Bundeskanzleramt – Verfassungsdienst
Ballhausplatz 2
1014 Wien
per Mail an v@bka.gv.at
begutachtungsverfahren@parlament.gv.at

Zu GZ BKA 810.026/0005-V/3/2009 Wien, am 17.06.2009

Stellungnahme des *Ludwig Boltzmann Instituts für Menschenrechte (BIM)* zum Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010)

Sehr geehrte Damen und Herren!

Das Ludwig Boltzmann Institut für Menschenrechte (BIM) nimmt mit Bezug auf das Schreiben vom 20.5.2009 zu GZ BKA 810.026/0005-V/3/2009 zum ausgesendeten Entwurf einer DSG-Novelle 2010 wie folgt Stellung:

1. Allgemeines:

Die technische Entwicklung und die damit einhergehenden neuen Kontroll-, Datenerfassungs- und Weiterverarbeitungsmöglichkeiten stellen den Gesetzgeber vor immer neue Herausforderungen.

Zu Recht wird vom Gesetzgeber erwartet, sich der technischen Entwicklung nicht zu verschließen. Gleichzeitig sind aber die (Grund-) Rechte wie das Recht auf Achtung der Privatsphäre und hieraus erfließend insbesondere das Grundrecht auf Datenschutz der Betroffenen bestmöglich zu wahren. Eine weitere Herausforderung liegt in der Notwendigkeit, ein für die zur Vollziehung berufenen Behörden möglichst effizientes Gesetz zu schaffen, welches auf der einen Seite der Wirtschaft keine unnötigen Belastungen auferlegt und auf der anderen Seite gleichzeitig eine effiziente Kontrolle der Datenverwender und bestmöglichen (und natürlich ebenso effizienten) Rechtsschutz für die Betroffenen sicherstellt.

Schließlich stellt sich angesichts der rasant voranschreitenden technischen Entwicklung die Frage, welches Ausmaß an Abstraktion im Hinblick auf Eingriffsmöglichkeiten in das Grundrecht auf Datenschutz wünschenswert bzw. erforderlich ist, ohne

dass die jeweilige Bestimmung aufgrund ihrer Unbestimmtheit in ein Spannungsverhältnis zum Legalitätsprinzip des Art. 18 B-VG gerät.

In diesem Sinne wird insbesondere die mit dem Entwurf verfolgte Absicht begrüßt, Bestimmungen des DSG 2000 – wie es in den erläuternden Bemerkungen hinsichtlich des Grundrechtes auf Datenschutz heißt – in eine *„sprachlich verbesserte Form“* zu bringen, wie auch das (teils damit in Zusammenhang stehende) Bemühen um Klarstellung *„in der Vollzugspraxis aufgetretener Rechtsfragen“.*

Bedauert wird, dass der im Vorschlag einer DSG-Novelle 2008 noch vorgesehene betriebliche Datenschutzbeauftragte nicht Eingang in den gegenständlichen Entwurf gefunden hat, zumal eine Sensibilisierung für datenschutzrechtliche Fragen auf betrieblicher Ebene und eine Verbesserung der Situation der von Kontrollmaßnahmen durch den Arbeitgeber betroffenen Arbeitnehmer dringend erforderlich gewesen wäre. Wie nicht zuletzt mehrere aktuelle Beispiele, z.B. in der Lebensmittelbranche und in einem großen Telekommunikationskonzern in Deutschland, gezeigt haben, ist die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften im Betrieb zum Schutz der Arbeitnehmer mehr denn je ein Gebot der Stunde. Den einzelnen Arbeitnehmern ist es aufgrund ihres typischerweise mangelnden Fachwissens sowie des regelmäßig vorliegenden Abhängigkeitsverhältnisses gegenüber dem Arbeitgeber oftmals nur schwer möglich, gegen in ihre Privatsphäre eingreifende Kontrollmaßnahmen vorzugehen, ohne dabei – aufgrund des faktisch bestehenden Ungleichgewichts – ihr Dienstverhältnis zu gefährden.
Gerade in diesen Fällen ist ein betrieblicher Datenschutzbeauftragter erforderlich, um Fachwissen im Bereich des Datenschutzes zur Verfügung zu stellen, das Bewusstsein für die Bedeutung von Datenschutz auf Arbeitgeber- und Arbeitnehmerseite zu stärken und an der Entwicklung von Lösungen mitzuwirken, die sowohl die Interessen der Mitarbeiter an der Wahrung ihrer Privatsphäre, als auch des Arbeitgebers an einem möglichst effektiven Einsatz der Arbeitskräfte hinreichend berücksichtigen. Zudem wäre der Datenschutzbeauftragte ähnlich den Mitgliedern des Betriebsrates unter besonderen Schutz zu stellen, um eine allfällige Benachteiligung aufgrund dieser Tätigkeit zu verhindern.

Bedauert wird zudem, dass die Novellierung des Datenschutzgesetzes nicht zum Anlass genommen werden soll, das in Ansehung der dem DSG zu Grunde liegenden Differenzierung zwischen direkt und indirekt personenbezogenen Daten bestehende Spannungsverhältnis zur Datenschutzrichtlinie 95/46/EG aufzulösen.

Zwar unterliegen sowohl direkt wie auch indirekt personenbezogene Daten dem Regime des Datenschutzgesetzes, doch zeigt sich bei näherer Betrachtung, dass der Schutz indirekt personenbezogener Daten nur ein scheinbarer ist. So sind schon nach der geltenden Rechtslage Datenanwendungen, die nur indirekt personenbezogene Daten enthalten, nicht meldepflichtig (§ 17 Abs 2 Z 3), auch besteht kein Geheimhaltungsanspruch. In den EBRV zum DSG 2000 wird zu § 17 ausgeführt: *„Bei der Verwendung nur indirekt personenbezogener Daten besteht nach § 1 Abs. 1 […] kein Geheimhaltungsanspruch, weshalb eine Meldepflicht sachlich gerechtfertigterweise entfallen kann.“* Für den Betroffenen wichtige Schutzinstrumente wie das Widerspruchsrecht, das Auskunftsrecht und das Recht auf Richtigstellung oder Löschung finden bei „nur“ indirekt personenbezogenen Daten keine Anwendung. Auch entfällt die grundsätzlich gegenüber dem Betroffenen bestehende Informationspflicht des Auftraggebers (siehe die EBRV zu § 24 Abs 6). Hieran soll sich auch nach dem vorliegenden Entwurf nichts ändern. Dass das Datenschutzgesetz indirekt personen-

bezogene Daten nicht sogleich expressis verbis vom Regelungsbereich des DSG ausschließt, erklärt sich wohl durch die Vorgaben der DatenschutzRL 95/46/EG, welche grundsätzlich auch indirekt personenbezogene Daten als schützenswert erachtet.

So heißt es im Erwägungsgrund 26 der besagten Richtlinie: *„Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder vom dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen [...]".* Aus Erwägungsgrund 26 in Zusammenschau mit der Definition der „personenbezogenen Daten" in Art. 2 lit. a) geht hervor, dass das entscheidende Kriterium für die Geltung der Schutzprinzipien die Bestimmbarkeit des Betroffenen ist. Ob dieser Personenbezug durch den Auftraggeber selbst oder „nur" durch einen Dritten hergestellt werden kann, ist für die Frage des Schutzumfanges nach der Richtlinie grundsätzlich irrelevant. In beiden Fällen finden die Schutzprinzipien der Richtlinie volle Anwendung.

Verabsäumt wurde im vorliegenden Entwurf zudem eine (dringend erforderliche) Verbesserung der Situation der Datenschutzkommission. Hier wird nachdrücklich angeregt, die finanziellen und personellen Ressourcen der DSK angemessen zu erweitern, damit sie die ihr zugewiesenen Aufgaben als Datenschutzbehörde zufriedenstellend erfüllen kann.

Insbesondere aufgrund der neuen Bestimmungen zur Videoüberwachung ist erheblicher zusätzlicher Aufwand zu erwarten, da Videoüberwachungsanlagen bisher in der Praxis – contra legem und entgegen der eindeutigen Rechtsprechung der DSK – mangels Meldung zum größten Teil nicht im Datenverarbeitungsregister erfasst wurden. Darüber hinaus bestehen heute schon massive Engpässe: Aus dem Datenschutzbericht 2007 geht hervor, dass die österreichische Datenschutzkommission hinsichtlich der personellen Ausstattung im europäischen Vergleich einen der hintersten Plätze belegt;[1] dies wirkt sich insbesondere bei jenen Befugnissen und Aufgaben aus, bei denen die DSK von Amts wegen tätig werden und Kontrollen durchführen sollte (§ 30 Abs 2 und 3), was aufgrund der aktuellen Personalsituation nicht bzw. kaum stattfindet. Diese Funktionen sind jedoch von enormer Bedeutung, da eine effiziente, wirkungsvolle Datenschutzbehörde gerade nicht nur im Anlassfall tätig werden, sondern auch ein gewisses Maß an begleitender Kontrolle erbringen sollte.

Zudem wäre eine Herauslösung der Datenschutzkommission aus der Organisationsstruktur des BKA notwendig, um die Voraussetzungen für eine unabhängige Datenschutzbehörde tatsächlich zu erfüllen. Zu kritisieren ist insbesondere die derzeit nicht vorhandene Budgethoheit der DSK, die zu einer massiven Abhängigkeit vom Wohlwollen des BKA führt. Hier bestehen massive Defizite bei der Umsetzung der DatenschutzRL, wie auch der Umstand zeigt, dass derzeit zu dieserr Frage ein Vertragsverletzungsverfahren gegen Österreich anhängig ist (03/5109, siehe 4880/AB, XXIII. GP).

Sehr positiv bemerkt wird, dass juristische Personen nach dem vorliegenden Entwurf – im Gegensatz zum Entwurf 2008 – nun weiterhin den Schutz des DSG 2000 genießen werden. Dies ist insofern relevant, als die bestehenden gewerblichen Rechts-

[1] Datenschutzkommission, Datenschutzbericht 2005-2007, S. 13.

schutzbestimmungen zu kurz greifen und keinen qualitativ und quantitativ dem DSG entsprechenden Datenschutz sicherstellen: Der gewerbliche Rechtsschutz greift nämlich nur gegenüber solchen (juristischen) Personen, die mit der betroffenen juristischen Person in einem Wettbewerbsverhältnis stehen (vgl. zB § 1 UWG: *„Wer im geschäftlichen Verkehr …“*). Auch das Regime des Urheberrechts bietet nur sehr beschränkten Schutz und ist auf viele Daten, wie etwa solche über die Gebarung oder die Personalpolitik eines Unternehmens, nicht anwendbar. Auch das Schadenersatzrecht vermag die Anwendbarkeit des DSG nicht adäquat zu substituieren, zumal z.B. § 1330 ABGB nur vor der Verbreitung unwahrer Tatsachen schützt, wohingegen Daten iSd DSG 2000 im Regelfall wahre Tatsachen beinhalten. Wenn also beispielsweise eine (in keinem Wettbewerbs-, Arbeits- oder sonstigen Vertragsverhältnis stehende) Person Geschäftsgeheimnisse einer juristischen Person auf einer privaten Website veröffentlicht, stellt sich die Frage, woraus sich mangels Anwendbarkeit des DSG 2000 die Rechtswidrigkeit eines solchen Verhaltens und damit verbundene Schadenersatz- und Unterlassungsansprüche ergeben sollten. Dasselbe Rechtsschutzdefizit entstünde auch gegenüber Behörden, insbesondere würde jeder Anspruch auf Information, Richtigstellung und Löschung abhanden kommen.
Zudem handelt es sich bei juristischen Personen vielfach um Personengemeinschaften wie z.B. gemeinnützige Vereine nach dem Vereinsgesetz 2002, für die gewerbliche Rechtsschutzinstrumente regelmäßig nicht in Frage kommen und deren Daten überdies ein gesteigertes Maß an Schutzwürdigkeit auch im Hinblick auf andere Grundrechte (z.B. Religionsfreiheit nach Art 9 EMRK) aufweisen.

Wünschenswert wäre zudem im Rahmen der DSG-Novelle 2010 eine Sanierung der Bestimmungen zu den Ausnahmen von der Informationspflicht, insbesondere des § 24 Abs 3 Z 1: Diese Bestimmung erlaubt einen Entfall der Information anlässlich der Ermittlung von Daten, wenn diese „*durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt*“ werden und *„die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist“.*
Wenn also ein Auftraggeber Daten für einen bestimmten Zweck ermittelt hat – egal ob er den Betroffenen darüber informiert hat oder nicht – und entweder der selbe Auftraggeber oder auch ein anderer Auftraggeber diese Daten später für einen anderen Zweck (ein völlig anderes Aufgabengebiet) verwendet, entfällt die Informationspflicht pauschal und automatisch dann, wenn diese geänderte Datenverwendung gesetzlich vorgesehen ist. Die Ausnahme knüpft dabei nicht etwa daran an, dass der Betroffene schon bei der ursprünglichen Datenerhebung darüber in Kenntnis war oder eine Information unterbleiben dürfte, wenn die Datenerhebung für den „neuen“ Zweck erstmals erfolgen würde.[2] Anders als die pauschale Ausnahme für jede gesetzlich vorgesehene Datenverwendung wären solche Ausnahmen zumindest sachlich nachvollziehbar.
Ein Fall pauschalen Ausschlusses der Informationspflicht liegt beispielsweise bei sämtlichen Auskunftsverlangen der Sicherheitsbehörden nach § 53 Abs 3a und 3b SPG vor. Die Polizei ermittelt hier Daten aus Anwendungen anderer Auftraggeber, nämlich der Kommunikationsdiensteanbieter, und die Verwendung dieser so ermittelten Stamm-, Verkehrs oder Standortdaten ist durch § 53 Abs 3a und 3b SPG gesetzlich vorgesehen. Da in der Praxis eine Information der Betroffenen über einen Grundrechtseingriff durch ein derartiges Auskunftsverlangen aufgrund dieser Ausnahme-

[2] Siehe dazu instruktiv die Entscheidung des deutschen Bundesverfassungsgerichts zur Rasterfahndung, BVerfG, 1 BvR 518/02: Durch eine Zweckänderung können sogar für sich gesehen belanglose Daten einen neuen Stellenwert bekommen, insbesondere bei neuen Verknüpfungen.

bestimmung unterbleibt (siehe dazu auch Rechtsansicht des BM.I in der parl. Anfragebeantwortung 4148/AB XXIII. GP zu 4130/J XXIII. GP), entsteht für die Betroffenen ein massives Rechtsschutzdefizit, weil sie mangels Kenntnis des Eingriffs keine Schritte zur Wahrnehmung ihrer Rechte setzen können.
Die Information der Betroffenen ist aber eine wesentliche Voraussetzung für die Wahrung ihrer Grundrechte nach § 1 DSG und Art. 8 EMRK; § 24 Abs 3 Z 1 schränkt die Informationspflicht der Auftraggeber hier jedoch ohne Notwendigkeit stark ein und reduziert damit den Rechtsschutz für die Betroffenen – gerade im Zusammenspiel mit den genannten Eingriffsbefugnissen – massiv.

Nun mag es zweifellos viele Fälle geben, in denen eine Ausnahme von der Informationspflicht bei Zweckänderung der Datenverwendung zweifellos sinnvoll ist. Die Information aber pauschal auszuschließen, allein weil der nunmehr geänderte Zweck gesetzlich oder durch Verordnung vorgesehen ist, vermag diese Fälle nicht in sachlicher Weise zu erfassen.

Aus diesem Grund wird angeregt, § 24 Abs 3 Z 1 dahingehend abzuändern, dass eine Ausnahme von der Informationspflicht für gesetzlich oder durch Verordnung vorgesehene Datenanwendungen nur dann besteht, wenn diese Ausnahmen für eben diese Datenanwendungen zuvor von der Datenschutzkommission in einem eigenen Verfahren genehmigt wurden. Der Auftraggeber der Datenanwendung hätte ein solches Verfahren vorab anzustrengen.

2. Zu Art. 1 (Änderung des Bundesverfassungsgesetzes):

Die kompetenzrechtliche Integration des Datenschutzes in Art. 10 B-VG und die damit verbundene Vereinheitlichung des Datenschutzrechtes in Österreich wird als positive Entwicklung erachtet und begrüßt.

3. Zu Art. 2 Z 11 und 12 (§ 1):

Dem Entwurf zu diesem Punkt ist insofern zuzustimmen, als die vereinfachte Formulierung jedenfalls keine einschränkende Änderung des Grundrechts auf Datenschutz bewirkt und daher im Hinblick auf eine bessere Verständlichkeit begrüßenswert ist.
Allerdings ist kein Grund ersichtlich, warum der Halbsatz „insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens“ in § 1 Abs 1 entfallen soll, da durch diesen Bezug auf Art. 8 EMRK der Kernbereich des Grundrechts auf Datenschutz abgesichert wird. Abgesehen von dieser verfassungsrechtlich verankerten materiellen Determinante ist der Schutzbereich dieses Grundrechts ausschließlich auf einfachgesetzlicher Ebene ausgestaltet (Datenbegriff und weitere Begriffsbestimmungen des § 4), und kann dementsprechend relativ einfach eingeschränkt werden (z.B. durch Einschränkung des Begriffs des Betroffenen auf natürliche Personen).
Zumal der Verweis auf den Schutzbereich des Art. 8 EMRK die Verständlichkeit des § 1 Abs. 1 nicht beeinträchtigt und gleichzeitig auf verfassungsrechtlicher Ebene den Kernbereich des Grundrechts auf Datenschutz absichert, sollte dieser Teil der Bestimmung erhalten bleiben.

Aus diesem Grund wird angeregt, von einem Entfall der Verweises auf den Schutzbereich des Art. 8 EMRK in § 1 Abs. 1 Abstand zu nehmen.

4. Zu Art. 2 Z 19 (§ 4 Abs 1 Z 4):

An dieser Stelle soll ein Problem angesprochen werden, welches bereits in der derzeitigen Rechtslage besteht und dessen Klärung hier anlässlich der Novellierung angeregt wird. Dieses besteht darin, dass sich im öffentlichen Bereich häufig schwer feststellen lässt, ob nun das „Organ einer Gebietskörperschaft" selbst oder lediglich eine Organisationseinheit („Geschäftsapparate") als „Auftraggeber" iSd DSG 2000 zu qualifizieren ist. Beispiel: Ein Polizeibeamter speichert die Daten einer Person, die verdächtig ist, eine Verwaltungsübertretung nach einem Landesgesetz begangen zu haben. Wer ist Auftraggeber: Polizeiinspektion, BH, BPD oder BM.I? Nach welchen Kriterien ist diese Frage zu beurteilen (sachlich in Betracht kommende Oberbehörde; Stellung innerhalb der Behördenorganisation;…)? Die Formulierung „*Die Stellung als Auftraggeber kann sich aus Gesetzen, Verordnungen oder Verhaltensregeln […] ergeben"* im § 4 Abs 1 Z 4 hilft in jenen Fällen, in denen ein Gesetz (wie z.B. das SPG) diesbezüglich keine Regelungen vorsieht, nicht.

Die Neuregelung des § 26 Abs 10 schwächt dieses Problem zwar ab, indem die Pflicht des Dienstleisters zur Nennung des Auftraggebers oder zur Weiterleitung an diesen normiert wird. Ebenso bedeutet der neue Abs 3 des § 31 diesbezüglich eine Verbesserung, wenn gem. dessen Z 2 eine Beschwerde *„die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner)*" nur enthalten muss, „*soweit dies zumutbar ist*". Angesichts der Spruchpraxis der DSK, wonach die Beschwerde für ihre Zulässigkeit den „Auftraggeber" genau zu bezeichnen hat, die insofern bislang auch vom VwGH unbeanstandet blieb (zB VwGH 21.10.2004, 2004/06/0086), erscheint eine Klarstellung auch im Hinblick auf Rechtssicherheit und Effizienz des Rechtsschutzes zumindest für den öffentlich-rechtlichen Bereich geboten.

Abhilfe könnte hier z.B. eine subsidiäre Regelung nachfolgender Art in § 4 Abs 1 Z 4 bringen: „Bei Zweifeln über die Auftraggebereigenschaft von Organisationseinheiten (Geschäftsapparaten) eines Organs gilt das Organ der Gebietskörperschaft selbst als Auftraggeber." Alternativ hierzu wären zumindest entsprechende Ausführungen in den EB wünschenswert.

5. Zu Art. 2 Z 18 und 27 (§ 4)

Grundsätzlich wird begrüßt, dass hinsichtlich manueller Daten, die nicht in Dateien enthalten sind, künftig eine klare Regelung darüber bestehen soll, welche Bestimmungen des DSG 2000 anwendbar sind. Allerdings wird darauf hingewiesen, dass durch die Formulierung „Dieses Gesetz gilt für Daten, die in einer Datenanwendung oder manuellen Datei verwendet werden." in § 4 Abs 2 der Eindruck entsteht, dass manuelle Daten gar nicht vom Schutzbereich des Grundrechts nach § 1 Abs 1 umfasst sind, sondern nur einzelne Bestimmungen des DSG 2000 auch auf sie anwendbar sind. Nach dem Wortlaut des § 1 Abs 1 iVm § 4 Abs 1 soll das Grundrecht

auf Datenschutz jedoch grundsätzlich alle personenbezogenen Daten schützen[3] (wenn auch die Regelungen für Datenanwendungen und manuelle Dateien in weiterer Folge umfassender sind). Versteht man § 4 Abs 2 als Einschränkung des Schutzbereichs des Grundrechts auf Datenschutz, so würde hinsichtlich manueller Daten, die nicht in einer Datei enthalten sind, die Horizontalwirkung dieses Grundrechts entfallen und ausschließlich einzelne einfachgesetzliche Regelungen zur Anwendung kommen. Zudem wären z.B. die Bestimmungen der §§ 51 f und die darin normierten Sanktionen auf die missbräuchliche Verwendung manueller Daten nicht anwendbar, was keine Ausweitung, sondern vielmehr eine Einschränkung des Schutzes dieser Daten wäre. Insofern ist die vorgeschlagene Bestimmung des § 4 Abs 2 missverständlich formuliert, da sie keinesfalls dazu führen sollte, dass manuellen Daten der grundrechtliche Schutz entzogen wird.

Die DSG-Novelle sollte zum Anlass genommen werden, den Umfang des Grundrechts auf Datenschutz zu klären, insbesondere, welche Bestimmungen für alle personenbezogenen Daten gelten und welche ausschließlich auf Datenanwendungen oder manuelle Dateien anwendbar sind. Um den grundrechtlichen Schutz für manuelle Daten – wenn auch in reduzierter Form – sicherzustellen, sollte eine Neuformulierung der Bestimmung erfolgen.

Aus diesen Gründen wird vorgeschlagen, § 4 Abs 2 wie folgt zu formulieren: „Die einfachgesetzlichen Bestimmungen dieses Bundesgesetzes gelten für Daten, die in einer Datenanwendung oder manuellen Datei verwendet werden. Wo in den folgenden Bestimmungen von Datenanwendungen die Rede ist, gelten sie auch für manuelle Dateien. Für alle übrigen manuellen Daten gelten § 6 Abs. 1 Z 1 bis 3 und Abs. 2, §§ 7 bis 9 und die Bestimmungen des 6. und 10. Abschnitts sinngemäß."

6. Zu Art. 2 Z 29 (§ 8 Abs 2)

Hier wird auf die Ausführungen unter 1. Allgemeines verwiesen, wonach die Reduktion der Rechtsschutzmöglichkeiten bei „*indirekt personenbezogenen Daten*" in einem deutlichen Spannungsverhältnis zur DatenschutzRL 95/46/EG steht. Dieser Ansicht zufolge stellt die Streichung des Widerspruchsrechts bzgl. solcher Daten – die allerdings (wie in den EB zutreffend bemerkt) bereits durch § 29 vorliegt – eine weitere Verschlechterung der ohnehin gemeinschaftsrechtlich bedenklichen Rechtslage dar.

7. Zu Art. 2 Z 30 (§ 8 Abs 4):

Die Verwendung strafrechtsrelevanter Daten wird nach wie vor gemeinsam mit den „nicht-sensiblen Daten" geregelt. Dies wird der von der RL 95/46/EG vorgegebenen besonderen systematischen Stellung solcher Daten nicht gerecht, zumal die RL in Art 8 „*besondere Kategorien personenbezogener Daten*" definiert und sich dabei sowohl auf strafrechtsrelevante Daten als auch auf „*sensible Daten*" iSd § 9 DSG bezieht. Sowohl Systematik als auch substantielle Ausgestaltung der RL 95/46/EG le-

[3] Vgl. Dohr/Pollirer/Weiss, Datenschutzrecht Kommentar, Wien 2002[2], RN 6) zu § 1.

gen daher nahe, dass strafrechtsbezogene Daten sensible Daten sind oder diesen zumindest näher stehen als nicht-sensiblen.

Es wird daher angeregt, die Bestimmung des § 8 Abs 4 entweder in einem neuen § 8a zwischen den nicht-sensiblen und den sensiblen Daten anzusiedeln oder diesen unter § 9 einzufügen, vorzugsweise – in Anlehnung an die Richtlinie – unter einer neuen Überschrift „Besondere Kategorien personenbezogener Daten".

8. zu Art. 2 Z 33 ff (§ 16 ff – Datenverarbeitungsregister)

Gemäß § 16 (alt) sind die der Einrichtung des Datenverarbeitungsregisters zu Grunde liegenden Zwecke einerseits die „*Prüfung der Rechtmäßigkeit*" von Datenanwendungen sowie andererseits die „*Information der Betroffenen*". Nach § 17 Abs 1 (alt wie neu) hat jeder Auftraggeber vor Aufnahme einer Datenanwendung *„eine Meldung an die Datenschutzkommission [...] zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten."* Durch den Wegfall der „*Kontrolle der Rechtmäßigkeit*" in § 16 Abs 1 ergibt sich aus der Zusammenschau dieser Bestimmungen, dass die Registrierung künftig ausschließlich der Information der Betroffenen dienen soll.
Verstärkt wird dieser Eindruck durch die Tatsache, dass nach § 20 Abs 1 des Entwurfes Meldungen von Datenanwendungen nunmehr *„nur automationsunterstützt auf ihre Vollständigkeit und Plausibilität zu prüfen"* sind. Diese Stoßrichtung, hinsichtlich einer eingelangten Meldung keine inhaltliche Prüfung vorzunehmen, also insbesondere keine Beurteilung der Frage, ob und inwieweit die beabsichtigte Datenanwendung mit den Bestimmungen des DSG, aber auch mit weiteren verfassungsgesetzlich gewährleisteten Rechten (insbesondere dem Recht auf Achtung der Privatsphäre) im Einklang steht, war bzw. ist bereits im DSG 2000 enthalten und wird durch den vorliegenden Entwurf noch weiter verstärkt.

Wie auch in den EB festgehalten wird, soll damit die derzeit bestehende Praxis der Führung des Datenverarbeitungsregisters lediglich zu Informationszwecken gesetzlich festgeschrieben werden. Dabei wird jedoch übersehen, dass einem derartigen Registrierungsverfahren die Vorschriften der DatenschutzRL 95/46/EG entgegenstehen.
Art. 18 Abs. 1 der RL sieht vor, dass die Meldung bei der Kontrollstelle vor Aufnahme der Verarbeitung stattzufinden hat; zu den inhaltlichen Erfordernissen dieser Meldung gehört gem. Art. 19 Abs. 1 lit f unter anderem *„eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach Artikel 17 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind"*. Dies impliziert, dass eine – zumindest vorläufige – Prüfung der Meldung sehr wohl vorgesehen und auch geboten ist. Das im Entwurf vorgesehene Registrierungsverfahren widerspricht damit eindeutig den europarechtlichen Vorgaben der RL 95/46/EG.

Auch aus grundrechtlichen, insbesondere rechtsstaatlichen Erwägungen wird diese Tendenz als ausgesprochen bedenklich erachtet; Betroffenen ist der Umstand der Datenerfassung oftmals nicht bewusst. Es bedarf daher zum einen im Anwendungsbereich des DSG 2000 gewisser Elemente eines kommissarischen Rechtschutzes, zum anderen sollte seitens der Republik Österreich schon aus rechtsstaatlichen Erwägungen ein Interesse an (grund-) rechtskonformem Vorgehen der Auftraggeber bestehen. Mit dem gegenwärtigen System, welches durch den vorliegenden Entwurf

in diesem Punkt nicht nur keine Verbesserung, sondern noch im Gegenteil weitere Abstriche erfährt, ist die (Grund-) Rechtskonformität der angemeldeten Datenwendungen in keiner Weise gesichert. Soweit die Meldung – wie § 20 des Entwurfes vorsieht – vollständig und plausibel ist, wobei dies nur durch einen *„automationsunterstützten Prüfalgorithmus“* (so die erläuternden Bemerkungen zu §§ 20 – 22) überprüft wird, „*ist sie sofort zu registrieren.“* Mit dieser Registrierung darf die Datenanwendung aufgenommen werden. Dies erscheint auch insofern bedenklich, als ein öffentliches Register prinzipiell die Vermutung begründet, die registrierten Anwendungen seien auch auf ihre Rechtmäßigkeit geprüft worden, und damit eine Enttäuschung des Vertrauens der Rechtsschutzsuchenden antizipiert.

Dass eine inhaltliche Prüfung der angemeldeten Datenanwendung, in manchen Fällen auch ergänzt durch einen Lokalaugenschein (evt. in Begleitung entsprechend ausgebildeter IT-Experten) zeit- und kostenintensiv ist, liegt auf der Hand. Der in dem gegenständlichem Entwurf gewählte Weg, die angestrebte Entlastung der Kommissionsmitarbeiter durch unter anderem (wie es in den erläuternden Bemerkungen zu § 22a heißt) *„den Entfall der Detailprüfung bei nicht vorabkontrollpflichtigen Datenanwendungen“* zu erreichen, anstatt der notorischen personellen Unterbesetzung der Datenschutzkommission durch eine entsprechende Aufstockung der Mittel entgegen zu treten, ist dem Rechtsschutz der Betroffenen abträglich und – wie schon zuvor angemerkt – rechtsstaatlich bedenklich.

Bedenklich ist auch die Regelung in Ansehung der Registrierung vorabkontrollpflichtiger Datenanwendungen. Diese sind zwar nach § 18 des Entwurfes (wie schon bisher) einer inhaltlichen Kontrolle zu unterziehen, jedoch entscheidet letztendlich der Antragsteller selbst (durch die Art der Bezeichnung der zu verarbeitenden Daten wie auch durch Ankreuzen des entsprechenden Kästchens) und nicht die Datenschutzkommission, ob eine der Vorabkontrollpflicht unterliegende, also in besonderer Weise zu prüfende Datenanwendung vorliegt. Gerade in so grundrechtsrelevanten Bereichen wie der Verarbeitung sensibler und/oder strafrechtsrelevanter Daten sollte aber eine behördliche Kontrolle der Datenanwendung (nicht nur in Bezug auf Plausibilität und Vollständigkeit) sichergestellt sein, was nach dem vorliegenden Entwurf nicht der Fall ist, da es dem Auftraggeber selbst überlassen bleibt, ob er seine Datenanwendung als vorabkontrollpflichtig bezeichnet und damit einer inhaltlichen Rechtmäßigkeitskontrolle unterwirft.

> **Es wird daher angeregt, die das Registrierungsverfahren regelnden Bestimmungen derart abzuändern, dass die Registrierung einer Datenanwendung erst erfolgt, sobald durch die Kommission überprüft und sichergestellt worden ist, dass die Datenanwendung mit den geltenden rechtlichen Bestimmungen (auch und gerade in materieller Hinsicht) im Einklang steht. Gleichzeitig sollten der Datenschutzkommission zur Bewältigung dieser rechtsstaatlich gebotenen Aufgabe entsprechende Mittel zur Verfügung gestellt werden.**
>
> **Als absolut gebotenes rechtsstaatliches Minimum sollte die Beurteilung der Frage, ob eine vorabkontrollpflichtige Meldung vorliegt, nicht dem Antragsteller überlassen, sondern durch eine inhaltliche Mindestkontrolle seitens der Datenschutzkommission vorgenommen werden.**

9. Zu Art. 2 Z 41 (§ 24 Abs. 2a):

Ausdrücklich begrüßt wird die Einführung einer Informationspflicht der Auftraggeber in Fällen, in denen ihnen bekannt wurde, dass Daten aus einer ihrer Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden, da die Kenntnis der Betroffenen über Datenmissbrauch eine wesentliche Voraussetzung für die Wahrung ihrer Rechte ist.
Allerdings ist die Informationspflicht diesbezüglich sehr beschränkt, da sie nur bei „systematischem" Missbrauch besteht, wobei mangels konkreter qualitativer und quantitativer Kriterien unklar ist, ab wann ein solcher vorliegt.
Punktueller Missbrauch ist damit – mag er auch im Einzelfall schwerwiegend sein – generell von der Informationspflicht ausgenommen, obwohl die Betroffenen auch hier typischerweise ein massives Interesse an Information haben. Angesichts der Tatsache, dass die Informationspflicht ohnehin nur dann besteht, wenn dem Auftraggeber der Datenmissbrauch tatsächlich bekannt wird, ist hier jedenfalls von einem überwiegenden Interesse der Betroffenen auszugehen. Warum der einzelne Betroffene geringeren Rechtsschutz genießen soll, wenn im Einzelfall nur seine Daten von schwerwiegendem Missbrauch betroffen sind, als wenn dies auch andere betrifft, ist ebenfalls nicht ersichtlich. Demgegenüber ist nicht davon auszugehen, dass eine Informationspflicht des Auftraggebers auch in solchen Fällen diesen unverhältnismäßig belasten würde.

Aufgrund dieser Erwägungen wird angeregt, die Voraussetzung des „systematischen" Datenmissbrauchs entfallen zu lassen und eine Informationspflicht des Auftraggebers bei Kenntnis jeder schwerwiegenden unrechtmäßigen Datenverwendung vorzusehen.

Zudem stellt sich die Frage, welche Konsequenzen der Auftraggeber zu gewärtigen hätte, der entgegen dieser Bestimmung von einer Information der Betroffenen Abstand nimmt. Zwar würde sein Verhalten, genauer sein Unterlassen, dem Regelungsgehalt der in Rede stehenden Bestimmung widerstreiten und wäre somit rechtswidrig, doch stünde zu befürchten, dass so mancher Auftraggeber nach entsprechender Kosten – Nutzen – Abwägung von einer Information der Betroffenen Abstand nehmen würde.

Gerade in jüngerer Zeit wurden wiederholt Fälle unrechtmäßiger Überwachungen und Datenverwendungen bei unterschiedlichen Großkonzernen (etwa im Lebensmittelbereich) bekannt. Datenschutzrechtlicher Auftraggeber ist in diesen Fällen in der Regel jenes Unternehmen, welches die Daten missbräuchlich verwendet hat oder die Überwachungsmaßnahmen unrechtmäßig angeordnet bzw. durchgeführt hat.

Die Gefahr, dass Unternehmen wie die beispielhaft angesprochenen, mit der Entscheidung konfrontiert, die Betroffenen zu informieren oder den „Vorfall" zu vertuschen, sich angesichts der sehr überschaubaren Gefahr wie auch Höhe von Sanktionen gegen eine an sich gebotenen Information der Betroffenen entscheiden, liegt auf der Hand.

§ 52 Abs 2 sieht als Höchststrafe für die unrechtmäßige Nichtinformation der Betroffenen eine Verwaltungsstrafe im Höchstausmaß von € 9.445 vor. Dieser Betrag mag zwar für viele Kleinunternehmen und einen Großteil der Privatpersonen schmerzhaft,

unter Umständen auch existenzgefährdend sein, doch wird diese Strafdrohung in Ansehung von Großkonzernen kaum abschreckende Wirkung entfalten können.

Dass ein Unternehmen die Information über schwerwiegenden systematischen oder auch einzelfallbezogenen Datenmissbrauch unterlässt, hat zumeist den Sinn, einen durch das Bekanntwerden des Vorfalls hervorgerufenen Imageschaden im Fall einer Veröffentlichung und die damit möglicherweise einhergehenden durchaus massiven finanziellen Einbußen abzuwenden. Wird eine solche Vertuschung dann doch bekannt – und nur dann kann schließlich eine angedrohte Sanktion überhaupt verhängt werden – wird der Imageschaden durch die Vertuschung potenziert, womit die Sanktionsfrage unter Umständen ohnehin in den Hintergrund tritt. Doch vermögen lediglich geringe Sanktionen die Entscheidungsträger (speziell größerer Unternehmen) kaum zusätzlich zu rechtskonformem Verhalten zu motivieren. Die Androhung einer empfindlichen Geldstrafe könnte hier bei einer Kosten – Nutzen – Risikoabwägung zum Zünglein an der Waage werden. Die Zumessung könnte in Bezug auf Unternehmen schließlich in fairer Weise ertragsbezogen nach den Regeln des VbVG über die Verbandsgeldbuße erfolgen.

Es wird daher angeregt, gerade in schwerwiegenden Fällen systematisch unrechtmäßiger Datenverwendungen die Nichtinformation, soweit sie mit dem Vorsatz erfolgt, sich oder einen Dritten dadurch unrechtmäßig zu bereichern bzw. eine sonst drohenden Vermögensschaden unrechtmäßig zu vermeiden oder mit der Absicht, einen anderen dadurch in seinen von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, mit gerichtlicher Strafe von bis zu einem Jahr Freiheitsstrafe, jedenfalls aber mit deutlich höherer Geldstrafe zu bedrohen.

10. Zu Art. 2 Z 45 (§ 26 Abs. 10):

Zur Durchsetzung seiner Rechte bedarf der Betroffene eines Ansprechpartners, welcher grundsätzlich der Auftraggeber ist. Dass die Identifizierung desselben für den Betroffenen auf mitunter kaum überwindbare Hindernisse stößt, wurde bereits oben unter Punkt 4. ausgeführt. Die hier angesprochene Regelung bringt für den Betroffenen eine partielle Entschärfung dieser Problematik mit sich und wird daher begrüßt.

11. Zu Art. 2 Z 51 (§ 30 Abs. 6a):

Ebenfalls begrüßt wird die Möglichkeit der Untersagung einer Datenanwendung durch Mandatsbescheid bei wesentlicher Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen. Dadurch wird sichergestellt, dass auch im Falle nicht meldepflichtiger bzw. ordnungsgemäß registrierter Datenanwendungen rascher Rechtsschutz für die Betroffenen zur Verfügung steht. Allerdings ersetzt dieses Mittel nicht die vorherige Prüfung der Rechtmäßigkeit einer Datenanwendung im Registrierungsverfahren, da hier nur auf bestehende Gefährdungen reagiert werden kann, während eine Rechtmäßigkeitskontrolle im Registrierungsverfahren die Gefährdung von Datenschutzinteressen schon vorbeugend verhindern kann. Zudem ist diese Maßnahme als Ausnahmebestimmung zu sehen, mittels derer die DSK anlassbezo-

gen auf ihr zur Kenntnis gelangte Vorfälle rasch und effizient reagieren kann, nicht aber als Teil des regulären Rechtmäßigkeitsprüfungsverfahrens. Im Übrigen wird hier auf die Ausführungen unter 8. verwiesen.

12. Zu Art. 2 Z 52 (§ 31 samt Überschrift):

Wie in den EB zutreffend bemerkt wird, haben die Bescheide der Datenschutzkommission gegenüber Auftraggebern des öffentlichen Rechts lediglich Feststellungscharakter, während in Verfahren gegen private Auftraggeber auch ein vollstreckbarer Leistungsauftrag zu erteilen ist. Dies führt insbesondere in Verfahren wegen Verletzungen der Auskunftspflicht zu dem unbefriedigenden Ergebnis, dass Betroffene auch bei Feststellung einer Verletzung darauf angewiesen sind, die gewünschte Auskunft von der Behörde auch tatsächlich zu erhalten; wird diese erneut unvollständig erteilt, so kann lediglich ein weiteres Verfahren angestrengt werden, das dann wiederum in der Feststellung endet, dass eine Verletzung des Auskunftsrechts stattgefunden hat.
Aus Gründen der Rechtssicherheit, des effektiven Schutzes der Interessen der Betroffenen und im Sinne der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit der Verwaltung könnten derartige Häufungen von Verfahren vermieden werden, indem die DSK auch gegenüber Behörden Leistungsaufträge erteilen dürfte, in denen dann zum Beispiel der Umfang einer zu erteilenden Auskunft konkret angeführt würde. Ein eindeutig umgrenzter Leistungsauftrag könnte solcherart insbesondere die Grundlage für allfällige Amtshaftungsansprüche und/oder einen konkreten Beurteilungsmaßstab darstellen, ob unter Umständen ein Amtsmissbrauch iSd § 302 StGB vorliegt. Dies würde den durch die DSK zunächst normativ gewährten Rechtsschutz effektiv in die Realität transportieren und damit deutlich stärken.
Dass der VwGH in verschiedenen Erkenntnissen die Möglichkeit des Erlasses von Leistungsbescheiden gegen Auftraggeber des öffentlichen Rechts durch die DSK verneint hat, ist ein Resultat der geltenden Rechtslage; der VwGH ist nicht in der Lage, sich über die hier bestehenden Bestimmungen hinwegzusetzen.
Vielmehr obliegt es hier dem Gesetzgeber, entsprechende Regelungen zu treffen, der an dieser Stelle aufgerufen ist, die aktuelle unbefriedigende Rechtslage zu verändern.

Aufgrund dieser Erwägungen wird angeregt, § 31 Abs 7 zu reformieren und auch gegenüber Auftraggebern des öffentlichen Rechts den Erlass von konkreten Leistungsaufträgen vorzusehen, zumindest im Hinblick auf das Auskunftsrecht.

13. Zu Art. 2 Z 67 (§ 38 Abs. 2):

Mit der gegenständlichen Bestimmung wird ein Informationsrecht des Bundeskanzlers über alle Gegenstände der Geschäftsführung der Datenschutzkommission normiert. In Anbetracht der bereits unter 1. Allgemeines dargelegten Bedenken hinsichtlich der Unabhängigkeit der Datenschutzkommission erscheint ein derartiges Aufsichtsrecht als weiterer Schritt weg von einer unabhängigen Datenschutzbehörde.

Aus diesem Grund wird angeregt, von einem derartigen Informationsrecht abzusehen und die Datenschutzkommission als zweifelsfrei unabhängige, eigenständige Behörde neu zu installieren, vorzugsweise auf Basis einer verfassungsrechtlichen Weisungsfreistellung.

14. Zu Art. 2 Z 82 (9a. Abschnitt Videoüberwachung):

Allgemeines

Grundsätzlich wird begrüßt, dass das Thema Videoüberwachung nunmehr eine ausdrückliche Regelung erfährt. Hierbei ist allerdings größte Behutsamkeit geboten, vor allem hinsichtlich der Frage, wann der hier im Vordergrund stehende Schutz eines Objekts bzw. einer Person tatsächlich einen Eingriff in die Grundrechte auf Privatsphäre und Datenschutz rechtfertigt.

Zunächst ist anzumerken, dass der in den EB angeführte Vorbehalt speziellerer Regelungen in Materiengesetzen – im Sinne der Rechtssicherheit – ausdrücklich in den Normtext Eingang finden sollte.

Dass bei einer Videoüberwachung in aller Regel auch sensible Daten (Hautfarbe, Gesundheit etc.) erfasst werden (wenn auch nicht intentional), ist bei der Regelung dieses Bereichs jedenfalls zu berücksichtigen. Schon aus diesem Grund sollte von pauschalen Zulässigkeitsbestimmungen, die eine Überwachung zu bestimmten Zwecken in jedem Fall erlauben, Abstand genommen werden. Zudem sollte eine Registrierung im Datenverarbeitungsregister die Regel und nicht die Ausnahme sein.

Die derzeitige datenschutzrechtliche Situation im Hinblick auf Videoüberwachung stellt sich zutiefst unzufriedenstellend dar: Die überwiegende Mehrheit der Überwachungsanlagen ist derzeit nicht im Datenverarbeitungsregister registriert und verletzt somit – nach geltender Gesetzeslage – die Bestimmungen des DSG 2000. Die Schaffung besonderer Regelungen in diesem Bereich sollte nun jedoch keinesfalls zum Anlass genommen werden, die bestehende unbefriedigende Praxis der umfassenden Videoüberwachung allerorts gesetzlich zu verankern, sondern vielmehr auf einen vernünftigen, kontrollierten Einsatz von Videoüberwachungsanlagen hinwirken.

§ 50a Abs 1 Z 2:

Der Begriff der „*gesetzlichen oder vergleichbaren rechtlichen Sorgfaltspflichten*“ des § 50a Abs 1 Z 2 als rechtmäßiger Überwachungszweck scheint – auch im Hinblick auf Art 18 B-VG – einen problematisch weiten Spielraum zu eröffnen, zumal gerade rechtliche Sorgfaltspflichten sehr einfach selbst geschaffen werden können (etwa durch vertragliche Vereinbarung mit Dritten). Dem allgemeinen Verweis auf den Verhältnismäßigkeitsgrundsatz sollte dessen konkrete Berücksichtigung bereits in der Formulierung der einzelnen Eingriffstatbestände jedenfalls vorangehen.

Aus diesem Grund wird angeregt, den Begriff der „vergleichbaren rechtlichen Sorgfaltspflichten“ in § 50a Abs 2 näher zu konkretisieren.

§ 50a Abs 4 Z 3:

Weiters ist die generelle Zulässigkeit einer Überwachung in Echtzeitwiedergabe (ohne Speicherung) zum Schutz des Eigentums des Auftraggebers (§ 50a Abs 4 Z 3) fragwürdig: Die Einschätzung in den erläuternden Bemerkungen, dass hier typischerweise von einem überwiegenden Interesse des Auftraggebers ausgegangen werden könne, ist insofern nicht zu teilen, als auch eine Echtzeitüberwachung erheblich in die Grundrechte der Betroffenen eingreifen kann, weil diese im Regelfall nicht unterscheiden können, ob es sich um ein Aufzeichnungsgerät oder eine bloße Echtzeitüberwachung handelt. Diesbezüglich ist zu differenzieren zwischen der Sicht des objektiven Betrachters (von dem der Normtext offensichtlich ausgeht) und der Sicht des tatsächlich Betroffenen, dem keine Informationen über Auftraggeber, Art und Zweck der Videoüberwachung zur Verfügung stehen. Für diese nicht informierten Betroffenen entsteht ein Überwachungsdruck, der letztendlich zu einer Verhaltensanpassung führt, weil für sie das Ausmaß der Überwachung nicht erfassbar ist.
Hier sind auch die Erwägungen des OGH zu berücksichtigen, der in einem derartigen Fall bereits in der Anbringung einer Überwachungskamera-Attrappe eine Verletzung der Privatsphäre des Betroffenen sah, da dieser einem ständigen Überwachungsdruck ausgesetzt wurde und sich aufgrund des Vorhandenseins der Kameraattrappe kontrolliert fühlen musste (OGH 28.3.2007, 6 Ob 6/06k).

Aus diesem Grund ist eine Bestimmung, die eine generelle Zulässigkeit der Echtzeitüberwachung zu Zwecken des Eigentumsschutzes normiert, ohne eine Verhältnismäßigkeitsprüfung im Einzelfall vorauszusetzen, abzulehnen.

§ 50 Abs 4 Z 1:

Ähnliches gilt für den Fall eines drohenden gefährlichen Angriffes (Z 1 leg cit), wobei dieser Begriff sehr weit ausgelegt werden kann. Zu bedenken ist, dass aufgrund dieser Bestimmung z.B. eine umfassende Videoüberwachung ganzer Wohngegenden durch eine selbsternannte Bürgerwehr zulässig wäre, wenn es in der Vergangenheit (wenn auch möglicherweise nur vereinzelt) zu Einbrüchen kam, da nach den Ausführungen der EB schon dann eine präventive Videoüberwachung zulässig sein soll, wenn noch gar kein gefährlicher Angriff auf das überwachte Objekt selbst stattgefunden hat. In der Praxis würde diese Bestimmung voraussichtlich jede Echtzeitüberwachung legitimieren, da ein möglicher gefährlicher Angriff – vor allem gegen das Eigentum gerichtet – wohl in fast jedem Fall argumentierbar ist. Die erläuternden Bemerkungen führen ausdrücklich an, dass sich der hier verwendete Begriff des „gefährlichen Angriffs“ nicht mit jenem des § 16 SPG deckt. Aufgrund des Zusammenhangs der vorliegenden (Überwachungs-)Bestimmung mit sicherheitspolizeilichen (Kern-) Aufgaben erschiene eine andere Begriffswahl der Rechtssicherheit äußerst zuträglich, zumal aus dem Gesetzeswortlaut allein der Eindruck entsteht, dass hier staatliche Kernaufgaben an Private übertragen werden. Eine derartige Entwicklung wird ausdrücklich abgelehnt.

Aus diesen Gründen wird dringend angeregt, die generelle Zulässigkeit von Echtzeitüberwachungen iSd § 50a Abs. 4 Z 1 und 3 entfallen zu lassen und eine Einzelfallsbeurteilung vorzusehen.

§ 50a Abs 5:

Das Verbot der Videoüberwachung zur Mitarbeiterkontrolle am Arbeitsplatz (§ 50a Abs 5) wird ausdrücklich begrüßt. Hinsichtlich der „*Orte […], die zum höchstpersönlichen Lebensbereich eines Betroffenen zählen*“ wäre jedoch eine Neuformulierung anzudenken, da die Bestimmung in dieser Form gewisse Bereiche nicht ausnehmen würde, die aus augenscheinlichen Gründen einer Videoüberwachung keinesfalls zugänglich sein sollten (z.B. ein öffentlicher FKK-Strand).

§ 50a Abs 6:

Grundsätzlich ist die Zulässigkeit der Übermittlung strafrechtlich relevanter „Zufallstreffer“ unbedenklich. Allerdings sollte durch geeignete Einschränkungen sichergestellt werden, dass diese Bestimmung in der Praxis nicht in eine pauschale Legitimierung an sich unzulässiger Videoüberwachungen durch selbsternannte „Hilfssheriffs“ umgedeutet werden kann.

§ 50c Abs 2:

Die Prüfung der Rechtmäßigkeit einer Videoüberwachung im Rahmen einer Vorabkontrolle ist ein wichtiges Instrument, um schon im Vorfeld der Überwachungstätigkeit Grundrechtseingriffe auf ihre Zulässigkeit hin zu prüfen. Umso weniger nachvollziehbar ist es daher, dass nach § 50c Abs 2 sowohl bloße Echtzeitüberwachungen als auch Videoüberwachungen, bei denen die Aufzeichnung nur auf analogen Speichermedien erfolgt, von der Meldepflicht generell ausgenommen sind.

Wie bereits unter 8. dargelegt, ist ein wichtiger Zweck der Registrierungspflicht die Information der Betroffenen. Zumal für die Betroffenen im Regelfall nicht erkennbar sein wird, ob eine Videoüberwachungsanlage zur Echtzeitüberwachung, zur Speicherung auf analogen Medien oder zur Speicherung auf digitalen Medien dient, besteht hier aus Sicht der Betroffenen in allen Fällen ein gleiches Interesse an der Registrierung im DVR, da für sie ansonsten gar nicht feststellbar ist, wie intensiv der Eingriff in ihre Grundrechte tatsächlich ist.

Zudem können Betroffene nicht davon ausgehen, dass nicht registrierte Videoüberwachungen bloß der Echtzeitüberwachung bzw. der Speicherung auf analogen Speichermedien dienen, da auch heute schon die überwiegende Mehrzahl von Videoüberwachungen (trotz bestehender Registrierungspflicht) nicht registriert ist.
Aus diesem Grunde ist nicht nachvollziehbar, warum die Registrierungspflicht und die damit verbundene Informationsmöglichkeit für die Betroffenen je nach Art der Videoüberwachung unterschiedlich ausgestaltet sein soll.

Auch das in den EB angeführte Argument, dass *„auf Grund der sehr beschränkten Strukturierbarkeit und damit Suchbarkeit die Gefährdung der Geheimhaltungsinteressen unbeteiligter Dritter deutlich herabgesetzt“* sei und damit eine Ausnahme von der Meldepflicht nach Maßgabe der RL 95/46/EG Art. 18 Abs 2 erster Unterabsatz zulässig sei, übersieht, dass eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen schon durch die Videoüberwachung selbst und nicht erst durch die Verarbeitung der damit erhobenen Daten entsteht. Da, wie in der oben bereits erwähnten Entscheidung des OGH dargelegt, sogar eine Videoüberwachungsattrappe unter

bestimmten Umständen Grundrechte verletzen kann, gilt dies umso mehr für tatsächlich stattfindende Echtzeitüberwachung bzw. Videoüberwachung unter Verwendung analoger Speichermedien.

Zuletzt erscheint es nicht wünschenswert, der bisher verbreiteten Praxis, unregistrierte Videoüberwachungsanlagen zu betreiben, damit zu begegnen, indem weite Teile von der Meldepflicht ausgenommen werden und somit der bisherige, unzulängliche Zustand, nämlich ein unkontrollierter Wildwuchs an Überwachungskameras, legalisiert wird.

Sehr zu begrüßen ist dagegen die Kennzeichnungspflicht für Videoüberwachungen.

Aus diesen Gründen wird dringend angeregt, vom Entfall der Meldepflicht für Echtzeitüberwachungen und Videoüberwachungen unter Verwendung ausschließlich analoger Speichermedien abzusehen.

15. Zu Art. 2 Z 83 und 84 (§ 51):

Ausdrücklich begrüßt wird die Neufassung des § 51, der nunmehr auch die bloße Schädigungsabsicht umfasst und nicht mehr auf das Vorhandensein eines Vermögensvorteils oder eines Nachteils für den Betroffenen abstellt. Ebenso positiv wird der Wegfall des § 51 Abs 2 gesehen, durch den missbräuchliche Datenverwendungen nunmehr Offizialdelikte darstellen und von Amts wegen zu verfolgen sind. Diese Maßnahme erhöht den Stellenwert des Grundrechts auf Datenschutz erheblich und gibt Anlass zur Hoffnung, dass diese Bestimmung künftig häufiger Anwendung finden wird.

16. Zu Art. 3 (§ 54 Abs. 8 SPG):

Wie bereits unter 14. ausgeführt, stellt auch die Echtzeitüberwachung einen Eingriff in das Grundrecht auf Datenschutz dar, wenngleich dieser Eingriff weniger intensiv sein mag als bei einer Speicherung der Daten. Die neue Befugnis des § 54 Abs 8 SPG ist nun insofern sehr weit, als die Sicherheitsbehörden zum Einsatz von Bildübertragungsgeräten zur Echtzeitüberwachung ermächtigt sind, sofern „*dies zur Erfüllung einer sicherheitspolizeilichen Aufgabe oder zur Unterstützung des Streifendienstes erforderlich ist*“. Nach ständiger Judikatur des EGMR sind beim Einsatz geheimer Überwachungsmaßnahmen, die in das Recht auf Achtung des Privatlebens nach Art. 8 EMRK eingreifen, besonders hohe Anforderungen an die gesetzliche Grundlage zu stellen: So müssen unter anderem Eingriffssituationen möglichst genau umschrieben sein, damit ein Eingriff für die Betroffenen vorhersehbar ist.[4] Dies ist beim vorgeschlagenen § 54 Abs 8 SPG gerade nicht der Fall.

Dass der Einsatz von Echtzeitüberwachungsgeräten ein gelinderes Mittel ist als eine Überwachung mit Speicherung, ändert zudem nichts an der Tatsache, dass es sich

[4] EGMR 16.2.2000, Amann vs die Schweiz, Nr. 27798/95; EGMR 25.3.1998, Kopp vs die Schweiz, Nr. 23224/94, para. 72; EGMR 24.4.1990, Kruslin vs Frankreich, Nr. 11801/85, para. 63.

um einen Grundrechtseingriff handelt, der nur unter Wahrung der Rechte der Betroffenen aufgrund einer Interessensabwägung im Einzelfall zulässig ist.

Darüber hinaus sind keine Rechtsschutzmaßnahmen wie beispielsweise eine begleitende Kontrolle durch den Rechtsschutzbeauftragten vorgesehen, weshalb die Wahrnehmung der Rechte der Betroffenen ausschließlich davon abhängt, dass diese von der Überwachung Kenntnis erlangen und selbst Rechtsmittel ergreifen.

Zuletzt wäre jedenfalls sicherzustellen, dass die Betroffenen einer derartigen Überwachungsmaßnahme über diesen Eingriff informiert werden, wobei die Information unterbleiben könnte, solange und soweit überwiegende Interessen entgegenstehen.

Aus diesem Grund wird angeregt, die Bestimmungen über eine Befugnis der Sicherheitsbehörden zum Einsatz von Bildübertragungsgeräten zur Echtzeitüberwachung so festzulegen, dass ein Eingriff für die Betroffenen vorhersehbar ist, eine Verhältnismäßigkeitsprüfung im Einzelfall sichergestellt wird und den Betroffenen entsprechender Rechtsschutz zur Verfügung steht.

Für das Ludwig Boltzmann Institut für Menschenrechte:

Mag. Stefanie Dörnhöfer
Mag. Christian Schmaus
Mag. Christof Tschohl