Bundeskanzleramt – Verfassungsdienst
Ballhausplatz 2
1014 Wien
per Mail an v@bka.gv.at
Zu GZ BKA-810.026/0002-V/3/2008 Wien, 21.05.2008

Stellungnahme des *Ludwig Boltzmann Instituts für Menschenrechte (BIM)* zum Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008)

Sehr geehrte Damen und Herren!

Das Ludwig Boltzmann Institut für Menschenrechte (BIM) nimmt mit Bezug auf das Schreiben vom 4.3.2008 zu GZ BKA-810.026/0002-V/3/2008 zum ausgesendeten Entwurf einer DSG-Novelle 2008 wie folgt Stellung:

1. Allgemeines

Die technische Entwicklung und damit einhergehend die immer 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, einen Ausgleich zwischen dem Bemühen, ein für die zur Vollziehung berufenen Behörden möglichst effizientes Gesetz, welches auch der Wirtschaft nicht unnötige Belastungen auferlegt auf der einen Seite und gleichzeitig eine effiziente Kontrolle der Datenverarbeiter und den bestmöglichen (und natürlich ebenso effizienten) Rechtsschutz für den Betroffenen auf der anderen Seite sicherzustellen. Schließlich stellt sich angesichts der rasant voranschreitenden technischen Entwicklung die Frage, welches Ausmaß an Abstraktion 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“*

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

zu bringen, wie auch das (teils damit im Zusammenhang stehende) Bemühen um *„Klarstellung von in der Vollzugspraxis aufgetretener Rechtsfragen“.*

Eine Sensibilisierung für datenschutzrechtliche Fragen auf betrieblicher Ebene wie auch eine Verbesserung der Situation der von Kontrollmaßnahmen durch den Arbeitgeber betroffenen Arbeitnehmer, wird voraussichtlich die Einführung des Instituts des betrieblichen Datenschutzbeauftragten bringen und wird daher begrüßt.

Bedauert wird hingegen, 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 im Verhältnis zur sogenannten Datenschutzrichtlinie (RL 95/46/EG) bestehende Spannungsverhältnis aufzulösen.

Zwar unterliegen sowohl direkt wie auch indirekt personenbezogenen Daten dem Regime des Datenschutzgesetzes, doch zeigt sich bei genauerem Hinsehen, dass der Schutz für indirekt personenbezogene 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 DSG 2000), auch besteht kein Geheimhaltungsanspruch. In den Erläuternden Bemerkungen der Regierungsvorlage 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, das Recht auf Richtigstellung oder Löschung finden keine Anwendung bei „nur“ indirekt personenbezogenen Daten. Auch entfällt die grundsätzlich dem Betroffenen gegenüber bestehende Informationspflicht des Auftraggebers (siehe die Erläuternden Bemerkungen der Regierungsvorlage zu § 24 Absatz 6). Hieran soll sich nach dem vorliegenden Entwurf nichts ändern. Dass das Datenschutzgesetz indirekt personenbezogene Daten nicht sogleich expressis verbis vom Regelungsbereich des DSG ausschließt, erklärt sich wohl durch die Vorgaben der Datenschutzrichtlinie, welche grundsätzlich auch indirekt personenbezogene Daten als zu 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 Auftrageber 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.

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

2. Zu Z 10 (§ 1):

Den EB zu diesem Punkt ist insofern zuzustimmen, als die vereinfachte Formulierung (bis auf die Ausnahme der juristischen Personen) keine substantielle Änderung des Grundrechts auf Datenschutz bewirkt und daher im Hinblick auf eine bessere Verständlichkeit begrüßenswert ist.

Anders ist jedoch die Ausnahme juristischer Personen zu beurteilen. Zunächst ist festzuhalten, dass ein Anteil von 7,75% aller Entscheidungen keinen vernachlässigbar kleinen Wert darstellt. Das die „Datenschutzrichtlinie“ 95/46/EG ihren Anwendungsbereich nur auf natürliche Personen erstreckt, liefert überdies keinen Grund, den langjährig praktizierten und demgegenüber erweiterten Rechtsschutz nachträglich nur aus Kostengründen und Praktikabilitätserwägungen wieder einzuschränken. Problematisch scheint die in den EB formulierte Annahme, dass Daten, die bislang durch das DSG geschützt sind, ohnehin durch andere Bestimmungen (zB des gewerblichen Rechtsschutzes oder des Urheberrechts) geschützt seien.

Der gewerbliche Rechtsschutz greift eben 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 über die Gebarung oder die Personalpolitik eines Unternehmens nicht anwendbar. Auch das Schadenersatzrecht vermag die Anwendbarkeit des DSG nicht adäquat zu substituieren, zumal zB § 1330 ABGB nur gegen die Verbreitung unwahrer Tatsachen schützt, wohingegen Daten iSd DSG 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. Den EB liegt weiters offenbar die Annahme zugrunde, dass unter juristischen Personen stets im wirtschaftlichen Verkehr tätige Unternehmen zu verstehen seien. Tatsächlich handelt es sich bei diesen aber vielfach um Personengemeinschaften wie zB gemeinnützige Vereine nach dem Vereinsgesetz 2002, für die gewerbliche Rechtsschutzinstrumente generell nicht in Frage kommen und deren Daten überdies ein gesteigertes Maß an Schutzwürdigkeit auch im Hinblick auf andere Grundrechte (zB Religionsfreiheit Art 9 EMRK) aufweisen.

Diesen Überlegungen entsprechend wird hier von einer Ausklammerung juristischer Personen aus dem Anwendungsbereich des DSG abgeraten.

3. Zu Z 16 (§ 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 zu qualifizieren ist. Beispiel: Ein Polizeibeamter speichert die Daten einer Person, die ver-

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

dächtig 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 DSG hilft in Fällen nicht, in denen ein Gesetz (wie zB das SPG) diesbezüglich keine Regelungen vorsieht.

Die Neuregelung des § 26 Abs 10 DSG schwächt dieses Problem zwar ab, in dem die Pflicht des Dienstleisters zur Nennung des Auftraggebers oder zur Weiterleitung an diesen normiert wird. Ebenso bedeutet der neue Abs 3 des § 31 DSG 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 öffentlichen Bereich geboten.

> **Abhilfe könnte hier zB eine subsidiäre Regelung in § 4 Abs 1 Z 4 nachfolgender Art 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.**

4. Zu Z 26 (§ 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 Datenschutzrichtlinie 95/46/EG stehen. Dieser Ansicht zufolge stellt die Streichung des Widerspruchsrechts bzgl. solcher Daten – die allerdings (wie in den EB zutreffend bemerkt) bereits durch § 29 DSG vorliegt – eine weitere Verschlechterung der ohnehin gemeinschaftsrechtlich bedenklichen Rechtslage dar.

5. Zu Z 28 (§ 8 Abs 3 Z 5) und Z 31 (§ 9 Z 9):

In beiden Bestimmungen entfällt durch die Novelle die Wortfolge „und die Daten rechtmäßig ermittelt wurden“, jeweils im Zusammenhang mit der Datenverwendung zur Anspruchsdurchsetzung.

Die EB merken hierzu an, dass eine Ermittlung von Daten für Zwecke der Anspruchsdurchsetzung nach dem bisherigen Wortlaut nicht erfasst ist. Dem ist soweit zuzustimmen, zumal die Wortfolge „und die Daten rechtmäßig ermittelt wurden“ davon ausgeht, dass solche Daten bereits vorher (rechtmäßig) ermittelt wurden und damit keinen Spielraum für die Datenermittlung zum Zweck der Anspruchsdurchsetzung selbst lässt.

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Allerdings kann dieses Problem auch beseitigt werden, in dem der Wortlaut ergänzt wird wie folgt: „und die Daten rechtmäßig ermittelt wurden oder zu diesem Zweck ermittelt werden“.

Diese Lösung ist vorzuziehen, weil ansonsten die Beseitigung der rechtmäßigen Ermittlung als Bedingung aus dem Wortlaut suggerieren würde, dass auch unrechtmäßig ermittelte Daten zur Anspruchsdurchsetzung verwendet werden dürfen (Thema „rechtswidrig erlangte Beweismittel“ bzw. Beweisverwertungsverbot). Allerdings zeigt eine richtlinien- und verfassungskonforme Interpretation, dass eine solche Datenverwendung dem Grundrecht auf Datenschutz und dessen Sinn und Zweck zuwider laufen würde. Nach hA findet die Zulässigkeit von Beweismitteln daher dort ihre Grenze, wo solche unter Verletzung von Grundrechten gewonnen wurden oder die Verwertung selbst ein Grundrecht verletzen würde. Auch aus der einfachgesetzlichen Norm des § 6 Abs 1 DSG ergibt sich, dass nur rechtmäßig erhobene Daten verwendet werden dürfen.

Aus Gründen der Rechtssicherheit und der Rechtsklarheit wird daher die oben vorgeschlagene Variante empfohlen.

6. Zu Z 29 (§ 8 Abs 4):

Die Verwendung von strafrechtsrelevanten Daten wird nach wie vor gemeinsam mit den „nicht-sensiblen Daten“ geregelt. Dies wird (und wurde) der von der Datenschutzrichtlinie 95/46/EG vorgegebenen besonderen systematischen Stellung solcher Daten nicht gerecht, zumal die RL in Art 8 „besondere Kategorien personenbezogener Daten“ definiert und dabei sowohl strafrechtsrelevante Daten als auch „sensible Daten“ iSd § 9 DSG umfasst. Sowohl Systematik als auch substantielle Ausgestaltung der RL 95/46/EG legen daher nahe, dass strafrechtsbezogene Daten sensible Daten sind oder diesen zumindest näher stehen als nicht-sensiblen.

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

7. Zu Z 34 (§ 15a):

Ausdrücklich begrüßt wird die beabsichtigte Einführung eines betrieblichen Datenschutzbeauftragten. Wie nicht zuletzt aktuelle Beispiele etwa von im Lebensmittelbereich tätigen Unternehmen gezeigt haben, ist die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften im Betrieb zum Schutz der Arbeitnehmer mehr denn je ein Gebot der Stunde. Dem einzelnen Angestellten ist es aufgrund des mangelnden Fachwissens, aber insbesondere auch aufgrund des oftmals vorliegenden Abhängigkeitsverhältnis nur schwer möglich, gegen in seine Privatsphäre eingreifende Kontrollmaßnahmen seitens des Arbeitsgebers vorzugehen. Im Optimalfall kann der betriebliche Datenschutzbeauftragte das für Fragen des Recht auf Datenschutzes erforderliche Fachwissen mit seinen persönlichen Erfahrungen und Kenntnissen des jeweiligen Unternehmens zum Vorteil eines gedeihlichen Miteinanders zwischen Firmenleitung, die regelmäßig an einem effektiven Einsatz der Arbeitskraft interessiert

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

ist, und den Mitarbeitern, welche ein Interesse an der Wahrung ihrer Privatsphäre haben, einsetzen.

Unklar bleibt, ob ein betrieblicher Datenschutzbeauftragter auch an öffentlichen Einrichtungen, wie etwa von Bund oder Ländern betriebenen Schulen einzurichten ist. § 15a des Entwurfes verweist zwar u.a. auf die weite Begriffsbestimmung des § 34 Abs. 1 ArbVG, derzufolge Datenschutzbeauftragte in jeder Arbeitsstätte einzurichten wären, *„die eine organisatorische Einheit bildet, innerhalb der (...) die Erzielung bestimmter Arbeitsergebnisse fortgesetzt verfolgt wird (...)“.* Doch bleibt unklar, ob und inwieweit § 33 ArbVG hierbei mitzulesen ist. Dieser schließt bestimmte Betriebe wie etwa bestimmte öffentliche Unterrichts- und Erziehungsanstalten vom Anwendungsbereich des II. Teiles des ArbVG, der eben auch besagten § 34 enthält, aus. Insoferne könnte die Rechtsansicht vertreten werden, dass für solche Betriebe ein Datenschutzbeauftragter nach dem vorliegenden Entwurf nicht zu bestellen ist.

Es wird daher angeregt, in § 15a Abs. 1 eine dahingehende Klarstellung aufzunehmen, dass § 33 ArbVG, soweit es sich um die Frage der Betriebsinhabereigenschaft iSd § 15a Abs. 1 handelt, nicht mitzulesen ist, sodass die Einschränkungen des § 33 nicht zum Tragen kommen.

8. zu Z 35 ff (§ 16 ff – Datenverarbeitungsregister)

Gemäß § 16 DSG (alt wie neu) ist der der Einrichtung des Datenverarbeitungsregister zu Grunde liegende Zweck 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.“* Aus der Zusammenschau dieser beiden Bestimmungen ergibt sich, dass auch der Zweck der Meldung grundsätzlich in der Information der Betroffenen und nicht in der Prüfung der Rechtmäßigkeit der zur Registrierung eingereichten Datenanwendung liegt. 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 der eingelangten Meldung keine inhaltliche Prüfung, also insbesondere keine Beurteilung der Frage, ob und inwieweit die beabsichtigte Datenanwendung mit dem Bestimmungen des DSG, aber auch weiteren verfassungsgesetzlich gewährleisteten Rechten, wie jenes auf Achtung der Privatsphäre, im Einklang steht, vorzunehmen, war bzw. ist bereits im DSG 2000 enthalten, wird aber durch den vorliegenden Entwurf noch verstärkt,

Aus grundrechtlichen, insbesondere rechtsstaatlichen Erwägungen wird diese Tendenz für ausgesprochen bedenklich erachtet. Betroffenen ist Umstand der Datenerfassung oftmals nicht bewusst. Es bedarf daher zum einen im Anwendungsbereich des DSG 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 die gegenständliche Novelle in diesem Punkt nicht nur keine Verbesserung, sondern noch im Gegenteil weitere Abstriche erfährt, ist die (Grund-) Rechtskonformität der angemeldeten Datenwendungen in keinster Weise gesichert. So weit die Meldung – wie es § 20 des Entwurfes sagt – vollständig und plausibel ist, wobei dies nur durch einen *„automationsunterstützten Prüfalgorithmus“* (so die erläuternden Bemerkungen zu §§ 20 – 22) überprüft wird,

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

„*ist die Meldung sofort zu registrieren.“* Mit dieser Registrierung darf die Datenanwendung aufgenommen werden.

Dass eine inhaltliche Prüfung der angemeldeten Datenanwendung, in manchen Fällen auch ergänzt durch einen Lokalaugenschein (evt. in Begleitung entsprechend ausgebildeten Computerexperten) 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 einer 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, doch entscheidet letztendlich grundsätzlich der Antragsteller (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 bei 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.

> **Es wird daher angeregt, die das Registrierungsverfahren regelnden Bestimmungen derart abzuändern, dass eine Registrierung einer Datenanwendung nur 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 Z 47 (§ 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 3. ausgeführt. Die hier angesprochene Regelung bringt für den Betroffenen eine partielle Entschärfung dieser Problematik mit sich und wird daher begrüßt.

10. Zu Z 55 (§ 31 Abs. 3):

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

Nach der (noch) geltenden Rechtslage kann die Datenschutzkommission im Zuge der Behandlung einer Beschwerde bei Gefahr im Verzug die Verwendung von Daten (bis zur endgültigen Entscheidung) untersagen. Dem vorliegenden Entwurf zu Folge entfällt diese Möglichkeit. Weshalb diese Möglichkeit der Gewährung vorläufigen Rechtsschutzes (im Einzelfall) ersatzlos gestrichen wurde, ist schon aus Gründen der (eingriffsminimierenden) Wahrung der Betroffenenrechte nicht nachvollziehbar. Die erläuternden Bemerkungen zu § 31a führen hierzu aus, dass der Regelungsgehalt des § 31 Abs. 3 (alt) durch den neuen § 22 Abs. 4 und 5 abgedeckt sei.

Der Bezugnahme auf § 22 Abs. 4. und 5. scheint ein Redaktionsversehen zu Grunde zu liegen, da besagte Norm (Abs. 5 existiert nicht) die Rechtsnachfolge für registrierte Auftraggeber regelt. Sollte sich der Hinweis in den erläuternden Bemerkungen allenfalls auf § 22a Abs. 4 und 5 beziehen, so ist hierzu festzuhalten, dass diese lediglich auf das (mangelhafte, falls nämlich die Meldung der Datenanwendung trotz Verbesserungsauftrag nicht erfolgt ist) Registrierungsverfahren bezugnehmen, nicht aber auf ein Verfahren, welches ein Betroffener aus Anlass der (vermuteten) Verletzung seiner Rechte nach dem DSG anstrengt.

> **Es wird daher angeregt, die Möglichkeit des (vorläufigen) Rechtsschutzes in Form der Untersagung der Datenverwendung bei Gefahr im Verzug in der geltenden Form beizubehalten. Dass diese Bestimmung in der Praxis bisher bedeutungslos – so die EB zu § 31a – geblieben sei, vermag die Abschaffung dieser Möglichkeit des vorläufigen Rechtsschutzes nicht zu rechtfertigen.**

11. Zu Z 82 (9a. Abschnitt Videoüberwachung):

Allgemein ist es begrüßenswert, das Thema Videoüberwachung nunmehr einer ausdrücklichen Regelung zuzuführen. Hierbei ist allerdings größte Behutsamkeit geboten, vor allem hinsichtlich der Frage, wann der hier im Vordergrund stehende Schutz eines Objekts tatsächlich den Eingriff in das Grundrecht auf Privatsphäre und Datenschutz rechtfertigt. So scheint zB fragwürdig, ob eine Überwachung in Echtzeitwiedergabe (ohne Speicherung) zum Schutz des Eigentums des Auftraggebers (§ 50a Abs 3 Z 4 DSG) generell zulässig sein soll, ohne weitere Voraussetzungen – etwa ein überwiegendes Interesse – zu verlangen. Ähnliches gilt für den Fall eines drohenden gefährlichen Angriffes (Z 5 leg cit).

Auch der Begriff der „speziellen Sorgfaltspflichten“ der Z 6 leg cit scheint – auch im Hinblick auf Art 18 B-VG – einen problematisch weiten Spielraum zu eröffnen. Dem allgemeinen Verweis auf den Verhältnismäßigkeitsgrundsatz sollte dessen konkrete Berücksichtigung bereits in der Formulierung der einzelnen Eingriffstatbestände jedenfalls vorangehen.

Für das Ludwig Boltzmann Institut für Menschenrechte:
Mag. Christian Schmaus und Mag. Christof Tschohl

Dieses Dokument wurde mittels e-Mail vom Verfasser zu Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.