05/2013

UIMCommunic@tion

Noch Fragen?
Treten Sie in einen Dialog ein!

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Datenschutz gegen Zollvorschriften: Ein Dilemma für Exportunternehmen?

Wie mangelnde Bestimmtheit von Rechtsvorschriften Unternehmen vor Probleme stellt

Im Rahmen der sog. Terrorbekämpfung werden exportierenden Unternehmen diverse Auflagen im Rahmen der Terrorbekämpfung aufgebürdet. Hierbei sind verschiedene „Vereinfachungen" möglich, wie z. B. die Anerkennungen als „zugelassener Wirtschaftsbeteiligter" oder als „bekannter Versender". Unternehmen, die diesen Status erhalten möchten, müssen besondere Anforderungen erfüllen. Als „zugelassener Wirtschaftsbeteiligter" wird beispielsweise die jährliche Durchführung eines Abgleichs der Personaldaten mit den sog. Terrorlisten der Vereinten Nationen verlangt.

Personenbezogene Daten dürfen aber nur dann verarbeitet werden, wenn eine „Rechtsvorschrift dies erlaubt oder anordnet". Dies stellt viele Unternehmen nun vor rechtliche Probleme, da die Voraussetzungen und Anforderungen nicht gesetzlich, sondern vielmehr nur in Dienstvorschriften des BMF bzw. eher unpräzisen EU-Verordnungen geregelt sind. Somit liegt zunächst keine ausreichende rechtliche Legitimierung eines Datenabgleichs vor, so dass dies einen datenschutzrechtlichen Verstoß für die Unternehmen bedeuten könnte. Diejenigen Unternehmen, die sich nicht zertifizieren lassen, werden sich aber auf intensivere Kontrollen durch die Zollverwaltung einstellen müssen, so dass natürlich – trotz datenschutzrechtlicher Bedenken – die Motivation steigt, eine solche Zulassung zu erhalten.

Der Bundesfinanzhof hat nun eine rechtliche Klarstellung herbeigeführt, die die Politik in der Form bislang noch nicht geschafft hatte. So sind berechtigte Interessen des Unternehmens gemäß § 28 Absatz 1 Nr. 2 BDSG erkennbar. Das Verfahren des Abgleichs ist solange unproblematisch, sofern es nicht zu Falschmeldungen kommt. Hierbei können schutzwürdige Interessen des Mitarbeiters überwiegen, so dass der Umgang mit entsprechenden Funden für die Beachtung der Persönlichkeitsrechte entscheidend ist.

Der Abgleich der Mitarbeiterstammdaten Name, Anschrift, Geburtstag und Geburtsort mit den Terrorlisten ist demnach in zulässiger Art und Weise möglich. Weitere Angaben – wie z. B. Lebenslauf oder Straffreiheitserklärung – sind jedoch für die Durchführung der Sicherheitsüberprüfung nicht erforderlich und damit nicht zu überprüfen. Da die Daten beim Arbeitgeber ohnehin vorliegen, sollte der Abgleich aus Gründen der Datensparsamkeit zudem „intern" erfolgen. Die Zollbehörde selbst erhält nur das Ergebnis des Abgleichs und keine personenbezogenen Daten der Mitarbeiter, so dass keine weiteren Datenschutz-Probleme drohen.

Empfehlenswert ist, die Einzelheiten des Verfahrens im Rahmen einer Betriebsvereinbarung zu regeln und sie den Mitarbeitern somit transparent zu machen. In einer Betriebsvereinbarung oder Dienstanweisung sind ferner gemeinsam mit dem Datenschutzbeauftragten verbindliche Verfahren zu definieren, wie mit Übereinstimmungen zwischen Mitarbeiter- und Antiterrorlisten umgegangen werden soll. Denn gerade durch eine Falschmeldung können massive Verletzungen des Persönlichkeitsrechts entstehen, die bis hin zu Schadensersatzforderungen führen können.

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

Neuer Datenschutz in der EU?

Die EU-Kommission plant eine EU-weit gültige Datenschutz-Grundverordnung, die das Datenschutzniveau in der EU auf ein einheitliches Maß zusammenführen soll. Diese soll zum einen die bisher gültige Datenschutz-Richtlinie aus dem Jahre 1995 ablösen und ist zum anderen (anders als bisherige Richtlinie) nicht mehr in nationales Recht umzusetzen, da sie „Eins-zu-Eins" in sämtlichen Mitgliedsländern sofort gelten soll. Zeitpunkt des Inkrafttretens und exakter Inhalt sind noch unbestimmt.

Wir werden Sie umgehend informieren, sobald die Regelungen in Kraft treten.

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

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

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Clean-Desktop-Policy: Umsetzung auch im „kreativen Chaos“ möglich

Als Datenschützer wird man oft mit dem Vorwurf konfrontiert, dass man durch die Einhaltung des Datenschutzes „nicht mehr arbeiten kann“. Dies wird oftmals mit überzogenen Anforderungen begründet.

Am Beispiel der sog. „Clean-Desktop-Policy“ (Richtlinie des aufgeräumten Schreibtisches) möchten wir Ihnen pragmatische Tipps zur Umsetzung geben:

1. **Keine vertraulichen Unterlagen offen herum liegen lassen!** Hierzu kann es auch mal ausreichend sein, die Arbeitspapiere umzudrehen oder zu verdecken. Dies verhindert zwar nicht den gezielten Diebstahl, aber die zufällige Kenntnisnahme. *Besonders vertrauliche* Unterlagen, wie z. B. im Personalbereich, sollten natürlich verschlossen werden.
2. **Das Passwort nicht hinterlegen!** Sofern Kollegen in Ihrer Abwesenheit auf Daten von Ihnen zugreifen müssen, ist dies problemlos durch die (temporäre) Erweiterung dessen Rechte möglich. Fragen/bitten Sie einfach Ihren Vorgesetzten!
3. **Den Arbeitsplatz-PC beim Verlassen sperren!** Das Sperren ist schnell durch Nutzen der Windows- und L-Taste erledigt (ab Windows XP).
4. **Zu vernichtende Unterlagen sind zu „shreddern“!** Hierzu können Sie die Unterlagen zunächst im Büro sammeln und erst zum Feierabend in einer „Datentonne“ oder mittels Shredder entsorgen. Damit sparen Sie sich „Lauferei“!
5. **Die Einsichtnahme auf den Monitor ist zu verhindern.** Dies ist oft schon durch ein leichtes Drehen des Monitors und/oder der Nutzung einer „Sichtschutzfolie“ zu erreichen.

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

Bisher erschienene Hinweise/Tipps:
„Rechtskonforme Nutzung von VNC-Tools“ (04/13)
„Beantwortung telefonischer Auskünfte“ (03/2013)
„Nutzung von sozialen Netzwerken“ (02/2013)
„Sichere Nutzung von Smartphones“ (01/2013)

Risiko Smartphone

Dem Nutzen von modernen Kommunikationsmitteln im Unternehmen stehen automatisch Gefahren gegenüber, denen ausreichend, aber auch pragmatisch begegnet werden sollte.

Diskutieren Sie Risiken und Lösungswege zum Management bzw. zur Organisation der Risiken im Rahmen unseres Praxis-Workshops „Mobile Devices und Bring Your Own Device (BYOD“.

19.06.2013, 13:30 Uhr

Risiko soziale Medien

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!

Sprechen Sie uns an!

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

☐ Datenschutz vs. Zollvorschriften: Umsetzung von Datenschutzanforderungen bei der Erlangung von Zoll-Stati

☐ Neuer Datenschutz in der EU: Was soll sich ändern?

☐ **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