

In § 3a des Bundesdatenschutzgesetzes (BDSG) steht unter der Überschrift "Datenvermeidung und Datensparsamkeit": "Insbesondere sind personenbezogene Daten zu anonymisieren und zu pseudonymisieren". Das bedeutet also auch, dass Videobilder, die unter der Beachtung von § 6b BDSG berechtigt entstehen, unter besonderen Schutzmaßnahmen gespeichert werden können. Diese besonderen Maßnahmen erfordern klar geregelte Aufzeichnungs- und Zugriffsmöglichkeiten, die nur unter dem Vier-Augen-Prinzip und der erforderlichen Dokumentation die Öffnung und den Zugriff auf die Videodaten ermöglichen. Der unbefugte Zugang und auch der Diebstahl solcher Daten darf letztlich nicht dazu führen, dass manipuliert werden kann und Personen erkennbar werden.

Eine wirklich sichere Lösung beginnt bereits bei der Aufzeichnung, indem ein intelligentes Video-Management-System (VMS) zum Einsatz kommt, welches in Echtzeit unterscheiden kann, ob es sich bei einer Videoaufnahme um statische Räume handelt oder um Personen. Idealerweise verfügt dieses VMS über zusätzliche Algorithmen, die bereits in Echtzeit alle Personenbilder verschlüsselt und die so geschützten Daten im öffentlich zugänglichen Speicher ablegt.

Selbstverständlich ist es wichtig, dass der Persönlichkeitschutz an die jeweiligen Situationen angepasst wird, so kann die Verpixelung in öffentlich stark frequentierten Räumen (Bahn-

**(BS) Wer Bilder einer Videoüberwachung aus öffentlich zugänglichen Bereichen ohne datenschutzkonforme Speicherung archiviert, handelt gesetzeswidrig. Eine mögliche Lösung ist es, Teile des Bildes mit sogenannten Privatzenen schwarz zu überblenden. Allerdings ist dann eine Identifikation von Übeltätern im geschwärzten Teil des Bildes nicht mehr möglich. Wie lässt sich also die Sicherheit effektiv verbessern, ohne dass Persönlichkeitsrechte der Bürger verletzt werden?**

höfe, Passagen, Parkgaragen etc.) weniger intensiv sein, damit die intelligente Analyse einen möglichen Unfall, Sturz oder auch andere Vorfälle sofort erkennen kann und automatisch Hilfe alarmiert. Im eigenen Bürogebäude oder in Schulen muss die Verpixelung berücksichtigen, dass Menschen nicht einfach an ihrem Gang und an ihrer Gestik erkannt werden können. Die Verpixelung muss daher an solchen Lokationen intensiver einstellbar sein.

Besteht nach einem Vorfall ein berechtigtes Interesse, einen aufgezeichneten Vorfall in einem klaren Videostream anzuzeigen, so kann nach dem gesicherten Zugang über ein mehrschichtiges Authentifizierungsverfahren der Rückverrechnungsvorgang gestartet werden. Auch bei diesem Vorgang ist darauf zu achten, dass der jeweilige Zugriff immer nur für eine klar begrenzte Periode gilt und daher auch nur der betreffende Zeitraum geöffnet und selbstverständlich protokolliert wird. Erst dann werden die Personen des jeweilig genehmigten Zeitraumes frei sichtbar und die Bilder können für die weitere Bewertung zur Verfügung stehen.

Dem Verfahren der personenbezogenen Verpixelung ist auf je-



## European Privacy Seal

DE-090017 / Valid till 2013-09

den Fall der Vorzug zu geben, da bei einer Maskierung von Teilbereichen des Videobildes einerseits nicht gesichert ist, dass sich eine Person immer in diesem Bereich aufhält und daher ungewollt erkennbar wird oder und das ist letztlich genauso schlimm, bei einem tatsächlichen Vorfall die Personen nicht mehr reproduzierbar werden. Bei einem professionellen Verfahren ist es sogar möglich, dass auch Personen festgestellt werden, die sich ruhig oder bewegungslos verhalten.

Die Entwickler des zuvor beschriebenen Verfahrens haben ihre Technologie über ein Jahr den rigorosen Tests des unabhängigen Landesentrums für Datenschutz Schleswig-Holstein unterworfen und letztlich das europäische Prüfzertifikat European Privacy Seal erhalten. Nur so hat der Betreiber einer Video-

überwachungsanlage auch die Gewähr, nicht nur seine wirtschaftlichen Interessen zu schützen, sondern sich auch auf rechtlich sicherem Boden zu bewegen.

Was ist also zu tun, um eine bestehende Videoüberwachungsanlage nach den Vorgaben des BDSG zu betreiben? Im einfachsten Fall werden die Kameras, die im öffentlichen Bereich installiert sind, von der bestehenden Aufzeichnung abgeschaltet. Die Anwendung KiwiVision Privacy Protector wird installiert und nach Aufschaltung der Kameras werden alle Videostreams datenschutzkonform gespeichert.

### Beispiele für den Einsatz der datenschutzkonformen Speicherung

#### **Einkaufszentren, Museen, Bibliotheken:**

Hier sind bekanntermaßen

häufig Personen mit kriminellen Absichten unterwegs, die den Kunden ihren Einkaufsbummel verderben können. Aber auch Unfälle an Rolltreppen oder Türen sind immer wieder durch Videoaufzeichnungen zur versicherungstechnischen Abwicklung zu belegen. Immer wieder werden in Museen Bilder oder Ausstellungsobjekte beschädigt, was eine Reproduktion der Vorgänge notwendig werden lässt.

#### **Öffentliche Flächen, Schulen, oder Verkehrsbetriebe:**

An z. B. Parkanlagen, Bushaltestellen ist mit dem Einsatz von Videoüberwachung Sicherheit erwiesenermaßen besser zu gewährleisten. Dies haben die Vorgänge in Bonn eindeutig belegt. Ebenso nutzen die Sicherheitsbehörden seit Jahren Videoüberwachung an Kriminalitätsschwerpunkten mit teilweise großem Erfolg. Dort, wo die Anlagen wieder abgebaut werden mussten, ist der Trend eindeutig negativ.

#### **Krankenhäuser:**

Hier sind die Patienten quasi immer im öffentlichen Raum, zumindest wenn sie das Haus betreten oder mit einem Krankentransport eingeliefert werden. Auch dabei ist die Dokumentation über das Verhalten der Patienten oder der Krankentransport-

teure häufig ein Streitpunkt, der mit einer sachgemäßen Videodokumentation eindeutig belegbar ist.

#### **Tankstellen:**

Die Verluste der Tankstellenbetreiber durch Diebstähle, im quasi öffentlichen Bereich der Tanksäulen, fressen oft den Gewinn einer Tankstelle wieder auf. Der umfangreiche Einsatz von Videotechnik hat dieses Problem in den letzten Jahren auf ein überschaubares Maß zurückgedrängt. Aber auch im Bereich der Kassen stellt sich das Problem Datenschutz.

#### **Banken:**

In allen öffentlich zugänglichen Bereichen von Banken und Sparkassen treffen die Forderungen der UVV-Kassen zum Schutz der Mitarbeiter konträr auf das Thema Datenschutz. Wenn man beide Funktionen mit einander verknüpft, wird man der UVV und dem Recht der Kunden am eigenen Bild gerecht.

Zusammenfassend kann man aus heutiger Sicht sagen, die bedarfsgerechte Videoüberwachung ist aus unserem Alltag nicht mehr wegzudenken. Das Persönlichkeitsrecht jedes Einzelnen ist aber auch ein hohes Gut unserer Gesellschaft und somit zu schützen. Durch den Einsatz innovativer Technik lassen sich auch beide Aspekte gut zusammenbringen.

Weitere Informationen unter: AVT - Alarm- und Video-Technik GmbH, Walter Schwinger, Schwalbenrainweg 30a, 63741 Aschaffenburg, Tel.: 06021/3471-0, E-Mail: info@avt-gmbh.de