

## ÄNDERUNG DES DATENSCHUTZGESETZES

### BERICHT UND ANTRAG DES REGIERUNGSRATES

VOM 11. DEZEMBER 2007

Sehr geehrter Herr Präsident

Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen eine Änderung des Datenschutzgesetzes vom 28. September 2000 (BGS 157.1). Es geht im Wesentlichen um die Anpassung der kantonalen Datenschutzgesetzgebung an das bilaterale Abkommen vom 26. Oktober 2004 zwischen der Schweiz und der Europäischen Gemeinschaft über die Assoziierung mit Schengen/Dublin. Das Inhaltsverzeichnis:

Das Wichtigste in Kürze .....	2
I. Ausgangslage.....	3
1. Europäische Union.....	3
a. Bilaterale II.....	3
b. Abkommen von Schengen/Dublin.....	4
c. Inhalt von Schengen/Dublin .....	5
d. Auswirkungen von Schengen/Dublin auf die Gesetzgebung des Kantons.....	6
e. Auswirkungen auf das Datenschutzrecht.....	6
2. Bund.....	8
II. Vorgehen bei der Anpassung des kantonalen Rechts.....	10
III. Vernehmlassungsverfahren.....	10

IV. Inhalt der Revision des Datenschutzgesetzes .....	12
1. Allgemeines.....	12
2. Geltungsbereich .....	13
3. Befugnisse der Datenschutzstelle .....	14
4. Unabhängigkeit der Datenschutzstelle .....	16
5. Aufgabenbereich der Datenschutzstelle.....	18
V. Finanzielle und personelle Auswirkungen .....	19
VI. Zu den einzelnen Bestimmungen des Datenschutzgesetzes.....	21
VII. Antrag .....	30

### **Das Wichtigste in Kürze**

Die Änderungen sind insbesondere aus zwei Gründen notwendig:

a. Die bilateralen Abkommen vom 26. Oktober 2004 zwischen der Schweiz und der Europäischen Gemeinschaft über die Assoziierung mit Schengen/Dublin verlangen nach einem höheren Datenschutz-Standard. Begründet wird dies insbesondere mit dem Anschluss der Schweiz an das Schengener Informationssystem SIS – einer europaweiten Fahndungsdatenbank – und an die elektronische Datenbank «Eurodac» zur Erkennung von mehrfach gestellten Asylgesuchen. In diesem Zusammenhang müssen Bearbeitungen von Personendaten den Datenschutzvorschriften der EU genügen. Gefordert wird unter anderem eine Vorabkontrolle durch die Datenschutzstelle bei besonders heiklen Bearbeitungen von Daten, die Möglichkeit, Entscheide im Bereich des Datenschutzes gerichtlich anzufechten, und die völlige Unabhängigkeit der Datenschutzstelle.

b. Am 24. März 2006 wurde das Bundesgesetz über den Datenschutz vom 19. Juni 2006 (SR 235.1, vgl. BBI 2006 3547) geändert und der Bundesbeschluss über den Beitritt der Schweiz zum *Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung* angenommen (vgl. BBI 2006 3649). Dies hat ebenfalls Auswirkungen auf die Kantone. Sie werden verpflichtet, unabhängige Kontrollorgane

einzuführen, denen namentlich eine Klagebefugnis oder die Befugnis, Rechtsverletzungen einer gerichtlichen Behörde zur Kenntnis zu bringen, zusteht. Das Datenschutzgesetz muss auch an diese Vorgaben angepasst werden. Der Regierungsrat prüfte, ob aufgrund der übergeordnet geforderten Unabhängigkeit die Wahl des oder der Datenschutzbeauftragten durch den Kantonsrat anstatt durch den Regierungsrat zu erfolgen hat. Zudem diskutierte er für sie bzw. ihn eine bestimmte Amtsdauer mit der Möglichkeit der Wiederwahl (z.B. 4 oder 6 Jahre). Der Regierungsrat lehnt beides ab und schliesst sich der analogen Regelung des Bundes an. Zudem steht für den Regierungsrat die im Datenschutzgesetz verankerte Unabhängigkeit im Vordergrund. Diese ist im Alltag konsequent umzusetzen und bot in der Vergangenheit keine Probleme. Der Regierungsrat ist bereit, im Rahmen des Budgets (als Steuerungsinstrument) der Datenschutzstelle zwei Stellen zu bewilligen. Somit ist die Zustimmung des Kantonsrates notwendig. *Analog* den Pragma-Ämtern soll die Datenschutzstelle vom Kantonsratsbeschluss betreffend Bewilligung von Personalstellen in den Jahren 2005 - 2008 (BGS 154.212) ausgenommen werden. Zu beachten ist in diesem Zusammenhang, dass die Datenschutzstelle nicht umfassend zu einer PRAGMA-Verwaltungsstelle wird. Es werden nur gewisse Elemente übernommen bzw. solche kommen analog zur Anwendung. So handelt es sich denn auch beim Budget nicht um ein *Globalbudget*.

Die obigen Ausführungen beziehen sich auch auf die allgemeinen Datenbearbeitungen von öffentlichen Zuger Organen (somit auf solche, die keinen Bezug zu «Schengen» haben).

c. Der Regierungsrat hält sich, wo immer möglich, an die entsprechenden Änderungen anderer Kantone, die die erforderlichen Anpassungen bereits vorgenommen haben (insbesondere unter Berücksichtigung von Bund und LU).

## **I. Ausgangslage**

### **1. Europäische Union**

#### **a. Bilaterale II**

Am 26. Oktober 2004 schloss die Schweiz die bilateralen sektoriellen Abkommen mit der Europäischen Gemeinschaft über landwirtschaftliche Verarbeitungserzeugnisse, Statistik, Umwelt, Medien, Pensionen, Schengen/Dublin, Betrugsbekämpfung und

Zinsbesteuerung ab (sogenannte «Bilaterale II»; vgl. Botschaft des Bundesrates vom 1. Oktober 2004, in: BBl 2004 5965 ff.). Die Umsetzungsgesetzgebung des Bundes wurde von den Eidgenössischen Räten gleichzeitig mit dem Genehmigungsbeschluss zu den Abkommen verabschiedet. Die bilateralen Abkommen II können unabhängig voneinander in Kraft treten. Bislang sind das Abkommen über landwirtschaftliche Verarbeitungserzeugnisse (30. März 2005), das Abkommen über die Vermeidung der Doppelbesteuerung von ehemaligen EU-Beamten (31. Mai 2005) sowie das Abkommen über die Zinsbesteuerung (1. Juli 2005) in Kraft getreten.

#### **b. Abkommen von Schengen/Dublin**

Für den Datenschutz von besonderer Bedeutung sind die bilateralen Abkommen zwischen der Schweiz und der Europäischen Gemeinschaft über die Assoziierung mit Schengen/Dublin (nachfolgend: Schengen/Dublin). An Schengen/Dublin sind alle EU-Mitgliedstaaten beteiligt, Grossbritannien und Irland allerdings nur in Teilbereichen. Mit Norwegen und Island nehmen auch zwei Nicht-EU-Mitgliedstaaten an Schengen/Dublin teil. Das Schweizer Stimmvolk stimmte am 5. Juni 2005 der Assoziierung mit Schengen/Dublin zu. Die Assoziierungsabkommen beschlagen Bereiche, die innerstaatlich teilweise im Kompetenzbereich der Kantone liegen oder deren Vollzug den Kantonen obliegt. Neben dem Bund sind folglich auch die Kantone gefordert, die Abkommen rechtlich und organisatorisch umzusetzen.

In aller Regel müssen völkerrechtliche Abkommen zum Zeitpunkt ihres Inkrafttretens in innerstaatliches Recht umgesetzt sein. Die Abkommen von Schengen/Dublin sehen hingegen ein spezielles Vorgehen zu ihrer Umsetzung und Weiterentwicklung vor. Dies hängt einerseits damit zusammen, dass sie kontinuierlich weiterentwickelt werden sollen und diese Änderungen von der Schweiz und damit auch von den Kantonen zu übernehmen sind. Andererseits wird Schengen/Dublin erst dann definitiv in Kraft gesetzt, wenn die Schweiz *alle* entsprechenden Bestimmungen des einschlägigen EU-Schengen-Acquis (Schengener Abkommen und die auf dieser Grundlage erlassenen Regelungen) ins innerstaatliche Recht übernommen hat. Die bisherigen Mitglieder des Schengen-Raums entscheiden, nach einer entsprechenden Kontrolle der korrekten Umsetzung aller einschlägigen Bestimmungen im Bund und in den Kantonen, durch einstimmigen Beschluss über die definitive Inkraftsetzung der Abkommen. Die Kontrollen sind in zwei Phasen aufgeteilt: In einer ersten Phase wird die Umsetzung der Vorgaben von Schengen/Dublin anhand von Fragekatalogen sowie der eingereichten Schengen-relevanten Gesetzgebung überprüft. Die zweite Phase umfasst Kontrollen vor Ort durch eine von der EU eingesetzte Kontrollgruppe,

die sich aus Juristinnen und Juristen, Informatikerinnen und Informatikern, sowie Datenschutzbeauftragten der EU-Länder zusammensetzt.

Das Abkommen von Schengen sieht damit folgende Phasen bis zum definitiven Inkrafttreten vor:

1. Mitwirkung der Schweiz an der Weiterentwicklung des Schengen-Acquis ab Unterzeichnung des Abkommens im Oktober 2004.
2. Inkrafttreten der Abkommen nach Ratifizierung durch die Vertragsparteien.
3. Prüfung der korrekten und vollständigen Umsetzung des Abkommens von Schengen durch die bisherigen Schengen-Mitglieder.
4. Beschluss der Schengen-Mitglieder über die Inkraftsetzung des Abkommens in Bezug auf die Schweiz.

Nach dem heutigen Wissensstand sind die EU-Kontrollen über die Umsetzung des Abkommens durch die Schweiz in der ersten Hälfte des Jahres 2008 zu erwarten. Mit einem Inkrafttreten der Abkommen für die Schweiz ist im Oktober 2008 zu rechnen.

Falls zum Beispiel der Kanton Zug die Kontrollen nicht bestehen würde, bestünde das Risiko, dass der Schweiz eine weitere Frist zur Umsetzung gesetzt würde. Die Abkommen von Schengen/Dublin würden dann für den Bund und alle übrigen Kantone erst zu einem späteren Zeitpunkt in Kraft gesetzt, womit der Zugang der Polizeiorgane zum erweiterten SIS ebenfalls für alle – somit für Bund und alle übrigen Kantone – erst später zustande käme.

### **c. Inhalt von Schengen/Dublin**

Im Rahmen der Schengener Zusammenarbeit haben die teilnehmenden Staaten ihre Personenkontrollen an den Binnengrenzen aufgehoben und gleichzeitig zur Stärkung der inneren Sicherheit eine Reihe von Ausgleichsmassnahmen beschlossen. Dazu gehören die Verstärkung der Kontrollen an den Aussengrenzen des Schengener Raums, eine gemeinsame Visumpolitik für Kurzaufenthalte, die Verbesserung der Zusammenarbeit im Bereich der Rechtshilfe in Strafsachen sowie die Intensivierung der grenzüberschreitenden Polizeizusammenarbeit. Zu den wichtigsten Instrumenten der Zusammenarbeit zählt das Schengener Informationssystem SIS, eine europaweite Fahndungsdatenbank. Dieses System enthält heute über 16 Millionen Datensätze über gesuchte und vermisste Personen und über verschwundene Gegenstände wie Fahrzeuge oder Waffen sowie über 20'000 verdeckte Überwachungen von Personen. Es besteht aus einem Zentralrechner, der in Strassburg steht, an den

die nationalen Schengener Informationssysteme (N-SIS) angeschlossen sind. Insgesamt können über 30'000 Polizeidienststellen SIS-Daten abfragen bzw. eingeben.

Die Dubliner Zusammenarbeit ist ein Element des europäischen Asylraums. Mit ihr soll sichergestellt werden, dass Asylsuchende im Dubliner Raum nur ein Asylgesuch stellen können. Das Abkommen von Dublin legt die Kriterien fest, gemäss denen der für die Behandlung eines Asylgesuches zuständige Staat bestimmt wird, und sorgt so für eine ausgewogene Verteilung der Asylsuchenden auf die Dublin-Staaten. Dank der elektronischen Datenbank «Eurodac» können mehrfach gestellte Asylgesuche erkannt werden (vgl. Botschaft des Bundesrates vom 1. Oktober 2004, in: BBI 2004 5968).

**d. Auswirkungen von Schengen/Dublin auf die Gesetzgebung des Kantons**

Neben Änderungen bezüglich Waffenrecht sind die bedeutendsten Änderungen aufgrund der Abkommen von Schengen/Dublin im Bereich des Datenschutzes notwendig.

**e. Auswirkungen auf das Datenschutzrecht**

Im Rahmen der Assoziierung der Schweiz mit Schengen/Dublin muss jede Bearbeitung von Personendaten, die unter den sogenannten ersten Pfeiler der EU fällt, den Anforderungen der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie; EU-DSRL; Amtsblatt der Europäischen Gemeinschaften Nr. L 281 vom 23. November 1995, S. 31 ff.) genügen (vgl. dazu Botschaft des Bundesrates vom 1. Oktober 2004, in: BBI 2004 6108). Unter den ersten Pfeiler fallen Grenzkontrollen, Visa, Feuerwaffen, teilweise Betäubungsmittel und Asyl. Anders als beim ersten Pfeiler der EU gelangt die EU-Datenschutzrichtlinie im Bereich des dritten Pfeilers der EU, somit bezüglich der polizeilichen und justiziellen Zusammenarbeit, *nicht unmittelbar zur Anwendung*. Hier enthält das Schengener Durchführungsübereinkommen selber die spezifischen, direkt anwendbaren Schutzvorschriften über die Datenbearbeitungen im Zusammenhang mit dem SIS und ausserhalb des SIS.

Das Zuger Datenschutzgesetz vom 28. September 2000 (BGS 157.1) muss an diese europäischen Grundlagen angepasst werden, soweit das kantonale Recht die persönlichen Daten nicht bereits im selben Ausmass schützt.

Die EU-Datenschutzrichtlinie enthält Vorschriften, die über das im Zeitpunkt des Vertragsschlusses geltende schweizerische und in den meisten Fällen auch kantonale Datenschutzrecht hinausgehen (FRANK SEETHALER, in: Basler Kommentar zum Datenschutzgesetz, 2. Aufl., Basel 2006, N 84 zur Entstehungsgeschichte des DSG). Insbesondere die Regelung von Artikel 28 der EU-Datenschutzrichtlinie über die Datenschutz-Kontrollstelle hat Auswirkungen auf die kantonale Datenschutzgesetzgebung. Artikel 28 lautet wie folgt:

*«Artikel 28 Kontrollstelle*

*(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.*

*Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.*

*(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.*

*(3) Jede Kontrollstelle verfügt insbesondere über:*

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;*
- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;*
- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie.*

*Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.*

*(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.*

*Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmässigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäss Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.*

*(5) Jede Kontrollstelle legt regelmässig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.*

*(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäss Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.*

*Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.*

*(7) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.»*

Auch für die Datenbearbeitung in den Bereichen des dritten Pfeilers gilt grundsätzlich, dass die Datenübermittlung erst beginnen kann, wenn unabhängige Kontrollinstanzen eingerichtet sind (Art. 126 SDÜ).

## **2. Bund**

Die Eidgenössischen Räte haben am 24. März 2006 die Revision des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992 (SR 235.1; in: BBl 2006 3547 ff.) verabschiedet sowie den Bundesbeschluss über den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Übermittlung (nachfolgend: Zusatzprotokoll; abgedruckt in: BBl 2003 2167 ff.) angenommen.

Grund für die Revision waren in den Jahren 1999 und 2000 von den Eidgenössischen Räten angenommene Motionen, die einerseits eine Verstärkung der Transparenz beim Beschaffen von Daten und andererseits eine formelle gesetzliche Grundlage für Online-Verbindungen zu Datenbanken des Bundes sowie einen Mindestschutz bei der Bearbeitung von Daten durch die Kantone beim Vollzug von

Bundesrecht verlangten. Im Zuge dieser Revision wurden einige Bestimmungen des Bundesgesetzes angepasst, damit die Schweiz dem oben erwähnten Zusatzprotokoll beitreten konnte.

Die Gesetzesänderung sieht für Datenbearbeitende die Verpflichtung zur aktiven Information der betroffenen Personen vor, wenn besonders schützenswerte Daten und Persönlichkeitsprofile beschafft werden. Bei Personendaten, die nicht besonders schützenswert sind und auch kein Persönlichkeitsprofil darstellen, muss für die betroffenen Personen zumindest erkennbar sein, dass Daten beschafft werden. Die Revision umfasst ausserdem gewisse Änderungen hinsichtlich der Pflicht zur Meldung von Datensammlungen, und sie stärkt die Position von Personen, die sich einer Bearbeitung der sie betreffenden Daten widersetzen. Sie legt ausserdem die Mindestanforderungen fest, denen die Kantone im Bereich des Datenschutzes genügen müssen, wenn sie Bundesrecht vollziehen, und sie verstärkt die Kontrollmöglichkeiten, wenn beim Vollzug von Bundesrecht Personendaten bearbeitet werden.

Mit dem Ziel einer Anpassung des DSG an das Zusatzprotokoll werden zudem die Kriterien für eine rechtmässige grenzüberschreitende Bekanntgabe von Daten festgelegt, und dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten wird ein Beschwerderecht im Rahmen der Aufsicht über Bundesorgane zugestanden. Weiter sind gewisse Bestimmungen des Bundesgesetzes fortan im Rahmen des Vollzugs von Bundesrecht durch kantonale Organe nicht nur dann subsidiär anwendbar, wenn überhaupt keine kantonalen Datenschutzvorschriften bestehen, sondern auch dann, wenn solche Vorschriften keinen angemessenen Schutz gewährleisten. Angemessen ist der Schutz dann, wenn er die Anforderungen erfüllt, die sich aus dem Europaratsübereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (nachfolgend: Europaratsübereinkommen STE Nr. 108; SR 0.235.1) und dem Zusatzprotokoll ergibt.

Das revidierte Eidg. Datenschutzgesetz tritt am 1. Januar 2008 in Kraft. Das Zusatzprotokoll dürfte für die Schweiz am 1. April 2008 in Kraft treten.

Aus der beschriebenen Gesetzesänderung ergibt sich beim kantonalen Recht insbesondere bezüglich der Beschwerdelegitimation der Datenschutzstelle, deren Unabhängigkeitsstatus und der grenzüberschreitenden Bekanntgabe von Daten ein Handlungsbedarf.

## **II. Vorgehen bei der Anpassung des kantonalen Rechts**

Auf interkantonomaler Ebene haben die Plenarversammlungen der Konferenz der Kantonsregierungen (KdK) und der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) am 1. Oktober 2004 beziehungsweise am 7. April 2005 Konzepte zur Mitwirkung der Kantone bei der Weiterentwicklung und bei der Umsetzung der Abkommen von Schengen und Dublin beschlossen. Das Generalsekretariat der KKJPD übernahm die Funktion der internationalen Kontrollstelle, die den Stand der Umsetzung in den Kantonen prüft, entsprechende Meldungen an den Bund verfasst und Informationen des Bundes an die Kantone weiterleitet. Am 8. November 2004 wurden die Kantone dazu eingeladen, Ansprechspartner auf technischer und politischer Ebene zu benennen, die den Informationsfluss zwischen KKJPD/KdK und den einzelnen Kantonen sowie die rechtzeitige Beschlussfassung innerhalb der einzelnen Kantone sicherstellen sollen. Zudem liess die KdK durch den unabhängigen Datenschutzexperten Dr. Beat Rudin eine Wegleitung zur Umsetzung von Schengen/Dublin in den Kantonen ausarbeiten (BEAT RUDIN, Umsetzung Schengen/Dublin in den Kantonen: im Auftrag der KdK erstellte Datenschutz-Wegleitung, Basel 2006; nachfolgend: Wegleitung).

## **III. Vernehmlassungsverfahren**

Das Ergebnis des Vernehmlassungsverfahrens lässt sich wie folgt zusammenfassen:

### **1. Kantonale Stellen**

Das Verwaltungsgericht und die Sicherheitsdirektion (wegen der Polizei besonders betroffen) unterbreiten keine Änderungsanträge. Das Obergericht schlägt lediglich eine Präzisierung bei § 2 Abs. 2 Bst. a vor.

### **2. Gemeinden**

Neun Gemeinden reichen eine weitgehend identische Stellungnahme ein. Aufgrund des übergeordneten Rechts "können wir uns - allerdings ohne grosse Begeisterung - mit den vorgeschlagenen Änderungen des Datenschutzgesetzes einverstanden erklären." Sie teilen die Auffassung des Regierungsrates, dass der Datenschutzbeauftragte durch den Regierungsrat anzustellen ist. Es spreche nichts gegen eine

Erhöhung der bisherigen Stellenprozente unter gleichzeitiger Kostenübernahme durch den Kanton. Sie bedauern, dass die Stellvertretung im Gesetz selber nicht geregelt ist. Es werde teilweise bei der Konkretisierung der Unabhängigkeit des Beauftragten - im Bericht - über das Ziel (Unabhängigkeit) hinausgeschossen. Sie sehen zudem nicht ein, weshalb sich eine betroffene Person direkt an die kantonale Datenschutzstelle wenden könne, wenn eine Gemeinde für ihren Aufgabenbereich eine eigene unabhängige Datenschutzstelle geschaffen habe.

Der Stadtrat von Zug hält kurz - ohne weitere Begehren - fest, dass er "ohne grosse Begeisterung" aufgrund des übergeordneten Rechts den vorgeschlagenen Änderungen zustimme. Der Gemeinderat Menzingen hat keine Einwände gegen die Gesetzesänderung, lehnt jedoch die Aufstockung der Personalstellen ab.

### 3. Im Kantonsrat vertretene Parteien

#### 3.1. CVP

Die Anpassungen aufgrund des übergeordneten Rechts sind unbestritten. Sie macht Vorbehalte bezüglich der geforderten völligen Unabhängigkeit der Datenschutzstelle. Sie ist nicht bereit, dem Datenschutzbeauftragten eine grössere Unabhängigkeit als den Zuger Gerichten einzuräumen. Sie schlägt - in Übereinstimmung mit dem Regierungsrat - die Wahl durch den Regierungsrat vor. Von einer Amtszeitbeschränkung und Wahlbestätigung durch den Kantonsrat möchte die CVP absehen. Der Ausbau auf zwei Vollzeitstellen sei zur Zeit nicht begründet.

#### 3.2. FDP

Sie ist allgemein besorgt über das Ausmass und den Aufwand, der für den Datenschutz betrieben wird. Sie stimmt der geforderten Unabhängigkeit nicht zu. Diese Stelle habe ebenfalls dem Stellenplafond zu unterstehen und es sei ihr kein Globalbudget einzuräumen. Sie dürfe nicht unabhängiger sein als die dritte Gewalt im Staat. Die Rechtsstellung der Ombudsstelle und des Datenschutzbeauftragten müsse gleichermassen ausgestaltet sein. Sie wendet sich gegen die personelle Aufstockung. Die grenzüberschreitende Datenbekanntgabe gemäss § 10a müsse restriktiv erfolgen und dürfe auch dann nicht stattfinden, wenn dadurch in schwerwiegender Weise gegen die schweizerische Rechtsordnung oder gegen den Ordre Public verstossen würde.

### 3.3. SVP

Die SVP ist ebenfalls besorgt über den Aufwand, der mit dem Datenschutz betrieben wird. Sie verlangt, dass die Wahl des Datenschutzbeauftragten durch den Regierungsrat alle sechs Jahre erfolgt und durch den Kantonsrat bestätigt wird. Die Stellen seien im Stellenplafond zu belassen und die Datenschutzstelle habe dem Kantonsrat jährlich ein detailliertes Budget vorzulegen.

### 3.4. Alternative

Sie unterstützt die Revision und begrüsst die völlige Unabhängigkeit der Datenschutzstelle sowie die sich daraus ergebenden Konsequenzen. Im Gegensatz zum Regierungsrat schlägt die Alternative vor, dass der Datenschutzbeauftragte für eine Amtsdauer von sechs Jahren vom Kantonsrat gewählt wird. Dies sichere ihm die für die Amtsausübung unabdingbare Unabhängigkeit.

### 3.5. SP

Bei Ernennung des Datenschutzbeauftragten durch den Regierungsrat auf unbestimmte Zeit bestehe die Gefahr, dass diese Aufgabe verpolitisiert wird. In § 28 der EU-Datenschutzrichtlinien würden aber ein völlig unabhängiges Kontrollorgan und eine völlig unabhängige Aufsichtsbehörde verlangt. Da jedoch in der Praxis die Unabhängigkeit nie in Frage gestellt worden sei, verzichtet die SP darauf, dass der Datenschutzbeauftragte für eine bestimmte Amtsdauer durch den Kantonsrat zu wählen ist. Die SP begrüsst, dass die Stellen des Datenschutzbeauftragten nicht mehr dem KRB betreffend Bewilligung von Personalstellen unterstellt sind.

## **IV. Inhalt der Revision des Datenschutzgesetzes**

### **1. Allgemeines**

Im jeweiligen Kompetenzbereich müssen die massgebenden internationalen Erlasse (EU-DSRL, SDÜ, Europaratsübereinkommen STE Nr. 108 und Zusatzprotokoll) auch von den Kantonen angewendet werden. Damit müssen die Kantone ein gleichwertiges Schutzniveau wie dasjenige der erwähnten Erlasse gewährleisten. Nach schweizerischem Recht versteht man unter gleichwertigem Datenschutz, dass die in Frage

stehenden Regelungen einander in ihrer Gesamtheit entsprechen (BBI 2004 6241). In der Folge werden die wesentlichen Punkte der vorgeschlagenen Revision erläutert. Dabei wird grundsätzlich anhand der von KdK bzw. KKJPD verabschiedeten Wegleitung vorgegangen. Diese Wegleitung gibt den «minimal-standard» an, der zur Einhaltung der bundesrechtlichen bzw. EU- und Europaratsvorgaben vorzusehen ist. Ein «Weniger» ist daher nicht zulässig, könnte diesfalls doch das Risiko bestehen, dass der Anschluss an das SIS verweigert wird.

Die Vorlage geht auf der anderen Seite aber nirgends weiter als die Vorgaben der KdK.

## **2. Geltungsbereich**

Die im Auftrag der KdK erstellte Wegleitung hält in Ziffer 2.4 zum Geltungsbereich der Datenschutzgesetze Folgendes fest: «Es ist zulässig, eine Ausnahme für hängige Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit vorzusehen, wenn die dadurch zur Anwendung gelangende Prozessordnung die nötigen Regelungen (insbesondere zur Beschaffung und Bekanntgabe von Personendaten sowie zu den Rechten der betroffenen Personen und zur Aufsicht) enthält (...). Auf keinen Fall kann das erstinstanzliche Verwaltungsverfahren aus dem Geltungsbereich ausgenommen werden; auch das verwaltungsinterne Rekursverfahren (Rekursinstanz Departement/Direktion oder Exekutive) rechtfertigt eine Ausnahme nicht.»

Auf Bundesebene ist der Geltungsbereich des Bundesgesetzes über den Datenschutz wie folgt definiert: Gemäss Artikel 2 Abs. 2 Bst. c des Bundesgesetzes über den Datenschutz (Eidg. DSG) ist dieses Gesetz nicht anwendbar auf hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren. Mit der Regelung im Eidg. DSG ist im Bund für den Schutz von Personendaten bei der verwaltungsinternen Rechtspflege das Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968 (VwVG; SR 172.021) massgebend, wogegen bei erstinstanzlichen Verwaltungsverfahren, die an und für sich ebenfalls in den Geltungsbereich des VwVG fallen, das Eidg. DSG massgebend ist. Der Bundesgesetzgeber wollte offensichtlich den Geltungsbereich des Eidg. DSG nicht allzu stark einschränken. Die Botschaft des Bundesrates zum Eidg. DSG hält dazu Folgendes fest: «Weil praktisch ausnahmslos alle Verwaltungstätigkeiten durch Verfügungen erledigt

werden, könnten sich die Bundesorgane den Pflichten des DSG entziehen, und die betroffenen Personen wären gänzlich schutzlos» (BBl 1988 II 443 f.).

Gemäss § 3 Abs. 2 Bst. a findet das Datenschutzgesetz des Kantons Zug (BGS 157.1, DSG-ZG) keine Anwendung auf hängige Verfahren der Zivil-, Verwaltungs- und Strafrechtspflege (§ 3 Abs. 2 Bst. a DSG-ZG). Es ist aber aufgrund der Materialien über den Wortlaut hinaus – und analog zu Art. 2 Abs. 2 Bst. c Eidg. DSG –, in erstinstanzlichen Verwaltungsverfahren klarerweise anzuwenden. Zu diesem Schluss kam denn auch ein von der Konferenz der Direktionssekretäre im Januar 2007 verabschiedetes Grundlagenpapier («Berichterstattung über das Recht auf Akteneinsicht», verfasst von PATRICK LINDAUER, Zug, 29. Januar 2007, S. 1 f.).

Zusammenfassend lässt sich somit festhalten, dass der Geltungsbereich des kantonalen Datenschutzgesetzes demjenigen des eidgenössischen Datenschutzgesetzes entspricht. Aus Gründen der Rechtssicherheit ist es aber angebracht, nun ausdrücklich festzuhalten, dass die in § 3 Abs. 2 Bst. a DSG-ZG genannten Ausnahmen für das erstinstanzliche nicht strittige Verwaltungsverfahren nicht gelten. Damit ergibt sich zum geltenden Recht *keine* Änderung, da nun nur ausdrücklich festgehalten wird, was bereits bis anhin anerkannter Praxis war.

Auf das *streitige* Verwaltungsverfahren (Einsprache- bzw. Beschwerdeverfahren) ist hingegen *nicht das Datenschutzgesetz*, sondern das Verwaltungsverfahrensrecht anwendbar. Auch hier ergibt sich *keine Änderung* zum geltenden Recht und zur bisherigen Praxis.

### **3. Befugnisse der Datenschutzstelle**

Gemäss Artikel 1 Ziff. 2 Bst. a des Zusatzprotokolls und Artikel 28 Abs. 3 der EU-Datenschutzrichtlinie muss das unabhängige Kontrollorgan über umfassende Untersuchungsbefugnisse, wirksame Einwirkungsbefugnisse und eine Klage- oder Anzeigebefugnis bei Verstössen gegen das Datenschutzrecht verfügen.

Unter der Bezeichnung «umfassende Untersuchungsbefugnisse» sind die Befugnisse – ungeachtet allfälliger Geheimhaltungspflichten – Ermittlungen durchzuführen, alle für die Erfüllung des Kontrollauftrages erforderlichen Informationen über Datenbearbeitungen einzuholen, Einsicht in alle Unterlagen zu nehmen, Besichtigungen

durchzuführen und sich Bearbeitungen vorführen zu lassen, zu nennen (Wegleitung, Ziff. 7.3.a). Das kantonale Datenschutzgesetz in der geltenden Fassung gesteht der Datenschutzstelle die genannten Untersuchungsbefugnisse in genügender Weise zu.

Einen Vorbehalt gilt es einzig bezüglich der Kontrolle des grenzüberschreitenden Datenverkehrs anzubringen. Gestützt auf das europäische Recht (Art. 12 Übereinkommen und Art. 2 Ziff. 1 Zusatzprotokoll sowie Art. 25 f. EU-Datenschutzrichtlinie) ist der Grundsatz festzuhalten, dass die grenzüberschreitende Übermittlung von Personendaten an Empfangende, für die das Übereinkommen nicht gilt, nur dann zulässig ist, wenn das Recht im Staate der Empfangenden ein adäquates Datenschutzniveau gewährleistet (Art. 2 Ziff. 1 Zusatzprotokoll: «einen angemessenen Schutz für die beabsichtigte Datenübermittlung»). Weiter ist im Sinne von Art. 2 Ziff. 2 Zusatzprotokoll zu regeln, unter welchen Bedingungen Personendaten ins Ausland bekannt gegeben werden dürfen, wenn es an einer Gesetzgebung fehlt, die den verlangten Schutz garantiert. Aus Art. 2 Ziff. 2 Bst. b Zusatzprotokoll ergibt sich ausserdem, dass die zuständige Behörde überprüfen muss, ob die Schutzmassnahmen angemessen sind, wenn die Gesetzgebung des Empfängerstaates keinen genügenden Schutz bietet. Es besteht also eine Informationspflicht gegenüber der Datenschutzstelle. Zweck dieser Informationspflicht ist es, dem Datenschutzbeauftragten beim grenzüberschreitenden Datenverkehr die Möglichkeit zu geben, seine Kontrollaufgaben wahrnehmen zu können.

Es gibt keine Vorschrift über einen Minimalsatz an Einwirkungsbefugnissen. Es ist erforderlich, dass das Kontrollorgan mit den gesetzlich festgelegten Einwirkungsbefugnissen in ihrer Gesamtheit tatsächlich Wirksamkeit entfalten kann. Als Beispiele werden in der Literatur die Befugnis zur Vorabkontrolle von heiklen Datenbearbeitungen, zur Anordnung der Sperrung, Löschung oder Vernichtung von Daten oder des vorläufigen oder endgültigen Verbots einer Datenbearbeitung, zur Verwarnung oder Ermahnung der Verantwortlichen oder die Möglichkeit, an das Parlament oder eine andere politische Institution zu gelangen, genannt (Wegleitung, Ziff. 7.3b; RENÉ HUBER, in: Basler Kommentar zum DSG, Vorbemerkungen zum 5. Abschnitt, N 27). Die Befugnis zur Vorabkontrolle von heiklen Datenbearbeitungen fehlt im Datenschutzgesetz des Kantons Zug. Sie muss daher eingefügt werden. Der Datenschutzstelle fehlt zudem die Möglichkeit, die im Verfahren gemäss § 20 Abs. 3 DSG-ZG gefällten Entscheide des Gemeinderats oder des Regierungsrats anzufechten, um datenschutzrechtlich erforderliche Massnahmen durchsetzen zu können. Die Daten-

schutzstelle wird gemäss geltendem Recht lediglich über den gefällten Entscheid informiert (§ 20 Abs. 3 DSG-ZG).

Ebenfalls nur rechtlich unverbindliche Empfehlungen abgeben konnte - wie im Kanton Zug - bis anhin der Eidgenössische Datenschutzbeauftragte (vgl. Art. 27 Abs. 4 Eidg. DSG). Im Rahmen der Änderung des Bundesgesetzes über den Datenschutz vom 24. März 2006 wurde nun aber Artikel 27 DSG dahingehend geändert, dass bei Ablehnung einer Empfehlung die Angelegenheit durch den Beauftragten dem Departement oder der Bundeskanzlei zum Entscheid vorgelegt werden kann. Der Entscheid wird den betroffenen Personen neu in Form einer Verfügung mitgeteilt, bezüglich welcher der Beauftragte berechtigt ist, Beschwerde zu führen (Art. 27 Abs. 5 und 6 Eidg. DSG in der revidierten Fassung).

Im kantonalen Datenschutzgesetz müssen die Einwirkungsbefugnisse des Datenschutzbeauftragten ebenfalls an die europäischen Vorgaben angeglichen werden. Um den Anforderungen insbesondere der EU-Datenschutzrichtlinie zu genügen, ist deshalb ein Beschwerderecht der Datenschutzstelle gegen Entscheide, die in Anwendung des Datenschutzgesetzes ergangen sind, vorzusehen. Der Bund hat dasselbe Vorgehen gewählt (vgl. BBl 2004 7154 und 7159).

Zu diesem Zweck hat das Organ sich in einen Entscheid verbindlich zu äussern, ob es der Empfehlung der Datenschutzstelle nachkommen will oder nicht. Andernfalls hat die Datenschutzstelle die Möglichkeit, ihre früher ergangene Empfehlung, oder Teile davon, dem Gemeinderat (gemeindliche Angelegenheit) oder dem Regierungsrat (kantonale Angelegenheit) zum Entscheid zu unterbreiten. Im weiteren Rechtsmittelverfahren kommt der Datenschutzstelle Parteistellung zu.

#### **4. Unabhängigkeit der Datenschutzstelle**

Artikel 28 der EU-Datenschutzrichtlinie schreibt ein öffentliches Kontrollorgan vor, das seine Aufgaben in «völliger Unabhängigkeit» wahrnimmt. Das ebenfalls massgebende Europaratsübereinkommen STE Nr. 108 verlangt, dass Datenbearbeitungen durch eine «völlig unabhängige» Aufsichtsbehörde überwacht werden müssen.

Zur Gewährleistung der völligen Unabhängigkeit des Datenschutz-Kontrollorgans werden in der Wegleitung (S. 23 f.) wie auch in der Literatur (RENÉ HUBER, Basler

Kommentar zum DSG, N 24 ff. zu Vorbemerkungen vor dem 5. Abschnitt) folgende Punkte angeführt:

1. a. Wahl durch das Parlament auf eine Amtsdauer von vier bis sechs Jahren oder  
b. Wahl durch die Exekutive auf eine Amtsdauer von sechs bis acht Jahren mit Vorbehalt der Genehmigung durch das Parlament oder  
c. Wahl durch die Exekutive auf eine Amtsdauer von acht Jahren.
2. Anstellungsverhältnis, das nur unter erschwerten Bedingungen aufgelöst werden kann.
3. Eigenes Budget, das vom Kontrollorgan erstellt und ohne Regierungsintervention dem Parlament zum Entscheid vorgelegt wird.
4. Administrative Zuordnung zu Parlament oder Staatskanzlei.

Der Bund hat mit der Änderung des Bundesgesetzes über den Datenschutz vom 24. März 2006 den Eidgenössischen Datenschutzbeauftragten nun ausdrücklich der Bundeskanzlei zugeordnet und ihm neu ein eigenes Budget zugestanden (Art. 26 Abs. 3 rev-Eidg. DSG). Er wird aber nach wie vor vom Bundesrat auf unbestimmte Amtsdauer gewählt.

Der Datenschutzbeauftragte wird heute - wie auf Bundesebene - vom Regierungsrat auf unbestimmte Zeit ernannt (§ 18 DSG; i. V. m. § 1 Abs. 4 des Personalgesetzes [BGS 154.21]). Diese Lösung hat sich bewährt. Entscheidend ist, dass der Datenschutzstelle - wie im geltenden Recht - auch in Zukunft eine gesetzliche Unabhängigkeit eingeräumt wird. Diese muss nicht nur auf Gesetzesstufe eingeräumt, sondern in der Rechtswirklichkeit auch konsequent umgesetzt werden. Regierungsrat und Verwaltung halten sich strikte an diesen Unabhängigkeitsstatus der Datenschutzstelle. Der Regierungsrat lehnt daher weitergehende Lösungen wie eine bestimmte Amtsdauer oder gar die Wahl durch den Kantonsrat ab.

Die Datenschutzstelle verfügt heute noch nicht über ein eigenes Budget für Personal- und Sachressourcen. Angesichts der hohen Anforderungen, die an die Unabhängigkeit des Datenschutzbeauftragten gestellt werden, muss sie – wie der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Art. 26 Abs. 3 rev. Eidg. DSG) und die übrigen kantonalen Datenschutzstellen (etwa Aargau, Basel-Landschaft, Freiburg, Schaffhausen, Schwyz, Uri, Zürich) – aufgrund der europäischen Vorgaben über ein eigenes Budget verfügen. Die Datenschutzstelle muss dieses ohne Intervention der Staatskanzlei bzw. des Regierungsrats direkt dem Kantonsrat zur Entscheidung vorlegen können.

## 5. Aufgabenbereich der Datenschutzstelle

Der Aufgabenbereich wird durch die europäischen Vorgaben *deutlich* erweitert. Es fällt zusätzlicher Aufwand in den folgenden Bereichen an:

### **Anfragen**

(seitens der privater Personen und den Verwaltungsstellen)

Die bisherigen Erfahrungen in den Schengen-Staaten haben gezeigt, dass zudem die Anfragen Betroffener markant zunehmen wird, geht es doch um die Einspeisung in europaweit abrufbare Datenbanken. Dies tangiert und interessiert die Bevölkerung wesentlich stärker als die bisherigen rein lokal auf Zug bezogenen polizeilichen Systeme. Werden nun aber die Personendaten von Zugerinnen und Zugern von Sizilien bis ans Nordkap und von Frankreich bis Polen zugänglich (und in naher Zukunft auch in den 10 neuen EU-Staaten), so steigt das Interesse nach Schutz- und Kontrollmassnahmen. Es ist ja zu bedenken, dass es sich bei SIS-Daten nicht nur um Angaben zu möglichen Straftätern handelt, sondern vielmehr auch Personendaten völlig unschuldiger Personen erfasst werden, so etwa waffenerwerbende Personen, Zeugen, Opfer oder Eigentümerdaten bei Diebstahl von Wertsachen oder Fahrzeugen.

### **Schulung**

Insbesondere sind alle Mitarbeitenden der Zuger Polizei, die über einen Zugang zum SIS verfügen, bezüglich Datenschutz speziell zu schulen.

### **Kontrollen**

Insbesondere sind *regelmässig Kontrollen* der Datenbearbeitungen im Bereich Schengen vorzunehmen, die den von den Schengen-Staaten etablierten internationalen Standards entsprechen müssen.

### **Rechtsmittelverfahren**

Im Weiteren ist mit einer Zunahme der Arbeitsbelastung aufgrund der Beschwerdebefugnis der Datenschutzstelle zu rechnen.

### **Medien**

Aufgrund der Brisanz des Inhaltes des SIS ist mit einer grösseren diesbezüglichen Medienbeachtung zu rechnen.

### **Hinweis bezüglich der Situation in anderen Kantonen**

Wird die Frage der erforderlichen Personalstellen mit der Situation von Datenschutzstellen in anderen Kantonen verglichen, so ist zu beachten, dass Organisation und Aufgabenverteilung in anderen Kantonen zum Teil ganz unterschiedlich gehandhabt werden. Es kann somit nicht einfach der Personaletat der kantonalen Datenschutzstellen miteinander verglichen werden. Vielmehr ist die Gesamtsituation zu beachten. So ist etwa auf Folgendes hinzuweisen:

Verfügt der Datenschutzbeauftragte des *Kantons Zürich* zurzeit über 7.2 Personalstellen (ab 01. Januar 2009: 8.2 Personalstellen), so ist zu beachten, dass zudem die folgenden Städte über eigene Datenschutzstellen verfügen: Stadt Zürich (2.7 Personalstellen), Winterthur (0.6 Personalstellen), Uster und Dietikon.

Im *Kanton Bern* muss *jede Gemeinde* von Gesetzes wegen zwingend eine eigene unabhängige Datenschutzstelle einrichten, womit sich der Aufwand der kantonalen Datenschutzstelle entsprechend reduziert.

Der *Kanton Freiburg* verfügt neben der Datenschutzbeauftragten über eine Datenschutzkommission, die selber sehr aktiv Geschäfte betreut. Zudem haben die Gemeinden Bulle, Freiburg, Marly und Villars-sur-Glâne eigene unabhängige Datenschutzstellen.

## **V. Finanzielle und personelle Auswirkungen**

Die personellen Ressourcen der Datenschutzstelle betragen zur Zeit 75 Stellenprozent (des Datenschutzbeauftragten) und zusätzlich 45 Stellenprozent (des juristischen Mitarbeiters), wobei letztere im Rahmen eines Aushilfsvertrages bis zum 30. September 2008 befristet sind. Die Datenschutzstelle konnte bereits bisher viele der im Gesetz vorgeschriebenen Aufgaben aufgrund mangelnder Ressourcen nicht erfüllen (Ausbildung, Kontrollen, Öffentlichkeitsarbeit). Zudem hat sie ohne zusätzliche Ressourcen *neue Aufgaben* zu übernehmen (Begleitung der Umsetzung der Datensicherheitsverordnung und der Online-Verordnung). Die Datenschutzstelle muss unter Berücksichtigung der Schengen/ Dublin-Vorgaben insgesamt zwei Personalstellen zur Verfügung haben. Ab Inkrafttreten dieses Gesetzes benötigt die Datenschutzstelle die Umwandlung der heutigen befristeten 0.45 Planstelle (Aushilfe) in eine unbefristete Stelle sowie – darüber hinaus – zusätzliche 0.8 Planstelle. Die

Mehrkosten durch diese Vorlage betragen rund Fr. 190'000.-- (inkl. Umwandlung der bisherigen Aushilfestelle in eine unbefristete). Dabei nahm der Regierungsrat jährliche Personalkosten pro Stelle von Fr. 150'000.-- an (inkl. Umwandlung der Aushilfestellen: 1.25 x Fr. 150'000.-- ergibt gerundet Fr. 190'000.--). Der Rat geht davon aus, dass der Sachaufwand ungefähr gleich bleiben wird.

Die obigen Ausführungen zu den zusätzlichen Personalstellen dienen nur dazu, die finanziellen Auswirkungen dieser Vorlage zu erläutern. Wie aus Ziff. II der Gesetzesvorlage hervorgeht, beantragt der Regierungsrat, das Personal der Datenschutzstelle nicht dem Kantonsratsbeschluss betreffend Bewilligung von Personalstellen in den Jahren 2005 - 2008 (BGS 154.212) zu unterstellen. Die finanzielle Steuerung erfolgt aufgrund von § 18 Abs. 5 und 6 der Gesetzesänderung über das eigene Budget der Datenschutzstelle, das vom Kantonsrat (und nur von diesem) zu genehmigen ist. Diese gesetzliche Regelung ist vergleichbar mit dem System der Pragmaämter.

A)	Investitionsrechnung		2008	2009	2010
1.	Gemäss Budget oder Finanzplan:				
	• bereits geplante Ausgaben				
	• bereits geplante Einnahmen				
2.	Gemäss vorliegendem Antrag:				
	• effektive Ausgaben				
	• effektive Einnahmen				

B)	Laufende Rechnung		2008	2009	2010
3.	Gemäss Budget oder Finanzplan:		292'000	228'700	231'900
	• bereits geplanter Aufwand				
	• bereits geplanter Ertrag				
4.	Gemäss vorliegendem Antrag:		304'000*	418'700*	421'900*
	• effektiver Aufwand				
	• effektiver Ertrag				

\* Annahmen: Inkrafttreten dieser Änderungen per 01. November 2008; Umwandlung der bisherigen Aushilfsanstellung per 01. November 2008, Anstellung der zusätzlichen Mitarbeitenden per 01. Januar 2009.

## VI. Zu den einzelnen Bestimmungen des Datenschutzgesetzes

### I.

#### § 3

Zu Abs. 2 Bst. a)

Die in § 3 Abs. 2 Bst. a DSG genannte Ausnahme gilt nicht für erstinstanzliche Verfahren der Verwaltungsrechtspflege (vgl. vorne IV. / 2). In solchen Verfahren ist somit auch nach geltendem Recht das Datenschutzgesetz zu beachten. Zwar fehlt, anders als in Art. 2 Abs. 2 Bst. c Eidg.-DSG eine Bestimmung, die das DSG *explizit* für erstinstanzliche Verwaltungsverfahren anwendbar erklärt. Der kantonale Gesetzgeber wollte aber in § 3 Abs. 2 Bst. a DSG klarerweise nur *streitige* Verfahren von der Anwendung des DSG ausschliessen, *nicht aber die Datenbearbeitung der Verwaltung bis zum Erlass einer erstinstanzlichen Verfügung*. Dies ergibt sich aus dem Bericht und Antrag des Regierungsrats vom 7. Dezember 1999 zum Datenschutzgesetz (S. 13 f. der Vorlage Nr. 733.1 - 10042). Als streitige Verwaltungsverfahren gelten jene Verfahren, in denen eine verfahrensbeteiligte Partei ein Rechtsmittel (Einsprache oder Beschwerde) gegen eine in erster Instanz ergangene Verfügung bzw. einen in erster Instanz ergangenen Entscheid einlegt. Die beantragte Änderung führt demnach nicht zu einer Erweiterung des Anwendungsbereichs des DSG, sondern dient *lediglich der Klarstellung* der jetzt schon geltenden Rechtslage und *demnach der Rechtssicherheit*.

Die Ergänzung, wonach auch hängige Verfahren der internationalen Rechtshilfe von der Anwendbarkeit des DSG ausgenommen sind, dient der Klarstellung.

#### § 4

Zu Bst. d

Aufgrund der europäischen Vorgaben ist explizit im Gesetz zu verankern, dass bei jeglicher Datenbearbeitung das Prinzip der Verhältnismässigkeit und der Grundsatz von Treu und Glauben zu beachten sind.

Da diese Grundsätze im schweizerischen Verwaltungsrecht bereits auch bisher stets zu beachten waren, ergibt sich hier in der Praxis keinerlei Änderung.

#### § 7

Artikel 7 des Europaratsübereinkommens STE Nr. 108 und Artikel 17 der EU-Datenschutzrichtlinie verlangen, dass die Datenschutzgesetze die Gewährleistung der

Datensicherheit mittels angemessener technischer und organisatorischer Massnahmen *ausdrücklich* festhalten. Absatz 1 wird in diesem Sinn ergänzt.

Es ergibt sich materiell dadurch zum geltenden Recht keinerlei Änderung.

#### § 10a

Wie bereits erwähnt, ist gemäss Artikel 2 des Zusatzprotokolls und Artikel 25 der EU-Datenschutzrichtlinie im Gesetz festzuhalten, dass die grenzüberschreitende Übermittlung von Personendaten an Empfangende, für welche die massgebenden europäischen Datenschutzerlasse nicht gelten, nur dann zulässig ist, wenn beim Empfangenden mit anderen Mitteln ein angemessenes Datenschutzniveau sichergestellt ist. Die Formulierung von § 10a lehnt sich weitgehend an Artikel 6 Eidg. DSG in der Fassung gemäss Änderung vom 24. März 2006 an. Eine Abweichung ergibt sich insofern, als dort nur eine «schwerwiegende» Gefährdung ausgeschlossen werden soll. Es ist aber zu beachten, dass das kantonale Datenschutzgesetz ausschliesslich die Datenbearbeitung kantonaler und gemeindlicher öffentlicher Organe betrifft, sich das Bundesrecht hingegen auch auf die Datenbearbeitungen von Privaten bzw. Unternehmen bezieht. Zuger Organe dürfen durch Datenbekanntgabe ins Ausland – wenn sie denn ausnahmsweise je solche vornehmen sollten – grundsätzlich keine Gefährdung der Persönlichkeitsrechte von Privatpersonen bewirken. Bearbeiten Zuger Organe Daten im gemeindlichen, kantonalen oder allenfalls nationalen Kontext, so dürfen diese Bearbeitungen grundsätzlich keine Gefährdungen von Persönlichkeitsrechten von Zuger Bürgerinnen und Bürger bewirken. Es wäre nicht einzusehen, dass bei Datenbekanntgaben ins Ausland – die in der Regel ja viel heikler, da grundsätzlich unkontrollierbar, sind – weniger strenge Anforderungen gelten sollen als im schweizerischen Rahmen.

Absatz 1 verlangt als grundsätzliche Voraussetzung für eine gesetzeskonforme Datenübermittlung ins Ausland, dass die Gesetzgebung im Bestimmungsland einen angemessenen Schutz gewährleistet.

Absatz 2 enthält eine Liste von alternativen Bedingungen, unter denen die Bekanntgabe von persönlichen Daten ins Ausland ebenfalls erlaubt ist. Die Aufzählung ist *abschliessend*. Dadurch verdeutlicht der Entwurf die verschiedenen Möglichkeiten der Sicherstellung einer gesetzeskonformen Übermittlung und lässt die Inhaberinnen und Inhaber der Datensammlungen in der Wahl ihrer Mittel frei. Die Gesetzgebung im Empfängerstaat gewährleistet dann ein angemessenes Schutzniveau, wenn sie

den Anforderungen des Europaratsübereinkommens STE Nr. 108 entspricht. Darüber hinaus ist aber insbesondere auch zu berücksichtigen, wie diese Gesetzgebung in der Praxis umgesetzt wird.

Gemäss Absatz 2 Bst. a ist eine Bekanntgabe ins Ausland beim Fehlen einer Gesetzgebung mit angemessenem Schutz zulässig, wenn andere hinreichende Garantien vorliegen. Solche können sich beispielsweise aus einem Verhaltenskodex ergeben, das heisst aus einem Regelwerk, dem sich der Datenempfänger freiwillig unterstellen kann, wie etwa dem «Safe Harbor Privacy Framework», das zwischen der EU-Kommission und den USA ausgehandelt wurde (<http://www.export.gov/safeharbor/>). Auf europäischer Ebene ergibt sich aus Artikel 2 Absatz 2 Bst. b des Zusatzprotokolls, dass die zuständige Behörde überprüfen können muss, ob die Schutzmassnahmen angemessen sind, wenn die Gesetzgebung des Empfängerstaates keinen genügenden Schutz bietet. Aus diesem Grund muss eine Informationspflicht gegenüber der Datenschutzstelle vorgesehen werden.

Absatz 2 Bst. b betrifft eine konkrete ausservertragliche Situation. Der Ausdruck «im Einzelfall» ist in dem Sinn weit zu interpretieren, als nicht jede einzelne grenzüberschreitende Datenübermittlung, sondern auch eine Gesamtheit von Übermittlungen erfasst werden kann. So ist zum Beispiel die Übermittlung von mehreren Protokollen einer Arbeitsgruppe, der Personen verschiedener Länder angehören, zulässig, ohne dass die Zustimmung der betroffenen Personen zur Übermittlung der Dokumente jedesmal erneut eingeholt werden muss.

Absatz 2 Bst. c lässt die Datenbekanntgabe ins Ausland für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht zu. Der Begriff des öffentlichen Interesses ist im eidgenössischen und kantonalen Recht hinlänglich bekannt.

Eine Bekanntgabe gestützt auf Absatz 2 Bst. d ist einzig dann zulässig, wenn es darum geht, lebenswichtige Interessen der betroffenen Person selber zu schützen. Dabei wird es in der Regel um Situationen gehen, in denen die betroffene Person nicht in der Lage ist, ihre eigenen Interessen geltend zu machen, und vermutet werden kann, dass sie ihre Zustimmung zu einer solchen Datenübermittlung gegeben hätten. Als konkretes Beispiel ist hier an Datenbekanntgaben im Rahmen der

Tsunami-Katastrophe zu denken, als Daten möglicher Opfer zur Identifizierung von öffentlichen Organen in die Katastrophengebiete übermittelt wurden.

Gemäss Absatz 3 darf eine Datenbekanntgabe ins Ausland dann nicht erfolgen, wenn dadurch in schwerwiegender Weise gegen die schweizerische öffentliche Ordnung («Ordre public») verstossen würde.

Der Vollständigkeit halber ist darauf hinzuweisen, dass Art. 6 Abs. 2 Bst. f rev. Eidg. DSG nicht übernommen wurde. Art. 6 Abs. 2 Bst. f rev. Eidg. DSG besagt, dass Daten ins Ausland übermittelt werden dürfen, welche die betroffene Person der Allgemeinheit zugänglich gemacht und deren Bearbeitung nicht ausdrücklich untersagt hat. Diese Bestimmung stellt auf Art. 19 Abs. 1 Bst. c rev. Eidg. DSG ab. Laut Art. 19 Abs. 1 Bst. c rev. Eidg. DSG dürfen Bundesorgane Personendaten – auch wenn dafür eine Rechtsgrundlage nicht besteht – bekannt geben, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht und eine Bekanntgabe nicht ausdrücklich untersagt hat. Eine solche Bestimmung findet sich auch in § 5 Abs. 2 Bst. c DSG-ZG, wonach Organe besonders schützenswerte Personendaten bearbeiten dürfen, wenn die betroffene Person ihre Daten allgemein zugänglich gemacht hat. Da die Bestimmung über die Datenbekanntgabe ins Ausland aber eine Spezialbestimmung zum bestehenden § 5 DSG-ZG darstellt, müsste die Möglichkeit der Bekanntgabe von allgemein zugänglich gemachten Personendaten ins Ausland zusätzlich in das Gesetz aufgenommen werden. Andererseits stellt sich die Frage, ob überhaupt ein Bedarf für eine solche Bestimmung besteht. Dies ist insofern zu verneinen, als Organe anderer Staaten die allgemein zugänglich Daten auch selber finden können. Im Übrigen dürften Staaten, die keinen angemessenen Schutz für Personendaten garantieren, in der Regel einen wenig vorteilhaften Ruf geniessen. Das Unterlassen einer Bestimmung, welche die Datenbekanntgabe allgemein bekannter Daten zulässt, dürfte die kantonalen und kommunalen Organe davor schützen, Hilfsdienste für solche Staaten leisten zu müssen. Dies kann dem Kanton Zug nur dienen. Mithin ist auch die Aufnahme einer Bestimmung im Sinne von Art. 6 Abs. 2 Bst. f rev. Eidg. DSG zu verzichten.

#### § 15 Abs. 4

Der betroffenen Person kommen nach dem Datenschutzgesetz in der geltenden Fassung folgende Kontrollrechte zu: Auskunfts- inklusive Einsichtsrecht (§ 13 DSG) sowie, bei Vorliegen eines schützenswerten Interesses, das Recht auf Feststellung der Widerrechtlichkeit einer Datenbearbeitung, der Anspruch auf Unterlassung der

widerrechtlichen Datenbearbeitung und der Anspruch auf Beseitigung der Folgen einer widerrechtlichen Datenbearbeitung (§ 15 DSG). Sie kann insbesondere verlangen, dass die Daten berichtigt oder vernichtet werden und dass der Entscheid oder die Berichtigung Dritten mitgeteilt und veröffentlicht wird (§ 15 Abs. 1 und 2 DSG). Das Datenschutzgesetz des Kantons Zug verfügt also grundsätzlich über die erforderlichen, in den massgeblichen internationalen Rechtsgrundlagen beschriebenen Ansprüche der betroffenen Person (vgl. Art. 8 Unterabs. c Europaratsübereinkommen STE Nr. 108 und Art. 12 Unterabs. b EU-DSRL).

Abs. 4 betrifft Daten, bei denen aufgrund ihrer Natur weder die Richtigkeit noch die Unrichtigkeit festgestellt und bewiesen werden kann. Dies gilt insbesondere für Werturteile, bei denen der Sachverhalt unterschiedlich gewertet werden kann. Wird in einem Bericht beispielsweise einer Person vorgeworfen, sie habe «aggressiv» gehandelt und verlangt der Betroffene, diese Information über sie sei zu löschen, so muss zuerst abgeklärt werden, ob letztere richtig oder falsch ist. Spricht mehr für die Richtigkeit und löscht das Organ die fraglichen Daten deshalb nicht, so hat der Betroffene auf jeden Fall das Recht, einen Bestreitungsvermerk bei den fraglichen Daten anzufügen. Für solche Fälle fehlte der erforderliche Rechtsbehelf. Auch § 15 Abs. 1 Bst. b regelt solche Fälle nicht, da ein Werturteil nicht schon deshalb rechtswidrig ist, weil auch eine andere Folgerung möglich ist. Dies kann für die betroffene Person unbefriedigend, ja sogar schädlich sein, weil sie in solchen Fällen keine Berichtigung erwirken kann, obwohl eine andere als die in der Datensammlung enthaltene Beurteilung ebenso richtig ist. Zur Wahrung der Interessen der betroffenen Person ist der Rechtsbehelf des Bestreitungsvermerks zu schaffen (vgl. KdK-Wegleitung, Erläuterung Checkliste, Ziff. 4.5). Dabei wird der betroffenen Person das Recht zugestanden, in Fällen, in denen aufgrund der Natur der Daten weder die Richtigkeit noch die Unrichtigkeit festgestellt werden kann, einen Bestreitungsvermerk bei den entsprechenden Daten – nicht irgendwo anders – anzubringen.

## § 18

### Abs. 2

Wie vorne dargelegt (vgl. IV. Kapitel Ziff. 4) soll der Regierungsrat Anstellungsbehörde des Datenschutzbeauftragten für eine unbefristete Dauer sein.

Auch wenn dies im Gesetz nicht ausdrücklich festgehalten wird, so ist doch davon auszugehen, dass der Datenschutzbeauftragte diese Tätigkeit hauptberuflich, jedenfalls mindestens im Rahmen eines 50%-Pensums ausübt. Allfällige Nebenbeschäftigungen oder Nebenämter dürfen die Unabhängigkeit in keinem Fall tangieren. Näheres zu Nebenbeschäftigung und Nebenerwerb ist übrigens im Personalgesetz (§ 34 und § 35) und in der Personalverordnung (§ 15) bereits geregelt.

Die Frage der Stellvertretung ist durch die bzw. den Datenschutzbeauftragten im Rahmen der personellen Besetzung der Datenschutzstelle selber zu lösen. Es ist somit nicht vorgesehen, dass auch diese Person durch den Regierungsrat anzustellen ist.

#### Abs. 3

Dieser Absatz hält fest, dass die Datenschutzstelle ihre Aufgaben in vollständiger Unabhängigkeit zu erfüllen hat. Aufgabenbezogene Weisungen seitens der Verwaltung, des Regierungsrates oder des Kantonsrates sind nicht zulässig. Ebenfalls ausgeschlossen sind Vereinbarungen über Zielvorgaben, Arbeitsschwerpunkte, Jahresziele etc. mit der Verwaltung.

Bezüglich dem administrativen Bereich ist erstens zu beachten, dass es sich nicht um eine Unterstellung, sondern um eine Zuordnung zur Staatskanzlei handelt, zweitens, dass viele Fragen, die auf den ersten Blick als administrativer Natur erscheinen könnten, in der Praxis häufig inhaltlicher Natur sind, somit Auswirkungen auf die Unabhängigkeit haben. Sobald deshalb die Unabhängigkeit tangiert sein kann, handelt es sich nicht mehr um administrative Fragen. Dies ist etwa bei den folgenden Aspekten der Fall: Bewilligung einer allfälligen Nebenbeschäftigung oder eines Nebenamtes, Lohneinstufung bzw. Beförderungen, Fragen der Weiterbildung, Urlaubsgewährung, Zurverfügungstellung von Büroräumlichkeiten etc. Sind solche Fragen zu klären, sind sie durch den Regierungsrat und nicht durch die Staatskanzlei zu entscheiden (vgl. zum Ganzen: Basler Kommentar um DSG, N 46 ff. zu Art. 26 DSG).

#### Abs. 4

Die Frage der personellen und finanziellen Ressourcen tangiert die Unabhängigkeit und die Erfüllung der gesetzlichen Aufgaben entscheidend (Basler Kommentar zum DSG, N34 ff. zu Art. 26 DSG). Sowohl die europäische Datenschutz-Richtlinie wie auch das Zusatzprotokoll machen diesbezüglich Vorgaben. Die Wegleitung schreibt

denn auch vor, dass die Datenschutzstelle eine wirksame und eine aktive Aufgabenerfüllung ausüben können muss (vgl. Wegleitung, Ziff. 7.7). Eine ressourcenmässige Ausstattung, die nur ein passives Reagieren zulässt, ist weder mit den Vorgaben von Schengen, noch denjenigen des Zusatzprotokolls zu vereinbaren.

#### Abs. 5 und Abs. 6

Auch die Budgethoheit hat einen zentralen Konnex zu den Vorgaben bezüglich Unabhängigkeit (Basler Kommentar zum DSG, N 34 zu Art. 26 DSG). Die für die Aufgabenerfüllung erforderlichen finanziellen Mittel sind durch den Kantonsrat der Datenschutzstelle im Rahmen eines Budgets zur Verfügung zu stellen. Nach dem Kantonsratsbeschluss entscheidet diese selber über den Einsatz dieser Finanzmittel. Aus diesem Grunde ist neu das Personal der Datenschutzstelle nicht mehr dem Kantonsratsbeschluss betreffend Bewilligung von Personalstellen unterstellt (BGS 154.312, vgl. Ziff. II der Gesetzesänderung). Es ist eine finanzielle Steuerung - analog den Pragmaämtern - vorgesehen. Dabei ist zu beachten, dass die Unabhängigkeit in der Aufgabenerfüllung nicht eingeschränkt werden darf. Die zu erbringenden Leistungen ergeben sich direkt aus § 19 DSG.

#### § 18a

Wie bereits erwähnt, entspricht § 18a weitgehend den heutigen Bestimmungen. Ausdrücklich ist festzuhalten, dass auch diese Datenschutzstellen unabhängig sein müssen, damit sie den Anforderungen des übergeordneten Rechts entsprechen.

#### § 19

##### Zu Bst. h)

Auch dem Kantonsrat, der über die personellen und finanziellen Ressourcen der Datenschutzstelle entscheidet, ist Bericht zu erstatten.

##### Zu Bst. k)

Die Amtshilfepflicht in Bezug auf Kontrollorgane der Kantone, des Bundes und auch anderer Staaten muss aufgrund der Vorgaben von Schengen verankert werden (Art. 1 Ziff. 5a Zusatzprotokoll und Art. 28 Abs. 6 EU-DSRL). Die hier vorgeschlagene Erweiterung des Pflichtenhefts der Datenschutzstelle trägt diesen Vorgaben Rechnung. Es ist hier darauf hinzuweisen, dass Amtspflichten bezüglich Datenbearbeitungen mit Auslandsberührung von Zuger öffentlicher Organe nicht etwa über Bundesstellen abgewickelt werden, sondern direkt zwischen der ausländischen zuständigen Stelle und dem kantonalen Organ bzw. der Datenschutzstelle. Deshalb ist es auch

erforderlich, dass die Zuger Datenschutzstelle in grundsätzlicher Weise mit den Datenschutzstellen des Auslandes zusammen arbeitet.

Im Rahmen der Vernehmlassung wurde verschiedentlich angeregt, die Zusammenarbeit mit ausländischen Datenschutzbehörden solle durch den Eidg. Datenschutz- und Informationsbeauftragten (EDÖB) wahrgenommen werden. Hier ist darauf hinzuweisen, dass der EDÖB ausschliesslich für die Datenbearbeitung der Bundesverwaltung und der Privaten zuständig ist (Art. 2 Abs. 1 Eidg. DSG). Bezüglich der Kantone hat er *keinerlei Kompetenzen und Aufgaben*. Ist im Rahmen von konkreten Fällen gemeindlicher oder kantonaler Organe aufgrund eines internationalen Konnexes eine Zusammenarbeit mit ausländischen Datenschutzbehörden erforderlich, so muss die Zuger Datenschutzstelle direkt mit diesen kommunizieren können. Der EDÖB hat hier *keinerlei Zuständigkeit* – und es wäre auch gar nicht denkbar, dass der Zuger Gesetzgeber Aufträge an den EDÖB erteilen könnte, weil dessen Zuständigkeit abschliessend durch das Bundesrecht definiert ist.

#### § 19a

Die Aufgaben des Beauftragten für den Datenschutz werden erweitert. Artikel 20 der EU-Datenschutzrichtlinie verlangt ausdrücklich die gesetzliche Verankerung einer Vorabkontrolle durch das Kontrollorgan bei der Bearbeitung von Daten, die besondere Risiken für die Rechte und die Freiheit der betroffenen Personen mit sich bringen können.

Diesen Forderungen wird mit dem materiell neuen § 19a Rechnung getragen. Dabei kann sich das Verletzungspotenzial der Bearbeitungsmethode entweder aus der Art der Bearbeitung oder aus den zu bearbeitenden Daten ergeben. Kriterien für die Beurteilung des Risikos können zum Beispiel die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensitivität der Daten – schützenswerte oder besonders schützenswerte Personendaten – sein. Objekt der Vorabkontrolle können vor allem Projekte für IT-Systeme oder für Datenbanken sein. Soweit Informatikprojekte betroffen sind, entspricht dies bezüglich der kantonalen Verwaltung denn auch bereits dem geltenden Recht (vgl. § 4 Abs. 1 bzw. § 20 der Informatikverordnung [ITV] vom 29. Juni 2004 BGS 153.53); stellt somit nicht Neues dar, sondern eine Regelung, die sich bewährt hat.

## § 20

### Abs. 2 – 6

Gemäss Absatz 2 hat der Beauftragte für den Datenschutz bei der Feststellung von Datenschutzverletzungen die verantwortliche sowie deren vorgesetzte Behörde aufzufordern, die erforderlichen Massnahmen zu ergreifen. Diese Aufforderungen haben heute lediglich empfehlenden Charakter. Wie im Eidg. Datenschutzgesetz und in den Kantonen Luzern und Zürich vorgesehen, kann die Datenschutzstelle nun analog Empfehlungen in letzter Instanz einem Gericht zum Entscheid vorlegen.

Damit wird den massgebenden europäischen Bestimmungen Rechnung getragen, die verlangen, dass dem Kontrollorgan die Befugnis zusteht, wegen Datenschutzverstössen bei gerichtlichen Instanzen Klage zu erheben oder eine Anzeige einzureichen (Art. 1 Ziff. a Zusatzprotokoll und Art. 28 Abs. 3 EU-DSRL). Da es sich bei dieser zusätzlichen Befugnis der Datenschutzstelle hauptsächlich um eine Massnahme im Sinn einer *ultima ratio* handelt, dürfte es sich – wie bereits in Kapitel V. erläutert – bei den dadurch verursachten Beschwerdeverfahren nur um wenige Einzelfälle handeln.

Dass der Datenschutzstelle bei allfälligen durch sie ergriffenen Rechtsmitteln keine Kosten auferlegt werden, ist sinnvoll. Es würde wirtschaftlich gesehen nichts bringen, wenn ein kantonales Organ einem anderen kantonalen Organ Verfahrenskosten auferlegen würde. Im Übrigen kann diese Rechtslage nicht mit derjenigen verglichen werden, in denen ein öffentliches Organ im Rahmen von Rechtsmitteln zu Kostentragung gegenüber *privaten* Verfahrensbeteiligten verpflichtet wird. Im vorliegenden Rahmen geht es dagegen ausschliesslich um Verfahren zwischen verschiedenen kantonalen Organen.

Im Übrigen: s. die Ausführungen in Kapitel IV.3.

## § 20a

Die Pflicht zur Verschwiegenheit ist nicht schrankenlos, ist es doch gerade auch die Pflicht der Datenschutzstelle, die Öffentlichkeit über wichtige Anliegen zu informieren. Soweit somit die Bekanntgabe von Daten, Tatsachen oder Kenntnissen für die Aufgabenerfüllung erforderlich ist, darf – ja muss – der Datenschutzbeauftragte Informationen an die Öffentlichkeit bringen können, ohne dass er seinerseits eine Amtsgeheimnisverletzung begeht. Die vorliegende Bestimmung geht somit den Bestimmungen über das Amtsgeheimnis im Personalrecht vor.

§ 24 (wird nicht geändert)

Gemäss Artikel 24 der EU-Datenschutzrichtlinie müssen Sanktionen vorgesehen werden, die bei Verstössen gegen das Datenschutzgesetz anzuwenden sind. Der Regierungsrat sieht davon ab, neue strafrechtliche Normen - neben dem bisherigen § 24 - zu schaffen. Er legt nötigenfalls das Schwergewicht auf personalrechtliche Massnahmen.

Das Amtsgeheimnis wird zudem durch Artikel 320 des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (StGB; SR 311.0) genügend geschützt. So wird die Verletzung der datenschutzrechtlichen Schweigepflicht durch eine Amtsperson der kantonalen oder kommunalen Verwaltung fast immer schon durch Artikel 320 StGB erfasst (Basler Kommentar zum DSG, N 8 zu Vorbemerkungen zum 7. Abschnitt). Es erübrigt sich damit, Strafbestimmungen für Amtsgeheimnisverletzungen in das kantonale Recht aufzunehmen.

## II.

### Personalstellen

Die Unabhängigkeit der Datenschutzstelle soll auch bezüglich ihrer personellen Besetzung umgesetzt werden. Im Rahmen des durch den Kantonsrat genehmigten Budgets soll die Datenschutzstelle diesbezüglich bestimmen können (so ausdrücklich etwa auch in den Kantonen Uri und Zürich). Dies hat zur Folge, dass das Personal der Datenschutzstelle neu nicht mehr dem Kantonsratsbeschluss betreffend Personalstellen (BGS 154.212) untersteht.

## VII. Antrag

Es sei auf die Vorlage Nr. 1620.2 - 12567 einzutreten und ihr zuzustimmen.

Zug, 11. Dezember 2007

Mit vorzüglicher Hochachtung

REGIERUNGSRAT DES KANTONS ZUG

Der Landammann: Joachim Eder

Der Landschreiber: Tino Jorio

**Beilage:** «Übersicht über das Wahlverfahren des DSB in verschiedenen Kantonen»

300/sk