An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 15. Mai 2008

Betreff: BKA-810.026/0002-V/3/2008
Stellungnahme der ARGE DATEN zur DSG-Novelle 2008

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

CN = Mag. Dr. Hans Gerhard ZEGER, Vertretung ARGE DATEN als Obmann, C = AT, L = Wien, S = Wien, O = ARGE DATEN - Oesterreichische Gesellschaft fuer Datenschutz
2008.05.15 18:10:12 +02'00'

Dr. Hans G. Zeger (Obmann)

Charlotte Schönherr (Schriftführerin)

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

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

Stellungnahme der ARGE DATEN vom 15. Mai 2008 zur *DSG-Novelle 2008*

Einleitung

Das Bundeskanzleramt hat das Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird, die sogenannte DSG-Novelle 2008 in Begutachtung gebracht. Der vorliegende Gesetzesentwurf bringt dabei – in einem kurzen Überblick zusammengefasst- einerseits durchaus einige gesetzliche Innovationen, die aus Sicht des Datenschützers positiv zu bewerten sind. Dazu zählen etwa die Bestimmungen zum betrieblichen Datenschutzbeauftragten sowie die Kompetenzbereinigung hinsichtlich nicht automationsunterstützter Datenverarbeitungen zugunsten des Bundesgesetzgebers.

Diesen durchaus positiven Ansätzen stehen umgekehrt geplante Bestimmungen gegenüber, die aus grundrechtlicher Sicht höchst bedenklich sind und jedenfalls eine Schlechterstellung der betroffenen Bürger darstellen.

Besonders problematisch sind dabei die Video-Überwachungsbestimmungen, die als Generalermächtigung für beliebige private und öffentliche Überwachungsmaßnahmen anzusehen sind. Abzulehnen ist auch eine geradezu kafkaesk ausufernde Bürokratisierung der Beschwerdeverfahren vor der DSK und eine offensichtlich verfassungs- und EU-widrige Beschränkung der Melderechte der Datenverarbeiter, die in Zukunft zur Verwendung der Bürgerkarte gezwungen werden sollen.

Vor allem ist aber festzuhalten, dass der vorliegende Gesetzesentwurf ein „Entwurf der verlorenen Chancen“ ist. Die ARGE DATEN hat in den vergangenen Jahren regelmäßig auf gravierende Mängel des österreichischen Datenschutzwesens hingewiesen, bei Reformvorschlägen wurde dabei oft auf eine umfassende Reform des DSG 2000 verweisen. Der vorliegende Begutachtungsentwurf hat in dieser Beziehung leider praktsich nichts zu bieten. Dabei gäbe es genug Handlungsbedarf, der durch die Verantwortlichen bislang einfach nicht genutzt wurde.

Im letzten Abschnitt wird noch auf eine Reihe von Grundrechtslücken verwiesen, die ebenfalls als datenschutzrelevant in anderen Bestimmungen zu sanieren sind.

Es wird daher empfohlen diesen Entwurf zur DSG-Novelle 2008 zurückzunehmen und völlig neu, systematisch zu überarbeiten.

Teil I.: Der Entwurf der verlorenen Chancen

(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.

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 spezialisiserte 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 es eine österreichische eBay-Gesellschaft gibt und 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.

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[1] 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 des EU-Schnittes. Für die Mitglieder sollten jedenfalls strenge Unvereinbarkeitsbestimmungen gelten.

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

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

Neben der EU-widrigen Ausnahme der "allgemein verfügbaren Daten" von wesentlichen 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 sensibler 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

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 Finanzminsiterium) 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 gerichtsähnliche Einrichtung sieht, bestätigte in der Vergangenheit diese Position. Diese 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 entsprechende Verletzungen datenschutzrechtlicher Bestimmungen durch Auftraggeber öffentlichen Rechts feststellen lassen, durchsetzbar sind daraus resultierende Ansprüche aber 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.

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

(7.) Keine Behebung zahlloser 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.

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", behaupteten 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 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

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 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.) 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

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 aktualisisere.

(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 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 jedenfalls wünschenswert, dass Betroffenen auch 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.) Verständigungpflicht bei Datenverlust und illegaler Datenweitergabe

Sowohl im In- als auch Ausland mehren sich die Fälle, dass personenbezogene Daten verloren gehen oder unzulässiger Weise an Dritte weitergegeben werden[2].

2 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

Als Datenverlust ist das Abhanden kommen von Daten ohne Kenntnis eines möglichen Empfängers oder Finders zu verstehen[3].

Datenverarbeiter, die Daten verlieren bzw. deren Daten von Dritte beschafft, kopiert oder sonstwie entwendet wurden, sollen verpflichtet werden, die davon Betroffenen zu verständigen.

Die Verständigung soll Angaben zum Umfang der 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.

Sinn der Maßnahme ist es, dass sich Betroffene individuell auf mögliche negative Konsequenzen des Datenverlustes einstellen können und auch individuelle Gegenmaßnahmen setzen können.

Weiters ist diese Verständigung notwendig für individuelle Rechtsdurchsetzung, etwa nach §33 DSG (materieller und imaterieller Schadenersatz). Datenverlust bzw. illegale Datenweitergabe, die zur Bloßstellung des Betroffenen führen können, insbesondere Daten über strafrechtliche Belange und zur Kreditwürdigkeit, sollen jedenfalls eine immaterielle Schadenersatzpflicht nach §33 DSG des ursprünglichen Datenverarbeiters und desjenigen auslösen, der die Daten weitergegeben hat.

(12.) 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).

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.

---

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)

[3] 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.

(13.) Sanierung des Löschungsverbots in §26

§26 Abs. 7 sieht vor *"Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten."*

Diese ursprünglich als Schutz des Betroffenen gedachte Bestimmung hat sich in der Praxis nicht bewährt. In jenen Fällen, in denen nach einer Auskunft der Betroffene die Löschung der Daten verlangte, wurde dies unter Hinweis auf die viermonatige Sperre verhindert. Dies führte dazu, dass fehlerhafte Daten vier weitere Monate verbreitet wurden.

Es sollte daher diese Bestimmung durch einen Zusatz ergänzt werden: "Das Löschungsverbot gilt nicht, wenn der Betroffene eine Löschung verlangt."

(14.) 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.

(15.) 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.

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.

Teil II.: Videoüberwachung im Entwurf fehlerhaft umgesetzt

Ziel allgemeiner Datenschutzbestimmungen kann es niemals sein, in einem Datenschutzgesetz Ermächtigungen zum Einsatz von Datenverarbeitungen zu definieren. Dies muss Materiegesetzen vorbehalten sein und würde ansonsten einerseits zu einer Parallelgesetzgebung führen, andererseits würde das Datenschutzgesetz, das als Schutzgesetz vor Datenverarbeitungen aller Art gedacht ist, völlig ausgehöhlt und in sein Gegenteil verkehrt werden.

Schon in der letzten DSG-Novelle 2005 war das der Fall, in der in einer Tsunami-Anlassgesetzgebung Datenverarbeitungsermächtigungen völlig system- und sinnwidrig in das Datenschutzgesetz eingebaut wurden.

Noch viel stärker ist das nunmehr bei den sogenannten "Videobestimmungen" der Fall.

(1.) Gescheiterter Videoüberwachungs-Entwurf

§50a des Entwurfes sieht in Abs. 3 eine Überfülle von Ermächtigungen vor, in denen Videoüberwachung keine "schutzwürdigen Geheimhaltungsinteressen" verletzt und somit generell zulässig ist. Die Bestimmungen im Einzelnen sind in sich widersprüchlich und unklar und letztlich entbehrlich, hält doch Z7 abschließend fest, dass jede "Videoüberwachung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche des Auftraggebers vor einem Gericht" zulässig sei. Da Vandalismus, Besitzstörung, Einbrüche, aber auch Kündigungen eines Mieters oder Entlassung eines Mitarbeiters gerichtsanhängig werden können, wird damit ein Freibrief für jede Videoüberwachung geschaffen.

Mit der neuen Bestimmung ist die Videoüberwachung durch Private praktisch überall und an allen Orten möglich. Während die Rechtssprechung bisher davon ausging, dass Videoüberwachung nur zur Lösung bestimmter, meist strafrechtlicher Konfliktsituationen einzusetzen ist (etwa Aufklärung und Verhinderung von Einbrüchen, Überfällen oder Diebstählen), fällt diese Beschränkung im neuen Entwurf weg.

Jedes öffentliche Verhalten, soll in Zukunft, ohne jede andere Voraussetzung überwacht werden dürfen (§50a Abs.3 Z2).

Die Hauszufahrt des Nachbarn, der Schanigarten des Konkurrenten, jede Kamera in Fußgängerzonen, selbst Kameras in Diskotheken oder Cafes, in Bussen, U-Bahnen oder Eisenbahnzügen wären nach dieser Bestimmung völlig voraussetzungsfrei zulässig. Der Entwurf bleibt damit hinter der bisherigen Rechtssprechung des OGH zurück, der unter anderem eine Videoüberwachung öffentlichen Verhaltens (Betreten und Verlassen eines Hauses) als unzulässig angesehen hat.

Bedeutsam ist auch, dass nach dieser Bestimmung jede Videoüberwachung des Straßenverkehrs, unabhängig von Gefahren- oder Gefährdungssituationen zulässig wäre, inklusive einer flächendeckenden Überwachung durch die Asfinag, die schon seit Jahren auf deren Wunschzettel steht.

Eine weitere Vollmacht zu unbeschränkter Überwachung besteht in der willkürlichen Festlegung der 100.000,- Euro Wertgrenze (§50a Abs 3 Z5 lit. d). Was auf den ersten Blick nach viel aussieht, entpuppt sich als weitere Generalermächtigung. Es wird wohl keinen Betrieb und kein Geschäftslokal geben, in dem nicht die Waren und Geschäftsunterlagen diesen Wert übersteigen werden. Selbst die meisten Wohnungen haben mittlerweile einen darüber liegenden Einrichtungswert. Gleichzeitig ist die Grenze völlig willkürlich und unsinnig gezogen, könnte doch der Verlust eines kleineren Betrages eines weniger begüterten Menschen existenzbedrohender sein, als 100.000,- bei jemandem, der schon mal diesen Betrag im Casino verspielt.

Tatsächlich ist jedenfalls der gesamte Absatz 3 des Videoparagraphen § 50a entbehrlich. Die Voraussetzungen für eine Datenverarbeitung sind im DSG längst unter §6 DSG allgemein umschrieben. Jede weitere "Präzisierung" hätte nur die Konsequenz, dass zusätzliche Datenverarbeitungen erlaubt wären.

Es wird daher empfohlen den §50a Abs. 3 ersatzlos zu streichen, die für eine Videoüberwachung erforderlichen Voraussetzungen müssen in den Materiegesetzen geregelt werden nd sind nach den Anforderungen des §6 DSG zu prüfen.

Bisher ist die Rechtssprechung davon ausgegangen, dass Aufzeichnungen, die für einen Zweck, z.B. Diebstahlsüberwachung eines Verkaufsraumes, angefertigt wurden, nicht für einen anderen Zweck verwendet werden durften. Selbstverständlich war die Verwendung des Materials für die Anzeige des Diebstahls zulässig, selbstverständlich konnte das Material auf Grund eines Gerichtsbeschlusses auch in anderen Gerichtsverfahren vorgelegt werden.

In der Novelle wird nun festgeschrieben, dass private Videoaufzeichnungen jederzeit auch für andere Straftaten der Polizei auszuhändigen sind (§50a Abs.5). Ausdrücklich wird festgehalten, dass die Daten auch dann auszuhändigen sind, wenn sie gar nicht den Zweck der Videoüberwachung betreffen.

Da kein Auftraggeber ständig sein Videomaterial nach anderen, ihn gar nicht betreffenden Delikten durchforsten wird, wird die Bestimmung in der Praxis darauf hinaus laufen, dass die Polizei bei einem Videoüberwacher vorstellig werden wird, diesen davon informieren wird, dass der Verdacht bestehe, dass auf seinem Videomaterial eine rechtswidrige Handlung aufgezeichnet ist. Laut Sicherheitspolizeigesetz (§53 Abs. 4) erhebe man Anspruch auf diese Daten.

Dem Auftraggeber wird damit nahegelegt, dass er sich dem "begründeten Verdacht" der Polizei anschließen könne, womit auch eine datenschutzrechtliche Grundlage für die Herausgabe des Materials geschaffen wäre!

Damit wird der Zugriff auf Videoüberwachung generell ohne richterliche Kontrolle und auch ohne eindeutige Zweckbestimmung freigegeben. In Zukunft erspart sich die Polizei eine große Zahl eigener Überwachungen, da sie direkt auf die Anlagen der Verkehrsunternehmen, der Straßenerhalter oder der Gemeinden zugreifen kann.

Aushändigen kann bedeuten, dass Aufzeichnungen nachträglich herausgegeben werden, es kann aber auch bedeuten, dass das Videosignal in Echtzeit an die Polizei weitergeleitet wird, die ideale Durchführungsbestimmung für die geforderte Kennzeichenüberwachung. Damit geht diese Bestimmung noch weiter als die zuletzt stark kritisierten Handyortungs- und Internetermittlungsermächtigungen.

Diese Bestimmung ist besonders in Hinblick auf Bestrebungen im Straßenverkehr, flächendeckende Überwachungen, sei es unter dem Titel der Mautvignetten-Überwachung, der KFZ-Kennzeichenerfassung, der Feststellung von Verstößen nach der StVO als kritisch anzusehen.

Es besteht die Gefahr, die jeweiligen Überwachungsbetreiber (ASFINAG, private "Verkehrssheriffs", Gemeinden, Parkgaragenbetreiber, ...) könnten angesichts der vielfältigen Übertretungsmöglichkeiten pauschal vom *"begründeten Verdacht [ausgehen], die Daten könnten ... 2. der Abwehr oder Beendigung eines gefährlichen Angriffs dienen"* und damit vorbeugend und auch um ein "gutes polizeiliches Einvernehmen zu erreichen" den Sicherheitsbehörden den Zugriff auf diese Daten erlauben. Ausgerechnet die "Datenschutz"-Bestimmung §53 Abs. 5 würde für dieses Vorgehen erstmal eine Rechtsgrundlage schaffen. Statt eines verbesserten Bürgerschutzes käme es dann zur "verbesserten" Bürgerüberwachung.

Diese Kameras könnten dann zur Prüfung der Geschwindigkeit, der Abstandskontrolle, der Mautabgaben, der Gurtenanlegepflicht, des Telefonierens am Steuer, der Zahl der Insassen, der Verschmutzung der Windschutzscheiben, defekter Blinker oder Scheinwerfer, selbst Konzentrationsmängel, wie das Wegschauen, könnten dann aufgezeichnet werden. Das Problem wären nicht die eindeutigen Regelverstöße, sondern die rasch steigende Zahl von Problemfeldern oder unklaren Situationen. Einen Vorgeschmack dazu lieferte das monatelange Problem der Feststellung der Fahrbahnfeuchtigkeit im Section-Control-Abschnitt der A2. Tausende Fahrer wurden bei trockener Fahrbahn erfasst, weil Sensoren irrtümlich Schmelz- und Abflusswasser als Farbahnnäse interpretierten.

Das Ergebnis wäre dann zwar eine Maximierung in der Aufdeckung von Übertretungen und eine sprudelnde Einnahmequelle, es ist aber mehr als fraglich, ob damit auch eine Erhöhung der Verkehrssicherheit gegeben wäre.

Eine Ausweitung der polizeilichen Zugriffsbefugnisse, die - weil unkontrolliert und unkontrollierbar - abzulehnen ist.

(2.) Kein ausreichender Schutz höchstpersönlicher Lebensbereiche

Nicht einmal die Überwachung in höchstpersönlichen Lebensbereichen wird ausreichend verhindert. Diese Bereiche werden nicht ausreichend umschrieben, die erläuternden Bemerkungen beschränken sich auf Privatwohnungen, Toilettenanlagen und Umkleidekabinen. Private Verrichtungen finden aber auch an einer Vielzahl weiterer Stellen statt, zu denken ist an die Andacht am Friedhof oder in der Kirche, an Krankenzimmer oder Gymnastikräume, aber auch Hotelzimmer.

Der Entwurf fällt sogar hinter eine Reihe von OGH-Entscheidungen zurück, in denen der Bereich vor einer Privatwohnung oder der eigene Garten als höchstpersönlicher Lebensbereich definiert ist. Tritt der Entwurf in Kraft, müsste wieder in jahrelangen Verfahren ausgelotet werden, was unter "höchstpersönlichem Lebensbereich" gemeint ist. Es ist dem Gesetzgeber zuzumuten, dass dieser Punkt eindeutig im Gesetz definiert wird.

Die Mindestforderung ist, dass im Gesetz jene höchstpersönlichen Lebensbereiche definiert sind, in denen Videoüberwachungen verboten bzw. nur unter den Bedingungen des Großen Lauschangriffs erlaubt sind.

(3.) Sachlich unbegründete Differenzierungen verschiedener Überwachungsmethoden

Pauschal werden Echtzeitüberwachungen und Aufzeichnungen auf einem "analogen" Speichermedium von der Registrierungspflicht ausgenommen (§50c Abs.1 Z1,2).

Dies ist sachlich unbegündet. Ein Eingriff in die Privatsphäre findet etwa auch dann statt, wenn, wie schon 2007 VfGH-Präsident Korinek kritisierte, jemandem bei der Trauer am Friedhof zugeschaut wird. Echtzeitüberwachungen können unter Umständen sogar schwerwiegendere Eingriffe darstellen, als eine Aufzeichnung, die unter Verschluss ist, die niemand ansieht und die nur bei einem Strafdelikt für den bestimmten Zeitraum geöffnet wird.

Die Vorstellung ist unerträglich, aber durch den Gesetzesentwurf abgesegnet, dass wurstsemmelkauende, witzereißende Schulabbrecher als sogenanntes Sicherheitspersonal den Menschen bei ihrer Andacht zusehen.

Besonders ärgerlich ist die Ausnahme der "analogen" Speichermedien. Die EU-Richtlinie "Datenschutz" schreibt völlig eindeutig Schutzmaßnahmen vor, sobald Personen bestimmt oder bestimmbar sind (Art. 2 lit a 95/46/EG). Selbstverständlich sind auch Personen auf Aufnahmen auf einer VHS-Kasette bestimmbar. Diese Ausnahmebestimmung ist eindeutig EU-widrig.

(4.) Lösung des Videoüberwachungsproblems

Der grundsätzliche Mangel des Entwurfs ist, dass er sich nicht mit der Frage auseinander gesetzt hat, was eigentlich eine Videoüberwachung von anderen Datenverarbeitungen unterscheidet. Nur diese Unterschiede rechtfertigen, dass es Sonderregeln für die Videoüberwachung gibt.

Kern des Unterschieds ist, dass bei allen Datenschutzregeln davon ausgegangen wird, dass eine Datenanwendung zu einem bestimmten Zweck eingerichtet ist (§4 Z7 DSG) und nur Daten von Personen enthält, die diesem Zweck entsprechen (§6 DSG).

Eine Mitarbeiterdatenbank darf nur Mitarbeiter enthalten, alle anderen sind zu löschen, eine Kundendatenbank nur Kunden usw.

Diese doppelte Zweckbestimmng, einerseits die Datenanwendung selbst unterliegt einem berechtigten Zweck, andererseits jeder Datensatz erfüllt diesen Zweck, ist bei der Videoüberwachung nicht gegeben.

Viele Videoüberwachungen erfüllen selbst keinen berechtigten Zweck im Sinne des §4 Z7, ihre Installationen sind bloß Ausdruck einer diffusen Angst, "dass etwas passieren könnte".

Selbst wenn jedoch die Vorbedingung einer klaren Zweckbestimmung der Installation erfüllt ist, ist für die Mehrzahl der ermittelten Daten nicht §6 DSG erfüllt. Es liegt in der Natur einer Videoüberwachung, die zum Beispiel gegen Ladendiebe installiert ist ("Zweck der Datenanwendung"), dass sie mehrheitlich Personen filmt, die nicht in den Anwendungsbereich fallen, schlicht keine Ladendiebe sind.

Es werden somit massenhaft Daten aufgezeichnet, die für den Zweck der Datenanwendung nicht wesentlich sind (§6 Abs. 1 Z3). Derartige Daten dürfen aber nicht aufbewahrt werden (§6 Abs.1 Z4,5) und sind unverzüglich zu löschen (§27 Abs.1 Z1).

Wir haben daher bei Videoüberwachungen das grundsätzliche Problem, dass einerseits Daten aufgezeichnet werden, die man gar nicht aufzeichnen dürfte (vereinfacht gesagt alle "Nicht-Täter") und zweitens, wenn sie schon aufgezeichnet sind, dass sie ehebaldigst zu löschen wären.

Eine sinnvolle Video-Datenschutzbestimmung muss sich daher auf genau diese Punkte beziehen, die abweichend von anderen Datenanwendungen sind.

Das Problem der Aufzeichnung von "Nicht-Tätern" kann durch Installation und Art und Weise des Betriebs reduziert werden. Eine Anlage, die nur einen Kassenraum überwacht wird weniger "Nicht-Täter" filmen, als eine die auch gleich den ganzen Vorplatz eines Geschäfts überwacht.

Kameras, die Überfälle dokumentieren sollen, werden kürzere Speicherfristen haben, als solche, die komplexe Betrügereien dokumentieren sollen. Es ist einem Geschäftsinhaber zuzumuten, am Ende eines Tages zu wissen, ob er überfallen wurde oder nicht.

Kern der Video-Datenschutzbestimmung muss daher das Zulassungsverfahren sein. Dieses ist jedoch im vorliegenden Entwurf völlig unzureichend geregelt.

Es muss gefordert werden, dass zu jeder Videoinstallation ein ausreichender Zweck genannt wird, dass detaillierte Installationspläne vorgelegt werden, die die Registrierungsbehörde in die Lage versetzen, zu erkennen welche Personen von der Überwachung erfasst sind. Weiters sind detaillierte Zugriffs- und Löschpläne vorzulegen, nach denen der Zugriff auf die Daten der "Nicht-Täter" beschränkt wird und eine ehebaldige Löschung sicher gestellt wird.

Die Zulassungsbehörde muss auch verpflichtet werden, vergleichbar jeder anderen Bau- oder Anlagengenehmigungsbehörde die Zweckmäßigkeit - in Hinblick auf die minimale Erfassung der "Nicht-Täter" - der Anlage vor Ort zu prüfen und gegebenenfalls Verbesserungen aufzutragen.

Die Vorschläge dazu sind im vorliegenden Entwurf völlig unzureichend.

Weiters sind umfassende Informationspflichten vorzusehen. Auch die Information über die Videoüberwachung ist im Entwurf nicht EU-konform umgesetzt. §50d erlaubt das Entfallen der Kennzeichnung und der Information der Betroffenen, bei "Unwahrscheinlichkeit der Beeinträchtigung der Betroffenenrechte", eine Formulierung, die eindeutig EU-widrig ist.

Die EU-Richtlinie sieht in Art. 10 und 11 eine generelle Informationpflicht vor, die nicht durch Klauseln beschränkt werden darf.

Auf Grund der Besonderheiten von Videoüberwachungen sind jedenfalls Informations- und Auskunftsrechte vorzusehen, die es Betroffenen erlauben, zu erkennen wo und mit welchen Wirkungskreis Videoinstallationen vorhanden sind. Dies könnte durch eine Erweiterung der Auskunftspflichten aus dem Datenverarbeitungsregister geschehen.

Schutz- oder Geheimhaltungszwecke können dieser erweiterten Informationspflicht nicht entgegenstehen, da Videoüebrwachung vorrangig präventiven Charakter hat und daher das Wissen, wo Installationen bestehen, diese präventive Aufgabe noch unterstützen. Ausnahmen von einer derartigen umfassenden Informationspflicht könnte bestenfalls bei Installationen erfolgen, deren ausschließlicher Zweck das Auffinden eines konkret Tatverdächtigen ist.

Auf Grund der besonderen Gefährdung der Datenschutzinteressen der Gruppe der "Nicht-Täter", die die Mehrzahl darstellt, sind auch die Auskunftsrechte auf diese spezifischen Bedürfnisse abzustellen.

Da ein "Nicht-Täter" von Videoinstallationen wiederholt gefilmt werden kann, etwa bei jedem Einkauf oder bei jedem Zutritt zu einem Haus, obwohl es keinerlei Verdachtsmomente oder Hinweise gibt, er könnte ein "Täter" sein, müssen auch die Auskunftsrechte besondere Garantien enthalten.

Ein einmaliges kostenloses Auskunftsrecht pro Jahr ist nicht ausreichend, da ja auch die Aufzeichnungen mehrfach erfolgen, aber bei den "Nicht-Tätern" keinesfalls so lange aufbewahrt werden dürfen. Der Auskunftsanspruch muss sich daher aus jeder neuerlichen Erfassung ergeben.

Auch eine Anpassung der Auskunfts- und Löschungsfristen ist erforderlich. Auf Grund der kurzen Aufbewahrungsdauer hat ein Auskunftsbegehren von Videoaufzeichnungen jedenfalls die Löschung der Daten zu hemmen. Um das Auskunftsrecht sinnvoll in Anspruch nehmen zu können ist auch erforderlich, dass die Aufbewahrungsfrist der Videoaufzeichnungen Teil der Informationspflicht wird.

Auf alle diese spezifischen Videoanforderungen nimmt der Entwurf keine Rücksicht.

Die Beschränkung der Auskunft auf eine Art Nacherzählung, was auf dem Video aufgezeichnet ist (§50e), widerspricht dem EU-Auskunftsrecht und ist abzulehnen.

Teil III.: Weitere Punkte des Entwurfs zur DSG-Novelle 2008

(1.) Betrieblicher Datenschutzbeauftragter

Als positivster Teil der geplanten Novelle ist sicherlich die Bestimmung des § 15a DSG zum vorgesehenen Betrieblichen Datenschutzbeauftragten zu sehen. Die Einrichtung einer derartigen Institution ist bereits in Erwägungsgrund 49 der EU- Datenschutz- RL vorgesehen. Es existieren dazu auf Ebene anderer europäischer Staaten bereits außerordentlich positive Erfahrungen.

Gerade jüngste Erfahrungen, wie auf betrieblicher Ebene oft mit Datenschutzinteressen sowie der Privatsphäre- vor allem der eigenen Mitarbeiter- umgegangen wird, lassen eine derartige Einrichtung jedenfalls als notwendig und überfällig erscheinen.

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.

Dies gelte jedenfalls für bestimmte Wirtschaftssektoren und/oder für größere Organisationen, einschließlich solcher des öffentlichen Bereichs. Dabei dürfe aber nicht vergessen werden, dass der Einsatz von Datenschutzbeauftragten die gesetzlichen Befugnisse der Datenschutzaufsichtsbehörden - insbesondere auch am Fall der Vorabkontrolle - unberührt lasse. Gerade die Vorabkontrolle sei ein wesentlicher Bestandteil der Vereinfachung und helfe der Aufsichtsbehörde dabei, sich auf bestimmte Verarbeitungsprozesse bzw. Sektoren zu konzentrieren, die für die Privatsphäre von Individuen von besonderer Bedeutung seien. Wenn man die Möglichkeit erwäge, den Datenschutzbeauftragten allgemein zu etablieren, d.h. insofern von administrativer zu interner Aufsicht überzugehen, müsse man sowohl die bisher in den Mitgliedstaaten gesammelten Erfahrungen als auch die in den einzelnen Ländern geltenden Gesetze und deren Rechtskultur insgesamt berücksichtigen.

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.

In diesem Sinne sind jedenfalls die vorgesehenen Bestimmungen zum arbeitsrechtlichen Beendigungsschutz sowie den verpflichtend zu vergebenden zeitlichen Ressourcen als positiv zu bewerten, wenn auch wünschenswert wäre, dass eine Freistellung in noch größerem Ausmaß erfolgen würde.

Weiters wäre eine gesetzliche Klarstellung wünschenswert, dass die Vermittlung von Fachkenntnissen sowie die Weiterbildung kostenmäßig durch den Betriebsinhaber zu tragen ist.

Zu kritisieren ist allerdings, dass im gegenständlichen Gesetzesentwurf der öffentliche Bereich nicht von der Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten betroffen ist. Es ist nicht einsichtig, warum sich diese Verpflichtung ausschließlich auf den privaten Bereich beziehen soll, da Fragen des Datenschutzes und der Privatsphäre im öffentlichen Bereich mindestens die gleiche Bedeutung haben wie in der Privatwirtschaft.

Die ARGE DATEN fordert daher, dass die an sich sehr positive Regelung auch auf den öffentlichen Bereich erweitert wird.

Diskussionswert ist jedoch die Mitarbeitergrenze, ab dem ein Datenschutzbeauftragter verbindlich vorgeschrieben ist, diese könnte von 20 MA auf 50 MA angehoben werden.

(2.) Defacto Aufhebung der Registrierungs- und Vorabkontrolle

Die vorgesehenen Bestimmungen der §§ 20-22 DSG, welche eine Vorabkontrolle nur mehr automationsunterstützt mittels Internetanwendung vorsieht, werden von den „Erläuternden Bemerkungen“ als das Herzstück der Reform gepriesen.

Aus Sicht des Grundrechtsschutzes sind die geplanten Bestimmungen hingegen überaus kritisch zu betrachten. Offensichtlich soll diese Aufweichung des Vorabkontrollverfahrens eine Art Gegengewicht zur Innovation des betrieblichen Datenschutzbeauftragten bilden, womit jedenfalls dem Geist der EU-Datenschutzrichtlinie nicht entsprochen wird.

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

Gemäß dem geplanten § 20 DSG sollen Meldungen von Datenanwendungen, die nach Angabe des Auftraggebers nicht vorabkontrollpflichtig sind , nur mehr automationsunterstützt im Rahmen der Internetanwendung (§ 17 Abs. 1a) auf ihre Vollständigkeit und Plausibilität geprüft werden. Ergibt diese Prüfung keine Fehlermeldung, so ist die Meldung sofort zu registrieren.

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 6 a 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 § 22 a 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 Stichproben hinaus Verwendung finden wird.

Die europarechtliche Konformität der geplanten Bestimmung ist dabei mehr als fragwürdig: Erwägungsgrund 54 der EU-Datenschutzrichtlinie hält jedenfalls 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 Vollständigkeits- und Plausibilitätskontrolle gibt alleine in den Händen des Auftraggebers

liegt, ist jedenfalls aus datenschutzrechtlicher Sicht nicht tragbar und mit der EU-Datenschutzrichtlinie nicht vereinbar. Aus einer Stellungnahme der Art. 29 Gruppe zum Institut des betrieblichen Datenschutzbeauftragten heißt es, dass nicht vergessen werden dürfe, dass der Einsatz von Datenschutzbeauftragten die gesetzlichen Befugnisse der Datenschutzaufsichtsbehörden - insbesondere auch am Fall der Vorabkontrolle - unberührt lasse. Gerade die Vorabkontrolle sei ein wesentlicher Bestandteil der Vereinfachung und helfe der Aufsichtsbehörde dabei, sich auf bestimmte Verarbeitungsprozesse bzw. Sektoren zu konzentrieren, die für die Privatsphäre von Individuen von besonderer Bedeutung seien.

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

(3.) Datenverarbeitungsregister als Lobby-Organisation für Bürgerkarte?

Laut §17 Abs. 1a sollen in Zukunft Registrierungen nur mehr elektronisch mittels "Bürgerkarte" eingebracht werden.

Damit soll den Bürgern (den Datenverarbeitern) zur Erfüllung einer gesetzlichen Verpflichtung, ohne sachliche Notwendigkeit, ein bestimmtes technisches System aufgezwungen werden. Dies ist offenbar gleichheitswidrig und verletzt damit Verfassungsbestimmungen.

Hier entpuppt sich die für den Entwurf verantwortliche Behörde als Lobby-Organisation für das längst gescheiterte und höchst unsichere Projekt "Bürgerkarte".

Es muss in Zukunft weiterhin möglich sein, dass Anträge an das Datenverarbeitungsregister auf mehreren Wegen, jedenfalls per Post, Fax und eMail eingebracht werden können.

(4.) Kompetenzänderung hinsichtlich nicht automationsunterstützt verarbeiteter Daten

Inhaltlich positiv ist zu bewerten ist, dass § 2 des vorliegenden Entwurfs nunmehr auch Gesetzgebung und Vollziehung hinsichtlich nicht automationsunterstützt verarbeiteter Daten in die Bundeskompetenz verlagert. Dass hinsichtlich der nicht automationsunterstützten Verarbeitung von Daten kein bundeseinheitliches Schutzniveau existiert hat, war jedenfalls in dieser Form mit den europarechtlichen Vorgaben unvereinbar, die Reform überfällig.

In diesem Zusammenhang zu begrüßen ist auch, dass nunmehr – offenbar als Folge der kompetenzrechtlichen Änderung - auch der Begriff des „Verwendens von Daten“ auf nicht - automationsunterstützte Handhabungen von Daten ausgeweitet und zumindest diese Europarechtswidrigkeit beseitigt wurde. Zu hoffen ist, dass diese Gesetzesänderung sich auch in der künftigen Judikatur niederschlagen wird.

Jedenfalls zu kritisieren ist allerdings, dass die Begriffsbestimmung der Datenanwendung, die nur auf – zumindest teilweise - automationsunterstützte Prozesse Bezug nimmt, im Zuge

der Kompetenzbereinigung nicht angeglichen wurde, was insbesondere aufgrund des geplanten § 4 Abs 2 DSG 2000 in der Folge zu Problemen führt.

Seitens der ARGE DATEN wird jedenfalls verlangt auch eine umfassende Eingliederung von nicht-automationsunterstützten Verarbeitungsprozessen in das DSG 2000 vorzunehmen und die Bestimmung des § 4 Z 7 DSG 2000 auf nicht automationsunterstützte Prozesse auszuweiten.

Formal ist diese Kompetenzregelung als deplaziert zu bewerten. Sachlich wäre sie in den Kopetenzregelungen der Bundesverfassung zu beschließen. Mit dem Schritt im DSG verfassungsrechtliche Kompetenzregelungen einzubauen, wird wieder ein Schritt weg von Verwaltungs- und Verfasungsvereinfachung gemacht.

Es wird daher angeregt die Kompetenzbestimmung in das Bundesverfassungsgesetz zu regeln.

(5.) Einschränkung des Geltungsbereichs des DSG auf in Datenanwendungen verarbeitete Daten

Kritisch zu betrachten ist die geplante Bestimmung des § 4 Abs 2 DSG 2000, mit welcher die Regelungen des 2., 3. 5. und 8. Abschnitts des DSG auf die einer Datenanwendung unterzogenen oder in einer Datei verwendeten Daten beschränkt werden.

Die betreffenden Abschnitte regeln die Verwendung von Daten, Datensicherheit, Betroffenrechte und Rechtsschutz. Als Datei gilt eine strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind. Als Datenanwendung, die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind

Sofern personenbezogene Daten nicht in diesem Rahmen verwendet werden, sind daher weite Bereiche des DSG 2000 aufgrund des vorliegenden Entwurfs nicht anwendbar. Auch wenn sich dies aus dem gesetzlichen Zusammenhang - auch schon aufgrund der bisherigen Gesetzeslage weitgehend so ergeben hat, ist darauf zu verweisen, dass diese Situation aus Sicht des Datenschutzes unbefriedigend und mit den europarechtlichen Vorgaben nicht vereinbar ist.

Im Sinne Art. 2 der EU-Datenschutzrichtlinie gilt nämlich als „Verarbeitung personenbezogener Daten" ("Verarbeitung") jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Da – wie bereits festgehalten - § 4 Abs 1 Z 9 DSG 2000. nicht auf nicht-automationsunterstützte Prozesse ausgeweitet wurde, ergibt sich im Zusammenhang, dass nicht-automationsunterstützte Prozesse, die nicht im Rahmen einer Datenanwendung erfolgen, europarechtswidrig aus weiten Bereichen des DSG 2000 ausgenommen werden sollen.

Hinsichtlich der Verwendung von Daten ist insbesondere zu kritisieren, dass durch die Nichtanwendung von § 7 Abs 1 DSG 2000 bei personenbezogenen Daten, die nicht einer Datenanwendung unterzogen oder in einer Datei verwendet werden, der Grundsatz der

zweckmäßigen Verwendung von Daten nicht mehr ausdrücklich gesetzlich normiert ist. Dies widerspricht insbesondere Erwägungsgrund 28 der EU-Datenschutzrichtlinie, welcher festhält, dass die Verarbeitung personenbezogener Daten dem angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen hat. Die Zwecke müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein.

Hinsichtlich des 5. Abschnitts des DSG- der rechtlichen Behelfe- ist festzuhalten, dass die Möglichkeiten zur Geltendmachung von Betroffenenrechten im Rahmen des DSG 2000 hinsichtlich der genannten Verarbeitungsprozesse ausdrücklich ausgeschlossen werden soll.

Auch das erweist sich aufgrund der Bestimmungen der EU-Datenschutzrichtlinie als nicht europarechtskonform. Art. 12 sowie Art. 14 zu Auskunftsrecht und Widerspruchsrecht nehmen ausdrücklich Bezug auf den Verarbeitungsbegriff der EU-Datenschutzrichtlinie, der- wie bereits beschrieben- einen umfassenderen Geltungsbereich als jener des DSG 2000 hat.

Weiters wird gemäß Art. 22 der Richtlinie garantiert, dass jede Person bei der Verletzung der Rechte, die ihr durch die für die betreffende Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen kann. Zwar behilft sich die österreichische Rechtsordnung damit, dass bei datenschutzrechtlichen Verletzungen, die keinem Rechtsbehelf des DSG 2000 zugänglich sind, Ansprüche eventuell auf die Bestimmungen von §16 ABGB bzw. §1328a ABGB gestützt werden können, doch sind diese Regelungen – im Gegensatz zu den Rechtsbehelfen des DSG- keineswegs deutlich an die Bestimmungen des DSG angeknüpft und generell als Schutzmechanismen zugunsten der Privatsphäre ausgerichtet. Selbst wenn anhand dieser Bestimmungen Datenschutzrechte in jenen Bereichen, die nicht dem 3. Abschnitt des DSG unterliegen, geltend gemacht werden könnten, muss jedenfalls auch die Frage gestellt werden, welchen Sinn eine derartige Aufsplitterung haben soll.

Aufgrund des österreichischen Verarbeitungsbegriffs, der nicht- automatisierte Prozesse europarechtswidrigerweise nicht erfasst, ist die geplante Bestimmung daher jedenfalls abzulehnen.

(6.) Einschränkung des Widerspruchsrechts

Keineswegs so deutlich, wie durch die Erläuternden Bemerkungen ausgeführt, ist im Ergebnis die vorgeschlagene Änderung des § 8 Abs 2 DSG. Dieser lautet in der gegenwärtigen Fassung: *„Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.“*

Der zweite Satz würde mit der vorgeschlagenen Gesetzesänderung entfallen. Ausgehend von der Klarstellung der „Erläuternden Bemerkungen“, dass bei öffentlich zugänglichen Daten gemäß § 28 Abs 2 DSG ohnedies auch ohne Behauptung der Verletzung

schutzwürdiger Interessen ein Widerspruchsrecht zusteht, ist zwar richtig, dass der Wegfall des zweiten Satzes keine Einschränkung des Widerspruchsrechts zur Folge hätte.

Allerdings ist anzumerken, dass hinsichtlich der Frage der widerspruchsweisen Datenlöschung aus öffentlichen Dateien gegenwärtig gerichtliche Verfahren anhängig sind und der Entfall des zweiten Satzes der genannten Regelung jedenfalls nicht als Einschränkung des Widerspruchsrechts gemäß § 28 Abs 2 DSG interpretiert werden darf.

(7.) Keine Verletzung von schutzwürdigen Geheimhaltungsinteressen bei Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde

Die vorgeschlagene Änderung der Bestimmung betrifft § 8 Abs 3 Z 5 DSG, der die Zulässigkeit zur Datenverwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde daran gebunden hat, dass die Daten rechtmäßig ermittelt wurden. Diese Voraussetzung soll nunmehr fallen, was nicht einsichtig ist.

Im Gegensatz zu den Ausführungen der „Erläuternden Bemerkungen“ ist dies nämlich nicht nur eine Klarstellung im Rahmen der europarechtlichen Vorgaben, welche nunmehr auch die Ermittlung von Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde einbeziehen soll, sondern würde die Regelung in der geplanten Form auch die Verwendung rechtswidrig ermittelter Daten rechtfertigen.

Zu befürchten ist weiters, dass hinkünftig jede Form von Datenerhebung und sonstiger Datenverwendung damit gerechtfertigt wird, man wolle sich etwa gegen künftige Prozesse, Forderungen absichern, etc….

Es sollte daher jedenfalls klargestellt sein, dass keine „vorratsweise“ Datenerhebung aufgrund dieser Bestimmung zulässig sein kann, sondern tatsächlich ein entsprechendes Verfahren bereits anhängig sein bzw. zumindest in konkreter Vorbereitung sein muss. Dass diese Fragen in der Praxis zu Problemen führen werden, ist nur evident, weshalb die Beibehaltung der bisherigen Regelung sicherlich die vernünftigste Variante wäre.

(8.) Kein Auskunftsrecht nach DSG bei öffentlich einsehbaren Daten

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 jedenfalls 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 durchaus 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 damit bisher zum letztendlich absurden Resultat, dass dort, wo personenbezogene Daten öffentlich gemacht wurden, umgekehrt 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.

(9.) Unnötiger Formalismus bei Beschwerden an die Datenschutzkommission

Durch die vorgesehene Bestimmung des § 31 Abs 3 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 dienen offensichtlich nur dazu, Bürger, die keine Datenschutz- und Verwaltungsexperten sind, vom Beschwerderecht auszuschließen. 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 fachkundig geschulte 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 sehr eindeutig hervor, dass die Möglichkeit, bei der nationalen datenschutzrechtlichen Kontrollstelle Eingaben machen zu können, gesichert sein muss. Von formellen Beschränkungen ist dabei nicht die Rede.

Es ist jedenfalls auch 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 inhaltlichen Voraussetzungen verfügten.

Falls das Interesse dahin gehen sollte, die DSK, die sich offenbar nicht mit Eingaben einfacher Bürger abgeben möchte, zu entlasten, sei darauf verwiesen, dass – durch notwendige Erlassung von Verbesserungsaufträgen- 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 in der Geschäftsordnung der Datenschutzkommission zu beseitigen.

(10.) Keine Verletzung von schutzwürdigen Geheimhaltungsinteressen bei Unterstützung des Nationalrats, Bundesrats oder eines Landtags bei Ausübung parlamentarischer Kontrolltätigkeit

Der geplante § 8 Abs 3 Z 2b DSG soll festlegen, dass keine Verletzung von schutzwürdigen Geheimhaltungsinteressen vorliegt, wenn zur Unterstützung des Nationalrats, Bundesrats oder eines Landtags bei Ausübung parlamentarischer Kontrolltätigkeit pesonenbezogene Daten verwendet werden.

Dazu ist anzuführen, dass die Zulässigkeit derartiger Verwendungen sich schon aus der geltenden Rechtslage ergeben hat.

Die Verpflichtung von Ämtern, an parlamentarischen Untersuchungsausschüssen mitzuwirken, ergibt sich schon aus der Verfassungsbestimmung des Art. 53 B-VG. Gerichte und andere Behörden sind verpflichtet, dem Ersuchen dieser Ausschüsse um Beweiserhebungen Folge zu leisten, auf Verlangen haben alle öffentlichen Ämter ihre Akten dem Ausschuss vorzulegen. Eine ähnliche Bestimmung findet sich auch nochmals in dem Gesetz über die Verfahrensordnung der Untersuchungsausschüsse. Die gebotenen Beweise werden dabei durch sogenannte "Beweisbeschlüsse" des Ausschusses erhoben.

Gegen derartige Verwendungen ist an sich natürlich aus datenschutzrechtlicher Sicht wenig einzuwenden, sofern auch garantiert ist, dass die Informationen durch die Ausschussmitglieder geheimgehalten werden. Auch gegen eine nochmalige gesetzliche Klarstellung spricht nichts, sofern an der geltenden Rechtslage tatsächlich Zweifel bestehen.

Weiters ist festzuhalten, dass die Überprüfung von Tätigkeiten von Organen der Gesetzgebung durch die Datenschutzkommission ausgeschlossen ist und eine Überprüfung durch die DSK dem Grundsatz der Gewaltentrennung widersprechen würde.

In Bezug auf die Auslegung der Kompetenzen der Datenschutzkommission vertritt die Rechtsprechung in dieser Hinsicht eine restriktive Auffassung (*dazu etwa VfgH B 2687/95, 12.3.1998*): Ausgenommen von der Überprüfung durch die DSK sind somit nicht nur Akte der Gesetzgebung oder der Rechtsprechung an sich sondern sämtliche Handlungen, welche durch Organe der Rechtsprechung oder der Gesetzgebung gesetzt werden.

Die Problematik besteht nicht grundsätzlich darin, dass Legislative und Judikative der Überprüfung durch die DSK entzogen sind. Bezüglich der Gerichtsbarkeit gibt es eigene Verfahrensvorschriften, wie mit Datenschutzfragen umzugehen ist, diese finden sich in § 85 Gerichtsorganisationsgesetz. Problematisch ist allerdings, dass es für Betroffene bei Verletzungen von Datenschutzrechten durch Organe der Gesetzgebung keinerlei Möglichkeit gibt, dagegen vorzugehen. Der Überprüfung durch die DSK sind diese Organe - wie beschrieben- entzogen, es gibt allerdings auch keine eigenständigen Regelungen, die es Bürgern ermöglichen, sich dagegen zu wehren, dass Organe der Gesetzgebung in ihre Datenschutzrechte eingreifen.

Daher wäre wünschenswert, dass, wenn nun die Übermittlung von Daten an parlamentarische Untersuchungsausschüsse ausdrücklich geregelt werden soll, bezüglich Datenschutzverletzungen auch Rechtsbehelfe für Betroffene eingerichtet werden.

Zusammenfassend sollte auch - aufgrund gegenwärtiger Vorkommnisse - beachtet werden, dass Datenschutz nicht zur reinen Anlassgesetzgebung und zu einem politischen Instrumentarium verkommen sollte.

Teil IV.: 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 geprüft werden.