
Fälle aus der Datenschutz-Praxis – Ausgabe 2011-1

Videoüberwachung – auch in Geschäften kein Patentrezept

Seit einiger Zeit häufen sich die Beschwerden von Bürgerinnen und Bürgern wegen der zunehmenden Videoüberwachung in Geschäften mittelständischer und kleiner Unternehmen mit Kundenverkehr. Hierzu zählen auch die unzähligen Filialen der Lebensmittelketten. Betroffen sind fast alle Branchen wie Friseurgeschäfte, Videotheken, Apotheken, Boutiquen, Imbissbuden, Kioske und Zeitungsstände.

Als Gründe für eine Videoüberwachung werden häufig generalpräventive Zwecke wie die Furcht vor Warendiebstahl, Einbruch, Sachbeschädigung und der Schutz der Beschäftigten vor tätlichen Übergriffen gewalttätiger Kunden genannt. Bevor jedoch eine Videoüberwachungsanlage installiert wird, müssen drei grundlegende Kriterien geprüft werden: Die Erforderlichkeit, die Geeignetheit und die Verhältnismäßigkeit einer solchen Maßnahme. Nur wenn alle drei Kriterien erfüllt sind, ist eine Videoüberwachung gerechtfertigt.



Es liegt im ureigenen Interesse einer Ladenbesitzerin oder eines -besitzers, sich vor Diebstahl, Einbruch und Übergriffen zu schützen. Allerdings ist eine Videoüberwachung nur dann erforderlich, wenn es auch tatsächlich zu solchen Vorfällen gekommen ist. Ladenbesitzerinnen und -besitzer sollten diese Vorfälle durch die Vorlage einer Strafanzeige bei der Polizei belegen können. Die Erforderlichkeit kann in Einzelfällen aber auch angenommen werden, wenn ein besonderes Schutzbedürfnis dargestellt werden kann, z. B. wenn das videoüberwachte Geschäft in einer Umgebung mit hoher Kriminalitätsdichte liegt.

Feststellung: Vor der Installation von Videoüberwachungskameras in Geschäften mit Kundenverkehr muss ihre Zulässigkeit nach § 6 b BDSG geprüft werden. Videoüberwachung muss erforderlich, geeignet und verhältnismäßig sein, und es ist zu prüfen, ob andere Mittel, die nicht in Persönlichkeitsrechte der Kundschaft und der Beschäftigten eingreifen, nicht in gleicher Weise zum Ziel führen.

Quelle: Datenschutzbericht 2009 des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Illegale Entsorgung von Daten

Aufgrund der Beobachtungen eines aufmerksamen Anwohners wurde der LfD im September 2009 davon in Kenntnis gesetzt, dass sich in mehreren Müll-Containern in Mainz-Weisenau hunderte von Personalakten frei zugänglich befanden. Nach den Feststellungen des LfD wurde – offenbar von einer Marketing-Firma aus dem Telekommunikationsbereich – eine große Anzahl von Personalakten, Steuerunterlagen und Bewerbungsmappen mit sensiblen und geschützten Daten wie Lebensläufen, Fotografien, Bankverbindungen, Telefon- und Mobilfunknummern etc. illegal deponiert. Auf Ersuchen des LfD stellte das Polizeipräsidium Mainz die Müllcontainer umgehend sicher.

Die Verantwortung für den entdeckten Datenschutzverstoß der Marketing-Firma konnte rasch aufgeklärt werden. Der verantwortliche Unternehmensleiter stellte sich aufgrund des öffentlichen Drucks den Behörden und legte ein umfassendes Geständnis ab. Die von den Polizeibehörden sichergestellten Unterlagen wurden unter Aufsicht des LfD eingehend gesichtet und sodann ordnungsgemäß vernichtet, so dass weiterer Schaden für die betroffenen Arbeitnehmer sowie die früheren Bewerber nicht mehr entstehen konnte. Wegen der gravierenden Verstöße gegen datenschutzrechtliche Bestimmungen zur sorgfältigen Vernichtung personenbezogener Daten wurde außerdem ein Bußgeldverfahren eingeleitet, welches mit der Verhängung eines Bußgeldes in vierstelliger Höhe abgeschlossen wurde.

Feststellung: Insgesamt zeigte der Vorfall, dass die Unternehmen mit Personaldaten besonders sorgfältig umgehen müssen. Dies gilt nicht nur bei der Erhebung und der Verwendung der Daten, sondern auch bei deren Vernichtung. Wer gegen diese Sorgfaltspflichten verstößt, richtet nicht nur erheblichen Schaden an, er enttäuscht auch das Vertrauen seiner Mitarbeiter und muss mit erheblichen Geldstrafen rechnen.

Quelle: Datenschutzbericht 2008/2009 des Landesbeauftragten für den Datenschutz Rheinland-Pfalz.

Gewinnspiele und unerwünschte Werbenachrichten (Spam)

Ein Petent beschwerte sich über den Eingang unerwünschter Werbenachrichten (Spam), die er nahezu zeitgleich von drei verschiedenen Absendern erhalten hatte. Nach eigener Aussage ging er mit seiner Mailadresse sehr zurückhaltend um und hatte bisher keine Probleme mit unerwünschten Werbenachrichten gehabt. Wie sich im Laufe der Sachverhaltsaufklärung zeigte, gehörten die drei Absenderadressen zu drei Unternehmen: zwei hatten denselben Geschäftsführer, das dritte arbeitete mit den beiden anderen zusammen. Alle drei betrieben Internetgewinnspiele und vergleichbare Angebote. Eines der Unternehmen gab an, die Kontaktdaten des Betroffenen von diesem selbst im Rahmen eines Internetgewinnspiels bekommen und die Einwilligung zur Weitergabe an verbundene Unternehmen erhalten zu haben. Als Beleg der Einwilligung wurden die Daten aus dem sogenannten Double Opt-In übersandt. Nach Rücksprache mit dem Betroffenen stellte sich heraus, dass diese Daten offensichtlich falsch waren, da die angegebene IP-Adresse, von der die Anmeldung zum Gewinnspiel erfolgte, nicht in den Adresskreis des Internetproviders des Betroffenen gehörte. Daher konnte der Betroffene sich nicht mit diesen Daten von seinem heimischen Rechner aus angemeldet haben. Um zu klären, ob sich der Betroffene möglicherweise von einem anderen Rechner aus angemeldet hatte oder ob die Daten eventuell gefälscht worden waren, wurde das Unternehmen um die Mitteilung der Daten des Gewinners des inzwischen abgeschlossenen Gewinnspiels, in dem ein Auto verlost wurde, gebeten. Nachdem es gelang, aktuelle Kontaktdaten der Gewinnerin in Erfahrung zu bringen, wurde diese zu ihrer Anmeldung im Gewinnspiel und dem Gewinn befragt. Sie erklärte, dass sie grundsätzlich nicht an Gewinnspielen teilnehme und auch noch nie ein Auto gewonnen habe.

Die überwiegende Mehrzahl der Internetplattformen, auf denen Gewinne versprochen werden, oder auf denen man sich z. B. als „Produkttester“ anmelden kann, um Waren übersandt zu bekommen, die man dann testet und anschließend behalten darf, zielen in erster Linie darauf ab, Kontaktdaten zu erhalten, um an die Betroffenen selbst unerwünschte Werbenachrichten zu senden oder um die Adressen für diesen Zweck weiter zu verkaufen.

Feststellung: Da es sich bei unerlaubten Werbenachrichten um unlauteren Wettbewerb handelt, können die Verbraucherzentralen (s. <http://www.vzbv.de/>) in diesen Fällen Unterlassungs- und Beseitigungsansprüche durchsetzen und gegenüber dem Versender einen Anspruch auf Ersatz von Aufwendungen oder Kosten der Rechtsverfolgung geltend machen. Allerdings sind auch den Möglichkeiten der Verbraucherzentralen regelmäßig dann Grenzen gesetzt, wenn der Versender seinen Sitz im Ausland hat.

Quelle: Web Site des Landesbeauftragten für den Datenschutz Niedersachsen, „Fälle aus der Praxis“.

Videoüberwachung von Demonstrationen

Im Rahmen eines Gerichtsverfahren ist bekannt geworden, dass bei einer Demonstration verdeckt ermittelnde Berliner Beamte des Landeskriminalamts zur Unterstützung der Dresdner Polizei sich dort aufgehalten und ohne Vorliegen einer unmittelbaren Gefahr für die öffentliche Sicherheit digitale Filmaufnahmen von einzelnen Demonstrierenden angefertigt haben. Die Beamten trugen Zivilkleidung.

Verdeckte Bildaufnahmen durch die Polizei bedürfen sowohl aus datenschutz-, als auch aus verfassungsrechtlichen Gründen einer hinreichend bestimmten Rechtsgrundlage. Nach §12 a Abs. 1 Versammlungsgesetz darf die Polizei Aufnahmen von Teilnehmenden anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit und Ordnung ausgehen. Eine Speicherung ist zur Verfolgung von Straftaten der Teilnehmenden oder im Einzelfall zur Gefahrenabwehr zulässig. Die Vorschrift regelt lediglich Bild- und Tonaufnahmen von Teilnehmern im Zusammenhang mit öffentlichen Versammlungen, aber keine Voraussetzungen für die Zulässigkeit verdeckter Videoaufnahmen.

Staatliches Handeln bei der Grundrechtsausübung hat grundsätzlich transparent zu erfolgen. Verdeckte Bildaufnahmen bei Versammlungen dürfen jedenfalls nur die Ausnahme sein. Heimliche bzw. verdeckte Maßnahmen der Datenerhebung stellen einen tiefer gehenden Grundrechtseingriff dar als offen erfolgende Maßnahmen. (*Anmerkung: Ebenso zutreffend im nicht-öffentlichen Bereich, durchgeführt von Unternehmen oder Privatpersonen!*)

Feststellung: Bildaufnahmen, die Polizeibeamte in Zivil bei Demonstrationen machen, sind unzulässig! (*Anmerkung: Grundsätzlich bedarf es einer Rechtsgrundlage!*)

Quelle: Datenschutzbericht 2009 des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

