BUNDESARBEITSKAMMER

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

www.arbeiterkammer.at

Bundeskanzleramt
zH Herrn Mag Alexander Flendrovsky
Ballhausplatz 2
1014 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel 501 65	Fax 501 65	Datum
810.026/00 05-V/3/09	BAK-KS/GSt/DZ/GS	Mag Daniela Zimmer	DW 2722	DW 2693	10.06.2009

Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010)

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, dass im Zuge der Überarbeitung des Erstentwurfes manche Bedenken ausgeräumt und einige Anliegen aufgegriffen worden sind. Wir möchten allerdings auch auf unsere umfangreiche Stellungnahme zum Erstentwurf aus 2008 verweisen und unser Bedauern ausdrücken, dass der Entwurf in mancher Hinsicht hinter unseren Erwartungen zurückbleibt.

Das Datenschutzrecht wird den gegenwärtigen Herausforderungen nur gewachsen sein, wenn es auf die fortschreitende Technologieentwicklung und ihrem Gefährdungspotential für die Privatsphäre – nicht zuletzt innerhalb der Arbeitswelt - auch ausdrücklich eingeht. Das DSG behält auch mit diesem Entwurf weiter den Charakter eines Schutzgesetzes vorrangig vor Eingriffen staatlicher Behörden – erkennbar etwa an den unterschiedlich hohen Hürden für den Zugang zum Recht abhängig davon, ob jemand von privaten oder behördlichen Datenanwendungen nachteilig betroffen ist.

Tatsächlich ist die Zahl problematischer Datenanwendungen vor allem im privatwirtschaftlichen Bereich exorbitant gewachsen. Vor diesem Hintergrund ist an ein zeitgemäßes Datenschutzgesetz die Anforderung zu stellen, über die spezifischen Regelungen zur privaten Videoüberwachung hinaus auch auf andere neuere Entwicklungen (zB schutzwürdige Geheimhaltungsinteressen im Internet, RFID u.v.m.) einzugehen, die beträchtlichen Rechtsschutzhürden für die Betroffenen bei mutmaßlichen Datenschutzverletzungen privatwirtschaftlicher Auftraggeber

abzubauen und bspw. durch die Einführung eines betrieblichen Datenschutzbeauftragten eine wirksamere Durchsetzung von Datenschutzbestimmungen in der Arbeitswelt zu ermöglichen.

Zusammengefasst

wird ausdrücklich begrüßt

- die Infopflicht des Auftraggebers bei schwerwiegenden Datenschutzverletzungen
- die strikteren Kennzeichnungsvorschriften für private Videoüberwachung
- die Klarstellung, dass Mitarbeiterkontrolle mittels Videoüberwachung jedenfalls untersagt ist
- die etwas adaptierten Auskunftsrechte über die Herkunft von Daten

Keinen Niederschlag findet aber das besondere Schutzbedürfnis

- von ArbeitnehmerInnen durch die inzwischen vollständige Durchdringung der Arbeitswelt mit IKT-Systemen
- von Internetnutzern, die in bestimmten Umfang Kontrolle über sie betreffende, im Internet veröffentlichte Daten behalten wollen
- von Konsumenten, deren Privatsphäre und Datenschutzrechte durch den Einsatz neuer Technologien, wie RFID, Scoringmethoden u.v.m beeinträchtigt werden können und
- von Betroffenen, die im Falle einer mutmaßlichen Verletzung ihrer Datenschutzrechte durch Auftraggeber der Privatwirtschaft, vor den erheblichen Rechtsschutzhürden regelmäßig zurückschrecken (Anwaltspflicht und Kostenrisiko einer Klage vor den GH 1.Instanz)

Vor diesem Hintergrund hält die BAK - wie im Wesentlichen auch schon in ihrer Stellungnahme zum Erstentwurf 2008 im Detail ausgeführt – u.a. folgende Maßnahmen für unbedingt notwendig:

- **einen betrieblichen Datenschutzbeauftragten - zumindest in größeren Betrieben**: Der Umstand, dass die Wirtschaftsseite die Einführung eines betrieblichen Datenschutzbeauftragten ablehnt, sollte nicht dazu führen, vom Vorhaben gänzlich abzusehen. Aus BAK-Sicht sollte diese an sich dringend erforderliche Maßnahme zumindest im Ansatz erhalten bleiben und allenfalls die genaue Ausgestaltung (Betriebsgröße, Kompetenzen) überarbeitet werden. So können und sollten Großunternehmen und der öffentliche Bereich diesbezüglich eine Vorreiterrolle einnehmen.

- **Mehr Schutz bei vorgefertigten Zustimmungserklärungen:** Nötig sind Transparenzvorschriften für Datennutzungsklauseln und in bestimmten Fällen Schriftlichkeitsgebote für erteilte Zustimmungen, um unseriösen Praktiken im Marketingbereich zu begegnen. Generell **Ausscheiden sollten Zustimmungserklärungen in Abhängigkeitssituationen, allen voran im Zusammenhang mit Arbeitsverhältnissen**, da von der Freiwilligkeit einer Zustimmung dabei nicht ausgegangen werden kann.

- ein **Beweisverwertungsverbot** für unrechtmäßig erlangte Daten mit Personenbezug, um dem Trend, sich ohne nennenswerte praktische Konsequenzen unfaire Vorteile durch günstigere Prozessaussichten in (arbeits-/zivil-) gerichtlichen Auseinandersetzungen verschaffen zu können, wirksam zu begegnen.

- eine grundsätzliche **Anerkennung der Schutzwürdigkeit auch von allgemein im Internet verfügbaren Daten** und Klarstellung, dass das **Widerspruchsrecht nach § 28 DSG** auch auf selbst- bzw fremdgenerierte Einträge mit Personenbezug im Internet anwendbar ist.

- **Datenschutzrechtliche Anforderungen an die Betreiber von Suchmaschinen**, etwa Zustimmungserfordernisse vor der Aufnahme in Personensuchmaschinen; Diensteanbieter haben Web 2.0 Nutzern technisch zu ermöglichen, die Suchmaschinenindizierung individueller Einträge zu unterbinden; Pflicht der Suchmaschinenbetreiber auf solcherart gekennzeichnete Inhalte auch nicht zuzugreifen.

- Verankerung der **Info- und Deaktivierungspflichten für die Anwender von RFID-Systemen** entsprechend der jüngsten Mitteilung der EU-Kommission aus 5/2009 im DSG

- **Zusätzliche Restriktionen für private Videoüberwachung,** etwa Aufnahme des Gebots, zunächst gelindere Mittel einzusetzen (Sicherheitstüren, Echtzeitüberwachung, Alarmanlagen, Warensicherungen uvm) aus den Erläuterungen direkt ins DSG; Befristung der Genehmigungen (Prüfung des Fortbestands/Wegfalls des Überwachungsinteresses); explizites Beweisverwertungsverbot für unzulässige Videoaufzeichnungen; Einsatz nur zur Abwehr und Verfolgung von gerichtlich strafbaren Delikten nicht aber für zivilgerichtliche- und verwaltungsrechtliche Auseinandersetzungen; keine wirksame Zustimmung zu Überwachungsmaßnahmen am Arbeitsplatz; keine Sekundärverwertung von Videoaufzeichnungen für Bagatellangelegenheiten (Datenweitergabe nur in Fällen, die dem Registriergrund zumindest gleichzuhalten sind).

- **Abbau von Rechtsschutzhürden: Verbandsklagsbefugnis** für Verbraucher- bzw Datenschutzorganisationen auch bei mutmaßlichen Datenschutzverletzungen, Stärkung der **Ombudsmannfunktion** der DSK, eine **leichtere Rechtsdurchsetzung** gegenüber privatwirtschaftlichen Auftraggebern, etwa für ArbeitnehmerInnen bei Datenschutzkonflikten mit engem Bezug zum Arbeitsverhältnis durch Verschiebung der Zuständigkeit zu den **Arbeits- und Sozialgerichten**

Zu den einzelnen Anliegen:

Allgemein verfügbare Daten § 1 Abs 1, § 8 Abs 2 iVm § 28

Sind Daten einmal zulässigerweise öffentlich zugänglich, dann wird ihnen in weitreichender Weise die Schutzwürdigkeit abgesprochen. Angesichts des Umfangs von im Internet veröffentlichten Daten, erscheint dieser Grundsatz in dieser Allgemeinheit inzwischen überholt.

Jeder, sei es als Blogger, Teilnehmer eines Chat- oder Diskussionsforums oder einer Online-Community, hinterlässt personenbezogene Angaben. Inzwischen ist es gängige Praxis geworden, nach einem Namen zu "googeln", wenn man etwas über eine Person (zB einem Jobbewerber) erfahren will. Internetkommentare, Forenbeiträge enthalten oft Informationen aus dem Privatleben, gerichtet vorrangig an einen definierten Freundes- oder Bekanntenkreis, aber letztlich häufig jedermann zugänglich. Jedwede Marketingnutzung dieser Daten, das Herstellen von Kopien auf anderen Webseiten, das Anlegen von Surfprofilen, die Datennutzung auch noch lange nach Löschung auf der Ursprungsseite etc. sollte nicht allein schon dadurch gerechtfertigt sein, dass die Daten auf einer Website zugänglich sind. Aus dem Umstand, dass personenbezogene Daten an einer Stelle frei zugänglich gehalten werden, kann nicht unmittelbar geschlossen werden, dass eine Schutzbedürftigkeit des Betroffenen bezüglich der Weiterverwendung in jedem anderen denkbaren Kontext und einer unlimitierten Weiterverbreitung nicht vorhanden wäre. Gerade für den Datenhandel sollten sich bei grundsätzlicher Anerkennung, dass an veröffentlichten Personendaten in bestimmten Umfang auch schutzwürdige Geheimhaltungsinteressen bestehen können, Grenzen ergeben. In der Praxis wird das Internet intensiv nach Angaben, die ein Personenprofil ergeben, durchkämmt, analysiert und verkauft. Gehen Nutzungseinschränkungen aus Webseiten klar hervor, wären etwa kommerzielle Datenverwertungen jedenfalls unzulässig.

Die EU-Datenschutzrichtlinie enthält selbst keinerlei Hinweis darauf, dass die Privatsphäre, sobald Daten zulässig veröffentlicht wurden, keinerlei Schutz mehr genießen darf. Schutzwürdige Geheimhaltungsinteressen sollten daher auch als verletzt gelten, wenn die Weiterverwendung von allgemein zugänglichen Daten mit dem ursprünglichen Zweck nicht im Einklang steht.

Es wird eine Änderung der §§ 1 und 8 Abs 2 DSG angeregt, mit der sichergestellt wird, dass zulässig veröffentlichte Daten nur in einer mit dem ursprünglichen Veröffentlichungszweck vereinbaren Weise genutzt werden dürfen.

Weiterer Adaptionsbedarf:

- Derzeit sind Web 2.0- Nutzer auch bei den einfachsten Datenschutzmaßnahmen auf den Goodwill der Anbieter angewiesen. Web 2.0 (Facebook, My Space uä) Nutzer sollten die Kontrolle über einmal im Internet veröffentlichte Daten behalten, etwa das Recht haben,

- **für selbsterzeugte Inhalte ein Verfallsdatum** vorzusehen. Internetnutzer beklagen aus unserer Sicht zu Recht, dass Internetbeiträge, die über viele Jahre im Netz hängen ein überholtes Bild von einer Person zeichnen ohne dass ein eindeutiger und leicht durchsetzbarer Anspruch auf eine Entfernung nach Ablauf einer bestimmten Zeit besteht.

- Eine Registrierung unter Nicknames wird derzeit nur zum Teil freiwillig angeboten, obwohl die Diensterfüllung bspw bei Web 2.0-Plattformen keinesfalls eine eindeutige Identifizierung voraussetzt. Jeder Web 2.0-Dienstanbieter sollte die Nutzung auch mit einem **Pseudonym** ermöglichen und
- **Suchmaschinenzugriffe** von der Zustimmung der Betroffenen abhängig machen.

- In diesem Zusammenhang sollten gängige Problemfälle mit **Internetsuchmaschinen** explizit angesprochen werden:

  - Personensuchmaschinen sollten Webeinträge über Personen nicht ohne deren Zustimmung verwerten dürfen (siehe dazu auch die Anforderungen der Art 29-Gruppe an Suchmaschinen WP 148/2008).
  - Diensteanbieter, die Nutzer zu selbstgestalteten Beiträgen einladen, sollten verpflichtet werden, eine Opt-Out-Funktion hinsichtlich einer Indizierung in Suchmaschinen anzubieten.
  - Der Wunsch von Betroffenen, die bezüglich ihrer Internetinhalte (etwa über den Robots Exclusion Standard), keine Suchmaschinen-Indizierung wollen, müsste von den Suchmaschinen-Betreibern beachtet und Widersprüchen gegen in Suchmaschinen aufgenommene Daten nach § 28 nachgekommen werden.

- Das **Widerspruchsrecht nach § 28** Abs 1 gestattet den Widerspruch gegen gesetzlich nicht vorgesehene Datennutzungen, wenn überwiegende schutzwürdige Geheimhaltungsinteressen verletzt sind. Abs 2 sieht ein begründungsloses Widerspruchsrecht vor, wenn der Betroffene in eine öffentlich zugängliche, aber nicht gesetzlich angeordnete Datei aufgenommen wurde. Beide Bestimmungen erfassen nicht die gängigsten Problemfälle des Internetzeitalters. Nicht jede Website oder Suchmaschine erfüllt den Dateienbegriff des DSG. Einen Widerspruch nur in begründeten Fällen nach Abs 1 zuzulassen, entspricht dem Rechtsschutzbedürfnis von Internetnutzern in keinster Weise. **Vor diesem Hintergrund sollte das Widerspruchsrecht nach Abs 2 auf alle selbstgenerierten, personenbezogenen Einträge im Internet ausgedehnt werden, bei fremdgenerierten Daten sollte zumindest das Widerspruchsrecht nach Abs 1 jedenfalls zur Verfügung stehen.**

Definition der Zustimmung § 4 Z 14

Im kommerziellen Bereich werden immer häufiger Daten basierend auf der Zustimmung der Betroffenen - vor allem für Marketingzwecke - verwendet. Der Rechtslage entsprechend sind Zustimmungen nur wirksam, wenn sie freiwillig und in Kenntnis der Sachlage und damit der Tragweite der Entscheidung getroffen werden.

In der Praxis übersehen die Betroffenen regelmäßig im Fließtext von Geschäftsbedingungen verborgene Zustimmungserklärungen bzw bekommen die dem Vertrag zugrundeliegenden Klauseln erst gar nicht zu Gesicht, etwa dann, wenn der Vertrag am Telefon abgeschlossen wird. Die Beweislast für die Wirksamkeit der Zustimmung trägt zwar der Verwender der Daten. Tatsächlich fallen den Betroffenen rechtswidrige Datennutzungen aufgrund fehlender, versteckter oder intransparenter Zustimmungserklärungen aber meist erst sehr spät auf - wenn Daten bereits weiterveräußert wurden und Haushalte etwa durch unerbetene Telefonwerbung belästigt werden. In mancher Hinsicht sind aber einfach die gesetzlichen Anforderungen an Opt-In/Opt-Out-Erklärungen nicht ausreichend.

Vor diesem Hintergrund sollte im DSG präzisiert werden, in welcher Deutlichkeit und Form Zustimmungserklärungen eingeholt werden können, um wirksam zu sein:

Zustimmungsklauseln sollten durch Hervorhebung des Textes und vom restlichen Vertrag getrennte Darstellung leicht erkennbar gemacht werden. In besonders missbrauchsgeneigten Bereichen – der Marketingnutzung durch Dritte, Adresshändler und Direktwerbeunternehmen, die nach § 151 GewO durch eine Opt-Out-Lösung privilegiert sind, aber auch andere Unternehmen, für die ein Zustimmungserfordernis gilt - sollte eine schriftliche Zustimmung erforderlich sein.

Weiters sollten jene Bereiche exemplarisch aufgezeigt werden, in denen Zustimmungserklärungen nicht zum Einsatz kommen sollten, weil ihnen die Freiwilligkeit grundsätzlich abzusprechen ist. In **Arbeitsbeziehungen** ist die Willensfreiheit eines Arbeitnehmers in der Regel derart verdünnt, dass von einer Einwilligung ohne jeden Zwang praktisch nicht ausgegangen werden kann. **Einige Verbrauchersituationen**, in denen Konsumenten mangels Angebotsalternative nur die Wahl haben, eine Zustimmung zu nachteiligen Datenschutzklauseln zu erteilen oder vom Geschäft gänzlich abzusehen, zählen ebenso dazu. Konsequenterweise wäre in derartigen Fällen ein Koppelungsverbot vorzusehen: Der Klauselverwender dürfte den Geschäftsabschluss nicht von der Erteilung einer Zustimmung abhängig zu machen, denn diesfalls wäre die Freiwilligkeit der Zustimmung derart in Zweifel zu ziehen, dass eine Zustimmungserklärung als Rechtsgrundlage für die Datennutzung eigentlich ausscheidet.

Beweismittelverwertungsverbot in § 8 Abs 3 Z 5 und § 9 Z 9

In Hinblick auf die wenig abschreckenden Strafsanktionen, die das DSG enthält und die in der Praxis zudem kaum verhängt werden, bedarf es anderer Maßnahmen, die wirksam davon abhalten, handfeste Vorteile aus unzulässigerweise erworbenen Daten zu ziehen. Datenschutzverstöße werden manchmal bewusst in Kauf genommen, um verwertbare Beweismittel sicher-

zustellen, die eine Streitpartei in Zivilprozessen (etwa bei Arbeitsrechtskonflikten) in eine vorteilhaftere Lage bringt. **Diesem Trend sollte durch ein ausdrückliches Beweisverwertungsverbot für unrechtmäßig erlangte Daten mit Personenbezug unbedingt Einhalt geboten werden.**

Meldepflichten §§ 17ff:

Eine Vereinfachung des Registrierungsverfahrens, die den Erfordernissen der Praxis gerecht wird, wird grundsätzlich unterstützt. Die Motive für die Neuregelung sind angesichts der rasant angestiegenen Zahl von Meldungen nachvollziehbar. Gegen die Einführung eines weitgehend automatisierten Prüfverfahrens für nicht-vorabkontrollpflichtige Verarbeitungen könnte ins Treffen geführt werden, dass Standardverarbeitungen schon jetzt als Filter für weitgehend unbedenkliche Datenanwendungen wirken. Der Rest – so der Umkehrschluss – muss eigens auf seine Unbedenklichkeit geprüft werden.

Das Register ist die einzige umfassende Informationsquelle für jedermann, der wissen möchte, welche Daten datenschutzrechtliche Auftraggeber verarbeiten. Die Richtigkeit und Vollständigkeit der Einträge darf deshalb durch ein Übergehen von Einzelprüfungen zu bloßer automatisierter Fehlersuche nicht beeinträchtigt werden. Schwachstelle einer automatisierten Prüfung ist die Abhängigkeit von den gemeldeten Angaben. § 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 Vorabkontrolle durchgeführt.

Infopflicht § 24

Die Einführung einer Infopflicht des Auftraggebers gegenüber Betroffenen bei schwerwiegenden Datenschutzverstößen in Abs 2 a wird außerordentlich begrüßt.

Angesichts der enormen Intransparenz vieler Datennutzungen kommt der Infopflicht nach § 24 inzwischen zentrale Bedeutung zu. Für das mit der Ausnahmebestimmungen des Abs 3 Z 3 eingeräumte, weitreichende Privileg besteht aus BAK-Sicht aber kein begründeter Anlass. Die Ausnahme sollte auf wissenschaftliche/statistische Zwecke beschränkt werden. Darüber hinaus sollten Einwände wegen der Höhe der Informationskosten bzw. der unwahrscheinlichen Beeinträchtigung von Betroffenenrechten keinesfalls von der Informationspflicht befreien.

Auskunftsrecht § 26

- **Herkunft der Daten**

Nach derzeitiger Rechtslage hat der Auftraggeber im Rahmen eines Auskunftsbegehrens nur "die verfügbaren Informationen über ihre Herkunft" bekanntzugeben. Diese Bestimmung verleitet Datennutzer insbesondere dann, wenn sie fragwürdig Datenquellen benutzen, dazu, zu behaupten, mangels Aufzeichnungen keine Angaben über die Datenherkunft machen zu können. Es wird deshalb ausdrücklich begrüßt, dass durch die Streichung des Wortes "verfügbar", Problembewusstsein signalisiert wird. Im Einzelnen bleibt die Tragweite dieser Textänderung unklar.

Der Begriff „verfügbare" Daten wurde der Datenschutz-RI entnommen. Bei Auslegung der Bestimmung gelangt man rasch wieder zu der rechtspolitisch unerwünschten Einschränkung, dass Daten - nur soweit verfügbar - zu beauskunften sind. **Vor diesem Hintergrund regen wir an, mit einer Protokollierungspflicht in § 26 klarzustellen, dass Herkunftsangaben zu dokumentieren sind**, es sei denn der Auftraggeber macht glaubhaft, weshalb dies im Einzelfall nicht möglich oder unzumutbar ist.

Eine solche Verpflichtung wäre sachlich gerechtfertigt, da sich Betroffene nur auf diese Weise gegen Unrechtmäßigkeiten an der Datenquelle wehren können. In vielen Fällen bedeutet ein Herkunftsnachweis auch, dass sich die Datenverwender (etwa ein Adresshändler oder eine Wirtschaftsauskunftei) überhaupt der Pflicht bewusst sind, ihren Datenbestand aktuell zu halten. Ohne Herkunftsdokumentation können weder zwischenzeitige Änderungen an der Datenquelle nachvollzogen werden, noch Löschungen von zugekauften Daten, bei denen sich nur allzu oft nachträglich herausstellt, dass sie auf unwirksamen Zustimmungserklärungen basieren, durchgeführt werden.

- **Löschverbot**

Nach § 26 Abs 7 darf "ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten". Entsprechend bisheriger DSK-Entscheidungen steht nach erfolgter Auskunft der gleichzeitig begehrten Datenlöschung die viermonatige Sperre entgegen. Diese Sperrwirkung entspricht nicht den Absichten eines an baldiger Löschung Interessierten. Es sollte deshalb klargestellt werden, dass vom befristeten Löschungsverbot abzusehen ist, wenn der Betroffene die Löschung ausdrücklich wünscht.

Maßnahmen bei Gefahr in Verzug § 30 Abs 6 iVm § 31 a Abs 2

Es wird begrüßt, dass die Befugnisse der Datenschutzbehörde erweitert werden. Sie kann künftig bei Gefahr in Verzug die Weiterführung einer Datenanwendung untersagen. Wenn die Voraussetzungen dafür vorliegen (eine besondere Beeinträchtigung von Geheimhaltungsinteressen), sollte die Behörde aber auch entsprechend tätig werden müssen. Es wird angeregt, an Stelle der „kann"-Bestimmung eine Verpflichtung vorzusehen.

Beschwerdeverfahren § 31

- **Anforderungen an Beschwerdevorbringen Abs 3**

Die inhaltlichen Anforderungen, die an eine Beschwerde gestellt werden, sind überaus anspruchsvoll und können rechtsunkundige Beschwerdeführer rasch an ihre Grenzen bringen. Insbesondere inhaltliche Elemente wie „die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt" und das „Begehren, die behauptete Rechtsverletzung festzustellen" stellen für durchschnittliche Antragssteller eine zu hohe formale Hürde dar. Im Sinn eines leichten Zugangs zum Recht sollte keinesfalls der Eindruck entstehen, man benötigt eine rechtskundige Vertretung um eine Datenschutzbeschwerde erfolgreich einzubringen.

- **Nachtrag bei Säumnis Abs 8**

Die Bestimmung sieht vor, dass die gesetzlich vorgesehenen Reaktionen auf Auskunfts-, Richtigstellungs- und Löschungsbegehren auch noch im laufenden Beschwerdeverfahren nachgeholt werden können. Vor allem bezüglich des Auskunftsrechtes wollen wir auf folgende unerwünschte Praxis hinweisen:

Auskünfte sind grundsätzlich innerhalb von 8 Wochen zu erteilen. Es besteht der Eindruck, dass Datennutzer auf Anfrage oftmals keine Auskunft erteilen, sondern erst einmal abwarten, ob der Betroffene nicht ohnedies den Aufwand scheut, eine Beschwerde bei der DSK einzubringen. Der säumige Datennutzer kann nach derzeitiger Judikatur die Auskunft noch im Beschwerdeverfahren mit der Konsequenz nachtragen, dass die Beschwerde diesfalls mangels Rechtsschutzinteresses abzuweisen ist. Wurde die verspätete Auskunft unvollständig erteilt, muss neuerlich ein Verfahren in Gang gesetzt werden. Für Betroffene ist es unvertretbar, derart lange und mit hohem Aufwand verbunden um eine Auskunft ringen zu müssen. Derzeit haben Auskunftsverzögerungen bis in ein allfälliges DSK-Verfahren hinein keinerlei nachteilige Folgen. Um ein taktisches Zuwarten unattraktiver zu machen, sollten Verwaltungsstrafen angedacht werden. Die Strafdrohung muss nicht hoch sein, sollte jedoch dem Eindruck entgegenwirken, dass auf ein Auskunftsersuchen in der Praxis erst reagiert werden muss, wenn ein Betroffener konsequent genug ist, eine förmliche Beschwerde einzubringen.

Videoüberwachung §§ 50a ff

Eingangs sei nochmals auf die BAK-Stellungnahme zum Erstentwurf aus 2008 verwiesen, insbesondere auf die Bedenken, dass es geringe Evidenz über die generelle Eignung von Videoüberwachung für die üblicherweise angestrebten Zwecke gibt. Im Zuge einer lokalen Videoüberwachung verlagert sich ein Sicherheitsproblem oft nur räumlich, mit der Konsequenz, dass damit eine gesellschaftspolitisch fragwürdige „Aufrüstungsspirale" von Überwachungsmaßnahmen in Gang gesetzt wird.

Besonders im Auge zu behalten ist, dass eine für einen Zweck gemeldete Überwachungsanlage die Gefahr birgt, dass das Bildmaterial faktisch und unerkannt auch für Sekundärzwecke verwendet wird. Diese Nutzungen können absolut unerlaubt sein (Mitarbeiterkontrolle) oder auch nur überschießend (Verhaltenskontrolle in Bagatellangelegenheiten). Beispielshaft für unsere Befürchtung verweisen wir auf eine uns vorliegende, aktuelle Mitteilung einer Hausverwaltung. Diese macht darauf aufmerksam, dass „Verunreinigungen des Objektes – dazu zählen auch auf den Postkasten abgelegte Postwurfsendungen – nun [mit erfolgter Installation einer Videokamera] auch den jeweiligen Parteien zuordenbar werden. Verstöße gegen die Hausordnung werden nicht toleriert und führen zur Einleitung weiterer Schritte."

Vor diesem Hintergrund...

...wird begrüßt, dass die **Kennzeichnungsvorschriften verschärft** und zur Klarstellung ein absolutes **Verbot der Videoüberwachung zur Mitarbeiterkontrolle** eingefügt wurde,

...ist es uns zum Schutz der von Aufzeichnungen betroffenen Personen (Passanten, Hausbewohner und -besucher, Mitarbeiter, Konsumenten uvm) vor unverhältnismäßigen Überwachungsmaßnahmen aber weiterhin **ein vordringliches Anliegen, dass**

- im Gesetzestext selbst auf das Gebot hingewiesen wird, zunächst **gelindere Mittel** einzusetzen (Sicherheitstüren, Echtzeitüberwachung, Alarmanlagen, Warensicherungen uvm) – und nicht nur in den Erläuterungen

- klargestellt wird, dass der Auftraggeber zunächst **ein Hausrecht** am überwachten Ort nachweisen muss und öffentlicher Grund (etwa Gehsteige; Ausnahme: schmaler Streifen zwecks Fassadenüberwachung) keinesfalls privat überwacht werden darf.

- im Gesetzestext selbst klargestellt wird, dass Videoüberwachung für behördliche Zwecke nur aufgrund ausdrücklicher gesetzlicher Ermächtigung im jeweiligen Materiengesetz gestattet ist

- **die Ausnahme vom Überwachungsverbot (Zustimmungserklärung) gestrichen wird. Die Ausnahme ist in Hinblick auf rechtliche Abhängigkeitsverhältnisse 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 entgegenstehen."*

- **der Abschnitt über die Videoüberwachung den besonderen Erfordernissen im Arbeitsverhältnis durch eigene Regelung besser Rechnung trägt.** Die Klarstellung, dass Mitarbeiterkontrolle kein zulässiger Überwachungszweck ist, wird begrüßt, schützt Arbeitnehmer naturgemäß aber nicht vor einer Betroffenheit bei Kameraeinsatz für andere Zwecke (etwa Sicherheit bei Bankenschaltern, Schutz hochpreisiger Waren). Ein **explizites Beweisverwertungsverbot** sollte zB die Weiterverwendung von Überwachungsmaterial für arbeitsrechtliche Konflikte unterbinden. Bezüglich weiterer Forderungen, etwa **Mindestanforderungen in schriftlichen Regelungen zwischen dem Arbeitgeber und dem Betriebsrat** verweisen wir auf die Details unserer Stellungnahme zum Erstentwurf (S 22-24).

- nur **befristete Genehmigungen** erteilt werden (Prüfung des Wegfalls/Fortbestands des Überwachungsinteresses). Eine entsprechende Ergänzung wäre aufzunehmen. Im Hinblick auf das Verhältnismäßigkeitsgebot ist es nicht nachvollziehbar, dass die Erläuterungen davon ausgehen, dass "ein gefährlicher Angriff, der sich innerhalb der vergangenen zehn Jahre ereignet hat", der berechtigte Anlass sein kann für eine unbefristete Überwachungsmaßnahme. Sowohl der Rückgriff auf in der Vergangenheit liegende Vorfälle, als auch die Befristung der Genehmigung der Überwachung müssen **zeitlich so gewählt** sein, dass das Bestehen einer **aktuellen Gefahr noch glaubwürdig** ist.

- Klargestellt wird, dass Videoanlagen **zur Abwehr und Aufklärung von gerichtlichen Vorsatzdelikten** eingesetzt werden dürfen, **nicht aber lediglich zur (primären) Durchsetzung zivil- oder verwaltungsrechtlicher Ansprüche:**

  Den Erläuterungen zufolge muss es sich um "eine Bedrohung mit gerichtlich strafbaren Vorsatztaten handeln", damit ein überwiegendes berechtigtes Interesse des Auftraggebers anzunehmen ist. Allerdings - so die Erläuterungen weiter - ginge der Begriff des „gefährlichen Angriffs" über den im Sicherheitspolizeigesetz definierten Begriff des „gefährlichen Angriffs" hinaus: unter Z 1 können auch konkrete Gefährdungen von Geschäfts- und Betriebsgeheimnissen sowie allenfalls auch die konkrete Gefahr einer groben Verwaltungsübertretung fallen.

  Die BAK spricht sich **entschieden gegen eine derart unbestimmte Formulierung** aus, die in der Praxis nur allzu leicht zu einem unverhältnismäßigen Gebrauch führen kann. Im Gegensatz zu den Ausführungen in den Erläuterungen halten wir **eine enge Auslegung des Begriffes im Sinn des SPG für unbedingt erforderlich. Diese restriktive Auslegung muss sowohl für den originären Überwachungszweck als auch eventuelle spätere Datenweitergaben aus anderem Anlass nach § 50 a Abs 6 gelten.**

- ein **Beweisverwertungsverbot für rechtswidrig erstellte Aufzeichnungen** verankert wird: Die wachsende Kameradichte kann dazu führen, dass über das eigentliche Installationsmotiv hinaus Datenmaterial auch als Beweismittel für Streitfälle benutzt wird, die überhaupt keinen zulässigen Überwachungsgrund darstellen. Um zu verhindern, dass gesetz- oder auflagenwidriges Bildmaterial dennoch erfolgreich eingesetzt wird, wird ein ausdrückliches Beweisverwertungsverbot unter allen Umständen benötigt.

- **abgebildete Personen besser vor missbräuchlicher Datennutzung geschützt werden:**

  Videoanlagen, die für einen bestimmten Überwachungszweck gemeldet wurden, zeichnen in der Regel über lange Zeit unendlich viele Bilder von Personen (Passanten, Mitarbeiter, Konsumenten uvm) auf, die für den Zweck der Datenanwendung nach § 6 Abs.1 Z 3 genaugenommen nicht wesentlich sind. Dieses „überschüssige" Datenmaterial sollte eigentlich nach § 6 Abs 1 Z 5 gar nicht vorhanden sein, ist aber jedenfalls unverzüglich zu löschen.

  Den Auflagen bei der Genehmigung der Anlagen (Datensicherheit, Zugriffs- und Auswertungsbedingungen, Löschung uvm) kommt daher mit Blick auf den Schutz aller Passanten im Aufzeichnungsbereich einer Kamera ganz besondere Bedeutung zu. Einige der zweckmäßigen Auflagen sind mit Zusatzkosten verbunden. Damit wird dem Auftraggeber letztlich auch vor Augen geführt, dass Überwachung mit **kostenrelevanten Sorgfaltspflichten** gegenüber den Betroffenen verbunden ist. Bei der Gegenüberstellung verschiedener Überwachungsmöglichkeiten wäre es rechtspolitisch auch absolut unerwünscht, wenn Auftraggeber davon ausgehen könnten, dass Videoüberwachung (abgesehen vom geringen Anschaffungspreis für die billigste Ausführung) keine nennenswerten Kosten verursacht. Wird die Verhältnismäßigkeitsprüfung wirklich ernst genommen, müssen Auftraggeber einigen Zusatzaufwand für **flankierende Maßnahmen zum Schutz der Betroffenen einkalkulieren** (und würden aus eigenem Videoüberwachung auf wirklich wohlüberlegte und notwendige Einsatzgebiete beschränken).

  - **Verschlüsselungspflicht:** Im Handel sind Kamerasysteme erhältlich, die die anfallenden Daten unmittelbar **verschlüsseln.** Bei Vorfällen, nach denen Aufzeichnungen ausgewertet werden müssen, sollte nur ein schlüsselverwahrender Treuhänder (zB Notar) die Entschlüsselung vornehmen dürfen. Derzeit fehlt die wichtige Schutznorm, dass Aufzeichnungen nur im begründeten Verdachtsfall ausgewertet werden dürfen. Allerdings wäre ein Verstoß ohnedies kaum nachzuweisen. Eine Verschlüsselungspflicht wäre eine geeignete Abhilfe.

  - **Gutachtenspflicht:** Analog zur behördlichen Abnahme eines fertig gestellten Bauvorhabens durch ein vom Bauherren vorgelegtes ziviltechnisches Gutachten sollten **Videoüberwacher der Registrierungsbehörde ein Gutachten vorlegen, dass System, Installationsort, Kennzeichnung, Aufzeichnungs- und Löschroutinen etc. gesetzes- und auflagenkonform sind**. Angesichts der Fülle an Registrierungsfällen ist andernfalls eine Prüfung der Einhaltung der aufgetragenen Bedingungen völlig illusorisch. Die „Aufsichts"-Kosten sollten wie in vielen anderen Bereichen vom Verursacher in einem bestimmten Umfang mitgetragen werden.

- **Strikte Löschungspflicht:** In Hinblick darauf, dass viele Personen mit abgebildet werden, für die überhaupt kein Speichergrund besteht, muss die **Speicherdauer extrem kurz** gehalten werden, um noch als verhältnismäßig zu gelten. 48 Stunden dürfen (im Regelfall) nicht überschritten werden. Die **weitreichenden Verlängerungsmöglichkeiten**, die die Erläuterungen vorsehen, sind bei Abwägung der wechselseitigen Interessen sachlich nicht gerechtfertigt und sind **zu streichen**. Demnach könnte die DSK eine längere Aufbewahrung vorsehen, um auf "die allgemeine Verkehrssitte, wie etwa die Öffnungszeiten von Geschäften, Urlaube dgl. Rücksicht zu nehmen". Da für bloße Passanten usw. eigentlich überhaupt kein berechtigter Speichergrund besteht, sind Urlaube, Fenstertage etc keine überzeugende Begründung für doppelt so lange Speicherzeiten. Dem Videoüberwacher darf zugemutet werden, sich so zu organisieren, dass er die Überwachung für die unfreiwillig Betroffenen schonend umsetzt. Medienberichte offenbaren in Einzelfällen große Nachlässigkeiten durch völlig überzogene Speicherdauern, weshalb auch eine Sanktionsbestimmung zweckmäßig wäre.

- **Sinn und Tragweite der § 50 c Abs 2 und § 50 d Abs 2 Z 4 (Videoüberwachung im Zusammenhang mit privaten Tätigkeiten) nochmals überdacht wird.** Die Bestimmungen verweisen bloß darauf, dass u.a. Datenanwendungen, die „für persönliche oder familiäre Tätigkeiten vorgenommen werden", soweit es sich dabei um Videoüberwachung handelt, weder melde- noch kennzeichnungspflichtig sind. Zweifelhaft bleibt, ob unter „Datenanwendungen für persönliche oder familiäre Tätigkeiten" (bei reiner Wortinterpretation und in Anbetracht der Beschreibung „privater Zwecke" in § 45 Abs 1 und der Zustimmungserfordernisse in Abs 2) überhaupt je auch Videoüberwachungen subsumierbar sind.

  Wollte man **Videoüberwachungen innerhalb der „eigenen vier Wände" durch Befreiung von Melde- und Kennzeichnungspflicht** aber unbedingt **privilegieren**, müsste dies durch eine eigene, **unzweideutige Bestimmung** erfolgen. Gegen ein solches Vorhaben spricht aber unseres Erachtens auch Grundsätzliches. § 50a Abs. 5 **verbietet Überwachungen an Orten, die dem höchstpersönlichen Lebensbereich** zuzurechnen sind. **Dazu zählen explizit Privatwohnungen**. Bei einer Ausnahme von der Meldepflicht für Videoüberwachungen im Eigenheim ist deshalb zu bedenken, inwieweit damit nicht ein Widerspruch zum absoluten Verbot des § 50a Abs 5 entsteht.

Strafbestimmung bei vorsätzlicher Gewinn- oder Schädigungsabsicht § 51

Es wird begrüßt, dass der Straftatbestand nunmehr zu einem Offizialdelikt wird.

Verwaltungsstrafbestimmungen § 52

Es wird begrüßt, dass die Strafhöhe zumindest geringfügig angehoben wird und bei Missachtung von Melde- und Kennzeichnungspflichten für private Videoüberwachung Sanktionen vorgesehen sind. Um Datenschutzansprüchen mehr Nachdruck zu verleihen, sollten für folgende Situationen ebenfalls Sanktionsmöglichkeiten vorgesehen werden:

- Nach § 52 Abs 1 Z 3 können Verstöße gegen Auskunfts-, Richtigstellungs- und Löschungsrechte erst geahndet werden, wenn Daten entgegen einer rechtskräftigen Entscheidung (Urteil, Bescheid) „verwendet, nicht beauskunftet, nicht richtiggestellt oder nicht gelöscht" werden. Es sollte unbedingt sichergestellt werden, dass auch schon der ursprüngliche Verstoß sanktioniert werden kann.
- Entzieht sich ein Auftraggeber einer Vorabkontrolle dadurch, dass er im automatischen Registrierverfahren seine Anwendung nicht als vorabkontrollpflichtig nach § 18 Abs 2 deklariert, sollte ebenfalls eine Verwaltungsstrafe verhängt werden können.
- Im Falle der Videoüberwachung sollten auch Verstöße gegen die Protokollierungs- und spezielle Löschpflicht nach § 50 b und
- Verstöße gegen Registrierungsauflagen der Datenschutzbehörde strafbar sein.

Themen, die überhaupt keine Berücksichtigung finden:

Einführung eines betrieblichen Datenschutzbeauftragten

Aus BAK-Sicht wird überaus bedauert, dass die in § 15a des Erstentwurfes vorgesehene Einführung eines betrieblichen Datenschutzbeauftragten aufgrund von Widerständen der Wirtschaftsseite ersatzlos gestrichen wurde. Angesichts der rasanten technischen Entwicklung (zB allein bei Standardsoftware) werden zunehmend höhere Anforderungen an ArbeitgeberInnen und MitarbeiterInnen gestellt. Es besteht weiterhin dringender Bedarf, einen betrieblichen Datenschutzbeauftragten vorzusehen, der die Einhaltung des innerbetrieblichen Datenschutzes sicherstellt.

Vor diesem Hintergrund wäre zumindest ein Kompromiss anzustreben, etwa dadurch, dass betriebliche Datenschutzbeauftragte in einem ersten Schritt in Großunternehmen, aber auch dem öffentlichen Bereich vorgesehen werden.

Rechtsschutz verbessern

Der **Zugang zur Rechtsdurchsetzung** der Betroffenen gegenüber **privaten Auftraggebern** ist unbedingt zu erleichtern. Die erstinstanzliche zivilgerichtliche Zuständigkeit mit Anwaltszwang stellt für viele Betroffene ein zu hohes Kostenrisiko und damit eine unüberwindbare 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 ganz selten Ansprüche eingeklagt. Vor diesem Hintergrund wäre es wichtig,

- das **Ombudsmannverfahren der Datenschutzkommission zeitgemäß und bedarfsgerecht auszubauen**
- eine **Verbandsklagsbefugnis** für Verbraucher- und Datenschutzorganisationen zu verankern, um datenschutzrechtliche Verstöße effektiver zugunsten der Verbraucher verfolgen zu können
- den zivilgerichtlichen Rechtsschutz dadurch zu erleichtern, dass für Datenschutzbelange in Zusammenhang mit Arbeitsverhältnissen **Arbeits- und Sozialgerichte** zuständig sind und
- Alternativen zum kostenintensiven Zivilprozess bei sonstigen Datenschutzverletzungen von privaten Rechtsträgern anzudenken (**außerstreitiges Verfahren, DSK-Reform** uä)

RFID

Die EU-Kommission verweist in ihrer Empfehlung vom 12.05.2009 (C(2009) 3200 final) über die Berücksichtigung von Privatsphäre und Datenschutz bei RFID-Anwendungen darauf, dass RFID-Technik die Verarbeitung personenbezogener Daten über kurze Distanzen ohne physischen Kontakt oder sichtbare Interaktion zwischen Chip und Lesegerät ermöglicht. Vor diesem Hintergrund besteht das Risiko, dass kommerzielle RFID-Anwendungen zum Einsatz kommen, bei denen Personen ohne ihr Wissen und ohne ihre Zustimmung zu Betroffenen im datenschutzrechtlichen Sinn werden. Personen, die Gegenstände mit RFID-Chips bei sich tragen, können über die eindeutige RFID-Kennzahl selbst zuorden- und identifizierbar werden.

Die überaus konkreten Auflagen der EU-Kommission gerichtet an Auftraggeber von RFID-unterstützten Datenanwendungen sollten jedenfalls ins DSG übernommen werden.

Die EU-Kommission empfiehlt,

- vor dem Inverkehrbringen einer RFID-Anwendung eine Privacy-Folgenabschätzung
- führt Informationspflichten an, die über die allgemeinen Anforderungen des DSG weit hinausgehen (neben Angaben über den Betreiber, Zweck und die betroffenen Datenarten, Hinweise auf Chips, die auf Produkten angebracht oder eingebaut sind, die denkmöglichen Privacy-Risken und Abhilfen für Betroffene). Die Mitgliedstaaten werden zudem aufgefordert, darauf hinzuwirken, dass ein einheitliches EU-Logo auf den Einsatz eines Lesegerätes hinweist.
- den Handel dazu zu verpflichten, die Chips vor der Übergabe an den Konsumenten unverzüglich und kostenlos zu entfernen oder zu deaktivieren, es sei denn der Verbraucher entscheidet sich nach Aufklärung über die Konsequenzen für die weitere Aktivierung. Konsumenten müssen außerdem in die Lage versetzt werden, zu prüfen, ob die Deaktivierung bzw vollständige Entfernung gelungen ist. Die vertragsrechtlichen Verpflichtungen des Händlers müssen davon unberührt bleiben.

Grenzen für Scoring Methoden § 49

Scoring-Methoden versuchen mit Hilfe von Fakten über eine Person, allgemeinen Erfahrungen und statistischen Werten möglichst zuverlässig das Verhalten eines Kunden vorherzusagen. ZB versucht man damit, die mathematisch-statistische Wahrscheinlichkeit zu berechnen, mit der ein Kunde seine Zahlungspflichten erfüllen bzw. verletzen wird. Da konkrete Ausübungsregeln fehlen, besteht die Gefahr, dass nicht selten unsachliche Merkmale, falsche oder veraltete Daten verarbeitet und „harte" mit „weichen" Fakten vermischt werden. Da viele Unternehmen (auch außerhalb der Branche Wirtschaftsauskunfteien) an Scoringprogrammen interessiert sind, sollten ins DSG Grundsätze für deren Einsatz aufgenommen werden Bspw.:

- Der Anwendungsbereich für Scoring-Verfahren, die über einen Vertragsabschluss und die Vertragskonditionen entscheiden, muss auf Rechtsgeschäfte mit nennenswerten Ausfallsrisken beschränkt werden. Allgemeine Vertragsrisken reichen nicht.
- Über den „logischen Ablauf der automatisierten Entscheidungsfindung" (§ 49 Abs 3) hinaus ist dem Betroffenen auf Nachfrage offenzulegen, aufgrund welcher Prognose- und Bewertungsmethoden, personenbezogenen und statistischen Datenarten, Gewichtungen etc das Ergebnis zustande gekommen ist.
- Angesichts der massiven persönlichen Nachteile durch „pseudowissenschaftliche" Scorings sollten auch nur wissenschaftlich anerkannte Methoden angewendet werden dürfen. So sollten etwa diskriminierende Verallgemeinerungen (gute/schlechte Wohnlagen, pauschale Alters- oder Geschlechtszuschreibungen u.v.m) in die Bewertung nicht einfließen dürfen.

Handy- und GPS-Ortung

Dienste, die GPS- oder Handy-Ortungen ermöglichen, also "Location Based Services" boomen. Nicht nur Gegenstände mit GPS-Signal können im Fall des Diebstahls geortet werden. Personen können aus unterschiedlichsten Gründen bemüht sein, herauszufinden, wo sich eine andere Person im Augenblick aufhält. Auch Mobilfunkbetreiber bieten zunehmend Mehrwertdienste auf Ortungen basierend an (Soziale Gruppenbildung; Angebote für standortbezogene Kurzeitversicherungen etc.). Soweit das Risiko besteht, dass der aktuelle Standort von Personen auch ohne deren Wissen und Zustimmung lokalisiert werden kann, ist Missbrauchsschutz erforderlich. Wünschenswert wäre ein ausnahmsloses Verbot privater Ortung ohne vorherige, ausdrückliche Zustimmung des Betroffenen.

Geodaten

Stadtansichten werden mit hohem Detaillierungsgrad (Gebäude und Grundstücke) durch unterschiedlichste Dienste digital erfasst und im Internet zugänglich gemacht. Dabei ist oft die Gebäudeadresse bestimmbar und in der Folge auch der Gebäudeeigentümer und Bewohner (via Telefonbuch, Grundbuch, Melderegister). Vor diesem Hintergrund wird angeregt, klarzustellen, dass etwa

- Dienste, die systematisch georeferenzierte Bilder liefern, schutzwürdige Interessen der Betroffenen nicht beeinträchtigen und
- Gesichter oder Fahrzeugkennzeichen nicht erkennbar sein dürfen,
- sowie potentiell Betroffene schon im Vorfeld von Aufzeichnungen Gelegenheit haben müssen, Widerspruchsrechte nach § 28 Abs 2 auszuüben.

Herbert Tumpel
Präsident

BUNDESARBEITSKAMMER

Werner Muhm
Direktor