



UIMC: Elektronische Bewerbungsverfahren - Risiken für die Persönlichkeitsrechte oder Chancen für den Datenschutz?

Elektronische Bewerbungsverfahren - Risiken für die Persönlichkeitsrechte oder Chancen für den Datenschutz?
Die Personalarbeit wird heutzutage maßgeblich technisch unterstützt. So werden auch zunehmend Softwareprodukte zur Bewerber-Verwaltung und -Auswahl eingesetzt. Hierbei sind natürlich auch datenschutzrechtliche Aspekte zu beachten. So sind Fragen wie "Dürfen diese Daten überhaupt erfasst werden?" über "Wer darf auf die Informationen zugreifen?" oder "Welche Sicherheitsmaßnahmen sind zu ergreifen?" zu klären. Viele Bewerbungen gehen heutzutage per E-Mail ein; zum Teil wird dies auch gezielt gefördert. Im weiteren Verlauf des Prozesses wird dann ein simpler elektronischer Workflow eingeführt, in dem die Unterlagen intern an jene Mitarbeiter per Mail weiter verteilt werden, die an der Personalauswahl beteiligt sind (z. B. Leiter der personaleinstellenden Abteilung). Da aber E-Mails ohne besondere Schutzmaßnahmen als unsicher zu betrachten sind - schließlich können sie "mitgelesen", fehladressiert oder unberechtigt weitergeleitet werden " ist stets zu empfehlen, dem Bewerber beide Wege der Bewerbung zu ermöglichen (E-Mail oder Postweg), um ihm so selbst die Entscheidung zu überlassen. Am Ende des Bewerbungsverfahrens sind diese Daten sicher zu löschen. Bei einem E-Mail-basierten Workflow ist dies oftmals nicht trivial: E-Mails befinden sich nicht nur im Ein- und Ausgangs-Ordner des E-Mail-Programms, sondern werden oftmals noch lokal oder in einem persönlichen Verzeichnis gespeichert. Dadurch liegt eine "Bewerbungsmappe" mehrfach vor, was datenschutzrechtlich sehr problematisch ist. 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. Immer beliebter werden hingegen auch integrierte Software-Lösungen für Bewerbungsprozesse, z. B. in Form von (firmeneigenen) Online-Plattformen. Hierbei werden online in der Regel fest vorgegebene Daten abgefragt und die Möglichkeit gegeben, Foto, Anschreiben und Lebenslauf als Datei hochzuladen. Die Online-Plattform sollte verschlüsselt werden, was als eine Verbesserung der Sicherheit gegenüber der E-Mail anzusehen ist. Die abgefragten Datenfelder sind so zu gestalten, dass nur Daten erfragt werden, die im konkreten Fall der Stellenausschreibung erforderlich sind. Diese stellenspezifische Individualisierung stellt einen datenschutzrechtlichen Vorteil gegenüber Papierfragebögen dar. Auch können durch temporär vergebene Berechtigungen die Zugriffe auf die Prozessbeteiligten beschränkt und der Datenschutz gestärkt werden. Ferner kann eine Datenlöschung (teil-) automatisiert umgesetzt werden. Natürlich sollten hierbei entsprechende Klagefristen - beispielsweise auf Basis des Antidiskriminierungsgesetzes (AGG) - berücksichtigt werden. Eine Abstimmung mit den betrieblichen Datenschutzbeauftragten ist dringend zu empfehlen, um positive Wirkungen auf die Persönlichkeitsrechte des Bewerbers und somit auf die Datenschutzsituation des Unternehmens zu erreichen. So ist eine Weitergabe der Unterlagen an weitere Konzerngesellschaften nur auf Basis einer Einwilligung möglich, die aber schon bei Einreichung der Bewerbung elektronisch eingeholt werden kann. Die Kennzeichnung von Datenfeldern als freiwillig ist oftmals problematisch, weil sich der Bewerber ggf. genötigt fühlt, Daten preiszugeben, um seine "Bewerbungschancen" nicht zu gefährden. Ferner ist eine Recherche im Internet oder in sozialen Netzwerken nur in Ausnahmefällen zulässig und sollte zuvor im Einzelfall rechtlich geprüft und mit dem Datenschutzbeauftragten abgestimmt werden. Dies zeigt, dass eine vorherige Festlegung erforderlich ist, wie mit den entsprechenden Daten umzugehen ist; idealerweise ist dies in das interne Datenschutzkonzept zu integrieren. Ferner zeigt es, dass insbesondere integrierte elektronische Bewerbungsverfahren auch Chancen für den Datenschutz bieten, sofern sie denn gemeinsam mit dem Datenschutzbeauftragten sinnvoll eingeführt werden.
UIMC Dr. Voßbein GmbH & Co KG
Dr. Jörn Voßbein
Nützenberger Straße 119
42115 Wuppertal
Tel.: (0202) 265 74 - 0
Fax.: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.uimc.de

Pressekontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Firmenkontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Die UIMC DR. VOSSBEIN GmbH & Co KG, gegründet 1997, hat die damals seit über 10 Jahren laufenden Beratungsgeschäfte der Partner und Gesellschafter Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik und Dr. Jörn Voßbein in einer Beratungsgesellschaft vereint. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig den Datenschutz betreut, als dritter Partner zur UIMC gestoßen. Kerngebiete ihrer Arbeit sind die IT-Sicherheit und der Datenschutz. Sie kann beachtliche Referenzen von Institutionen aus einer Vielzahl von Wirtschaftszweigen sowie Behörden aufweisen und hat eine umfangreiche Projekt- und Betreuungserfahrung, auch international. Felder, auf denen ihre Erfahrungen branchenführend sind. Ihr Leistungsspektrum/Produktprogramm unterscheidet sich von dem anderer Beratungsunternehmen: Sie setzt ein toolgestütztes Analyse- und Konzeptionierungssystem mit einer wissensbasierten Expertensystem-Komponente in Form einer Shell ein, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationale und kostengünstige Analyse betriebswirtschaftlicher sowie IT-sicherheits- und datenschutzspezifischer Kern- und Teilgebiete sowie die Berichterstattung und Konzeptionserstellung, womit Rationalisierungs- und Effizienzvorteile für ihre Kunden generiert werden. Im Verlaufe der Zeit wurden eine Vielzahl von individuellen Füllungen für diese Shell erarbeitet und in diese eingebracht. Firmenindividuelle Füllungen sind konzeptionell vorgesehen und auf der Basis der Struktur des Tools komplikationslos zu realisieren. Sie führt Workshops, Schulungen sowie Fortbildungsmaßnahmen auf den Sektoren IT-Sicherheit und Datenschutz mit ihrer Marke UIMCollege auch als Inhouse-Veranstaltungen durch.