06/2014

UIMCommunic@tion

Stets auf dem Laufenden sein?
www.UIMC.de/Communication

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

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 und 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.

Mehr Pressemitteilungen finden Sie hier: www.UIMC.de/communication

Schon gewusst?

Im Rahmen des Beschäftigtenverhältnisses (was das Bewerberverfahren und auch die etwaige Kündigung einschließt) müssen die Aspekte der Antidiskriminierung gemäß Allgemeinen Gleichbehandlungsgesetz (AGG) beachtet werden.

§ 12 AGG verpflichtet jeden Arbeitergeber, die Mitarbeiter im Hinblick auf die Antidiskriminierung zu schulen. Dies kann mittels E-Learning besonders effizient umgesetzt werden.

eCollege.UIMC.de

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

Noch Fragen?
Treten Sie in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Neue Orientierungshilfe der Datenschutz-Aufsichtsbehörden:

Videokameras im Betrieb („OH Video“)

Die Datenschutz-Aufsichtsbehörden haben eine Orientierungshilfe erstellt, anhand dessen zum Teil auch vor Ort geprüft wird. Folgende Aspekte sollten vor der Installation einer Videokamera im Betrieb bzw. in den eigenen Räumlichkeiten u. a. beachtet werden:

1. Vor Verwendung bzw. Installation einer Videokamera sind folgende Aspekte zu definieren:
   - » Grund/Zweck der Installation;
   - » Zugriffsberechtigte
   - » Sofern erforderlich: Speicherdauer bzw. Löschungsfristen
   - » Konkrete Orte sowie Überwachungsbereiche und -zeiträume
2. Eine frühzeitige Einbeziehung des Datenschutzbeauftragten ist vor der Installation erforderlich. Dieser hat eine Abwägung zwischen den betrechtigten Interessen des Unternehmens und der schutzwürdigen Interessen der Beobachteten vorzunehmen.
3. Es sind die Zeiträume der Videoüberwachung festzulegen; u. U. ist eine Aufzeichnung in den Nachtstunden ausreichend.
4. Es ist zu prüfen, ob eine reine Beobachtung (Live-Streaming) ausreichend ist, oder ob es einer (eingriffsintensiveren) Aufzeichnung bedarf.
5. Die rechtlichen Voraussetzungen für die Videoinstallation sollte regelmäßig überprüfen werden. Insbesondere die Frage der Geeignetheit und Erforderlichkeit der Maßnahme ist zu evaluieren.

Auch „Dummys“ (also nicht funktionsfähige Kameras) greifen in die Persönlichkeitsrechte der Betroffenen ein („Kontroll-/Beobachtungsdruck“), so dass auch hierbei der Datenschutz zu beachten ist.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Auszug aus bisher erschienenen Hinweisen/Tipps:
„Sichere Nutzung von E-Mails“ (09/2013)
„Fernwartung durch Dienstleister“ (02/2014)
„Smartphones und Apps“ (05/2014)

Social Media im Unternehmen

Der Einsatz von Facebook, Twitter & Co wird immer beliebter: Bei der Personalsuche und -recherche (E-Recruiting), zur Kundenansprache oder zur Nutzung „viraler Effekte“ im Marketing. Hierbei entstehen aber auch **Risiken** im Hinblick auf den Datenschutz und die Informationssicherheit.
Es ist daher dringend zu empfehlen, vor dem Einsatz innerhalb des Umsetzungskonzepts dieses Aspekte zu berücksichtigen!

Workshop: 23.09.2014

Koordinierte Dienstleister-Audits

Sobald personenbezogene Daten durch einen Dienstleister eingesehen werden können, muss sich der Auftraggeber von der Einhaltung Ordnungsmäßigkeit überzeugen. Die UIMCert kann eine solche Auditierung auch koordinieren, indem weitere Kunden des Dienstleisters angesprochen und von einer gemeinsamen Auditierung überzeugt werden. Dies kann zu umfasssenden Kostenersparnissen führen. Mehr unter

uimcert.de/dienstleisterauditierung

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ Technikeinsatz im Personalbereich – Chance für den Datenschutz?
- ☐ Schulungsanforderungen im Rahmen der Antidiskriminierung (AGG)
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de