ARGE DATEN

DB RECHT / STELL / Unser Zeichen: dsg-novelle-2010.doc

An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 8. Juni 2009

Betreff: BKA-810.026/0005-V/3/2009
Stellungnahme der ARGE DATEN zur DSG-Novelle 2010

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

_____ _____
Dr. Hans G. Zeger (Obmann) Charlotte Schönherr (Schriftführerin)

Stellungnahme elektronisch übermittelt (*begutachtungsverfahren@parlinkom.gv.at)*

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/ veröffentlicht.

ARGE DATEN - Österr. Gesellschaft für Datenschutz A-1160 Wien, Redtenbacherg. 20 ☎ +43/676/9107032, Fax +43/1/4803209
www.argedaten.at DVR 0530794 info@argedaten.at Gerichtsstand Wien
ZVR 774004629 UID ATU 56627966 PSK 7.214.741 (BLZ 60000, IBAN: AT15 6000 0000 0721 4741, BIC: OPSKATWW)

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.

Stellungnahme der ARGE DATEN vom 8. Juni 2009 zur *DSG-Novelle 2010*

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.

Stellungnahme der ARGE DATEN vom 8. Juni 2009 zur DSG-Novelle 2010

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.

Übersicht

Das Bundeskanzleramt hat das Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird, die sogenannte DSG-Novelle 2010 in Begutachtung gebracht. Damit wurde offensichtlich auf die umfassende Kritik zahlloser Bürger zur geplanten DSG-Novelle 2008 reagiert (siehe Stellungnahmen zur Begutachtung 2008 http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml).

Diese Vorgangsweise wird von der ARGE DATEN als positiv begrüßt. Obwohl auf viele Anregungen der ARGE DATEN Rücksicht genommen wurde, wurde leider die Neuformulierung der Novelle nicht dazu genutzt alle grundsätzlichen Schwächen des alten Novellenentwurfs zu bereinigen.

Neben einigen durchaus positiven Ansätzen wurde nicht vollständig auf die Kritik bezüglich der Korrektur fehlerhafter alter, inpraktikabler und teilweise EU-vertragswidriger Regelungen ausreichend eingegangen. Ebenso wurde auf neue technologische Entwicklungen nicht angemessen reagiert.

Darüber hinaus wurden positive Ansätze der Novelle 2008, insbesondere die verpflichtende Einführung betrieblicher Datenschutzbeauftragter, wieder zurückgenommen und ersatzlos gestrichen. Die Rücknahme kann nur als sachlich unbegründetes Nachgeben einer einseitigen Klientelpolitik interpretiert werden. Dies wird von der ARGE DATEN ausdrücklich bedauert und geht im übrigen auch an den Interessen der Mehrheit mittlerer und größerer Betriebe vorbei. Diese wünschen eine klare Regelung zur datenschutzrechtlichen Verantwortlichkeit und auch zur innerbetrieblichen Positionierung eines Datenschutzbeauftragten. Sie erwarten sich im Gegenzug eine weitgehende Entbürokratisierung datenschutzrechtlicher Bestimmungen.

(1.) Wiederaufnahme des Datenschutzbeauftragten in Novelle

Es wird vorgeschlagen den Datenschutzbeauftragten in die Novelle 2010 wieder aufzunehmen, allenfalls die Betriebsgrenzen, ab denen der Datenschutzbeauftragte verpflichtend vorgeschrieben ist auf 50 Mitarbeiter zu erhöhen. Zusätzlich sollten Unternehmen die einen Datenschutzbeauftragten nominieren und diesen bei der Datenschutzkommission melden, von der Verpflichtung zur Meldung von Datenanwendungen befreit werden und stattdessen die datenschutzrechtlich relevanten Informationen für Betroffene unternehmensintern Unternehmen bereit halten können.

Neben der Reduzierung des bürokratischen Aufwandes für die Unternehmen hätte diese Lösung auch den Vorteil, dass die unternehmensinternen Informationen aktueller wären als die bisherigen Registrierungsunterlagen beim DVR, die durchwegs veraltet und unvollständig sind. Auch für die Datenschutzkommission käme es dadurch zu einer erheblichen Entlastung und sie könnte sich besser der wichtigen Aufgabe der Kontrolle widmen, statt der Verwaltung fehlerhafter Registrierungs"zettel".

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.) Informationspflicht

Ausdrücklich begrüßt wird die nun vorgesehen Einführung der im §24 Abs. 2a vorgesehenen Informationspflicht der Betroffenen bei schwerwiegenden und systematischen Rechtsverletzungen von Daten aus einer Datenanwendung. Es wird damit eine alte Forderung der ARGE DATEN erfüllt. Es wird auch eine EU-weite Entwicklung zu einer verbesserten Informationspflicht der Betroffenen aufgegriffen und in Österreich umgesetzt.

Leider wurde jedoch verabsäumt klare Sanktionen bei Verletzung dieser Informationspflicht vorzusehen. Da bei Datenschutzverletzungen, wie die letzten dreißig Jahre zeigten, in der Regel selten eine kausale Schadenskette, wie sie das materielle Schadensersatzrecht verlangt, darstellbar ist, wäre jedenfalls ein immaterielles Schadenersatzrecht vorzusehen. Dies hatte 1999, auch der Gesetzgeber richtigerweise erkannt und mit §33 DSG 2000 eine entsprechende Bestimmung eingeführt.

Mittlerweile haben mehrere Urteile die Grenzen dieses Schadenersatzrechtes abgesteckt und man kann sagen, dass sich diese Bestimmung bewährt hat. Im Zusammenhang mit der jetzt neuen Informationspflicht sollte jedenfalls von der Annahme einers Schadens des Betroffenen ausgegangen werden. Eine Verletzung der Informationspflicht sollte daher einen pauschalierten immateriellen Schadenersatzes begründen. Aktuelle OLG-Entscheidungen (GZ 14 R 74/08t) gehen von einem Satz von 750,- Euro als angemessenen Schadensersatzanspruch selbst bei geringfügigen Datenschutzverletzungen aus.

Es wird daher vorgeschlagen die Bestimmungen des §33 soweit zu erweitern, dass eine Verletzung des neuen §24 Abs. 2a einen immateriellen Schadensersatzanspruch begründen und es sollte eine Untergrenze von 750,- Euro für derartige Verletzungen festgelegt werden.

(3.) Fehlende Berücksichtigung technischer Entwicklungen

Besonders problematisch ist im vorliegenden Entwurf das Ignorieren neuer technologischer und gesellschaftspolitischer Entwicklungen, die seit nunmehr vielen Jahren erkennbar sind und international von Datenschutz- und Grundrechtsexperten diskutiert werden. Unter anderem sei auf die zahllosen Stellungnahmen der Artikel-29-Gruppe der EU-Datenschutzbeauftragten zu neuen Technologien verwiesen, weiters auf die Empfehlung der EU-Kommission zu RFID vom 12. Mai 2009 (http://ec.europa.eu/information_society/policy/rfid/index_en.htm). Die spezifischen Datenschutzanforderungen dieser neuen Techniken sollten im Gesetzesentwurf berücksichtigt werden.

In der täglichen Beratungspraxis zeigen sich Lücken im Schutz der Privatsphäre beim Einsatz von *Ortungssystemen* und bei der *Verwertung biometrischer Daten*. Ortungssysteme werden verstärkt im Zusammenhang mit zivilrechtlichen Auseinandersetzungen, im Rahmen von Partnerschaftskonflikten ("Rosenkrieg") oder zur Mitarbeiterüberwachung eingesetzt. Diese Ortungsdaten sind derzeit nicht als Telekommunikationsdaten definiert und fallen daher aus diesem Schutzsystem heraus. Es wird vorgeschlagen Ortungs- und

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.

Navigationsdaten, sofern sie mit einer Person verknüpfbar sind, anderen Telekommunikationsdaten gleichzustellen und den Datenschutzbestimmungen nach dem TKG 2003 zu unterwerfen.

Weiters werden biometrisch hinterlassene Datenspuren, etwa DNA-Spuren oder Fingerabdrücke unter Missachtung der Persönlichkeitsrechte ausgewertet und in privatrechtlichen Auseinandersetzungen eingesetzt (etwa "Vaterschaftstests" ohne gerichtliche Anordnung).

Derartige Daten, selbst wenn sie rechtswidrig beschafft wurden, können vor Gerichten verwertet werden, es fehlen Beweisverwertungsverbote für Daten die unter Verletzung der Datenschutzbestimmungen ermittelt und verarbeitet werden. Es sollten daher eindeutige Beweisverwertungsverbote geschaffen werden.

(4.) Fehlende Regelung von Scoringsystemen

Ein zunehmendes Problem bilden auch die ausufernden *Scoringsysteme*. Es handelt sich dabei um Systeme zur individuellen Beurteilung einer Person aufgrund allgemeiner oder statistischer Informationen und Erfahrungen.

Im Rahmen dieser Scoringmethoden werden nicht für eine Sache unmittelbar erforderliche Informationen gesammelt und ausgewertet, sondern andere allgemeine erhebbare soziale, soziographische oder demoskopische Daten, die einer Person zugeordnet werden können.

Im Gegensatz zu klassischen Kreditbeurteilungssystemen, wie sie früher bei Banken und dem KSV von 1870 verwendet wurden, in denen Ausgaben, offene Forderungen, Kredite und Zahlungsverpflichtungen einer Person zur Beurteilung seiner wirtschaftlichen Leistungsfähigkeit herangezogen werden und versucht wird das Risiko eines weiteren Kredites oder der Zahlungsunfähigkeit abzuschätzen, verwenden die neuen Scoringsysteme allgemeine Persönlichkeitsmerkmale zur Beurteilung der Betroffenen.

So führt die arbeitsrechtliche Position einer Person als "Arbeiter" gegenüber einem Angestellten zu einem Bewertungsabschlag, ebenso wenn er ledig ist, wenn er in einer Mietwohnung ist, wenn er jung ist, wenn er erst kurz eine Arbeit hat oder auch wenn er schlicht in einer "falschen" Wohngegend wohnt. Damit werden im statistischen Sinn möglicherweise richtige Informationen auf individuelle Personen übertragen, unabhängig davon ob diese Person nicht durch ihr individuelles Verhalten eine völlig andere Beurteilung verdient. Damit wird die Variabilität der Informationen ignoriert, eine klassische sachlich unbegründete Ungleichbehandlung.

Diese Scorings führen zum Ausschluß von bestimmten Leistungen, zu verschlechterten Kredit- und Versicherungskonditionen oder Verhindern die Eröffnung eines Bankkontos.

Scorings stellen einen wesentlichen Eingriff in die persönliche Lebensführung dar, ignorieren sie doch individuelle persönliche Eigenschaften zugunsten allgemeiner Bewertungsraster. *Scorings enthalten somit ein erhebliches Diskriminierungspotential.*

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.

Diese Scorings werden immer stärker von Telekom-Unternehmen, Versandhäusern, Banken, Leasingunternehmen, ja sogar von Vermietern, Möbelhändlern und Supporthotlines verwendet.

Die bisherigen Schutzmechanismen des DSG, insbesondere § 49 DSG 2000, "Automatisierte Einzelentscheidungen" gegen die willkürliche Verwertung allgemeiner Persönlichkeitsangaben haben sich als nicht tragfähig erwiesen, da diese Regelungen auf eine vollautomatisierte Entscheidung abstellen, die jedoch beim Scoring in der Praxis nicht vorkommt. Die Scoringwerte werden offiziell nur als Empfehlungen ausgewiesen, wobei jedoch die Mitarbeiter (Verkäufer) der Unternehmen, die diese Scorings anwenden gar keine Möglichkeit haben eine andere Entscheidung zu treffen, als es das Scoring vorgibt.

Während in Deutschland die Regelung und Beschränkung dieser Scoringmethoden offen und umfassend diskutiert wird, fehlen im vorliegenden DSG-Entwurf jegliche Ansätze zu Lösungsversuchen.

Es wird daher vorgeschlagen die bestehenden Scoring-Exzesse so weit wie möglich zurückzudrängen und vorzusehen, dass Unternehmen die Scoringverfahren einsetzen diese Verfahren generell offenlegen müssen und dass diese Verfahren von der Datenschutzkommission in Hinblick auf ihre sachliche Notwendigkeit zu prüfen sind. Soweit Scoringverfahren Voraussetzung oder Grundlage eines Vertragsabschlusses darstellen, sollen sie vor Vertragsabschluss den Interessenten offen gelegt werden müssen.

(5.) EU-vertragswidriger Ausschluss des Datenschutzes veröffentlichter Daten

Seit Jahren weist die ARGE DATEN darauf hin, dass die Bestimmung des §1 DSG 2000, die generell den Anspruch auf Achtung der Privatsphäre und Grundrechte ausschließt, wenn Daten "allgemein verfügbar sind" nicht der EG-Datenschutzrichtlinie 95/46/EG entspricht.

Diese generelle Ausschließung widerspricht Art. 1 der Richtlinie und ist somit EU-vertragswidrig. Auch die grundsätzlich positiveNeuformulierung des §1 DSG 2000 im Rahmen des vorliegenden Entwurfs saniert nicht diesen rechtswidrigen Zustand.

Besonders im Zusammenhang mit Web2.0-Diensten, den sozialen Netzwerken und den Personensuchmöglichkeiten im Internet gewinnt die Frage eines angemessenen Grundrechtsschutzes veröffentlichter Daten verstärkt an Bedeutung.

Es widerspricht der Entwicklung der Informationsgesellschaft diese Daten pauschal als vogelfrei zu erklären, die jeder nach eigenem Gutdünken verwerten und letztlich auch missbrauchen darf. Das wäre vergleichbar einer Regelung, die es jedem Menschen erlauben würde, ein auf der Straße abgestelltes und nicht abgesperrtes Auto oder Fahrrad nach Belieben in Betrieb nehmen zu können und zu benutzen.

Während eine derartige Nutzung ohne Einwilligung des Eigentümers Jeder als kriminelles Delikt sehen würde, ist die beliebige Nutzung veröffentlichter Daten in Österreich möglich.

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.

Dieser Missstand könnte einfach und EU-konform durch eine Verbesserung des §1 DSG saniert werden. Es müsste festgehalten werden, dass veröffentlichte Daten nur für jene Zwecke genutzt werden dürfen, zu denen der Betroffene im Rahmen der Veröffentlichung zugestimmt hat bzw. zu dessen Zweck er die Daten veröffentlicht hat. Weiters soll ihm das Recht gegeben werden, die Veröffentlichung jederzeit zu widerrufen. Benutzer von veröffentlichten Daten dürfen diese nicht diskriminierend einsetzen.

Mit einer derartigen Bestimmung wären die Probleme der sogenannten Web2.0-Plattformen und Social Communities weitestgehend und grundrechtskonform vermieden. Diese Communities dienen klar abgegrenzten Zwecken, etwa zum persönlichen Meinungsaustausch, zum Aufbau von Freundeskreisen, zur Partnersuche oder um berufliches Fortkommen zu erleichtern. Ein Verbot der Verwendung für andere Zwecke würde einerseits dazu führen, dass Personalabteilungen nicht mehr Informationen aus persönlichen Communities benutzen dürfen und andererseits wäre die Nutzung beruflicher Netzwerke (etwa XING, LINKEDIN, ...) durch Arbeitgeber weiterhin möglich.

Eine derartige Bestimmung hätte den Vorteil, dass sie in ganz Österreich wirksam wäre und alle Betroffenen schützen würde, unabhängig davon, ob die benutzte Plattform von einem österreichischen, einem innergemeinschaftlichen oder einem außerhalb der EU liegenden Unternehmen betrieben wird.

(6.) Verbesserter Rechtsschutz der Betroffenen

Ein weiterer Mangel des Entwurfs ist das Fehlen einer Verbandsklagsbefugnis. Die Vergangenheit zeigte, dass besonders die schwerwiegenden Datenschutzverletzungen im Regelfall nicht einzelne Personen betreffen, sondern viele Personen umfassen.

Typische Beispiele sind etwa rechtswidrige Datenverarbeitungen durch Wirtschaftsauskunftsdienste. Aufgrund der zahlreichen Beschwerden, der Auskünfte der Wirtschaftsauskunftsdienste und des vorliegenden Datenmaterials muss allein in dieser Branche mit 700.000 bis 1 Million Bürgern gerechnet werden, über die rechstwidrig Daten verwertet und weitergegeben werden.

Es wird daher eine Verbandsklagemöglichkeit vorgeschlagen, die jedenfalls Konsumentenschutzorganisationen, Kammern und besonders befugten Interessensvereinigungen einzuräumen ist.

(7.) Fehlende Behebung zahlloser Mängel und Fehler des alten DSG

Bezüglich der fehlenden Behebung zahlloser Mängel des alten DSG wird auf die zuletzt abgegebenen Stellungnahmen verwiesen und auf den folgenden Abschnitt "Teil II".

Die wichtigsten Punkte seien in Stichworten aufgelistet:
- Schaffung einer richtlinienkonformen unabhängigen Datenschutz-Aufsichtsbehörde
- Schaffung ausreichender materieller Zuständigkeiten der Datenschutz-Aufsichtsbehörde

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.

- Abschaffung des Österreich-Unikums "indirekt personenbezogene Daten", diese Datenart ist richtlinienwidrig
- Schaffung der Durchsetzbarkeit von Entscheidungen der Datenschutz-Aufsichtsbehörde gegenüber belangten Behörden (Exekutionsrecht)
- Präzisierung der Anforderungen einer gültigen Zustimmungserklärung durch Betroffene
- Verbesserung des Auskunftsrechts inklusive der Durchsetzbarkeit der Auskunft bei nur bestimmbaren Daten, wenn entsprechende Identifikationsdaten vorgelegt werden (Auskünfte im Zusammenhang mit Cookies, Videodaten usw.)
- Sanierung des Vier-Monate-Löschungsverbots im Zuge eines Auskunftsverfahrens nach §26 DSG 2000
- Schaffung einer Parteienstellung und eines Informationsrechts von Betroffenen in Verwaltungsstrafverfahren
- Schaffung durchsetzbarer Kontrollbefugnisse der Datenschutz-Aufsichtsbehörde (Durchsetzbarkeit des Zutritts-/Prüfrechts)
- Behebung der fehlerhaften Bestimmungen bei der Anrufung der Zivilgerichte (Unklare Zuständigkeiten, unzulässige Beschränkung der Durchsetzung einstweiliger Verfügungen), im vorliegenden Entwurf nur unvollständig saniert
- Beweisverwertungsverbot rechtswidrig gesammelter Daten vor Zivilgerichten und Verwaltungsbehörden
- BR-Rechte auch für den Bereich der nicht-sensiblen Daten sichern (derzeit nur in §9 für sensible Daten geregelt)
- Möglichkeit, dass Beschwerdeführer über die Ergebnisse einer §30 DSG Beschwerde informiert werden
- Verbesserung des immateriellen Schadenersatzrechts

(8.) Videoüberwachung weiterhin ungeeignet geregelt

Gegenüber dem Entwurf aus dem Jahr 2008 weisen die geplanten Bestimmungen zur Videoüberwachung (§§50a-e) deutliche Verbesserungen auf. Insbesondere ist positiv zu erwähnen, dass die ursprünglich geplante generelle Ermächtigung zur Videoüberwachung ("Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht", §50a Abs.3 Z7) gestrichen wurde. Diese Bestimmung hätte *jede denkbare Videoüberwachung* erlaubt, da ein Auftraggeber immer behaupten könnte, er müsse rechtliche Ansprüche vor Gericht geltend machen.

Trotzdem ist die jetzt vorgeschlagene Regelung weiterhin unzureichend. §50a Abs. 2 würde generell eine Videoüberwachung erlauben, die zur "Erfüllung gesetzlicher *oder vergleichbarer rechtlicher Sorgfaltspflichten*" dient. Dies ist eine weitgehend unbestimmte Formulierung, die auch Videoüberwachungen aus selbstgeschaffenen rechtlichen Verpflichtungen erlauben würde.

Ein Videoüberwacher könnte in letzter Konsequenz sich selbst den "rechtlichen " Auftrag geben, sein Eigentum besonders sorgfältig zu schützen, seine Mitarbeiter oder sonstige Dritte vor Unfällen zu schützen usw. und dazu eben Videoüberwachung zu benötigen. Jeder der Videoüberwachung einsetzen möchte, könnte auf Grund dieser Bestimmung seine Sorgfaltspflichten nach Belieben ausdehnen und damit jede Videoüberwachung rechtfertigen.

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.

Es wird daher vorgeschlagen in §50a Abs. 2 den Zusatz "*oder vergleichbarer rechtlicher*" ersatzlos zu streichen.

(9.) Resumee

Entgegen den ambitionierten Ankündigungen im Jahr 2008 kann auch der vorliegende Entwurf nicht als *"großer Wurf"* oder wesentliche Weiterentwicklung der Bürger- und Grundrechte in einer entwickelten Informationsgesellschaft angesehen werden. Trotz Verbesserungen im vorliegenden Entwurf muss auch dieser Gesetzesentwurf als „Entwurf vieler verlorener Chancen“ eingestuft werden.

Der vorliegende Entwurf verzettelt sich in einer Vielzahl kleinlicher bürokratischer Adaptionen (siehe Ausführungen im speziellen Teil dieser Stellungnahme), die offenbar von den Verwaltungs-Interessen der Datenschutzkommission diktiert wurden und weder Vorteile für Datenverarbeiter, noch für Betroffene bringen.

Die wenigen für Betroffene und/oder Auftraggeber positiven Aspekte reichen in Summe nicht aus, um eine Novelle des DSG zum gegenwärtigen Zeitpunkt zu rechtfertigen. Dies umso mehr als Vertreter der Bundesländer schon im Vorfeld angekündigt haben, die für diese Novelle notwendige kompetenzrechtliche Änderung der Bundesverfassung (B-VG Art. 10, 102) blockieren zu wollen und erst im Rahmen einer Gesamt-Bundesstaatsreform zustimmen zu wollen.

Es wird daher dringend empfohlen den vorliegenden Entwurf zurückzunehmen und eine tatsächliche Gesamtnovelle des DSG 2000 vorzubereiten, die sowohl die neuen technischen Entwicklungen berücksichtigt, als auch alte Mängel und EU-vertragswidrige Bestimmungen behebt und wichtige Bereiche, wie betrieblichen Datenschutzbeauftragten, Videoüberwachung und Informationspflichten in einer Weise regelt, die die Grund- und Freiheitsrechte in einer Informationsgesellschaft in zeitgemäßer und rechtlich einwandfreier Form sichert.

Im Rahmen einer umfassenden Reform wird es auch notwendig sein Teile der Gewerbeordnung (etwa im Zusammenhang mit der Tätigkeit von Wirtschaftsauskunftsdiensten), des Telekommunikationsgesetzes (etwa bei der Gleichstellung von Ortungssystemen mit anderen Telekommunikationseinrichtungen), der Zivilprozessordnung (Beweisverwertungsverbote rechtswidrig gesammelter Daten) anzupassen.

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.

Teil I.: Punkte des Entwurfs zur DSG-Novelle 2010 im Detail

(1.) Fehlender betrieblicher Datenschutzbeauftragter

Die Streichung der vorgesehenen Position eines "betrieblichen Datenschutzbeauftragten" im vorliegenden Entwurf ist als datenschutzpolitischer Rückschritt anzusehen.

Es existieren zu dieser Einrichtung auf Ebene anderer europäischer Staaten bereits außerordentlich positive Erfahrungen.

Die Art. 29-Gruppe hat in einem Bericht zur deutschen Datenschutzsituation festgehalten, dass das Prinzip der betrieblichen Selbstkontrolle sehr gut funktioniere. Positiv hervorgehoben wurde in diesem Zusammenhang, dass den Datenschutzbeauftragten in Deutschland geeignete Fachliteratur sowie Aus- und Weiterbildungsmöglichkeiten zur Verfügung stehen. Schließlich wird festgestellt, dass der Datenschutzbeauftragte nach allgemeiner Meinung die Schlüsselrolle bei der „Success Story“ des Datenschutzes in Deutschland gespielt habe. Mit dem Datenschutzbeauftragten sei ein neuer Beruf mit eigener Ausbildung geschaffen worden. Kongresse, Seminare und andere Veranstaltungen böten inzwischen wichtige Plattformen für den Erfahrungsaustausch. Die Art. 29-Gruppe führt abschließend aus, dass die Stärke der deutschen Datenschutz-Community nicht zuletzt durch die Resonanz auf die Konsultation der EU-Kommission zur Umsetzung der EG-Datenschutzrichtlinie belegt sei; danach stammten nahezu 50 % aller Antworten von deutschen Unternehmen oder Einzelpersonen.

Abschließend stellt die Datenschutzgruppe nach Art. 29 im Rahmen ihrer Empfehlungen zum Einsatz von Datenschutzbeauftragten sinngemäß Folgendes fest: *"In Anbetracht der positiven Erfahrungen in den Mitgliedstaaten, in denen Datenschutzbeauftragte eingeführt worden sind bzw. traditionell vorhanden waren, wäre eine breitere Anwendung des Prinzips der betrieblichen Selbstkontrolle durch Datenschutzbeauftragte als Ausnahme von der Meldepflicht nützlich."*

Wesentlich am Institut des Datenschutzbeauftragten auf Betriebsebene sind jedenfalls folgende Voraussetzungen: Unabhängigkeit, geeignete Ausbildung, finanzielle Ausstattung, ausreichende Kompetenzen sowie Verfügung über die nötigen zeitlichen Ressourcen zur Erfüllung der Tätigkeit.

Die ARGE DATEN fordert daher, dass der betriebliche Datenschutzbeauftragte jedenfalls wieder in die Novelle aufgenommen wird.

Diskussionswert ist jedoch die Mitarbeitergrenze, ab dem ein Datenschutzbeauftragter verbindlich vorgeschrieben ist, diese könnte statt mit 20 MA mit 50 MA festgelegt werden.

Alternativ könnte auch die Einführung eines freiwilligen betrieblichen Datenschutzbeauftragten geregelt werden. Als Anreiz für einen unabhängigen Datenschutzbeauftragten sollten Unternehmen, die sich dazu entschließen von den Registrierungspflichten befreit werden. Informationspflichten über die Datenanwendungen sollten dann direkt vom betrieblichen Datenschutzbeauftragten erfüllt werden.

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.) §1 Abs. 2 Erster Satz - Grundrecht auf Datenschutz

Der generelle Ausschluss von Grundrechtsinteressen bei allgemein verfügbaren Daten ist nicht Richtlinienkonform. Stattdessen sollte festgehalten werden, dass auch veröffentlichte Daten nur zu Zwecken verwendet werden dürfen, die mit dem ursprünglichen Veröffentlichungszweck vereinbar sind und Grundrechtsschutz genießen.

(3.) §8 Abs. 2 - Datenverwendung/Einschränkung des Widerspruchsrechts

Der generelle Ausschluß der Verletzung schutzwürdiger Geheimhaltungsinteressen bei "zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten" ist nicht EU-vertragskonform und sollte gestrichen werden.

(4.) §17 Abs. 1a - Registrierung von Datenanwendungen

Positiv ist, dass verpflichtende Verwendung der Bürgerkarte für die Meldung von Datenanwendungen, wie im Entwurf 2008 vorgesehen, entfallen ist. Trotzdem bleibt die neue Regelung unklar. Es sollte festgelegt werden, dass bei einer Internetanwendung zur Meldung von Datenanwendungen jedenfalls *eine Meldemöglichkeit ohne Bürgerkarte vorzusehen ist*. Diese alternative Meldemöglichkeit kann mit einem Benutzeraccount wie Benutzerkennung und Passwort, vergleichbar FinanzOnline, realisiert werden.

Darüber hinaus muss auch weiterhin eine nicht-elektronische Meldung möglich sein. Gerade kleineren Unternehmen oder Einzelpersonen ist nicht zuzumuten, sich für die ganz seltene Meldungen eine Bürgerkarte oder einen Benutzeraccount zuzulegen.

Ansonsten ist zu befürchten, dass die schon bisher nur lückenhaft erfolgten Registrierungen noch weniger beachtet werden und der Sinn eines - unvollständigen - Registers noch mehr in Frage zu stellen ist.

(5.) §§19-22a - Registrierungsverfahren

Das nunmehr vorgeschlagene Registrierungsverfahren mag zwar bürokratische Bedürfnisse des geschäftsführenden Mitglieds der Datenschutzkommission befriedigen, bedeutet jedoch eine generelle Schlechterstellung der Betroffenen.

Aus Sicht des Grundrechtsschutzes sind die geplanten Bestimmungen überaus kritisch zu betrachten. Diese Aufweichung des Vorabkontrollverfahrens entspricht nicht dem Geist der EU-Datenschutzrichtlinie nicht.

Schon aus der Bestimmung des § 16 DSG zum Datenverarbeitungsregister ergibt sich, dass künftig generell keine Rechtmäßigkeitsprüfung der zu registrierenden Datenverarbeitungen stattfinden soll.

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.

Sofern eine Datenverarbeitung der Vorabkontrolle unterliegt oder bei der automationsunterstützten Prüfung „durchgefallen“ ist, gibt es die Möglichkeit der Mangelhaftigkeitsprüfung gemäß § 19 Abs 3 DSG, welche sich allerdings nur auf die Mangelhaftigkeit der Meldung bezieht.

Bei Datenanwendungen, die gemäß § 18 der Vorabkontrolle unterliegen, können zwar weiterhin auf Grund der Ergebnisse des Prüfungsverfahrens dem Auftraggeber Auflagen, Bedingungen oder Befristungen für die Aufnahme der Datenanwendung durch Bescheid erteilt werden, es erscheint allerdings fraglich, wie hinkünftig die Überprüfung, ob es sich um eine vorabkontrollpflichtige Verarbeitung handelt, von statten gehen soll.

Selbes gilt im übrigen auch für die Möglichkeit nach § 30 Abs 6a DSG, sofern durch den Betrieb einer Datenanwendung eine wesentliche Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen vorliegt, die Weiterführung der Datenanwendung mit Bescheid gemäß § 57 Abs. 1 AVG zu untersagen.

Das Grundproblem besteht jedenfalls darin, dass es völlig dem Auftraggeber überlassen wird, ob er eine Datenanwendung als vorabkontrollpflichtig bezeichnet oder nicht, somit ist dem Missbrauch Tür und Tor geöffnet.

Zwar ist nach § 22a DSG ein „Verfahren zur Überprüfung der Erfüllung der Meldepflicht“ vorgesehen, im Zuge dessen registrierte Meldungen von der Datenschutzkommission jederzeit auf Mangelhaftigkeit geprüft werden können, doch ist nicht zu erwarten, dass dieses Verfahren über zufällige Stichproben hinaus Verwendung finden wird.

Die europarechtliche Konformität der geplanten Bestimmung ist daher mehr als fragwürdig: Erwägungsgrund 54 der EU-Datenschutzrichtlinie hält fest, dass die Zahl der Verarbeitungen mit besonderen Risiken sehr beschränkt sein soll und die Mitgliedstaaten für diese Verarbeitungen vorsehen müssen, dass vor ihrer Durchführung eine Vorabprüfung durch die Kontrollstelle oder in Zusammenarbeit mit ihr durch den Datenschutzbeauftragten vorgenommen wird. Als Ergebnis dieser Vorabprüfung kann die Kontrollstelle gemäß einzelstaatlichem Recht eine Stellungnahme abgeben oder die Verarbeitung genehmigen. Diese Prüfung kann auch bei der Ausarbeitung einer gesetzgeberischen Maßnahme des nationalen Parlaments oder einer auf eine solche gesetzgeberische Maßnahme gestützten Maßnahme erfolgen, die die Art der Verarbeitung und geeignete Garantien festlegt.

Auch gemäß Artikel 20 der Richtlinie haben die Mitgliedstaaten festzulegen, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und tragen dafür Sorge, dass diese Verarbeitungen vor ihrem Beginn geprüft werden.

Aufgrund des vorliegenden Gesetzesentwurfs wäre hinsichtlich der von Österreich als vorabkontrollpflichtig festgelegten Verarbeitungen keine Überprüfung mehr garantiert, weshalb der vorliegende Entwurf in dieser Form abzulehnen ist.

Dass hinsichtlich vorabkontrollpflichtiger Verarbeitungen künftig keinerlei Kontrolle der Rechtmäßigkeit stattfinden soll, sowie dass die Frage, ob es überhaupt eine

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.

Vollständigkeits- und Plausibilitätskontrolle gibt alleine in den Händen des Auftraggebers liegt, ist aus datenschutzrechtlicher Sicht nicht tragbar und mit der EU-Datenschutzrichtlinie nicht vereinbar.

Die automatisierte Registrierung ist ein unsinniger Bürokratismus und wird entschieden abgelehnt. Da wäre es schon ehrlicher, auf die Registrierung gänzlich zu verzichten.

(6.) §24 Abs. 2a - Informationspflicht

Die vorgesehene Informationspflicht wird ausdrücklich begrüßt. Gleichzeitig wird angeregt bei Verletzung dieser Informationspflicht einen immateriellen Schadenersatz mit einer Mindesthöhe von 750,- Euro je Betroffenen vorzusehen.

Sowohl im In- als auch Ausland mehren sich die Fälle, dass personenbezogene Daten verloren gehen oder unzulässiger Weise an Dritte weitergegeben werden[1].

Als Datenverlust ist das Abhanden kommen von Daten ohne Kenntnis eines möglichen Empfängers oder Finders zu verstehen[2].

Die Verständigungspflicht sollte jedoch Angaben in Hinblick auf die Daten und die Umstände des Datenverlustes enthalten. Entfallen könnte die Verständigung nur dann, wenn die Betroffenen nicht identifzierbar sind oder nicht erreichbar sind. Auf jeden Fall sollte über den Vorfall selbst die Datenschutzkommission verständigt werden. Diese hat eine öffentliche Liste über derartige Vorfälle zu führen.

(7.) §26 Abs. 7, 8 - Auskunftsrecht

1 In Österreich ist zum Beispiel dokumentiert, dass das Innenministerium CDs über Personen, die einer Sicherheitsüberprüfung unterzogen wurden, verloren hat.
London, Großbritannien. Die Steuerbehörde verliert zwei CDs mit den Daten von 25 Millionen Kindergeldempfängern. Die CD enthält Informationen, wie Namen, Bankdetails, Adressen und Sozialversicherungsnummern (futurzone, ORF, 21.11.2007)
London, Großbritannien, Die britische Regierung gibt zu, dass die Daten von drei Millionen britischen Führerscheinbesitzern im US-Staat Iowa verloren gegangen waren. Das Verkehrsministerium hat weiters 7.500 Fahrzeugdaten verloren (Der Standard, 19.12.2007)
London, Großbritannien, Neun Verwaltungszentren des nationalen Gesundheitssystems haben mehrere hunderttausend Patientendaten verloren (heise online, 23.12.2007)
Stockholm, Schweden, USB-Stick mit Armee-Akten steckte im Computer einer Leihbibliothek, enthalten unter anderem Geheimdienstberichte über den Nato-Einsatz in Afghanistan und das Attentat auf den Außenminister von Sri Lanka (Die Presse, 5.1.2008)

2 Nicht als Datenverlust im Sinne dieses Absatzes ist der Verlust von Daten durch technische Gebrechen zu verstehen, wenn ausgeschlossen werden kann, dass dadurch Daten in die Hände Dritter gelangen können.

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.

Ursprünglich als Schutzbestimmung für den Betroffenen geschaffen existiert im §26 Abs. 7 DSG 2000 ein Löschungsverbot von Daten vier Monate nach Kenntnis eines Auskunftsverlangens. Die Praxis hat jedoch gezeigt, dass dieses Löschungsverbot zu einer Beschränkung der Grundrechte des Betroffenen führte, insbesondere zu einer Beschränkung seiner Löschungsrechte.

Es wird daher vorgeschlagen den Abs. 7 dahingehend zu verbessern, dass das Löschungsverbot von vier Monaten dann nicht wirksam ist, wenn der Betroffene eine Löschung von Daten verlangt, kein Beschwerdeverfahren vor der Datenschutzkommission vorliegt und die rechtlichen Bedingungen zur Löschung, insbesondere §27 oder §28 DSG 2000 erfüllt sind.

Der geplante § 26 Abs 8 DSG legt fest, dass in dem Umfang, in dem eine Datenanwendung für eine natürliche Person hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, diese das Recht auf Auskunft nur nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen hat.

Bei der vorgesehenen Bestimmung soll sich demnach der Anwendungsbereich der auch in der aktuellen Gesetzeslage bestehenden Regelung von „öffentlich einsehbaren“ auf für den Betroffenen von Gesetzes wegen einsehbare Anwendungen ändern.

Grundsätzlich ist festzuhalten, dass die Regelung des § 26 Abs 8 DSG 2000 schon in der bestehenden Form deshalb zu kritisieren ist, weil sie zur Einschränkung der Parteienrechte führt. Die jeweiligen Verfahren zur Einsichtnahme - etwa bei Grund- und Firmenbuch, aber auch im Melderegister, welche schon bisher nicht nach § 26 DSG beauskunftet wurden - sind für Betroffene mit Mühen und auch Kosten verbunden die ein datenschutzrechtliches Auskunftsbegehren in der Regel nicht mit sich bringt. Dies gilt auch für Einsichtnahmen im Rahmen des allgemeinen Verwaltungsrechts.

Die entsprechende Gesetzesbestimmung führte bisher zum absurden Resultat, dass dort, wo personenbezogene Daten öffentlich gemacht wurden, die Auskunftsmöglichkeit des Betroffenen eingeschränkt war, indem diesem zusätzliche Anstrengungen zur Geltendmachung seiner Rechte aufgebürdet werden, die er bei sonstigen Datenverarbeitungen nicht hätte.

Diese Bestimmung widerspricht auch Art. 12 der EU-Datenschutz-Richtlinie, der die Ausübung des Auskunftsrechts als „frei und ungehindert“, „ohne zumutbare Verzögerung“ sowie „ohne übermäßige Kosten“ definiert. Durch eine Ausweitung der Bestimmung auf alle Arten von „einsehbaren“ Daten werden Parteienrechte weiter beschränkt. Diese geplante Änderung is abzulehnen.

Weiters ist der in den „Erläuternden Bemerkungen“ festgehaltenen Rechtsauffassung, die davon ausgeht, dass bei teilweise öffentlichen Registern grundsätzlich kein Anspruch auf Auskunft über konkrete Empfänger bestünde, so nicht zu folgen.

(8.) §31 Abs. 3 und folgende, §31a - Beschwerdeverfahren

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.

Durch die vorgesehenen Bestimmungen des § 31 Abs 3ff DSG wird das Verfahren zur Beschwerde vor der Datenschutzkommission in unnötiger Weise formalisiert.

Entsprechend der vorgesehenen Bestimmung haben Beschwerden künftig jedenfalls zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),
3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

Weiters sind Beschwerden künftig das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen.

Die Bestimmungen sind geeignet, Bürgern, die keine Datenschutz- und Verwaltungsexperten sind, das Beschwerderecht zu erschweren. Darüber hinaus sind die Bestimmungen in sich widersprüchlich, besteht doch im DSG §26 ausdrücklich auch die Möglichkeit mündlicher Auskunftsersuchen. Damit würden derartige Auskunftsverfahren automatisch vom Beschwerderecht ausgeschlossen.

Gemäß § 13 AVG soll die Datenschutzkommission künftig ermächtigt sein, Eingaben, welche die genannten Voraussetzungen nicht erfüllen, nach fruchtloser Erteilung eines Verbesserungsauftrages zurückzuweisen.

Die geplanten Bestimmungen, welche selbst in den „Erläuternden Bemerkungen“ als Formalisierung bezeichnet werden, bringen hinsichtlich der Wahrung von Betroffenenrechten eine erhebliche Verschlechterung mit sich. Gerade das Verfahren vor der Datenschutzkommission hat sich bislang dadurch ausgezeichnet, dass es auch durch nicht fachkundige Bürger ohne einen rechtlichen Beistand in Anspruch genommen werden konnte.

Damit widerspricht der Entwurf der Idee der EU-Datenschutzrichtlinie, welche in Art. 28 Abs 4 festhält, dass jede Person sich zum Schutz der betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden können muss. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

Dass Verfahren auch verfahrensrechtliche Vorschriften habe, sei nicht bestritten. Aus dem Wortlaut der Datenschutzrichtlinie geht aber eindeutig hervor, dass die Möglichkeit, bei der nationalen datenschutzrechtlichen Kontrollstelle Eingaben machen zu können, gesichert sein muss. Von formellen Beschränkungen ist nicht die Rede.

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.

Es ist nicht einsichtig, welcher Sinn hinter der Formalisierung stehen soll. Bislang ist es der Datenschutzkommission auch gelungen, Beschwerden zu behandeln, die nicht über die nunmehr genannten formalen Voraussetzungen verfügten.

Falls das Interesse dahin gehen sollte, die DSK, zu entlasten, sei darauf verwiesen, dass – durch notwendige Erlassung formal begründeter Verbesserungsaufträge - auf die DSK möglicherweise sogar mehr Arbeitsaufwand zukommen könnte als bisher.

Die Bestimmungen sind jedenfalls als unnötige und bürgerfeindliche Formalisierungen abzulehnen. Sofern es Probleme in der administrativen Abwicklung von Beschwerden gibt, sind diese über die Geschäftsordnung der Datenschutzkommission zu beseitigen.

(9.) §32 Abs.4 - Zuständigkeit der Gerichte

Begrüßenswert ist, dass das Problem der unklaren Regelung der Gerichtszuständigkeit, insbesondere im Zusammenhang mit Anträge zu einstweiligen Verfügungen erkannt wurde und ein Sanierungsversuch unternommen wurde. In der Vergangenheit gab es einige Klagsabweisungen durch Gerichte und damit Verfahrensverzögerungen für den Betroffenen.

Die in Abs. 4 gewählte Formulierung "*Klagen (Anträge)* können aber auch beim Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder Niederlasung hat." ist jedoch unbefriedigend. Diese Formulierung lässt weiter offen auf welche Art von Anträge sie sich bezieht.

Vorgeschlagen wird folgende Formulierung "*Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz* können auch beim Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder Niederlassung hat."

Damit wird zweifelsfrei die Zuständigkeit des Landesgerichtes auch für einstweilige Verfügungen festgehalten.

(10.) §36 Abs3a - Berufstätigkeit der Mitglieder der Datenschutzkommission

Überaus problematisch ist die neue Bestimmung zu sehen, in der ausdrücklich die Tätigkeit der Datenschutzkommission als Nebentätigkeit definiert ist.

Damit wird keinesfalls die Unabhängigkeit der Datenschutzkommission verbessert, ganz im Gegenteil, werden mögliche Interessenskonflikte mit der Haupttätigkeit geradezu in Gesetzesrang erhoben.

Zu fordern ist, dass die Mitglieder der Datenschutzkommission hauptberuflich für diese Tätigkeit abzustellen sind, eine entsprechende Qualifikation aufweisen und damit wesentlich intensiver und direkter die von der Datenschutzrichtlinie geforderten Überwachungsaufgaben wahrnehmen. Die bisherige Praxis weniger jährlicher

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.

Zusammenkünfte in denen die von Sachbearbeitern und dem "geschäftsführenden Mitglied" erstellten Entscheidungen unter hohem Zeitdruck abgenickt werden, sollte saniert werden.

Die Kommissionsmitglieder sollten durchgehend als Ansprechstelle für Bürgeranliegen verfügbar sein.

(11.) §38 Abs. 2 - Informationsrecht des Bundeskanzlers

Als neue Bestimmung ist vorgesehen, dass der Bundeskanzler das Recht hat sich jederzeit "über alle Gegenstände der Geschäftsführung der Datenschutzkommission" zu unterrichten.

Ein Informationsrecht wird üblicherweise nur Aufsichtsstellen und vorgesetzten Dienststellen eingeräumt. Berichts- bzw. Informationspflicht gelten generell als Hinweis auf ein Abhängigkeitsverhältnis. Diese neue Bestimmung bedeutet eine weitere Beschränkung der Unabhängigkeit der Datenschutzkommission und ist abzulehnen.

Diese Bestimmung verletzt die von der Datenschuztrichtline geforderte völlige Unabhängigkeit der Aufsichtstelle. Der Abschnitt zur Organisation der Datenschutzkommission bedarf einer völligen Neuordnung und wird wohl ohne Anpassungen der Bundesverfassung nicht die von der EU geforderte völlige Unabhängigkeit ermöglichen.

(12.) §46 - Wissenschaftliche Forschung und Statistik

Die neuen Bestimmungen enthalten einige Systembrüche und Inkonsistenzen. In Abs.1 Z2 und Z3 wird nunmehr von der Bindung der Datenverwendung an den Auftraggeberbegriff abgewichen. Nunmehr soll ein Auftraggeber auch dann Daten verwenden dürfen wenn "2. er [Daten] für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat".

Im Ergebnis bedeutet diese - neue und missglückte - Formulierung, dass ein Auftraggeber in Zukunft auch Daten für wissenschaftliche Forschung und Statistik verwenden dürfte, die er bloß als Dienstleister für Dritte ermittelt hat. Dies ist insbesondere bei sensiblen Daten, wie den Gesundheitsdaten ein Problem. Erlaubt doch diese Bestimmung die Verwertung von Gesundheitsdaten durch Dritte, wie Labors, Gutachter usw. die diese Daten nur als Dienstleister zur Erstellung eines bestimmten - anderen - Werkes erhalten haben.

Mit dieser Bestimmung wäre auch die beliebige Datenverwertung zu Zwecken von "Wissenschaftlicher Forschung und Statistik", zu denen auch Marktforschung zählt, durch Betreiber von Callcentern möglich. Diese hätten dann in Zukunft das Recht die Daten ihrer Kunden ohne weitere Einwilligung auszuwerten und zu verwerten.

Gerade die Vorkommnisse der letzten zwei Jahre in Deutschland zeigten, dass Callcenter eine Schlüsselrolle bei Datenschutzverletzungen spielen. Statt die Aufsichtspflichten zu

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.

verschärfen und die Datenverwendungsmöglichkeiten dieser Art von Dienstleistern einzuschränken, werden sie in diesem Entwurf ausgeweitet.

Eine analoge problematische Bestimmung wurde in Z3 formuliert.

Diese Ausdehnung der Datenverwendung auch auf jene Daten, die nur im Rahmen einer Dienstleistereigenschaft ermittelt wurden, ist abzulehnen.

Der neue Abs. 3a verwendet - völlig systemfremd und inkonsistent - den Begriff des *"Eigentümers der Datenbestände"*.

Wesentliches Kennzeichen der Datenschutzrichtlinie und des DSG 2000 ist, dass es keine Eigentümerschaft an personenbezogene Daten kennt. Persönliche Daten dürfen nur für *bestimmte Zwecke verwendet* werden. Es gibt kein Szenario im DSG 2000 in dem Personendaten in das Eigentum irgendeines Auftraggebers übergehen können.

Dieser Absatz sollte entweder ersatzlos gestrichen oder richtlinienkonform neu formuliert werden.

(13.) §§50a und folgende - Videoüberwachung

Die jetzt vorgeschlagene Regelung ist weiterhin unzureichend. §50a Abs. 2 würde generell eine Videoüberwachung erlauben, die zur "Erfüllung gesetzlicher *oder vergleichbarer rechtlicher Sorgfaltspflichten*" dient. Dies ist eine weitgehend unbestimmte Formulierung, die auch Videoüberwachungen aus selbstgeschaffenen rechtlichen Verpflichtungen erlauben würde.

Ein Videoüberwacher könnte in letzter Konsequenz sich selbst den "rechtlichen " Auftrag geben, sein Eigentum zu schützen, seine Mitarbeiter oder sonstige Dritte vor Unfällen zu schützen und dazu eben Videoüberwachung zu benötigen. Jeder der Videoüberwachung einsetzen möchte, könnte auf Grund dieser Bestimmung seine Sorgfaltspflichten nach Belieben ausdehnen und damit jede Videoüberwachung rechtfertigen.

Es wird daher vorgeschlagen in §50a Abs. 2 den Zusatz "*oder vergleichbarer rechtlicher*" ersatzlos zu streichen.

§50a Abs. 3 Z1 enthält eine vermeidbare Ungenauigkeit. Videoüberwachung soll zulässig sein, wenn "diese im lebenswichtigen Interesse *einer Person* erfolgt". Dies ist im Ergebnis eine unbestimmte Formulierung, da unter diesem Titel beliebige Dritte mit Hinweis darauf überwacht werden könnten, es wäre im lebenswichtigen Interesse irgendeiner anderer Person.

Soll diese Bestimmung auf Einrichtungen im Rahmen von Intensivstationen und vergleichbaren Gesundheitseinrichtungen abstellen, dann würde es genügen auf "diese im lebenswichtigen Interesse *seiner Person und der betreuenden Person*" einzuschränken. Sind andere Szenarien gedacht, sollten diese präzise formuliert werden.

In §50a Abs. 5 ist der "höchstpersönliche Lebensbereich" insoweit unklar definiert, da nicht nur die in den Erläuternden Bemerkungen angesprochenen Bereiche der eigenen

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.

Wohnung oder WC- und Umkleidekabinen darunter fallen können, sondern auch Umkleideräumlichkeiten die von mehreren Personen benutzt werden können, aber auch FKK-Bereiche, Saunaanlagen und Einrichtungen, die zur Befriedigung verschiedener sexueller Neigungen dienen (etwa sog. Swinger-Klubs). Generell empfinden Personen es nicht als Eingriff in ihre Privatsphäre sich etwa unter gleichgesinnten oder gleichgeschlechtlichen Personen entblößt zu bewegen, sehr wohl jedoch wenn ihr Verhalten aufgezeichnet, beobachtet oder einer unbekannten Zahl von Personen zugänglich gemacht werden kann.

Es ist daher notwendig den "höchstpersönlichen Lebensbereich" gesetzlich so zu definieren, dass alle Bereiche in denen Personen sich - zu welchen Zwecken auch immer - entblößen vor Videoüberwachung geschützt sind.

Weiters sollte eine Überwachung "höchstpersönlicher Lebensbereiche" auch nicht durch Vorliegen von Abs.3 Z3 ("Zustimmung durch den Betroffenen") möglich sein. Eine Zustimmungsmöglichkeit zur Videoüberwachung "höchstpersönlicher Lebensbereiche" würde im Ergebnis dazu führen, dass Betreiber von Schwimmbädern, sonstiger Sportstätten mit Umkleideeinrichtungen, einschlägiger (Sex-)Einrichtungen, sogar von Kaufhäusern usw. durch Aufnahme derartiger Zustimmungserklärungen in AGBs, "Hausordnungen" oder Anschlag bei Eingängen oder Kassen eine derartige Zustimmung erreichen und damit den Persönlichkeitsschutz systematisch unterlaufen.

Die Notwendigkeit der Videoüberwachung "höchstpersönlicher Lebensbereiche" ist generell auszuschließen, da alle Orte "höchstpersönlicher Lebensbereiche" von Orten mit gefährlichen Angriffen auf Eigentum oder Personen getrennt werden können.

Beispielhaft sei nur erwähnt, dass die Aufbewahrung von Wertsachen, die regelmäßig Ziel von Einbrüchen in Schwimmbädern und ähnlichen Einrichtungen sind, leicht von den eigentlichen Umkleidebereichen zu trennen sind.

Als weiteres Beispiel sei darauf hingewiesen, dass statt eine Sauna selbst zu überwachen ausreichender Schutz gegeben ist, wenn - sofern Notwendigkeit besteht - der Zugang dazu, der in der Regel bekleidet/bedeckt erfolgt, überwacht wird.

Ausdrücklich begrüßt wird das Verbot der Viedeoüberwachung zur Mitarbeiterkontrolle (§50a Abs. 5).

(14.) §50c Abs. 2 Z2 - Registrierungspflicht

Die Ausnahme der Registrierungspflicht von Aufzeichnungen auf analogen Speichermedien ist sachlich nicht begründet.

Abgesehen davon, dass analoge Speichermedien zunehmend an Bedeutung verlieren, bedeutet eine Analogaufzeichnung nicht, dass eine digitale Weiterverarbeitung nicht möglich wäre.

Analoge Aufzeichnungen können heute ohne nennenswerten Qualitätsverlust, automatisiert und rasch digitalisiert werden. Das Umkopieren wäre zwar eine neue

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.

Datenermittlung, aber keine neue Videoüberwachung. Diese Unterscheidung ist jedoch nur für (Rechts-)Experten verständlich und nicht praktikabel. Im Ergebnis käme kein Auftraggeber auf die Idee den Umkopiervorgang als neue Datenanwendung zu registrieren. Eine digitale Auswertung ursprünglich analoger Aufzeichnungen wäre damit im Regelfall nicht registriert und daher nicht kontrollierbar.

Darüber hinaus ist diese rein technische Unterscheidung zwischen Analogaufnahme und Digitalaufnahme richtlinienwidrig. Die Datenschutzrichtlinie kennt keine derartige Unterscheidung.

Es wird daher empfohlen §50c Abs. 2 Z2 ersatzlos zu streichen.

(15.) §50d - Kennzeichnungspflicht

Die Kennzeichnungspflicht ist unzureichend geregelt. Kennzeichnungspflichtige Videoüberwachungsanlagen sollten in gut lesbarer Schrift auch die Registrierungsnummer/Bescheidnummer der Datenschutzkommission enthalten. Nur auf diese Weise ist es Betroffenen ohne unzumutbaren Aufwand möglich, rasch und einfach genehmigte Videoüberwachungen von "wilden", rechtswidrigen Anlagen zu unterscheiden.

(16.) §50e Abs2 - Auskunftsumfang

Die Beschränkung des Auskunftsumfangs auf eine "schriftliche Beschreibung" ist nicht Richtlinienkonform und wird daher abgelehnt.

Wie das Beispiel Großbritannien zeigt, ist es Auftraggebern zuzumuten in allen Fällen im Auskunftsfall das entsprechende Videomaterial auszuhändigen. Soweit Dritte erkennbar sind, können diese durch entsprechendes "Auspixeln" anonymisiert werden. Diesbezügliche Software ist mittlerweile sehr kostengünstig bis gratis über Internetanbieter verfügbar.

Die Einschränkung der Auskunftspflicht auf "schriftliche Beschreibung" soll daher gestrichen werden.

(17.) §52 - Anhebung der Verwaltungsstrafbestimmungen

Grundsätzlich wird die Anhebung der Strafsätze begrüßt. Die Erhöhung auf 25.000,- Euro bzw. 10.000,- Euro erscheint jedoch unzureichend. Einerseits sind diese Sätze weit hinter dem EU-weiten Durchschnitt, andererseits sind diese Sätze weit unter vergleichbaren Strafsätzen im Zusammenhang mit gewerblichen Verwaltungsstrafbestimmungen.

Es sei nur auf die Strafbestimmungen zu §107 TKG 2003 verwiesen. Für das bloße Versenden eines unerwünschten Mails (sog. "Spam-Mail") kann eine Verwaltungsstrafe bis 37.000,- Euro verhängt werden. Nun mag ein Spammail eine Belästigung darstellen, die durch Auftraggeber verursachbaren Eingriffe und Verletzungen der Privatsphäre,

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.

insbesondere durch rechtswidrige Datenübermittlungen oder Veröffentlichungen sind jedenfalls als wesentlich weitreichender zu bewerten.

Geringe Strafbestimmungen signalisieren den Auftraggebern eine Geringschätzung des Schutzes der Privatsphäre durch den Gesetzgeber und ermutigen ihn geradezu Datenschutzbestimmungen nicht allzu ernst zu nehmen.

Eine Anpassung der Verwaltungsstrafen auf das Niveau des TKG 2003, also auf 37.000,- Euro ist gerechtfertigt. Die Differenzierung in zwei unterschiedlich hohe Strafobergrenzen ist sachlich nicht gerechtfertigt und sollte entfallen.

Die Verwaltungsbehörden haben sowieso die Möglichkeit durch Bemessung der konkreten Strafhöhe auf die unterschiedliche Intensität einer Privatsphäreverletzung Rücksicht zu nehmen. Und eine vorsätzlich begangene, wiederkehrende Verletzung von Sicherheitsbestimmungen durch einen großen Datenverarbeiter, insbesondere wenn er sensible Daten verarbeitet, wie es Krankenanstalten sind, ist als zumindest genauso schwerwiegend einzustufen, wie eine möglicherweise einmalige rechtswidrige Veröffentlichung der Mitgliedernamen eines Tennisklubs.

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.

Teil II.: Mängel, Fehler und EU-Widrigkeiten des bisherigen DSG 2000 die nicht behoben wurden

(1.) Weiterhin kein Schutz für "allgemein" verfügbare Daten

Das nur im österreichischen DSG verwendete Prinzip, dass „allgemein verfügbare“ Daten grundsätzlich keinem Schutz zugänglich sein sollen, wird durch die vorliegende Novelle fortgeführt.

Festzuhalten ist dazu, dass die europarechtlichen Grundlagen diese Ausnahme nicht kennen: Ausdrücklich finden die Prinzipien der EU-Datenschutz-RL nach Art. 1 nämlich grundsätzlich auf alle personenbezogenen Daten Anwendung. Auch Art. 2, welcher Ausnahmen von diesem Prinzip festlegt, nimmt auf die allgemeine Verfügbarkeit von Daten keinerlei Bezug. Ausnahmen finden sich lediglich zu einzelnen Regelungsbereichen, wie etwa bei der Registrierung.

Eine Gesetzesdefinition, was unter „allgemeiner Verfügbarkeit“ zu verstehen ist, liegt überdies nicht vor. Sofern dabei jegliche Form allgemeiner Zugänglichkeit gemeint sein soll, ist diese Einschränkung jedenfalls abzulehnen. Es kann nicht so sein, dass die Tatsache, dass personenbezogene Daten an irgend einer Stelle für die Allgemeinheit zugänglich sind, schon dazu führt, dass damit entgegen jeder datenschutzrechtlichen Einschränkung verfahren werden darf. Zu verweisen ist dabei insbesondere darauf, dass es eben verschiedene Formen der Zugänglichmachung gibt und die Tatsache, dass personenbezogene Daten an irgendeiner Stelle zugänglich sind, nicht rechtfertigen kann, dass diese – mangels Geheimhaltungsanspruch - inflationär weiter verbreitet werden dürfen.

Besondere Bedeutung gewinnt der Schutz einmal veröffentlichter Daten insbesondere in Hinblick auf die Gepflogenheiten des Internets. Hier existieren eine Fülle von Foren und Publikationsmöglichkeiten, in denen Menschen zu einem Thema ihre Meinung abgeben oder Informationen aus ihrem Privatleben für einen definierten Freundes- oder Bekanntenkreis veröffentlichen. Auch wenn diese Informationen theoretisch von vielen Menschen abgerufen werden können, wenden sie sich ausdrücklich an einen eng umgrenzten Personenkreis und erlauben deren Verwendung nur für bestimmte Zwecke. So existieren viele medizinische Selbsthilfegruppen, in denen sehr offen über gesundheitliche Probleme diskutiert wird. Diese Informationen sind aber nicht dafür vorgesehen, dass Arbeitgeber oder Versicherungen mit technischen Mitteln das Internet nach Informationen von Bewerbern oder Versicherungsnehmern absuchen.

Ein modernes Datenschutzrecht muss sicherstellen, dass Informationen nur im Umfang ihres ursprünglichen Zweckes verwendet werden dürfen. Ansonsten wären Betroffene in ihren persönlichen Grundrechten schlechter gestellt als Urheber in ihren wirtschaftlichen Interessen. Bei Urhebern führt keine Veröffentlichung eines Werkes zum Verlust aller Verwertungsrechte.

Vorgeschlagen wird daher eine Änderung des §1 DSG, die sicher stellt, dass veröffentlichte Daten nur in dem mit dem ursprünglichen Veröffentlichungszweck vereinbaren Umfang verwendet werden dürfen.

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.

Dass personenbezogene Daten infolge „allgemeiner Verfügbarkeit“ aus dem Schutzbereich des DSG gänzlich ausscheiden, ist EU-widrig und gegenüber Betroffenen als überaus bedenklich abzulehnen. Hier hätte eine DSG-Novelle, die den Namen verdient, dringenden Sanierungsbedarf.

Zusätzlich wird angeregt, dass die Verwendung von Daten in einem widmungsfremden Zusammenhang, etwa ein im Internet veröffentlichtes privates Partyfoto für die Beurteilung eines Stellenbewerbers, als Diskriminierung, vergleichbar einer Diskriminierung auf Grund religiöser oder sexueller Orientierung, sanktioniert wird.

(2.) Notwendigkeit spezifischer Regeln für Onlinedienste

Nicht mehr zeitgemäß sind die Datenschutzbestimmungen in Hinblick auf Online-Dienste.

Auf die Notwendigkeit einer Neudefinition der Datenschuzrechte im Rahmen veröffentlichter Daten wurde schon im obigen Absatz verwiesen. Gerade bei Onlinediensten, die nur für eine spezialisierte Gruppe, etwa eine Selbsthilfegruppe vorgesehen sind, sollte der Begriff einer lokalen oder beschränkten Öffentlichkeit definiert werden.

Auch die Rollenverteilungen (Betroffener/Auftraggeber/Dienstleister) sind bei Onlinediensten, etwa im Rahmen eines Weblogs, einer Social-Network-Seite oder eines Forums nicht mehr in ausreichender Klarheit anwendbar und bedürfen zeitgemäßer Ergänzungen.

Ein weiteres Problem stellt die Anwendbarkeit des Datenschutzrechts bei Onlinediensten dar. Immer mehr international agierende Anbieter verlegen den formalen Betreibersitz in ein datenschutzfreundliches EU-Land, zumindest aber in ein Land, dem gegenüber auf Grund von Sprach- und Rechtsunterschieden die Durchsetzung der Betroffenenrechte erschwert wird. Ein österreichischer Benutzer, der einen eBay-Account nutzt, schließt einen Vertrag mit eBay-Luxemburg ab, obwohl eBay unter ebay.at als "österreichisches" Unternehmen auftritt!

Für die Konsumenten gelten zwar nach wie vor österreichische Konsumentenschutzbestimmungen, für die Durchsetzung der Datenschutzrechte gilt damit jedoch luxemburgisches Recht! Für diese Fälle wäre vorzusehen, dass bei Bestehen einer nationalen Niederlassung Datenschutzrechte bei der nationalen Niederlassung nach nationalem Recht geltend zu machen sind.

(3.) Weiterhin keine Unabhängigkeit der Datenschutzkommission/DSK

Seit mehreren Jahren läuft wegen der fehlenden Unabhängigkeit der DSK ein EU-Vertragsverletzungsverfahren gegen die Republik Österreich. Es wird zwar formal im DSG die Unabhängigkeit der Datenschutzkommission postuliert, diese Unabhängigkeit wird jedoch sachlich in vielen Bereichen aufgehoben.

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.

Diese Unabhängigkeit ist aus mehreren Gründen nicht gegeben:

-) Die organisatorische Eingliederung der Datenschutzkommission nebst Geschäftsstelle und Personal in die Behörde Bundeskanzleramt sowie die Stellung des "Bundesbeamten als geschäftsführendes Mitglied" sind mit Art. 22 der EU-Datenschutzrichtlinie unvereinbar

-) Die Datenschutzkommission ist beim Bundeskanzleramt eingerichtet und hängt in zentralen organisatorischen, wirtschaftlichen und administrativen Punkten vom Wohlwollen des Bundeskanzlers ab. Kern ist die fehlende Budgethoheit, die letztlich die Datenschutzkommission völlig abhängig vom politischen Wohlverhalten gegenüber dem Bundeskanzler macht.

-) Die mangelnde budgetäre Ausstattung und der fehlende Wille des Gesetzgebers eine tatsächlich unabhängig arbeitende Datenschutz-Aufsichtsstelle zu haben, manifestiert sich in geradezu skandalöser Weise in der geringen personellen Ausstattung des "Geschäftsapparates". Formal sind zwar zwanzig Mitarbeiter angestellt, diese sind jedoch zum überwiegenden Teil in der reinen Ablage der Datenverarbeitungsregistrierungen "geparkt". Selbst diese geschönte Zahl liegt nicht einmal bei der Hälfte des EU-Schnitts (45 Mitarbeiter), zieht man die Gruppe der 11 vergleichbar großen Staaten[3] heran, dann liegt Österreich an vorletzter Stelle.

-) Die befristete Bestellung von Behördenmitgliedern ist dadurch, dass diese nach Ablauf ihrer Amtszeit wieder zur Behörde zurückkehren zu müssen, unvereinbar mit den Unabhängigkeitsgarantien.

-) Auch personell ist keine Unabhängigkeit gegeben. Durch die Entsendung von Interessensvertretern, eine typisch „österreichische Lösung“ wird die Einflussnahme von Außen geradezu institutionalisiert. Interessensvertretungen sind - wie der Name schon sagt - dazu da, die Interessen ihrer Klientel zu vertreten, als Garanten für die Unabhängigkeit einer Behörde taugen sie nicht.

-) Zudem wäre wünschenswert, dass - wie in anderen europäischen Ländern - auch an die persönlichen Anforderungen der Mitglieder Ansprüche gestellt werden, etwa hinsichtlich Ausbildung sowie Erfahrungen in den informationstechnischen und datenschutzrechtlichen Bereichen. Bloß allgemein juristische Kenntnisse, wie sie jetzt genügen, sind sicher nicht ausreichend.

Eine DSG-Novelle sollte jedenfalls eine unabhängige Behörde mit eigenem Budget, ohne Interessensvertreter und zumindest mit einer personellen Ausstattung im Umfang des EU-Schnittes. Für die Mitglieder sollten jedenfalls strenge Unvereinbarkeitsbestimmungen gelten.

3 EU-Länder zwischen 5-10 Millionen Einwohner: FINNLAND, DÄNEMARK, SLOWAKEI, ÖSTERREICH, SCHWEDEN, GRIECHENLAND, UNGARN, TSCHECHISCHE REPUBLIK, BELGIEN, PORTUGAL, BULGARIEN

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.

(4.) Nicht abgeschafft - Österreich-Unikum "indirekt personenbezogene Daten"

Neben dem EU-widrigen Ausschluss der "allgemein verfügbaren Daten" von Grundrechten kennt das österreichische DSG auch EU-widrige Ausnahmen bei "indirekt personenbezogenen Daten". Diesen Begriff gibt es nach der EU-Richtlinie Datenschutz gar nicht, ein österreichisches Kuriosum, welches entgegen der europäischen Rahmenbedingungen reihenweise Daten von fundamentalen datenschutzrechtlichen Grundsätzen ausschließt.

Statt jedoch dieses Datenschutzproblem endlich in einer Novelle zu beseitigen, bleibt es unverändert bestehen.

Als indirekt personenbezogene Daten bezeichnet der österreichische Gesetzgeber jene Daten, bei denen der Auftraggeber einer Datenanwendung die Identität einer betroffenen Person mit rechtlich zulässigen Mitteln nicht feststellen kann. Beispiele für indirekt personenbezogene Daten sind etwa die Sozialversicherungsnummer einer Person, das Kennzeichen eines KFZ, die Matrikelnummer eines Studenten oder jene Weblog-Files mit IP-Adresse, die entstehen, wenn die Zugriffe auf Webserver protokolliert werden.

Nach DSG 2000 ist die Verwendung von indirekt personenbezogenen Daten – auch sensiblen Daten - ohne Einwilligung des Betroffenen zulässig.

Sensible Daten, welche die rassische und ethnische Herkunft von Personen, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben betreffen dürfen nach geltender Gesetzeslage auch verwendet werden, wenn die betroffene Person dieser Verwendung nicht zugestimmt hat, sofern sie nur in indirekt personenbezogener Form vorliegen.

Das bedeutet beispielsweise, dass ohne Zustimmung der Betroffenen Datenanwendungen betrieben werden dürfen, die gesundheitliche Informationen über bestimmte Personen mit deren Sozialversicherungsnummer verknüpfen, solange die konkrete Person selbst für den Auftraggeber nicht identifiziert ist.

Die laut Datenschutzgesetz 2000 den Betroffenen einer Datenanwendung zugesicherten Rechte stehen in Bezug auf Anwendungen mit ausschließlich indirekt personenbezogenen Daten nicht zu. Dazu gehören das Recht auf inhaltliche Auskunft über eine Datenanwendung, das Recht auf Richtigstellung und Löschung bei unrichtigem Inhalt oder unzulässiger Datenverarbeitung sowie das Recht auf Widerspruch bei Verletzung schutzwürdiger Geheimhaltungsinteressen des Betroffenen.

Im Gegensatz dazu betont die Richtlinie, dass auch jene Daten personenbezogen sind, die einer Person „nur indirekt zugeordnet werden können“. Bei der Frage, ob eine Person aufgrund bestimmter Daten ermittelbar ist, sollen nach den Erwägungsgründen der Richtlinie sämtliche Mittel berücksichtigt werden, die vernünftigerweise durch den Datenverarbeiter oder einen Dritten eingesetzt werden können, um die jeweilige Person zu ermitteln.

Keine Anwendung soll die Richtlinie nur auf Daten finden, die derart anonymisiert sind, dass sich die entsprechende Person überhaupt nicht mehr ermitteln lässt. Eine

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.

Unterscheidung danach, ob die Ermittlung einer Person aufgrund vorhandener Daten nur mit rechtswidrigen Mitteln möglich ist oder nicht, enthält die Datenschutzrichtlinie nicht.

Europarechtlich ist es somit nicht vereinbar, diese Gruppe von personenbezogenen Daten pauschal aus den wichtigsten Grundsätzen des Datenschutzes auszunehmen. Die österreichische Rechtslage widerspricht hier einmal mehr grundlegend dem Geist der europäischen Datenschutzrichtlinie.

In seiner Entscheidung zur „section-control" hat sich auch der VfGH klar gegen den Begriff des „indirekt personenbezogenen Datums" gestellt.

Dass der vorliegende Entwurf in diesem Bereich keinerlei Anstrengungen unternimmt, ein europaweit einmaliges Kuriosum, welches auf Kosten der Betroffenrechte geht, endlich zu entsorgen, stellt sicherlich eines der gravierendsten Versäumnisse des Entwurfs dar.

(5.) Entscheidungen der Datenschutzkommission gegenüber Behörden nicht durchsetzbar

Wie wenig der Gesetzgeber an wirksamem Datenschutz und einer unabhängigen Behörde interessiert ist, zeigen die fehlenden Sanktionsmöglichkeiten gegenüber öffentlich-rechtlichen Einrichtungen.

Gegenüber Auftraggebern des öffentlichen Rechts sind Verletzungen der Bestimmungen des DSG 2000 nach § 40 Abs 4 DSG 2000 durch die Datenschutzkommission nur festzustellen.

In zahllosen Verfahren wurden in der Vergangenheit Datenschutzverletzungen von Behörden, Körperschaften und Ministerien (zuletzt Finanzministerium) festgestellt. Wenn sich jedoch die Behörde weigerte den datenschutzkonformen Zustand wieder herzustellen, dann gab es für die Bürger keine Durchsetzungsmöglichkeit.

Die Datenschutzkommission erklärte sich bisher als unzuständig, der VwGH, der in der DSK nur eine Verwaltungseinrichtung und nicht eine unabhängige gerichtsähnliche Einrichtung sieht, bestätigte in der Vergangenheit diese Position. Dieser entschied bereits in *2005/06/0366*, dass gegenüber Auftraggebern des öffentlichen Rechts im Falle von Verletzungen gegen das Datenschutzgesetz kein durchsetzbarer Leistungsauftrag erwirkt werden kann. Bei entsprechenden Entscheidungen handelt es sich bloß um Feststellungsbescheide, welche nicht exekutierbar sind.

Betroffene können daher nach österreichischer Rechtslage zwar Verletzungen datenschutzrechtlicher Bestimmungen durch Auftraggeber öffentlichen Rechts feststellen lassen, durchsetzbar sind daraus resultierende Ansprüche nicht.

Diese Rechtslage ist offensichtlich EU-widrig. Art. 12 der Richtlinie 95/46/EG verankert das datenschutzrechtliche Auskunftsrecht. Art. 24 der Richtlinie 95/46/EG verpflichtet die Mitgliedstaaten dazu, geeignete Maßnahmen zu ergreifen, um die volle Anwendung der Bestimmungen der Richtlinie sicherzustellen und Sanktionen festzusetzen, die bei Verstößen gegen die Umsetzung der erlassenen Vorschriften anzuwenden sind.

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.

Entsprechend der Richtlinie 95/46/EG besteht somit nicht nur die Verpflichtung, gesetzliche Datenschutzbestimmungen zu erlassen sondern ist es für Mitgliedsstaaten der EU auch verpflichtend, mittels effizienter und geeigneter Regelungen für die Einhaltung der Bestimmungen zu sorgen.

Ein reiner Feststellungsbescheid, der nicht durchsetzbar ist, bietet Betroffenen keinerlei Möglichkeit zur Rechtsdurchsetzung. Da gegenüber Auftraggebern öffentlichen Rechts im österreichischen Recht die Möglichkeit einer effizienten Rechtsdurchsetzung - mangels Vollstreckbarkeit entsprechender Entscheidungen zu Verstößen gegen Datenschutzbestimmungen - nicht gegeben ist, ist die derzeitige Rechtslage mit den genannten Regelungen der Richtlinie 95/46/EG nicht vereinbar.

Auch in Punkt "Datenschutzdurchsetzung bei Behörden" verabsäumt es der Entwurf eine der EU-Richtlinie 95/46/EG konforme Situation herzustellen.

(6.) Notwendige Präzisierung der Zustimmungsanforderungen

Die Datenverwendung auf Grund der Zustimmung des Betroffenen als ausdrückliche Willenserklärung gewinnt immer mehr an Bedeutung. Moderne Informationstechnologien haben jedoch dazu geführt, dass für Betroffene der Vorgang der zu einer Zustimmung führte vielfach nicht nachvollziehbar und transparent war. Es entstanden dadurch in der Vergangenheit Situationen, in denen die Frage der Willenserklärung zumindest strittig war.

Die bekanntesten Beispiele betreffen etwa telefonisch abgeschlossene Kaufverträge, bei denen der Tonbandmitschnitt zum Vertragsbestandteil wurde. In vielen Fällen wendeten sich Betroffene ursprünglich mit einer Informationsanfrage an die Telefonstelle und dachten gar nicht an einen neuen Vertragsabschluss.

Es sollte daher die Definition von "Zustimmung" (§4 Z14) dahingehend präzisiert werden, dass für Datenverwendungen, die Grundlage eines Vertrages werden, jedenfalls eine schriftliche Zustimmung erforderlich ist.

Weiters sollten zusätzliche Zustimmungen, die nicht notwendiger Teil eines Vertrags sind, insbesondere zusätzliche Datenverwendungs- und Übermittlungsermächtigungen für Marketingzwecke, vom eigentlichen Vertrag getrennt sein und eine gesonderte ausdrückliche Zustimmung erfordern.

(7.) Keine Behebung zahlloser praktischer Auskunftsprobleme

Zu wissen, wer welche Daten über eine Person sammelt, woher diese stammen und an wen sie weiter gegeben werden, ist DAS zentrale Informationsrecht für Betroffene. Die bisherigen Bestimmungen haben sich jedoch nicht als praxistauglich erwiesen.

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.

Regelmäßig werden Auskünfte über Herkunft und Weitergabe der Daten verweigert oder die Auskunft wird - sanktionslos - verzögert und der Betroffene versäumt dadurch wichtige Fristen.

So sind von Daten nur "die verfügbaren Informationen über ihre Herkunft" zu beauskunften (§26 DSG), was regelmäßig dazu führt, dass Datenverarbeiter, die "etwas zu verbergen haben", behaupten nicht mehr zu wissen, woher sie die Daten haben.

Nun kann es tatsächlich im Einzelfall so sein, dass die Herkunft von Daten nicht mehr nachvollziehbar ist, es darf aber nicht zur Pauschal-Schutzbehauptung für ganze Branchen werden.

Für Datenverarbeiter, die berufsmäßig oder gewerblich mit Daten handeln, sollte hier jedoch ein Sanktionsmechanismus vorgesehen werden. Derartigen Datenverarbeitern, wie Kreditschutzverbänden, Wirtschaftsauskunftsdiensten oder Adressenverlagen sollte die Weitergabe von Daten, deren Herkunft ungewiss oder unbekannt ist, verboten werden.

Ein derartiges Verbot ist auch sachlich begründet, da mangels Herkunftsinformation auch nicht mehr die Aktualität der Daten oder allfällige Änderungen erkannt werden können.

Bezüglich der Auskunft über Herkunft und Datenweitergabe ist die Klarstellung dringend erforderlich, dass dazu alle beim Auftraggeber verfügbaren Informationen heranzuziehen sind, dies betrifft etwa auch Buchhaltungsunterlagen.

In der Vergangenheit gab es mehrfach Fälle, in denen der Händler einer CD mit Daten von Privatpersonen die Auskunft über die Weitergabe verweigerte, obwohl er laut Bescheid der Datenschutzkommission verpflichtet war, Aufzeichnungen über die Bezieher der CD zu führen.

Erfolgreich wird von Datenverarbeitern "die etwas zu verbergen haben", auch die Auskunftsfrist von acht Wochen umgangen. Immer mehr Datenverarbeiter geben keinerlei Auskunft und warten eine Beschwerde vor der DSK ab. Diese entscheidet erst nach etwa sechs Monaten. Wenn in dieser Zeit der Datenverarbeiter doch eine Auskunft erteilt, und sei sie noch so unvollständig und rechtswidrig, wird die Beschwerde abgewiesen! Zur unvollständigen Auskunft beginnt ein neues Verfahren, das wieder sechs Monate dauert. Auf diese Weise können unseriöse Datenverarbeiter die Auskunftsverfahren auf vierzehn Monate verlängern.

Damit können für die Betroffenen wichtige Fristen verloren gehen.

Gemäß dem geplanten § 31 Abs 8 DSG kann ein Beschwerdegegner, gegen den wegen Verletzung in Rechten nach den §§ 26 bis 28 Beschwerde erhoben wurde, bis zum Abschluss des Verfahrens vor der Datenschutzkommission durch Reaktionen gegenüber dem Beschwerdeführer gemäß § 26 Abs. 4 oder § 27 Abs. 4 die behauptete Rechtsverletzung nachträglich beseitigen. Erscheint der Datenschutzkommission durch derartige Reaktionen des Beschwerdegegners die Beschwerde als gegenstandslos, so hat sie den Beschwerdeführer dazu zu hören. Gleichzeitig ist er darauf aufmerksam zu machen, dass die Datenschutzkommission das Verfahren formlos einstellen wird, wenn er nicht innerhalb einer angemessenen Frist begründet, warum er die ursprünglich

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.

behauptete Rechtsverletzung zumindest teilweise nach wie vor als nicht beseitigt erachtet. Wird durch eine derartige Äußerung des Beschwerdeführers die Sache ihrem Wesen nach geändert (§ 13 Abs. 8 AVG), so ist von der Zurückziehung der ursprünglichen Beschwerde und der gleichzeitigen Einbringung einer neuen Beschwerde auszugehen. Auch diesfalls ist das ursprüngliche Beschwerdeverfahren formlos einzustellen und der Beschwerdeführer davon zu verständigen. Verspätete Äußerungen sind nicht zu berücksichtigen.

Es wird daher gefordert, die Strafbestimmungen (§52 DSG) dahingehend zu ergänzen, dass bei fruchtlosem Verstreichen der achtwöchigen Auskunftsfrist und mit Vorlage des Auskunftsverlangens die zuständige Verwaltungsbehörde unabhängig vom Auskunftsverfahren eine Versäumnisstrafe zu verhängen hat, wobei auch eine Mindeststrafe von zumindest 100,- Euro vorzusehen ist.

Weiters ist dringend erforderlich, zahllose Auskunftslücken zu schließen, die sich aus den Entwicklungen der modernen Informationstechniken ergeben haben. So besteht derzeit kein Auskunftsrecht auf Auswertungen, die das Wohngebiet, den Häuserblock, die soziale oder ethnische Gruppe des Betroffenen betreffen, auch dann wenn diese Daten zur Beurteilung des Betroffenen herangezogen werden. Feststellungen, wie sie im Bereich "Data-Mining" oder "Direktmarketing" üblich sind, wie etwa "Bewohner eines sozial unterentwickelten Gebietes" usw. unterliegen derzeit nicht der Auskunftspflicht, obwohl sie direkten Einfluss auf die informationelle Selbstbestimmung der Person haben.

Die diesbezügliche Gesetzeslage ist auch fragwürdig hinsichtlich ihrer europarechtlichen Vereinbarkeit. Art. 8 der EU-Datenschutz-RL garantiert Betroffenen jedenfalls, „frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten“ die Bestätigung, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden.
Eine Gesetzeslage, die es ungeahndet lässt, wenn Betroffene regelmäßig nur im Rahmen aufwendiger Beschwerdeverfahren ihre Ansprüche gegenüber Datenverarbeitern durchsetzen können, kann sich mit dieser Auskunftsgarantie jedenfalls nicht vertragen. Entsprechende Auftraggeber werden- mangels Sanktionen- gegenwärtig in Wahrheit geradezu eingeladen, Ersuchen erst im Rahmen eines Verfahrens unter behördlicher Mitwirkung zu beantworten.

Die Behebung dieser Mängel wäre auch angesichts der umfassenden Auskunftspflichten nach der EU-Richtlinie 95/46/EG, die in Österreich nur lückenhaft umgesetzt sind dringend geboten.

(8.) Notwendige Sanierung des Informationsrechts

EU-widrig war bisher im §24 DSG das Informationsrecht umgesetzt. Abs.3 Z3 enthält Ausnahmen, die nach der EU-Richtlinie 95/46/EG nicht vorgesehen sind (Art. 10, 11).

Die bisherige Erfahrung zeigte, dass Datenverarbeiter, "die etwas zu verbergen haben", insbesondere aus dem Bereich der Kreditinformationen und Wirtschaftsauskunftsdienste

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.

diese Ausnahmen der Informationspflicht in Anspruch nehmen und Betroffene nicht über die Aufnahme in ihre Datenverarbeitungen informieren.

Eine Streichung der Ausnahmebestimmungen des §24 Abs. 3 zur Herstellung eines EU-konformen Zustandes ist dringend geboten.

(9.) Verbandsklagemöglichkeit bei schweren Datenschutzverletzungen

Für die Fälle schwerer und viele Personen betreffender Datenschutzverletzungen sollte eine Verbandsklagemöglichkeit geschaffen werden.

Derzeit existieren Datenanwendungen mit mehreren hunderttausend rechtswidrigen Datenverwendungen, die nur durch Zivilverfahren jedes einzelnen Betroffenen beseitigt werden können. Abgesehen vom Prozess- und Kostenrisiko ist es unzumutbar, dass Betroffene zur Sicherung ihrer Grundrechte jahrelange Prozesse anstrengen müssen, obwohl in vergleichbarer Sache schon entschieden wurde.

Einrichtungen die sich mit der Durchsetzung von Datenschutzrechten beschäftigen, sollten auf Antrag durch das Bundeskanzleramt zur Verbandsklage ermächtigt werden können. Dies hätte auch den Vorteil der Entlastung der personell unterbesetzten Datenschutzkommission.

Die Voraussetzungen einer Verbandsklage könnten eindeutig geregelt werden,
a) wenn es zu einer Sache schon eine vergleichbare Judikatur gibt und Beschwerden von Betroffenen darauf hinweisen, dass auch andere von der Datenschutzverletzung betroffen sind,
b) wenn es Empfehlungen der Datenschutzkommission gibt und Hinweise schließen lassen, dass diesen Empfehlungen nicht nachgekommen wird oder
c) wenn das Verhalten eines Datenverarbeiters auf Datenschutzverletzungen für mehrere Personen schließen lässt (etwa rechtswidrige Ankündigungen oder Veröffentlichungen des Datenverarbeiters).

Als typisches Beispiel seien die Aktivitäten eines Kreditinformationsdienstes genannt, der von sich - völlig rechtswidrig - behauptet, dass er Daten entgegen den Bestimmungen des DSG §27 nicht aktualisiere.

(10.) Verbesserung des immateriellen Schadenersatzrechts

An der derzeitigen Gesetzeslage kritikwürdig ist, dass es keine geeignete Ersatzbestimmung hinsichtlich immaterieller Schäden aus Datenmissbräuchen gibt.

Gemäß § 33 DSG 2000 hat zwar ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Nur dann, wenn durch die öffentlich zugängliche Verwendung von Daten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt

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.

werden, die einer Eignung zur Bloßstellung gleichkommt, besteht ein Anspruch auf angemessene Entschädigung für die erlittene Kränkung.

In anderen Fällen, in denen etwa Daten von Betroffenen zweckwidrig verwendet oder Betroffene in ihren Datenschutzrechten rechtswidrig beschränkt werden, besteht eine Ersatzpflicht bislang nur dann, wenn tatsächlich auch ein finanzieller Schaden bescheinigt wird.

Relevant sind derartige Fragen etwa bei Dauerschuldverhältnissen, wie Bankverbindungen oder Handyverträgen, etwa dann wenn derartige Schuldverhältnisse durch den Unternehmer beendet werden, weil ein Betroffener auf datenschutzrechtliche Ansprüche pocht oder die Beendigung Ergebnis einer rechtswidrigen Datenverwendung ist.

Für diese Fälle wäre es wünschenswert, dass Betroffenen unabhängig vom Nachweis eines Vermögensnachteils ein Schadenersatzanspruch zugebilligt wird.

Vom Schadenersatzrecht ausgenommen sind auch jene Fälle, in denen ein Dritter, der von Daten eines Betroffenen rechtswidrig Kenntnis erlangt hat, diese gegen den Betroffenen verwendet oder weiter verbreitet. Das Schadenersatzrecht des DSG zielt ausschließlich auf Auftraggeber und nicht auf andere Datennutzer.

Diese Bestimmung ist in Zeiten des Internet überholt, in der es auch dem einfachen Benutzer ("Surfer") möglich ist, persönliche Daten über Betroffene zu sammeln und weiter zu verbreiten, ohne dass er Auftragegeber im Sinne des DSG wird.

Ein Schadenersatzanspruch sollte gegen jeden Verwender persönlicher Daten durchsetzbar sein. Dies ist insbesondere in Hinblick auf die Weiterverbreitungsmöglichkeiten von Daten im Internet geboten.

In der Vergangenheit wurden vielfach Urteile im RIS oder sonstige Dokumente auf Behördenservern unzureichend anonymisiert veröffentlicht.

Bezüglich Behörden, die Entscheidungen, Bescheide oder Urteile unzureichend anonymisieren und dadurch personenbezogene Daten veröffentlichen, sollte unabhängig vom Inhalt der veröffentlichten Daten ein Mindestschadenersatz von 200,- Euro eingeführt werden.

Auch in diesem Bereich wurde es durch den vorliegenden Entwurf versäumt, entsprechende Stärkungen der Betroffenenrechte vorzunehmen.

(11.) Parteienstellung/Informationsrecht des Betroffenen in Verwaltungsstrafverfahren

Eine Reihe der Verwaltungsstrafbestimmungen betreffen unmittelbar Betroffenenrechte. Unter anderem sind dies die Frage der Einhaltung des Informationsrechts (§24), der Registrierungspflichten (§17) oder der rechtswidrigen Löschung von Daten (§26).

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.

Trotzdem hatte bisher der Betroffene, auch wenn er Anzeiger war weder Parteienstellung, noch ein Informationsrecht.

Zumindest in den Fällen, in denen ein Anzeiger sein individuelles Rechtsschutzinteresse glaubhaft macht, ist eine verpflichtende Information über das Ergebnis des Verfahrens vorzusehen.

(12.) Verbot der Verwertung biologischer Spuren

In Hinblick auf die wachsende Bedeutung biometrischer Identifikationsmaßnahmen sollte ein generelles Verbot der Verwertung biologischer Spuren (Fingerabdrücke, DNA-Spuren, Irisscan, ...), solange keine ausdrückliche gesetzliche Ermächtigung oder kein ausdrücklicher gerichtlicher Auftrag besteht, festgehalten werden.

In vielen anderen entwickelten Ländern wurde ein derartiges Verbot schon verabschiedet und stellt sicher, dass nicht weggeworfene Zigarettenkippen oder Taschentücher für privatrechtliche DNA-Analysen, private Vaterschaftstests, Versicherungsabschlüsse oder ähnliches herangezogen werden.

Das Verbot sollte als Präzisierung des §6 DSG formuliert werden.

(13.) Schaffung wirksamer Kontrollbefugnisse der Datenschutzkommission

Nicht bewährt haben sich die bisherigen Kontrollbefugnisse der Datenschutzkommission. Dies betrifft sowohl die Rechte der Prüfung vor Ort ("Einschau" §30 Abs. 4), als auch die Möglichkeit inhaltliche Feststellungen zur Umsetzung der Grundlagen nach §§1,6 und 7 (Prüfung der sachlich angemessenen Datenverwendung).

§30 Abs. 4 DSG sieht zwar ein Einschaurecht der Datenschutzkommission, jedoch keinerlei Durchsetzungsmöglichkeiten vor. Wenn ein Datenverarbeiter, "der etwas zu verbergen hat", und nur bei diesen ist ja die Einschau gerechtfertigt, der Datenschutzkommission den Zutritt verweigert, kann dieser nicht erzwungen werden. Auch dann nicht, wenn Millionen Menschen von einer dubiosen Datenverarbeitung betroffen sind.

Damit ist die Datenschutzkommission schlechter gestellt als die ORF-GIS, die für den vergleichweise läppischen Zweck der Eintreibung von Radio- und Fernsehgebühren den Zutritt zu Wohnungen erzwingen kann.

Die Einschaurechte sollten jedenfalls um ein Zutrittsrecht ergänzt werden oder gänzlich aufgehoben werden.

Weiters ist eine Verpflichtung der Datenschutzkommission vorzusehen, im Falle der Datenverwendung immer auch zu prüfen, ob die Grundsätze des gelindesten Eingriffs, der Angemessenheit der verwendeten Daten überhaupt eingehalten wurden. Dazu wäre es notwendig die Alternativen einer Datenverwendung zu prüfen und zu bewerten.

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.

Die DSK weigert sich jedoch in ihrer ständigen Praxis derartige Bewertungen durchzuführen, sie beschränkt sich auf das sogenannte „Übermaßverbot“: Wenn es denkmöglich ist, dass die von einer in der Sache zuständigen Behörde ermittelten Daten nach Art und Inhalt für die Feststellung des relevanten Sachverhaltes geeignet seien, sei die Zulässigkeit der Ermittlung aus Sicht der DSK immer gegeben. Die Inanspruchnahme einer tiefergehenden Beurteilung der Eignung der von der sachlich zuständigen Behörde gewählten Ermittlungsschritte würde - nach ständiger DSK-Auffassung - einen Eingriff in die sachliche Behördenzuständigkeit bedeuten und wird daher von der DSK nicht durchgeführt.

Diese ständige Vorgangsweise der DSK steht im klaren Widerspruch zur Verfassungsbestimmung des Datenschutzgesetzes §1, der Eingriffe nur mit dem "gelindesten zum Ziel führenden Mittel" erlaubt und der EG-Richtlinie Datenschutz (95/46/EG), die in Art. 28 die Kontrolle der Datenschutzbestimmungen durch eine unabhängige Behörde verlangt. Selbstverständlich bedeutet eine derartige Prüfung, ob in einem Verfahren tatsächlich nur die gelindesten Mittel eingesetzt wurden, einen Eingriff in die für das Strafverfahren zuständige Behörde. Aus diesem Grund sieht ja die Richtlinie eine unabhängige und weisungsfreie Kontrollbehörde vor.

Eine Verpflichtung bei einer behaupteten Datenschutzverletzung zur Beurteilung der Angemessenheit einer Datenverwendung alle Möglichkeiten einer Datenverwendung zu prüfen wäre auch in Hinblick auf die Umsetzung der einschlägigen EU-Richtlinie und einer tatsächlich unabhängigen Datenschutzbehörde erforderlich.

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.

Teil III.: Weiterer grundrechtlicher Sanierungsbedarf

Die Vergangenheit zeigte, dass eine Reihe von Datenschutz-Problemstellungen nicht im DSG selbst gelöst werden können, sondern zusätzlicher Regelungen bedürfen.

Eine umfassende Datenschutznovelle sollte auch diese Bereiche - allenfalls in Zusammenarbeit mit anderern Dienststellen - berücksichtigen.

(1.) Beseitigung des Interessenskonflikts in der Datenschutzkommission

Das E-Government-Gesetz sieht die Datenschutzkommission als verantwortliche Behörde zur Verwaltung der Stammzahlen vor.

Dies ist eine eindeutig operative Verwaltungstätigkeit und steht im Widerspruch zur Aufgabe einer unabhängigen Kontrollstelle in allen Datenverarbeitungsangelegenheiten.

Im Zusammenhang mit Datenschutzfragen des Stammzahlregisters wäre somit die Datenschutzkommission durchführende und beaufsichtigende Behörde gleichzeitig! Eine klassische Unvereinbarkeit, die im Zuge der Änderung des DSG zu sanieren ist.

(2.) Datenschutz im Bereich Gerichte und Legislative

Immer wieder kommt es zu Eingriffen in die Grundrechte unbescholtener Bürger, weil deren Daten ohne ihre Zustimmung in parlamentarischen Anfragen zitiert werden, auf der Webseite des Parlaments oder in Urteilen im RIS veröffentlicht werden, weil Politiker diese Daten auf ihren Homepages veröffentlichen. Für diese Datenschutzverletzungen ist das DSG nicht zuständig.

Es wird daher angeregt für die Gerichte, den Nationalrat, den Bundesrat und die Landtage ausreichende moderne Datenschutzgarantien zu verabschieden.

(3.) Beweisverwertungsverbot rechtswidrig erlangter Daten

Auch ein Beweisverwertungsverbot vor Gericht und vor Verwaltungsbehörden von rechtswidrig erhaltenen Daten sollte verabschiedet werden.

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.