08/2014

UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Embargo- vs. Datenschutzverstoß: Kein Export ohne Gesetzesverstoß?

Durch EU-Verordnungen zur Terrorismusbekämpfung sind alle Unternehmen zu Prüfmaßnahmen verpflichtet, damit verbotene Geschäftskontakte erkannt und verhindert werden können. Ein Verstoß gegen die EG-Antiterrorismusverordnung wird hierbei als Embargoverstoß gemäß Außenwirtschaftsgesetz (AWG) mit der Strafandrohung von mindestens zwei Jahren Freiheitsstrafe bewertet. Ferner droht eine Umsatzabschöpfung. Dem gegenüber stehen Bußgelder aufgrund von Datenschutzverstößen gemäß Bundesdatenschutzgesetz (BDSG). ***Diese widerstreitenden Gesetzesanforderungen sind ein Dilemma für viele deutsche Unternehmen.***

Im Zusammenhang mit dem Verfahren zur Erlangung des AEO-Status [zollrechtlicher Status eines zugelassenen Wirtschaftsbeteiligten („**Authorised Economic Operator**")] ist regelmäßig ein Abgleich der Kunden-, Lieferanten- und Mitarbeiterdaten mit sog. Anti-Terrorlisten vorzunehmen. Hierbei sind dann personenbezogene Daten zu verarbeiten, so dass der Datenschutz zu betrachten ist. Eine personenbezogene Datenverarbeitung ist aber ausschließlich auf Basis einer Rechtsgrundlage zulässig.

Die EU-Verordnungen und das AWG sind laut Datenschutz-Aufsichtsbehörden aber zu unspezifisch, als dass sie als Rechtsgrundlage herangezogen werden können. So sei diesen Normen nicht zu entnehmen, dass dazu ein Datenabgleich mit den Anti-Terrorlisten zwingend erforderlich ist.

Des Weiteren ist eine Datenverarbeitung auch dann zulässig, soweit sie zur Wahrung **berechtigter Interessen des Unternehmens** erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Eine Datenverarbeitung erfolgt dann zur Wahrung berechtigter Interessen, wenn sie zur Erreichung der Geschäftszwecke der verantwortlichen Stelle im weitesten Sinne erforderlich ist. Hierunter fallen auch wirtschaftliche Interessen, die zur Optimierung der satzungsgemäßen Institutionsgegenstands dienen, wie z. B. Verbesserung des Betriebsergebnisses oder Verringerung der Kosten (z. B. Aufwand bei Zollkontrollen). Diese Interessen scheinen demnach vorzuliegen.

Die Datenverarbeitung ist aber dann nicht zulässig, wenn das **schutzwürdige Interesse der Betroffenen** die berechtigten Interessen der verantwortlichen Stelle überwiegt. Nicht nur allgemein, sondern auch in diesem konkreten Fall geben die Datenschutz-Aufsichtsbehörden den schutzwürdigen Interessen ein hohes Gewicht. Dieser Vorrang der schutzwürdigen Interessen der Betroffenen ist in diesem Fall diskutabel. Insbesondere wenn Mitarbeiterdaten hier geprüft werden sollten, kann dies problematisch werden. Gerade dann, wenn sich ein Fund als falsch herausstellt (z. B. Namensgleichheit), können die Persönlichkeitsrechte des Betroffenen massiv beeinträchtigt werden.

Das Verfahren ist solange unproblematisch, wie es nicht zu Meldungen – insbesondere Falschmeldungen – kommt. Denn neben der **Gefahr des „Nicht-Entdeckens" von Personen** (Verstoß gegen das AWG), die auf den besagten Listen stehen, liegt datenschutzrechtlich dann ein Problem vor, wenn Personen z. B. aufgrund einer Namensgleichheit **unberechtigt verdächtigt werden** (möglicher Verstoß gegen das BDSG).

Hierbei ist insbesondere der Umgang mit entsprechenden Funden entscheidend. So sollten zwingend interne Regelungen, Verfahren und Prozesse etabliert werden, wie mit dem Datenabgleich und insbesondere mit „Treffern" umgegangen wird. Ein diskretes Vorgehen mit einer sehr (!) restriktiven Anzahl an Beteiligten sowie eine Verifizierung der Meldung sind daher dringend zu empfehlen. Dies zeigt einmal mehr, dass das Erreichen von Compliance, also die Ordnungsmäßigkeit, nicht nur vielschichtig ist, sondern auch widerstreitende Rechtsnormen beachtet werden. **Somit sollte nicht nur der Export-, sondern auch der Datenschutzbeauftragte einbezogen werden,** um allen rechtlichen Anforderungen im Unternehmen angemessen Rechnung zu tragen.

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

Schon gewusst?

Sofern Daten, die sich auf (vermeintlich) strafbare Handlungen oder Ordnungswidrigkeiten beziehen, **unrechtmäßig** einem Dritten zur Kenntnis gelangt sind, ist dies **unverzüglich** der zuständigen Aufsichtsbehörde sowie den/dem Betroffenen mitzuteilen. Hierbei ist die Art und Weise nicht entscheidend (bewusste Weitergabe, Verlust eines Datenträgers oder fehladressierte E-Mail). **Eine „Nicht-Meldung" ist bußgeldbewährt.** Sofern Sie weitere Fragen zu diesem Thema haben:

Kommen Sie auf uns zu!

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

Leasing von Hardware: Was ist bei Wartung und der Rückgabe zu beachten?

Wenn interne IT-Leistungen nach Außen verlagert werden, d. h. an Dritte vergeben werden, werden durch den Datenschutzbeauftragten stets schriftliche Vereinbarungen eingefordert. Hierüber haben wir bereits im Rahmen der Anforderungen an eine Auftragsdatenverarbeitung informiert.

Beim Leasing von Hardware wird dies aber oftmals vergessen.

Diese Anforderungen gelten in Regel aber auch beim Leasing von Laptops, Druckern, Kopierern und anderen Geräten mit eingebauten Festplatten. Nicht nur, weil der Leasinggeber im Rahmen der Wartung und **bei Rückgabe selbst** auf diese Speicher zugreifen kann, sondern auch (oder insbesondere), weil Leasing-Rückläufer oftmals noch zweitverwertet werden (Leasing oder **Verkauf von Gebrauchtgeräten**), sind Maßnahmen zu ergreifen, so dass keine Unberechtigten auf die Daten zugreifen können. Andernfalls könnten Dritte auf gedruckte Dokumente usw. zugreifen (vielleicht ja auch Ihr Wettbewerber!?).

Hierzu bieten sich folgende Möglichkeiten an, die vertraglich mit dem Leasinggeber vereinbart werden sollten:

1. eigenständiger Ausbau der Speichereinheiten vor der Rückgabe,
2. eigenständige (sichere) Löschung der Speichereinheiten auf dem Gerät und/oder
3. (sichere) Löschung durch den Dienstleister (hierbei liegt eine Auftragsdatenverarbeitung vor, so dass die Vernichtung/Löschung vertraglich definiert werden muss und Kontrollrechte eingeräumt werden sollten).

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:
„Veröffentlichung von Fotos von Veranstaltungen“ (07/2014)
„Tipps für die Nutzung öffentlicher WLAN-/Wifi-Hotspots“ (04/2014)
„Nutzung von sozialen Netzwerken“ (08/2013)

Social Networken?

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 müssen aber auch Aspekte im Hinblick auf den Datenschutz und die Informationssicherheit beachtet werden.
Es ist daher dringend zu empfehlen, vor dem Einsatz innerhalb des Umsetzungskonzepts dieses Aspekte zu berücksichtigen!

Wuppertal, 23.09.2014

ISO 27001:2013

Die ISO-Norm wurde novelliert; Erst- und Re-Zertifizierungen können ab Oktober nur noch gemäß ISO/IEC 27001:2013 durchgeführt werden.

Im Seminar werden Struktur und Inhalt der Norm vermittelt. Auch können Vorgehensweise der Auditierung und normgemäße Zertifizierungsvorbereitung etc. diskutiert werden. Natürlich wird hierbei schon die Novelle berücksichtigt. Auch besteht genügend Zeit, mit dem Referenten zu diskutieren!

Wuppertal, 05.11.2014

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

- ☐ Embargo- vs. Datenschutzverstoß: Kein Export ohne Gesetzesverstoß?
- ☐ Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG)
- ☐ **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