09/2014

UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Polizeiliche Führungszeugnisse im Betriebsalltag?

Zunehmend werden Unternehmen von Ihren Auftraggebern dazu aufgefordert, neben entsprechenden Qualifikationsnachweisen der eingesetzten Mitarbeiter auch ein polizeiliches Führungszeugnis nachzuweisen. Dies wirft datenschutzrechtliche Fragen der Zulässigkeit dahingehend auf, ob der Arbeitgeber dazu berechtigt ist, diese Führungszeugnisse einzufordern, und ob er ferner dazu berechtigt ist, diese dann auch weiterzuleiten.

Unabhängig von der Fragestellung einer **Weitergabe des polizeilichen Führungszeugnisses** stellt sich bereits das Problem der Datenerhebung durch den Arbeitgeber selbst. Gemäß § 32 BDSG dürfen „personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung (…) oder für dessen Durchführung oder Beendigung erforderlich ist."

Ein eigener Anspruch des Arbeitgebers auf **Vorlage des Führungszeugnisses** gegen die zuständige Behörde besteht nicht. Ob der Arbeitgeber die Vorlage eines Führungszeugnisses verlangen kann, ist davon abhängig, ob diese Informationen für das Beschäftigungsverhältnis relevant sind. Regelmäßig bedarf es hierzu einer individuellen Betrachtungsweise. Zum Teil ersetzt aber auch die Wertung des Gesetzgebers oder Rechtsprechung der Arbeitsgerichte eine Einzelfallabwägung; Hilfe bietet hierbei in der Regel ein kompetenter Datenschutzbeauftragter.

Das Bundesarbeitsgericht (BAG) bestimmt die Zulässigkeit von Fragen in Verbindung mit dem Beschäftigungsverhältnis durch Abwägung vom dem berechtigten Informationsinteresse des Arbeitgebers einerseits und dem Interesse des Arbeitnehmers am Schutz seines Persönlichkeitsrechtes und an der Unverletzlichkeit seiner Individualsphäre andererseits. Für die Zulässigkeit ist es erforderlich, dass **die konkrete Frage in einem sachlichen und inneren Zusammenhang mit dem Arbeitsplatz steht** und deren Beantwortung für den Arbeitsplatz und die zu verrichtende Tätigkeit selbst von Bedeutung ist. Hinsichtlich des Fragerechts nach Vorstrafen hält das BAG nur solche Fragen für zulässig, die für die Art des zu besetzenden Arbeitsplatzes von Bedeutung sind. So ist z. B. die Frage nach Verkehrsdelikten für eine Kraftfahrertätigkeit zulässig, für eine Sekretariatsstelle hingegen nicht. Ferner gibt es z. T. eine gesetzliche Verpflichtung, wie beispielsweise in Einrichtungen der Kinder- und Jugendhilfe.

Bei Übertragung der Rechtsprechung des BAG auf die Frage, ob der Arbeitgeber die Vorlage eines polizeilichen Führungszeugnisses verlangen kann, gelangt man zu dem Ergebnis, dass dies **grundsätzlich unzulässig** ist. Hierzu haben sich bereits Datenschutz-Aufsichtsbehörden eindeutig geäußert (so z. B. auch Hamburgische Beauftragte für Datenschutz und Informationsfreiheit). Grund hierfür ist, dass in dem polizeilichen Führungszeugnis sämtliche Strafen aufgeführt sind, also auch solche, die zum Arbeitsverhältnis keinen konkreten Bezug aufweisen. Insofern könnte der Arbeitgeber die ihm durch die Rechtsprechung des BAG zum Fragerecht nach Vorstrafen gesetzten Grenzen mittels polizeilicher Führungszeugnisse umgehen.

Auch die **„freiwillige" Vorlage** des polizeilichen Führungszeugnisses ist keine rechtmäßige Alternative, da ein freier Willensentschluss aufgrund der wirtschaftlichen Abhängigkeit des Arbeitnehmers grundsätzlich nicht angenommen werden kann. Ein Arbeitnehmer wird kaum eine entsprechende Bitte verneinen. Hierzu gibt es eine eindeutige Entschließung des sog. „Düsseldorfer Kreises" (Konferenz der Datenschutzbeauftragten des Bundes und der Länder).

Die Vorlage und somit auch die Weitergabe eines polizeilichen Führungszeugnisses der Beschäftigten sind somit datenschutzrechtlich nicht zulässig. **Ausnahmen** bilden hierbei nur zwingende gesetzliche Vorgaben in bestimmten Branchen. Die UIMC empfiehlt in diesem Kontext, eine schriftliche Bestätigung der jeweiligen Mitarbeiter einzuholen und dem Auftraggeber zur Verfügung zu stellen, dass bestimmte, für die Tätigkeit relevante – und idealerweise vom Auftraggeber definierte – Vorstrafen nicht vorliegen.

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

Schon gewusst?

Wenn die **private Nutzung von Firmengeräten** oder die dienstliche Nutzung von **privaten Smartphones** nicht verboten oder anderweitig rechtlich sauber geregelt ist, können Sie große Probleme beim Zugriff auf die dienstlichen E-Mail-Postfächer, auf die Einzelverbindungsnachweise oder grundsätzlich auf die Geräte bekommen. Dies kann bei Krankheit/Urlaub, hohen Telefonrechnungen, Sicherheitsprüfungen oder Geräteverlust zu Schwierigkeiten im Betriebsalltag führen.

Fragen Sie Ihren Datenschutzbeauftragten

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

Basis-Tipps für die Verbesserung der Sicherheit von Serverräumen

Serverräume sind besonders sicherheitsempfindliche Bereiche, die einen spezifischen Schutzbedarf haben. Hierbei kann schon durch pragmatische Maßnahmen die Sicherheit erhöht werden:

1. Server sollten nur in dedizierten Räumen aufgestellt werden (keine Mischnutzung mit Druckern, Lager oder Archiv, bei der auch Nicht-IT-Mitarbeiter Zutritt erhielten).
2. In den Serverräumen sind keine Brandlasten aufzubewahren. Auch sollten keine wasserführenden Rohre oder Risikobereiche angrenzen.
3. Es sind sehr restriktive Schließgruppen zu bilden, so dass nur sehr wenige Schlüssel und diese nur an IT-Mitarbeiter ausgegeben werden.
4. Die Räume sollten nur mit Schlüssel geöffnet werden können (Knauf statt Türklinke).
5. Reinigungskräfte und externes Servicepersonal sollten nur unter Aufsicht den Serverraum betreten dürfen.
6. Bei Verlust von Schlüsseln sind die Schlösser unverzüglich zu tauschen. Alternativ könnne elektronische Schließanlagen aufgrund vereinfachter Zutrittsrechte-Administration erwägt werden.
7. Es ist darauf zu achten, dass Türen und Fenster verschlossen sind, wenn sich niemand in der Sicherheitszone aufhält.
8. Es ist für eine ausreichende Klimatisierung zu sorgen und Vorkehrungen für Stromausfall zu treffen (z. B. mittels USV).

Weitere Empfehlungen erhalten Sie von Ihrem Ansprechpartner in der UIMC oder UIMCert.

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:
„Fernwartung durch einen externen Dienstleister“ (02/2014)
„Datenschutzkonformer Einsatz von Fernwartungs-Tools“ (04/2013)
„Leasing/Miete von Hardware“ (08/2014)

Matrix-Organisation / Internationaler Datentransfer

In vielen Unternehmensverbünden und Konzernen findet tagtäglich ein Transfer von Daten statt, weil die Mitarbeiter in Projektteams arbeiten oder eine Unternehmensgrenzen-übergreifende Aufbau- und Ablauforganisation etabliert wurde.

Diskutieren Sie über die rechtlichen Anforderungen und Lösungsmöglichkeiten in diesem Praxis-Workshop mit einem erfahren Berater der UIMC!

Wuppertal, 15.10.2014

Datenschutz im Gesundheitswesen

Im Rahmen der ambulanten und stationären Krankenversorgung werden besonders sensible Daten erhoben, verarbeitet und genutzt. Die Datenverarbeitung dient nicht nur dem Behandlungsteam als Gedächtnisstütze im Behandlungsprozess, sie wird dem Patienten auch als Nebenpflicht aus dem Behandlungsvertrag geschuldet.

Bilden Sie sich mit unserem UIMCollege-Seminar fort und profitieren Sie von unseren erfahrenen Beratern!

Saarbrücken, 27.11.2014

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

- ☐ Polizeiliche Führungszeugnisse im Betriebsalltag?
- ☐ Regelungsbedarf für die private Nutzung dienstlicher (und dienstliche Nutzung privater) Geräte
- ☐ **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