übertragen. Freilich können immer mal wieder technische Probleme entstehen.“

Ein technisches Konzept, das verspricht, Widrigkeiten und Risiken zu beherrschen, sind sogenannte „virtuelle Datenräume“. Hinein kommt allein, wer als zulässig identifiziert wird. Sobald sich eine Bewerbung im virtuellen Datenraum befindet, können beteiligte Personen, deren Zugriffsrecht zuvor definiert worden ist, in jeder Bearbeitungsphase auf das Dokument zugreifen. Die Zuordnung, erklärt Thomas Drechsel, Leiter Professional Services bei der Münchner Firma Brainloop, die virtuelle Datenräume zum Schutz von Bewerbungen anbietet, könne etwa durch die Abbildung der Organisationsstruktur des Unternehmens erfolgen. Der Zugriff auf die Bewerbung erfolge schließlich „durch ein zweistufiges Autorisierungsverfahren mit Passwort sowie einer SMS-PIN“.

Automatisch generierte Nachrichten zur Beschleunigung

Um den Bearbeitungsprozess zu beschleunigen, werden daran beteiligte Personen durch automatisch generierte Benach-

richtigungen aufgefordert, die jeweils erforderlichen Schritte einzuleiten. Laut Drechsel führt eine deutlich verringerte Bearbeitungszeit dazu, Prozesse effizienter zu gestalten, „während Reaktionszeiten im Bewerbungsprozess sinken“. Im Idealfall erhält ein Bewerber eine E-Mail, die etwa so lauten könnte: „Ihre Bewerbung ist eingegangen, wir brauchen noch ein bisschen Zeit, ehe wir uns wieder melden.“

Solche Nachrichten erhalten Bewerber laut Neufeld, weil die Personalabteilung vor allem daran interessiert ist, den Bewerbungsprozess möglichst effektiv abzuwickeln, weniger aber, „weil das Unternehmen datenschutzrechtlich sicher handeln will“. Das bestätigt Drechsel. Seiner Erfahrung nach sei der überwiegende Teil von Anwendern an einer Lösung interessiert, die Prozesse optimiert und vor allem beschleunigt. „Erst auf den zweiten Blick kommt das Thema Sicherheit ins Spiel.“ Daraus macht Allianz-Sprecherin Kluge keinen Hehl. Der Vorteil des zentralen E-Recruitings liege in der Tat in einem schnelleren Bewerbungsprozess. Das sei auch erforderlich, „um den heutigen Ansprüchen von Bewerbern nach unkomplizierter und rascher Bewerbung nachkommen zu können“.

Beide Themen, Sicherheit und effiziente Prozesse, gehören untrennbar zusammen. Drechsel: „Sonst geraten schützenswerte Dokumente womöglich in falsche Hände oder ihr Bearbeitungsstatus ist nicht mehr hinreichend nachvollziehbar.“

Viele Personaler wöhnen sich in Sicherheit, weil sie Datenschutz und Prozessoptimierung einem technischen System überantworten. Alle Bewerbungen, die etwa beim Tüv Süd eingehen, laufen Personalleiter Frank Maaß zufolge über ein elektronisches Bewerbungssystem, das mit der Standardsoftware von SAP verkoppelt und auf Datenschutzbestimmun-

gen geprüft und zertifiziert worden ist. Auch beim Autobauer Audi werden Bewerberdaten in einem E-Recruiting-Tool, so HR-Sprecher Armin Zimny, „entsprechend der allgemeingültigen datenschutzrechtlichen Bestimmungen gepflegt“.

Schlupflöcher und Gefahren

Doch ebenso wenig, wie sich auf diese Weise alle Schlupflöcher und Gefahren ausschalten lassen, trägt der Einsatz von hierfür geeigneten Programmen noch nicht zu einem Verfahren bei, das auch tatsächlich im Interesse der Bewerber ist. Konkret vernachlässigen Personaler laut Kemedler, Bewerber über den Status quo ihres Stellengesuchs zu unterrichten. „Nicht immer werden Bewerber informiert, wozu Personaler verpflichtet sind.“ Ob die Unterlagen empfangen und weitergeleitet worden sind oder ob der Bewerber in die Vorauswahl kommt oder nicht, werde dem Bewerber ebenso verschwiegen wie der zeitnahe Hinweis über die gesetzlich vorgeschriebene Löschung von Daten zum Abschluss des Bewerbungslaufs.

Das bestätigt Peter Meier, stellvertretender Leiter des Bayerischen Landesamtes für Datenschutzaufsicht in Ansbach. „Viele Anrufer beschwerten sich bei uns, weil sie auf die Bitte nach Löschung ihrer Unterlagen von den Unternehmen keine Antwort bekommen.“ Aber auch in anderer Hinsicht gibt es Klagen zuhauf. Meier weist darauf hin, dass inzwischen viele Firmen wegen des gestiegenen Einstellungsdrucks dazu übergehen, Dienstleister in den Bewerbungsprozess einzuschalten. Das habe Konsequenzen: „Bewerber sollten erfahren, dass ihre Daten auch an Externe gehen, und um Einverständnis gebeten werden.“ Diese Informationspflicht wird Personälern vom Gesetzgeber auferlegt. Die Frage ist nur, ob diese Maßgabe auch für jene Informationen gilt, die über Kandidaten gesammelt werden, die noch nicht den Status eines Bewerbers haben. Viele Unternehmen ziehen derlei Daten aus allen denkbaren Kanälen zusammen, um

„Viele Firmen gehen inzwischen dazu über, Dienstleister einzuschalten.“

solche „Reserven“ aufzubauen. Die Allianz etwa verzeichnet in ihrem externen „Talent Pool“ weltweit rund 150 000 Kandidaten. Erste Kontakte auf Karriere- und Hausmessen, Empfehlungen, aber auch Informationen über Kandidaten, die sich bereits einem Bewerbungsprozess unterzogen haben, ohne zum Zuge gekommen zu sein, fließen hier ein. De facto handelt es sich meist nicht um Bewerberdaten. Für den Umgang mit solchen Informationen wählen Unternehmen verschiedene Ansätze. Daten, die zum Beispiel Cirquent über Talente erhebt, mit denen das Unternehmen in beidseitigem Interesse Kontakte unterhält, werden Recruitingchef Kinkel zufolge wie herkömmliche Bewerberdaten ebenfalls im Bewerbermanagementsystem gespeichert. „Hier sind sie geschützt und nach wie vor Eigentum des Kandidaten.“ Die Telekom geht einen anderen Weg. Sie ist auf eine App-Entwicklung umgestiegen, die Informationen von Bewerbern oder Interessenten über ein hinterlegtes Datenschutzkonzept aufnimmt. „Auf Basis dieser Daten“, sagt Staffler, „können wir im Anschluss an Veranstaltungen mit Interessenten in Kontakt bleiben und sie bei Bedarf auf offene Stellen vermitteln.“

Daten nicht frei verfügbar

Aus Sicht des Gesetzgebers sind Information über Kandidaten ohne Bewerberstatus nicht frei verfügbar. Die Speicherung von personenbezogenen Daten etwa für den Aufbau einer „Talent Pipeline“, so Rechtsanwalt Neufeld, untersage der Gesetzgeber „nach der Grundmechanik des BDSG mit Erlaubnisvorbehalt“. Für Bewerbungssituationen folge die Erlaubnis aus § 32 BDSG. „Die Erhebung nicht öffentlicher Daten, die zum Beispiel über Auskunftseien oder Dritte bezogen werden können, ist nur in sehr engem Rahmen zulässig.“

Ein weiterer Knackpunkt, der Personälern zu schaffen macht, ist das Allgemeine Gleichbehandlungsgesetz, kurz AGG. Zwischen dem Schutz von Bewerberdaten nach dem BDSG und den Regelungen des AGG ergibt sich durchaus Konfliktpotential. Einerseits dürfen Unternehmen, wie bereits erläutert, Bewerberdaten nach Abschluss des Bewerbungsverfahrens nicht aufbewahren. Sie müssen die Daten löschen. Auf der anderen Seite, erläutert Neufeld, benötige der Arbeitgeber solche Daten eventuell, um sich im Falle einer AGG-Klage eines gescheiterten Bewerbers verteidigen zu können. „Der Gesetzgeber hat diesen Konflikt nicht ausdrücklich aufgelöst.“ Würden Daten aber für einen Rechtsstreit benötigt, ergebe sich eine Interessenabwägung: „Der Arbeitgeber darf die Daten als Beweise oder zur Begründung einer Position so lange aufbewahren, wie ein AGG-Klagerisiko droht.“

Cirquent-Recruiter Kinkel versucht den Konflikt zwischen Bewerberdatenschutz und AGG auf seine Weise zu lösen. Fragen Bewerber nach den Gründen für eine Absage, kann er ihnen oftmals keine Auskunft geben, weil Bewerberdaten gelöscht werden, sobald in der Fachabteilung die Entscheidung abzusagen getroffen wird. Das sei zwar frustrierend für Bewerber. „Umgekehrt bleibt auch der positive Eindruck: Cirquent nimmt Datensicherheit ernst.“

Um die zumeist jungen Bewerber, die aus Feedback lernen wollen, nicht allein zu lassen, schaut sich Kinkel die jeweiligen Bewerbungen, die er sich erneut zusenden lässt, noch einmal an und erteilt den ein oder anderen Ratschlag zur Verbesserung des Dokuments und seiner inhaltlichen Gestaltung. Konkrete Gründe, die zur Absage beitrugen, darf er hingegen nicht benennen. So will es das Gesetz.

Winfried Gertz, freier Journalist, München