

Zeitgemäßer Datenschutz

Am 1. Jänner 2010 ist die Datenschutzgesetzes-Novelle 2010 in Kraft getreten. Es gibt wesentliche Änderungen im Datenschutzrecht, insbesondere eine Regelung der privaten Videoüberwachung.

Das Datenschutzgesetz 2000, BGBl I 1999/165, ist in den vergangenen zehn Jahren seit seinem Inkrafttreten am 1. Jänner 2000 nur wenig geändert worden. Mit Ministerialentwurf 182/ME 23. GP wurde ein Begutachtungsverfahren zu einer DSGVO-Novelle 2008 (mit beabsichtigtem Inkrafttreten am 1.8.2008) eingeleitet, das schließlich zur Regierungsvorlage der DSGVO-Novelle 2010, RV 472 BlgNR 24. GP, geführt hat. In diese nicht übernommen wurden die im Ministerialentwurf vorgesehenen Bestimmungen über die Bestellung eines betrieblichen Datenschutzbeauftragten.

Die Regierungsvorlage, die am 17.11.2009 im Nationalrat eingelangt ist, wurde im Zuge der parlamentarischen Beratungen nur wenig verändert und ist, unter Ausklammerung jener Bestimmungen, die, als Verfassungsbestimmungen, einer Zwei-Drittel-Mehrheit bedürft hätten, in die DSGVO-Novelle 2010 übernommen worden. Diese wurde unter BGBl I 2009/133 veröffentlicht und ist am 1. Jänner 2010 in Kraft getreten, zusammen mit den Änderungen, die sich durch Art. 37 des Eingetragene Partnerschaft-Gesetz – EPG, BGBl I 2009/135, in § 48a Abs. 5 DSGVO ergeben haben (Einfügung der Wortfolge „eingetragene Partner“ nach „Ehegatten“).

Die verfassungsgesetzlichen Bestimmungen hätten im Wesentlichen eine alleinige Kompetenz des Bundes zum Schutz personenbezogener Daten begründet und hiezu bestehende landes-



Private Videoüberwachung: Konkretere Regelungen in der Datenschutzgesetzes-Novelle 2010.

rechtliche Vorschriften außer Kraft gesetzt (vornehmlich hinsichtlich manuell geführter Dateien, § 58 DSGVO).

Die Schwerpunkte der Novelle liegen in Neuerungen im Verfahren zur Registrierung und bei der Richtigstellung des Registers; der Neugestaltung des Verfahrens zur Überprüfung der Erfüllung der Meldepflicht; begleitenden Maßnahmen im Beschwerdeverfahren und in einer Regelung der Videoüberwachung durch Private (9a. Abschnitt).

Registrierung. Soweit Datenanwendungen meldepflichtig sind (ausgenommen sind nach § 17 Abs. 2 DSGVO u. a. Standardanwendungen nach der Standard- und Musterverordnung 2004 sowie die in § 17 Abs. 3 aufgezählten, im öffentlichen Interesse begründeten Ausnahmen), hat der Auftraggeber wie bisher eine Meldung an das von der Datenschutzkommission zu führende Datenverarbeitungsregister (DVR) zu erstatten. Die Meldepflicht besteht auch für Umstände, die nachträglich die Unrichtigkeit und Unvoll-

ständigkeit einer Meldung bewirken (Änderungsmeldung).

Meldungen an das DVR können nur mehr in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung eingebracht werden. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte erfolgen. Eine Meldung per E-Mail oder in nicht elektronischer Form ist (nur mehr) für manuelle Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig (§ 17 Abs. 1a). Als längeren technischen Ausfall bezeichnet die RV einen solchen von mindestens 48 Stunden.

Neu ist auch, dass der Auftraggeber selbst zu beurteilen hat, ob die zu registrierende Datenanwendung der Vorabkontrolle unterliegt (§ 18 Abs. 2 sowie, in Bezug auf Videoüberwachung, § 50c Abs. 1 2. Satz DSGVO) oder nicht. Eine entsprechende Erklärung ist, neben den sonst erforderlichen, in § 19 Abs. 1 Z 1 bis 7 DSGVO angeführten Angaben, in die Meldung an das

DVR aufzunehmen (neue Z 3a).

Wird eine Erklärung dahingehend abgegeben, dass keine Vorabkontrollpflicht (nach den Tatbeständen des § 18 Abs. 2 Z 1 bis 4) gegeben ist, wird das Registrierungsverfahren vollautomatisch durchgeführt, wobei nur eine Prüfung auf Vollständigkeit und Plausibilität der Angaben erfolgt. Ist demnach die Meldung nicht fehlerhaft, ist sie sofort zu registrieren (§ 20 Abs. 1). Der Umstand, dass der Meldungsinhalt nur automatisonsunterstützt geprüft wurde, ist in der Registrierung zu vermerken (§ 21 Abs. 5). Unmittelbar nach Abgabe einer derartigen Meldung darf der Vollbetrieb der meldepflichtigen Datenanwendung aufgenommen werden (§ 18 Abs. 1).

Eine Absicherung dagegen, dass Datenanwendungen in der Meldung fälschlich als nicht der Vorabkontrolle unterliegend bezeichnet werden, bildet § 30 Abs. 2a DSGVO, wonach bei behaupteten Verstößen oder bei begründetem Verdacht auf Verletzung der Meldepflicht die Datenschutzkommission die Erfüllung der Meldepflicht überprüfen und Berichtigungen des DVR oder Streichungen aus diesem durchführen kann. Nach dem neu formulierten § 52 Abs. 2 Z 1 DSGVO ist das Betreiben einer Datenanwendung auf eine von der Meldung abweichende Weise eine mit Geldstrafe bis zu 10.000 Euro zu bestrafende Verwaltungsübertretung.

Neu ist auch, dass der Auftraggeber sich bereits bei Einbringung der Meldung oder danach bis zum Ab-

POWERSERV® AUSTRIA

Arbeit nach Maß
23 Jahre Erfahrung für Sie!
45x in Österreich. In 10 Ländern.



Aktuelle Jobangebote finden Sie unter:
www.powerserv.at | Jobline ☎ 059 007

WWW.MARIA-MARDINI.COM

Der LUXUS-EINKAUFWS-WEBSHOP

10% - 15% PREISNACHLASS f. POLIZEIBEAMTE!!



für exklusive Geschenke und Produkte!

**Geburtstage, Hochzeitstage, Weihnachten,
Pensionierungen, Maturageschenke, etc... :**

Sie wissen nicht was Sie schenken sollen?
Besuchen Sie uns im Webshop!

**Kristalle, Sonnenbrillen, Designerwaren, Schmuck,
Parfums, hochwertigste Kosmetik,
u.v.m...**

10% - 15% PREISNACHLASS f. POLIZEIBEAMTE!!

Maria Mardini © - Design & Luxusartikel !



Maria Mardini© steht für aussergewöhnliches Design,
new lifestyle, hochwertige Luxusgüter und Qualität!

Maria Mardini,EU© | Liniengasse 50-52/1/12 | 1060 Wien
www.maria-mardini.com | office@maria-mardini.com

DATENSCHUTZRECHT

schluss des Registrierungsverfahrens verpflichtet kann, sich beim Betrieb der Datenanwendung bestimmten Auflagen oder Bedingungen zu unterwerfen oder die Datenanwendung nur befristet zu betreiben. Mit der Registrierung werden diese Zusagen rechtsverbindlich (§ 19 Abs. 2). Zu erwartende Vorschreibungen der Datenschutzkommission können somit vorweggenommen werden, was im Interesse sowohl der Verfahrens- als auch der Verwaltungsökonomie liegt.

Wird bei der automatisierten Prüfung ein Fehler der Meldung festgestellt, ist dem Auftraggeber die Möglichkeit zur Verbesserung einzuräumen. Gleichzeitig ist er darauf hinzuweisen, dass die Meldung als nicht eingebracht gilt, wenn keine Verbesserung erfolgt oder er auf die Einbringung der unverbesserten Meldung besteht. In diesem Fall kann er die Meldung schriftlich der Datenschutzkommission übermitteln (§ 20 Abs. 2).

Diese überprüft sie auf Mangelhaftigkeit so wie jene, die von vornherein als vorabkontrollpflichtig bezeichnet wurden oder nicht über das Internet eingebracht worden sind. Bei Vorliegen von Mangelhaftigkeit wird dem Auftraggeber innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung unter Setzung einer angemessenen Frist aufgetragen (§ 20 Abs. 4). Wird diesem Auftrag nicht entsprochen, wird die Registrierung der Meldung durch eine schriftliche Mitteilung abgelehnt. Ein Bescheid ist nur dann zu erlassen, wenn dies innerhalb von zwei Wochen ab Zustellung der Mitteilung beantragt wird (§ 20 Abs. 5).

Ergibt das Prüfungsverfahren keine Fehlerhaftigkeit, wurden die Verbesserungen durchgeführt oder sind nach Einlangen einer

auf Mangelhaftigkeit zu prüfenden Meldung bei der Datenschutzkommission zwei Monate verstrichen, ohne dass ein Verbesserungsauftrag erteilt wurde, ist die Registrierung durchzuführen und der Auftraggeber hievon und vom Inhalt der Registrierung zu verständigen. Bei erstmaliger Registrierung ist ihm eine Registernummer zuzuteilen (§ 21).

Änderungen des Registers oder Streichungen aus diesem sind auf Grund einer Änderungsmeldung durchzuführen oder von Amts wegen, etwa dann, wenn der Datenschutzkommission aus amtlichen Verlautbarungen Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers zur Kenntnis gelangen oder der Wegfall seiner Rechtsgrundlage (§ 22 Abs. 2). Rechtsnachfolger eines registrierten Auftraggebers können Meldungen des Rechtsvorgängers durch entsprechend glaubhaft gemachte Erklärung gegenüber der Datenschutzkommission übernehmen (§ 22 Abs. 4).

Meldepflicht. Wie ausgeführt, kann die Datenschutzkommission jederzeit die Erfüllung der Meldepflicht durch einen Auftraggeber überprüfen, was auch für rechtswidrig unterlassene Meldungen gilt. Das entsprechende Verfahren wird durch eine begründete Verfahrensordnung eingeleitet, mit einer Aufforderung zur Verbesserung einer registrierten Meldung oder einer Aufforderung zur Nachmeldung innerhalb einer Frist. Wird dem Verbesserungsauftrag nicht entsprochen, wird mit Bescheid die Streichung der Meldung oder auch nur von Teilen davon verfügt. Eine Streichung ist auch zu verfügen, wenn mit Bescheid festgestellte Mängel bei Datensicherheitsmaßnahmen nicht innerhalb angemessener Frist be-

hoben worden sind. Wird einer Aufforderung zur Nachmeldung nicht entsprochen, wird mit Bescheid der Datenschutzkommission der weitere Betrieb der Datenanwendung untersagt und gleichzeitig Anzeige nach § 52 Abs. 2 Z 1 DSGVO erstattet (§ 22a Abs. 4).

Beschwerdeverfahren.

Die Ausübung des – verfassungsgesetzlich (§ 1 Abs. 3 Z 1) gewährleisteten – Rechts auf Auskunft, wer welche Daten über den Auskunftswerber verarbeitet, woher die Daten stammen und wozu sie verwendet werden, insbesondere an wen sie übermittelt werden, ist in § 26 DSGVO einfachgesetzlich näher ausgeführt.

An die Datenschutzkommission kann sich wenden, wer behauptet, in diesem Recht verletzt worden zu sein – gleichgültig, ob der Auftraggeber in Vollziehung der Gesetze tätig geworden ist oder sich der Anspruch gegen private Rechtsträger richtet (§ 31 Abs. 1).

Verletzungen der – ebenfalls verfassungsgesetzlich gewährleisteten (§ 1 Abs. 1 und 3 Z 2) – Rechte auf Geheimhaltung, Richtigstellung oder Löschung sind im privaten Bereich auf dem Zivilrechtsweg geltend zu machen (§ 32 Abs. 1), und zwar durch Klage beim Landesgericht, in dessen Sprengel der Kläger (Antragsteller) oder, fakultativ, der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz hat (§ 32 Abs. 4). Die Datenschutzkommission erkennt über behauptete Verletzungen der angeführten Rechte nur dann, wenn die Verletzungen in Vollziehung der Gesetze erfolgt sind (§ 31 Abs. 2). Allenfalls hat sie einem Zivilverfahren als Nebenintervenient beizutreten, wenn ein Einschreiter dies verlangt und dies zur Wahrung der nach dem DSGVO geschützten Interessen einer

größeren Zahl von natürlichen Personen geboten ist (§ 33 Abs. 6).

Das Beschwerdeverfahren wurde nach dem Muster des § 67c Abs. 2 AVG formalisiert, und zwar durch Aufzählung jener Mindestanforderungen, die eine Beschwerde zwingend zu enthalten hat (§ 31 Abs. 3 Z 1 bis 6). Die gestellten Anträge auf Auskunft, Richtigstellung oder Löschung und die allfälligen Antworten des Beschwerdegegners sind anzuschließen. Wenn sich eine Beschwerde als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ansonsten ist die Beschwerde abzuweisen (§ 31 Abs. 7). Wenn der Beschwerdegegner im Verfahren die behauptete Rechtsverletzung beseitigt und die Beschwerde dadurch als gegenstandslos erscheint, hat die Datenschutzkommission das Verfahren nach vorheriger Anhörung des Beschwerdeführers formlos einzustellen (§ 31 Abs. 8).

Informationsverpflichtung. Eine weitere Neuerung besteht darin, dass ein Auftraggeber die Betroffenen unverzüglich in geeigneter Form zu informieren hat, wenn ihm bekannt wurde, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden und den Betroffenen Schaden droht. Diese Verpflichtung besteht nicht, wenn die Information angesichts der Drohung eines nur geringfügigen Schadens der Betroffenen einerseits oder der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert (§ 24 Abs. 2a). – Die Regierungsvorlage geht davon aus, dass ein gänzliches Absehen von der Information angesichts der Möglichkeit der Information durch Medi-

KENT RESTAURANT

**Täglich von 6 bis 2 Uhr früh
KEIN RUHETAG
Gastgarten von 9 bis 22 Uhr geöffnet**

Brunnengasse 67
1160 Wien

☎ 405 91 73 Fax: 405 91 73 74

kent_restaurant@gmx.at
www.kent-restaurant.at

Cafè Central

Inh. Zemann Franziska



Geöffnet von
Mo bis Sa von 08-02 Uhr
Sonntag von 14-02 Uhr

1110 Wien
Simmeringer Hauptstraße 50
Tel. 01/749 32 71
Mobiltel. 0664/520 49 11

en eine eher in nur besonderen Fällen in Anspruch zu nehmende Ausnahme bleiben wird.

Videouberwachung. Der neu in das DSGVO eingefügte Abschnitt 9a. (§§ 50a bis 50e) regelt vornehmlich die Videouberwachung durch Private. Videouberwachung im Sinn dieses Abschnittes definiert § 50a Abs. 1 allgemein als die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte. – Tonaufnahmegeräte („Lauschangriffe“) werden nicht erfasst (RV).

Die Grundsätze für die Verwendung von Daten (§§ 6 und 7) gelten auch für die Videouberwachung, insbesondere der Verhältnismäßigkeitsgrundsatz des § 7 Abs. 3. Rechtmäßige Zwecke einer Videouberwachung, insbesondere der Auswertung und Übermittlung der dabei ermittelten Daten, sind jedoch nur der Schutz des überwachten Objekts oder der überwachten Person oder die Erfüllung

rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung (§ 50a Abs. 2).

Ein von einer Videouberwachung Betroffener wird nach § 50a Abs. 3 dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt,

1. wenn diese im lebenswichtigen Interesse einer Person erfolgt,

2. Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden [Beispiel in der RV: Straßentheater], oder

3. er der Verwendung seiner Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat.

Durch die Videouberwachung Privater (also nicht im Rahmen der Vollziehung hoheitlicher Aufgaben erfolgend) wird ein Betroffener nach § 50a Abs. 4 weiters dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen (§ 7 Abs. 2 Z 3) verletzt, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines

gefährlichen Angriffs werden, oder

2. unmittelbar anwendbare Rechtsvorschriften des Völker- oder des Gemeinschaftsrechts, Gesetze, Verordnungen, Bescheide oder gerichtliche Entscheidungen dem Auftraggeber spezielle Sorgfaltspflichten zum Schutz des überwachten Objekts oder der überwachten Person auferlegen, oder

3. in Fällen der Echtzeitüberwachung, die zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt.

Mit einer Videouberwachung nach Abs. 4 dürfen nicht Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen. Weiters ist die Videouberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt (§ 50a Abs. 5). Was die Kontrolle von Arbeitnehmern durch technische Systeme betrifft, ist auch auf die §§ 96 und 96a ArbVG zu verweisen.

Mit Videouberwachung aufgezeichnete Daten dürfen nach § 50a Abs. 6 ferner, ohne dass schutzwürdige Geheimhaltungsinteressen Betroffener verletzt werden,

1. an die zuständige Behörde oder das zuständige Gericht übermittelt werden, weil beim Auftraggeber der begründete Verdacht entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder

2. an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs. 5 des SPG eingeräumten Befugnisse,

auch wenn sich die Handlung oder der Angriff nicht gegen das überwachte Objekt oder die überwachte Person richtet. Die Befugnisse von Behörden und Gerichten zur Durchsetzung der Herausgabe von Beweismaterial und zur Beweismittelsicherung sowie damit korrespondierende Verpflichtungen des Auftraggebers bleiben unberührt.

Mit einer Videouberwachung gewonnene Daten von Betroffenen dürfen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden (§ 50a Abs. 7).

Jeder Verwendungsvorgang einer Videouberwachung ist zu protokollieren. Aufgezeichnete Daten sind,

DATENSCHUTZ-GESETZESNOVELLE 2010

Straftatbestände

Der gerichtliche Straftatbestand des § 51 DSGVO wurde, durch Streichung des § 51 Abs. 2 DSGVO alte Fassung, von einem Ermächtigungsdelikt zu einem Officialdelikt umgestaltet. Die Strafverfolgung ist nunmehr von Amts wegen durchzuführen.

Zudem wurde der Tatbestand dahingehend erweitert, dass von der subjektiven Tatseite her nunmehr statt *Absicht* bereits der (allenfalls bedingte) *Vorsatz* ausreicht, sich oder einen Dritten un-

rechtmäßig zu bereichern (§ 51 1. Fall). Absicht wird nur mehr gefordert beim 2. Fall des Tatbestands, nämlich einen anderen in seinem Geheimhaltungsanspruch zu schädigen. Dass dem Betroffenen ein Nachteil zugefügt wird (§ 51 Abs. 1 a. F.), ist nicht mehr Tatbestandsmerkmal. Bloßes „Schnüffeln“ in personenbezogenen Daten reicht also zur Erfüllung des Tatbestands aus, wenn die weiteren Tathandlungen gesetzt werden. Diese Tathandlungen bestehen darin, dass der Täter personenbezogene

Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.

Strafbestände. Die Tat ist wie bisher vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen. Der Strafrahmen für die unverändert

gebliebenen Tatbestände der Verwaltungsübertretungen nach § 52 Abs. 1 DSGVO wurde auf 25.000 Euro angehoben, jener für die neu gefassten des § 52 Abs. 2 auf 10.000 Euro.

Wer Daten entgegen den §§ 26, 27 oder 28 nicht fristgerecht beauskunftet, richtigstellt oder löscht, begeht nunmehr, sofern kein mit strengerer Strafe bedrohtes Delikt vorliegt, nach § 52 Abs. 2a eine Verwaltungsübertretung, die mit einer Strafe bis zu 500 Euro zu ahnden ist.



Videüberwachung durch Private: Die Kennzeichnung muss so erfolgen, dass der Auftraggeber eindeutig hervorgeht und dass jeder potenziell Betroffene die Möglichkeit hat, der Videüberwachung auszuweichen.

sofern sie nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- oder Beweissicherungszwecke oder zur Anzeigeerstattung benötigt werden, spätestens nach 72 Stunden zu löschen. § 33 Abs. 2 AVG gilt, dass also dann, wenn das Ende dieser Frist auf einen Samstag, Sonntag, gesetzlichen Feiertag oder den Karfreitag fällt, der nächste Werktag letzter Tag der [anzunehmen: noch verbleibenden Stunden-] Frist ist.

Videüberwachungen unterliegen der Meldepflicht, ausgenommen Echtzeitüberwachungen und wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Medium erfolgt (§ 50c Abs. 2). Der Vorabkontrolle unterliegen Videüberwachungen dann, wenn der Auftraggeber nicht in der Meldung zusagt, die Videüberwachungsdaten zu verschlüsseln und unter Hinterlegung des einzigen Schlüssels bei

der Datenschutzkommission sicherstellt, dass eine Auswertung der Videoaufzeichnungen nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet (§ 50c Abs.1).

Echtzeitüberwachung. Eine Echtzeitüberwachung liegt nach § 50a Abs. 4 Z 3 vor, wenn sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignisse erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet werden.

Ein von dieser Form der Videüberwachung Betroffener ist

- in seinen schutzwürdigen Geheimhaltungsinteressen nicht verletzt (§ 50a Abs. 4 Z 3; die RV begründet dies damit, dass ihr Zweck nicht in der Beweissicherung, sondern in der Einleitung von Sofortmaßnahmen liegt),

- es besteht keine Meldepflicht (§ 50c Abs. 2),
- ein Auskunftsrecht ist ausgeschlossen (§ 50e Abs. 3).

Auskunftsrecht. Ein Auskunftswerber hat zunächst den Zeitraum, in dem er möglicherweise von der Überwachung betroffen war, und den Ort möglichst genau zu benennen und seine Identität nachzuweisen. Die Auskunft über die zu seiner Person verarbeiteten Daten ist ihm dann durch Übersendung einer Kopie der zu seiner Person verarbeiteten Daten in einem üblichen technischen Format zu gewähren. Alternativ kann der Auskunftswerber eine Einsichtnahme auf Lesegeräten des Auftraggebers verlangen, wobei ihm auch in diesem Fall die Ausfolgung einer Kopie zusteht. Die übrigen Bestandteile der Auskunft (verfügbare Informationen über die Herkunft, Empfänger oder Empfängerkreise von Übermittlungen, Zweck,

Rechtsgrundlagen sowie allenfalls Dienstleister) sind auch im Fall der Überwachung schriftlich zu erteilen, wenn nicht der Auskunftswerber einer mündlichen Auskunftserteilung zustimmt (§ 50e Abs. 1).

Kennzeichnung. Der Auftraggeber einer Videüberwachung (ausgenommen solche, die nach § 17 Abs. 3 wegen übergeordneter öffentlicher Interessen von der Meldepflicht ausgenommen sind) hat diese zu kennzeichnen. Aus der Kennzeichnung hat der Auftraggeber eindeutig hervorzugehen, es sei denn, dieser ist den Betroffenen nach den Umständen des Falles bereits bekannt. Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potenziell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, die Möglichkeit hat, der Videüberwachung auszuweichen (§ 50d Abs. 1). *Kurt Hickisch*