RA Dr. Clemens Thiele, LL.M. Tax (GGU)

■ jusIT 2010/107, 219

Aktuelles zur Videoüberwachung – Erste Erfahrungen nach der DSG Novelle 2010, Teil 1

Die Videoüberwachung nach der DSG-Novelle 2010[1] unterscheidet zwischen der privaten und der hoheitlichen Videoüberwachung danach, ob ein öffentlicher oder privater Auftraggeber überwacht.[2] Der vorliegende Beitrag befasst sich mit ersten Praxiserfahrungen im Bereich der privaten Videoüberwachung, der geänderten StMV 2004 und versucht eine erste dogmatische Einordnung vorzunehmen.

Deskriptoren: Videoüberwachung, Datenschutz, Standard- und Musterverordnung 2004

Normen: DSG 2000: §§ 50a, 50b

1. Rechtmäßigkeit

Die Rechtmäßigkeit einer Videoüberwachung hat zunächst mit der Frage der Registrierung(spflicht) nichts zu tun. Die Rechtmäßigkeit, manchmal auch „datenschutzrechtliche Zulässigkeitsprüfung" genannt, stellt darauf ab, ob zumindest ein rechtmäßiger Zweck mit der Videoüberwachung verfolgt wird sowie auf das Vorliegen von Rechtfertigungsgründen, die notwendig sind, um in die geschützte Grundrechtsposition der Betroffenen einzugreifen.

1.1. Zweckgebundenheit

Gemäß § 50a Abs 2 DSG muss die Videoüberwachung einen *zulässigen* (rechtmäßigen, rechtlich anerkannten) *Zweck* erfüllen:

- Schutz des/der überwachten Objekts/Person (oder)
- Erfüllung rechtlicher Sorgfaltspflichten
- jeweils einschließlich der Beweissicherung

Dazu zählen der Schutz von Leben, Gesundheit und Eigentum sowie die Einhaltung rechtlicher Sorgfaltspflichten, bspw im Zusammenhang mit der Straßenverkehrsordnung oder der Arbeitnehmer-Sicherheit (zB Wegehalterhaftung). Mit diesen Zwecken verbunden und daher als zulässige Ziele der Videoüberwachung gelten auch Beweissicherungszwecke.

Während der Überwachung ist darauf zu achten, dass die in § 50a Abs 5 und 7 DSG genannten „*verbotenen Zwecke*" vermieden bzw nicht verfolgt werden:

- Eine Mitarbeiterkontrolle (im Sinne der Kontrolle der Arbeitsleistung) ist ausdrücklich verboten. Es kommt also hier allein auf die Zweckbestimmung an.[3]
- Die Überwachung eines höchstpersönlichen Bereiches, zB Toilettenanlagen, Schlafräume und dgl ist ebenfalls nicht gestattet.[4]
- Ein Datenabgleich, dh eine Weiterleitung der gewonnenen Daten an Dritte zum Zwecke des Vergleichs mit bereits bestehenden, ist unzulässig.[5] Die Weitergabe bei einer entsprechenden Verdachtslage an die Sicherheitsbehörden ist jedoch nach wie vor zulässig.

Praxistipp:

Die Datenschutzkommission prüft bei einer meldepflichtigen Videoüberwachung lediglich die Zweckgebundenheit.

1.2. Rechtfertigungsgründe für eine Videoüberwachung

In diesem Zusammenhang ist zu erwähnen, dass § 50a Abs 3 und 4 DSG Sonderbestimmungen zu den §§ 8, 9 DSG vorsehen, insoweit sie eigene Rechtfertigungsgründe für die private Videoüberwachung enthalten (mit anderen Worten: die Videoüberwachung darf keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzen). Diese liegen vor, wenn die Videoüberwachung erfolgt

- im lebenswichtigen Interesse einer Person;
- von einem Verhalten, das zweifelsfrei auf öffentliche Wahrnehmung gerichtet war;
- bei ausdrücklicher Zustimmung[6] des Betroffenen;
- in bloßer Echtzeitwiedergabe;
- in Wahrnehmung spezieller rechtlicher Sorgfaltspflichten[7];
- weil bestimmte Tatsachen die Annahme rechtfertigen, dass das/die überwachte Objekt/Person Ziel eines „gefährlichen Angriffs"[8] werden könnte, wie zB Vorfälle in der Vergangenheit, eine an sich erhöhte Gefährdung (zB hot spot oder bekannte Persönlichkeit) oder ein erheblicher Geldwert (zB Bank) oder künstlerischer Wert (zB Museum).

Bei der Aufstellung der Videokameras und Auswertung der Videoaufzeichnung ist darauf zu achten, dass die verbotenen Zwecke der Mitarbeiterkontrolle ebenso vermieden werden wie die (beiläufige) Überwachung eines höchstpersönlichen Bereichs. Ein Datenabgleich darf auf keinen Fall mit privaten Auftraggebern vorgenommen werden. Die Befugnisse der Sicherheitsbehörden bleiben davon unberührt.

1) BGBl I 135/2009, in Kraft seit 1. 1. 2010.
2) Vgl § 50a Abs 3 und Abs 4 DSG iVm § 50d Abs 2 DSG; vgl auch § 17 Abs 3 DSG.
3) § 50a Abs 5 Satz 2 DSG; dazu *Hattenberger*, Videoüberwachung in *Jahnel* (Hg), Jahrbuch 2010, 29; *Heilegger*, Novelle zum Datenschutzgesetz (DSG) 2010, infas 2010, 49; *Sabara*, Die Datenschutznovelle im Arbeitsrecht, ARD 6039/11/2010 jeweils mwN.
4) § 50a Abs 5 Satz 1 DSG; dazu *Hattenberger*, Videoüberwachung im Arbeitsverhältnis – im Besonderen: § 50a Abs 5 DSG in *Jahnel* (Hrsg), Datenschutzrecht Jahrbuch 2010 (2010) 29; *Heilegger*, infas 2010, 49; *Sabara*, ARD 6039/11/2010; jeweils mwN.
5) § 50a Abs 7 DSG; dazu *Pollirer/Weiss/Knyrim*, § 50a DSG Anm 13, die ein absolutes Verbot für praxisfremd halten.
6) Vgl § 4 Z 14 DSG.
7) ZB nach § 8 Sbg Veranstaltungsgesetz *„für die Erfüllung der im Bewilligungsbescheid vorgeschriebenen Auflagen"*.
8) Nach den EBRV 485 BlgNR 24. GP (abgedruckt in der Textausgabe *ProLibris*, DSG³ [2010] 196) ist der Begriff nicht iSd § 16 Abs 2 und 3 SPG zu verstehen, sondern eigenständig und weiter zu definieren, da auch Geschäfts- und Betriebsgeheimnisse geschützt werden bzw grobe Verwaltungsübertretungen die Gefährlichkeit begründen können.

1.3. Verhältnismäßigkeitsgrundsatz

Die private Videoüberwachung muss das *gelindeste Mittel der Überwachung* darstellen. So verdient zB eine codegeschützte Zutrittskontrolle zu einem Tresorraum den Vorzug gegenüber einer Bildüberwachung.

Gerade darin zeigt sich deutlich der allgemein datenschutzrechtliche Charakter der Videoüberwachung, die letztlich lediglich eine besondere Datenanwendung darstellt. Zu beachten sind jedenfalls die verfassungs- und europarechtlichen Vorgaben.[9)]

Praxistipp:

Im Hinblick auf den verfolgten Zweck muss von Fall zu Fall der Grundsatz der Verhältnismäßigkeit angewandt werden, der eine *Pflicht der Datenminimierung* bei den für die Verarbeitung Verantwortlichen beinhaltet.

2. Zulässigkeit

Grundsätzlich unterliegen alle Videoüberwachungen durch Private der Meldepflicht und der Vorabkontrolle nach § 17 Abs 1 iVm § 19 DSG. Dies bedeutet, dass eine private Videoüberwachung im Grundsatz erst dann vorgenommen werden darf, wenn die entsprechende technische Anlage von der Datenschutzkommission genehmigt und ggf unter Erteilung von Auflagen bescheidmäßig erlaubt worden ist. Das diesbezügliche Verfahren kann nach den bisherigen in anderen Vorabkontrollverfahren gemachten Erfahrungen durchaus Monate in Anspruch nehmen, wobei in der Praxis die als Erledigungsfrist konzipierte Prüfungsfrist des § 20 Abs 1 DSG von zwei Monaten zu einer bloßen „Reaktionsfrist" der DSK geführt hat.

Praxistipp:

Jedenfalls besteht aber eine *Kennzeichnungspflicht der Videoüberwachung*, die nach § 25 Abs 1 Satz 2 DSG nicht nur den Auftraggeber, sondern idR auch dessen DVR-Nummer nennen muss.

Eine entsprechende Antragstellung *vor* Inbetriebnahme der Anlage,[10)] in der sowohl das technische System, als auch der genaue Standort und die Art der Videoüberwachung dargelegt werden müssen, ist erforderlich, sofern nicht eine „nicht meldepflichtige Datenanwendung" nach § 17 Abs 2 DSG vorliegt. Die Meldung an die DSK erfolgt zum Zweck der Registrierung im DVR und dient der Publizität der Datenanwendung, insb der Gewährleistung des jedermann zustehenden Einsichtsrechts nach § 16 Abs 2 DSG. Die Anmeldung ist nach § 53 Abs 1 DSG gebührenfrei.

3. Geänderte Standard- und Musterverordnung 2004

3.1. Überblick

Sogenannte „Standard- oder Musteranwendungen" nimmt § 17 Abs 2 Z 6 DSG von der allgemeinen Vorabmeldepflicht des Auftraggebers aus. Dabei handelt es sich durch Verordnung des Bundeskanzlers[11)] um bestimmte Typen von Datenanwendungen, die massenhaft in gleichartiger Weise vorgenommen werden, wie zB Rechnungswesen, Personalverwaltung für privatrechtliche Dienstverhältnisse, Mitgliederverwaltung, Kundenbetreuung und Marketing für eigene Zwecke, Patientenverwaltung und Honorarabrechnung für Ärzte udgl. Derzeit sind 32 Standardanwendungen und fünf Musteranwendungen festgelegt.

Die DSG-Novelle 2010 sieht für bestimmte Anwendungen privater Videoüberwachung zB beim Eigentumsschutz von Einfamilienhäusern udgl die Möglichkeit vor, durch sogenannte „Standardanwendungen" generelle Ausnahmen von der Meldepflicht und damit der Vorabkontrolle vor. Dadurch würde eine sofortige Inbetriebnahme zulässig.

Eine entsprechende Verordnung zum Datenschutzgesetz ist mit der Novelle zur StMV 2004 nunmehr kundgemacht.[12)] Mit der Standardanwendung „*SA032 Videoüberwachung*" sind seit dem Inkrafttreten der Novelle am 28. Mai 2010 Videoüberwachungen für

(1) Banken,
(2) Juweliere, den Handel mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmiede,
(3) Trafiken,
(4) Tankstellen sowie
(5) bebaute Privatgrundstücke (samt Hauseingang und Garage)

von der Meldepflicht beim Datenverarbeitungsregister ausgenommen. Demzufolge lässt sich eine „geschäftsbezogene" oder „geschäftliche" Videoüberwachung im „*(beschränkt) öffentlichen Raum*" (1 bis 4) von einer solchen des „*privaten Raumes*" (5) unterscheiden.[13)]

3.2. Einschränkende Bedingungen der Standardanwendungen

3.2.1. Besondere Zweckgebundenheit

In den ersten vier der genannten Fälle des *(beschränkt) öffentlichen Raumes* ist weiter vorausgesetzt, dass es sich um eine verschlüsselte Videoüberwachung zum Zweck des Eigenschutzes (Schutz des Eigentums und Schutz der Mitarbeiter des Auftraggebers) und des Verantwortungsschutzes (Wahrnehmung von Verkehrssicherungspflichten, Vertragshaftung gegenüber Kunden etc) sowie zum Zweck der Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens, insoweit davon der Aufgabenbereich des Auftraggebers betroffen ist, mit ausschließlicher Auswertung in dem durch den Zweck definierten Anlassfall, handelt.

Für die Überwachung im *privaten Raum* kommen als berechtigte Zwecke lediglich Eigenschutz sowie die Verhinderung, Eindämmung und Aufklärung strafrechtlich relevanten Verhaltens in Betracht.

3.2.2. Erfasste Daten der Videoüberwachung

Als zu verarbeitende Datenarten (samt Historie) kommen in allen Fällen neben dem Ort[14)] und der Zeit[15)] der Bildaufzeichnung zunächst die Bilddaten[16)] der Betroffenen, die sich im überwachten Bereich aufhalten, in Betracht. Zusätzlich dürfen die Bilddaten von Personen aufgezeichnet werden, die im Rahmen der Videoüberwachung aufgenommen und im Anlassfall identifiziert werden. Von diesen dürfen sowohl deren Identität als auch deren Rolle (zB Täter, Opfer, Zeuge) aufgezeichnet werden, soweit diese aus der Aufzeichnung erkennbar sind.

9) Zu diesem Ineinandergreifen der drei Ebenen instruktiv *Jahnel*, Datenschutzrecht, Rz 1/21 f, 2/67 f.
10) Vgl § 18 DSG.
11) Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl II 312/2004 idF BGBl II 255/2009 und BGBl II 152/2010.
12) BGBl II 152/2010 in Kraft mit 28. 5. 2010; dazu bereits *Jahnel*, Gesetzgebungsmonitor Datenschutz: Meldefreiheit für bestimmte Videoüberwachungen, neue Standardvertragsklauseln, jusIT 2010, 141.
13) Vgl zur begrifflichen Unterscheidung den Anhang zum Datenschutzbericht 2005-2007, 64 ff, abrufbar unter http://www.dsk.gv.at/DocView.axd?CobId=30637 (11. 11. 2010).
14) Räumlichkeit, Standort der Kamera.
15) Datum, Uhrzeit, Beginn/Ende der Bildaufzeichnung.
16) Aussehen, Verhalten.

3.2.3. Protokollierungspflicht

Sowohl für die Überwachung des (beschränkt) öffentlichen als auch des privaten Raumes besteht nach § 50b Abs 1 DSG eine *Protokollierungspflicht* für den Auftraggeber für jeden Verwendungsvorgang, aus der die Betriebszeiten bzw Aufzeichnungszeiten und Speicherungen ersichtlich sind. Außer im Fall der Echtzeitüberwachung ist jeder Verwendungsvorgang von Bilddaten „lückenlos zu protokollieren".[17] Die Verpflichtung zur Protokollierung umfasst mE demnach nicht nur die Aufzeichnung der überwachten Ereignisse selbst, sondern auch die Zugriffe und Auswertungen, dh

- die Einrichtung und die per Einstellung aktivierten Funktionen der Anlage zu dokumentieren;
- die Betriebstätigkeit an den Anlagesystemen in einem Logbuch festzuhalten;
- den Zugriff auf gespeicherte Daten zu Auswertungszwecken oder zur Überprüfung der Funktionsfähigkeit zu dokumentieren;
- Zugriffe auf Bilddaten unter Angabe der Person und des Anlasses in geeigneter, dh nachvollziehbarer und dauerhafter Form festhalten;
- alle Auswertungen in einem Protokoll festzuhalten, aus dem hervorgeht, wer wann aus welchem Anlass und auf welche Speichermedien zugegriffen hat.

Die jeweilige Nutzung ist schriftlich zu fixieren. Aus dem Aspekt der Datensicherheit folgt, dass der Auftraggeber sicherzustellen hat, dass die aufgezeichneten (Bild-)Daten nicht verändert werden können. Der Zugriff muss beschränkt werden. Einem Teil der Lehre[18] ist demnach darin beizupflichten, dass der Betreiber zweckmäßigerweise eine Videoüberwachungsordnung zu erstellen hat.

3.2.4. Höchstdauer der zulässigen Datenaufbewahrung

Die Videodaten sind in allen Fällen spätestens nach 72 Stunden zu löschen; es gilt die Regel des § 50b Abs 2 Satz 2 DSG, wonach § 33 Abs 2 AVG auf die Fristenberechnung anzuwenden ist. Fällt demnach das Ende der Aufbewahrungsfrist auf einen Samstag, Sonntag, gesetzlichen Feiertag oder den Karfreitag, so ist der nächste Werktag letzter Tag der Frist.

Praxistipp:

Eine *längere Löschungsfrist* erfordert jedenfalls eine Vorabgenehmigung durch die DSK und ist im Antragsverfahren entsprechend zu begründen.

3.2.5. Zulässige Empfängerkreise

Die durch eine Videoüberwachung gewonnenen Daten dürfen ausschließlich im Anlassfall in den Fällen (2) bis (5) an Sicherheitsbehörden, Staatsanwaltschaft, Gerichte und Versicherungen weitergegeben werden. Bei Videoüberwachungen in Banken (1) kommen zusätzlich noch die Kontoinhaber und die kontoführende Bank in Betracht.

3.3. Überwachung privater Räume

3.3.1. Bebautes Privatgrundstück

Den insoweit einzig von der Vorabkontrolle ausgenommenen privaten Raum definiert die SA032 in ihrem Abschnitt E als *„ein bebautes, in der Verfügungsbefugnis des Auftraggebers stehendes Privatgrundstück (samt Hauseingang und Garage), welches der privaten Nutzung des Auftraggebers und der mit dem Auftraggeber gemeinsam im Haus lebenden Personen dient und zu dessen Betreten außer dem Auftraggeber und der mit dem Auftraggeber gemeinsam im Haus lebenden Personen grundsätzlich niemand berechtigt ist"*.

Die durch den letzten Halbsatz[19] getroffene Einschränkung macht zunächst deutlich, dass es sich um einen privaten Raum handelt, der insoweit vom bloß nichtöffentlichen Raum iSd bisherigen Unterscheidung[20] abgegrenzt wird.

Nach allgemeinem Begriffsverständnis erfasst ein *„Privatgrundstück"* ein nicht beruflichen, geschäftlichen oder dienstlichen Zwecken[21] dienendes Stück Land, maW aus datenschutzrechtlicher Perspektive eine nichtöffentliche Liegenschaft. Aus dem Klammereinschub (*„samt Hauseingang und Garage"*) sowie aus der beigefügten Eigenschaft *„bebautes"* wird deutlich, dass es sich beim überwachten Privatraum um eine Liegenschaft samt der darauf befindlichen (iS von betretbaren) Bauwerke handeln muss. Aus *„der im Wege einer Zutrittskontrolle zum Gebäude vorgenommenen Videoüberwachung"* ist abzuleiten, dass lediglich die äußeren Bereiche des Gebäudes überwacht werden dürfen, also zB der Hauseingang, das Gartentor, die Zu- oder Einfahrt, nicht hingegen der Innenbereich, wie zB Wohnungseingangstüren, das Treppenhaus oder die Gänge.[22]

Als weitere Einschränkung muss das Grundstück *„der privaten Nutzung des Auftraggebers und der mit dem Auftraggeber gemeinsam im Haus lebenden Personen"* dienen. Nach allgemeinem Sprachverständnis scheidet damit ein rein beruflicher, geschäftlicher oder dienstlicher Gebrauch aus. Verwendet der Auftraggeber die Liegenschaft zur Deckung seines Wohnbedarfs oder zu Erholungs- bzw Freizeitzwecken,[23] dann schadet mE selbst eine untergeordnete geschäftliche Verwendung eines Teils, wie zB die Einrichtung eines Arbeitszimmers in einem Wohnhaus, nicht. Die Privatheit ist letztlich wiederum als Gegenbegriff zur Öffentlichkeit auszulegen, sodass die nicht-öffentliche Verwendung der bebauten Liegenschaft im Vordergrund steht.

Dieses Tatbestandselement der Privatheit grenzt allerdings auch die *Person des Auftraggebers* ab. Offensichtlich hat Abschnitt E die Videoüberwachung für ein Einfamilienhaus zum Vorbild, die vom privaten Eigentümer durchgeführt wird. Diese ist im Wesentlichen unproblematisch und durch die SA032 gedeckt. Unproblematisch ist auch die Videoüberwachung durch den Mieter eines ganzen Einfamilienhauses, da die Verfügungsbefugnis nicht mit der Eigentümerschaft gleichzusetzen ist.

Denkbar ist allerdings auch die Videoüberwachung eines ganzen Hauses mit verschiedenen Mietern – die Zustimmung[24] aller im Mietshaus lebenden Personen vorausgesetzt –, wenn der Vermieter eine natürliche Person ist[25] und zugleich im Haus wohnt, denn in seiner „Verfügungsbefugnis" als Eigentümer und Vermieter steht das ausschließlich zu Wohnzwecken genutzte Privathaus. Demgegenüber scheiden bloße Wohnungseigentümer oder Mieter als Auftraggeber

17) EBRV 485 BlgNR 24. GP, abgedruckt in der Textausgabe *ProLibris*, DSG[3] (2010), 198 f; *Pollirer/Weiss/Knyrim*, DSG § 50b Anm 1.

18) *Pollirer/Weiss/Knyrim*, DSG § 50b Anm 1.

19) *„…und zu dessen Betreten außer dem Auftraggeber und der mit dem Auftraggeber gemeinsam im Haus lebenden Personen grundsätzlich niemand berechtigt ist"*.

20) Dazu *König*, Videoüberwachung, in *Bauer/Reimer* (Hg), Handbuch Datenschutzrecht (2009), 315, 330.

21) Vgl *Duden*, Deutsches Universalwörterbuch, 975 lSp zur Bedeutung von „privat".

22) Dies ist auch aus persönlichkeitsrechtlichen Überlegungen idR unzulässig vgl OGH 30. 1. 1997, 6 Ob 2401/96y, MR 1997, 150 = NZ 1998, 173 = SZ 70/18 = MietSlg 49.002 = immolex 1997/71 = ImmZ 1997, 214; 14. 5. 1997, 7 Ob 89/97g, JBl 1997, 641 = EWr III/16 A/1 ff = MietSlg 49.003 = immolex 1997/174.

23) ZB ein Ferienhaus, ein Bootshaus, eine Jagdhütte oder eine Alm.

24) Dazu gleich unten 3.3.2.

25) Bei einer juristischen Person, zB einer GmbH, fehlt es idR an der privaten Nutzung.

einer Videoüberwachung nach Abschnitt E der SA032 aus, da sie nicht über das (ganze) Privatgrundstück (samt Hauseingang und Garage) rechtlich verfügungsbefugt sind, sondern über bloße einzelne Teile des Hauses bzw ihre zugewiesenen Wohnräumlichkeiten.

3.3.2. Zustimmung aller Hausgenossen

Bei einer Videoüberwachung eines bebauten Privatgrundstücks gilt darüber hinaus die Besonderheit, dass die „*Zustimmung aller mit dem Auftraggeber gemeinsam im Haus lebenden Personen*" vorliegen muss. Für die Wirksamkeit einer derartigen Zustimmung ist grundsätzlich an § 4 Z 14 DSG anzuknüpfen.[26] Es besteht selbstverständlich eine jederzeitige Möglichkeit die Zustimmung zu widerrufen, auch ohne Angabe von Gründen.[27]

Erforderlich ist die gültige, insbesondere ohne Zwang abgegebene *Willenserklärung*[28] des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt.[29] „In Kenntnis der Sachlage" erfordert eine Aufklärung über Umfang der Datenarten, Inhalt der Daten, Zweck der Datenweitergabe sowie Empfänger der Daten und zwar so detailliert, dass der Betroffene die konkreten Empfänger erkennen kann.[30] Die konkrete Verwendung ergibt sich aus der Überwachung des privaten Raumes. Die Zustimmung muss zu einer „*im Wege einer Zutrittskontrolle zum Gebäude vorgenommenen Videoüberwachung*" eingeholt werden.

Wegen der zu verarbeitenden Bilddaten, die idR sensible Daten iSd § 4 Z 2 DSG darstellen, hat die Zustimmung gem § 9 Z 6 DSG *ausdrücklich* zu erfolgen. Dies bedeutet, dass eine Erklärung durch schlüssiges Handeln – abweichend von der allgemeinen Regelung in § 8 Abs 1 Z 2 DSG – nicht ausreicht. Eine Schriftlichkeit ist für die Zustimmungserklärung nicht erforderlich, jedoch empfehlenswert.

Aufgrund der jederzeitigen Widerrufbarkeit der datenschutzrechtlichen Zustimmung kann bei Ablehnung auch nur durch einen Hausgenossen die Überwachungsmaßnahme nicht mehr „im vereinfachten Verfahren" nach § 17 Abs 2 Z 6 DSG durchgeführt werden.

Zu beachten ist schließlich, dass die datenschutzrechtliche Zustimmung höchstpersönlicher Natur ist.[31] Auf eine Geschäftsfähigkeit iSd § 865 ABGB oder gar ein bestimmtes Alter des Betroffenen abzustellen, ist mE verfehlt. Es kommt demgegenüber gerade bei im Haushalt lebenden minderjährigen oder besachwalteten Personen darauf an, ob diese kognitiv in der Lage sind, die Überwachung und deren Einfluss auf ihren Alltag abzuschätzen.[32] Liegen diese persönlichen Voraussetzungen im Einzelfall vor, kann eine wirksame Zustimmung von dem Betroffenen abgegeben werden.

Anmerkung:

Lesen Sie die Fortsetzung des Beitrags in jusIT 1/2011.

26) Statt vieler *Jahnel*, Datenschutzrecht Rz 3/130 ff mwN.

27) Vgl OGH 20. 3. 2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*); 20. 3. 2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*).

28) Vgl §§ 861, 869 ABGB.

29) OGH 22. 3. 2001, 4 Ob 28/01y – *Creditanstalt*, ÖBA 2001/977, 645 (*Koziol*) = ecolex 2001/147, 438 (*Rabl*) = RdW 2001/557, 531 = SZ 74/52 = ÖBA 2004, 737 (*Apathy*) = KRES 1h/31.

30) Vgl *Knyrim*, Datenschutzrechtliche Zustimmungserklärungen in *Knyrim/Leitner/Perner/Riss*, Aktuelles AGB-Recht (2008) 133, 138.

31) Statt vieler *Jahnel*, Datenschutzrecht Rz 3/143 ff mwN.

32) Ähnlich zur Zustimmungsproblematik beim höchstpersönlichen Recht am eigenen Bild nach § 78 UrhG *Dokalik*, „Mein Baby ist ein Star!" – Zum Recht des Kindes am eigenen Bild, FamZ 2006, 4,7, der mit überzeugenden Argumenten von einer individuellen Beurteilung ausgeht.

Der Autor:
RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), studierte US-amerikanisches Steuerrecht in San Francisco; Gründer der RA-Kanzlei EUROLAWYER® in Salzburg; Fachbuch-Autor; Verfasser des Standardkommentars zum Werbeabgabegesetz (2000); gerichtlich beeideter Sachverständiger für Urheberfragen aller Art, insb Neue Medien und Webdesign.

Publikationen des Autors (Auszug):
Rechtssichere Verwendung von Schutzzeichen, RdW 2010/568, 557; Zero Intern – Rechtswidrige AGBs als Lauterkeitsverstoß, RdW 2010/424, 388; Urheberrecht und Erben, in: *Bogendorfer/Ciresa* (Hrsg), Urheberrecht (2009) 51; Co-Autor in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Salzburger Kommentar zum Strafgesetzbuch.