



## **UIMC: Datenschutzbeauftragter kann Schadensersatzansprüche verhindern**

**UIMC: Datenschutzbeauftragter kann Schadensersatzansprüche verhindern**  
Der Umfang der Videoüberwachung im Rahmen der Arbeit nimmt immer stärker zu. Neben der Motivation der Verfolgung von Diebstählen und Vandalismus, der Abschreckung, der Überführung von Straftaten, der Überwachung von Gefahrenschwerpunkten oder aufgrund von behördlichen Auflagen liegen verschiedene Zweckbestimmungen vor. Doch oftmals wird hierbei der Datenschutz nicht beachtet, was neben Bußgeldern und Imageschäden zunehmend auch zu (erfolgreichen) Schmerzensgeldverfahren führt, wie ein aktuelles Urteil des Bundesarbeitsgerichts zeigt. Die gewissenhafte Betrachtung der rechtlichen Anforderungen durch den Datenschutzbeauftragten kann dies verhindern.  
In der täglichen Praxis erlebt Dr. Heiko Haaz, mehrfach bestellter Datenschutzbeauftragter, dass immer mehr Unternehmen zum Mittel der Videoüberwachung greifen. Neben den durchaus üblichen Zielsetzungen der Einbruchsbekämpfung (Überführung und Abschreckung) werden aber zunehmend Tendenzen offenkundig, die Videoüberwachung auf Arbeitsbereiche der Mitarbeiter auszuweiten. Gerade bei solchen Projekten ist der Datenschutzbeauftragte frühzeitig einzubinden, um den Persönlichkeitsrechten ausreichend Rechnung zu tragen. Andernfalls drohen nicht nur Verfahren durch die Aufsichtsbehörden, sondern auch, und das zeigt die aktuelle Rechtsprechung, entsprechend Schadensersatzforderungen.  
So hat das Bundesarbeitsgericht jüngst entschieden - wie auch andere Gerichte schon -, dass eine dauerhafte und verdachtsunabhängige Videoüberwachung am Arbeitsplatz unverhältnismäßig und damit unzulässig ist. Die Schadensersatzforderungen können hierbei durchaus nennenswerte Beträge erreichen [z. B. 25.000 Euro; ArbG Iserlohn, Urteil vom 04.06.2008 - 3 Ca 2636/07]. Auch ein etwaiger Imageschaden bei Kunden, Belegschaft und Betriebsrat ist sicherlich nicht zu vernachlässigen.  
Zur Aufdeckung von Straftaten kann eine (verdeckte) Videoüberwachung nur dann eingesetzt werden, wenn "zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen", dass eine Straftat begangen wurde. Dabei muss die Videoüberwachung "zur Aufdeckung erforderlich" und nicht unverhältnismäßig sein. So sprach Dr. Haaz in einem konkreten Fall, bei dem es um rechtsradikale Schmierereien in Werkshallen ging, beispielsweise folgende Empfehlung aus:  
- Ausführliche Dokumentation des Anfangsverdachts;  
- Zeitlich beschränkte Nutzung der Videoüberwachung (ca. ein Monat);  
- Unverzügliche Löschung, sobald Aufzeichnungen nicht mehr erforderlich sind (z. B. werktäglich);  
- Sehr restriktive Zugriffsrechte (z. B. durch geteiltes Passwort geschützt);  
- Ausschließlich zweckgebundene Zugriffe.  
Ohne entsprechende Regelungen und Verfahren hätten die Videoaufzeichnungen ggf. später bei einem Gerichtsverfahren nicht verwendet werden können und der bzw. die Betroffenen hätten das Unternehmen auf Schadensersatz verklagen können. Es konnte demnach durch die Einbindung des Datenschutzbeauftragten u. U. Schaden vom Unternehmen oder gar vom Geschäftsführer persönlich abgewendet werden. Dies zeigt die Bedeutung des Datenschutzes in vielen Bereichen des Unternehmens.  
UIMC Dr. Voßbein GmbH & Co KG  
Dr. Jörn Voßbein  
Nützenberger Straße 119  
42115 Wuppertal  
Tel.: (0202) 265 74 - 0  
Fax.: (0202) 265 74 - 19  
E-Mail: consultants@uimc.de  
Internet: [http://www.pressrelations.de/new/pmcounter.cfm?n\\_pinr\\_=590283](http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=590283)

### **Pressekontakt**

UIMC

42115 Wuppertal

consultants@uimc.de

### **Firmenkontakt**

UIMC

42115 Wuppertal

consultants@uimc.de

Die UIMC DR. VOSSBEIN GmbH & Co KG, gegründet 1997, hat die damals seit über 10 Jahren laufenden Beratungsgeschäfte der Partner und Gesellschafter Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik und Dr. Jörn Voßbein in einer Beratungsgesellschaft vereint. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig den Datenschutz betreut, als dritter Partner zur UIMC gestoßen. Kerngebiete ihrer Arbeit sind die IT-Sicherheit und der Datenschutz. Sie kann beachtliche Referenzen von Institutionen aus einer Vielzahl von Wirtschaftszweigen sowie Behörden aufweisen und hat eine umfangreiche Projekt- und Betreuungserfahrung, auch international. Felder, auf denen ihre Erfahrungen branchenführend sind. Ihr Leistungsspektrum/Produktprogramm unterscheidet sich von dem anderer Beratungsunternehmen: Sie setzt ein toolgestütztes Analyse- und Konzeptionierungssystem mit einer wissensbasierten Expertensystem-Komponente in Form einer Shell ein, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationelle und kostengünstige Analyse betriebswirtschaftlicher sowie IT-sicherheits- und datenschutzspezifischer Kern- und Teilgebiete sowie die Berichterstattung und Konzeptionserstellung, womit Rationalisierungs- und Effizienzvorteile für ihre Kunden generiert werden. Im Verlaufe der Zeit wurden eine Vielzahl von individuellen Füllungen für diese Shell erarbeitet und in diese eingebracht. Firmenindividuelle Füllungen sind konzeptionell vorgesehen und auf der Basis der Struktur des Tools komplikationslos zu realisieren. Sie führt Workshops, Schulungen sowie Fortbildungsmaßnahmen auf den Sektoren IT-Sicherheit und Datenschutz mit ihrer Marke UIMCollege auch als Inhouse-Veranstaltungen durch.