Regierungsrat des Kantons Basel-Stadt

An den Grossen Rat 05.1024.01

JD/P051024
Basel, 26. September 2007

Regierungsratsbeschluss
vom 25. September 2007

Ratschlag und Entwurf

betreffend

Teilrevision des Gesetzes über den Schutz von Personendaten (Datenschutzgesetz) vom 18. März 1992 (SG 153.260): Anpassung an Schengen/Dublin

Den Mitgliedern des Grossen Rates des Kantons Basel-Stadt zugestellt am 28. September 2007

Ratschlag betreffend Teilrevision des Gesetzes über den Schutz von Personendaten (Datenschutzgesetz): Anpassung an Schengen/Dublin

Inhaltsverzeichnis

A Kurzübersicht

Zum Schutz der Rechte und Freiheiten der Personen haben sich die Mitgliedstaaten der Europäischen Union (EU) sowie der Europarat darauf geeinigt, dass alle Mitgliedstaaten im Datenschutz die gleichen Mindest-Regeln vorsehen, um ein einheitliches Schutzniveau gewährleisten zu können. Dazu hat sich mit dem **Beitritt zu den Abkommen von Schengen/Dublin** am 5. Juni 2005 auch die Schweiz verpflichtet. Der Bund und die Kantone sind gehalten, ihre Datenschutzgesetze an das europäische Datenschutzniveau anzugleichen, sofern diese das Datenschutzniveau noch nicht erreichen.

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 EU-Datenschutzrichtlinie, genügen.

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.

Der Vergleich zwischen den Anforderungen aufgrund des EU-Rechts mit dem gegebenen Recht ergibt, dass das Datenschutzgesetz den Anforderungen des EU-Rechts weitgehend Stand hält. **Handlungsbedarf** besteht aber in folgenden Punkten: Der Ausschluss der Anwendbarkeit des Datenschutzgesetzgesetzes auf hängige Verwaltungsverfahren und verwaltungsinterne Rekursverfahren ist unzulässig. Die Transparenz der Datenbearbeitungen ist für die betroffene Person nicht genügend gewährleistet. Es fehlt – ausser gegenüber den Einwohnerkontrollen – ein Anspruch der betroffenen Person auf Sperrung der Bekanntgabe ihrer Daten. Auch fehlen griffige Bestimmungen zur Gewährleistung eines angemessenen Schutzes bei der Bekanntgabe von Personendaten ins Ausland und eine Vorabkontrolle durch die Datenschutz-Aufsichtsstelle bei Datenbearbeitungen mit einem höheren Gefährdungspotential. 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.

Die Kantone Basel-Stadt und Basel-Landschaft sind derzeit daran, ihre Datenschutzgesetze einer Totalrevision zu unterziehen. Die Anpassungen an das EU-Recht müssen allerdings vorgezogen werden, da bis im August 2007 eine Vorlage zur Anpassung des Datenschutzgesetzes an das Parlament vorliegen muss. Im Hinblick auf eine übereinstimmende Gesetzgebung stimmen die Gesetzesentwürfe der beiden Kantone weitgehend überein.

B Ausgangslage

I. Schengen/Dublin

1. Abkommen von Schengen/Dublin

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»[1]). Die Umsetzungsgesetzgebung des Bundes wurde von den Eidgenössischen Räten am 17. Dezember 2004 gleichzeitig mit den Genehmigungsbeschlüssen verabschiedet.[2]

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**[3]. 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% 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 Weiterentwicklung 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.[4]

---

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

2 BBl 2004 7149 ff.

3 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.

4 Art. 15 SAA (Fn. 3).

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 Ratifikation der Verträge von Schengen/Dublin durch die EU voraussichtlich Ende dieses Jahres wird die EU in einem speziellen Evaluationsverfahren die Umsetzung der Schengen Vorschriften in der Schweiz prüfen. Mit dem definitiven Inkrafttreten der Abkommen für die Schweiz ist im Herbst 2008 zu rechnen.

Die Kantone wurden aufgefordert, sich an diesen Zeitplan zu halten. Die kantonalen Gesetze müssen im Zeitpunkt der Evaluation noch nicht in Kraft sein. Der Gesetzgebungsprozess in den Kantonen muss aber so weit fortgeschritten sein, dass für die EU ersichtlich ist, welches Recht bei der Inkraftsetzung von Schengen/Dublin gelten wird. Daraus ergibt sich, dass eine Vorlage zur Anpassung des Datenschutzgesetzes an Schengen/Dublin im August 2007 vorliegen muss, weshalb die zur Zeit partnerschaftlich laufende Totalrevision der Datenschutzgesetze BS und BL nicht abgewartet werden kann.

2. 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 ausgewoge-

ne Verteilung der Asylsuchenden auf die Dublin-Staaten. Dank der elektronischen Datenbank «Eurodac» können mehrfach gestellte Asylgesuche systematisch erkannt werden.[5]

3. Auswirkungen im Bereich des Datenschutzes

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 einem **entsprechenden Datenschutzstandard**. Die Europäische Union hat deshalb nicht bloss die Aufgabenerfüllung umschrieben und wirkungsvolle Informationssysteme bereitgestellt (das Schengener Informationssystem SIS[6] und – für Dublin – Eurodac[7]), 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)[8] datenschutzrechtliche Regelungen. Darüber hinaus müssen alle Datenbearbeitungen, die unter den so genannten ersten Pfeiler der EU fallen, den Anforderungen der **EU-Datenschutzrichtlinie**[9] genügen. Unter den ersten Pfeiler fallen die Bereiche Grenzkontrollen, Visa, Feuerwaffen, teilweise Betäubungsmittel und Asyl. Durch Artikel 2 Abs. 2 in Verbindung mit Anhang B des Schengen-Assoziierungs-Abkommens (SAA)[10] 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 die spezifischen, direkt anwendbaren Schutzvorschriften über die Datenbearbeitungen im Zusammenhang mit dem SIS und ausserhalb des SIS. Es verlangt dabei die Gewährleistung eines Datenschutzstandards, der zumindest dem ent-

---

5 Vgl. Botschaft des Bundesrates vom 1. Oktober 2004, BBl 2004 5968.

6 Vgl. Teil IV (Art. 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.).

7 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.).

8 Vgl. oben Fn. 6.

9 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. L 281 vom 23/11/1995 S. 0031-0050,

10 Vgl. oben Fn. 3 (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.

spricht, 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)[11] ergibt.[12] Es ist aber absehbar, dass die EU für die Bearbeitungen im Bereich des dritten Pfeilers demnächst vergleichbare Datenschutzregeln aufstellen wird.[13]

Das kantonale Datenschutzgesetz vom 18. März 1992 (SG 153.260) 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.[14]

II. Datenschutzgesetzrevision im Bund und Ratifikation des Zusatzprotokolls zur Europarats-Konvention 18

Die Eidgenössischen Räte haben am 24. März 2006 die **Revision[15] 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**)[16] 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 Datenübermittlung beitreten kann. Eine generelle Anpassung an das europäische Datenschutzrecht war aber erklärtermassen noch nicht das Ziel der DSG-Revision des Bundes.

---

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

12 Art. 117 SDÜ für Datenbearbeitungen im Rahmen des SIS, Art. 126 SDÜ für Datenbearbeitungen ausserhalb des Rahmens des SIS.

13 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).

14 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.

15 BBl 2006 3547 ff.

16 BBl 2003 S. 2167 ff.

Die Gesetzesänderung sieht für datenbearbeitende Personen 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 Angaben des Bundesamtes für Justiz – voraussichtlich nicht vor Herbst 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.[17] Dem Bund kommt keine umfassende Datenschutz-Kompetenz zu.[18] Auch der – in der beschlossenen Revision qualitativ verstärkte – Art. 37 Bundesdatenschutzgesetz gilt ausschliesslich dann, wenn kantonale Organe Bundesrecht vollziehen;[19] die subsidiäre Geltung bestimmter Bestimmungen des Bundesdatenschutzgesetzes vermag also gerade in den Bereichen kantonaler Rechtsetzungskompetenzen das Fehlen kantonaler Datenschutzbestimmungen nicht zu kompensieren.[20] 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.

Auf interkantonaler Ebene haben die Plenarversammlungen der Konferenz der Kantonsregierungen (KdK) und der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -di-

---

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

18 Vgl. allgemein zum Handlungsbedarf in den Kantone BEAT RUDIN/ BRUNO BAERISWYL, (Fn. 10), 169 ff.

19 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.

20 Zur innerstaatlichen Rechtsetzungskompetenz vgl. BEAT RUDIN/ BRUNO BAERISWYL (Fn. 10), insb. 178 f.

rektoren (KKJPD) am 1. Oktober 2004 bzw. 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.

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 begleitet. Die KdK-Wegleitung[21] 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 des Kantons Basel-Landschaft hat den Verfasser der KdK-Wegleitung anschliessend beauftragt, den Handlungsbedarf im basellandschaftlichen Recht zu beurteilen und Vorschläge für die notwendigen Anpassungen vorzulegen. Die vorliegende Vorlage orientiert sich an diesem Entwurf, da bereits Bestrebungen im Gange sind, die beiden Datenschutzgesetze BS und BL gemeinsam zu revidieren. Ein entsprechender Entwurf wird dem Grossen Rat gemäss dem im Zusammenhang mit dem Systemwechsel von der Datenschutzkommission zum Datenschutzbeauftragten im Jahr 2005 erteilten Auftrag im Jahr 2008 unterbreitet werden.

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-Stadt Handlungsbedarf in folgenden Punkten:

Der Ausschluss der Anwendbarkeit des Datenschutzgesetzgesetzes auf hängige Verwaltungsverfahren und verwaltungsinterne Rekursverfahren ist unzulässig. Die Transparenz der Datenbearbeitungen ist für die betroffene Person nicht genügend gewährleistet und es fehlt – ausser gegenüber den Einwohnerkontrollen – ein Anspruch der betroffenen Person auf Sperrung der Bekanntgabe ihrer Daten. Ebenso 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

[21] Abrufbar unter <http://www.datenschutz.ch/themen/2006_kdk_schengen_dublin_datenschutz_wegleitung.pdf> (letztmals kontrolliert: 7.9.2007).

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. 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 können die fehlenden Regelungen relativ einfach eingefügt werden. Zur Behebung der ermittelten Defizite schlägt der Regierungsrat dafür die folgenden Anpassungen vor:

- Um einen genügenden Schutz der Personendaten in hängigen Verwaltungsverfahren und verwaltungsinternen Rekursverfahren zu gewährleisten, werden diese beiden Verfahren in § 4 Abs. 2 ausgenommen und damit der Geltungsbereich des Datenschutzgesetzes auf diese ausgedehnt.

- Um dem Transparenzgebot zu genügen, wird in § 9 verlangt, dass die Datenerhebung in der Regel für die betroffene Person erkennbar sein muss.

- In § 13 wird ebenso der Anspruch der betroffenen Person, die Bekanntgabe ihrer Personendaten sperren zu lassen, festgehalten (mit der Möglichkeit der Bekanntgabe trotz Sperrung).

- Die Voraussetzungen für den Datentransfer ins Ausland werden in § 14 eingefügt.

- In § 18a wird die Pflicht zur Vorabkontrolle eingefügt.

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.[22] 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.[23]

---

22 Siehe Art. 28 EU-Datenschutzrichtlinie oben B.I.4.

23 Zum Datenschutzkontrollorgan vgl. Abs. 2 der Präambel sowie Art. 1 Zusatzprotokoll zur Europarats-Konvention 108.

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»[24]. *«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.»*[25]

Um die verlangte völlige Unabhängigkeit des Datenschutz-Kontrollorgans zu gewährleisten, sind nach der KdK-Wegleitung[26] – leicht gekürzt – die folgenden institutionellen Garantien unabdingbar:

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.

---

24 KdK-Wegleitung, 21 (Erläuterungen zur Checkliste, Ziff. 7.5).

25 KdK-Wegleitung, 21 f. (Erläuterungen zur Checkliste, Ziff. 7.6).

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

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.

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.

Der Regierungsrat schlägt die entsprechenden Regelungen in den §§ 26 und 26a vor. § 26 enthält die Bestimmungen, welche die Datenschutz-Aufsichtsstelle generell betreffen; § 26a enthält die Bestimmungen, welche die Datenschutzbeauftragte oder den Datenschutzbeauftragten als Leiterin oder Leiter der Datenschutz-Aufsichtsstelle betreffen. Die oder der Datenschutzbeauftragte soll von Regierungsrat unter Vorbehalt der Genehmigung durch den Grossen Rat gewählt werden. Mit dieser Lösung kann erreicht werden, dass beide Gewalten – Grosser Rat und Regierungsrat – an der Wahl beteiligt sind, was die Datenschutz-Aufsichtsstelle in ihrer Stellung gegenüber der datenbearbeitenden Verwaltung stärkt. Die Amtsdauer soll nicht, wie es für unabhängige Behördenmitglieder üblich ist, sechs Jahre betragen, sondern bloss vier Jahre. Damit wird eine einheitliche Regelung mit dem Kanton

Basel-Landschaft getroffen. In § 53 Kantonsverfassung BL ist eine Amtsdauer von vier Jahren für Behördenmitglieder und gewählte Mitarbeiterinnen und Mitarbeiter explizit geregelt. Die vollständige Unabhängigkeit des Kontrollorgans wird ausdrücklich festgeschrieben; ausserdem wird festgelegt, dass es über ein eigenes Budget verfügt und dass es die weiteren Mitarbeitenden der Datenschutz-Aufsichtsstelle selbständig anstellt.

b. Aufgaben

Die **Aufgaben** des Datenschutzkontrollorgans sind in § 28 festgehalten. Der bisherige Katalog ist unvollständig. Es fehlen z.B. der Hinweis auf die Veröffentlichung der Berichterstattung sowie die Pflicht zur Zusammenarbeit mit den Datenschutzkontrollorganen der anderen Kantone, des Bundes und des Auslandes. Aus diesem Grund ist der Aufgabenkatalog anzupassen.

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 § 29 Abs. 2 und 4 festgeschrieben. Dabei schränkt Abs. 4 die Aufsichtsbefugnisse der Aufsichtsstelle gegenüber Drittpersonen, die von einem verantwortlichen Organ mit dem Bearbeiten von Personendaten beauftragt sind oder von ihm Personendaten erhalten haben, ein: Anders als wenn die verantwortlichen Organe die Daten selber bearbeiten, soll sie keine Besichtigung durchführen und sich keine Bearbeitungen vorführen lassen dürfen; hingegen darf sie – wie gegenüber den die Daten selber bearbeitenden Organen – mündlich oder schriftlich Auskunft über Datenbearbeitungen einholen sowie Einsicht in alle Unterlagen nehmen. Solche Restriktionen sind nach Art. 28 Abs. 3 EU-Datenschutzrichtlinie und Art. 1 Ziff. 2 lit. a Zusatzprotokoll zur Europarats-Konvention 108 nicht vorgesehen. Es ist im Übrigen auch nicht im Interesse der auftraggebenden Organen, die Aufsicht schwächer ausfallen zu lassen, bleiben diese doch gegenüber den in ihren Persönlichkeitsrechten verletzten betroffenen Personen vollumfänglich verantwortlich, auch wenn die rechtswidrige Bearbeitung durch Dritte entgegen ihrer Weisung verschuldet wird (§ 7 Abs. 1: «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 Organen wie gegenüber Dritten, die in ihrem Auftrag Daten bearbeiten, gleich zu regeln.

Bei der Frage der «**wirksamen Einwirkungsbefugnisse**» legt die 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.[27] Es muss somit mit einer Kombination von Befugnissen erreicht werden, dass die Kontrolle insgesamt wirksam erfolgen kann.

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 auffordern, die erforderlichen Massnahmen zu ergreifen – eine Art aufsichtsrechtliche Anzeige ohne rechtlich verbindliche Wirkung. Diese 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 **Rekurs** gegen die Weisung des Datenschutzkontrollorgans bei der zuständigen Rechtsmittelinstanz (in der Regel beim Regierungsrat oder beim Appellationsgericht 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 § 99 Strafprozessordnung (Anzeigepflicht bei konkreten Anzeichen, die auf eine strafbare Handlung oder deren Täterschaft hinweisen) und § 51 Organisationsgesetz (aufsichtsrechtliche Anzeige) die nötigen Befugnisse bereits einräumen und es deshalb keiner Anpassung im Datenschutzgesetz bedarf.

---

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

C Kommentar zu den einzelnen Bestimmungen

I. Vorbehaltenes Recht (§ 4)

Gemäss § 4 Abs. 2 findet das Datenschutzgesetz keine Anwendung auf Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege. Der Grund liegt darin, dass die Verfahrensgesetze den Anspruch auf rechtliches Gehör, auf Akteneinsicht und die Begründungspflicht selbständig ordnen. Es soll vermieden werden, dass nebeneinander zwei Regelungen bestehen, welche im Wesentlichen denselben Schutzzweck verfolgen.[28] Gemäss KdK-Wegleitung[29] ist es zulässig, eine Ausnahme für hängige Verfahren der Zivil- und Strafrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit vorzusehen, wenn die dadurch zur Anwendung gelangende Prozessordnung die nötigen Regelungen (insb. zur Beschaffung und Bekanntgabe von Personendaten sowie zu den Rechten der betroffenen Personen und zur Aufsicht) enthält. Das Verwaltungsverfahren und das verwaltungsinterne Rekursverfahren können indes nicht vom Geltungsbereich ausgenommen werden. Aus diesem Grund wird der Ausschluss der Anwendbarkeit des Datenschutzgesetzes auf hängige Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit beschränkt.

II. Erhebung (Erkennbarkeit der Beschaffung, § 9)

Transparenz bezüglich der Bearbeitung von Personendaten ist eines der Kernanliegen des Datenschutzrechts. Das **Transparenzgebot**, wie es in Art. 10, 11 und 21 EU-Datenschutzrichtlinie und Art. 8 lit. 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 der datenbearbeitenden Person) 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 (vgl. § 8 und § 19). § 9 enthält unter dem Titel „Erhebung“ bisher bloss ein Transparenzgebot für den Fall der systematischen Erhebung von Personendaten, namentlich mit Fragenbogen (Abs. 1), und der Erhebung von besonders schützenswerten Personendaten (Abs. 2). 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 § 9 Satz 1 wird neu zum Abs. 2 mit einer bloss terminologischen Änderung: Der Begriff «bekanntgeben» wird im Datenschutzrecht verwendet für die Bekanntgabe von Per-

---

[28] Ratschlag und Entwurf zu einem Gesetz über den Schutz der Personendaten (Datenschutzgesetz) Nr. 7940 vom 10. Oktober 1986, S. 19 f.

[29] KdK-Wegleitung, 11 (Erläuterungen zur Checkliste, Ziff. 2.3 und 2.4).

sonendaten an Dritte (an andere als die datenbearbeitende Behörde oder an Private gemäss § 10 bzw. §§ 11 f.); hier geht es einfach darum, dass die erwähnten Informationen auf dem Fragebogen angegeben sind.

III. Recht auf Sperrung (§ 13)

§ 13, der sich bisher nur an die Einwohnerkontrolle richtet, wird in ein allgemeines Sperrrecht umformuliert. Art. 12 lit. b EU-Datenschutzrichtlinie postuliert das Recht der betroffenen Person, die Bekanntgabe der sie betreffenden Personendaten sperren zu lassen. Danach kann die betroffene Person bei der verantwortlichen Behörde die **Bekanntgabe ihrer Daten sperren** lassen. Nicht jede Bekanntgabe kann ins Belieben der betroffenen Person gelegt werden. Deshalb ist die Bekanntgabe – wie bisher nach § 13 lit. a und b gegenüber der Einwohnerkontrolle – trotz Sperrung zulässig, wenn die Behörde zur Bekanntgabe gesetzlich verpflichtet ist oder die um Auskunft ersuchende Person glaubhaft macht, dass die Personendaten zur Durchsetzung ihrer Rechtsansprüche erforderlich sind. Zusätzlich ist analog zur Regelung in BL vorzusehen, dass die Bekanntgabe trotz Sperrung auch zulässig ist, wenn die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist. Mit dieser Ergänzung und der gesetzlichen Verpflichtung zur Bekanntgabe sind die beiden Fälle der Bekanntgabe von Personendaten an öffentliche Organe abgedeckt. Da es sich also bei § 13 nicht mehr nur um Bekanntgabe von Personendaten an Private oder Organisationen handelt, kann der Zusatz „an Private oder Organisationen“ gestrichen werden.

IV. Einschränkungen der Bekanntgabe (§ 14)

§ 14 enthält Bestimmungen zur Einschränkung der Bekanntgabe nach den §§ 10-12. Hier lassen sich die Bestimmungen zur Bekanntgabe von Personendaten in Staaten oder Organisationen, die nicht der Europarats-Konvention 108 beigetreten sind, anfügen. Art. 2 Zusatzprotokoll zur Europarats-Konvention 108 stellt bestimmte Anforderungen an den Personendatentransfer an Empfänger, die nicht der Rechtshoheit eines Staates oder einer Organisation unterstehen, welche der Europarats-Konvention 108 beigetreten sind.[30] 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 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 § 14 Abs. 3 formuliert. Eine Behörde, die **Daten ins Ausland bekannt geben** will, muss sich also zuerst vergewissern, ob der Staat oder die Organisation, dessen bzw. deren Rechtshoheit die empfangende Stelle (Amtsstelle oder Private) unter-

[30] 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.

steht, die Europarats-Konvention 108 ratifiziert hat (§ 14 Abs. 3). Falls nicht, ist zu prüfen, ob die Gesetzgebung des Staates einen angemessenen Schutz gewährleistet (lit. a), wozu auch die Beurteilung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu Rate gezogen werden kann;[31] ist auch das nicht gegeben, so ist der angemessene Schutz durch vertragliche Vereinbarung zu garantieren (lit. 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 (lit. 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 (lit. d).

V. Vorabkontrolle (§ 18a)

Der Art. 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 § 18a hier eingefügt werden. Das Datenschutzkontrollorgan soll seine Feststellungen – entsprechend der neuen Regelung in § 29 Abs. 4 – 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.

VI. Vermittlung durch die Aufsichtsstelle (§ 23)

Im Titel zu § 23 ist noch von der Geschäftsstelle der Datenschutzkommission die Rede, die mit der letzten Revision vom 29. Juni 2005 abgeschafft wurde. Dabei wurde der Titel von § 23 nicht angepasst, was hiermit nachgeholt wird.

VII. Unabhängige Datenschutz-Aufsichtsstelle (§ 26)

Die Bestimmungen über die Datenschutz-Aufsicht werden zur Übersichtlichkeit auf zwei Paragraphen (§§ 26 und 26a) aufgeteilt: § 26 enthält die Bestimmungen, welche die Datenschutz-Aufsichtsstelle generell betreffen; § 26a enthält die Bestimmungen, welche die Datenschutzbeauftragte oder den Datenschutzbeauftragten als Leiterin oder Leiter der Datenschutz-Aufsichtsstelle betreffen.

---

[31] Der EDÖB hat nach dem (revidierten) Art. 31 Abs. 1 lit. d Bundesdatenschutzgesetz zu begutachten, inwieweit die Datenschutzgesetzgebung im Ausland einen angemessenen Schutz gewährleistet.

Mit § 26 Abs. 1 wird die **Grundlage** für die vollständige unabhängige Datenschutz-Aufsichtsstelle des Kantons geschaffen.

§ 26 Abs. 2 und 3 regeln die **Unabhängigkeit**: Es wird in Abs. 2 festgehalten, dass die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben an keine Weisungen gebunden ist (bisher Abs. 3). Ausserdem wird in Absatz 3 festgelegt, dass die Aufsichtsstelle über ein eigenes Budget verfügt.

Über die administrative Zuordnung der Aufsichtsstelle entscheidet der Regierungsrat.

VIII. Beauftragte oder Beauftragter für Datenschutz (§ 26a)

§ 26a Abs. 1 bestimmt die Wahlbehörde für die Datenschutzbeauftragte oder den Datenschutzbeauftragten und legt fest, dass sie oder er auf **Amtsperiode** gewählt wird, die in Übereinstimmung mit der Regelung im Kanton Basel-Landschaft vier Jahre beträgt (vgl. auch die Ausführungen vorne B.IV.3.a.). Wahlbehörde ist der Regierungsrat unter Vorbehalt der Genehmigung durch den Grossen Rat.[32] Dem Regierungsrat ist es wichtig, beide Institutionen, Grosser Rat und Regierungsrat, am Wahlprozess der oder des 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 ausdrückliche Verankerung der Möglichkeit einer Wiederwahl ist nicht erforderlich.

Wie bisher gemäss § 26 Abs. 2 kann das Amt der/des Datenschutzbeauftragten auf zwei Personen mit maximal 100 Stellenprozenten aufgeteilt werden (Abs. 2).

Die/die Datenschutzbeauftragte leitet die Aufsichtsstelle (Abs. 3). Da mit dem bisherigen Personenbestand die Anforderungen gemäss Schengen/Dublin nicht erfüllt werden können, muss dieser erhöht werden (vgl. nachfolgend D.) Zur Unabhängigkeit der Aufsichtsstelle gehört es auch, dass die oder der Datenschutzbeauftragte – im Rahmen des vom Grossen Rat genehmigten Budgets – das weiter benötigte **Personal** der Aufsichtsstelle selbständig anstellt (§ 26a Abs. 4).

IX. Kommunale Aufsichtsstellen (§ 27)

§ 27 sieht bisher vor, dass die Gemeinden für den kommunalen Bereich ein eigenes Datenschutzkontrollorgan schaffen können. Diese Kompetenz kann bestehen bleiben (vgl. Abs. 1), 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 § 27 Abs. 2 nun festgehalten.

---

[32] Die gleiche Lösung wurde in Zürich gewählt: § 30 Abs. 1 des (vom Zürcher Kantonsrat am 12.2.2007 beschlossenen, aber noch nicht vollständig in Kraft getretenen) Gesetzes über die Information und den Datenschutz (IDG).

Der neue Absatz 3 verweist für die Aufgaben und Befugnisse auf die (primär für die kantonale Datenschutz-Aufsichtsstelle geltenden) §§ 28 und 29. Das verantwortliche Organ kann die Weisung mit einem Rekurs nach den allgemeinen Vorschriften beim Gemeinderat anfechten, sofern ihm gegenüber dem Organ Aufsichtsbefugnisse zukommen (vgl. Ausführungen zu § 29).

X. Aufgaben der Aufsichtsstelle (§ 28)

§ 28 enthält den Aufgabenkatalog der Aufsichtsstelle. Dieser Katalog muss, wie vorne erwähnt[33], ergänzt werden.

- Zunächst wird der **Kontrollauftrag genannt**; 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.

- Lit. a-c bleiben unverändert.

- Gemäss bisherigem lit. d hat die Aufsichtsstelle über ihre Tätigkeit, Feststellungen und Erfahrungen der Wahlbehörde zuhanden des Grossen Rates jährlich Bericht zu erstatten. Da der Grosse Rat neu zur Wahlbehörde zählt (vgl. § 26 Abs. 1) ist der Zusatz „zuhanden des Grossen Rates“ obsolet und ist daher zu streichen. Hingegen muss aus Gründen der Transparenz die Pflicht aufgenommen werden, den **Bericht zu veröffentlichen**.

- Lit. e-g bleiben gleich.

- Lit. h macht die **Vorabkontrolle** gemäss § 18a zur Aufgabe.

- Lit. i enthält neu die von Art. 28 Abs. 6 EU-Datenschutzrichtlinie und von Art. 1 Ziff. 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**.

XI. Arbeitsweise der Aufsichtsstelle (§ 29)

§ 29 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 Datenschutzkon-

[33] Vgl. B.IV.3.b.

trollorgans rechtfertigt, und zweitens die Verstärkung der Einwirkungsbefugnisse. Aus diesem Grund werden in § 29 Abs. 2 die gleichen **Untersuchungsbefugnisse** gegenüber Privaten, die Personendaten im Auftrag von Behörden bearbeiten, wie gegenüber den die Daten selber bearbeitenden Behörden vorgesehen. Absatz 3 wird beibehalten und hält wie bisher fest, dass die verantwortlichen Organe verpflichtet sind, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen.

In den Abs. 4-7 wird das oben[34] dargestellte Konzept zur Stärkung der **Einwirkungsbefugnisse** umgesetzt:

- In Abs. 4 wird festgehalten, dass das Datenschutzkontrollorgan zu Datenbearbeitungen **Empfehlungen** abgeben kann und dass das verantwortliche Organ, an welches 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 auch 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 das verantwortliche Organ 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 (Abs. 5). 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 § 17 zu ergreifen. Mit der Formulierung «in Form einer Verfügung» wird erreicht, dass für alle hier nicht separat geregelten Modalitäten an das Organisationsgesetz angeknüpft werden kann.

- Weil im Kanton letztlich das Appellationsgericht als oberste richterliche Behörde über eine Weisung des Datenschutzkontrollorgans zu entscheiden hat, macht es keinen Sinn, dass die oder der Datenschutzbeauftragte gegenüber dem Appellationsgericht Weisungen erlassen kann (Abs. 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 § 4 Abs. 2 Datenschutzgesetz[35] keine Anwendung, womit auch die Zuständigkeit des Datenschutzkontrollorgans entfällt.

- Nach Abs. 6 kann das verantwortliche Organ, an welches die Weisung gerichtet ist, diese mit einem **Rekurs** gemäss den allgemeinen Vorschriften beim Regierungsrat anfechten. Auf den ersten Blick spricht die Unabhängigkeit der Aufsichtsstelle gegen den Regierungsrat als Rekursinstanz. Es soll ihm als Exekutivspitze aber die Gelegenheit gegeben werden, über den Gegenstand der Weisung zuerst zu entscheiden. Mit dem Rekursrecht der Aufsichtsstelle nach § 25 Abs. 6 wird der Weg zu einer gerichtlichen

---

34 Vgl. B.IV.3.c.
35 Siehe vorne C.I.

Instanz aber sichergestellt. Die Weisung stellt eine erstinstanzliche Verfügung im Sinne der §§ 38 f. Organisationsgesetz dar. Mit dem Verweis auf die allgemeinen Vorschriften wird erreicht, dass die Vorschriften des Organisationsgesetzes über Rekursgründe, Form und Frist ohne weiteres anwendbar werden. Da auch weitere Behörden Adressaten einer solchen Weisung sein können, über welche der Regierungsrat keine Aufsichtsbefugnis besitzt, ist in Abs. 6 ausserdem vorgesehen, dass hier der Rekurs direkt ans Appellationsgericht zu richten ist.

- Zur Sicherstellung der Unabhängigkeit des Datenschutzkontrollorgans ist es erforderlich, dass das Datenschutzkontrollorgan gegen Entscheide des Regierungsrates **rekursberechtigt** ist (Abs. 7). 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 diese Rekursinstanzen den Rekurs eines Weisungsadressaten (ganz oder teilweise) gutheissen, kann die Aufsichtsstelle den Entscheid also an die nächsten Rechtsmittelinstanzen weiterziehen; so wird gewährleistet, dass der Rechtsweg zu einer gerichtlichen Instanz offen steht.

Die bisher in § 29 Abs. 6 geregelte Befugnis der Aufsichtsstelle, das verantwortliche Organ aufzufordern, unverzüglich Datenbearbeitungen bis zu einer weiteren Überprüfung durch seine vorgesetzte Stelle einzuschränken oder einzustellen, wenn schutzwürdige Interessen einer betroffenen Person offensichtlich oder schwerwiegend verletzt werden, wird neu zu Absatz 8.

D Finanzielle und personelle Folgen

Die Umsetzung des revidierten Datenschutzgesetzes infolge der Assoziierung an Schengen/Dublin bringt der Datenschutzaufsicht BS, auch als Grenzkanton, gegenüber heute wegen der Erweiterung von Aufgaben und Kompetenzen einen Mehraufwand (zusätzliche Kontrollaufgaben, erweiterte Berichterstattungspflicht, Anzeige- und Klagerechte, Vorabkontrollen, u.a.m.). Wir gehen davon aus, dass der Mehraufwand im Rahmen eines Pensums von mindestens 50% liegen wird. Daraus ergeben sich jährliche Mehrkosten von rund CHF 100'000.— (einschliesslich Sachkosten). Es ist nicht möglich, die Mehrarbeit mit dem aktuellen, an sich schon knappen Personalbestand von einer Vollzeitstelle (d.h. 100%, kein Sekretariat) und damit ohne Personalerhöhung ordentlich, korrekt und angemessen zu bewältigen.

E Antrag

Das Finanzdepartement hat den vorliegenden Ratschlag gemäss § 55 des Gesetzes über den kantonalen Finanzhaushalt (Finanzhaushaltgesetz) vom 16. April 1997 überprüft.

Aufgrund der vorstehenden Ausführungen beantragt der Regierungsrat dem Grossen Rat, der vorgelegten Teilrevision des Gesetzes über den Schutz von Personendaten zuzustimmen.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Eva Herzog
Präsidentin

Dr. Robert Heuss
Staatsschreiber

Beilage: - Gesetzesentwürfe

F Synopse

Geltendes Datenschutzgesetz	Revidiertes Datenschutzgesetz
Vorbehaltenes Recht **§ 4.** Besondere Bestimmungen über den Schutz von Personendaten sind anwendbar, soweit sie strengere Voraussetzungen für das Bearbeiten von Personendaten enthalten oder dieses Gesetz näher ausführen.	*Vorbehaltenes Recht* **§ 4.** bleibt gleich
[2] In hängigen Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege gelten die Bestimmungen über den Personendatenschutz der massgeblichen Verfahrensordnungen.	[2] In hängigen Verfahren der Zivil- und Strafrechtspflege und in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit gelten die Bestimmungen über den Personendatenschutz der massgeblichen Verfahrensordnungen.
[3] Vorbehalten sind auch die vom Bund erlassenen Datenschutzvorschriften.	[3] bleibt gleich
Erhebung **§ 9.** Werden Personendaten systematisch, namentlich mit Fragebogen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung bekannt gegeben werden. In den übrigen Fällen sind diese Angaben der befragten Person auf Wunsch bekannt zu geben, ausser wenn dadurch die Erfüllung der gesetzlichen Aufgaben gefährdet oder verunmöglicht wird.	*Erhebung (Erkennbarkeit der Beschaffung)* **§ 9.** Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe gefährdet wird.
[2] Besonders schützenswerte Personendaten sind wenn immer möglich bei der betroffenen Person selbst zu erheben.	[2] Werden Personendaten systematisch, namentlich mit Fragebogen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein.
Recht auf Sperrung **§ 13.** Die betroffene Person kann die Bekanntgabe ihrer Daten durch die Einwohnerkontrolle an private Personen oder Organisationen sperren lassen. Die Bekanntgabe ist trotz Sperrung zulässig, a) wenn die Einwohnerkontrolle zur Bekanntgabe gesetzlich verpflichtet ist oder b) im Gesuch glaubhaft gemacht wird, dass die Daten zur Durchsetzung von Rechtsansprüchen erforderlich sind.	*Recht auf Sperrung* **§ 13**. Die betroffene Person kann beim verantwortlichen Organ die Bekanntgabe ihrer Daten sperren lassen. Die Bekanntgabe ist trotz Sperrung zulässig, a) wenn das verantwortliche Organ zur Bekanntgabe gesetzlich verpflichtet ist, b) die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder c) im Gesuch glaubhaft gemacht wird, dass die Daten zur Durchsetzung von Rechtsansprüchen erforderlich sind.

Einschränkungen der Bekanntgabe **§ 14.** Die Bekanntgabe von Personendaten kann aus wichtigen öffentlichen oder aus schutzwürdigen Interessen der betroffenen Personen eingeschränkt oder mit Auflagen verbunden werden. [2] Stehen Personendaten unter dem Schutz besonderer Geheimhaltungsvorschriften, so dürfen sie nur Personen oder Organen bekanntgegeben werden, die einer entsprechenden Geheimhaltungspflicht unterstehen oder eine solche übernehmen. Eine gesetzlich vorgesehene Einwilligung der betroffenen Personen bleibt vorbehalten.	*Einschränkungen der Bekanntgabe* **§ 14.** bleibt gleich [2] bleibt gleich [3] Organe dürfen Personendaten anderen Organe oder Privaten, die nicht der Rechtshoheit eines Staates oder einer Organisation unterstehen, welche dem Europaratsübereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten beigetreten sind, nur bekannt geben, wenn: a) die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet; b) durch vertragliche Vereinbarungen ein angemessener Schutz garantiert wird; c) dies im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist, oder d) es 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.
	Vorabkontrolle **§ 18a.** Wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab der Aufsichtsstelle zur Kontrolle vorgelegt werden. [2] Die Aufsichtsstelle gibt ihre Beurteilung in Form einer Empfehlung gemäss § 29 Abs. 4 ab.

Vermittlung durch die Geschäftsstelle der Datenschutzkommission **§ 23.** Die Aufsichtsstelle kann jederzeit um Beratung oder um Vermittlung zwischen betroffener Person und verantwortlichem Organ ersucht werden.	*Vermittlung durch die Aufsichtsstelle* **§ 23.** bleibt gleich
Kanton **§ 26.** Der Regierungsrat wählt als kantonale Aufsichtsstelle eine Beauftragte oder einen Beauftragten für den Datenschutz. [2] Das Amt der/des Beauftragten für den Datenschutz kann auf zwei Personen mit maximal 100 Stellenprozenten aufgeteilt werden. [3] Die Aufsichtsstelle erfüllt die Aufgaben fachlich unabhängig und selbständig.	*Unabhängige Datenschutz-Aufsichtsstelle* **§ 26.** Der Kanton führt eine unabhängige Datenschutz-Aufsichtsstelle (Aufsichtsstelle). [2] Die Aufsichtsstelle erfüllt ihre Aufgaben weisungsunabhängig. [3] Die Aufsichtsstelle hat ihr eigenes Budget.
	Beauftragte oder Beauftragter für Datenschutz **§ 26a**. Der Regierungsrat wählt, unter Vorbehalt der Genehmigung durch den Grossen Rat, eine Beauftragte oder einen Beauftragten für Datenschutz auf eine feste Amtsdauer von vier Jahren. [2] Das Amt der oder des Beauftragten für den Datenschutz kann auf zwei Personen mit maximal 100 Stellenprozenten aufgeteilt werden. [3] Die oder der Beauftragte leitet die Aufsichtsstelle. [4] Sie oder er ist im Rahmen des vom Grossen Rat genehmigten Budgets für die Anstellung der weiteren Mitarbeitenden der Aufsichtsstelle zuständig.
Gemeinden **§ 27.** Sehen die Gemeinden davon ab, eine eigene Aufsicht einzusetzen, so ist die kantonale Aufsicht zuständig.	*Kommunale Aufsichtsstellen* **§ 27**. Die Gemeinden können für den kommunalen Bereich eine eigene Aufsichtsstelle schaffen. [2] Sehen sie davon ab oder erfüllt die kommunale Aufsichtsstelle die Anforderungen an die Unabhängigkeit nicht, so ist die kantona-

	le Aufsichtsstelle zuständig. [3] Die §§ 28 und 29 gelten für die kommunale Aufsichtsstelle in ihrem Zuständigkeitsbereich.
Aufgaben der Aufsicht **§ 28.** Die Aufsichtsstelle überwacht die Anwendung der Vorschriften über den Datenschutz fachlich selbständig und unabhängig. Sie erfüllt insbesondere folgende Aufgaben: a) Sie berät die verantwortlichen Organe in Fragen des Datenschutzes und der Datensicherung, namentlich bei Vorhaben für elektronisches Bearbeiten von Personendaten. b) Sie prüft das Gesuch um generelle Einsicht in bestimmte Datensammlungen anderer Organe und erteilt die Autorisierungen. c) Sie nimmt Stellung zu Erlassen, die für den Datenschutz erheblich sind. d) Sie erstattet der Wahlbehörde zuhanden des Grossen Rates jährlich Bericht über ihre Tätigkeit, Feststellungen und Erfahrungen. e) Sie berät die betroffenen Personen über ihre Rechte. f) Sie vermittelt zwischen betroffenen Personen und verantwortlichen Organen. g) Sie führt das zentrale Register der Datensammlungen gemäss § 8.	*Aufgaben der Aufsichtsstelle* **§ 28**. Die Aufsichtsstelle kontrolliert nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Datenschutz. Sie erfüllt insbesondere folgende Aufgaben: a) bis c) bleiben gleich d) Sie erstattet der Wahlbehörde jährlich Bericht über ihre Tätigkeit, Feststellungen und Erfahrungen; der Bericht wird veröffentlicht. e) bis g) bleiben gleich h) Sie kontrolliert Datenbearbeitungen gemäss § 18a. i) Sie arbeitet zur Erfüllung ihrer Aufgaben mit den Datenschutz-Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen.

Arbeitsweise der Aufsicht **§ 29.** Die Aufsichtsstelle kann von sich aus oder aufgrund von Meldungen Dritter tätig werden.	*Arbeitsweise der Aufsichtsstelle* **§ 29**. bleibt gleich
[2] Sie kann bei öffentlichen Organen direkt schriftlich oder mündlich Auskünfte über Datenbearbeitungen einholen, Einsicht in Unterlagen und Akten bestimmter Bearbeitungen nehmen, Besichtigungen durchführen, sich Bearbeitungen vorführen lassen und in Gremien zu datenschutzrelevanten Themen beratend Einsitz nehmen.	[2] Die Aufsichtsstelle kann bei öffentlichen Organen und bei Drittpersonen, die von einem verantwortlichen Organ mit dem Bearbeiten von Personendaten beauftragt sind oder von ihr Personendaten erhalten haben, ungeachtet allfälliger Geheimhaltungspflichten, schriftlich oder mündlich Auskunft über Datenbearbeitungen einholen, Einsicht in alle Unterlagen nehmen, Besichtigungen durchführen und sich Bearbeitungen vorführen lassen.
[3] Die verantwortlichen Organe sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben zu unterstützen.	[3] bleibt gleich
[4] Soweit es zum Schutz der betroffenen Personen notwendig ist, kann die Aufsichtsstelle auch bei Dritten, die vom verantwortlichen Organ mit dem Bearbeiten von Personendaten beauftragt oder von ihm Personendaten erhalten haben, schriftlich oder mündlich Auskünfte einholen sowie Einsicht in Unterlagen und Akten bestimmter Bearbeitungen nehmen.	[4] Die Aufsichtsstelle kann zu Datenbearbeitungen Empfehlungen abgeben. Das verantwortliche Organ, an welches die Empfehlung gerichtet ist, hat gegenüber der Aufsichtsstelle zu erklären, ob es der Empfehlung folgen will.
[5] Werden schutzwürdige Interessen einer betroffenen Person gefährdet oder verletzt, so beantragt die Aufsichtsstelle dem verantwortlichen Organ oder dessen vorgesetzter Behörde, das Bearbeiten der Personendaten unverzüglich einzuschränken oder einzustellen.	[5] Wenn ein verantwortliches Organ erklärt, der Empfehlung der Aufsichtsstelle nicht folgen zu wollen, oder tatsächlich der Empfehlung nicht folgt, kann die Aufsichtsstelle, soweit das Interesse an der Durchsetzung schwer wiegt, ihre Empfehlung oder Teile davon als Weisung im Form einer Verfügung erlassen. Keine Weisung kann gegenüber dem Appellationsgericht erlassen werden. [6] Das verantwortliche Organ, an welches die Weisung gerichtet ist, kann sie mit einem Rekurs nach den allgemeinen Vorschriften beim Regierungsrat anfechten, sofern ihm gegenüber dem Organ Aufsichtsbefugnisse zukommen. In den übrigen Fällen ist der Rekurs direkt an das Appellationsgericht zu richten.

	[7] Die Aufsichtsstelle ist rekursberechtigt gegen Entscheide des Regierungsrates.
[6] Ist die Verletzung offensichtlich oder schwerwiegend, so kann die Aufsichtsstelle anordnen, dass das verantwortliche Organ die Bearbeitung bis zur erfolgten Überprüfung durch seine vorgesetzte Stelle einschränkt oder einstellt.	[8] Werden schutzwürdige Interessen offensichtlich oder schwerwiegend verletzt, so kann die Aufsichtsstelle anordnen, dass das verantwortliche Organ die Bearbeitung bis zur erfolgten Überprüfung durch seine vorgesetzte Stelle einschränkt oder einstellt.

Gesetz über den Schutz von Personendaten (Datenschutzgesetz)

Änderung vom

Der Grosse Rat des Kantons Basel-Stadt, nach Einsichtnahme in den Ratschlag des Regierungsrates Nr. 05.1024.01 vom 26. September 2007 sowie in den Bericht der Justiz-, Sicherheits- und Sportkommission Nr. ..... vom ..... , beschliesst:

I.

Das Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 18. März 1992 wird wie folgt geändert:

§ 4 Abs. 2 erhält folgende neue Fassung:

[2] In hängigen Verfahren der Zivil- und Strafrechtspflege und in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit gelten die Bestimmungen über den Personendatenschutz der massgeblichen Verfahrensordnungen.

§ 9 samt Titel erhält folgende neue Fassung:

Erhebung (Erkennbarkeit der Beschaffung)
§ 9. Die betroffene Person muss erkennen können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden, soweit dadurch nicht die Erfüllung der gesetzlichen Aufgabe gefährdet wird.
[2] Werden Personendaten systematisch, namentlich mit Fragebogen, erhoben, so müssen Rechtsgrundlage und Zweck der Bearbeitung angegeben sein.

§ 13 Einleitungssatz und lit. a erhalten folgende neue Fassung:

§ 13. Die betroffene Person kann beim verantwortlichen Organ die Bekanntgabe ihrer Daten sperren lassen. Die Bekanntgabe ist trotz Sperrung zulässig,
a) wenn das verantwortliche Organ zur Bekanntgabe gesetzlich verpflichtet ist,

Es wird folgende neue lit. b eingefügt:

b) die Bekanntgabe zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder

Dadurch wird die bisherige lit.b zu lit.c.

In § 14 wird folgender neuer Abs. 3 beigefügt:

[3] Organe dürfen Personendaten anderen Organen oder Privaten, die nicht der Rechtshoheit eines Staates oder einer Organisation unterstehen, welche dem Europaratsübereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten beigetreten sind, nur bekannt geben, wenn:
a) die Gesetzgebung des Empfängerstaates einen angemessenen Schutz gewährleistet;
b) durch vertragliche Vereinbarungen ein angemessener Schutz garantiert wird;
c) dies im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist, oder

d) es 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.

Neu wird nach § 18 ein § 18a samt Titel eingefügt:

Vorabkontrolle
§ 18a. Wenn eine Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss diese Bearbeitung vorab der Aufsichtsstelle zur Kontrolle vorgelegt werden.
[2] Die Aufsichtsstelle gibt ihre Beurteilung in Form einer Empfehlung gemäss § 29 Abs. 4 ab.

Der Titel vor § 23 erhält folgende neue Fassung:

Vermittlung durch die Aufsichtsstelle

§ 26 samt Titel erhält folgende neue Fassung:

Unabhängige Datenschutz-Aufsichtsstelle
§ 26. Der Kanton führt eine unabhängige Datenschutz-Aufsichtsstelle (Aufsichtsstelle).
[2] Die Aufsichtsstelle erfüllt ihre Aufgaben weisungsunabhängig.
[3] Die Aufsichtsstelle hat ihr eigenes Budget.

Nach § 26 wird § 26a samt Titel eingefügt:

Beauftragte oder Beauftragter für Datenschutz
§ 26a. Der Regierungsrat wählt, unter Vorbehalt der Genehmigung durch den Grossen Rat, eine Beauftragte oder einen Beauftragten für Datenschutz auf eine feste Amtsdauer von vier Jahren.
[2] Das Amt der oder des Beauftragten für den Datenschutz kann auf zwei Personen mit maximal 100 Stellenprozenten aufgeteilt werden.
[3] Die oder der Beauftragte leitet die Aufsichtsstelle.
[4] Sie oder er ist im Rahmen des vom Grossen Rat genehmigten Budgets für die Anstellung der weiteren Mitarbeitenden der Aufsichtsstelle zuständig.

§ 27 samt Titel erhält folgende neue Fassung:

Kommunale Aufsichtsstellen
§ 27. Die Gemeinden können für den kommunalen Bereich eine eigene Aufsichtsstelle schaffen.
[2] Sehen sie davon ab oder erfüllt die kommunale Aufsichtsstelle die Anforderungen an die Unabhängigkeit nicht, so ist die kantonale Aufsichtsstelle zuständig.
[3] Die §§ 28 und 29 gelten für die kommunale Aufsichtsstelle in ihrem Zuständigkeitsbereich.

§ 28 Titel, Einleitungssatz und lit. d erhalten folgende neue Fassung:

Aufgaben der Aufsichtsstelle
§ 28. Die Aufsichtsstelle kontrolliert nach einem durch sie autonom aufzustellenden Prüfprogramm die Anwendung der Bestimmungen über den Datenschutz. Sie erfüllt insbesondere folgende Aufgaben:

d) Sie erstattet der Wahlbehörde jährlich Bericht über ihre Tätigkeit, Feststellungen und Erfahrungen; der Bericht wird veröffentlicht.

In § 28 werden nach lit. g folgende neuen lit. h und i beigefügt:

h) Sie kontrolliert Datenbearbeitungen gemäss § 18a.
i) Sie arbeitet zur Erfüllung ihrer Aufgaben mit den Datenschutz-Kontrollorganen der anderen Kantone, des Bundes und des Auslandes zusammen.

§ 29 Abs. 2, 4-6 erhalten folgende neue Fassung:

[2] Die Aufsichtsstelle kann bei öffentlichen Organen und bei Drittpersonen, die von einem verantwortlichen Organ mit dem Bearbeiten von Personendaten beauftragt sind oder von ihr Personendaten erhalten haben, ungeachtet allfälliger Geheimhaltungspflichten, schriftlich oder mündlich Auskunft über Datenbearbeitungen einholen, Einsicht in alle Unterlagen nehmen, Besichtigungen durchführen und sich Bearbeitungen vorführen lassen.

[4] Die Aufsichtsstelle kann zu Datenbearbeitungen Empfehlungen abgeben. Das verantwortliche Organ, an welches die Empfehlung gerichtet ist, hat gegenüber der Aufsichtsstelle zu erklären, ob es der Empfehlung folgen will.
[5] Wenn ein verantwortliches Organ erklärt, der Empfehlung der Aufsichtsstelle nicht folgen zu wollen, oder tatsächlich der Empfehlung nicht folgt, kann die Aufsichtsstelle, soweit das Interesse an der Durchsetzung schwer wiegt, ihre Empfehlung oder Teile davon als Weisung im Form einer Verfügung erlassen. Keine Weisung kann gegenüber dem Appellationsgericht erlassen werden.
[6] Das verantwortliche Organ, an welches die Weisung gerichtet ist, kann sie mit einem Rekurs gemäss den allgemeinen Vorschriften beim Regierungsrat anfechten, sofern ihm gegenüber dem Organ Aufsichtsbefugnisse zukommen. In den übrigen Fällen ist der Rekurs direkt an das Appellationsgericht zu richten.

In § 29 werden folgende neuen Abs. 7 und 8 beigefügt:

[7] Die Aufsichtsstelle ist rekursberechtigt gegen Entscheide des Regierungsrates.
[8] Werden schutzwürdige Interessen offensichtlich oder schwerwiegend verletzt, so kann die Aufsichtsstelle anordnen, dass das verantwortliche Organ die Bearbeitung bis zur erfolgten Überprüfung durch seine vorgesetzte Stelle einschränkt oder einstellt.

II.

Diese Änderung ist zu publizieren; sie unterliegt dem Referendum und wird nach Eintritt der Rechtskraft sofort wirksam.