UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Verschuldensunabhängige Haftung beim Mindestlohn führt zu Datenschutzproblemen

In kaum einem Unternehmen werden heutzutage keine externen Leistungen eingekauft. Dies hat meist Kapazitäts-, Kompetenz- oder auch Kostengründe. Doch auch hierbei gelten die Bestimmungen des Mindestlohngesetzes, egal ob IT-Support, Reinigungsdienstleistungen, Beratung oder im Rahmen der Logistik und Auslagerung von Produktionsschritten. Für die Einhaltung auch beim Auftragnehmer haften die Auftraggeber dieser Dienstleistung (verschuldensunabhängig). Dies führte in der jüngeren Vergangenheit zu umfangreichen Abfragen bei den Auftragnehmern, welche teilweise weder erforderlich noch rechtlich angemessen sind. Doch dies geht auch datenschutzkonform, so Dr. Jörn Voßbein.

Für einen Auftraggeber, welcher einen Auftragnehmer mit der Erbringung von Werk- oder Dienstleistungen beauftragt, gilt nach § 14 Satz 1 AEntG (Arbeitnehmerentsendegesetz) auch § 13 MiLoG (Mindestlohngesetz), so dass er dafür haftet, wenn die von ihm beauftragten Unternehmen sowie die von diesen beauftragten Subunternehmen ihren Beschäftigten den gesetzlichen Mindestlohn nicht zahlen sollten (verschuldensunabhängige Haftung des Auftraggebers).

In der jüngeren Vergangenheit, was sicher auch den unpräzisen gesetzlichen Vorgaben geschuldet ist, führte dies – so Dr. Jörn Voßbein, mehrfach bestellter Datenschutzbeauftragter – dazu, dass verschiedene Auftraggeber von ihren Dienstleistern umfangreiche Daten angefordert haben. So wurden Personalunterlagen wie Arbeitsverträge, Lohnnachweise und weitere umfassende Informationen verlangt.

Eine Übermittlung von personenbezogenen Daten ist gemäß § 4 BDSG dann zulässig soweit eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Einwilligung, die freiwillig gegeben werden muss, scheidet in diesem Falle aus. Daher wurden vielfach als „Rechtsvorschrift“ pauschal die Regelungen des AEntG und MiLoG angeführt. Doch beide Gesetze geben keine ausreichende rechtliche Basis für eine legale Datenübermittlung, so auch die Datenschutz-Aufsichtsbehörden.

Eine solch umfangreiche und pauschale Abfrage von Daten ist nicht zu rechtfertigen. So sind beispielsweise Angaben zum Familienstand, zur Schwerbehinderteneigenschaft, zum Geburtsdatum oder zur Privatanschrift des Beschäftigten weder geeignet noch erforderlich, um die Haftungssituation des Auftraggebers zu verbessern. Die verschuldensunabhängige Haftung des Auftraggebers kann ohnehin nicht vollkommen ausgeschlossen werden, unabhängig wie sorgfältig die Auswahl und die Überwachung der Nachunternehmer vorgenommen werden.

Vielmehr sollte zum Schutz der Beschäftigten – und letztlich auch des Auftragnehmers, der unberechtigt personenbezogene Daten übermitteln soll – zunächst datensparsam agiert werden. So sind zunächst andere Möglichkeiten zu nutzen, wie z. B. eine Erklärung des Auftragnehmers, die Vereinbarung von Vertragsstrafen und/oder die Einforderung anonymisierter Aufzeichnungen über die gezahlten Löhne an die für den Auftraggeber tätigen Beschäftigten. Auch weiterführende vertragliche Vereinbarungen über Haftungsausschlüsse, Zustimmungspflicht bei der Beauftragung von Subunternehmen, Bankbürgschaften usw. sind der ausufernden Datenabfrage vorzuziehen. Erst bei entsprechenden Verdachtsmomenten, dass der Auftragnehmer oder die Subunternehmen die Vorgaben des MiLoG nicht einhalten, sollten in Abstimmung des betrieblichen Datenschutzbeauftragten andere Vorgehensweisen geprüft werden.

Schon gewusst?

Einwilligungserklärungen müssen grundsätzlich freiwillig, informativ und schriftlich sein. Von der Schriftform darf nur in besonderen Fällen abgewichen werden (bspw. am Telefon, wobei hier eine schriftliche Bestätigung zugesandt werden muss oder auf der Internetpräsenz unter Beachtung des § 13 Absatz 2 TMG). Im Hinblick auf die Freiwilligkeit sind insbesondere im Beschäftigtenverhältnis Grenzen gesetzt, da Mitarbeiter in einem Abhängigkeitsverhältnis zum Arbeitgeber stehen. Was genau möglich und nicht möglich ist?

Fragen Sie Ihren Datenschutzbeauftragten

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

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

ÜIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Passwörter sind Haustürschlüssel zu IT-Systemen

Haustüren werden oftmals abgeschlossen und der Schlüssel liegt nicht unter der Fußmatte. Leider werden diese Verhaltensmuster oftmals nicht auf PC, Internetkonten usw. angewendet.

Folgende Tipps sollten Sie daher im dienstlichen, aber auch im privaten Umfeld beachten:

» Ein **sicheres Passwort** ist nicht zu kurz (mindestens 8 Zeichen) und sollte alphanumerisch, aus Groß- und Kleinbuchstaben sowie aus Sonderzeichen ($ & # @) bestehen.

» Bauen Sie sich lieber „**Eselsbrücken**“ zum besseren Merken (Sätze, Erlebnisse o. ä.) bevor Sie
- zu einfache Standardpasswörter (z. B. „12345678“, „passwort“) oder
- einfach zu erratende Passwörter (Geburtstage, Namen) benutzen.

» **Sperren** Sie Ihren Rechner beim Verlassen und/oder melden Sie sich aus den Systemen ab... Ihre Haustür lassen Sie schließlich auch nicht offen.

» **Ändern** Sie Ihr Passwort regelmäßig oder sobald Sie vermuten, dass es gefährdet ist.

» Nutzen Sie **nicht überall das gleiche Passwort**. Sonst probiert der (erfolgreiche) „Angreifer“, ob es auch bei anderen Accounts funktioniert (ggf. sind sogar Hinweise im „geknackten“ E-Mail-Account wie z. B. Newsletter von Einkaufsportalen).

» Verwenden Sie auch nicht die gleichen Passwörter für geschäftliche und private Konten.

» Halten Sie Ihre Passwörter **geheim** und notieren Sie sie nirgendwo in Klartext. Ihre Bankkarten-PIN notieren Sie ja auch nicht auf der Rückseite oder teilen Sie Ihren Freunden mit.

» **Denken Sie nicht,** dass Sie nicht wichtig genug sind. Die meisten Kriminellen greifen willkürlich an... und Ihr Geld ist denen „wichtig“ genug!

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

Wünschen Sie sich Tipps oder Wissenswertes zu einem bestimmten Thema? Dann schicken Sie uns eine Mail an communication @uimc.de.

IT-Sicherheit für DSB

[Aus-, Fort- und Weiterbildung gemäß § 4f III BDSG]

Datenschutz und IT-Sicherheit sind nicht nur kaum voneinander trennbar. Auch müssen Datenschutzbeauftragte zunehmend im Rahmen der technischen und organisatorischen Maßnahmen entsprechende Kenntnisse über die IT und deren Sicherheit haben. Auch sollte man die „Sprache“ der IT-Mitarbeiter verstehen, um entsprechende Lösungen zu finden.

Melden Sie sich schon jetzt an!

Wuppertal, 23.06.2015

Mehr unter Termine.UIMC.de

BSI IT-Sicherheitskongress

Der IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist ein etablierter Fachkongress für Unternehmen und Behörden. **Wir freuen uns auf Ihren Besuch!**

Unter allen UIMCommunication-Abonnenten verlosen wir **Freikarten**. Einfach eine Mail mit dem Betreff „Freikarte BSI“ an communication@uimc.de senden. Die Freikarte ist nur Gültigkeit für den Zutritt zu der Begleitausstellung in bestimmten Zeiträumen.

Bonn, 19. bis 21.05.2015

Mehr unter Termine.UIMC.de

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

☐ Mindestlohn, verschuldensunabhängige Haftung und der Datenschutz – Rechtliches Dilemma?

☐ Rechtliche Anforderungen an eine Einwilligungserklärung

☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

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

Mehr Informationen, Hinweise und Tipps finden Sie hier: www.UIMC.de/communication

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.