

23.03.2011

Gesetzeskonformer Umgang mit digitalen Bewerbungsunterlagen

Produktvorstellung

Mit der HR-Lösung ermöglicht die Brainloop AG Personalabteilungen den gesetzeskonformen Umgang mit digitalen Bewerberunterlagen.

Die Dokumente werden per Link an die Entscheider verteilt und sind durch ein zweistufiges Authentifizierungsverfahren automatisch vor unbefugter Einsicht geschützt. Nach Ablauf des Bewerberprozesses werden alle Kopien nachweisbar gelöscht. Damit schneidet der führende Anbieter von Lösungen für den sicheren Umgang mit vertraulichen Dokumenten seine DCM-Lösungssuite exakt auf die Belange im sorgfältigen Umgang mit personenbezogenen Daten zu.

Nach dem deutschen Gesetz (§ 3 Absatz 1 Bundesdatenschutzgesetz) müssen Bewerberunterlagen als personenbezogene Daten einer natürlichen Person geschützt werden. Nicole Dietrich, Senior Marketing Director, Brainloop AG, erläutert: „Die übliche Praxis, Bewerbungen als unsicheren E-Mail-Anhang zu versenden, verstößt eindeutig gegen die Compliance-Auflagen und scheidet damit als Option aus. Wie schnell ist der falsche Empfänger eingetippt, oder die Dokumente werden gedruckt oder weitergeleitet und werden durch diese Praxis für jedermann einsehbar. Dementsprechend müssen Unternehmen den Umgang mit digitalen Bewerbungsmappen auf eine neue Basis stellen.“ Per E-Mail oder über Portale eingegangene Bewerbungsdokumente müssen vor unbefugter Einsicht geschützt sicher zwischen der Personalabteilung, den Fachabteilungen und Externen wie beispielsweise Personalberater, Anwalt und Steuerberater zirkulieren. Ebenfalls müssen die Firmen nachweisen und sicherstellen, dass die Unterlagen nach Ablauf des Bewerbungsprozesses fristgerecht gelöscht werden und keine Kopien zurückbleiben.



Die HR-Lösung von Brainloop löst diese Herausforderungen. Nach Eingang im Unternehmen werden die digitalen personenbezogenen Unterlagen verschlüsselt, geschützt nur den Personen zur Verfügung gestellt, die berechtigt sind, diese einzusehen. Auf Wunsch erfolgt die Auslieferung auch mit personalisiertem Wasserzeichen oder mit Digital Rights Management-Technologien, die den Dokumenten schon bei der Erzeugung Beschränkungen mit auf den Weg geben. Dadurch kann beispielsweise ein Ausdruck der Unterlagen oder deren Weiterleitung wirksam unterbunden werden. Auf diese Weise wird verhindert, dass Server-Provider, Operator oder unbefugte Kollegen die vertraulichen Bewerbungen einsehen können. Beliebige Dritte, seien es interne Mitarbeiter oder externe Geschäftspartner, können jedoch unmittelbar und ohne jegliche Installation von Software bzw. Training in den sicheren Bewerbungsprozess eingebunden werden. Sie erhalten einen Link per E-Mail, der ihnen den Zugriff auf das vertrauliche Bewerberdokument ermöglicht. Um dieses zu öffnen, müssen sie ein zweistufiges Authentifizierungsverfahren mit Passwort und SMS-PIN durchlaufen. Mit

Hilfe der Protokollfunktion, die den gesamten Lebenszyklus des Dokuments bis hin zur Archivierung oder Löschung dokumentiert, wird am Ende des Bewerbungsprozesses der abschließend geforderte Nachweis der Vernichtung aller Kopien erbracht.

http://www.datakontext.com/index.php?seite=artikel_detail&navigation=346&system_id=175381