Kanton Basel-Landschaft Regierungsrat

Vorlage an den Landrat

Vom: 10.Juli 2007

Revision des Gesetzes über den Schutz von Personendaten (Datenschutzgesetz) vom 7. März 1991: Anpassung an Schengen/Dublin

Inhaltsverzeichnis

A Kurzübersicht

Eine Änderung des Gesetzes vom 7. März 1991 über den Schutz von Personendaten (Datenschutzgesetz)[1] ist aus zwei Gründen notwendig.

Zum einen verlangen die **bilateralen Abkommen** zwischen der Schweiz und der Europäischen Gemeinschaft über die **Assoziierung an Schengen/Dublin** nach einem erhöhten 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 in weiten Bereichen den Datenschutzvorschriften der EU – insbesondere der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (fortan: EU-Datenschutzrichtlinie) – genügen. Gefordert werden unter anderem ein geeigneter Schutz für sensitive Personendaten, die Verankerung der Grundsätze des Datenbearbeitens, eine Vorabkontrolle durch die Datenschutz-Kontrollstelle bei Datenbearbeitungen mit einem höheren Gefährdungspotenzial und eine wirksame Kontrolle durch ein völlig unabhängiges Datenschutzkontrollorgan.

Zum andern haben die Eidgenössischen Räte am 24. März 2006 – zusammen mit der Revision des Bundesgesetzes über den Datenschutz – den Beitritt der Schweiz zum **Zusatzprotokoll** vom 8. November 2001 **zum Europarats-Übereinkommen** zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung beschlossen. Dies hat ebenfalls Auswirkungen auf die Kantone. Sie werden verpflichtet, Aufsichtsbehörden zu schaffen, die ihre Aufgaben wirksam und in vollständiger Unabhängigkeit wahrnehmen, und für die Datenbekanntgabe in Staaten, welche der Europarats-Konvention 108 nicht beigetreten sind, strengere Voraussetzungen vorzusehen.

---

1 SGS 162.

B Ausgangslage

I. Sektorielle bilaterale Abkommen mit der EU

1. Bilaterale II

Am 26. Oktober 2004 schloss die Schweiz die bilateralen sektoriellen Abkommen mit der Europäischen Gemeinschaft über landwirtschaftliche Verarbeitungserzeugnisse, Statistik, Umwelt, Media, Pensionen, Schengen/Dublin, Betrugsbekämpfung und Zinsbesteuerung ab (so genannte «Bilaterale II»[2]). Die Umsetzungsgesetzgebung des Bundes wurde von den Eidgenössischen Räten am 17. Dezember 2004 gleichzeitig mit den Genehmigungsbeschlüssen verabschiedet[3].

Die bilateralen Abkommen II können unabhängig voneinander in Kraft treten. Bereits in Kraft sind das Abkommen über die verarbeiteten Landwirtschaftsprodukte (seit 30. März 2005), das Abkommen über die Ruhegehälter (seit 31. Mai 2005), das Abkommen über die Zinsbesteuerung (seit 1. Juli 2005), das Abkommen über die Media-Programme und das Umweltabkommen (seit 1. April 2006) sowie das Statistikabkommen (seit 1. Januar 2007)[4].

2. Abkommen von Schengen/Dublin

Für den Datenschutz von besonderer Bedeutung sind die bilateralen Abkommen zwischen der Schweiz und der Europäischen Gemeinschaft über die **Assoziierung an Schengen und an Dublin**[5]. 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 und Dublin teil. Das Schweizer Stimmvolk stimmte am 5. Juni 2005 im Rahmen eines fakultativen Referendums der Assoziierung mit Schengen/Dublin mit einem Ja-Stimmenanteil von 54.6% (BL: 58.3%) zu. Die Assoziationsabkommen beschlagen auch Bereiche, welche innerstaatlich 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.

Im Normalfall müssen völkerrechtliche Abkommen zum Zeitpunkt ihres Inkrafttretens in innerstaatliches Recht umgesetzt sein. Die Assoziierungsabkommen zu Schengen/Dublin sehen hingegen eine spezielle Konstellation hinsichtlich ihrer Umsetzung und Weiterentwick-

---

2 Vgl. Botschaft des Bundesrates vom 1. Oktober 2004, BBl 2004 5965 ff.

3 BBl 2004 7149 ff.

4 Gemäss Angaben auf der Website des Integrationsbüros EDA/EVD: <http://www.europa.admin.ch/themen/00500/00507/index.html?lang=de> (letztmals kontrolliert: 15.04.2007).

5 Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes (Schengen-Assoziierungs-Abkommen, SAA) vom 26. Oktober 2004, BBl 2004 6447 ff.; Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrages (Dublin-Assoziierungs-Abkommen, DAA) vom 26. Oktober 2004, BBl 2004 6479 ff.; Bundesbeschluss vom 17. Dezember 2004 über die Genehmigung und die Umsetzung der bilateralen Abkommen zwischen der Schweiz und der EU über die Assoziierung an Schengen und an Dublin, BBl 2004 7149 ff.

lung vor. Dies hängt einerseits damit zusammen, dass die Abkommen eine dynamische Weiterentwicklung vorsehen, welche von der Schweiz und damit auch von den Kantonen zu übernehmen ist. Andererseits erfolgt eine definitive Inkraftsetzung des Abkommens – und vor allem der Anschluss ans SIS – erst dann, 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 und die bisherigen Mitglieder des Schengen-Raums nach einer entsprechenden Kontrolle einen Beschluss gefasst haben, wonach der Bund und die Kantone alle einschlägigen Bestimmungen korrekt umgesetzt haben[6].

Das Assoziationsabkommen zu Schengen sieht folgende Phasen bis zum definitiven Inkrafttreten vor:

a. Mitwirkung der Schweiz an der Weiterentwicklung des Schengen-Acquis ab Unterzeichnung des Abkommens im Oktober 2004.

b. Inkrafttreten der Abkommen nach Ratifizierung durch die Vertragsparteien.

c. Prüfung der korrekten und vollständigen Umsetzung des Abkommens zu Schengen durch die bisherigen Schengen-Mitglieder im Rahmen eines Monitorings.

d. Beschluss der Schengen-Mitglieder über die Inkraftsetzung des Schengener Abkommens in Bezug auf die Schweiz.

Nach der ursprünglichen Planung sollte sich die Schweiz nicht mehr am derzeit installierten Schengener Informationssystem SIS I beteiligen können, sondern erst am SIS II, das nicht vor Ende 2007 in Betrieb genommen werden sollte. Aufgrund technischer Gründe seitens der EU wird sich die operative Einführung von SIS II aber bis mindestens Ende 2008 verzögern. Damit die zehn 2004 beigetretenen neuen EU-Staaten trotzdem rasch in die Schengener Sicherheitszusammenarbeit eingebunden werden können, hat die EU die Einführung der Übergangslösung SISone4all beschlossen. Diese würde bereits Ende 2007 operativ. Der Bundesrat hat sich am 16. Mai 2007 für die Beteiligung an der Übergangslösung SISone4all entschieden[7]. Die Absicht ist, die vor zwei Jahren vom Volk angenommenen Schengen/Dublin-Assoziierungsabkommen und damit den Volkswillen möglichst rasch umzusetzen. Insofern zusätzliche Verzögerungen bei der Entwicklung des SIS II möglich sind, wollte man kein Risiko einer weiteren Verspätung bei der Inkraftsetzung von Schengen/Dublin eingehen. Innerhalb der EU ist die Ratifizierung der Abkommen durch die einzelnen Mitgliedstaaten im Tun. Nach dem heutigen Wissensstand soll der erste Teil der Evaluation Ende 2007, der zweite, die Evaluation vor Ort, im ersten Halbjahr 2008 stattfinden. Zurzeit wird damit gerechnet, dass die Abkommen für die Schweiz am 1. November 2008 in Kraft treten können.

---

6 Art. 15 SAA (Fn. 5).

7 Medienmitteilung des Eidgenössischen Justiz- und Polizeidepartements vom 16. Mai 2007 («Schengener Informationssystem: Bundesrat legt weiteres Vorgehen fest»).

3. 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 insbesondere die Verstärkung der Kontrollen an den Aussengrenzen des Schengener Raums, eine gemeinsame Visumspolitik 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 beinhaltet über 12 Millionen Datensätze über gesuchte und vermisste Personen beziehungsweise verschwundene Gegenstände wie Fahrzeuge oder Waffen. Es besteht aus einem Zentralrechner, der in Strassburg steht. Daran sind die nationalen Schengener Informationssysteme (N-SIS) angehängt.

Die **Dubliner Zusammenarbeit** ist ein Element des **europäischen Asylraums**. Mit ihr soll sichergestellt werden, dass Asylsuchende nur ein Asylgesuch im Dubliner Raum 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 systematisch erkannt werden[8].

4. Auswirkungen von Schengen/Dublin auf die kantonale Gesetzgebung

Die bedeutendsten Änderungen aufgrund der Abkommen von Schengen/Dublin sind im Bereich des Datenschutzes notwendig (vgl. dazu sogleich Ziffer 5). Ausserdem besteht im Bereich des Waffenwesens ein geringer Anpassungsbedarf. In der Verordnung vom 26. Januar 1999 zum Bundesgesetz über Waffen, Waffenzubehör und Munition[9] muss die Meldestelle für die Übertragung von Waffen ohne Waffenerwerbsschein bezeichnet werden. Im Betäubungsmittelbereich ist das Dekret vom 12. April 1973 über die Betäubungsmittel[10] zu ändern: Unter dem Recht von Schengen/Dublin dürfen Reisende die im Rahmen einer ärztlichen Behandlung notwendigen Betäubungsmittel mit sich führen, soweit sie eine besondere Bescheinigung besitzen. Im Dekret muss deshalb die Rechtsgrundlage für die Ausstellung der Bescheinigung für das grenzüberschreitende Mitführen von Betäubungsmitteln für kranke Reisende geschaffen werden.

5. Auswirkungen im Bereich des Datenschutzes im Speziellen

Die Schengener Polizeizusammenarbeit beinhaltet einen intensiven Austausch von Personendaten. Regelmässig werden personenbezogene Daten, darunter häufig besonders sensitive Personendaten und Persönlichkeitsprofile, zwischen den Polizeibehörden der Teilnehmerstaaten ausgetauscht. Diese **intensive Bearbeitung von Personendaten** verlangt nach

---

8 Vgl. Botschaft des Bundesrates vom 1. Oktober 2004, BBl 2004 5968.
9 SGS 704.11.
10 SGS 953.1.

einem **entsprechenden Datenschutzstandard**. Die Europäische Union hat deshalb nicht bloss die Aufgabenerfüllung umschrieben und wirkungsvolle Informationssysteme bereitgestellt (das Schengener Informationssystem SIS[11] und – für Dublin – Eurodac[12]), sondern im Bewusstsein, dass solche Systeme auch schwerwiegende Eingriffe in die Persönlichkeitsrechte der betroffenen Personen bedeuten, entsprechende Datenschutzregeln dafür aufgestellt. Wer die Systeme verwenden will, muss sich auch an die dafür aufgestellten Regeln halten – so auch die Schweiz an die Datenschutzregelungen bezüglich Schengen/Dublin.

Für die Datenbearbeitungen im Rahmen von Schengen/Dublin enthält einmal das **Schengen-Durchführungsübereinkommen** (SDÜ)[13] datenschutzrechtliche Regelungen. Darüber hinaus müssen alle Datenbearbeitungen, die unter den so genannten ersten Pfeiler der EU fallen, den Anforderungen der **EU-Datenschutzrichtlinie**[14] genügen. Unter den ersten Pfeiler fallen die Bereiche Grenzkontrollen, Visa, Feuerwaffen, teilweise Betäubungsmittel und Asyl. Durch Artikel 2 Absatz 2 in Verbindung mit Anhang B des Schengen-Assoziierungs-Abkommens (SAA)[15] hat sich die Schweiz ausdrücklich verpflichtet, die EU-Datenschutzrichtlinie umzusetzen und anzuwenden. Für die polizeiliche und justizielle Zusammenarbeit – also den Bereich des dritten Pfeilers der EU – ist die EU-Datenschutzrichtlinie nicht anwendbar; hier enthält das SDÜ selber spezifische, direkt anwendbare Schutzvorschriften über die Datenbearbeitungen im Zusammenhang mit dem SIS und ausserhalb des SIS. Es verlangt dabei die Gewährleistung eines Datenschutzstandards, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (**Europarats-Konvention 108**, SR 0.235.1)[16] ergibt[17]. Es ist aber absehbar, dass die EU für die

---

11 Vgl. Teil IV (Artikel 92 ff.) des Übereinkommens vom 19. Juni 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (SDÜ, ABl. L 239 vom 22. September 2000, 19 ff.), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:DE:PDF> (letztmals kontrolliert: 15.04.2007).

12 Vgl. die Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist (Dublin-Verordnung, ABl. L 50 vom 25. Februar 2003, 1 ff.), welche das Dubliner Übereinkommen ablöste, sowie insb. die Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von «Eurodac» für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens (Eurodac-Verordnung, ABl. L 316 vom 15. Dezember 2000, 1 ff.).

13 Vgl. oben Fussnote 11.

14 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie), Amtsblatt der Europäischen Gemeinschaften Nr. L281 vom 23/11/1995 S. 0031-0050, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML> (letztmals kontrolliert: 15.04.2007).

15 Vgl. oben Fussnote 5 (BBl 2004 6449 und 6467); vgl. dazu ASTRID EPINEY/ SARAH THEUERKAUF, Datenschutz in Europa – Überblick und Implikationen in den Bilateralen II, sowie BEAT RUDIN/ BRUNO BAERISWYL, «Schengen» und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, beide in: Astrid Epiney/ Sarah Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz – La protection des données en Europe et la Suisse, Zürich/ Basel/ Genf 2006, 45 ff. bzw. 169 ff.

16 Von der Bundesversammlung genehmigt am 5. Juni 1997, für die Schweiz in Kraft getreten am 1. Februar 1998.

17 Artikel 117 SDÜ für Datenbearbeitungen im Rahmen des SIS, Artikel 126 SDÜ für Datenbearbeitungen ausserhalb des Rahmens des SIS.

Bearbeitungen im Bereich des dritten Pfeilers demnächst vergleichbare Datenschutzregeln aufstellen wird[18].

Das kantonale Datenschutzgesetz 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[19]. Insbesondere die Regelung von Artikel 28 der EU-Datenschutzrichtlinie über die Datenschutz-Kontrollstelle hat Auswirkungen auf die kantonale Datenschutzgesetzgebung. Sie 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 Kontroll-*

---

[18] Vgl. den Vorschlag der Kommission der Europäischen Gemeinschaften für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (SEC (2005) 1241) (<http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/com/2005/com2005_0475de01.pdf> [letztmals kontrolliert: 15.04.2007])

[19] FRANK SEETHALER, N 84 zu Entstehungsgeschichte DSG, in: Basler Kommentar Datenschutzgesetz, hrsg. von Urs Maurer-Lambrou/ Nedim Peter Vogt, 2. Aufl., Basel/ Genf/ München 2006.

stelle 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 im Bereich des dritten Pfeilers der EU gilt grundsätzlich, dass die Datenübermittlung erst beginnen kann, wenn unabhängige Kontrollinstanzen eingerichtet sind (Artikel 126 SDÜ).

II. Datenschutzgesetzrevision im Bund und Ratifikation des Zusatzprotokolls zur Europarats-Konvention 108

Die Eidgenössischen Räte haben am 24. März 2006 die **Revision**[20] **des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz** (DSG; SR 235.1) 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 (**Zusatzprotokoll zur Europarats-Konvention 108**)[21] angenommen.

Ziel dieser Änderung war nicht primär eine Anpassung des Bundesdatenschutzgesetzes an die Vorgaben von Schengen/Dublin. Auslöser für die Revision waren vielmehr zwei in den Jahren 1999 beziehungsweise 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. Ausserdem mussten einige Bestimmungen des Bundesgesetzes angepasst werden, damit die Schweiz dem Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Daten-

[20] BBl 2006 3547 ff.
[21] Abgedruckt in: BBl 2003 2167 ff.

übermittlung beitreten kann. Eine generelle Anpassung an das europäische Datenschutzrecht war aber erklärtermassen noch nicht das Ziel der DSG-Revision des Bundes.

Die Gesetzesänderung sieht für Datenbearbeiter die Verpflichtung zur aktiven Information der betroffenen Person vor, wenn besonders schützenswerte Daten und Persönlichkeitsprofile beschafft werden. Bei Personendaten, die nicht besonders schützenswert sind und auch kein Persönlichkeitsprofil darstellen, muss für die betroffene Person 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.

Das Datum des Inkrafttretens der Revision des DSG ist noch nicht definitiv festgelegt. Die Revision wird nach der Website des Bundesamtes für Justiz[22] – voraussichtlich nicht vor Mitte 2007 in Kraft gesetzt werden. Was das Zusatzprotokoll betrifft, so ist beabsichtigt, dem Bundesrat die Ratifikation per Ende 2007 vorzuschlagen. Das Zusatzprotokoll würde drei Monate nach der Hinterlegung der Ratifikationsurkunde, also auf 1. April 2008, in Kraft treten. Das Inkrafttreten des Zusatzprotokolls zur Europarats-Konvention 108 bedeutet für Bund und Kantone, dass sie bis zu diesem Zeitpunkt in ihrer Gesetzgebung und in der Organisation die nötigen Anpassungen an die erhöhten Anforderungen vorgenommen haben müssen.

III. Vorgehen betreffend Anpassung des kantonalen Rechts

Die Gesetzgebung des Bundes ersetzt die erforderliche Gesetzgebung der Kantone nicht. Diese müssen selber dafür sorgen, dass ihr Datenschutz – was die Gesetzgebung wie auch die Umsetzung betrifft – den Anforderungen genügt. Darauf hat auch der Bundesrat in der Botschaft zu den «Bilateralen II» ausdrücklich hingewiesen[23]. Dem Bund kommt keine umfassende Datenschutz-Kompetenz zu. Auch der – in der beschlossenen Revision qualitativ verstärkte – Artikel 37 Bundesdatenschutzgesetz gilt ausschliesslich dann, wenn kantonale Organe Bundesrecht vollziehen[24]; die subsidiäre Geltung bestimmter Bestimmungen des Bundesdatenschutzgesetzes vermag also gerade in den Bereichen kantonaler Rechtsetzungskompetenzen das Fehlen kantonaler Datenschutzbestimmungen nicht zu kompensieren[25]. Dass der Bund als Vertragspartei einen internationalen Vertrag ratifiziert, der «die Vertragsparteien» zu einem bestimmten Tun verpflichtet, vermag im föderalistischen Staat logischerweise die verfassungsrechtliche Kompetenzordnung nicht abzuändern; die Verpflichtung trifft somit die Kantone, soweit es ihren Kompetenzbereich betrifft.

---

22 <http://www.bj.admin.ch/bj/de/home/themen/staat_und_buerger/gesetzgebung/datenschutz.html> (letztmals kontrolliert: 15.04.2007).

23 BBl 2004 6175 f., 6181 ff., insb. 6183.

24 Vgl. BEAT RUDIN, Art. 37 N. 9 ff., in: Basler Kommentar Datenschutzgesetz, hrsg. von Urs Maurer-Lambrou/ Nedim Peter Vogt, 2. Aufl., Basel/ Genf/ München 2006.

25 Zum kantonalen Handlungsbedarf vgl. BEAT RUDIN/ BRUNO BAERISWYL (Fn. 15), insb. 178 f.

Auf interkantonaler 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 interkantonalen 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, Ansprechpartner auf technischer und politischer Ebene zu benennen, welche den Informationsfluss zwischen KKJPD/KdK und den einzelnen Kantonen sowie die rechtzeitige Beschlussfassung innerhalb der einzelnen Kantone sicherstellen sollen.

In Absprache mit der KKJPD hat die Konferenz der Kantonsregierungen (KdK) einen externen Experten damit beauftragt, zuhanden der Kantone im Frühjahr 2005 eine Wegleitung zur Umsetzung der mit Schengen und Dublin übernommenen Datenschutzvorschriften auszuarbeiten. Diese Arbeiten wurden von der Arbeitsgruppe Datenschutz der Begleitorganisation Schengen/Dublin – unter dem Vorsitz von Regierungsrätin Sabine Pegoraro – begleitet. Die KdK-Wegleitung[26] zeigt auf, welchem Standard der kantonale Datenschutz genügen muss, einerseits bezüglich des materiellen Inhalts (der Grundsätze, welche beim Bearbeiten von Personendaten zu beachten sind, und der Rechte und Ansprüche der betroffenen Personen), anderseits bezüglich einer unabhängigen und wirksamen Datenschutzkontrolle.

Die Justiz-, Polizei- und Militärdirektion hat den Verfasser der KdK-Wegleitung anschliessend beauftragt, den Handlungsbedarf im basellandschaftlichen Recht zu beurteilen und Vorschläge für die notwendigen Anpassungen vorzulegen.

IV. Inhalt der Revision des Datenschutzgesetzes

1. Handlungsbedarf

Der Vergleich zwischen den Anforderungen aufgrund der EU-Datenschutzrichtlinie, der Europarats-Konvention 108 und des Zusatzprotokolls zur Europarats-Konvention 108 mit dem gegebenen Recht ergibt für den Kanton Basel-Landschaft Handlungsbedarf in folgenden Punkten:

Bei den Grundsätzen des Datenbearbeitens fehlt die ausdrückliche Erwähnung von Treu und Glauben, des Verhältnismässigkeitsprinzips und der Zweckbindung. Das Datenschutzgesetz unterscheidet nicht zwischen «gewöhnlichen» und besonders schützenswerten (sensitiven) Personendaten und sieht dementsprechend auch keinen besonderen Schutz dafür vor. Ebenso wenig ist die Transparenz der Datenbearbeitungen für die betroffene Person gewährleistet, und es fehlt – ausser gegenüber den Einwohnerkontrollen – ein Anspruch der

[26] Abrufbar unter <http://www.datenschutz.ch/themen/2006_kdk_schengen_dublin_datenschutz_wegleitung.pdf> (letztmals kontrolliert: 15.04.2007).

betroffenen Person auf Sperrung der Bekanntgabe ihrer Daten. Es fehlen griffige Bestimmungen zur Gewährleistung eines angemessenen Schutzes bei der Bekanntgabe von Personendaten ins Ausland. Das Datenschutzgesetz sieht bei Bearbeitungen von Personendaten, die (aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten) besondere Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringen können, keine Pflicht zu Vorabkontrolle vor. Beim Register der Datensammlungen geht das Gesetz einerseits weiter als nötig, anderseits fehlen bestimmte Angaben im Register. Bei der Datenbekanntgabe ins Ausland fehlt die Berücksichtigung der Voraussetzungen, wie sie Artikel 2 des Zusatzprotokolls zur Europarats-Konvention 108 umschreibt. Grosser Handlungsbedarf besteht schliesslich beim Datenschutzkontrollorgan, in Bezug auf seine Untersuchungs- und Einwirkungsbefugnisse, seine Aufgaben und Pflichten, ganz besonders aber in Bezug auf seine Unabhängigkeit und die Gewährleistung der Wirksamkeit der Kontrolle.

2. Anpassungen im materiellen Teil

Im materiellen Teil (Abschnitte A bis D) können die fehlenden Regelungen relativ einfach eingefügt werden. Zur Behebung der ermittelten Defizite schlägt der Regierungsrat dafür die folgenden Anpassungen vor:

- Für das Bearbeiten von besonderen (d.h. sensitiven) Personendaten und von Persönlichkeitsprofilen werden in § 6 qualifizierte Voraussetzungen festgelegt; die beiden Datenkategorien werden in die Begriffsbestimmungen des § 5 aufgenommen.

- Die fehlenden Grundsätze des Datenbearbeitens werden in § 6 eingefügt.

- Um dem Transparenzgebot zu genügen, wird in § 7 verlangt, dass die Datenerhebung für die betroffene Person erkennbar sein muss (mit Ausnahmen).

- Die Voraussetzungen für den Datentransfer ins Ausland werden in § 11 eingefügt.

- In § 11 wird ebenso der Anspruch der betroffenen Person, die Bekanntgabe ihrer Personendaten sperren zu lassen, festgehalten (mit der Möglichkeit der Bekanntgabe trotz Sperrung).

- In § 15a wird die Pflicht zur Vorabkontrolle eingefügt.

- In § 16 wird das zentrale Register der Datensammlungen ersetzt durch dezentrale Verzeichnisse der Datensammlungen der verantwortlichen Behörden.

3. Anpassungen im institutionellen Teil

Grösserer Handlungsbedarf besteht im institutionellen Teil, beim Datenschutzkontrollorgan. Das Ziel der internationalrechtlichen Regelungen ist klar: Das Datenbearbeiten soll einer **unabhängigen und wirksamen Kontrolle** unterliegen. Die EU-Datenschutzrichtlinie verlangt deshalb ein Datenschutzkontrollorgan, das seine Aufgaben in völliger Unabhängigkeit

wahrnimmt, und legt auch fest, über welche Befugnisse es verfügen muss und welche Pflichten es zu erfüllen hat[27]. Die Europarats-Konvention 108 sagt selber aus Gründen, die in ihrer Entstehungsgeschichte liegen, nichts zum Datenschutzkontrollorgan aus; diese Lücke wird nun geschlossen durch das Zusatzprotokoll zur Europarats-Konvention 108, welches einerseits Regeln für die Datenbekanntgabe ins Ausland und anderseits für das Datenschutzkontrollorgan aufstellt[28].

a. Unabhängigkeit

Zur Gewährleistung der **Unabhängigkeit** hält die KdK-Wegleitung in den Erläuterungen fest: *«Die rechtlichen Vorgaben verlangen ein Kontrollorgan, das seine Aufgabe ‹in völliger Unabhängigkeit› wahrnehmen kann. Das verlangt einerseits, dass die Unabhängigkeit ausdrücklich im Gesetz festgehalten ist. Anderseits muss die Unabhängigkeit auch mit institutionellen Sicherungen garantiert werden»*[29]. *«Neben der ausdrücklichen Festschreibung der völligen Unabhängigkeit des Kontrollorgans braucht es auch institutionelle Garantien dafür. Unabhängigkeit ist beispielsweise nicht gegeben, wenn die Spitze der zu kontrollierenden Organe (die Spitze der Verwaltung) das Kontrollorgan mit einem jederzeit kündbaren Arbeitsvertrag anstellt, über die Zuteilung (und Kürzung) von personellen und finanziellen Ressourcen entscheidet oder die Planung und Durchführung der Kontrolltätigkeit beeinflussen kann. Zum Vergleich: die meisten Kontrollorgane in den europäischen Staaten werden vom Parlament auf eine feste Amtsdauer gewählt, verfügen über ein eigenes Budget, das ohne Regierungsintervention vom Parlament beschlossen wird, und legen ihr Prüfungsprogramm autonom fest. Es gibt (in deutschen Bundesländern) für bestimmte Teilausschnitte der Kontrolle noch vereinzelte Kontrollorgane, die den Innenministerien der Bundesländern unterstellt sind; solche Kontrollorgane erfüllen – wie die Intervention der Europäischen Kommission bei der deutschen Bundesregierung zeigt – das Erfordernis der Unabhängigkeit nicht (…)»*[30]. *«Die rechtlichen Vorgaben verlangen eine wirksame aktive Kontrolle. Eine solche aktive Kontrolle muss anlassfrei möglich sein und aufgrund eines autonom aufgrund einer Risikobeurteilung erstellten Prüfprogramms erfolgen. Das verlangt, dass das Kontrollorgan erstens die nötigen Befugnisse besitzt (…), dass [es] zweitens die erforderlichen personellen und finanziellen Ressourcen zugeteilt erhält, und dass drittens an das Kontrollorgan (bzw. an seine Leitung) hohe fachliche Anforderungen gestellt werden (Weiterbildung)»*[31]. Um die verlangte völlige Unabhängigkeit des Datenschutz-Kontrollorgans zu gewährleisten, sind nach der KdK-Wegleitung[32] – leicht gekürzt – die folgenden institutionellen Garantien unabdingbar:

---

27 Siehe Artikel 28 EU-Datenschutzrichtlinie oben S. 7.

28 Zum Datenschutzkontrollorgan vgl. Absatz 2 der Präambel sowie Artikel 1 Zusatzprotokoll zur Europarats-Konvention 108.

29 KdK-Wegleitung, 21 (Erläuterungen zur Checkliste, Ziffer 7.5).

30 KdK-Wegleitung, 21 f. (Erläuterungen zur Checkliste, Ziffer 7.6) mit Verweis auf das Schreiben der Kommission der Europäischen Gemeinschaften vom 5. Juli 2005 an den Bundesminister des Auswärtigen, 2003/4820/ C(2005) 2098); dazu ebenfalls PETER SCHAAR, Unabhängige Datenschutzaufsicht im Innenministerium? Zum Massstab der «völligen Unabhängigkeit» der Datenschutzaufsicht nach Artikel 28 EG-Datenschutzrichtlinie, in: DuD 2005, 579 ff.

31 KdK-Wegleitung, 22 (Erläuterungen zur Checkliste, Ziffer 7.7).

32 KdK-Wegleitung, 23 f. (Anhang zu den Erläuterungen der Checkliste: Gewährleistung der völligen Unabhängigkeit des Datenschutz-Kontrollorgans: Institutionell und personell).

Budget für Personal- und Sachressourcen, Anstellung weiteren Personals: Das Kontrollorgan muss über ein eigenes Budget für Personal- und Sachressourcen (inkl. der Möglichkeit, im Falle von Kapazitätsproblemen externe Fachspezialisten beizuziehen) verfügen; das Budget ist durch das Kontrollorgan zu erstellen und dem Parlament ohne Regierungsintervention zu unterbreiten.

Unabhängigkeit bei der Planung und Durchführung der Kontrolltätigkeit des Kontrollorgans: Das Kontrollorgan muss sein Prüfprogramm – im Rahmen seines gesetzlichen Auftrages – autonom aufstellen. Es muss über umfassende Untersuchungsbefugnisse (ungeachtet allfälliger Geheimhaltungspflichten), wirksame Einwirkungsbefugnisse und eine Klage-/Anzeigebefugnis verfügen. Es muss die Kompetenz haben, Sonderaufträge zur Prüfung abzulehnen, wenn diese die Realisierung des Prüfprogramms gefährden.

Sicherung der persönlichen Unabhängigkeit: Das Kontrollorgan muss über Fachkompetenz verfügen, als Wahlvoraussetzung und als Pflicht zur Erhaltung durch Fortbildung. Das Anforderungsprofil muss grossen Wert legen auf die persönliche Integrität. Zur Vermeidung von Interessenkonflikten ist eine Pflicht zur Offenlegung von Interessenbindungen der leitenden Person und der weiteren mit Kontrollaufgaben betrauten Mitarbeitenden des Kontrollorgans vorzusehen. Zudem ist die Frage der Nebenerwerbstätigkeit zu regeln.

Anstellungsverhältnis des Kontrollorgans (der leitenden Person des Kontrollorgans), Auflösung des Anstellungsverhältnisses: Das Kontrollorgan ist auf eine feste Amtsdauer ohne die Möglichkeit der vorgängigen ordentlichen Kündigung seitens des Kantons anzustellen. Die vorzeitige Auflösung soll ausschliesslich bei schwerwiegenden Amtspflichtverletzungen zulässig sein; eine solche Auflösung muss gerichtlich anfechtbar sein.

Kontrolle: Die Prüfung des administrativ-finanziellen Gebarens erfolgt durch Rechenschaftsablage durch das Kontrollorgan wie durch die Gerichte (Kontrolle durch oberstes Finanzaufsichtsorgan). Eine Kontrolle der Erfüllung des gesetzlichen Kontrollauftrags muss die Unabhängigkeit wie bei den Gerichten achten. Audits durch die Exekutive oder im Auftrag der Exekutive sind unzulässig, allenfalls durch Organe der parlamentarischen Oberaufsicht oder durch externe Stellen in deren Auftrag. Eine öffentliche Kontrolle wird ermöglicht durch die Veröffentlichung der Tätigkeitsberichte des Kontrollorgans.

Unterschiedliche Lösungen sind denkbar bezüglich des Wahlorgans und der Stellung/ Zuordnung des Kontrollorgans:

Wahl (Ernennung, Bezeichnung o.ä.) des Kontrollorgans (der leitenden Person des Kontrollorgans): Für die Frage nach Wahlorgan und Amtsdauer sieht die KdK-Wegleitung drei Varianten vor:

- *Variante A*: Wahl (Ernennung, Bezeichnung o.ä.) durch das Parlament auf eine Amtsdauer von 4 bis 6 Jahren (mit der Möglichkeit der Wiederwahl)

- *Variante B*: Wahl (Ernennung, Bezeichnung o.ä.) durch die Exekutive mit Vorbehalt der Genehmigung durch das Parlament auf eine Amtsdauer von 6 bis 8 Jahren (mit der Möglichkeit der Wiederwahl)

- *Variante C*: Wahl (Ernennung, Bezeichnung o.ä.) durch die Exekutive auf eine Amtsdauer von 8 oder mehr Jahren (mit der Möglichkeit der Wiederwahl)

Stellung/ Zuordnung des Kontrollorgans: Bei der Wahlvariante A ist eine administrative Zuordnung zur Geschäftsleitung des Parlaments denkbar, bei den Wahlvarianten B und C eine selbständige Stellung mit lediglich administrativer Zuordnung zu einer Direktion oder zur Stabsstelle der Exekutive (BL: Landeskanzlei).

Fazit daraus: Es gibt nicht eine einzige richtige Lösung, sondern es ist in der **Kombination von institutionellen Garantien** die Unabhängigkeit zu gewährleisten. Insbesondere kann nicht geschlossen werden, dass allein die Wahl durch das Parlament die verlangte Unabhängigkeit schaffen kann. Die schweizerische Spezialität der Volkswahl der Exekutive in den Kantonen ist mit zu berücksichtigen. Allerdings hält die KdK-Wegleitung dazu auch fest:

> *«Eine Wahl ausschliesslich durch die Exekutive (Variante C) stellt eine Wahl der Kontrollierenden durch die Kontrollierten dar. Sie kann unter dem Aspekt der verlangten völligen Unabhängigkeit allerhöchstens dann genügen, wenn dieses offensichtliche Manko durch andere Sicherungen in höchster Qualität kompensiert werden kann:*
>
> - *durch ein Maximum bei den übrigen institutionellen Sicherungen (siehe Seite 1[33] sowie Amtsdauer und Stellung/ Zuordnung des Kontrollorgans),*
> - *durch ein Maximum an Einwirkungsbefugnissen des Kontrollorgans (…) sowie*
> - *durch eine Ausstattung mit entsprechenden finanziellen und personellen Ressourcen.»*[34]

Der Regierungsrat schlägt die entsprechenden Regelungen in den §§ 22 und 22a vor. § 22 enthält die Bestimmungen, welche die Datenschutz-Aufsichtsstelle generell betreffen; § 22a enthält die Bestimmungen, welche die Datenschutzbeauftragte oder den Datenschutzbeauftragten als Leiterin oder Leiter der Datenschutz-Aufsichtsstelle betreffen. Die oder der Datenschutzbeauftragte soll vom Regierungsrat unter Vorbehalt der Genehmigung durch den Landrat gewählt werden. Mit dieser Lösung kann erreicht werden, dass beide Gewalten – Landrat und Regierungsrat – an der Wahl beteiligt sind, was die Datenschutz-Aufsichtsstelle in ihrer Stellung gegenüber der datenbearbeitenden Verwaltung stärkt. Die Amtsdauer soll nicht (wie in der KdK-Wegleitung für diesen Fall postuliert) sechs bis acht Jahre betragen, sondern bloss vier Jahre, wie es § 53 Kantonsverfassung für Behördenmitglieder und die gewählten Mitarbeiterinnen und Mitarbeiter vorsieht. Die Unabhängigkeit des Kontrollorgans wird ausdrücklich festgeschrieben; ausserdem wird festgelegt, dass es über einen eigenen Voranschlag verfügt, der von ihm selber erstellt und vom Regierungsrat unverändert an den Landrat weitergeleitet wird und dass es die weiteren Mitarbeitenden der Aufsichtsstelle Datenschutz selbständig anstellt.

b. Aufgaben

Die Aufgaben des Datenschutzkontrollorgans sind in § 24 festgehalten. Der bisherige Katalog ist einerseits unvollständig – es fehlen der Hinweis auf die Veröffentlichung der Berichterstattung sowie die Pflicht zur Zusammenarbeit mit den Datenschutzkontrollorganen der anderen Kantone, des Bundes und des Auslandes –, anderseits enthält er Doppelspurigkeiten. Weil der Aufgabenkatalog ohnehin anzupassen ist – beispielsweise an die neue Regelung der dezentralen Führung der Verzeichnisse der Datensammlungen –, schlägt der Regierungsrat gleich eine Gesamtüberarbeitung vor.

---

33 Siehe die oben (13 f.) erwähnten Garantien.

34 KdK-Wegleitung, 24 (Anhang zu den Erläuterungen der Checkliste: Gewährleistung der völligen Unabhängigkeit des Datenschutz-Kontrollorgans: Institutionell und personell).

c. Wirksamkeit

Zur Gewährleistung der **Wirksamkeit** der Datenschutzkontrolle verlangen die EU-Datenschutzrichtlinie und das Zusatzprotokoll zur Europarats-Konvention 108 insbesondere die Einräumung weitgehender Untersuchungsbefugnisse, wirksamer Einwirkungsbefugnisse und einer Klage-/Anzeigebefugnis.

Die **Untersuchungsbefugnisse** sind heute in § 25 Absätze 1 und 2 festgeschrieben. Dabei schränkt Absatz 2 die Aufsichtsbefugnisse der Aufsichtsstelle gegenüber Drittpersonen, die von einer Behörde mit dem Bearbeiten von Personendaten beauftragt sind oder von ihr Personendaten erhalten haben, ein: Anders als wenn die Behörden die Daten selber bearbeiten, soll sie keine Besichtigung durchführen dürfen und sich keine Bearbeitungen vorführen lassen; hingegen darf sie – wie gegenüber den die Daten selber bearbeitenden Behörden – mündlich oder schriftlich Auskunft über Datenbearbeitungen einholen sowie Einsicht in alle Unterlagen nehmen. Solche Restriktionen sind nach Artikel 28 Absatz 3 EU-Datenschutzrichtlinie und Artikel 1 Ziffer 2 Buchstabe a Zusatzprotokoll zur Europarats-Konvention 108 nicht vorgesehen. Es ist im Übrigen auch nicht im Interesse der auftraggebenden Behörden, die Aufsicht schwächer ausfallen zu lassen, bleiben diese Behörden doch gegenüber den in ihren Persönlichkeitsrechten verletzten betroffenen Personen vollumfänglich verantwortlich, auch wenn die rechtswidrige Bearbeitung durch Dritte entgegen ihrer Anweisung verschuldet wird (§ 4 Absatz 2: «oder bearbeiten lässt»). Gerade angesichts der zunehmenden Häufigkeit von Outsourcing ist es deshalb notwendig, die gleichen Untersuchungsbefugnisse vorzusehen. Der Regierungsrat schlägt deshalb vor, die Untersuchungsbefugnisse gegenüber Behörden wie gegenüber Dritten, die in ihrem Auftrag Daten bearbeiten, gleich zu regeln.

Bei der Frage der «**wirksamen Einwirkungsbefugnisse**» legt Artikel 28 Absatz 3 zweiter Spiegelstrich EU-Datenschutzrichtlinie nicht genau fest, über welche Einwirkungsbefugnisse das Kontrollorgan konkret oder mindestens verfügen muss – aus Gründen, die in ihrer Entstehungsgeschichte liegen: Als sie geschaffen wurde, verfügten etliche der EU-Mitgliedstaaten schon über eigene Datenschutzgesetze, die aber nicht einem einheitlichen Konzept folgten[35]. Es muss somit mit einer Kombination von Befugnissen erreicht werden, dass die Kontrolle insgesamt wirksam erfolgen kann. Dabei ist zu beachten, dass die Einwirkungsbefugnisse umso stärker ausfallen müssen, je schwächer die Unabhängigkeit institutionell garantiert ist[36], also etwa bei der Wahl durch den Regierungsrat.

Die zugrunde liegende Problematik lässt sich wie folgt umschreiben: Das Datenschutzkontrollorgan äussert sich im Normalfall mittels «Empfehlungen». Die Empfehlungsadressaten können über solche Empfehlungen hinweggehen. Ohne weitere Regelungen kann das Kontrollorgan rechtlich dagegen nichts unternehmen. Zwar kann es, wenn schutzwürdige Interessen einer betroffenen Person offensichtlich gefährdet oder verletzt werden, die vorgesetzte(n) Behörde(n) des verantwortlichen Organs aufzufordern, die erforderlichen Massnahmen zu ergreifen – eine Art aufsichtsrechtliche Anzeige ohne rechtlich verbindliche Wirkung. Die-

---

35 Vgl. dazu SPIROS SIMITIS, Einleitung: Geschichte – Ziele – Prinzipien, in: Spiros Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage, 61 ff, insb. 117 ff. (Kapitel «Internationale Regelungen»).

36 Siehe oben Seite 14 das Zitat aus der KdK-Wegleitung.

se Befugnis genügt den Anforderungen an «wirksame Einwirkungsbefugnisse» keineswegs. Es geht nicht darum, dem Kontrollorgan Entscheidungsbefugnisse einzuräumen, sondern nur darum, die Möglichkeit zu schaffen, dass es erreichen kann, dass die datenschutzrechtlichen Anliegen in ein förmliches rechtliches Verfahren Eingang finden.

Der Regierungsrat schlägt deshalb vor, dass das Datenschutzkontrollorgan seine Empfehlungen wie bisher ohne besonderes Formerfordernis erlässt. Die Empfehlungs-Adressaten werden durch das Datenschutzgesetz neu verpflichtet, sich anschliessend dazu zu äussern: Sie können die Empfehlung annehmen oder sie (ganz oder teilweise) ablehnen. Das ist – wie die bisherige Praxis zeigt, in den allermeisten Fällen problemlos, weil die Adressaten ja an das Kontrollorgan gelangen, um sich beraten zu lassen, wie eine bestimmte Aufgabe datenschutzkonform erfüllt werden kann. Wenn die Empfehlung aber (ganz oder teilweise) abgelehnt wird, hat das Datenschutzkontrollorgan die Möglichkeit, seine **Empfehlung** als Ganzes oder teilweise **als Weisung in Form einer Verfügung** zu erlassen. Das wird es dann und soweit tun, als nach seiner Beurteilung das Durchsetzungsinteresse überwiegt. Das Datenschutzgesetz räumt den Empfehlungs-Adressaten sodann die Befugnis ein, sich mittels einer **Beschwerde** gegen die Weisung des Datenschutzkontrollorgans bei der zuständigen Rechtmittelinstanz (in der Regel beim Regierungsrat oder – bei Anstalten des kantonalen öffentlichen Rechts – beim Kantonsgericht als der zuständigen gerichtlichen Instanz) zu wehren. Es ist davon auszugehen, dass es sich nur um sehr wenige Fälle pro Jahr handeln wird.

Es bleibt schliesslich die verlangte Klage-/Anzeigebefugnis. Der Regierungsrat geht davon aus, dass § 121 Strafprozessordnung (Anzeigepflicht bei konkreten Anzeichen, die auf eine strafbare Handlung oder deren Täterschaft hinweisen) und § 43 Verwaltungsverfahrensgesetz (aufsichtsrechtliche Anzeige) die nötigen Befugnisse bereits einräumen und es deshalb keiner Anpassung im Datenschutzgesetz bedarf.

Nicht zu vergessen ist, dass eine wirksame Datenschutzkontrolle nur mit genügenden personellen und finanziellen Ressourcen zu gewährleisten ist.

C Ergebnisse des Vernehmlassungsverfahrens

An der Vernehmlassung haben sich vier Kantonalparteien (CVP, FDP, SP, SVP), drei Verbände (Basellandschaftlicher Anwaltsverband, Arbeitgeberverband, Handelskammer beider Basel) sowie acht Gemeinden (Allschwil, Binningen, Bretzwil, Gelterkinden, Ormalingen, Pfeffingen, Zwingen, Therwil) beteiligt.

Zwei Verbände (Gewerkschaftsbund Baselland, Verband Basellandschaftlicher Gemeinden) und neun Gemeinden (Arboldswil, Bottmingen, Diepflingen, Ettingen, Lausen, Muttenz, Nenzlingen, Titterten und Waldenburg) haben ausdrücklich auf eine Stellungnahme verzichtet, da sie sich als nicht direkt betroffen erachten.

Ein Vernehmlassungsteilnehmer (FDP) hat sich negativ zum Vernehmlassungsentwurf geäussert.

- Die *FDP* hält fest, dass sie dem Entwurf gemäss der Vernehmlassungsvorlage nicht zustimmen könne. Das Datenschutzgesetz habe sich bewährt, es hätten sich weder grössere Mängel gezeigt noch seien eigentliche Missstände bekannt geworden. Die Behörden seien genügend sensibilisiert für die Probleme des Datenschutzes und der Beizug der Aufsichtsstelle funktioniere auch im Gesetzgebungsverfahren. Die Assoziierungsabkommen zu Schengen und Dublin erforderten nun zwar eine Überprüfung, und daraus ergebe sich zwar ein Revisionsbedarf, der aber nicht so weit gehe, wie in der Vorlage postuliert. Das Schengener Durchführungsübereinkommen (SDÜ) bringe keinen Handlungsbedarf, weil es bloss die «Vertragsparteien» (und damit wohl den Bund, nicht aber die Kantone) verpflichte. Auch verlange das SDÜ keine Regelung, die der EU-Datenschutzrichtlinie genüge, sondern bloss einen Standard, der mindestens der etwas weniger weit gehenden Europarats-Konvention 108 entspreche – wobei, soweit sei hier auf die Argumentation eingegangen, übersehen wird, dass nach Anhang B in Verbindung mit Artikel 2 Absatz 2 des Schengen-Assoziierungs-Abkommens die EU-Datenschutzrichtlinie ausdrücklich als anwendbar erklärt wird. Das Zusatzprotokoll zur Europarats-Konvention 108 bringe bezüglich der Kontrollstelle eine Annäherung an die EU-Richtlinie, übernehme aber deren Detaillierungsgrad nicht. Die FDP hält im Einzelnen fest, es möge Freude bereiten, die Prinzipien von Treu und Glauben, des Verhältnismässigkeitsprinzips und der Zweckbindung im Datenschutzgesetz aufzuführen, aber es sei nicht sinnvoll, in jedem Gesetz die Grundprinzipien staatlichen Handelns (§ 4 Kantonsverfassung) nochmals aufzuführen. Die Voraussetzung einer «klaren» gesetzlichen Grundlage für das Bearbeiten besonderer Personendaten bringe den verlangten qualifizierten Schutz für diese Daten nicht; in der (ihres Erachten nicht anwendbaren) EU-Datenschutzrichtlinie mache die Qualifikation Sinn, weil sonst ein grundsätzliches Bearbeitungsverbot mit ausdrücklich genannten Ausnahmen gelte. Sie schlägt vor, § 6 in der bisherigen Form zu belassen. § 11 Absatz 2 sei mit einer Bestimmung zu ergänzen, wonach Abweichungen vom Grundsatz (Verbot der Bekanntgabe von Personendaten an Behörden oder Private, die nicht der Rechtshoheit eines Staates unterstehen, welcher der Europarats-Konvention 108 beigetreten ist) – wie in Artikel 2 Absatz 2 des Zusatzprotokolls zur Europarats-Konvention 108 vorgesehen – etwa wegen berechtigter überwiegender Interessen, insbesondere wichtiger öffentlicher Interessen, zulässt; andernfalls entstünde eine völlig unmögliche Situation, weil bei der Rückschaffung abgewiesener Asylbewerber etwa nach Westafrika ein Laisser passer nur eingeholt werden dürfte, wenn die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleiste oder ein solcher vertraglich garantiert würde. Bei § 15a sei vom Gesetzgeber festzulegen, welche Datenbearbeitungen einer Vorabkontrolle zu unterstellen sind. In § 16 seien die Bestimmungen über die Art und über die Herkunft der Daten (§ 16 Absatz 2 Buchstaben c^{bis} und e) zu streichen. Bezüglich der Anpassungen im institutionellen Teil (Abschnitt E) schiesse der Entwurf weit über die Anforderungen hinaus: Es sei ein Unding, neben den «klassischen» drei Staatsgewalten eine vierte Gewalt zu installieren, deren Stellung stärker wäre als jene der Gerichte, welche – anders

als der oder die Datenschutzbeauftragte – nicht von sich aus, sondern nur dann tätig werden, wenn sie (von aussen) angerufen würden. Die Zuordnung und Unterstellung unter die Exekutive wie bisher verleihe der Aufsichtsstelle auch einen institutionellen Schutz; die Kooperationsbereitschaft der Verwaltung sei grösser mit einer Stelle, die auch einer Direktion angegliedert sei. Die Aufsichtsstelle sei nach wie vor in die JPMD einzugliedern, aber durch eine gesetzliche Bestimmung als nicht an Weisungen gebunden zu erklären (analog zum kantonalen Vormundschaftsamt bei Fürsorgerischen Freiheitsentzügen). Die FDP schlägt eine übliche Anstellung nach Personalgesetz vor sowie den Verzicht auf die Regelungen betreffend Budget und Anstellung weiterer Mitarbeitender (§ 22 Absätze 3 und 4 [im überarbeiteten Entwurf neu: § 22 Absatz 4 und § 22a Absatz 3]). Sie beantragt in § 25 Absatz 1 – mit Bezugnahme allerdings auf die Beschränkung des Geltungsbereiches der (ihres Erachtens nicht anwendbaren) EU-Datenschutzrichtlinie – zusätzlich die Aufnahme von Einschränkungen der Aufsichtskompetenzen in weit gehenden Bereichen (öffentliche Sicherheit, Landesverteidigung, Sicherheit des Staates, Tätigkeiten des Staates im strafrechtlichen Bereich). Ein Weisungsrecht der Aufsichtsstelle sei nicht zwingend; die FDP erachtet das Recht der Aufsichtsstelle, für eine geeignete Veröffentlichung ihrer Stellungnahmen zu sorgen, als ausreichend. Und schliesslich erübrige sich mit dem Weisungsrecht auch das Beschwerderecht gegen Entscheide der Beschwerdeinstanzen (§ 25 Abs. 6).

Die *grosse Mehrheit* der Vernehmlassungsteilnehmer hingegen stimmt der Vorlage zu (*CVP, SP, Basellandschaftlicher Anwaltsverband, Arbeitgeberverband, Handelskammer beider Basel, Gemeinden Allschwil, Binningen, Bretzwil, Gelterkinden, Ormalingen, Pfeffingen, Zwingen, Therwil*) oder opponiert nicht grundsätzlich (*SVP*). Im Einzelnen bringen sie Folgendes vor:

- Die *CVP* begrüsst die Entwicklung der Aufsichtsstelle Datenschutz zur unabhängigen Kontrollinstanz und ihre Wahl durch den Regierungsrat mit dem Vorbehalt der Genehmigung durch den Landrat.

- Die *SP* betont die Wichtigkeit der Unabhängigkeit und des Know-hows der Datenschutzbeauftragten. Sie beantragt die Einführung einer Pflicht, die betroffenen Personen über das Bearbeiten ihrer Daten zu informieren; zwingend soll diese Informationspflicht bei einer Datenbekanntgabe trotz Sperrung (nach § 11) sein. Ausserdem soll – über den engen Kontext der Anpassung an Schengen/Dublin hinaus – § 20 Abs. 3 präzisierend ergänzt werden. Schliesslich beantragt die SP die administrative Zuordnung der Aufsichtsstelle Datenschutz zur Landeskanzlei, wie es eine überwiesene Motion für die Finanzkontrolle fordert (Motion 2003/234 der SVP-Fraktion vom 16. Oktober 2003, am 23. September 2004 als Postulat überwiesen).

- Für die *SVP* erweisen sich die vorgeschlagenen Änderungen als sachlich unnötig, da sie staatliche Abläufe tendenziell verkomplizieren, den bürokratischen Aufwand ver-

mehren und zu einer weiteren unerwünschten Aufblähung des kantonalen Datenschutzapparates führen. Allerdings geht die SVP mit dem Regierungsrat einig, dass die in der Vorlage enthaltenen Bestimmungen in der Tat als unumgängliche Konsequenzen der Assoziierung an Schengen/Dublin sowie des Zusatzprotokolls zur Europarats-Konvention 108 erscheinen. Deshalb kann sie der Vorlage nicht grundsätzlich opponieren, hält aber ausdrücklich fest, dass sie das Übereinkommen von Schengen/Dublin anlässlich der Volksabstimmung vom 5. Juni 2005 – leider erfolglos – bekämpft habe. Sie sieht sich einmal mehr darin bestätigt, dass sich die Schweiz internationalen Abkommen nicht unbesehen anschliessen sollte. Im Einzelnen plädiert sie dafür, in § 6 Absatz 2 das zweimal verwendete Attribut «klar» ersatzlos zu streichen, da es mehr Fragen aufwerfe, als dass solche gelöst werden. Bezüglich der Wahl des Datenschutzbeauftragten (§ 22 Absatz 1) wehrt sich die SVP gegen die zwitterhafte Ausgestaltung der Wahlkompetenz, welche dem Gebot der eindeutigen Zuordnung von Zuständigkeiten und Verantwortlichkeiten arg zuwiderlaufe; der Landrat als oberste gesetzgebende Behörde würde mit dieser Regelung faktisch vor vollendete Entscheide des Regierungsrates gestellt und diese als blosses Akklamationsorgan nur noch nachträglich «abnicken». Solche Bestätigungsakte seien eines Parlaments unwürdig; da sich die SVP seit jeher für eine materielle Stärkung der Stellung des Landrates engagiere, fordere sie die Wahl des Datenschutzbeauftragten einzig und allein durch den Landrat, entsprechend den bewährten Vorgaben der Kantonsverfassung auf vier Jahre. Schliesslich verlangt die SVP, dass die Neuerungen, die allesamt auf die Ratifizierung internationaler Abkommen seitens des Bundes zurückgingen, ohne Erhöhung des Personalbestandes der Aufsichtsstelle Datenschutz vollzogen würden. Einen perfektionistischen Vollzug in der Art eines Musterschülers – wie in unserem Land bezüglich internationaler Verträge leider allgegenwärtig – halte sie für nicht angebracht.

- Der *Basellandschaftliche Anwaltsverband* begrüsst die Legaldefinitionen, weil sie der Vereinheitlichung der Terminologie und der Verbesserung der Benutzerfreundlichkeit dienen, und hat gegen die Benennung der sensitiven Daten als «besondere Personendaten» (§ 5 Absatz 1^{bis}) nichts einzuwenden. Er erachtet dezentrale Verzeichnisse der Datensammlungen (anstelle des zentralen Registers) als zweckmässig (§ 16), begrüsst die vorgeschlagene Regelung zur Gewährleistung der Unabhängigkeit der Aufsichtsstelle (landrätliche Genehmigung, anderweitige Sicherungen wie bloss administrative Zuordnung zur JPMD, eigenes Budget zuhanden Regierungsrat und Landrat und ausdrückliche Statuierung der Unabhängigkeit bzw. Weisungsunabhängigkeit, § 22) sowie die Regelung, dass die Aufsichtsstelle eine Empfehlung ganz oder teilweise in Form einer Verfügung erlassen kann, gegen die Beschwerde bei der zuständigen Rechtsmittelinstanz eingelegt werden kann (§ 25). Hingegen schlägt der Anwaltsverband vor, als qualifizierte Voraussetzung für das Bearbeiten von besonderen Personendaten eine ausdrückliche gesetzliche Grundlage oder eine ausdrücklich umschriebene Aufgabe zu verlangen oder – in Anlehnung an die Regelung in Art. 17 Bundesdatenschutzgesetz –

festzulegen, dass besondere Personendaten nur bearbeitet werden dürfen, wenn sich die Zulässigkeit aus einem formellen Gesetz ausdrücklich ergibt oder wenn es zur Erfüllung einer in einem formellen Gesetz ausdrücklich umschriebenen Aufgabe erforderlich ist (§ 6 Absatz 2).

- Die *Handelskammer beider Basel* begrüsst die vorgeschlagene Wahl des Datenschutzkontrollorgans durch den Regierungsrat unter Vorbehalt der Genehmigung durch den Landrat auf eine Amtsdauer von vier Jahren; zur Verdeutlichung der Unabhängigkeit sei die Zulässigkeit der Wiederwahl ausdrücklich im Gesetz zu verankern. Sie beantragt ausserdem – über den engen Kontext der Anpassung an Schengen/Dublin hinaus – präzisierende Ergänzungen des Gesetzes in § 7 Absatz 2, § 14 Absatz 1 und 20 Absatz 3. Schliesslich fordert sie, dass der durch die notwendige Anpassung entstehende Mehraufwand mit einer Aufstockung des bisherigen Personals um 50% bewältigt werden müsse.

- Die Gemeinde *Therwil* regt an zu überlegen, ob die Person, über welche Auskunft erteilt wird (§ 11), nicht im Voraus über die Auskunfterteilung informiert werden sollte; ausserdem wäre in § 11 Absatz 2 Buchstabe c und Absatz 3 Buchstabe b eine Präzisierung angebracht, wonach das öffentliche Interesse bzw. die gesetzliche Aufgabe, welche eine Bekanntgabe ins Ausland beziehungsweise die Durchbrechung einer Sperre der Datenbekanntgabe rechtfertigen, in der Schweiz vorliegen müssten.

Soweit die Vorbringen nicht berücksichtigt worden sind, wird dies im Kommentar zu den einzelnen Bestimmungen begründet.

D Kommentar zu den einzelnen Bestimmungen

I. Abschnitt A. Allgemeine Bestimmungen (§§ 1-5)

Zweck (§ 1) und Geltungsbereich (§ 2 allgemein und § 3 zur Umschreibung der Behörden, deren Datenbearbeiten durch das Datenschutzgesetz erfasst wird) benötigen aufgrund der Assoziierung der Schweiz an Schengen/Dublin keine Anpassung.

Aber es hat sich eine «Geburtsschwäche» des Datenschutzgesetzes gezeigt: In § 3 wird bestimmt, was «Behörden im Sinne dieses Gesetzes» sind. Das stellt nicht eine gesetzliche Begriffsbestimmung (Legaldefinition) dar, sonst hätte sie in § 5 platziert werden müssen. Hier in § 3 geht es um einen Aspekt der Bestimmung des Geltungsbereichs des Datenschutzgesetzes: wenn und soweit die hier erwähnten Behörden Personendaten bearbeiten, gilt das Datenschutzgesetz. Wenn weiter hinten im Gesetz von Behörden die Rede ist – bereits ab § 4 bei den für eine Datenbearbeitung verantwortlichen Behörden –, ist damit nicht der gleiche (formelle) Behördenbegriff gemeint, sondern ein materieller, ein funktionsbezogener: Es ist beispielsweise in Bezug auf die Bearbeitung von Personendaten nicht die Polizei Basel-Landschaft eine einzige Behörde, sondern sie stellt – je nach Aufgabe – verschiedene «Be-

hörden» dar. Die Hauptabteilung Kriminalitätsbekämpfung hat eine andere Aufgabe zu erfüllen als die Hauptabteilung Verkehrssicherheit, und deshalb dürfen sie nach § 6 auch nicht einfach «alle» Daten bearbeiten, sondern nur diejenigen, die jeweils für die Erfüllung ihrer Aufgabe erforderlich ist. Die Weitergabe von Daten, beispielsweise von der Verkehrsabteilung an die Kriminalabteilung, ist nicht absolut verboten, aber sie ist an die Voraussetzung der Datenbekanntgabe nach § 8 gebunden. Die Aufgabe einer Verwaltungseinheit ist deshalb – dem Zweckbindungsprinzip entsprechend – bestimmend für die Abgrenzung von «Behörden», nicht die Organisationsform. Der Regierungsrat ist aber der Ansicht, dass mit dieser bisher vorgenommenen Auslegung des Begriffs «Behörden» die Schwierigkeit, auf welche im Zusammenhang mit der Stellung der Schulleitungen hingewiesen wurde, gelöst werden kann (siehe unten zu §25). Allenfalls kann bei einer Schaffung der rechtlichen Grundlagen für die Einführung des Öffentlichkeitsprinzips eine begriffliche Klärung herbeigeführt werden.

Eine weitere «schengen-unabhängige» Lücke ist aber hier in **§ 3 Buchstabe c** zu beheben: Diese Bestimmung sieht vor, dass «Private, soweit sie in Erfüllung öffentlicher Aufgaben hoheitlich handeln», als **Behörden** gelten, deren Bearbeiten von Personendaten in den Geltungsbereich des Datenschutzgesetzes fallen. Bearbeiten Private Personendaten zwar in Erfüllung öffentlicher Aufgaben, handeln dabei aber nicht hoheitlich, dann ist – so die Vorstellung bei der Schaffung dieser Bestimmung – das Bundesgesetz über den Datenschutz anwendbar. Diese Annahme hat sich allerdings als falsch herausgestellt. Nach einer Stellungnahme des Bundesamtes für Justiz ist das Bundesgesetz nicht anwendbar, sobald Private Personendaten in Erfüllung einer kantonalen oder kommunalen öffentlichen Aufgabe erfüllen, unabhängig davon, ob sie hoheitlich handeln oder nicht. Das hat – in unserem Kanton, die meisten anderen kennen die Voraussetzung des hoheitlichen Handelns nicht – zur Folge, dass in solchen Fällen (z.B. bei den Spitex-Organisationen, welche in unserem Kanton gestützt auf das Spitexgesetz mit öffentlichen Aufgaben betraut sind, aber nicht hoheitlich handeln) weder das Bundesdatenschutzgesetz noch das kantonale Datenschutzgesetz Anwendung finden. Aus diesem Grund ist es sinnvoll, § 3 Buchstabe c so anzupassen, dass (auch) «Private, soweit sie mit der Erfüllung öffentlicher Aufgaben betraut sind», Behörden im Sinne des Datenschutzgesetzes sind.

Zur Verantwortung (§ 4) sind keine Anpassungen notwendig, hingegen besteht Anpassungsbedarf bei den **Begriffsdefinitionen** (§ 5). Wie weiter hinten dargestellt wird (zu § 6 Absatz 2), verlangen die EU-Datenschutzrichtlinie und die Europarats-Konvention 108 einen geeigneten Schutz sensitiver Personendaten. Die Regelung in § 6 setzt voraus, dass hier die entsprechenden Legaldefinitionen eingefügt werden. Es besteht Freiheit, wie diese Daten genannt werden. Der häufig verwendete Begriff der «besonders schützenswerten Personendaten» ist eine Wertung, die in der Praxis regelmässig zum Missverständnis führen, die anderen («gewöhnlichen») Personendaten seien nicht schützenswert. Der Regierungsrat schlägt deshalb vor, in § 5 Absatz 1bis diese Kategorie – wie im neuen Informations- und Datenschutzgesetz des Kantons Zürich[37] – «**besondere Personendaten**» zu nennen und die

[37] § 3 des (kantonalzürcherischen) erst teilweise in Kraft gesetzten Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4).

Besonderheit, nämlich die besondere Gefahr der Grundrechtsverletzung, auch zu erwähnen, weil die anschliessende Aufzählung nicht abschliessend ist. Die Aufzählung der besonderen Personendaten in § 5 Absatz 1bis Buchstaben a-d übernimmt die Umschreibung des Artikel 3 litera c Ziffern 1-4 des Bundesdatenschutzgesetzes. Sinnvollerweise wird in § 5 Absatz 1ter auch die Kategorie des «**Persönlichkeitsprofils**» analog Artikel 3 litera d Bundesdatenschutzgesetz übernommen: Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, womit die Gefahr der Grundrechtsverletzung besteht wie bei den besonderen Personendaten. Die Eidgenössische Datenschutzkommission hat in einem Entscheid dazu festgehalten: *«Der Begriff des Persönlichkeitsprofils kann nicht generell formuliert werden»*, *«[…] Menge und Inhalt der personenbezogenen Daten sind ausschlaggebend. Daten, die über einen längeren Zeitraum zusammengetragen werden und so ein biografisches Bild ergeben (Längsschnitt), sind eher als Persönlichkeitsprofil zu qualifizieren als solche, die eine blosse Momentaufnahme darstellen (Querprofil)»*[38].

II. Abschnitt B. Bearbeiten von Personendaten (§§ 6-15a)

§ 6 hat sich bisher darauf beschränkt, das Erfordernis der gesetzlichen Grundlage und – etwas verklausuliert für einen Teil der Datenbearbeitungen – die Erforderlichkeit als Aspekt des Verhältnismässigkeitsprinzips als Voraussetzungen für behördliches Datenbearbeiten zu statuieren. Es bietet sich an, in diesem Paragrafen alle **Grundsätze für das Bearbeiten von Personendaten** zusammenzufassen. Der bisherige Paragrafentext wird zum Absatz 1. Durch Absatz 2 wird der in Artikel 8 EU-Datenschutzrichtlinie («besondere Kategorien personenbezogener Daten») und Artikel 6 Europarats-Konvention 108 («besondere Arten von Daten») geforderte geeignete Schutz für die sensitiven Personendaten geschaffen, indem für das Bearbeiten der in § 5 Absatz 1bis und 1ter neu umschriebenen besonderen Personendaten und Persönlichkeitsprofile qualifizierte Voraussetzungen gegeben sein müssen. Nachdem die in der Vernehmlassungsvorlage in Anlehnung an die Regelung in anderen kantonalen Datenschutzgesetzen[39] und im Bundesdatenschutzgesetz[40] noch vorgeschlagene Formulierung («wenn sich die Zulässigkeit aus einer gesetzlichen Grundlage klar ergibt oder wenn es zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe erforderlich ist» als für die Praxis wenig tauglich kritisiert wurde (Vernehmlassungen der FDP, SVP, des Basellandschaftlichen Anwaltsverbandes), beantragt der Regierungsrat nun, das Wort «klar» durch «ausdrücklich» zu ersetzen, wie es der Anwaltsverband vorschlägt. Eine andere Möglichkeit wäre die Voraussetzung der Regelung in einem Gesetz im formellen Sinn, wie es im Bundesdatenschutzgesetz[41] und in neueren kantonalen Datenschutzgesetzen[42] verlangt wird

---

38 Urteil der Eidgenössischen Datenschutzkommission vom 27.01.2000, VPB 65.48.

39 Z.B. an § 5 litera a-b DSG-ZH.

40 Artikel 17 Absatz 2 litera a Bundesdatenschutzgesetz.

41 Artikel 17 Absatz 2 Bundesdatenschutzgesetz.

42 § 8 Absatz 2 des (kantonalzürcherischen) erst teilweise in Kraft gesetzten Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4); § 8 Absatz 2 Buchstabe a des (vom Aargauer Grossen Rat am 24. Oktober 2006 beschlossenen, aber noch nicht in Kraft getretenen) Gesetzes über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG), welcher eine «gesetzliche Grundlage» für das Bearbeiten besonders schützenswerter Personendaten verlangt – in Abgrenzung zu einer «Rechtsgrundlage» für das Bearbeiten von nicht besonders schützenswerten Personendaten.

und wie es der Anwaltsverband zusätzlich vorschlägt. Damit wäre sichergestellt, dass die mit der Bearbeitung dieser sensitiven Daten verbundene Einschränkung des Grundrechts auf informationelle Selbstbestimmung demokratisch stärker legitimiert ist.

In Absatz 3 wird neu ausdrücklich festgehalten, dass das Bearbeiten von Personendaten nach Treu und Glauben zu erfolgen hat und verhältnismässig sein muss, was bisher aus § 4 Absatz 2 und 3 Kantonsverfassung hergeleitet werden musste. Ein Verstoss gegen Treu und Glauben wäre beispielsweise die verdeckte Datenerhebung ohne ausdrückliche Gesetzesgrundlage. In Absatz 4 wird das Zweckbindungsgebot als eines der Kernstücke des Datenschutzrechts, wie es Artikel 6 Absatz 1 Buchstabe b EU-Datenschutzrichtlinie und Artikel 5 Buchstabe b Europarats-Konvention 108 fordern, ausdrücklich festgehalten: Es verbietet, dass die zu einem bestimmten Zweck erhobenen Personendaten (z.B. die Personaldaten oder Lohndaten) zu einem anderen Zweck (z.B. für Referenzauskünfte an Vermieter oder Kreditunternehmen) verwendet werden, soweit nicht eine Legitimation (z.B. eine gesetzliche Grundlage oder die Einwilligung der betroffenen Person) diese Zweckänderung rechtfertigt. Zwar ist sich der Regierungsrat sehr wohl bewusst, dass Gesetzmässigkeit (anstelle der Zweckbindung, welche in einer Vernehmlassung unzutreffenderweise angeführt wird), Treu und Glauben und Verhältnismässigkeit gemäss § 4 Kantonsverfassung Grundsätze rechtsstaatlichen Handelns sind. Trotzdem hält er am Antrag fest, die Prinzipien hier aufzuführen. Es wäre in der Tat kaum verständlich, wenn bei einer Norm, die das behördliche Datenbearbeiten grundsätzlich und umfassend regeln soll, ausgerechnet die verfassungsrechtlichen Grundsätze fehlen.

Schliesslich wird in Absatz 5 das in Artikel 6 Absatz 1 Buchstabe d EU-Datenschutzrichtlinie und Artikel 5 Buchstabe d Europarats-Konvention 108 postulierte Prinzip festgehalten, dass Personendaten richtig und, soweit es der Verwendungszweck erfordert, vollständig sein müssen. Dieses Prinzip fand bisher seinen Niederschlag bloss in Form eines Anspruchs der betroffenen Person auf Berichtigung unrichtiger Daten (§ 20). Aus der Verankerung in § 6 kann – analog der Regelung in Artikel 5 Bundesdatenschutzgesetz – ein Vergewisserungsanspruch abgeleitet werden, was bisher aus dem Verhältnismässigkeitsprinzip hergeleitet wurde: Die Bearbeitung unrichtiger Daten kann nicht verhältnismässig sein. Der Grad der erforderlichen Sorgfalt bei der Vergewisserung ergibt sich aus der Sensitivität der Daten: Je sensitiver die Daten sind, je grösser das Diskriminierungs- oder Stigmatisierungspotenzial eines Datums ist, umso sorgfältiger muss sich die datenbearbeitende Behörde über die Richtigkeit vergewissern; ein grösseres Augenmerk wird ausserdem verlangt, wenn die Daten nicht nur von der erhebenden Behörde bearbeitet werden, sondern nach § 8 oder § 9 auch an Dritte (andere Behörden oder Private) weitergegeben werden. Der ebenfalls erwähnte Vollständigkeitsanspruch gilt nicht absolut, sondern nur, soweit es der Verwendungszweck erfordert.

Transparenz bezüglich der Bearbeitung von Personendaten ist eines der Kernanliegen des Datenschutzrechts. Das Transparenzgebot, wie es in Artikel 10, 11 und 21 EU-Datenschutzrichtlinie und Artikel 8 litera a Europarats-Konvention 108 zum Ausdruck kommt, besteht einerseits aus dem allgemeinen Recht zu wissen, welche Datenbearbeitungen erfolgen oder

welche Datensammlungen bestehen (samt den wichtigsten Angaben dazu: Hauptzwecke, verantwortliches Organ), anderseits aus dem Informationsanspruch der von einer behördlichen Datenbearbeitung betroffenen Person (bzw. der Informationspflicht des Datenbearbeiters) über die sie betreffenden Daten. Als Minimalvariante erscheint die Erkennbarkeit der Datenerhebung und des Bearbeitungszwecks für die betroffene Person zusammen mit der Registrierpflicht für Datensammlungen in einem öffentlichen Register oder in einem Register mit einem ausdrücklichen Einsichtsrecht für jede Person (dazu hinten zu §§ 16 und 17). § 7 enthielt unter dem Titel «Erhebung» bisher bloss ein Transparenzgebot für den Fall der systematischen Erhebung von Personendaten, namentlich mit Fragebogen; in anderen Fällen sollten Rechtsgrundlage und Zweck der Bearbeitung bloss auf Wunsch der betroffenen Person bekannt gegeben werden. Darum soll nun die Minimalvariante in Absatz 1 als Grundsatz vorangestellt werden: Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden. Begrenzt wird dieses Transparenzgebot durch den Vorbehalt, dass durch die Erkennbarkeit der Beschaffung nicht die Erfüllung der gesetzlichen Aufgabe gefährdet werden darf; das kann etwa bei Ermittlungshandlungen der Polizei im Vorfeld eines Zugriffs der Fall sein. Der bisherige § 7 Satz 1 wird neu zum Absatz 2 mit einer bloss terminologischen Änderung: Der Begriff «bekanntgeben» wird im Datenschutzrecht verwendet für die Bekanntgabe von Personendaten an Dritte (an andere als die datenbearbeitende Behörde oder an Private gemäss § 8 bzw. § 9); hier geht es einfach darum, dass die erwähnten Informationen auf dem Fragebogen bzw. bei der Onlineerfassung angegeben sind. Wie in der Vernehmlassung von der Handelskammer beider Basel gefordert, soll die Formulierung «namentlich mit Fragebogen» ergänzt werden zu «namentlich mit Fragebogen oder Onlineerfassungen», um klarzustellen, dass auch die moderneren systematischen Erhebungen dadurch erfasst werden. Die Einführung einer (allgemeinen) Pflicht, die betroffenen Personen über das Bearbeiten ihrer Daten zu informieren, wie sie von der SP in ihrer Vernehmlassung gefordert wird, erachtet der Regierungsrat hingegen als unnötig. Durch das Abstellen auf eine gesetzliche Grundlage für jedes behördliche Datenbearbeiten wird bis zu einem gewissen Grad die gewünschte Transparenz geschaffen.

Die Vorschriften über die **Bekanntgabe von Personendaten** unter Behörden (§ 8) bzw. an Private (§ 9) erfordern keine Anpassungen. Die neu in § 6 Absatz 2 geregelten qualifizierten Voraussetzungen für das Bearbeiten von besonderen Personendaten («wenn sich die Zulässigkeit aus einer gesetzlichen Grundlage ausdrücklich ergibt oder wenn es zur Erfüllung einer gesetzlich ausdrücklich umschriebenen Aufgabe unentbehrlich ist») wirken sich selbstredend auch auf die Voraussetzungen für die Bekanntgabe als eine Art des Bearbeitens aus.

Die bisherige Regelung der **Bekanntgabe von Personendaten durch die Einwohnerkontrollen** (§ 10) kennt das Recht der betroffenen Person, die Bekanntgabe ihrer Daten sperren zu lassen (Absatz 4), wobei die Sperre unter bestimmten Voraussetzungen durchbrochen werden kann (Absatz 4 Buchstaben a-c). Weil ein allgemeines, nicht nur die Einwohnerkontrollen betreffendes Sperrrecht neu in § 11 Absatz 2 festgelegt wird, kann der Absatz 4 hier gestrichen werden. Absatz 5 wird nur daran angepasst, dass das Sperrrecht nun eben in § 11 Absatz 2 geregelt ist.

§ 11 enthält **gemeinsame Bestimmungen für die Bekanntgabe** nach den §§ 8-10. Hier lassen sich die Bestimmungen zur Bekanntgabe von Personendaten in Staaten, die nicht der Europarats-Konvention 108 beigetreten sind, sowie zum Sperrrecht der betroffenen Personen anfügen. Dementsprechend muss der Paragraphentitel angepasst werden.

Artikel 2 Zusatzprotokoll zur Europarats-Konvention 108 stellt bestimmte Anforderungen an den Personendatentransfer an Empfänger, die nicht der Rechtshoheit eines Staates unterstehen, welcher der Europarats-Konvention 108 beigetreten ist[43]. Danach ist die Datenbekanntgabe im Wesentlichen nur zulässig, wenn durch die Gesetzgebung des Staates oder durch vertragliche Vereinbarungen trotzdem ein angemessener Schutz gewährleistet ist. Ausserdem spricht nichts dagegen, die Bekanntgabe zuzulassen, wenn sie – analog der Regelung in § 9 Buchstabe c – im Interesse der betroffenen Person liegt und diese ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, ihre Zustimmung vorausgesetzt werden darf. Diese Anforderungen werden im neuen § 11 Absatz 2 formuliert. Eine Behörde, die **Daten ins Ausland bekannt geben** will, muss sich also zuerst vergewissern, ob der Staat, dessen Rechtshoheit die empfangende Stelle (Amtsstelle oder Private) untersteht, die Europarats-Konvention 108 ratifiziert hat (§ 11 Absatz 2). Falls nicht, ist zu prüfen, ob die Gesetzgebung des Staates einen angemessenen Schutz gewährleistet (Buchstabe a), wozu auch die Beurteilung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu Rate gezogen werden kann[44]; ist auch das nicht gegeben, so ist der angemessene Schutz durch vertragliche Vereinbarung zu garantieren (Buchstabe b). Ohne solche Garantien ist eine Bekanntgabe nur zulässig, wenn die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist (Buchstabe c), oder wenn die Bekanntgabe im Einzelfall im Interesse der betroffenen Person liegt und diese ausdrücklich zugestimmt hat oder, falls sie dazu nicht in der Lage ist, ihre Zustimmung vorausgesetzt werden darf (Buchstabe d). Der Regierungsrat geht davon aus, dass der in der Vernehmlassung der FDP angeführte Fall (Einholung eines Laisser passer bei der Rückschaffung eines abgewiesenen Asylbewerbers) mit der Wahrung eines überwiegenden öffentlichen Interesses im Einzelfall (Buchstabe c) gerechtfertigt werden kann, sich also eine Ergänzung erübrigt. Ausserdem geht der Regierungsrat mit der Gemeinde Therwil davon aus, dass das öffentliches Interesse, das eine Bekanntgabe nach Buchstabe c auch ohne gesetzliche oder vertragliche Garantie eines angemessenen Schutzes rechtfertigt, grundsätzlich in der Schweiz gegeben sein muss; insbesondere kann sich ein Staat, der die geforderte Ga-

---

43 Zur Zeit (31.10.2006) haben die folgenden Staaten die Europarats-Konvention 108 ratifiziert: Albanien, Belgien, Bosnien und Herzegowina, Bulgarien, Dänemark, Deutschland,Ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Georgien, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern und – als Nichtmitglied des Europarates – Montenegro. Vier weitere Staaten (Moldawien, Russland, Türkei und Ukraine) haben das Übereinkommen unterzeichnet, aber noch nicht ratifiziert. Vgl. die aktualisierte Liste unter <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=10/31/2006&CL=GER> (letztmals kontrolliert: 15.04.2007).

44 Der EDÖB hat nach dem (revidierten) Artikel 31 Absatz 1 litera d Bundesdatenschutzgesetz zu begutachten, inwieweit die Datenschutzgesetzgebung im Ausland einen angemessenen Schutz gewährleistet; vgl. die aktuelle Liste auf der EDÖB-Website (<http://www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de>, [letztmals kontrolliert: 15.04.2007]).

rantie eines angemessenen Schutzes nicht gewährleistet, nicht auf ein bei ihm liegendes öffentliches Interesse berufen, um den durch das Zusatzprotokoll zur Europarats-Konvention verlangten Schutz gerade auszuhebeln.

In § 11 lässt sich in neuen Absätzen 3 und 4 zudem das von Artikel 12 Buchstabe b EU-Datenschutzrichtlinie postulierte Recht der betroffenen Person, die Bekanntgabe der sie betreffenden Personendaten sperren zu lassen, einfügen. Danach kann die betroffene Person bei der verantwortlichen Behörde schriftlich die **Bekanntgabe ihrer Daten sperren** lassen. Nicht jede Bekanntgabe kann ins Belieben der betroffenen Person gelegt werden. Deshalb ist die Bekanntgabe – wie bisher nach § 10 Absatz 4 Buchstaben a-c für das Sperrrecht gegenüber der Einwohnerkontrolle – trotz Sperrung zulässig, wenn die Behörde zur Bekanntgabe gesetzlich verpflichtet ist oder die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder wenn die um Auskunft ersuchende Person glaubhaft macht, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind. Die Motorfahrzeugkontrolle hat für die Bekanntgabe von Halterdaten das Sperrrecht in diesem Sinne auf Begehren der Aufsichtsstelle Datenschutz bereits vor Jahren eingeführt. Die von der SP in ihrer Vernehmlassung geforderte Einführung einer Informationspflicht bei der Durchbrechung der Sperrung braucht nach der Meinung des Regierungsrates nicht ausdrücklich im Gesetz verankert zu werden: Für die Durchbrechungen nach den Buchstaben a und b gilt auch hier, dass die verlangte gesetzliche Grundlage bereits die erwünschte Transparenz schafft. Für eine Durchbrechung nach Buchstabe c, wenn also die um Auskunft ersuchende Person glaubhaft macht, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich seien, war es nach der Auslegung des geltenden Gesetzestextes (§ 10 Absatz 4 Buchstabe c betreffend die Datenbekanntgabe durch die Einwohnerkontrolle) bereits bisher erforderlich, der betroffenen Person das rechtliche Gehör zu gewähren[45]: Sie ist über das Gesuch zu informieren, und es ist ihr Gelegenheit zur Stellungnahme zu geben; der Behörde (bisher also der Einwohnerkontrolle, bei welcher die Durchbrechung der Sperre beantragt wird) obliegt es sodann, die auf jeder Seite vorgebrachten Argumente auf ihre Glaubhaftigkeit hin zu prüfen und gegeneinander abzuwägen; das Ergebnis der Interessenabwägung ist gestützt auf § 27 Datenschutzgesetz in Form einer begründeten Verfügung zu erlassen und sowohl der gesuchstellenden Person oder Organisation als auch der betroffenen Person zu eröffnen. Der Regierungsrat geht ausserdem mit der Gemeinde Therwil davon aus, dass die gesetzliche Aufgabe, welche eine Bekanntgabe trotz Sperrung rechtfertigt (Buchstabe b), im schweizerischen (kantonalen oder Bundes-)Recht verankert sein muss.

Keine Anpassungen sind nötig in § 12 (Bearbeiten für nichtpersonenbezogene Zwecke) und § 13 (Bearbeiten im Auftrag). Hingegen schlägt der Regierungsrat vor, den Paragraphentitel des § 14 (bisher: Datensicherung) anzupassen: Unter Datensicherung wird heute das Backup von Daten verstanden. Bei der Regelung in § 14 geht es hingegen um das, was heute unter dem umfassenderen Begriff «**Informationssicherheit**» verstanden wird. Es ist möglich, gleich auch noch ergänzend im Gesetzestext darauf hinzuweisen, dass, wer Personendaten bearbeitet, «durch angemessene organisatorische und technische Massnahmen» für

---

[45] Vgl. dazu die in «datenschutz konkret» veröffentlichte Stellungnahme der Datenschutzbeauftragten (Nr. 131); <http://www.bl.ch/docs/jpd/ds/konk/konk-131.htm> (letztmals kontrolliert: 15.04.2007).

ihre Sicherung vor Verlust, Entwendung, unbefugter Bearbeitung und Kenntnisnahme sorgt. Nachdem die Handelskammer beider Basel in der Vernehmlassung diese präzisierende Ergänzung gefordert hat, schlägt der Regierungsrat diese Änderung vor, auch wenn sie nicht durch die Assoziierung an Schengen/Dublin notwendig wird.

Der Artikel 20 EU-Datenschutzrichtlinie verlangt, dass Bearbeitungen von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich bringen können, vor ihrem Beginn durch das Kontrollorgan mindestens geprüft (evtl. genehmigt) werden müssen. Kriterien für die Beurteilung der Risiken sind etwa die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe, die Sensitivität der Daten usw. Objekt der **Vorabkontrolle** können v.a. Projekte für IT-Systeme, für Datenbanken, Register usw. sein. Eine solche Verpflichtung fehlt im Gesetz. Sie soll in einem § 15a hier eingefügt werden. Dabei soll bloss eine Prüfung, kein Genehmigungsverfahren durchgeführt werden, und das Datenschutzkontrollorgan soll seine Feststellungen – entsprechend der neuen Regelung in §25 Absatz 3 – in Form der Empfehlung abgeben. So wird sichergestellt, dass Aspekte des Datenschutzes rechtzeitig in Projekte einfliessen und nicht erst nachträglich und mit Mehrkosten integriert werden müssen. Die in der Vernehmlassung der FDP geforderte Präzisierung der Voraussetzungen erachtet der Regierungsrat nicht als nötig und sinnvoll. Erstens bleibt es auch ohne Präzisierung nicht der Datenschutzaufsicht überlassen, zu entscheiden, welche Bearbeitungen zur Vorabkontrolle vorzulegen sind; die Beurteilung obliegt primär der Behörde, welche solche Bearbeitungen vorsieht. Zweitens käme eine Umschreibung im Gesetzestext ihrerseits nicht ohne unbestimmte Rechtsbegriffe aus: Es könnte zwar festgelegt werden, dass IT-Systeme zur Vorabkontrolle vorzulegen sind; damit nicht jedes noch so kleine System erfasst wird, müssten Attribute wie «gross» oder «umfangreich» verwendet werden, was letztlich auch keinen wirklichen Gewinn für die Beurteilung brächte. Der Regierungsrat ist überzeugt, dass mit der Erwähnung der Kriterien für die Beurteilung der Risiken (siehe oben in diesem Absatz) mehr erreicht wird.

III. Abschnitt C. Verzeichnisse der Datensammlungen (§ 16)

Das Datenschutzgesetz sah bisher vor, dass die verantwortlichen Behörden alle ihre Datensammlungen (mit bestimmten Ausnahmen: §16 Absatz 3) dem Datenschutzkontrollorgan zur **Registrierung** melden müssen. Diese Pflicht geht gegenüber dem, was Artikel 19 Absatz 1 Buchstabe c in Verbindung mit Artikel 21 EU-Datenschutzrichtlinie verlangen, zu wenig weit, indem Angaben zur Art der Daten fehlen. Die bisherige Lösung leidet aber vor allem daran, dass das Datenschutzkontrollorgan, welches bisher das Register führte, in keiner Weise für die Vollständigkeit und Richtigkeit des Registerinhalts verantwortlich sein kann. Es ist vom durch die Assoziierung an Schengen anwendbar werdenden Recht her keine *zentrale* Führung eines Registers erforderlich. Deshalb geht der Trend klar in Richtung dezentraler Verzeichnisse[46]. Dementsprechend sieht §16 Absatz 1 neu vor, dass die verantwortlichen

[46] Siehe auch §13 Absatz 4 des (kantonalzürcherischen) erst teilweise in Kraft gesetzten Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4).

Behörden (§ 4) ein vollständiges Verzeichnis über ihre Datensammlungen veröffentlichen. Die Schaffung von dezentralen Verzeichnissen anstelle des zentralen Registers wurde in der Vernehmlassung ausdrücklich begrüsst (Basellandschaftlicher Anwaltsverband). Der Aufwand für die neu zur Verzeichnisführung verpflichteten Behörden wird gegenüber der heutigen Rechtslage (Meldepflicht) nicht verändert und kann zusätzlich durch IT-Unterstützung (Datenbanklösung für alle Dienststellen/Direktionen, Zugänglichkeit gemäss § 17 übers Internet) und/oder durch die Konzentration auf Direktionsebene bzw. beim Kantonsgericht reduziert werden. Der bisherige Satz 2 von Absatz 1 ist nicht mehr nötig, da der Absatz 3 direkt für die Verzeichnisführung anwendbar wird. Für die Veröffentlichung der Verzeichnisse wird in § 32a eine angemessene Übergangsfrist festgelegt.

Der Inhalt der Verzeichnisse (Absatz 2) entspricht dem bisherigen Inhalt der Registeranmeldung, ergänzt um die Angaben zur Art und Herkunft der Daten (neuer Buchstabe c^{bis} und Anpassung des Buchstaben e, wobei in den Angaben zur Herkunft der Daten die «Behörden, welche regelmässig die Personendaten liefern» [bisheriger Buchstabe e] mitenthalten sind). Diese beiden Verzeichnisinhalte wurden in der Vernehmlassung von der FDP kritisiert. Im Sinne des mit der Erstellung und Veröffentlichung der Verzeichnisse verfolgten Hauptzweckes – Transparenz für die betroffenen Personen – ist es zweckmässig und sinnvoll, in die Verzeichnisse diese Angaben aufzunehmen. Gewisse Datensammlungen dürften gleichsam entmystifiziert werden, wenn von vorneherein ersichtlich ist, was für *Arten von Daten* darin enthalten sind, was zu einer Reduktion der Auskunfts- und Einsichtsbegehren führen wird. Bei kleinen Datensammlungen (strukturierte Dateien mit wenigen Datenfeldern) wird es am einfachsten sein, die Datenfelder anzugeben; bei komplexeren Datenbanken wird es sich empfehlen, Datenkategorien anzugeben (etwa «Personalien» als Oberbegriff für Name, Vorname, Geburtsdatum usw.). Die *Herkunft der Daten* ist von entscheidender Bedeutung, wenn es darum geht, Datenflüsse transparent zu machen und unrichtige Daten berichtigen zu lassen. Der Hauptfall – andere Behörden, welche regelmässig Daten liefern – war, wie bereits erwähnt, bisher schon Inhalt des Registers der Datensammlungen; mit der «neutraleren» Formulierung wird zudem der Tatsache Rechnung getragen, dass beispielsweise bei Datenpools (etwa bei einem Geografischen Informationssystem) Daten aus Datenbanken zusammengefügt werden, also nicht mehr eine physische Lieferung stattfindet. Selbstverständlich meint Buchstabe e nur – und nicht anders als bisher – die verfügbaren Angaben über die Herkunft der Daten.

Absatz 3 wird ausschliesslich terminologisch angepasst, ebenso der Titel des Abschnitts C. vor § 16.

Die Bemerkung des Kantonsgerichts zur Verzeichnung der in den Geschäftskontrollen gespeicherten Daten (Annahme einer Ausnahme nach § 16 Absatz 3 Buchstabe d) betrifft im Kern nicht das Verzeichnis der Datensammlungen, sondern den Geltungsbereich des Datenschutzgesetzes bzw. die Reichweite der Aufsicht durch die oder den Datenschutzbeauftragten und wird deshalb bei § 22 behandelt.

IV. Abschnitt D. Rechte der betroffenen Personen (§§ 17-21)

Eine bloss terminologische Anpassung an die neue Regelung in § 16 erfährt auch die Bestimmung über die **Einsicht in die Verzeichnisse der Datensammlungen** (§ 17).

Die Regelung der **Rechte der betroffenen Personen** (§§ 18-21) genügen den Anforderungen der EU-Datenschutzrichtlinie (Artikel 12 Buchstaben a und c sowie Artikel 13) und der Europarats-Konvention 108 (Artikel 8 Buchstaben b und c sowie Artikel 9 Absatz 2). Allerdings – so zeigen häufige Fragen aus der Praxis – ist eine Präzisierung zu § 20 Absatz 3 zweckmässig. Der bisherige Text ist missverständlich: Es geht nicht um Abkehr von der Beweislastverteilung nach § 20 Absatz 2 (wenn dieser Beweis misslingt, ist die Berichtigung vorzunehmen), sondern um den Fall, wo *nach der Natur der Daten* weder die Richtigkeit noch die Unrichtigkeit bewiesen werden kann (z.B. bei Werturteilen). Nachdem diese klärende Präzisierung in mehreren Vernehmlassungen (SP, Handelskammer beider Basel und ausserdem vom Kantonsgericht) gefordert worden ist, schlägt der Regierungsrat die entsprechende Anpassung vor, obwohl sie nicht durch die Assoziierung an Schengen/Dublin notwendig wird.

V. Abschnitt E. Aufsicht (§§ 22-26)

Die Bestimmungen über die Datenschutz-Aufsicht sollen übersichtlicher werden. Deshalb werden die im Vernehmlassungsentwurf noch in einem einzigen Paragraphen (§ 22) vorgeschlagenen Regelungen neu in zwei Paragraphen (§§ 22 und 22a) aufgeteilt: § 22 enthält die Bestimmungen, welche die Datenschutz-Aufsichtsstelle generell betreffen; § 22a enthält die Bestimmungen, welche die Datenschutzbeauftragte oder den Datenschutzbeauftragten als Leiterin oder Leiter der Datenschutz-Aufsichtsstelle betreffen.

Mit § 22 Absatz 1 wird die Grundlage für die unabhängige Datenschutz-Aufsichtsstelle des Kantons geschaffen.

§ 22 Absätze 2, 3 und 4 regeln die **Unabhängigkeit**: Es wird festgehalten, dass die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben an **keine Weisungen** gebunden ist. Administrativ wird sie der Justiz-, Polizei- und Militärdirektion **zugeordnet**. Zwar wäre es, wie in den Vernehmlassungen der SP und in der Konsequenz wohl auch SVP vorgeschlagen, möglich, sie aus der Zentralverwaltung auszugliedern und der Landeskanzlei oder dem Landrat[47] zuzuordnen. Die administrative Zuordnung zu einer Direktion dürfte aber die einfachere Lösung sein; dieselbe Lösung gilt bekanntlich auch (noch) für die Finanzkontrolle, eine Institution mit einer vergleichbaren Unabhängigkeitsanforderung (§ 38 Absatz 2 Finanzhaushaltgesetz). Ausserdem wird zur Sicherstellung der Unabhängigkeit im finanziellen Sinn festgelegt, dass die Aufsichtsstelle einen eigenen **Voranschlag** zuhanden des Regierungsrats und des Landrats erstellt (Absatz 4). Der Regierungsrat kann – wie beim Voranschlag und vor allem bei den Nachtragskreditbegehren der richterlichen Behörden nach § 25 Gerichtsorganisations-

[47] Im Kanton Zürich ist die oder der Beauftragte für Datenschutz der Geschäftsleitung des Kantonsrates zugeordnet; vgl. § 30 Absatz 2 des diesbezüglich bereits in Kraft gesetzten Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4).

gesetz – einen anderen Antrag stellen, muss aber den von der Aufsichtsstelle erstellten Voranschlag unverändert mit an den Landrat weiterleiten.

Der bisherige Absatz 2 wird neu zum Absatz 5. Eine Erweiterung der Ausnahmen, etwa auf alle gerichtlichen und Strafverfolgungsbehörden, erscheint nicht sachgerecht. Die grundsätzliche Abgrenzung hat der Gesetzgeber bei der Festlegung des Geltungsbereiches vorgenommen: In hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verwaltungs- und Verfassungsgerichtsbarkeit gilt das Datenschutzgesetz nicht (§ 2 Absatz 2 Buchstaben d und e). Vor Eröffnung eines Verfahrens, nach dem Ende der Hängigkeit eines Verfahrens und im Bereich der Justizverwaltung gilt das Datenschutzgesetz aber uneingeschränkt. Die Kontrolle durch das Datenschutzkontrollorgan bezüglich der Datenbearbeitungen in diesem Kontext beeinträchtigt die richterliche Unabhängigkeit so wenig wie die Kontrolle des Finanzgebarens der Gerichte durch die Finanzkontrolle (§ 41 Finanzhaushaltsgesetz). Eine Spezialregelung drängt sich hingegen bei § 25 auf (siehe dort).

§ 22a Absatz 1 (§ 22 Absatz 1 im Vernehmlassungsentwurf) bestimmt die Wahlbehörde für die Datenschutzbeauftragte oder den Datenschutzbeauftragten und legt fest, dass sie oder er auf **Amtsperiode** gewählt wird, die gemäss Kantonsverfassung vier Jahre beträgt. **Wahlbehörde** ist der Regierungsrat unter Vorbehalt der Genehmigung durch den Landrat[48]. Personalrechtlich sind die Bestimmungen für auf Amtsperiode Gewählte nach §§ 56 ff. Personalgesetz anwendbar. Die Regelung der Wahl war Gegenstand etlicher Stellungnahmen im Vernehmlassungsverfahren: Sie wurde einerseits ausdrücklich begrüsst (CVP, Basellandschaftlicher Anwaltsverband, Handelskammer beider Basel). Anderseits wurde geltend gemacht, sie gehe viel zu weit, sei untauglich zur Sicherung der Unabhängigkeit; daraus entstand die Forderung, es solle wie bisher der Regierungsrat den oder die Datenschutzbeauftragte anstellen (FDP). Schliesslich wurde aber auch gefordert, die oder der Datenschutzbeauftragte sei einzig und allein durch den Landrat zu wählen (SVP), wie es übrigens auch für den Vorsteher oder die Vorsteher der Finanzkontrolle, einer Institution mit einer vergleichbaren Unabhängigkeitsanforderung, gesetzlich vorgesehen ist (§ 39 Finanzhaushaltsgesetz). Dem Regierungsrat ist es wichtig, beide Institutionen, Landrat und Regierungsrat, am Wahlprozess des oder der Datenschutzbeauftragten zu beteiligen, um dadurch dem Datenschutzkontrollorgan eine erhöhte Legitimation zu verschaffen. Dafür erscheint die vorgeschlagene Lösung als geeignetes Verfahren. Eine Wiederwahl ist selbstverständlich möglich. Die von der Handelkammer beider Basel geforderte ausdrückliche Verankerung der Möglichkeit einer Wiederwahl ist nach Ansicht des Regierungsrates nicht erforderlich. Es wurde im Übrigen bewusst der Begriff «Wahl» gewählt, obwohl das Personalgesetz (und der bisherige § 22) seit 1998 von «Anstellen» spricht; ein Anstellen erscheint als mit der Vertragsunterzeichnung abgeschlossenes Verfahren für die vertragliche Verpflichtung von Mitarbeitenden der Verwaltung. Mit der Ernennung auf Amtsperiode und dem Vorbehalt der Genehmigung durch den Landrat erscheint dies schlecht verträglich.

---

[48] Die gleiche Lösung wurde im Kanton Zürich gewählt: § 30 Absatz 1 des diesbezüglich bereits in Kraft gesetzten Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4).

Zur Unabhängigkeit der Aufsichtsstelle gehört auch, dass der oder die Datenschutzbeauftragte – natürlich im Rahmen des vom Landrat genehmigten Voranschlags – die weiteren **Mitarbeitenden** der Aufsichtsstelle selbständig anstellt (§ 22a Absatz 3).

§ 23 sieht bisher vor, dass die Gemeinden für den **kommunalen Bereich** ein eigenes Datenschutzkontrollorgan schaffen können. Diese Kompetenz kann bestehen bleiben, doch muss ein solches kommunales Datenschutzkontrollorgan den Anforderungen an Unabhängigkeit und Wirksamkeit genügen, sonst kann es eben nicht das von der EU-Datenschutzrichtlinie und vom Zusatzprotokoll zur Europarats-Konvention 108 geforderte Kontrollorgan sein. Diese Konsequenz wird in § 23 nun festgehalten. Weil keine einzige Gemeinde bisher eine kommunale Datenschutzaufsichtsstelle geschaffen hat – bzw. die Gemeinde Gelterkinden als einzige, die es getan hat, sie inzwischen wieder abgeschafft hat –, könnte auf die Bestimmung auch gerade verzichtet werden. Es ist jedoch nicht erforderlich, die Gemeindeautonomie in diesem Punkt zu beschneiden. Der neue Absatz 3 verweist für die Aufgaben und Befugnisse auf die (primär für die kantonale Datenschutz-Aufsichtsstelle geltenden) §§ 24 und 25.

§ 24 enthält den **Aufgabenkatalog** der Aufsichtsstelle. Dieser Katalog wird, wie vorne erwähnt[49], gesamthaft neu formuliert:

- Buchstabe a enthält den **Kontrollauftrag**; anstelle des Begriffs «überwachen», der – unzutreffenderweise – die Vorstellung einer permanenten, lückenlosen Überwachung weckt, wird neu das Verb «kontrollieren» verwendet. Ausserdem wird im Sinne einer Garantie der Unabhängigkeit festgehalten, dass diese Kontrolle nach einem durch die Aufsichtsstelle **autonom aufzustellenden Prüfprogramm** durchzuführen ist.

- Buchstabe b in seiner bisherigen Fassung wird durch die Änderung des § 16 hinfällig. Dafür wird hier die **Vorabkontrolle** gemäss § 15a zur Aufgabe gemacht.

- Buchstabe c enthielt bisher relativ nebensächliche Bestimmungen: Die Aufgabe der Zustimmung zur Bekanntgabe von Personendaten zu nicht-personenbezogener Bearbeitung durch Private und ausserkantonale Amtsstellen (gemäss § 12 Absatz 4 Buchstabe a) wird neu in Buchstabe h erwähnt. Der Satzteil 2, die Aufgabe der Entscheidung über die Registrierpflicht, kann gestrichen werden. Bei den dezentralen Verzeichnissen der Datensammlungen nach § 16 liegt die Verantwortung bei den verantwortlichen Behörden; ist die Aufsichtsstelle der Auffassung, eine nicht verzeichnete Datensammlung sei zu Unrecht nicht in ein Verzeichnis aufgenommen worden, so kann sie eine Empfehlung gemäss § 25 Absatz 3 (neu) erlassen. Neu wird an dieser Stelle die Aufgabe der **Beratung der Behörden** aufgenommen; sie war bisher in Buchstabe g erwähnt, wird hier aber auf das Wesentliche reduziert.

---

[49] Oben S. 14.

- In Buchstabe d war bisher die Aufgabe zur Bezeichnung der verantwortlichen Behörde gemäss § 4 Absatz 2 enthalten; sie hat in der Praxis keine grosse Bedeutung und wird neu in Buchstabe h aufgeführt. Neu wird – unmittelbar nach dem Auftrag zur Beratung der Behörden – die Aufgabe, die **betroffenen Personen über ihre Rechte zu beraten** (bisher Buchstabe e), festgehalten.

- In Buchstabe e folgt sodann in logischer Abfolge die Aufgabe, zwischen betroffenen Personen und Behörden zu **vermitteln** (bisher Buchstabe f).

- In Buchstabe f wird anschliessend die Aufgabe, **zu Erlassen**, die für den Datenschutz erheblich sind, **Stellung zu nehmen** (bisher Buchstabe h), aufgeführt.

- Nachdem der bisherige Inhalt des Buchstaben g (Beratung der Behörden) – auf das Wesentliche reduziert – bereits in Buchstabe c aufgenommen worden ist, kann hier die Pflicht aufgenommen werden, der Wahlbehörde periodisch – wohl jährlich – über die Tätigkeit, Feststellungen und Erfahrungen **Bericht** zu erstatten, wie es Artikel 28 Absatz 5 EU-Datenschutzrichtlinie verlangt.

- Buchstabe h (bisher die Pflicht zur Stellungnahme zu datenschutzrelevanten Erlassen, neu in Buchstabe f) nimmt die oben erwähnten Nebenpflichten auf: die Kompetenz zur **Bezeichnung der verantwortlichen Behörde** gemäss § 4 Absatz 2 (bisher Buchstabe d) und die Kompetenz zur Zustimmung zur Bekanntgabe von Personendaten zu nicht-personenbezogener Bearbeitung durch Private und ausserkantonale Amtsstellen (bisher Buchstabe c Satzteil 1).

- Buchstabe i (bisher die Berichterstattungspflicht, neu in Buchstabe g) enthält neu die von Artikel 28 Absatz 6 EU-Datenschutzrichtlinie und von Artikel 1 Ziffer 5 Zusatzprotokoll zur Europarats-Konvention 108 verlangte Aufgabe des Kontrollorgans, zur Erfüllung seiner Aufgaben mit den Datenschutzkontrollorganen der Gemeinden, der anderen Kantone, des Bundes und des Auslandes **zusammenzuarbeiten**.

§ 25 behandelt die **Arbeitsweise der Aufsichtsstelle** und hält deren **Befugnisse** fest. Um die Anforderungen der EU-Datenschutzrichtlinie und der Europarats-Konvention 108 samt Zusatzprotokoll zu erfüllen, sind – wie oben bereits dargestellt – schwergewichtig zwei Anpassungen notwendig: eine erste bei den Untersuchungsbefugnissen, wo die Auslagerung der Datenbearbeitung an Dritte keine Einschränkung der Befugnisse des Datenschutzkontrollorgans rechtfertigt, und zweitens die Verstärkung der Einwirkungsbefugnisse. Aus diesem Grund werden in § 25 Absatz 1 der Aufsichtsstelle die gleichen **Untersuchungsbefugnisse** gegenüber Privaten, die Personendaten im Auftrag von Behörden bearbeiten, wie gegenüber den die Daten selber bearbeitenden Behörden vorgesehen. Der bisherige Absatz 2 entfällt deshalb; an seine Stelle rückt die Pflicht der Behörden, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu **unterstützen** (bisher Absatz 4). Der Inhalt des bisherigen Absatzes 3 bleibt am Ende des § 25, wird damit neu zum Absatz 7.

In den Absätzen 3-6 wird das oben[50] dargestellte Konzept zur Stärkung der **Einwirkungsbefugnisse** umgesetzt:

- In Absatz 3 wird festgehalten, dass das Datenschutzkontrollorgan zu Datenbearbeitungen **Empfehlungen** abgeben kann und dass die Behörde, an welche die Empfehlung gerichtet ist, gegenüber der Aufsichtsstelle zu erklären hat, ob es der Empfehlung **folgen** will. Nicht jede Äusserung der Aufsichtsstelle ist eine Empfehlung in diesem Sinne: Sie kann auf formlos – zum Beispiel auf telefonische Anfrage oder im Rahmen von Besprechungen mit einer Behörde – Auskünfte erteilen oder zu Fragen Stellung nehmen.

- Für den Fall, dass die Behörde erklärt, der Empfehlung nicht folgen zu wollen, oder der Empfehlung tatsächlich nicht folgt, so kann die Aufsichtsstelle, soweit das Interesse an der Durchsetzung überwiegt, ihre Empfehlung als Ganzes oder Teile davon als **Weisung** in Form einer Verfügung erlassen (Absatz 4). Dabei wird sich die Aufsichtsstelle auf den wesentlichen Kern einer Empfehlung beschränken, z.B. eine bestimmte, als rechtswidrig oder unverhältnismässig beurteilte Datenbearbeitung zu unterlassen oder die erforderlichen organisatorischen oder technischen Massnahmen nach § 14 zu ergreifen. Mit der Formulierung «in Form einer Verfügung» wird erreicht, dass für alle hier nicht separat geregelten Modalitäten an das Verwaltungsverfahrensgesetz angeknüpft werden kann. Mögliche Weisungsadressaten sind sicher alle Behörden im Sinne von § 3; darüber hinaus kommen aber auch Behörden im Sinne des materiellen, funktionsbezogenen Behördenbegriffs (vgl. oben Seite 20 zu § 3) in Betracht; das bedeutet, dass beispielsweise Schulleitungen, die auch selber Verfügungen erlassen können, im Bereich ihrer Datenbearbeitungen – die häufig gerade im Verhältnis Schulleitung/ Schulrat/ Gemeinderat heikle Rechtsfragen aufwerfen – Weisungsadressaten gemäss § 25 Absatz 4 sein können.

- Nach Absatz 5 kann die Behörde, an welche die Weisung gerichtet ist, diese mit einer **Beschwerde** gemäss den §§ 27 ff. Verwaltungsverfahrensgesetz beim Regierungsrat anfechten (im Sinne von § 29 Absatz 1 Buchstabe f Verwaltungsverfahrensgesetz). Auf den ersten Blick spricht die Unabhängigkeit der Aufsichtsstelle gegen den Regierungsrat als Beschwerdeinstanz. Es soll ihm als Exekutivspitze aber die Gelegenheit gegeben werden, über den Gegenstand der Weisung zuerst zu entscheiden. Mit dem Beschwerderecht der Aufsichtsstelle nach § 25 Absatz 6 wird der Weg zu einer gerichtlichen Instanz aber sichergestellt. Die Weisung stellt eine erstinstanzliche Verfügung im Sinne des § 27 Absatz 1 Buchstabe a Verwaltungsverfahrensgesetz dar. Mit dem Verweis auf das Verwaltungsverfahrensgesetz wird erreicht, dass die Vorschriften dieses Gesetzes über Beschwerdegründe, Form und Frist ohne weiteres anwendbar werden. Da auch Anstalten des kantonalen öffentlichen Rechts Adressaten einer solchen Weisung sein können (z.B. die Sozialversicherungsanstalt des Kantons Basel-Landschaft),

[50] Oben S. 15 f.

über welche der Regierungsrat keine Aufsichtsbefugnis besitzt, ist in Absatz 5 ausserdem vorgesehen, dass hier die Beschwerde direkt ans Kantonsgericht zu richten ist.

- Weil im Kanton letztlich das Kantonsgericht als oberste richterliche Behörde über eine Weisung des Datenschutzkontrollorgans zu entscheiden hat, macht es keinen Sinn, dass der oder die Datenschutzbeauftragte gegenüber dem Kantonsgericht Weisungen erlassen kann (Absatz 5 Satz 2). Gegenüber anderen richterlichen Behörden ist der Erlass von Weisungen im Bereich der Justizverwaltung möglich; in hängigen Verfahren der Zivil- und Strafrechtspflege sowie der Verwaltungs- und Verfassungsgerichtsbarkeit findet das Datenschutzgesetz nach § 2 Absatz 2 Buchstaben d und e keine Anwendung, womit auch die Zuständigkeit des Datenschutzkontrollorgans entfällt.

- Zur Sicherstellung der Unabhängigkeit des Datenschutzkontrollorgans ist es erforderlich, dass das Datenschutzkontrollorgan gegen Beschwerdeentscheide des Regierungsrates gegen seine Weisungen **beschwerdeberechtigt** ist (Absatz 6). Andernfalls würde der Regierungsrat als Spitze der Verwaltung endgültig über die Weisung des Datenschutzkontrollorgans entscheiden, was mit der Anforderung der völligen Unabhängigkeit nach der EU-Datenschutzrichtlinie und dem Zusatzprotokoll zur Europarats-Konvention 108 nicht vereinbar wäre. Falls der Regierungsrat die Beschwerde eines Weisungsadressaten (ganz oder teilweise) gutheisst, kann die Aufsichtsstelle den Entscheid also an das Kantonsgericht weiterziehen; nur so kann gewährleistet werden, dass der Rechtsweg zu einer gerichtlichen Instanz offen steht.

Die bisher in § 25 Absatz 3 geregelte Befugnis der Aufsichtsstelle, die verantwortliche Behörde oder deren vorgesetzte Behörden aufzufordern, unverzüglich die erforderlichen Massnahmen zu ergreifen, wenn schutzwürdige Interessen einer betroffenen Person offensichtlich gefährdet oder verletzt werden, wird neu zu Absatz 7.

Die in der Vernehmlassung der FDP verlangte Belassung des bisherigen Rechts (einzig mit dem Recht des Kontrollorgans, für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen), vermag den Anforderungen an wirksame Einwirkungsbefugnisse in keiner Weise zu genügen. Vom Basellandschaftlichen Anwaltsverband wird die vorgeschlagene Regelung ausdrücklich begrüsst; insbesondere wird als zweckmässig erachtet, dass nicht die verantwortliche Behörde, die sich einer Empfehlung der Aufsichtsstelle widersetzt, eine anfechtbare Verfügung zu erlassen habe, wie dies in anderen Kantonen zur Diskussion stehe[51]. Mit der gewählten Lösung kann der Streitgegenstand gezielt auf den wesentlichen Gehalt der nicht oder teilweise nicht befolgten Empfehlung reduziert werden.

Die Geheimhaltungspflicht (§ 26) entspricht den Anforderungen der EU-Datenschutzrichtlinie und des Zusatzprotokolls zur Europarats-Konvention 108 und bedarf deshalb keiner Anpassung.

---

[51] Vgl. z.B. im Kanton Zürich Artikel 36 Absatz 2 des (kantonalzürcherschen) erst teilweise in Kraft gesetzten Gesetzes vom 12. Februar 2007 über die Information und den Datenschutz (IDG-ZH, LS 170.4).

Für auf Amtsperiode Gewählte muss eine Disziplinarbehörde bestimmt werden. Disziplinarbehörde der oder des Datenschutzbeauftragten ist der Landrat (Änderung von § 60 Buchstabe a des Personalgesetzes).

VI. Abschnitt F. Verfahren und Rechtsschutz

§ 27 Absatz 1 beinhaltet die **Anfechtbarkeit** jeder Art von Entscheidungen des Datenschutzkontrollorgans in dem Masse, als ihnen verbindliche Wirkung zukommt. Damit entspricht er den Anforderungen von Artikel 28 Absatz 3 am Ende EU-Datenschutzrichtlinie und von Artikel 1 Ziffer 4 Zusatzprotokoll zur Europarats-Konvention 108. Absatz 2 kann bestehen bleiben, solange die Kompetenz der Gemeinden, ein eigenes Datenschutzkontrollorgan im Sinne von § 23 zu schaffen, besteht.

§ 28 (Rechtsschutz im medizinischen und sozialen Bereich sowie im Straf- und Massnahmenvollzug) bedarf keiner Anpassung aufgrund der Assoziierung der Schweiz an Schengen/ Dublin.

§ 29 regelt die **Gebühren**, die für Verrichtungen nach dem Datenschutzgesetz erhoben werden dürfen. Eine terminologische Anpassung ist einzig in Absatz 2 Buchstabe c wegen der Schaffung dezentraler Verzeichnisse der Datensammlungen anstelle des bisherigen zentralen Registers erforderlich.

VII. Abschnitt G. Schlussbestimmungen

Übergangsfristen sind für zwei Bereiche vorzusehen:

- Nach dem neuen Absatz 2 des § 6 dürfen **besondere Personendaten und Persönlichkeitsprofile** bearbeitet werden, wenn sich die Zulässigkeit aus einer gesetzlichen Grundlage klar ergibt oder wenn es zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe unentbehrlich ist. Wo diese qualifizierten Anforderungen zurzeit noch nicht erfüllt werden, sind innert zweier Jahre ab Inkrafttreten des revidierten § 6 nötigen Anpassungen zu schaffen (§ 32a Absatz 1).

- Nach dem revidierten § 16 veröffentlichen die Behörden ein vollständiges **Verzeichnis über ihre Datensammlungen**. Diese Verzeichnisse sind innert zweier Jahre nach Inkrafttreten des revidierten § 16 zu veröffentlichen (§ 32a Absatz 2).

- Beide Übergangsfristen können vom Regierungsrat auf begründetes Gesuch hin um ein Jahr verlängert werden (§ 32a Absatz 3).

E Finanzielle und personelle Folgen

Die Umsetzung des revidierten Datenschutzgesetzes infolge der Assoziierung an Schengen/Dublin bringt der Aufsichtsstelle Datenschutz gegenüber heute einen Mehraufwand (zu-

sätzliche Kontrollaufgaben, erweiterte Berichterstattungspflicht, Anzeige- und Klagerecht, Vorabkontrolle u.a.). Wir gehen davon aus, dass der Mehraufwand im Rahmen eines Pensums von 50% bis 100% liegen wird. Daraus ergeben sich jährliche Mehrkosten in der Grössenordnung von CHF 120'000.-- und 170'000.-- (eingeschlossen Raum- und Ausstattungskosten). Es ist – auch bei einer pragmatischen und unkomplizierten Weise der Umsetzung, wie sie von der SVP in ihrer Vernehmlassung gefordert und von der Aufsichtsstelle Datenschutz auch bereits in der Vergangenheit gelebt wurde – nicht möglich, die Mehrarbeit mit dem aktuellen, eher knapp bemessenen Mitarbeiterbestand (200 Stellenprozente) und damit ohne Personalerhöhung zu bewältigen.

F Antrag an den Landrat

Der Regierungsrat beantragt dem Landrat, auf die Vorlage einzutreten und gemäss beiliegendem Entwurf zu beschliessen.

Liestal, 10. Juli 2007

Im Namen des Regierungsrates
die Präsidentin:
Pegoraro

der Landschreiber:
Mundschin

Beilagen:
1. Entwurf zur Revision des Datenschutzgesetzes
2. Synopse