BUNDESARBEITSKAMMER

PRINZ EUGEN STRASSE 20-22
1040 WIEN
T 01 501 65-0

DVR NR. 1048384

Bundeskanzleramt
zH Herrn Mag Alexander Flendrovsky
Ballhausplatz 2
1014 Wien

E-Mail: v@bka.gv.at

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel 501 65	Fax	Datum
810.026/0002-V/3/08	BAK-KS/GSt/DZ/GS	Mag Daniela Zimmer	DW 2722	DW 2693	15.05.2008

Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008)

Sehr geehrter Herr Mag Flendrovsky!

Die Bundesarbeitskammer (BAK) erlaubt sich zum übermittelten Entwurf, mit dem das Datenschutzgesetz geändert wird, wie folgt Stellung zu nehmen:

Die BAK begrüßt grundsätzlich, dass mit der geplanten Gesetzesnovelle auf die fortschreitende Technologieentwicklung und ihrem Gefährdungspotential für die Privatsphäre – nicht zuletzt innerhalb der Arbeitswelt -, eingegangen wird.

Zusammengefasst wären aus BAK-Sicht allerdings unbedingt folgende Anliegen zu berücksichtigen

Beibehaltung der bisherigen Rechtslage:

- Bezüglich des Grundrechts (Abs 2) keine Änderungen bezüglich „lebenswichtiger Interessen dritter Personen"
- Bezüglich der Datenverwendung zur Durchsetzung von Rechtsansprüchen (§ 8 Abs 3 Z 5 und § 9 Z 9) ist ein Festhalten an der Voraussetzung, dass die Daten zuvor rechtmäßig ermittelt werden müssen, unbedingt erforderlich. Andernfalls könnten Unternehmen, Arbeitgeber, Privatpersonen etc dazu übergehen, Daten „auf Vorrat" für alle nur erdenklichen künftigen Rechtskonflikte zu sammeln
- Bezüglich des für den Rechtsanwender wichtigen Hinweises (in § 8 Abs 2), dass auch bei veröffentlichten Daten ein Widerspruchsrecht nach § 28 DSG besteht

Betrieblicher Datenschutzbeauftragter

- Die Einführung eines betrieblichen Datenschutzbeauftragten stellt einen wichtigen Schritt in Richtung einer wirksameren Durchsetzung von Datenschutzbestimmungen in der Arbeitswelt dar und wird ausdrücklich begrüßt
- Teilzeitbeschäftigte (unter 20 Stunden pro Woche) sollten auf die erforderliche Betriebsgröße angerechnet werden
- Dem Datenschutzbeauftragten ist die für seine Aufgabenerfüllung und Weiterbildung tatsächlich benötigte Zeit (unter Entgeltfortzahlung) zur Verfügung zu stellen
- Um die Unabhängigkeit des Datenschutzbeauftragten zu stärken, sollte über die Weisungsfreiheit hinaus auch ein Benachteiligungsverbot verankert werden
- Aufnahme einer Sanktionsbestimmung, wenn kein Datenschutzbeauftragter bestellt wird

Videoüberwachung

- Ziel sollte ein auch für Rechtsunkundige verständlicher Rechtsrahmen sein, der (unter weitestmöglichen Verzicht auf unbestimmte Gesetzesbegriffe) darüber Auskunft gibt, wer diese Technik, wann, wo, unter welchen Bedingungen einsetzen darf
- Zulässigkeit nur bei über das gewöhnliche Maß hinausgehenden, besonderen Gefährdungslagen
- Stärkere Betonung der Verhältnismäßigkeit – Nachweis, weshalb schonendere Mittel (Alarmanlage, Aufsichtspersonen, Echtzeitüberwachung etc.) nicht ausreichen
- Einsatz für Zwecke der Beweismittelsicherung nur aufgrund rechtmäßiger Datenermittlung; als Primärzweck nur für die Durchsetzung von Ansprüchen, die dem Grundrechtseingriff zumindest gleichwertig sind
- Spezielle, äußerst restriktive Regelungen für Videoüberwachung am Arbeitsplatz (zB Nachweis bei Echtzeitüberwachung und Bilddatenspeicherung, dass über den Aufzeichnungszweck hinausgehende, gezielte Mitarbeiterkontrolle ausgeschlossen ist; Mindestanforderungen in schriftlichen Regelungen zwischen dem Arbeitgeber und dem Betriebsrat und den Betriebsrat bzw den Arbeitnehmer in betriebsratslosen Betrieben)
- Ausnahmslose Kennzeichnungspflicht – Verbot verdeckter Videoüberwachung
- Erteilung von unbefristeten Genehmigungen nur ausnahmsweise - ansonsten Festlegung einer Frist, nach deren Ablauf die weitere Erforderlichkeit der Anlage glaubhaft gemacht werden muss
- Lösung des Vollzugsproblems bezüglich der Vielzahl bestehender - aber nicht gemeldeter und nach dem DSG neu rechtswidriger - Überwachungsanlagen

Registrierungsverfahren:

- Einwände bestehen dagegen, dass nach Ablauf von zwei Monaten nach Meldung vorabkontrollpflichtige Datennutzungen (zB betreffend sensibler Daten, Datenverbundsysteme, Videoüberwachung) bereits in Betrieb gehen können. Da es sich häufig um komplexe wie heikle Verarbeitungsvorhaben handelt, ist die Frist für eine sorgfältige Zulässigkeitsprüfung viel zu kurz. Wie bisher sollte die Inbetriebnahme erst nach Abschluss der Prüfung zulässig sein

- Die Registrierung soll auch - aber nicht ausschließlich - unter Verwendung der Bürgerkarte möglich sein. Zugangshürden (Anschaffung, Kosten) könnten „kleine" Auftraggeber von einer Meldung abhalten
- Die Vollständigkeit und rechtliche Zulässigkeit der eingetragenen Datenanwendungen darf durch das Übergehen von Einzelprüfungen zu bloßer automatisierter Fehlersuche und gelegentlichen Stichproben, nicht beeinträchtigt werden

Rechtsdurchsetzung:

- Neuordnung des Rechtsschutzes: Arbeits- und Sozialgerichte sollten für Datenschutzbelange in Zusammenhang mit Arbeitsverhältnissen zuständig sein
- Abbau der Rechtsschutzhürden bei Datenschutzverletzungen von privaten Rechtsträgern (Zivilgerichte 1.Instanz): Ausbau des Ombudsverfahrens bei der Datenschutzkommission als Alternative zum kostenintensiven Zivilprozess

Zu den Bestimmungen im Einzelnen

Art 1 Grundrecht auf Datenschutz

- **Kein Einwand gegen die Beschränkung auf natürliche Personen:**

Gegen die Ausklammerung juristischer Personen aus dem Grundrechtsschutz besteht aus AK-Sicht kein Einwand, da durch diese Maßnahme kein Rechtsschutzdefizit entsteht. Unternehmensdaten unterliegen ohnedies - gestützt auf den Schutz der Betriebs- oder Geschäftsgeheimnisse - der Geheimhaltung.

- **Beibehaltung des bisherigen Wortlautes in Abs 2 aus AK-Sicht erforderlich:**

Als geringfügig bezeichnen die Erläuterungen die Änderung in Abs 2, der den Umfang der Eingriffsmöglichkeiten ins Grundrecht absteckt. Tatsächlich geraten dadurch aber die bisher klar voneinander abgegrenzten Interessenssphären komplett durcheinander: Gründe auf der Betroffenenseite (seine lebenswichtigen Interessen bzw. seine Zustimmung) auf der einen und überwiegende berechtigte Interessen dritter Personen auf der anderen Seite.

Während nach bisheriger Rechtslage die Verwendung von Daten nur im lebenswichtigen Interesse **des Betroffenen** zulässig ist, erweitert der Entwurf den Eingriffsumfang insoweit, als **künftig auch lebenswichtige Interessen dritter Personen, unmittelbar auf §1 Abs 2 gestützt,** als Rechtfertigung herangezogen werden können.

Der Entwurf geht damit ohne erkennbare Notwendigkeit über die Vorgaben der RI 95/46/EG hinaus. Eine Datenverwendung darf nach Art 7 d) nur erfolgen, wenn *„die Verarbeitung für die Wahrung lebenswichtiger Interessen der **betroffenen Person** erforderlich ist."* Darüber hinaus sind lebenswichtige Interessen Dritter selbstverständlich als überwiegende berechtigte Interessen im Sinn des Art 7 f) RI 95/46 EG (bzw § 8 Abs 3 Z 3 und § 9 Z 8 DSG 2000) beachtlich. Soweit derartige Sachverhalte künftig nicht mehr auf das überwiegende berechtigte Interesse Dritter gestützt werden müssen, bedürfen Eingriffe staatlicher Behörden auch keiner besonderen gesetzlichen Anordnung. Explizite gesetzliche Ermächtigungen sind aus AK-Sicht wünschenswert, um sicherzustellen, dass auch der Schutz der Geheimhaltungsinteressen Betroffener angemessen garantiert wird.

Zu § 2 Zuständigkeit

Gegen eine Kompetenzbereinigung zugunsten einer durchgängigen Bundeszuständigkeit in Gesetzgebung und Vollziehung besteht kein Einwand.

Zu § 4 Definitionen

Grundsätzlich wird jede Überarbeitung, die der besseren Lesbarkeit und Verständlichkeit des DSG dient, sehr begrüßt. Es bestehen allerdings Bedenken, ob mit der Neuformulierung nicht auch maßgebliche inhaltliche Veränderungen vorgenommen werden:

- **Begriff des Auftraggebers:** Die Erläuterungen betonen zwar, dass mit der Neutextierung nur eine Vereinfachung des Auftraggeberbegriffes beabsichtigt ist. Folgende inhaltliche Korrekturen fallen jedoch auf:

  Bislang galt: *Auftraggeber ist auch derjenige, der „einem anderen Daten zur Herstellung eines aufgetragenen Werkes überlässt und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten."* Nunmehr heißt es:*"... Sie gelten auch dann als Auftraggeber, wenn sie einen Dienstleister mit der Herstellung eines Werks beauftragen und erst dieser die Entscheidung trifft, zu diesem Zweck Daten zu verwenden."*

  Da nicht mehr auf die **Überlassung der Daten durch den Auftraggeber** abgestellt wird, der Dienstleister -mit anderen Worten- Daten auch aus anderen Quellen zur Erfüllung des Werkauftrages verwenden kann, stellt sich doch die Frage, ab wann der Dienstleister bezüglich der Verarbeitung von Daten Dritter nicht selbst zum Auftraggeber wird. Als „Überlassung" wurden zwar auch bisher nicht nur Fälle einer Übergabe von Daten des Auftraggebers an den Dienstleister betrachtet. Auch eine Daten-

beschaffung von dritter Seite ist denkbar, setzte nach bisherigem Verständnis aber voraus, dass der Auftraggeber zumindest die Berechtigung zu diesem Vorgang eingeräumt hat. Eine entsprechende Ergänzung könnte diesbezüglich Klarheit schaffen.

- **Begriff des Dienstleisters:** Die Erläuterungen nennen einige Fallbeispiele, die nicht dem Charakter eines „Ermittlungsdienstleisters" entsprechen. Aus der Legaldefinition lässt sich diese Interpretation allerdings nicht ohne weiteres ableiten. Um Klarheit zu schaffen, sollten die beschriebenen Fallvarianten in den Gesetzestext selbst aufgenommen werden.

- **Geltungsbereich für Datenanwendungen/manuelle Daten (Abs 2):** Da es mittlerweile kein Aufwand ist, analoges Videomaterial zu digitalisieren, wird angeregt, den Abschnitt 9 a auf alle Daten zu beziehen, um durch die vorgeschlagene Beschränkung auf „Datenanwendungen" nicht allzu leicht eine Umgehung zu ermöglichen.

Zu § 8 Abs 2 veröffentlichte Daten

Beibehaltung der bisherigen Rechtslage: Der bisherige ausdrückliche Hinweis, dass das Widerspruchsrecht nach § 28 DSG auch für veröffentlichte Daten gilt, sollte aus Transparenzgründen beibehalten werden. Aufgrund des vorausgehenden Satzes (Bei veröffentlichten Daten gelten schutzwürdige Geheimhaltungsinteressen nicht als verletzt) ist ein Hinweis, dass trotzdem Abwehransprüche bestehen, essentiell. Aus § 28 DSG selbst lässt sich dieser Umstand nicht zweifelsfrei ableiten.

Zu § 8 Abs. 3 Z 5 (bzw. § 9 Z 9) Geheimhaltungsinteressen

Gegen die beabsichtigte Aufweichung der beiden Bestimmungen bestehen erhebliche Einwände:
In beiden Bestimmungen soll der Halbsatz entfallen *„und die Daten rechtmäßig ermittelt werden"*. Begründet wird diese Änderung mit einer Anpassung an die RI 95/46/EG (Art Abs 2 lit e). Nach dem bisherigen Wortlaut war die Ermittlung von Daten für eine Anspruchsdurchsetzung nicht erfasst. Die Erläuterungen leiten aus dem Verhältnismäßigkeitsgebot nur die Einschränkung ab, dass es „denkmöglich" sein muss, dass die Daten für ein behördliches/gerichtliches Verfahren „relevant" sind. Der Anspruch müsse im Ermittlungszeitpunkt daher „relativ bestimmt" sein.

Auf die Uferlosigkeit eines solchen Erlaubnistatbestandes wird auch im Kapitel Videoüberwachung näher eingegangen. Aufgrund der Vielzahl an denkbaren Sachverhalten, bei denen ein empfindlicher Eingriff in die Privatsphäre zur Durchsetzung aller denkbaren zivil- oder verwaltungsrechtlicher Ansprüche stattfinden würde, darunter auch absolute Bagatellanliegen, bereitet allergrößtes Unbehagen. Wird Beweismittelsicherung allgemein als primärer Ermittlungszweck von Daten anerkannt, darf prognostiziert werden, dass vorbauend für alle nur erdenklichen künftigen Rechtskonflikte Daten standardmäßig gesammelt würden:

- von Unternehmen im Rahmen ihrer Vertragsbeziehungen gegenüber Konsumenten und sonstigen Geschäftspartnern
- von Arbeitgebern gegenüber Arbeitnehmern in Hinblick auf allfällige künftige Arbeitsprozesse
- von Nachbarn bei Austragung klassischer Nachbarschaftskonflikte uvm

Da sich das Verhältnismäßigkeitsgebot auch nur in ganz wenigen einschränkenden Anmerkungen in den Erläuterungen niederschlägt, wäre eine beinahe schrankenlose Datenermittlung zulässig, die sogar eingriffsintensive Mittel wie Videoüberwachung, Tonbandprotokolle uä umfassen könnte.

§ 15 a betrieblicher Datenschutzbeauftragter

Das Vorhaben, einen betrieblichen Datenschutzbeauftragten einzuführen, wird ausdrücklich begrüßt.

Angesichts der rasanten technischen Entwicklung (zB allein bei Standardsoftware) werden zunehmend höhere Anforderungen an ArbeitgeberInnen und MitarbeiterInnen gestellt. Es besteht deshalb dringender Bedarf, einen betrieblichen Datenschutzbeauftragten vorzusehen, der die Einhaltung des innerbetrieblichen Datenschutzes sicherstellt.

- **Weiter Mitarbeiterbegriff:** Seine Bestellung ist für Betriebe mit mehr als 20 Mitarbeitern vorgesehen. Zumindest in den Erläuterungen sollte klargestellt werden, dass bei der Ermittlung der Mitarbeiterzahl der Mitarbeiterbegriff weit auszulegen ist: Alle im Betrieb tätigen Personen sollten erfasst sein, da sie unabhängig von der Rechtsform der Beschäftigung jedenfalls datenschutzrechtlich „Betroffene" sind. (Arbeitnehmer, freie Dienstnehmer, Werkvertragsnehmer, Leiharbeitnehmer, Lehrlinge). Allenfalls könnten Aushilfen, Ferialpraktikanten uä bei der Ermittlung der Mitarbeiterzahl außer Betracht bleiben.

- **Ausnahme bezüglich Teilzeitbeschäftigte nicht sachgerecht:** Nachvollziehbar ist, dass Inhaber von Kleinbetrieben nicht mit der Bestellung eines betrieblichen Datenschutzbeauftragten belastet werden sollen. Darüber hinaus ist aber kein Grund ersichtlich, warum Teilzeitbeschäftigte (unter 20 Stunden pro Woche) nicht auf die erforderliche Betriebsgröße angerechnet werden sollen. Die Zahl potentiell datenschutzrechtlich Betroffener steigt letztlich mit jedem Arbeitnehmer unabhängig von seinem Beschäftigungsausmaß an.

- **Regelungsbedarf bez. des Zusammenwirkens zwischen Betriebsrat und Datenschutzbeauftragten:** Auch dem Betriebsrat kommen wesentliche Befugnisse in Bezug auf die betriebliche Verwendung von Arbeitnehmerdaten zu (vgl. §§ 91 Abs. 2, 96, 96a und 97 ArbVG). Vor diesem Hintergrund wird - im Sinne eines effektiven betrieblichen Datenschutzes - eine Zusammenarbeit von betrieblichem Datenschutzbeauftragten und Betriebsrat notwendig sein. Nach dem Vorbild der organisatorischen Bestimmungen über Sicherheitsvertrauenspersonen, wo eine vergleichbare Vertre-

tungskonstellation gegeben ist, regt die BAK deshalb an, dem Betriebsrat das Recht auf **Verlangen nach einer Abberufung** des betrieblichen Datenschutzbeauftragten einzuräumen. In gleicher Weise wären auch einem Drittel der Arbeitnehmer in Betrieben, in denen keine Belegschaftsorgane bestehen, ein solches Recht einzuräumen. Denkbar wäre natürlich auch, über Abs 2 (Beratung) überhaupt die Notwendigkeit seiner **Zustimmung zur Bestellung** vorzusehen.

- **Berücksichtigung des Zeitaufwandes:**

1. Der Betriebsinhaber hätte aus BAK-Sicht sicherzustellen, dass dem betrieblichen Datenschutzbeauftragten die **zur Erfüllung seiner Aufgaben tatsächlich erforderliche Zeit - unter Anrechnung auf seine Arbeitszeit-** zur Verfügung steht. Der Betriebsinhaber wäre zudem zu verpflichten, ihm die für die Erfüllung seiner Aufgaben erforderlichen Behelfe und Mittel sowie alle **datenschutzrelevanten Unterlagen zur Verfügung** zu stellen und ihm Zugang zu sämtlichen Datenanwendungen und Datenbeständen (Dateien; *Anm.:* nämlich auch zu den bereits bestehenden!) aber auch zu möglichen externen Dienstleistern zu gewähren.

2. Zum Erwerb von **Fachkenntnissen und zur Weiterbildung** auf dem Gebiet des Datenschutzes ist dem Datenschutzbeauftragten ebenso die erforderliche Arbeitszeit (unter Entgeltfortzahlung), zumindest aber (entsprechend Abs 4) im ersten Jahr 40 Stunden und in den Folgejahren jeweils 20 Stunden zur Verfügung zu stellen. Die Kosten dafür hat der Arbeitgeber zu tragen.

3. Jedem Mitarbeiter und Betriebsratsmitglied sind **für Beratungen** durch den Datenschutzbeauftragten Arbeitszeit im erforderlichen Ausmaß (unter Fortzahlung des Entgeltes) zumindest aber die in Abs 4 vorgeschlagenen 8 Stunden (im ersten Dienstjahr) bzw 4 Stunden (in den Folgejahren) zur Verfügung zu stellen.

- **Infopflichten:** Erlangt der Betriebsinhaber vom Verdacht einer Verletzung datenschutzrechtlicher Vorschriften Kenntnis, ist zugleich auch der Betriebsrat / Betriebsausschuss zu informieren.

- Klarzustellen ist, dass zur raschen Herstellung eines rechtmäßigen Zustandes vom Datenschutzbeauftragten auch externe Stellen kontaktiert werden können (Interessensvertretungen, Datenschutzkommission, Gerichte; siehe dazu die korrespondierende Bestimmung in § 30 Abs 1a). Wir regen an, in den erläuternden Bemerkungen darauf hinzuweisen, dass dem Betriebsrat/Betriebsausschuss die Möglichkeit, externe Stellen zu kontaktieren, nach § 90 ArbVG zukommt. Weiters ersuchen wir, im DSG ausdrücklich zu normieren, dass auch der Betriebsrat/Betriebsausschuss die Möglichkeit hat, sich in seiner Funktion als betriebliche Arbeitnehmervertretung an die Datenschutzkommission zu wenden.

- **Uneingeschränkte Weisungsfreiheit**: Wünschenswert wäre es, in den Erläuterungen die Klarstallung aufzunehmen, dass der betriebliche Datenschutzbeauftragten in Ausübung dieser Funktion **generell** weisungsfrei gestellt ist.

- Der vorgesehene **Kündigungs- und Entlassungsschutz wird selbstverständlich begrüßt.** Anzumerken ist allerdings, dass im vorgeschlagenen § 15a Abs.5 Satz 3 sprachlich der unbestimmte statt eines bestimmten Artikels korrekt wäre (dh *einen* Kündigungs- und Entlassungsschutz statt „*den*", da ja erst durch diese Bestimmung ein solcher konstituiert wird). Im Interesse besserer Lesbarkeit ist überhaupt anzuraten, die Liste der **Motivkündigungstatbestände in § 105 Abs. 3 Z 1 ArbVG** um den Tatbestand „*wegen seiner Tätigkeit als betrieblicher Datenschutzbeauftragter*" zu erweitern, statt mit einem Querverweis auf den Kündigungs- und Entlassungsschutz der Sicherheitsfachkräfte zu verweisen (der obendrein nicht im zitierten § 73 Abs. 1 ASchG verankert ist).

- Zum Zwecke der faktischen Ermöglichung einer (weitgehend) unabhängigen Überwachung der Einhaltung der Vorschriften des DSG wäre es weiters begrüßenswert, wenn ein **„Benachteiligungsverbot"** des betrieblichen Datenschutzbeauftragten, zB wie folgt normiert würde: *Der betriebliche Datenschutzbeauftragte darf wegen der Ausübung dieser Tätigkeit, insbesondere hinsichtlich des Entgelts, der Aufstiegsmöglichkeiten und einer Versetzung sowie hinsichtlich der sonstigen Arbeitsbedingungen, nicht benachteiligt werden.*

- **Zumutbarer Meldeaufwand:** Angesichts des vorgeschlagenen verzögerten Inkrafttretens der Bestimmungen über den betrieblichen Datenschutzbeauftragten (erst mit 1.7.2009) ist es aus unserer Sicht nicht ganz nachvollziehbar, warum die Meldung in Bezug auf den betrieblichen Datenschutzbeauftragen (nach der vorgeschlagenen Fassung der Übergangsbestimmung des § 61 Abs. 8) noch weiter (unter Umständen jahrelang) verzögert werden kann.

- **Fehlende Sanktion:** Konsequenterweise wäre in § 52 Abs 2 DSG 2000 eine Verwaltungsstrafbestimmung für den Fall aufzunehmen, dass entgegen § 15a kein betrieblicher Datenschutzbeauftragter bestellt wurde. Eine entsprechende Pflicht zur Erstattung einer Anzeige sollte in § 22a Abs 6 aufgenommen werden.

Zum Registrierungsverfahren:

Zu § 16:
Klarzustellen wäre, dass das Datenschutzregister dem Zweck dient, nicht nur Betroffene sondern **auch betriebliche Datenschutzbeauftragte sowie Betriebsräte/Betriebsausschüsse)** über Auftraggeber und Datenanwendungen zu informieren.

Zu § 17ff:

Eine Vereinfachung des Registrierungsverfahrens, die den Erfordernissen der Praxis gerecht wird, wird grundsätzlich unterstützt. Die Motive für die Neuregelung ist angesichts der rasant angestiegenen Zahl von Meldungen nachvollziehbar. Die Einführung eines weitgehend automatisierten Prüfverfahrens für nicht-vorabkontrollpflichtige Verarbeitungen bietet einerseits die Chance, sich auf besonders heikle Fälle zu konzentrieren. Andererseits ist zu bedenken

- **Standardverarbeitungen wirken jetzt schon als Filter:** Es darf nicht übersehen werden, dass für sehr viele Standardverarbeitungen (ohne besonders grundrechtsrelevante Auswirkungen für die Betroffenen) ohnedies keine Meldepflicht besteht. Datenschutzrechtliche Sensibilität wird daher grundsätzlich allen meldepflichtigen Anwendungen zu eigen sein.

- **Sorge des Qualitätsverlustes:** Das Register ist die einzige umfassende und leicht zugängliche Informationsquelle für jedermann, der wissen möchte, welche Daten datenschutzrechtliche Auftraggeber verarbeiten. Eine über das Register gewährleistete Transparenz über Verarbeitungspraktiken ist die elementare Vorbedingung, dass Betroffene von ihren Datenschutzrechten überhaupt Gebrauch machen können. **Die Richtigkeit und Vollständigkeit der Einträge darf deshalb durch ein Übergehen von Einzelprüfungen zu bloßer automatisierter Fehlersuche und Stichproben, nicht beeinträchtigt werden.**

- **Bedenken gegen einen Zwang zur Nutzung der Bürgerkarte:** Eine elektronische Registrierung sollte zwar **auch – aber nicht ausschließlich** - unter Verwendung der Bürgerkarte möglich sein. Daneben müssen weitere Möglichkeiten (zB elektronischer Zugang via Passwort) zur Verfügung stehen. Die strikten Zugangsvoraussetzungen könnten vor allem kleinere Betriebe und vor allem Privatpersonen von einer Meldung abhalten. Angesichts geschätzter 200.000 nicht gemeldeter privater Videoüberwachungsanlagen wäre es vordringlich, diese – ohne zusätzliche abschreckende Hürden – zu einer nachträglichen Registrierung zu motivieren. Abgesehen von den Anschaffungskosten ist auch die Verbreitung der Bürgerkarte bzw. Lesegeräten in der Bevölkerung viel zu gering. **Dies könnte die Qualität des Registers beeinträchtigen, soweit beabsichtige Meldungen aus diesem Grund in größerer Zahl unterbleiben.**

- **Die Abhängigkeit von den gemeldeten Angaben ist die Schwachstelle einer automatisierten Prüfung**. § 20 Abs 3 sieht vor, dass Meldungen, die der Auftraggeber als vorabkontrollpflichtig bezeichnet hat, auf Mängel zu prüfen sind. Bezeichnet der Auftraggeber seine Datenanwendung nicht korrekt, wird keine gründliche Vorabkontrolle durchgeführt. Konsequenz: eventuelle Rechtswidrigkeiten fallen (lange) nicht auf.

- **Erhebliche Bedenken bestehen gegen die automatische Registrierung und Inbetriebnahme von vorabkontrollpflichtigen Datenanwendungen nach Verstreichen einer zweimonatigen Frist:** Eine Zweimonatsfrist nach deren Verstreichen auch mit der heikelsten Verarbeitung begonnen werden kann, erscheint angesichts der Fülle komplexer Meldungen zu kurz. Aus BAK - Sicht ist es nicht schlüssig, die besondere Brisanz von Infoverbundsystemen, Verarbeitungen sensibler Daten, Videoüberwachung und Vergleichbarem einerseits gesetzlich hervorzustreichen, dafür auch eine strikte Vorabkontrollpflicht vorzusehen, dann aber keinen realistischen Zeitraum für die behördliche Prüfung einzuräumen. § 73 Abs 1 AVG sollte hinreichend vor der Gefahr einer Untätigkeit der Behörde schützen.

  Nach § 21 sind auch Meldungen von vorabkontrollpflichtigen Datenanwendungen im Register einzutragen, wenn zwei Monate nach Einlangen der Meldung bei der Datenschutzkommission verstrichen sind, ohne dass ein Verbesserungsauftrag erteilt wurde. Angesichts komplexer, oft erst im Detail zu ermittelnder Sachverhalte bei vorabkontrollpflichtigen Anwendungen erscheint diese Frist zu kurz. Allein wenn künftig Meldungen über Videoüberwachungsvorhaben noch zahlreicher werden und die Frage nach der Zulässigkeit der Überwachung im Einzelfall – anhand einer Auseinandersetzung mit den örtlichen Gegebenheiten, der dokumentierten besonderen Gefährdung, Betroffenenkreisen, Vereinbarungen usw. – zu klären ist, schließt die im Entwurf enthaltene Frist eine sorgfältige Prüfung praktisch aus.

  Präferiert wird aus BAK-Sicht ein Entfall der Frist, zumindest aber sollte § 18 Abs 2 iVm § 20 Abs 3 DSG 2000 beibehalten werden.

Zu § 32 Anrufung der Gerichte

Zuständigkeit für Rechtsdurchsetzung in Zusammenhang mit Arbeitsverhältnissen:
Im Zusammenhang mit dem Arbeitsverhältnis wäre es unbedingt zweckmäßig, wenn das Grundrecht auf Datenschutz, dh der Rechtsschutz von Arbeitnehmern - als Betroffene – aber auch dem Betriebsrat/Betriebsausschuss in der Funktion als betriebliche Arbeitnehmervertretung sowie dem betrieblichen Datenschutzbeauftragen bei den **örtlich zuständigen Arbeits- und Sozialgerichten** geltend gemacht werden könnte. Eine derartige Regelung erscheint uns im Hinblick auf § 50 ASGG konsequent und sinnvoll, um eine Zersplitterung der gerichtlichen Zuständigkeit in Arbeitsrechtssachen zu vermeiden.

Zu § 49 automatisierte Einzelentscheidung

Es wird ausdrücklich begrüßt, dass den von automatisierten Einzelentscheidungen Betroffenen die Auskunftsrechte nach § 26 DSG 2000 zukommen sollen.

Zur Videoüberwachung (§§ 50a ff)

Ausgangslage

Mit einem gesetzlichen Rahmen für die Videoüberwachung, an der Unternehmen und Privatpersonen aus den unterschiedlichsten Motiven Bedarf anmelden, wird einem dringenden Bedürfnis nach mehr Rechtssicherheit entsprochen. Grenzen und Auflagen für die private Speicherung von Bilddaten ergeben sich – sieht man von den bisherigen Einzelentscheidungen einmal ab – nur aus den allgemeinen Datenschutzprinzipien. Die Zahl der in Österreich privat genutzten Videokameras mit Speicherfunktion wird auf rund 200.000 geschätzt, wobei nur ein kleiner Teil korrekt dem Datenschutzregister gemeldet wurde.

Sicherheit zählt zweifellos zu den elementaren Bedürfnissen der Bevölkerung. Vor diesem Hintergrund ist die Popularität digitaler Sicherheitstechnik grundsätzlich nachvollziehbar. Zumindest Teile der Bevölkerung würden einem (vermeintlichen) Sicherheitsgewinn durch Videoüberwachung ohne weiteres den Vorrang gegenüber Datenschutzbedenken einräumen. Datenschutzrechtlich sollte dennoch die eindeutige Maxime bestehen: **Videoüberwachung muss die Ausnahme bleiben und darf nicht der Regelfall werden.** So wäre es aus BAK-Sicht ein absolut bedenklicher Effekt, wenn Videoüberwachung sich zu einem derart weit verbreiteten Sicherheitsstandard entwickelte, dass zB Versicherungen die Existenz derartiger Anlagen bei der Übernahme eines Deckungsfalles allgemein voraussetzen. Zu den völlig unerwünschten „Nebenwirkungen" von Videoüberwachung zählen ua:

- **Videoüberwachung von Arbeitsplätzen:** Videoüberwachung kann bspw. in schwerwiegender Weise in das **allgemeine Persönlichkeitsrecht** der Arbeitnehmer eingreifen. Im schlimmsten Fall werden diese einem ständigen Überwachungsdruck ausgesetzt. Der Arbeitnehmer kann zum Objekt der Überwachungstechnik werden, was zu einer erhöhten Abhängigkeit und zur Behinderung der freien Entfaltung der Persönlichkeit führt.

  Die Angst, die vielfach Resultat der **Ungewissheit über Art und Umfang der Kontrolle und deren Auswirkungen** ist, sowie die fehlende Einflussmöglichkeit des Arbeitnehmers auf diese Kontrolle und auf die Verwertung ihrer Ergebnisse durch den Arbeitgeber sowie schließlich das darin zum Ausdruck kommende massive Misstrauen des Arbeitgebers **widerspricht der mit der Menschenwürde** in unmittelbarem Zusammenhang stehenden **Selbstverwirklichung des Menschen in der Arbeit** (siehe dazu OGH 13.06.2002, 8 ObA 288/01p)

- **Geringe Evidenz über die generelle Eignung von Videoüberwachung für die angestrebten Zwecke**: Der tatsächliche Zugewinn an Sicherheit, der mit der Installation von Videoüberwachung im privaten Raum verbunden sein soll, wird oft überschätzt. Vereinzelte Fälle, wo Videoüberwachung die Aufklärung spektakulärer Straftaten ermöglichte, sind keine geeignete Basis für generelle Schlussfolgerungen. Ob und wann Videoüberwachung zur Gefahrenabwehr und nachträglicher Deliktsaufklärung wirklich geeignet ist, ist auch unter Sicherheitsexperten umstritten. Für Teile der Bevölkerung erfüllt Videoüberwachung oft auch nur „weiche" Ziele, wie die Stärkung des subjektiven Sicherheitsgefühls oder eine symbolische Präsenz an Orten, wo es an polizeilicher Präsenz mangelt.

- **Unerwünschte Verhaltensreflexe:** Als gesichert gilt, dass Videoüberwachung Effekte erzielt, die deutlich über die erhoffte Abschreckung von Personen hinausgeht, die sich ordnungswidrig verhalten könnten. Menschen, die damit rechnen müssen, dass ihre Handlungen registriert werden, werden nicht auffallen wollen und neigen zu einem sehr viel stärker angepassten Verhalten. So hob etwa das deutsche Bundesverfassungsgericht schon in seinem Volkszählungsurteil die potentiell hemmende (psychische) Wirkung von Überwachungsmaßnahmen auf die Bereitschaft von Bürgern, ihre Grundrechte auszuüben (etwa an Versammlungen teilzunehmen), hervor. Österreichische und deutsche Entscheidungen stellten bereits klar, dass auch schon durch die bloße Befürchtung überwacht zu werden, ein Grundrechtseingriff vorliegen kann. Folglich kommt es nicht darauf an, ob eine Videoüberwachung tatsächlich Bilddaten erfasst oder diese Funktion mit einer Kameraattrappe bloß vorgetäuscht wird. Maßgeblich ist die Sicht des Betroffenen. Neben gesteigerter Selbstkontrolle und Befangenheit in Gegenwart von Kameras kann Videoüberwachung auch als räumliche Zugangskontrolle eingesetzt oder zumindest subjektiv als solche erlebt werden. Dies kann den Einzelnen (gewünschter oder nicht gewünschter Weise; bewusst oder auch unbewusst) davon abhalten, bestimmte Orte aufzusuchen - mit allen negativen Wirkungen auf das soziale Leben und die gesellschaftliche Integration.

- **Aufrüstungsspirale vorbeugen:** Nicht selten verlagert sich im Zuge einer lokalen Videoüberwachung ein Sicherheitsproblem nur räumlich – etwa mit der Folge, dass einen Häuserblock weiter sicherheitstechnisch ebenfalls aufgerüstet wird. Soziologen warnen deshalb vor einer Aufrüstungsspirale: aufgrund von Verdrängungseffekten würde Videoüberwachung über kurz oder lang flächendeckend eingesetzt. Bedacht zu nehmen ist daher auch darauf, dass die Gesellschaft im Zuge einer solchen Entwicklung längerfristig den Freiraum einbüßt, sich großflächig unbeobachtet bewegen zu können.

- **Gefahr der Überschreitung gemeldeter Zwecke:** Besonders im Auge zu behalten ist, dass eine für einen Zweck gemeldete Überwachungsanlage die Gefahr birgt, dass das Bildmaterial (meist unerlaubterweise) für Sekundärzwecke verwendet wird. Dient die Überwachung einer Handelsfiliale vorrangig dem Schutz vor Ladendiebstählen, kann nicht gänzlich ausgeschlossen werden, dass das Bildmaterial faktisch auch zur Kontrolle des Arbeitsverhaltens von Mitarbeitern herangezogen wird. Die

Vorfälle bei deutschen Diskontsupermärkten belegen dies eindrucksvoll. Der vorliegende Entwurf ermöglicht aber (in bestimmten Umfang) die Verwertung von Bilddaten über den ursprünglich gemeldeten Zweck hinaus.

- **Sensibilität der Videoüberwachung im Zusammenhang mit rechtlichen Abhängigkeitsverhältnissen, etwa am Arbeitsplatz**: Brisant ist Videoüberwachung letztlich vor allem in allen Situationen, in denen Betroffenen nicht die Wahlfreiheit zukommt, einer Überwachung auszuweichen, weil dem ein rechtliches Abhängigkeitsverhältnis gegenüber dem Auftraggeber der Überwachungsanlage faktisch entgegensteht. Dazu zählen Arbeitsverhältnisse oder auch die Kontrolle von Schülern an Schulstandorten. Die Wirksamkeit einer eventuellen Zustimmungserklärung von Betroffenen zu derartigen Maßnahmen ist in Hinblick auf die verdünnte Willensfreiheit regelmäßig in Zweifel zu ziehen. Auch wenn sich das Vorhaben auf andere Rechtsgrundlagen stützt, bleibt immer zu bedenken, dass Videoüberwachung diese Kategorien an Betroffenen besonders intensiv und nachteilig berührt: Sie können sich der Überwachung weder ohne weiteres entziehen, noch ziehen sie irgendeinen einen persönlichen Nutzen daraus.

- **Unterschiedlichste Betroffenenkategorien:** Passanten, Kunden uä sind natürlich ebenfalls einem Grundrechtseingriff ausgesetzt. Dieser ist in der Regel weniger einschneidend, soweit einer Bildaufzeichnung etwa durch Ausweichen entgangen werden kann. Vor diesem Hintergrund ist eine lückenlose Kennzeichnung von Videoüberwachung der BAK ein ganz zentrales Anliegen. Auch die Judikatur der Höchstgerichte betonte wiederholt die Bedeutung von Alternativen für Personen, die nicht aufgezeichnet werden möchten (BGH zur Überwachung von Einkaufspassagen) bzw der Bedachtnahme bei der Wahl der Installationsorte, dass die Gefahr der Verwendung für weitere Zwecke möglichst gering ist (OGH zur Überwachung von Hauseingangsbereichen). Auch Fahrgäste von Verkehrsmittel können - außer durch Verzicht auf die Nutzung - Überwachungssituationen nicht entgehen. Allerdings sind sie (wie Mieter) je nach Blickwinkel nicht nur Betroffene sondern auch Profiteure einer Überwachung, die auch ihrem Schutz (vor Diebstählen, Einbrüchen uä) dient.

Vor dem Hintergrund der ungeheuer vielfältigen Interessenslagen wird ein Rechtsrahmen benötigt, der

- ...auch **rechtsunkundigen Personen übersichtlich vermittelt**, wer diese Technik, wann, wo, unter welchen Rahmenbedingungen einsetzen darf.
- ...der Tendenz zu einem ausufernden Einsatz visueller Sicherheitstechnik klare Grenzen setzt - sie etwa auf Einsatzgebiete beschränkt, wo eine **über das übliche Maß hinausgehende besondere Gefährdungslage** unstrittig besteht.
- ...sich ausschließlich auf gefährdete Rechtsgüter bezieht, die allgemein (und nicht aus subjektiver Sicht des Auftraggebers) ganz besonders schützenswert sind. Der **Durchsetzung bagatellhafter Ansprüche soll Videoüberwachung nicht dienen**.

- ..die **Überwachung an Arbeitsplätzen - wenn überhaupt - dann nur unter besonders strengen Auflagen** zulassen. Zentrale Voraussetzung wäre zB der Nachweis, dass ein Missbrauch der Daten zur Verhaltens- oder Leistungskontrolle aufgrund der Umstände jedenfalls ausgeschlossen ist.
- ... bei Vorliegen eines überwiegenden Überwachungsinteresses den Auftraggeber außerdem dazu anhält, glaubhaft zu machen, **weshalb „gelindere Mittel** (etwa Alarmanlagen, Aufsichtspersonen, Echtzeitüberwachung uvm) **ungeeignet oder unzumutbar sind.**
- **...eine Verwendung für Sekundärzwecke grundsätzlich untersagt** (wenige Ausnahmen)
- **...die Vollziehung praxisnah regelt**. Praktische Folge gesetzlicher Restriktionen wird sein, dass nicht alle bestehenden Anlagen (geschätzte Zahl 200.000) als zulässig einzustufen sind und demontiert werden müssen. Da ein Großteil der in Betrieb befindlichen Kameras nicht ordnungsgemäß gemeldet wurde, zeichnen sich Vollzugsdefizite ab. Diesen sollte rechtzeitig etwa durch eine Nachmeldefrist begegnet werden, nach deren Verstreichen spürbare Verwaltungsstrafen verhängt werden können. Zu regeln wäre auch, wie Beseitigungsansprüche effizient und kostengünstig (zivil- oder verwaltungsrechtlich; auf Initiative der DSK) durchgesetzt werden können.

Zu Abs 1 Definition Videoüberwachung

Die Definition steckt zugleich auch den Anwendungsbereich der nachfolgenden Bestimmungen ab. Vermisst wird eine allgemeine Klarstellung bereits am Beginn des Abschnittes, **wer** Überwachungsanlagen **wo** verwenden darf - mit anderen Worten die Festlegung

- wer grundsätzlich als Auftraggeber einer Videoüberwachung nach dem DSG in Frage kommt und
- auf welches Terrain sich Überwachungsanliegen maximal beziehen können.

Überwachung durch private oder öffentlich-rechtliche Auftraggeber im privaten oder öffentlichen Raum:

Dem Entwurf zufolge können private und öffentliche Rechtsträger ihr Überwachungsvorhaben auf das DSG stützen. Auftraggeber des öffentlichen Bereiches dürfen aber bei Vollziehung hoheitlicher Aufgaben nur überwachen, wenn lebenswichtige Interessen einer Person berührt sind. Soweit die Überwachung in den Bereich der Privatwirtschaftsverwaltung fällt (oder Aufgaben ausgegliedert wurden) bestehen dieselben Überwachungsmöglichkeiten wie bei Privatpersonen (zB Schulen, Krankenhäuser, Asfinag uvm).

- **Eine Zusammenführung der Überwachungsinteressen von Privaten, Privatwirtschaftverwaltung bzw. Hoheitsverwaltung in einer Bestimmung sollte vermieden werden.** Die Erläuterungen betonen selbst, dass Videoüberwachung etwa für Zwecke der Hoheitsverwaltung - vom Fall lebensnotwendiger Interessen abgesehen

- nur auf Basis besonderer gesetzlicher Bestimmungen erfolgen soll. Beispielshaft wird das Sicherheitspolizeigesetz angeführt. Da aber Überwachung durch Sicherheitsbehörden regelmäßig lebenswichtige Interessen einer Person berührt, kann sich die Behörde offenbar auch auf das DSG stützen. Eine derartige Vermischung von Anspruchsgrundlagen ist aus BAK-Sicht nicht wünschenswert.

- Gegen eine Reduktion der Auftraggeber auf private Rechtsträger spricht freilich, dass auch öffentlich-rechtliche Institutionen zum Teil Interessen verfolgen, die jenen von Privaten absolut vergleichbar sind. Dazu zählt etwa die Überwachung von Bürogebäuden, Fuhrparks, Schulgebäuden uä, die von Behörden, Anstalten öffentlichen Rechts usw benutzt werden. Soweit die Überwachung dem **Schutz von (beweglichen und unbeweglichen) Objekten dient, die von öffentlichen Rechtsträgern benutzt werden,** sollten derartige Überwachungen in den Anwendungsbereich fallen.

- **Die Überwachung durch öffentliche Stellen (auch im Rahmen der Privatwirtschaftsverwaltung) auf allgemein zugänglichen öffentlichen Grund weist hingegen Besonderheiten auf, die besser in den jeweiligen Materiengesetzen regelbar sind.** Die Überwachung des öffentlichen Raums (Straßen, Plätze, Parkanlagen, öffentliche Veranstaltungsflächen uä) unterscheidet sich doch maßgeblich von jener rein privater (beschränkt zugängliche / halböffentliche) Räume:

  1. Großteils berühren derartige **Sachverhalte das staatliche Sicherheitsmonopol**, für das es ein eigenes Materiengesetz gibt (ein Nebeneinander von Überwachungsmöglichkeiten nach dem Sicherheitspolizeigesetz und dem DSG ist schon allein aus Gründen der Übersichtlichkeit jedenfalls abzulehnen).

  2. Bei Überwachungsabsichten im öffentlichen Raum im Rahmen der Privatwirtschaftsverwaltung ist auch eine **Vielzahl an Auftraggebern** denkbar, die ein und denselben Ort parallel überwachen möchten (weil für die Schutzobjekte Personen, Grünflächen, Denkmäler, Parkbänke jeweils andere Auftraggeber in Frage kommen). Hierbei stellen sich besondere Fragen in Bezug auf sinnvolle Koordination und Beschränkungen, die außerhalb des DSG zu klären sind. Bezüglich eines privaten Schutzgegenstandes wird hingegen in der Regel nur ein Auftraggeber – meist aufgrund eines Hausrechts im weitesten Sinn - überwachungsberechtigt sein.

mobile/fixierte Überwachungsanlagen:

Aus BAK-Sicht sollte nur Videoüberwachung, die ortsfest ist, in den Anwendungsbereich fallen. Mobile Videoüberwachung wäre folglich unzulässig, soweit sich die Zulässigkeit nicht aus anderen Gesetzen ergibt.

- Werden nämlich mobile Anwendungen mitberücksichtigt, gelingt dies nur – wie der Entwurf zeigt - unter gleichzeitiger massiver **Aufweichung der Nutzungsauflagen**. Dies sollte unbedingt vermieden werden. ZB ist für mobile Videoüberwachung eine Ausnahme von der Kennzeichnungspflicht der Anlagen vorgesehen. Der damit ein-

hergehende Transparenz- und in der Folge auch Rechtsschutzverlust ist aus BAK-Sicht nicht vertretbar.

- Als denkmögliche Anwendungsfälle kommen außerdem nur Situationen weitab üblicher privater Überwachungsanliegen in Betracht. zB der **Begleitschutz** von Staatsoberhäuptern oder Ermittlungspraktiken von **Detekteien**. Hierfür stehen eigene Materiengesetze zur Verfügung (die §§ 249 ff GewerbeO enthalten detaillierte Ausübungsregeln für Detektive). Welche Ermittlungsmethoden das Gewerbe rechtmäßig verwenden darf, sollte im Rahmen der Ausübungsvorschriften geregelt werden.

Im Hinblick auf die mit einer Videoüberwachung oft verknüpfte **akustische Überwachung** sollte jedenfalls klargestellt werden, dass diese mit diesem Abschnitt nicht abgedeckt ist. Zu ergänzen wäre deshalb: „*unter Ausschluss einer akustischen Erfassung oder Aufzeichnung*".

Zu Abs 2 iVm Abs 3 Z 7 Beweismittelsicherung als zulässiger Zweck

Videoüberwachung ist dem Entwurf zufolge erlaubt zum Schutz überwachter Objekte und zur Beweissicherung. Schutzwürdige Geheimhaltungsinteressen werden nicht berührt, wenn Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht erforderlich ist. Dieser Erlaubnistatbestand eröffnet unvertretbar weite Spielräume. **Der Beweissicherungszweck ist deshalb aus BAK-Sicht entweder ersatzlos zu streichen oder Abs 2 ist in Verbindung mit Abs 3 Z 7 restriktiver zu gestalten:**

- **§ 8 Abs 3 Z 5 (bzw § 9 Z 9) DSG enthält bezüglich der Beweisverwertung rechtmäßig ermittelter Daten vor Gerichten bereits eine Regelung.** Demnach sind schutzwürdige Geheimhaltungsinteressen dann nicht verletzt, wenn die Daten *zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig sind **und die Daten rechtmäßig ermittelt wurden.*** Mit dem Hinweis, dass nur solche Daten vor Gericht benutzt werden dürfen, die zuvor rechtmäßig verarbeitet wurden, bringt der Gesetzgeber zum Ausdruck, dass es für die Daten einen zulässigen primären Speichergrund geben muss, damit sie auch für einen Sekundärzweck – nämlich als gerichtliches Beweismittel – eingesetzt werden dürfen. Ergibt sich mit anderen Worten die Zulässigkeit für die Videoüberwachung aus den §§ 50 a ff (etwa weil ein Ort überwacht wird, der schon gefährlichen Angriffen ausgesetzt war), so kann der Überwacher Bildmaterial im Klagsfall ohnedies aufgrund von § 8 Abs 3 Z 5 nutzen.

- **Vielfach wird die Videoüberwachung aber auf nichts anderes als die Sicherung von Beweismittel abzielen.** Diese Ausgangslage ist datenschutzrechtlich bei weitem problematischer. Die Daten befinden sich – im Gegensatz zu § 8 Abs 3 Z 5 – noch nicht zulässigerweise in den Händen des Auftraggebers. Die Verbesserung der Rechtsposition im Klagsfall ist damit der eigentliche Speicheranlass. **Dem Entwurf zufolge wäre Videoüberwachung auch zur bloßen Beweismittelgewinnung**

grundsätzlich in Hinblick auf jede erdenkliche Form gerichtlicher Auseinandersetzungen zulässig (siehe § 50 a Abs 3 Z 7) – vorbehaltlich einer Verletzung des Verhältnismäßigkeitsgrundsatzes. Den Erläuterungen zufolge muss der Anspruch im Überwachungszeitpunkt nur bereits hinreichend „manifest" sein. **Gegen eine derart weitreichende Erlaubnis bestehen massive Datenschutzbedenken, weshalb die Ziffer 7 restriktiver formuliert oder am Besten ersatzlos gestrichen werden sollte.**

- Ersatzlos streichbar wäre die Ziffer 7 deshalb, weil § 8 Abs 3 DSG (bzw § 9 Z 9) keine abschließende sondern eine demonstrative Aufzählung enthält. Damit können auch Fälle, wo Videoüberwachung primär auf Beweismittelsicherung abzielt, unter diese Bestimmung subsumiert werden. **Unbedingt nachzuweisen ist aber jedenfalls, worin das überwiegende berechtigte Interesse an dieser eingriffsintensiven Vorgangsweise besteht**. So hat bspw ja auch die jeweils andere Streitpartei in einem Klagsfall ebenso ein berechtigtes Interesse daran, ihre Rechtsposition im Verfahren zu verbessern. Von einem automatischen Überwiegen der Überwachungsinteressen kann jedenfalls – wenn die Streitpartei gleichzeitig auch Betroffene der Videoüberwachung ist – nicht ausgegangen werden.

- So stellte etwa der **OGH** fest **(2001/09/27, 6 Ob 190/01m),** dass Aufzeichnung und Verwertung von Tonbandaufnahmen ohne Zustimmung des Betroffenen die Privatsphäre verletzt. **Überwiegende berechtigte Interessen können den Eingriff im Ausnahmefall rechtfertigen** - zB wenn ein **Beweisnotstand bei der Durchsetzung eines mit dem Grundrecht auf Datenschutz gleichwertigen - etwa auch verfassungsrechtlich geschützten - Rechtsanspruches** besteht, jedenfalls nicht bei Bagatellansprüchen. Ein allgemeines Beweisinteresse einer Prozesspartei reicht als Rechtfertigungsgrund keinesfalls. Eine analoge Wertung ist für den Fall, dass keine Ton - sondern Bilddaten beschafft werden, angebracht.

- Soweit Beweismittelsicherung als Speicherzweck eigens geregelt werden soll, müsste daher unbedingt auf die Art der Ansprüche näher eingegangen werden.

  1) Eine **Gleichwertigkeit der verfolgten Rechtsansprüche mit der in Kauf genommenen Verletzung der Privatsphäre** wird vorauszusetzen sein,

  2) außerdem muss das **Schadensausmaß bzw die Streitwerthöhe** erheblich sein

  3) möglichst **keine unbeteiligten Dritten zu den von der Überwachung Betroffenen** zählen uä

Zu Abs 3

- **Die Positionen des Auftraggebers und des Betroffenen sind ungleichgewichtig**: Der vorgesehene Rechtsrahmen enthält eine Reihe an „Erlaubnistatbeständen". Während der Auftraggeber einer Videoüberwachung in der Regel vergleichsweise leicht eine Rechtsgrundlage für seine Überwachungsabsichten finden wird, sind die von der Überwachung Betroffenen in der weitaus schwierigeren Position. Sie müssen überzeugende Abwehrgründe erst finden und ausformulieren.

- **Unbedingt erforderlich ist, das Verhältnismäßigkeitsprinzip stärker hervorzuheben:** Eine explizite Grenze für Überwachungswünsche zieht der Entwurf lediglich in Hinblick auf Orte, die zum höchstpersönlichen Lebensbereich zählen. Für die Entscheidung im Rahmen der datenschutzrechtlichen Einzelfallsprüfung, wann die beabsichtigte Videoüberwachung gemessen an den Eingriffen in die Privatsphäre von Mitbewohnern, Arbeitnehmern, Passanten, Konsumenten, Auszubildenden uvm. überhaupt verhältnismäßig (vor allem das schonendste Mittel zur Erreichung des Zweckes) ist und wann nicht, bietet der Gesetzestext selbst keine Abgrenzungshilfen. Hingewiesen wird lediglich darauf, dass *„im übrigen auch für Videoüberwachung die §§ 6 und 7, inbesondere der Verhältnismäßigkeitsgrundsatz"* gelten. An die letzte Stelle in Abs 7 verwiesen signalisiert der Satz dem Rechtsanwender auch nicht ausreichend, dass es sich hierbei um eine entscheidende Zulässigkeitsvoraussetzung handelt.

- **Damit ist zu befürchten, dass viele Rechtsanwender diese wichtige Zulässigkeitsvoraussetzung übersehen**: Beim Rechtsanwender kann nur allzu leicht der irrige Eindruck entstehen, dass jede Überwachung zulässig ist, sobald sich ein Überwachungsmotiv findet, das einem der Erlaubnistatbestände des Abs 3 zugeordnet werden kann. Tatsächlich ist damit aber bloß ein Teil des Prüfprozesses abgeschlossen. Die Rechtsfrage nach der Verhältnismäßigkeit ist genauso mit Bedacht zu klären: ist der Eingriff in die Privatsphäre der (potentiell) Betroffenen in diesem Umfang erforderlich und gibt es eventuell andere gelindere, zielführende Mittel?

- **Vorschlag: Abs 3 könnte lauten:**

  1. ***„Ein Betroffener ist durch eine Videoüberwachung dann nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt, wenn [...einzelne Ziffern....] und nachweislich keine gelinderen Mitteln zur Verfügung stehen und sich die Überwachung (insbes. räumlich und zeitlich) auf das unbedingt erforderliche Maß beschränkt (so kann etwa die Überwachungserlaubnis auch nur befristet erteilt werden) und Videoüberwachung sich zur Erreichung des angegebenen Zweckes überhaupt als geeignet erweist."***

  2. **Kriterienkatalog:** Mit einem beispielhaften Katalog an typischen Abwägungsfragen sollte der Rechtsanwender die unbedingt notwendige Orientierungshilfe erhalten. Einige wichtige grundsätzliche Wertungen, finden sich ohnedies in den Erläuterungen. Damit diesen Abwägungen das nötige Gewicht zukommt, sollten

sie in Form einer exemplarischen Aufzählung auch in den Gesetzestext aufgenommen werden. Bspw.:

„Vor einer Entscheidung zugunsten einer Videoüberwachung mit Speicherung der Bilddaten sind zunächst gelindere Mittel in Betracht zu ziehen und nachzuweisen, weshalb insbesondere

- mit anderen technischen Hilfsmitteln, bei denen kein Personenbezug entsteht (Alarmanlagen, Warensicherungssysteme, Sicherheitstüren u.v.m)

- die Anwesenheit von Aufsichtspersonen

- oder einer Echtzeitüberwachung

nicht das Auslangen gefunden werden kann."

3. Unter weiter: ***„Der Auftraggeber hat bei Meldung seines Überwachungsvorhabens einen Plan vorzulegen, aus dem die Installationsorte der Kameras hervorgehen, gegebenenfalls auch jene Orte, an denen er Vorfälle im Sinn des Abs 3 Z5 a) nachweisen kann."***

4. Außerdem: ***„ Die Videoüberwachung hat sich auf das zu überwachende Objekt zu beschränken. Eine Erfassung, die auch die Persönlichkeitsrechte vom Schutzzweck nicht erfasster Dritter berührt, ist dabei zu vermeiden. Ist dies aufgrund der Umstände nicht gänzlich vermeidbar, ist eine Überwachung nur dann zulässig, wenn die berechtigten Interessen des Auftraggebers an der Überwachung gegenüber jenen der (potentiell) Betroffenen an der Geheimhaltung eindeutig überwiegen."***

- **Klarstellender Hinweis, dass Fremdschutzinteressen nie eine geeignete Basis sind:** Die Entscheidung, ob ein überwiegendes Interesse an der Überwachung vorliegt und die Maßnahme verhältnismäßig ist, kann nur für den Einzelfall getroffen werden. Während **"Eigenschutz"- Interessen** des Auftraggebers (bezogen auf den Schutz von Personen und Eigentum) und **"Verantwortungsschutz"** (zB zivilrechtliche Verkehrssicherungspflichten) grundsätzlich denkbare berechtigte Interessen sind, gilt dies in diesem Zusammenhang für den **"Fremdschutz"** nicht. Damit ist der Schutz von Personen gemeint, mit denen der Auftraggeber in keinerlei Rechtsbeziehung steht (der Bereich ist den Sicherheitsbehörden vorbehalten).

Zu Abs 3 Z 2 öffentlich wahrnehmbares Verhalten

Nach dem bloßen Wortlaut ist nicht zweifelsfrei ausgeschlossen, dass unter diesen Tatbestand **auch bereits das bloße Sich-Bewegen einer Person an einem öffentlichen Ort** fällt. Damit wäre eine Überwachung von Fußgängerzonen, Lokalen oder öffentlichen Verkehrsmitteln ohne Vorliegen weiterer Voraussetzungen möglich. Da eine solche schrankenlose Erlaubnis absolut **unverhältnismäßig** wäre, sollte der Tatbestand umformuliert werden. Den Erläuterungen ist zu entnehmen, dass Sachverhalte wie zB **Stra-**

ßenkunst und Auftritte bei Veranstaltungen erfasst sein sollen. Dies sollte im Gesetzestext auch klarer zum Ausdruck kommen.

Zu Abs 3 Z 3 Zustimmung

Auf die jederzeitige Widerrufsmöglichkeit einer erteilten Zustimmung ist hinzuweisen.

Zu Abs 3 Z 4: Echtzeitwiedergabe

Zuzustimmen ist, dass eine Echtzeitüberwachung in Hinblick auf die fehlende Beweissicherungsmöglichkeit und geringere Missbrauchsgefahr grundsätzlich weniger Eingriffstiefe haben wird. Allerdings kommt es dabei auch sehr auf den Kontext an. Die Betrachtung von massenhaft vorbeiströmenden Menschen in einem Großkaufhaus ist anders zu beurteilen als ein Echtzeitmonitoring, das Personen in besonderen Abhängigkeitssituationen erfasst (Arbeitsplatz, Schule uä). Auf die Notwendigkeit, Missbrauchspotential mit zu bedenken, wurde bereits eingangs hingewiesen (Missbrauch von Bilddaten von Mitarbeitern in deutschen Diskontsupermärkten).

Vor diesem Hintergrund sollte der Abs zB in folgender Weise ergänzt werden: *„Dient die Überwachung dem Schutz von Eigentum, ist sie derart durchzuführen, dass eine gezielte Verhaltenskontrolle von Personal oder anderen Personen, die regelmäßig – etwa aufgrund einer Anwesenheitspflicht – anwesend sind, ausgeschlossen ist."*

Zu Abs 3 Z 5 a: Gefährlicher Angriff

Dem Entwurf zufolge reicht es, wenn der Auftraggeber auf einen Vorfall (innerhalb der strafrechtlichen Verjährungsfrist) verweisen kann und eine Wiederholung wahrscheinlich ist. Erfasst wären damit auch vergleichsweise geringfügige Sachbeschädigungen. Diebstähle von auch geringwertigeren Sachen etc. Aus BAK-Sicht sollte dieser besonders weite Erlaubnistatbestand mit Blick auf das Verhältnismäßigkeitsgebot restriktiver formuliert werden:

- **Nachweis einer überdurchschnittlichen Gefährdungslage und eines besonderen Schadensausmaßes:** Bei bestimmten Auftraggebern wird ohne weiteres eine solche besondere Gefahr bzw. – gegebenenfalls – ein nicht nur bagatellhafter Schaden oft pauschal angenommen werden dürfen (etwa Banken, Juweliere, Taxigewerbe). **Dies gilt insbesondere wenn die Überwachung dem Schutz von Personen dient.** Aus BAK-Sicht sollte jedoch nicht jedes denkbare Eigentumsdelikt zum Anlass genommen werden können, Videoüberwachung einzusetzen. **Hohe finanzielle Schadensrisken sollten die Voraussetzung sein**. In derartigen Fällen wird der Auftraggeber anhand der Umstände glaubhaft machen müssen, weshalb es sich bei seinem Überwachungsanliegen nicht bloß um die Abwehr vergleichsweise bagatellhafter, allgemeiner Risken (zB geringfügiger Ladendiebstahl) handelt, die durch andere Maßnahmen (Versicherung, Alarmanlagen, Warensicherung uvm) auch in den Griff zu bekommen wären.

- **Befristete Genehmigung – danach Nachweis des Fortbestands der Gefahr:** Um zu verhindern, dass ein einmaliger Vorfall (zB Diebstahl) zum Anlass genommen wird, eine Videoüberwachungsanlage unlimitiert über Jahrzehnte zu betreiben, sollte zumindest in Hinblick auf den „Erlaubnistatbestand" des § 50a Abs 3 Z 5a eine Befristung von zB 2 Jahren festgelegt werden, nach deren Ablauf der Auftraggeber den Fortbestand des Risikos (bei sonstigem Wegfall der Registrierung und damit der Zulässigkeit) nachzuweisen hat. Diese Maßnahme wäre nicht zuletzt deshalb wichtig, weil dem Entwurf zufolge es für den Nachweis einer Gefährdung reicht, dass ein gefährlicher Angriff sich (bezüglich mancher Deliktsarten) innerhalb der letzten zehn Jahre ereignet hat.

Zu Abs 3 Z 5 d Wertgrenze

Videoüberwachung wäre dem Entwurf zufolge auch ohne Nachweis eines bereits erfolgten gefährlichen Angriffs auf das zu schützende Gut möglich. Dann nämlich, wenn es sich um einen besonders hochwertigen, beweglichen Gegenstand handelt. Unklar ist, ob von dieser Regelung tatsächlich nur Objekte erfasst sind, deren **Einzelwert 100.000 Euro** übersteigt. Würde sich die Überwachungserlaubnis auf alle Geschäfts- oder Betriebsräume erstrecken, in denen sich Sachgüter befinden, deren **Gesamtwert** diesen Betrag übersteigt, so käme dies **einer generellen Überwachungserlaubnis im Handel und an vielen Arbeitsplätzen** gleich. Aus BAK-Sicht wäre deshalb unbedingt darauf zu achten, dass zumindest in den Erläuterungen darauf hingewiesen wird, dass sich die Wertgrenze auf Einzelgegenstände bezieht.

Andernfalls wären zusätzliche Einschränkungen mit Blick auf berechtigte Datenschutzinteressen von Kunden und Mitarbeitern unbedingt erforderlich: Etwa (wie schon unter Z 5a ausgeführt) der Nachweises einer **extremen Gefahrenlage.** Banken und Juweliere u.ä können wiederum eine besondere Gefährdungslage (sowie ein besonders hohes Schadensausmaß) im Falle eines Diebstahls oder Raubes im Vergleich zu anderen Branchen glaubhaft machen. Videoüberwachung in jeder Textilkette oder jedem Supermarkt wäre aus BAK-Sicht jedoch keinesfalls ein angemessenes Mittel. Der Schaden, der aus einem einzigen Vorfall resultiert, ist überschaubar. Kommt es regelmäßig zu Entwendungen, so kann sich der Auftraggeber ohnedies auf Abs 5 a) stützen.

Zu Abs 3 Z 7 Beweismittelsicherung für die Durchsetzung gerichtlicher Ansprüche

Die Bestimmung ist aus AK-Sicht ersatzlos zu streichen oder maßgeblich einzuschränken: Der Erlaubnistatbestand würde in der Praxis zwangsläufig dazu führen, dass Beweismittel quasi auf Vorrat in Erwartung eines künftig möglicherweise eintretenden Rechtskonfliktes gesammelt werden. Als Generalermächtigung ausgelegt dient nämlich nahezu jede Videoüberwachung auch dazu, bei Vorfällen über Beweismittel zu verfügen. Aus der Störung, Beschädigung oder Entwendung von Eigentum oder auch einem Personenschaden resultieren immer rechtliche Ansprüche, die gerichtlich geltend gemacht werden können. Dem einschränkenden Hinweis in den Erläuterungen, dass der An-

spruch schon manifest sein soll, würde - ist zu befürchten - in der Praxis wenig Bedeutung zukommen.

Weitere Anmerkungen dazu siehe Abs 2

Zu Abs 4 Überwachungsschranken für Behörden und Überwachungsverbot im höchstpersönlichen Lebensbereich

Bezüglich der Bedenken an einer Zusammenführung von Überwachungsinteressen von hoheitlich agierenden Behörden und Privatrechtsträgern in denselben Bestimmungen verweisen wir auf unsere Anmerkungen zu Abs 1.

Das explizite Überwachungsverbot in „höchstpersönlichen Bereichen" (sofern nicht lebenswichtigen Interessen berührt sind oder eine Zustimmung vorliegt) wird grundsätzlich begrüßt.

- Die Erläuterungen erwähnen beispielshaft **Privatwohnungen, Umkleidekabinen und WCs.** Die beispielshafte Aufzählung sollte sich angesichts des äußerst unbestimmten Gesetzesbegriffs im Gesetzestext selbst wiederfinden.
- **Auch Arbeitsplätze zählen zu den hochsensiblen Überwachungsbereichen**. Videodaten können nur allzu leicht (wie die Praxis zeigt) zu Verhaltens- und Leistungskontrollen missbraucht werden. Vor diesem Hintergrund sollte mit einer eigenen Bestimmung klargestellt werden, dass **Videoüberwachung an Arbeitsorten überhaupt nur zulässig sein kann, wenn der überwachte Bereich nachweislich** (zB aufgrund des Installationsortes der Kameras) **keine gezielte Mitarbeiterkontrolle erlaubt** (Ausnahme: lebenswichtige Interessen des Mitarbeiters – etwa im Bankenbereich). Siehe auch **Kapitel Fehlende Bestimmungen zur Videoüberwachung.**
- **Die Ausnahme vom Überwachungsverbot (Zustimmungserklärung) ist in Hinblick auf rechtliche Abhängigkeitsverhältnisse äußerst problematisch**, da die Freiwilligkeit und damit die Wirksamkeit einer Zustimmung regelmäßig bezweifelt werden muss. Da derartige Überwachungsvorhaben in der Regel massiv die Menschenwürde berühren, sollte von einer Zulässigkeit der Überwachung höchstpersönlicher Orte und Arbeitsplätze aufgrund einer Zustimmung überhaupt abgegangen werden. Auch bezüglich der Überwachung von Privatwohnungen sollte einschränkend angemerkt werden: *„soweit nicht andere Vorschriften, die dem Schutz von Persönlichkeitsrechten und allgemein der Menschenwürde dienen, dem nicht entgegenstehen."*

Fehlende Spezialvorschriften für Videoüberwachung, die Arbeitnehmer erfasst

Ähnlich wie im höchstpersönlichen Bereich ein Überwachungsverbot gilt, das nur in wenigen Ausnahmefällen durchbrochen werden kann, wäre dies auch explizit für die Überwachung von Orten notwendig, an denen sich Arbeitnehmer regelmäßig aufhalten. Die Situationen sind in ihrer Brisanz durchaus vergleichbar: In beiden Fällen

- wird allzu leicht die Menschenwürde berührt
- wirkt sich Missbrauch besonders schädlich auf die Betroffenen aus.

Aufgrund gesetzlicher Vorschriften sind die **Arbeitgeber verpflichtet, für Sicherheit und Gesundheitsschutz der Arbeitnehmer in Bezug auf alle Aspekte, die die Arbeit betreffen, zu sorgen** (§ 3 Abs 1 ASchG). Eine spezifisch gesetzliche Regelung in Hinblick auf Videoüberwachung in Arbeitsstätten gibt es nicht, wäre allerdings dringend erforderlich. Bei der gesetzlichen Regelung der Videoüberwachung sollte der in einem Arbeitsverhältnis immanenten persönlichen Abhängigkeit des Arbeitnehmers Rechnung getragen werden.

- Werden Menschen in der Öffentlichkeit überwacht, sind sie in der Regel demjenigen, der die Überwachungsmonitore oder Aufzeichnungen anschaut, nicht bekannt. Im Arbeitsverhältnis verhält es sich demgegenüber ganz anders, die Personen sind bekannt, es kann daher zu einem sehr viel stärkeren Überwachungs-, Anpassungs- und auch Einschüchterungsdruck kommen.

- Videoüberwachungsanlagen lösen erfahrungsgemäß bei den betroffenen Arbeitnehmern negative Gefühle aus. Sie können das Wohlbefinden, die psychische Gesundheit und damit die Leistungsfähigkeit der Arbeitnehmerinnen beeinträchtigen.

- Schon derzeit ist eine Videoüberwachung als technisches Kontrollinstrument oder Kontrollmaßnahme zur Kontrolle der Arbeitnehmer, sofern durch diese Maßnahme die **Menschenwürde verletzt wird, unzulässig** (bspw. Kameraüberwachungssysteme in Toiletten, Waschräumen oder wenn eine Kamera dauernd auf den Arbeitsplatz eines Arbeitnehmers gerichtet ist). Wird dadurch die Menschenwürde zwar nicht verletzt aber dennoch **berührt** (bspw. wenn sich der Arbeitsbereich im Blickfeld der Kamera befindet oder die Überwachung im Betrieb ein solches Ausmaß erreicht, dass beim Arbeitnehmer das Gefühl dauernder Überwachung entstehen kann), kann Videoüberwachung nur dann eingesetzt werden, wenn zuvor eine **Betriebsvereinbarung** abgeschlossen wurde (§ 96 ArbVG) bzw wenn kein Betriebsrat vorhanden ist, die **Zustimmung der einzelnen ArbeitnehmerInnen** eingeholt wurde (§ 10 AVRAG). Selbst wenn die Menschenwürde nicht einmal berührt wird, fällt die Anwendung unter § 96a ArbVG (Personaldatensysteme), und der AG hat demnach vor Installation mit dem Betriebsrat eine Betriebsvereinbarung abzuschließen.

Der geplante Abschnitt 9a trägt den besonderen Erfordernissen im Arbeitsverhältnis nicht Rechnung. Die BAK fordert daher eine eigene Regelung zur Videoüberwachung am Arbeitsplatz, unabhängig davon ob diese analog oder digital erfolgt.

Alle bisher genannten Anliegen betreffend Videoüberwachung sind der BAK in Hinblick auf die Überwachung von Arbeitsplätzen ganz besonders wichtig. Als elementare Voraussetzungen (nach den allgemeinen DSG-Bestimmungen) sollten sie für jeden Anlassfall gelten. Soweit die BAK-Anliegen nicht generell berücksichtigt werden, so muss (im Wege einer speziellen Vorschrift) sichergestellt sein, dass die folgenden Grundsätze für Videoüberwachung am Arbeitsplatz jedenfalls ausnahmslos gelten:

- die **Voraussetzungen zu normieren**, unter denen Videoüberwachung am Arbeitsplatz zulässig sein soll und
- welche **Mindestanforderungen in schriftlichen Regelungen** zwischen dem Arbeitgeber und dem Betriebsrat bzw Arbeitnehmer (wenn kein Betriebsrat vorhanden ist) **zu vereinbaren und kundzumachen** sind.
- Generell muss gelten, dass die offene (unverdeckte) Videoüberwachung am Arbeitsplatz die **streng begrenzte Ausnahme** ist.
- Eine **heimliche Videoüberwachung muss immer verboten** sein, weil dadurch die Menschenwürde verletzt wird.
- Die Videoüberwachung ist örtlich **immer geeignet zu kennzeichnen**. Akustische Überwachung oder Aufzeichnung soll ausgeschlossen sein.
- Beim Einsatz einer Videoüberwachung ist zu vermeiden, dass es zu einer permanenten zeitlichen oder örtlichen Überwachung der Arbeitnehmer kommt.
- Für die Videoüberwachung am Arbeitplatz gelten die allgemeinen Voraussetzungen: es ist ein geeigneter Zweck zu definieren, sie muss zur Zweckerreichung geeignet sein, das gelindeste Mittel darstellen und darf nur im erforderlichen Ausmaß eingesetzt werden. Das bedeutet, dass eine Verhältnismäßigkeitsprüfung in jedem einzelnen Fall stattfinden muss. Weiters hat in jedem Fall eine Interessenabwägung zu erfolgen.

Die BAK fordert daher eine Regelung wie folgt:

1. Videoüberwachung am Arbeitsplatz soll stets die streng begrenzte Ausnahme sein. Eine heimliche Videoüberwachung soll immer verboten sein.

2. Für die Zulässigkeit einer Videoüberwachung am Arbeitsplatz müssen folgende Voraussetzungen erfüllt sein:

- Videoüberwachung muss zur Erreichung eines rechtmäßigen Zwecks geeignet sein, sie muss das gelindeste aller zur Zweckerreichung zur Verfügung stehenden Mittel sein und sie ist nur im erforderlichen Ausmaß einzusetzen. Die Verhältnismäßigkeitsprüfung muss in jedem einzelnen Fall stattfinden.
- Videoüberwachung ist nur zulässig, wenn sie durch die Wahrnehmung überwiegend schutzwürdiger Interessen des Arbeitgebers gerechtfertigt ist. Bei Videoüberwachung am Arbeitsplatz hat daher in jedem Fall eine Interessenabwägung unter Berücksichtigung der Umstände des Einzelfalles zu erfolgen. (Videoüberwachung ist beispielsweise dann nicht zulässig, wenn die Überwachung **nicht auf einen bestimmten – angemessen kurz zu haltenden – Zeitraum oder örtlich auf eine spezielle Perspektive, aus der sich der Arbeitnehmer überwiegend zurückziehen** kann, beschränkt ist und kein hinreichend begründeter Anfangsverdacht vorliegt, wobei auch

die Zumutbarkeit der Inanspruchnahme von behördlicher Hilfe zu prüfen ist.). Eine akustische Überwachung oder Aufzeichnung ist auszuschließen.

Eine systematische Anwendung von Videoüberwachungssystemen im Unternehmen greift stärker in das Persönlichkeitsrecht der betroffenen Arbeitnehmer ein und ist bei der Prüfung der Voraussetzungen nach Abs 1 und 2 entsprechend zu berücksichtigen.

3. Vor Einsatz der Videoüberwachung sind **Mindestanforderungen in schriftlichen Regelungen zwischen dem Arbeitgeber und dem Betriebsrat** (Betriebsvereinbarung iSd ArbVG) **bzw zwischen Arbeitgeber und Arbeitnehmer** (arbeitsvertragliche Regelung, wenn kein Betriebsrat vorhanden ist) zu vereinbaren und gehörig kundzumachen. Der betriebliche Datenschutzbeauftragte hat beratend mitzuwirken. Zu den Mindestinhalten zählen zB Ausschluss einer Verhaltenskontrolle, Kamerastandorte, Auswertung nur bei Verdacht auf strafrechtsrelevantes Verhalten uvm.

4. Die Videoüberwachung am Arbeitsplatz darf ohne ausdrückliche Genehmigung durch die Datenschutzkommission nicht eingesetzt werden. Die Vereinbarung über die Mindestanforderungen ist der Meldung an die Datenschutzkommission beizulegen.

5. Die Videoüberwachung ist den Beschäftigten und Besuchern durch entsprechende Hinweise erkennbar zu machen, bevor sie den Aufnahmebereich betreten.

Zu Abs 5 Umgang mit „Zufallstreffern"

Die Möglichkeiten einer Weitergabe von Bilddaten an Behörden oder Gerichte im Falle von „Zufallstreffern", die über den eigentlichen Überwachungszweck hinausgehen, sind viel zu weitreichend. Zu bedenken ist, dass Behörden und Gerichte ohnedies eine Herausgabe von Beweismaterial verlangen können. Vor diesem Hintergrund sollte die Funktion der Auftraggeber als „Hilfssheriffs" grundsätzlich nicht zulässig sein. Eine Ausnahme ist aus BAK-Sicht nur im Falle ganz offensichtlicher Straftaten vertretbar. Übermittlungen von Auftraggebern aufgrund bloßer Mutmaßungen und ohne Rechtskenntnisse können ansonsten sehr rasch unerwünschte, ausufernde Dimensionen erreichen:

- Ob ***„eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung"*** (Ziffer 1) auf den Bildern dokumentiert ist, kann vom verantwortlichen Überwacher eventuell noch richtig eingeschätzt werden. Die Zulässigkeit der Datenübermittlung sollte sich aber **auf ganz offenkundige Straftaten (und nicht auf einen bloßen Verdacht)** beschränken .Der Halbsatz *„weil beim Auftraggeber der begründete Verdacht entstanden ist"* ist deshalb unbedingt zu streichen und statt dessen einzufügen: *"..., weil die Daten offenkundig eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren"*.

- Ob die Bilder **„der Abwehr oder Beendigung eines gefährlichen Angriffs dienen“**, kann der Auftraggeber kaum abschätzen. Das Risiko überschießender Übermittlungen aufgrund von Missinterpretation des Bildinhaltes zulasten von Betroffenen wäre unvertretbar. **Ziffer 2 sollte deshalb ersatzlos gestrichen werden.**

Zu Abs 6 Verbot des Datenabgleichens

Die Regelung wird begrüßt.

Zu Abs 7 Verhältnismäßigkeit

Weder die Platzierung noch der allgemeine Verweis auf § 7 Abs 3 DSG wird der Bedeutung dieser Zulässigkeitsvoraussetzung annähernd gerecht. Näheres dazu siehe Anmerkungen zu Abs 3.

Zu § 50c Meldepflicht

Die Ausnahmen von der Meldepflicht sollten überdacht werden: Von der Meldepflicht ausgenommen wird die **Echtzeitüberwachung**. Zu bedenken ist, dass auch diese Überwachungsform zB kennzeichnungspflichtig ist. Kommt ein Auftraggeber aus Nachlässigkeit seiner Pflicht nicht nach, wäre die Meldung - soweit zumindest diese Pflicht beachtet wurde - die einzige Chance für Betroffene auf Transparenz.

Auch Aufzeichnungen auf **analogen Speichermedien** sollen nicht meldepflichtig sein. Begründet wird dies mit der sehr beschränkten Strukturierbarkeit und gezielten Auffindbarkeit bestimmter Daten, womit die Gefährdung von Geheimhaltungsinteressen unbeteiligter Dritter deutlich herabgesetzt sei. Da analoges Videomaterial ohne besonderen Aufwand digitalisierbar ist, könnte die Umgehungen begünstigen.

Zu § 50d: Kennzeichnung

Die Kennzeichnungspflicht wird als eines der Kernstücke der Regelung betrachtet. Absolute Transparenz ist unverzichtbar. Vor diesem Hintergrund fordert die BAK auch eine ausnahmslose Kennzeichnungspflicht:

- Dass die Kennzeichnung entfallen kann, wenn die Beeinträchtigung von Betroffenenrechten unwahrscheinlich oder für den Auftraggeber die Kennzeichnung zu kostspielig ist, schafft sehr weitreichende Ausnahmetatbestände. In der ersten Fallgruppe schadet eine Info jedenfalls nicht und ist dem Auftraggeber offensichtlich kostenmäßig auch zumutbar. In der zweiten Fallgruppe fehlt eine Abwägung mit der Eingriffsintensität ins Grundrecht: auch wenn die Kennzeichnung schwierig bzw teuer ist, sollte sie erfolgen, wenn die Beeinträchtigung für den Betroffenen nicht unwesentlich ist. **Im Ergebnis sollte dieser Ausnahmetatbestand unbedingt ersatzlos gestrichen werden.**

- Mit der Herausnahme mobiler Videoüberwachung aus dem Anwendungsbereich entfällt auch der Kernbereich der Ausnahme der Ziffer 2 **(Vereitelung der Beweismittelsicherung).** Aber auch bei fix installierten Kameras eröffnet die Ausnahme ein enormes Spannungsfeld zwischen dem Allgemeininteresse an Transparenz und dem individuellen Interesse an verdeckten Ermittlungen. Da im Regelfall ersteres überwiegt, **sollte auch diese Ausnahme unbedingt ersatzlos gestrichen werden.**

Ausnahmen würden auch ein **Abgehen von den Transparenzprinzipien des § 24 DSG 2000 bedeuten**. **Heimlichkeit berührt außerdem die Menschenwürde**: Arbeitgeber könnten bspw ein überwiegendes Interesse an einer heimlichen Videoüberwachung im Kassabereich behaupten, wiewohl dadurch unzweifelhaft die Menschenwürde der betroffenen Arbeitnehmer berührt würde (vgl. dazu auch die Materialien zu § 10 AVRAG ErlRV 1590 BlgNR 18. GP 128); Auch der **OGH hat eine verdeckte Videoüberwachung** mit abrufbarer Bildaufzeichnung immer als einen **Eingriff** in das gemäß § 16 ABGB iVm Artikel 8 MRK geschützte Recht auf Achtung der Geheimsphäre bezeichnet (OGH 19.12.2005, 8 Ob 108/05y).

Vollziehung des Abschnittes „Videoüberwachung"

Praktische Folge gesetzlicher Restriktionen wird sein, dass nicht alle bestehenden Anlagen (geschätzte Zahl 200.000) als zulässig einzustufen sind und demontiert werden müssen. Da ein Großteil der in Betrieb befindlichen Kameras nicht ordnungsgemäß gemeldet wurde, zeichnen sich Vollzugsdefizite ab. Diesen sollte rechtzeitig begegnet werden, zB

- durch eine gesetzlich fixierte „**Nachmeldefrist**", nach deren Verstreichen spürbare **Verwaltungsstrafen** verhängt werden können
- in Form **erweiterter Ermittlungsbefugnisse der Datenschutzkommission**, zB einer **unangekündigten** Einschau vor Ort, **Sanktionen** bei Verweigerung des Zutritts uä
- Zu regeln wäre unbedingt auch, wie **Beseitigungsansprüche** effizient und kostengünstig (zivil- oder verwaltungsrechtlich; auf Initiative der DSK) durchgesetzt werden können
- Auch für andere Verstöße (etwa gegen die Kennzeichnungspflicht) sind in § 52 **Verwaltungsstrafen** vorzusehen oder bestehende Strafbestimmungen zu adaptieren.

Sonstige Anpassungen im DSG

§ 26 Auskunftsrecht

Die Auskunft über **die Herkunft von Daten** ist nur zu erteilen, wenn diese Informationen **noch verfügbar** sind. Wollen Auftraggeber die zweifelhafte Herkunft von Daten aus gutem Grund verschleiern, teilen sie mit, dass die Daten nicht mehr verfügbar sind. Lösungsvorschlag: Die Herkunft ist immer zu beauskunften (Ausnahme: der Auftraggeber macht glaubhaft, warum eine Protokollierung der Datenherkunft ein unverhältnismäßiger Aufwand wäre und das Fehlen der Information den Betroffenen nicht bei der Durchsetzung seiner Rechte auf Löschung usw. beeinträchtigt).

Die Auskunft ist außerdem zu erteilen über **"Empfänger oder Empfängerkreise"** von Daten. Wann es reicht, bspw nur eine Branche als Datenadressat zu bezeichnen (zB Banken, Versicherungen, Wirtschaftsauskunfteien usw) und wann das konkrete Unternehmen anzugeben ist, gerät häufig zum Streitpunkt. Lösungsvorschlag: auch hier ist immer der konkrete Empfänger zu nennen (Ausnahme: wie oben).

Leichterer Zugang zur Rechtsdurchsetzung

Der **Zugang zur Rechtsdurchsetzung** der Betroffenen gegenüber **privaten Auftraggebern** ist unbedingt zu erleichtern. Die erstinstanzliche zivilgerichtliche Zuständigkeit mit Anwaltszwang stellt für viele Betroffene eine Hürde dar. Obwohl die Datenverarbeitungen auf Seiten privater Unternehmen in den letzten Jahren rasant gestiegen sind und sich damit auch Rechtsverletzungen bzw. das Missbrauchspotential zwangsläufig vergrößert haben müssen, werden nur selten Ansprüche eingeklagt. Vor diesem Hintergrund wäre es wichtig, das **Ombudsmannverfahren der Datenschutzkommission zeitgemäß und bedarfsgerecht auszubauen.**

Einführung eines österreichischen Datenschutz-Gütesiegels:
Ein derartiges Vorhaben wird von der BAK unterstützt.

Mit freundlichen Grüßen

Herbert Tumpel
Präsident

BUNDESARBEITSKAMMER

Johanna Ettl
iV des Direktors