

Hinweise des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen (Nr. 39)

Bekanntmachung des Innenministeriums vom 25.01.2001 Az. 2-0552.1/16.

Die Veröffentlichung erfolgt im Anschluss an die Hinweise Nr. 38
im Staatsanzeiger für Baden-Württemberg Nr. 2 vom 24.01.2000, Seite 12.

A. Übermittlung personenbezogener Daten im internationalen Bereich

1. Problemstellung, Rechtsgrundlagen, Anwendungsbereich der EG-Datenschutzrichtlinie 95/46

Bisher gibt es für den nicht-öffentlichen Bereich im Bundesdatenschutzgesetz (BDSG) keine eigenständigen Regelungen für Datenübermittlungen ins Ausland.

Die EG-Datenschutzrichtlinie 95/46 (veröffentlicht im Amtsblatt der EG Nr. L 281 vom 23. November 1995) - im nachfolgenden Richtlinie genannt - sieht dafür in Artikel 25 und 26 differenzierte Regelungen vor, die auch für den nicht-öffentlichen Bereich gelten und mit der Novellierung des BDSG in §§ 4b und 4c (BDSG-E) in Bundesrecht umgesetzt werden sollen.

Bedeutsam sind diese Neuregelungen insbesondere auch für den Datenfluss zwischen den verschiedenen Konzernteilen eines internationalen Konzerns, da das deutsche Recht weiterhin keinen „Konzernschutz“ kennt und deshalb der Datenfluss nur unter den auch sonst geltenden Übermittlungsvorschriften zulässig ist, es sei denn, es liegt eine Auftragsdatenverarbeitung in Deutschland oder im Anwendungsbereich der Richtlinie vor.

Die Aufsichtsbehörde für den Datenschutz möchte an sie gestellte Fragen im internationalen Datenverkehr aufgreifen und im Vorgriff auf die Novellierung des BDSG behandeln. Die nachstehende Darstellung ist deshalb nicht als abschließend anzusehen. Zugrundegelegt wird der Gesetzentwurf der Bundesregierung vom 18. August 2000 (BT-Drs. 461/00), der sich derzeit im Gesetzgebungsverfahren befindet.

Nach den Regelungen ist zunächst zu unterscheiden zwischen Datenübermittlungen an Stellen

- innerhalb der Mitgliedstaaten der EU im Anwendungsbereich der Richtlinie (1. Fallgruppe) und
- innerhalb der Mitgliedstaaten der EU außerhalb des Anwendungsbereichs der Richtlinie oder an Nicht-EU-Länder, sogenannte Drittstaaten (2. Fallgruppe).

Innerhalb der 2. Fallgruppe ist weiter zu unterscheiden, ob bei den Stellen, an die personenbezogene Daten übermittelt werden sollen, ein angemessenes Datenschutzniveau gewährleistet ist oder nicht. Ist ein angemessenes Datenschutzniveau nicht gewährleistet, schließen sich weitere Differenzierungen an. Eine zulässige Datenübermittlung ist immer mit dem Hinweis zu versehen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden (§ 4b Abs. 6 und § 4c Abs. 1 S. 2 BDSG-E).

Mitgliedsstaaten der Europäischen Union sind derzeit (Stand Januar 2001):

Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Irland, Italien, Luxemburg, Niederlande, Österreich, Portugal, Schweden und Spanien.

Der Anwendungsbereich der Richtlinie ist in Artikel 3 geregelt. Nach Artikel 3 Abs. 1 der Richtlinie erstreckt er sich auf die automatisierte und nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Nicht unter den Anwendungsbereich fallen nach Artikel 3 Abs. 2 u.a. die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates, die Tätigkeit des Staates im strafrechtlichen Bereich und ausschließlich persönliche oder familiäre Tätigkeiten, die von einer natürlichen Person ausgeübt werden (Aufzählung der Tätigkeiten nach den Titeln V und VI des EU-Vertrags).

2. Zulässigkeit der Datenübermittlung innerhalb des Anwendungsbereichs der Richtlinie (1. Fallgruppe)

Innerhalb des Anwendungsbereichs der Richtlinie gelten keine Besonderheiten. Nach § 4 b Abs. 1 BDSG-E wird die Europäische Union insoweit datenschutzrechtlich als einheitlicher Rechtsraum mit „angemessenem Datenschutzniveau“ angesehen.

Eine Datenübermittlung ist unter den Voraussetzungen der §§ 28 bis 30 BDSG-E oder auf Grund einer Einwilligung zulässig. Auch für die Auftragsdatenverarbeitung gelten keine Besonderheiten.

Beispielsfall:

Ein baden-württembergisches Unternehmen verarbeitet personenbezogene Daten und möchte Teile der Datenverarbeitung im Wege der Auftragsdatenverarbeitung nach Frankreich auslagern. Die Daten verbleiben – wie auch sonst - in der Verantwortung des baden-württembergischen Unternehmens. Dass sich der Auftragnehmer in Frankreich befindet, ändert an der datenschutzrechtlichen Beurteilung nichts, da er dem Geltungs- und Anwendungsbereich der Richtlinie unterfällt. Eine Datenübermittlung findet nicht statt. Im Falle einer Funktionsübertragung müssten die auch sonst bestehenden Übermittlungsvorschriften beachtet werden. Zusätzliche Zulässigkeitsvoraussetzungen wegen der Übermittlung nach Frankreich bestehen nicht.

3. Zulässigkeit der Datenübermittlung außerhalb des Geltungs- oder Anwendungsbereichs der Richtlinie (2. Fallgruppe)

Eine zulässige Datenübermittlung setzt neben dem Vorliegen der Voraussetzungen der §§ 28 bis 30 BDSG-E nach § 4b Abs. 2 BDSG-E zusätzlich voraus, dass der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Ein solches schutzwürdiges Interesse ist insbesondere dann gegeben, wenn bei der Stelle, an die die Daten übermittelt werden sollen, kein angemessenes Datenschutzniveau gewährleistet ist. Eine Datenübermittlung hat dann zu unterbleiben

- an Drittstaaten oder eine über- oder zwischenstaatliche Stelle, es sei denn, die Datenübermittlung ist nach § 4c BDSG-E ausnahmsweise zulässig,
- im Übrigen ausnahmslos innerhalb der Mitgliedstaaten der EU außerhalb des Anwendungsbereichs der Richtlinie.

3.1 Angemessenes Schutzniveau wird/ist festgestellt

3.1.1 § 4 b Absatz 3 BDSG-E und Artikel 25 der Richtlinie

Ob ein angemessenes Datenschutzniveau gewährleistet ist, ist nach den in § 4b Abs. 3 BDSG-E niedergelegten Kriterien im Einzelfall von der übermittelnden Stelle zu beurteilen. Da diese Feststellung sehr aufwendig sein kann, kann die Europäische Kommission nach Artikel 25 Abs. 6 der Richtlinie für ein Drittland allgemein die Feststellung treffen, es gewährleistet ein angemessenes Datenschutzniveau oder nicht. Die Kommissionsentscheidung ist für alle EU-Mitgliedsstaaten bindend.

Für die Staaten Schweiz und Ungarn hat die EU-Kommission am 26. Juli 2000 ein angemessenes Datenschutzniveau festgestellt (veröffentlicht im Amtsblatt der EG Nr. L 215 vom 25. August 2000).

3.1.2 Safe Harbor/Spezialfall USA

Ein Spezialfall bilden die „Safe Harbor Regelungen“ mit den USA, für die die EU-Kommission ebenfalls am 26. Juli 2000 ein angemessenes Datenschutzniveau festgestellt hat. Damit wird die Möglichkeit geschaffen, personenbezogene Daten aus der EU in die Vereinigten Staaten von Amerika zu übermitteln. Voraussetzung dafür ist, dass sich die Unternehmen den „Grundsätzen des sicheren Hafens zum Datenschutz“ (Safe Harbor) und den „Häufig gestellten Fragen“ (Frequently Asked Questions FAQ) unterwerfen.

Für internationale Unternehmen, die ihren Sitz in den USA haben und den o.a. Grundsätzen und den „Häufig gestellten Fragen“ beigetreten sind, führt das US-Handelsministerium (Federal Trade Commission) eine Liste. Für Unternehmen, die der internationalen Reiseverkehrsbranche (u.a. Luftverkehrsunternehmen) angehören, führt das US-Verkehrsministerium diese Liste. Die Liste mit den beigetretenen Unternehmen sowie weitere Informationen zu Safe Harbor können derzeit unter den Adressen Safe-Harbor-Liste:

(<http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>)

Weitere Informationen:

<http://www.export.gov/safeharbor/> und

http://www.europa.eu.int/comm/internal_market/de/media/dataprot/news/datatransf.htm

abgerufen werden. Die jeweils aktuellen Internetadressen können über unsere Internetseite (<http://www.innenministerium.baden-wuerttemberg>) unter der Rubrik „Datenschutz - Links“ abgerufen werden.

Hinweis: Unternehmen, die in den Bereichen Banken, Sparkassen und Telekommunikation tätig sind, fallen bisher nicht unter das Abkommen.

Beispielsfall:

Ein Tochterunternehmen mit Sitz in Baden-Württemberg und einer Konzernmutter mit Sitz in den USA beabsichtigt die Übermittlung von Arbeitnehmerdaten von Deutschland in die USA zur Erstellung einer konzernweiten Personalstatistik. Die 1999 begonnenen und im Jahr 2000 fortgesetzten Gespräche führten zuerst zur Empfehlung eines Vertrags, der geeignet ist, die Verarbeitung der Arbeitnehmerdaten in den USA einem angemessenen Datenschutzniveau zu unterwerfen. Nach Vorliegen der Safe-Harbor-Regelungen könnte das US-Unternehmen sich auch in die Liste des US-Handelsministeriums eintragen und somit ein entsprechendes Datenschutzniveau garantieren.

3.2 Angemessenes Schutzniveau wird nicht festgestellt

3.2.1 Ausnahmen nach § 4c BDSG-E

Die strikten Regelungen des § 4b Abs. 2 BDSG-E für die Übermittlung personenbezogener Daten in einen Staat ohne angemessenes Datenschutzniveau werden durch die Ausnahmetatbestände in § 4c Abs. 1 BDSG-E etwas erleichtert. Dazu zählen insbesondere die Einwilligung und Übermittlungen im Rahmen eines Vertrags oder Vorvertrags, der durch den Betroffenen selbst oder durch einen Dritten in seinem Interesse geschlossen wird. Damit soll sichergestellt werden, dass der Wirtschaftsverkehr mit Drittstaaten nicht unangemessen beeinträchtigt wird.

3.2.2 Vertragsklauseln oder verbindliche Unternehmensregelungen

Der Ausschluss der Übermittlung mangels angemessenen Datenschutzniveaus kann auch dann vermieden werden, wenn beim Datenempfänger Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte bestehen; diese Garantien können sich nach § 4c Abs. 2 BDSG-E insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben.

Die Datenübermittlung auf der Grundlage ausreichender Garantien hinsichtlich des Datenschutzes bedarf der Genehmigung durch die zuständige Aufsichtsbehörde. Die Genehmigung kann sich auch auf eine Kategorie von Übermittlungen beziehen.

Die EU-Kommission kann nach Artikel 26 Abs. 4 der Richtlinie feststellen, dass durch die Verwendung bestimmter Standardvertragsklauseln ausreichende Garantien hinsichtlich des Datenschutzes gegeben sind. Ein vorläufiger Entwurf der Entscheidung der Kommission zu Standardvertragsklauseln (Stand 08.12.2000) liegt vor, das Verfahren ist jedoch noch nicht abgeschlossen.

Der Entscheidungsentwurf und die Mustervertragsklauseln können aufgerufen werden unter http://europa.eu.int/comm/internal_market/de/media/dataprot/news/index.htm.

Beispielsfall:

Ein mit Hauptsitz in Baden-Württemberg ansässiges Unternehmen plant den Aufbau eines Tochterunternehmens in Rumänien. Es ist dabei vorgesehen, die Verarbeitung personenbezogener Daten im Wege der Funktionsübertragung nach Rumänien zu verlagern. Da Rumänien ein Drittland ist, das derzeit noch kein angemessenes Schutzniveau aufweist, ist eine Datenübermittlung nach § 4b Abs. 2 BDSG-E unzulässig. Es empfiehlt sich deshalb der Abschluss eines Vertrags zur Absicherung des Datenschutzniveaus in Rumänien oder die Einführung von verbindlichen unternehmensweiten Datenschutzrichtlinien. Die

Datenübermittlung auf der Grundlage des Vertrags oder der verbindlichen Unternehmensregelungen ist genehmigungspflichtig.

3.3 Besonderheit der Auftragsdatenverarbeitung in Drittstaaten

Weder die Richtlinie noch der Entwurf des BDSG enthalten eine Regelung, die sich auf die Auftragsdatenverarbeitung durch in Drittstaaten ansässige Auftragnehmer bezieht. Nach dem Wortlaut des § 3 Abs. 8 BDSG-E ist davon auszugehen, dass Auftragsdatenverarbeitung nur innerhalb der Europäischen Union zulässig ist (Beschränkung des Begriffs des „Dritten“). Daher liegt hier ein Fall der Datenübermittlung vor, der wie auch sonst einer Rechtsgrundlage bedarf.

3.4 Datenverarbeitung innerhalb internationaler Konzerne mit Sitz von Konzernteilen in Drittstaaten ohne angemessenes Datenschutzniveau

Der Entwurf des Bundesdatenschutzgesetzes regelt in Übereinstimmung mit der Richtlinie nur die Datenübermittlung von Deutschland ins Ausland. Sonderregelungen für Konzerne gibt es nicht. Es ist jedoch davon auszugehen, dass die Erhebung, Verarbeitung und Nutzung der Daten bei international tätigen Unternehmen mit ihren Teilunternehmen grenzüberschreitend stattfindet, unabhängig davon, ob sich diese innerhalb der EU oder in einem Drittland befinden. Bei einer datenschutzrechtlichen Gesamtbetrachtung internationaler Unternehmen ist es daher wesentlich, dass die Verarbeitung mit der Übermittlung der Daten in ein Teilunternehmen nicht endet, sondern sich fortsetzt.

Aus der Sicht des internationalen Konzerns können dabei bezogen auf einzelne Teile des Konzerns viele datenschutzrechtliche „weiße Flecken“ auftauchen. Um ungehindert von der jeweiligen nationalen Gesetzgebung eine datenschutzgerechte Verarbeitung personenbezogener Daten zu ermöglichen, empfiehlt sich deshalb die Schaffung eines konzerninternen angemessenen Datenschutzniveaus durch verbindliche Unternehmensregelungen. Bezogen auf die Konzernteile mit Sitz in der EU müssen die Vorgaben der Richtlinie eingehalten werden, sowie bezogen auf die Konzernteile in Deutschland muss die Übermittlung entsprechend einer verbindlichen Unternehmensregelung zusätzlich von der zuständigen Aufsichtsbehörde nach § 4c Abs. 2 BDSG-E genehmigt werden.

Beispielsfall:

Ein mit Hauptsitz in Baden-Württemberg international tätiges Unternehmen hat in verschiedenen Ländern Teilkonzerne, mit denen u.a. auch personenbezogene Daten ausgetauscht werden. Wegen der datenschutzrechtlich bestehenden „weißen Flecken“ wurde

die Schaffung eines konzerninternen angemessenen Datenschutzniveaus durch verbindliche Unternehmensregelungen empfohlen. Die Gespräche sind noch nicht abgeschlossen.

B. Personaldaten im Internet

Vermehrt gehen Arbeitgeber dazu über, Personaldaten im Internet zu veröffentlichen, um den (potentiellen) Kunden kompetente Ansprechpartner zu benennen.

Die Zulässigkeit der Nutzung von Personaldaten durch das Unternehmen ist in erster Linie nach arbeitsrechtlichen Gesichtspunkten zu beurteilen. Voraussetzung ist in jedem Fall, dass die Nutzung im Zusammenhang mit dem Arbeitsverhältnis steht. Die Zulässigkeit der Bekanntgabe von Personaldaten – auch über Internet - kann sich schon direkt aus dem Arbeitsvertrag ergeben. Im Übrigen richtet sie sich nach § 28 Abs. 1 Nr. 1 BDSG, wonach die Nutzung von Daten zur Erfüllung eigener Geschäftszwecke im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen zulässig ist. Mitarbeiterinnen und Mitarbeiter, insbesondere in Funktionen mit Außenwirkung und unmittelbarem Kundenkontakt, müssen es hinnehmen, wenn die Geschäftsleitung im Rahmen ihres Direktionsrechts entscheidet, die Daten, wie beispielsweise Name, Funktion, Spezialkenntnisse, telefonische und elektronische Erreichbarkeit, bekannt zu geben.

Eine darüber hinausgehende Bekanntgabe von Daten, wie z.B. Privatanschrift, Anzahl der Kinder, Familienstand, Geburtsdatum, fällt nicht unter diese allgemeine Zulässigkeitsnorm, sondern bedarf einer ausdrücklichen Einwilligung des Betroffenen. Im Übrigen ist auch die Veröffentlichung von einem Bild des Betroffenen von einer Zustimmung des Betroffenen abhängig.

Sicherlich ist es wünschenswert und auch angebracht, die betroffenen Mitarbeiterinnen und Mitarbeiter von Firmenseite aus darüber zu unterrichten, dass eine Veröffentlichung der Daten im Internet erfolgt. Rechtlich vorgeschrieben ist dies aber nicht.

C. Zulässigkeit von Webcams im Internet

In der letzten Zeit gehen bei der Aufsichtsbehörde verstärkt Anfragen zur Zulässigkeit sogenannter Webcams, meist von potenziellen Aufstellern, ein. Aufnahmegegenstände sind i. d. R. touristische Sehenswürdigkeiten, die Außenansicht von Gewerbeobjekten oder Internetcafés, die als Werbung für das einstellende Unternehmen angeboten werden.

Unter einer Webcam versteht man eine Kamera, die optisch-elektronische Bilder der Umgebung auf einem ans Internet angeschlossenen Rechner zum Abruf aus dem Internet bereitstellt¹. Im Regelfall werden die Bilder in periodischem Zeitabstand aktualisiert und mit

der Uhrzeit verknüpft. Durch das Bereitstellen der Bilder werden diese während des Aufnahmeintervalls gespeichert und dann durch das nächste Bild überschrieben.

Das Bereitstellen von Bildern auf einem Server zum Abruf über das Internet ist ein öffentliches Verbreiten, ähnlich dem Veröffentlichen von Bildern in einer Zeitschrift.

Mit den Bildern einer Webcam, bei denen meist die Aufnahmezeit mitangezeigt wird, können personenbezogene Daten übermittelt werden. Ein Personenbezug liegt vor, wenn auf dem Bild die Person direkt oder über ein personenbezogenes Kennzeichen, wie z.B. das Fahrzeugkennzeichen, eindeutig identifizierbar ist, d.h. wenn festgestellt werden kann, dass eine bestimmte Person zu einem bestimmten Datum an einem bestimmten Ort war.

1. Beurteilung nach dem gültigen BDSG

Nach dem derzeit² gültigen Bundesdatenschutzgesetz (BDSG) fallen Webcam-Aufnahmen nicht unter die Vorschriften dieses Gesetzes, da sie nicht den Dateibegriff des § 3 Abs. 2 BDSG erfüllen.

2. Beurteilung nach dem Entwurf der BDSG-Novelle³

Voraussetzung für die Anwendbarkeit des BDSG ist, dass personenbezogene Daten vorliegen, d.h., dass Personen auf den Bildern identifiziert werden können (s.o.). Mit der kommenden Novellierung des BDSG sollen in § 6 b (BDSG-E) Regelungen zur Videoüberwachung in das Gesetz aufgenommen werden. Danach ist die Beobachtung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Aufgabenerfüllung, zur Wahrnehmung des Hausrechts oder zur Erfüllung eigener Geschäftszwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das Merkmal der Beobachtung ist dann gegeben, wenn eine Webcam in regelmäßigen Zeitabständen Bilder erzeugt. Für die Beobachtung ist es nicht erforderlich, dass die Bilder gespeichert werden. Ein öffentlich zugänglicher Raum ist jeder Bereich, der ohne besondere Voraussetzungen betreten werden kann. Er kann innerhalb oder außerhalb von Gebäuden liegen. Der Begriff stellt nicht auf das Eigentumsverhältnis (öffentliches Grundstück, privates Grundstück) ab.

In den bisher vorliegenden Fällen dient die Beobachtung mittels Webcam weder der Aufgabenerfüllung noch der Wahrnehmung des Hausrechts⁴. Ob sie für die Erfüllung eigener Geschäftszwecke erforderlich ist, ist fraglich und kann nur im konkreten Einzelfall entschieden werden.

Im Falle einer Webcam in einem Internetcafé kann die Beobachtung beispielsweise dann der Erfüllung eigener Geschäftszwecke dienen, wenn dem Nutzer ermöglicht werden soll, von sich selbst durch die Webcam aufgenommene Bilder zu versenden. In diesem Fall ist auch nicht davon auszugehen, dass seine schutzwürdigen Interessen überwiegen. Es muss jedoch in jedem Fall ausgeschlossen sein, dass unbeteiligte Dritte außerhalb des Internetcafés mit einer Bildqualität, die eine Identifizierung ermöglicht, aufgenommen werden.

Die Beobachtung muss nach § 6 b Abs. 2 BDSG-E erkennbar gemacht werden. Dies bedeutet, dass in dem Bereich, aus dem die Webcam personenbezogene Bilder liefern kann, ein Hinweis auf die Webcam so gut erkennbar angebracht ist, dass dieser, ehe der Bereich betreten wird, ohne weiteres wahrgenommen werden kann. Dies lässt sich am besten durch optische Markierungen und auffällige Informationsschilder realisieren. Ebenso ist die für die Beobachtung verantwortliche Stelle nach § 6 b Abs. 2 BDSG-E erkennbar zu machen.

Liegen die Voraussetzungen für die Zulässigkeit der Videoüberwachung nicht vor, was in der Regel der Fall sein dürfte, so ist der Einsatz der Webcam nur zulässig, wenn der Betroffene, d.h. jeder von der Kamera Erfasste, nach § 4 BDSG-E in die Übermittlung einwilligt. Die Voraussetzungen für die Wirksamkeit der Einwilligung sind in § 4 a BDSG-E festgelegt. Danach muss der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie die Folgen der Verweigerung hingewiesen werden. Das Gesetz geht von dem Grundsatz aus, dass die Einwilligung der Schriftform bedarf, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

In den hier bekannten Fällen des Einsatzes einer Webcam ist es praktisch nicht möglich, die schriftliche Einwilligung der Betroffenen einzuholen. Die Kameras werden ohne Bedienerpersonal betrieben. Personal wäre erforderlich, um die schriftliche Einwilligung einzuholen, und wenn diese nicht gegeben wird, um die Aufnahme auszusetzen. Wenn die schriftliche Einholung einer Einwilligung sonach faktisch nahezu unmöglich ist, können besondere Umstände vorliegen, die eine Einwilligung in „anderer Form“ zulassen. Eine Einwilligung in anderer Form ist z.B. eine konkludente Handlung. In diesem Fall müssen jedoch Schilder mit dem Hinweis auf die Webcam und die Einwilligung an allen Zugangswegen zum Aufnahmebereich gut erkennbar aufgestellt sein. Der Passant muss zudem darüber informiert werden, dass die Webcam Bilder für jedermann abrufbar ins Internet einstellt, dass er mit dem Betreten des Aufnahmebereichs seine Einwilligung zur Aufnahme und zum Einstellen erteilt und dass er im Falle der Verweigerung seiner Einwilligung die Aufnahme nur vermeiden kann, indem er den Bereich nicht betritt. Hierbei ist auf die Freiwilligkeit der Erklärung zu achten. Befindet sich die Webcam z. B. an einer Stelle, die der Betroffene passieren muss, um zu seinem Ziel zu gelangen (z.B. Eingang von einer Se-

henswürdigkeit, öffentliche Verkehrsfläche), so liegt mangels Freiwilligkeit keine wirksame Einwilligung vor. Webcams müssen beispielsweise vor Sehenswürdigkeiten so aufgestellt werden, dass sie nicht den gesamten Eingangsbereich erfassen.

3. Telediensterecht

Das Bereitstellen von Bildern über das Internet ist ein Teledienst im Sinne von § 2 Abs. 2 Nr. 1 des Teledienstegesetzes. Der Schutz personenbezogener Daten bei der Durchführung von Telediensten ist im Teledienstedatenschutzgesetz (TDDSG) geregelt. Daten zur Nutzung eines Teledienstes können Bestands- und Nutzungsdaten sowie Abrechnungsdaten als Unterform der Nutzungsdaten sein. Davon unterscheiden sich die Inhaltsdaten, die nicht vom TDDSG erfasst sind. Die von dem Teledienst Webcam erstellten Aufnahmen sind Inhaltsdaten.

4. Auswirkungen des Kunsturheberrechts und des Privatrechts

Das unbefugte Aufnehmen und Verbreiten von Bildaufzeichnungen kann eine Straftat nach dem Kunsturheberrechtsgesetz sein. Nach § 23 Abs. 1 des Kunsturheberrechtsgesetzes dürfen ohne Einwilligung der Betroffenen Bilder nur veröffentlicht werden, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen. Die Beantwortung der Frage, ob eine mittels Webcam identifizierbar aufgenommene Person nur Beiwerk in Sinne des § 23 Abs. 1 des Kunsturheberrechtsgesetzes ist, hängt von den Umständen des Einzelfalls ab. Aus Gründen der Rechtssicherheit sollte in allen Fällen, in denen Aufnahmen mit Personenbezug möglich sind, über die Webcam informiert und die Einwilligung des Betroffenen zur Veröffentlichung eingeholt werden. Diese Einwilligung lässt sich mit der datenschutzrechtlichen Einwilligung verbinden.

Je nach Einzelfall sind eventuelle privatrechtliche Beschränkungen (allgemeines Persönlichkeitsrecht, Eigentumsrecht) zu beachten.

¹ Webcams für Benutzergruppen, die Nutzungsvereinbarungen unterliegen, oder reine Überwachungskameras, die das Internet lediglich als Übertragungsweg nutzen, werden hier nicht behandelt.

² Bearbeitungsstand 25. Januar 2001.

³ Entwurfassung der Bundesregierung vom 18. August 2000 (BDSG-E).

⁴ Diese Hinweise beziehen sich auf für die Allgemeinheit zugängliche Webcams und nicht auf Überwachungskameras (siehe Ziff.: 1).