Technikeinsatz im Personalbereich ? Chance für den Datenschutz?

Technikeinsatz im Personalbereich - Chance für den Datenschutz?
Personalarbeit findet heute nicht mehr ausschließlich in Papierform statt, sondern wird in vielen Phasen maßgeblich technisch unterstützt: ob bei der Bewerberauswahl, zur Personalverwaltung, zur Zeiterfassung, zur Personalentwicklung bis hin zu vollintegrierten Systemen inkl. elektronischer Personalakte. Darüberhinaus werden viele Aufgaben an Dienstleister weitergereicht; sei es "nur" der Support der entsprechenden IT-Anwendung oder die nahezu vollständige Auslagerung der Personalprozesse. Doch, wo personenbezogene Daten verarbeitet werden, sind auch datenschutzrechtliche Aspekte zu beachten.
Viele Softwareprodukte zur Personalverwaltung bieten mittlerweile auch die Möglichkeit, eine elektronische Personalakte zu integrieren. So sind die wichtigen Unterlagen der Personalakte über das Programm abrufbar und können zielgruppenorientiert auch dezentral zur Verfügung gestellt werden, wie z. B. dem Vorgesetzten oder dem Mitarbeiter selbst. Hierbei ist auf Folgendes zu achten:
 gewissenhafte und restriktive Zugriffsberechtigungsvergabe; Unterscheidung zwischen Lese-, Schreib- und Änderungsrechten; Unterbinden/Restriktion der Downloadmöglichkeiten; Protokollierung jeglicher Änderungen (z. T. ist auch eine Protokollierung von Lesevorgängen sinnvoll).
Im Rahmen der Personalentwicklung werden weitere Daten über die Mitarbeiter gespeichert, die über die bloße Abwicklung des Arbeitsverhältnisses hinausgehen. So werden Informationen über die Qualifikationen, aber z. T. auch weitere Informationen im Rahmen von Zielvereinbarungsgesprächen verarbeitet. Neben einer gegenüber dem Mitarbeiter transparenten Verarbeitung, sollte auch auf ein sehr restriktives Zugriffsrechtemodell geachtet und Regeln aufgestellt werden, wie mit besonders vertraulichen Informationen umgegangen werden sollte (beispielsweise private oder finanzielle Probleme).
Bei Austritt eines Mitarbeiters aus dem Unternehmen sollten die erforderlichen Stellen schnellstmöglich informiert werden (IT-Abteilung und ggf. Werksschutz/Portier zur Sperrung der entsprechenden Rechte). Dies kann durch ein "intelligentes" System automatisiert gesteuert werden. Des Weiteren sind jene Daten und Unterlagen nach dem Austritt zu vernichten bzw. zu löschen, die nun nicht mehr benötigt werden (gesetzliche Aufbewahrungsfristen sind für spezifische Daten natürlich zu beachten).
Eine Löschung bzw. Sperrung von Daten sollte aber nicht nur beim Ausscheiden eines Mitarbeiters durchgeführt werden; vielmehr sollten auch Abmahnungen, Arbeitszeitprotokolle etc. dann gelöscht werden, wenn die Speicherung nicht mehr erforderlich ist. Im Rahmen einer elektronischen Personalakte oder anderer Systeme kann dies automatisiert werden. Dies kann dadurch erreicht werden, dass Daten entweder nach einem zuvor definierten Zeitraum automatisch gelöscht oder zumindest automatisch Hinweise geniert werden, dass eine Löschung geprüft werden sollte. Somit kann eine sinnvoll konfigurierte Software den Datenschutz unterstützen.
Die genannten Beispiele zeigen, dass durch die Technisierung die Anforderungen an den Datenschutz sowohl auf der technischen als auch auf der organisatorischen Seite z. T. erheblich komplexer werden. Deshalb ist es besonders wichtig, die Datenschutzaspekte schon in die Überlegungen zur Softwareauswahl und -implementierung einzubeziehen. Sinnvoll ist es daher, den Datenschutzbeauftragten frühzeitig und in allen Phasen eines solchen Projekts umfassend einzubinden, da die Erfahrung zeigt, dass eine notwendige nachträgliche Änderung zur Sicherstellung der Compliance wesentlich aufwendiger ist.

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: a href=' https://uimc.de/communication. html?pk_campaign=pressrelation' > www.uimc.de </a</p><img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=566656" width="1" height="1">

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 rationelle 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.