



**Gemeinsamer Antrag des Regierungsrates
und der Kommission**

**Datenschutzgesetz (KDSG)
(Änderung)**

Vortrag des Regierungsrates an den Grossen Rat betreffend Änderung des Datenschutzgesetzes

1. Ausgangslage

1.1 Geltendes Datenschutzrecht

Der Datenschutz betrifft einen zentralen Bereich der menschlichen Persönlichkeit. Er ist Teil des mit Art. 13 der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV)¹⁾ gewährleisteten Schutzes der Privatsphäre²⁾. Art. 13 Abs. 2 BV schützt in diesem Zusammenhang ausdrücklich vor dem Missbrauch persönlicher Daten. Die Verfassung des Kantons Bern vom 6. Juni 1993 (Kantonsverfassung; KV)³⁾ enthält in Art. 18 eine umfassende verfassungsrechtliche Gewährleistung des Datenschutzes.

Im Bereich des Datenschutzes kommen sowohl dem Bund als auch den Kantonen Gesetzgebungszuständigkeiten zu. Der Bund regelt mit dem Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)⁴⁾ die Datenbearbeitung durch Private und durch Organe des Bundes. Die Kantone sind zuständig für die Regelung der Datenbearbeitung durch kantonale und kommunale Organe. Mit dem kantonalen Datenschutzgesetz vom 19. Februar 1986 (KDSG)⁵⁾ verfügt der Kanton Bern über ein Datenschutzrecht, das nach wie vor als zeitgemäss bezeichnet werden darf und das sich in der Praxis insgesamt auch bewährt hat.

1.2 Recht der Europäischen Union

Am 26. Oktober 2004 genehmigten die Eidgenössischen Räte die bilateralen sektoriellen Abkommen mit der Europäischen Union (EU) über landwirtschaftliche Verarbeitungserzeugnisse, Statistik, Umwelt, Media, Pensionen, Schengen/Dublin, Betrugsbekämpfung und Zinsbesteuerung (so genannte «Bilaterale II»)⁶⁾. Dem Abkommen über die Assoziierung mit Schengen/Dublin hat die schweizerische Stimmbevölkerung in der Referendumsabstimmung vom 5. Juni 2005 zugestimmt. Gegenstand dieses Abkommens ist eine enge Zusammenarbeit der Schweiz mit der EU in den Bereichen Polizei, Justiz und Asylwesen. Kernpunkt der polizeilichen

¹⁾ SR 101

²⁾ Im Unterschied zum europäischen Recht schützt das schweizerische Datenschutzrecht nicht nur natürliche, sondern auch juristische Personen.

³⁾ BSG 101.1

⁴⁾ SR 235.1

⁵⁾ BSG 152.04

⁶⁾ Vgl. dazu die Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II») vom 1. Oktober 2004, BBI 2004 S. 5965 ff.

Zusammenarbeit ist das Schengener Informationssystem (SIS), eine europaweite Plattform zum Austausch polizeilicher Fahndungsinformationen. Im Bewusstsein, dass derartige Systeme gleichzeitig schwer wiegende Eingriffe in Persönlichkeitsrechte der betroffenen Personen bedeuten, hat die EU strenge Datenschutzregeln erlassen, die aufgrund der Assoziierung mit Schengen/Dublin auch durch die Schweiz zu beachten sind.

Welche Regelungen im Einzelnen anwendbar sind, richtet sich danach, zu welchem «Pfeiler» das betreffende Aufgabengebiet gehört. Die zu Schengen gehörenden Rechtsakte und Massnahmen, der so genannte Schengen-Besitzstand, wurden mit dem Vertrag von Amsterdam in den rechtlichen Rahmen der EU integriert, der seit dem Vertrag von Maastricht aus den drei «Pfeilern» EG (Vertrag zur Gründung der Europäischen Gemeinschaft), gemeinsame Aussen- und Sicherheitspolitik sowie polizeiliche und justizielle Zusammenarbeit in Strafsachen besteht. In diesem Schengen-Besitzstand sind die Vorgaben in Bezug auf den Datenschutz, welche die Eidgenossenschaft mit der Assoziierung an Schengen/Dublin übernehmen muss, im Einzelnen bezeichnet. Von Bedeutung sind namentlich die 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 Datenverkehr⁷⁾ (EU-Datenschutzrichtlinie) sowie das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten⁸⁾ (Übereinkommen) und das Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung⁹⁾ (Zusatzprotokoll), welches die Eidgenössischen Räte am 24. März 2006 zusammen mit der Revision des DSG angenommen haben¹⁰⁾.

1.3 Umsetzung der europäischen Vorgaben

Das bilaterale Abkommen über die Assoziierung mit Schengen/Dublin betrifft sowohl Bereiche, die in der Zuständigkeit des Bundes liegen, als auch solche, für welche die Kantone zuständig sind oder in denen zumindest der Vollzug den Kantonen obliegt. Damit ist die Umsetzung der Abkommen nicht nur Sache des Bundes, sondern auch der Kantone. Der Bund hat den europäischen Vorgaben mit der Revision des DSG vom 24. März 2006 Rechnung getragen.

Im Hinblick auf die Umsetzung der datenschutzrechtlichen Vorgaben des EU-Rechts ist im Auftrag der Konferenz der Kantonsregierungen (KdK) die Wegleitung «Umsetzung Schengen/Dublin in den Kantonen: Datenschutz» vom 15. März 2006 (im Folgenden KdK-Wegleitung) erarbeitet worden. Die KdK-Wegleitung besteht aus einer Checkliste und dazugehörigen Erläuterungen. Sie soll es den Kantonen ermöglichen

⁷⁾ Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031–0050

⁸⁾ SR 0.235.1

⁹⁾ BBI 2003 S. 2167 ff.

¹⁰⁾ BBI 2006 S. 3547

zu prüfen, inwiefern ihre Datenschutzgesetzgebung den europäischen Anforderungen entspricht und wo noch Handlungs- oder Regelungsbedarf besteht.

Die KdK-Wegleitung bildete auch die Grundlage für die Vorarbeiten zur Revision des kantonalen Datenschutzgesetzes. Gestützt auf erste Vorabklärungen beauftragte der Regierungsrat am 28. Juni 2006 die Justiz-, Gemeinde- und Kirchendirektion (JGK), den Anpassungsbedarf im Kanton Bern zu prüfen und entsprechende Vorschläge zu erarbeiten. Die durch die JGK eingesetzte Projektorganisation lieferte am 28. November 2006 einen Zwischenbericht an den Regierungsrat ab. Die hiermit unterbreitete Vorlage ist gestützt auf die KdK-Wegleitung, die Ergebnisse des Zwischenberichts der Projektorganisation und die Entscheidungen des Regierungsrats über einzelne Anträge und Empfehlungen der Projektorganisation erarbeitet worden.

Die EU wird in den Jahren 2007 und 2008 im Rahmen einer zweistufigen Evaluation überprüfen, ob die schweizerische Gesetzgebung – auf eidgenössischer wie auf kantonaler Stufe – dem Schengen-Standard entspricht. Danach wird vor Ort die praktische Umsetzung geprüft werden.

1.4 Ziele und Leitlinien der Revision

Für die Revision des Datenschutzgesetzes sind die folgenden Ziele und Leitlinien formuliert worden:

- Vorrangiges Ziel ist eine mit dem EU-Recht kompatible Datenschutzgesetzgebung des Kantons Bern. Das kantonale Recht soll in dem Sinn «umsetzungssicher» sein, als die vorgesehenen Kontrollen der EU über die Umsetzung in den Jahren 2007 und 2008 zu keinem Hindernis für das Inkrafttreten der Abkommen von Schengen und Dublin führen.
- Gleichzeitig sollen die Vorgaben des EU-Rechts pragmatisch umgesetzt werden. Die Revision soll sich auf Anpassungen beschränken, die aufgrund dieser Vorgaben oder aus andern Gründen zwingend erscheinen. Wo Anpassungsbedarf besteht, sollen die Neuerungen nach Möglichkeit in das Gefüge bewährter bisheriger Regelungen eingepasst werden und, soweit sich aus konkreten Gegebenheiten im Kanton Bern nichts anderes ergibt, auch mit den Regelungen übereinstimmen, die der Bund im Rahmen der Umsetzung des EU-Rechts gewählt hat.

2. Grundzüge der Vorlage

2.1 Übersicht über den Anpassungsbedarf

Die Überprüfung des geltenden Rechts im Licht der europäischen Vorgaben und der KdK-Wegleitung hat ergeben, dass Anpassungsbedarf vor allem im Hinblick auf die rechtliche Stellung der Datenschutzaufsicht und die Zuständigkeiten der Aufsichtsstelle besteht. Verlangt wird vorab, dass das Gesetz die «völlige Unabhängigkeit» der Aufsichtsstelle vorschreibt und durch entsprechende organisatorische Bestimmungen (Wahl/Ernennung und Rechtsstellung der für die Aufsicht verantwortlichen

Personen, Verfügung über Ressourcen, Stellung der Aufsichtsstelle im staatlichen Aufbau) sichert. Im Zusammenhang mit den Zuständigkeiten der Aufsichtsstelle werden deren Aufgaben und Befugnisse sowie die Instrumente, die zur wirkungsvollen Wahrnehmung dieser Zuständigkeiten erforderlich sind, teilweise neu zu regeln sein.

Im Übrigen besteht aufgrund der europäischen Vorgaben nur punktueller Regelungs- bzw. Anpassungsbedarf, so in Bezug auf die Geltung der datenschutzrechtlichen Bestimmungen in hängigen Verwaltungsverfahren, die Kosten für die Einsicht in Daten und Auskünfte und den grenzüberschreitenden Datenverkehr. Über die durch Schengen/Dublin bedingten Anpassungen hinaus werden, aus Gründen der Zweckmässigkeit, eine teilweise Neuregelung der Datenschutzregister und der Berichterstattung durch die Aufsichtsstelle, die Streichung einer Bestimmung ohne praktische Bedeutung (Art. 27 KDSG, Beschwerden gegen die Aufsichtsstelle) sowie eine Präzisierung zum Verfahren und Rechtsschutz vorgeschlagen.

2.2 Punktuelle Anpassungen des Datenschutzgesetzes

2.2.1 Geltungsbereich des Gesetzes

Nach der heute geltenden Regelung findet das Datenschutzgesetz keine Anwendung auf hängige Verfahren der Zivil-, Verwaltungs- oder Strafrechtspflege sowie auf Ermittlungen einer parlamentarischen Untersuchungskommission (Art. 4 Abs. 2 Bst. c KDSG). Vom Geltungsbereich des Gesetzes ausgenommen ist insbesondere auch das so genannte Verwaltungsverfahren, d.h. das Verfahren auf Erlass einer Verfügung¹¹⁾. Mit Art. 4 Abs. 2 Bst. c KDSG sollte dem Umstand Rechnung getragen werden, dass für die genannten Verfahren besondere Prozess- und Verfahrensgesetze, nämlich das Gesetz vom 7. Juli 1918 über die Zivilprozessordnung (ZPO)¹²⁾, das Gesetz vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG)¹³⁾ und das Gesetz vom 15. März 1995 über das Strafverfahren (StrV)¹⁴⁾, bestehen, die den Umgang mit Daten selbständig regeln. Es sollte vermieden werden, dass nebeneinander zwei Regelungen bestehen, welche im Wesentlichen denselben Schutzzweck verfolgen.

Gemäss der KdK-Wegleitung darf jedenfalls das Verwaltungsverfahren nicht vom Geltungsbereich der kantonalen Datenschutzgesetze ausgenommen werden. Eine entsprechende Anpassung des Geltungsbereichs ist auch in der Sache angezeigt. So kann die Aufsichtsstelle für Datenschutz nur in diesem Fall auch in einem Verfahren auf Erlass einer Verfügung, beispielsweise im Rahmen einer Steuerveranlagung, von ihren Befugnissen (dazu hinten Ziff. 2.4) Gebrauch machen. Zudem findet im Rahmen des Vollzugs von Bundesrecht das eidgenössische Datenschutzgesetz auch dann auf erstinstanzliche Verwaltungsverfahren Anwendung, wenn eine kantonale Behörde zum Vollzug zuständig ist (Art. 2 Abs. 2 Bst. c in Verbindung mit Art. 37

¹¹⁾ VGE Nr. 18226 vom 26. August 1991, wiedergegeben in BVR 1992 S. 80 ff.

¹²⁾ BSG 271.1

¹³⁾ BSG 155.21

¹⁴⁾ BSG 321.1

Abs. 1 DSG). Mit einer entsprechenden Anpassung des KDSG wird vermieden, dass die Geltung des Datenschutzes davon abhängt, ob (auch) der Vollzug von Bundesrecht betroffen ist oder nicht. Diese beiden Fälle werden namentlich im Rahmen der neu eingeführten Vorabkontrolle (vgl. hinten Ziff. 2.4.2 und 3.1, Bemerkungen zu Art. 17a) nicht sauber getrennt werden können, womit sich bei einer Beibehaltung des heutigen Geltungsbereichs des KDSG praktisch kaum lösbar Probleme ergäben.

Die KDK-Wegleitung erachtet es auch als heikel, wenn das verwaltungsinterne Beschwerdeverfahren vom Geltungsbereich des Datenschutzgesetzes ausgenommen wird. Zur Begründung verweist sie indes einzig auf die bundesrechtliche Regelung in Art. 2 Abs. 2 Bst. c DSG, wonach das Datenschutzrecht des Bundes nur auf Verwaltungsverfahren, nicht aber auf Verwaltungsjustizverfahren Anwendung findet. Im Rahmen einer pragmatischen Anpassung des Datenschutzrechts in Anlehnung an das Bundesrecht erscheint es deshalb angezeigt, Art. 4 Abs. 2 KDSG im Sinn des DSG, aber nicht weiter gehend, anzupassen und neu die Verwaltungsverfahren dem Geltungsbereich des KDSG zu unterstellen. Es kann davon ausgegangen werden, dass der Datenschutz und die Rechte der Betroffenen in förmlichen Beschwerdeverfahren durch die anwendbaren Bestimmungen des VRPG hinreichend gewährleistet sind.

Die Ausdehnung des Geltungsbereichs führt nicht dazu, dass das KDSG die Bestimmungen des VRPG in jedem Fall und ohne Weiteres verdrängt. Im konkreten Fall wird anhand anerkannter Kriterien für die Auslegung von Erlassen (z.B. Vorrang der *lex specialis*) zu prüfen sein, welche Vorschrift im Fall konkurrierender Bestimmungen vorgeht. Soweit ersichtlich hat die gleichzeitige Anwendbarkeit datenschutzrechtlicher und verfahrensrechtlicher Bestimmungen beim Bund denn bisher auch nicht zu nennenswerten Problemen bei der Rechtsanwendung geführt.

2.2.2 Kosten für Auskünfte und Einsichtnahme in Datensammlungen

Das Recht auf Auskunft über Personendaten und auf Einsicht in Datensammlungen ist ein wesentlicher Bestandteil des verfassungsrechtlichen Persönlichkeitsschutzes (Art. 18 Abs. 1 KV). Art. 12 Bst. a EU-Datenschutzrichtlinie schreibt deshalb vor, dass dieses Recht nicht durch eine übermässige Kostenbeteiligung der betroffenen Personen erschwert oder gar vereitelt werden darf. Im Gesetz ist deshalb ausdrücklich festzuschreiben, dass die Einsichtnahme oder Auskunft grundsätzlich kostenlos ist und nur in Ausnahmefällen eine Gebühr erhoben werden darf.

2.2.3 Grenzüberschreitender Datenverkehr

Nach Art. 2 Ziff. 1 Zusatzprotokoll ist die grenzüberschreitende Übermittlung von Personendaten nur zulässig, wenn der Empfängerstaat «einen angemessenen Schutz für die beabsichtigte Datenübermittlung gewährleistet» (vgl. auch Art. 12 Übereinkommen und Art. 25 f. EU-Datenschutzrichtlinie). Nach Art. 2 Ziff. 2 Zusatzprotokoll müssen Ausnahmen von diesem Grundsatz gesetzlich geregelt werden.

Aus dieser Bestimmung ergibt sich ausserdem eine Pflicht zur Information der Datenschutzaufsichtsstelle.

Der Datenverkehr mit dem Ausland war im Kanton Bern bisher von geringer praktischer Bedeutung und ist dementsprechend im geltenden Recht auch nicht geregelt. Die allgemeine «Ordre-public-Klausel» in Art. 14 Abs. 1 KDSG genügt im Licht der erwähnten europäischen Vorgaben als Regelung des grenzüberschreitenden Datenverkehrs nicht, weil es ihr an der erforderlichen Bestimmtheit fehlt. Damit wird neu eine Regelung im Sinn von Art. 2 Zusatzprotokoll in das Gesetz aufzunehmen sein. Der Bund hat dem Zusatzprotokoll mit der Revision des DSG Rechnung getragen. Es empfiehlt sich, das KDSG in Anlehnung an das revidierte DSG anzupassen.

2.2.4 Register der Datensammlungen

Die Registrierung der Datensammlungen dient den betroffenen Personen als Hilfsmittel zur Geltendmachung ihrer Rechte, namentlich des Rechts auf Auskunft und Einsicht (Art. 21 KDSG), auf Berichtigung oder Vernichtung unrichtiger oder unnötiger Daten (Art. 23 KDSG) und auf Sperrung (Art. 13 KDSG). Das Datenschutzgesetz und Art. 21 Abs. 2 EU-Datenschutzrichtlinie schreiben deshalb vor, dass sämtliche Datensammlungen in ein Register aufzunehmen sind. Das Register ist nach der EU-Datenschutzrichtlinie durch die Kontrollstelle zu führen. Auch im Kanton Bern wird das Register heute durch die Aufsichtsstelle geführt (Art. 34 Bst. a KDSG). Die verantwortliche Behörde meldet die bei ihr angelegten Datensammlungen zur Registrierung (Art. 18 KDSG).

In der Praxis bieten das Erstellen und vor allem das Nachführen eines zentralen Registers von Datensammlungen erhebliche Schwierigkeiten, weil nur die für die Datenbearbeitung verantwortliche Stelle, nicht aber die Aufsichtsstelle weiss, welche Datensammlungen bestehen, neu erstellt oder vernichtet werden. Es erscheint deshalb angezeigt, die Registrierung teilweise neu zu regeln. Weil Art. 21 Abs. 2 EU-Datenschutzrichtlinie ausdrücklich die Kontrollstelle zur Führung des Registers verpflichtet, dürfte eine vollständige Dezentralisierung in dem Sinn, dass ausschliesslich die Daten bearbeitenden Stellen die bei ihnen bestehenden Datensammlungen registrieren, unzulässig sein. Zweckmässig und mit der EU-Datenschutzrichtlinie vereinbar erscheint eine Lösung, wonach die Aufsichtsstelle ein zentrales Register führt, das – nach den Vorgaben der Aufsichtsstelle – durch die verantwortlichen Behörden «bewirtschaftet», d.h. erstellt und im Bedarfsfall nachgeführt wird. Auch mit dieser Lösung kann erreicht werden, dass sich Interessierte an einem Ort über den Bestand sämtlicher im Kanton oder in einer gemeinderechtlichen Körperschaft angelegten Datensammlungen informieren können. Die Aufsichtsstelle wird mit geeigneten Vorgaben sicherzustellen haben, dass die Datensammlungen auch tatsächlich registriert werden.

2.2.5 Verfahren und Rechtsschutz

Bereits nach geltendem Recht stehen gegen datenschutzrechtliche Anordnungen zwar in der Regel, aber nicht ausschliesslich die Rechtsmittel oder Rechtsbehelfe an Verwaltungsjustizbehörden, sondern in bestimmten Fällen auch solche an Zivil- und Strafjustizbehörden offen (vgl. dazu hinten Ziff. 3.1, Bemerkungen zu Art. 26 KDSG). Dies kommt indes im Datenschutzgesetz nicht zum Ausdruck. Art. 26 KDSG verweist für das Verfahren und den Rechtsschutz vielmehr einzig auf die Bestimmungen des Verwaltungsrechtspflege- und des Gemeindegesetzes, was in der Praxis Fragen zum Rechtsweg aufgeworfen hat. Diese Unsicherheiten sollen mit einer präziseren Fassung von Art. 26 KDSG beseitigt werden.

2.3. Stellung der Datenschutzaufsicht

2.3.1 Grundsatz der Unabhängigkeit

Nach Art. 28 Abs. 1 der EU-Datenschutzrichtlinie müssen die mit der Überwachung der datenschutzrechtlichen Vorschriften beauftragten Stellen «die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit» wahrnehmen. Auch das Zusatzprotokoll verlangt, dass die Datenschutzaufsichtsstellen «ihre Aufgaben in vollständiger Unabhängigkeit wahrnehmen» (Präambel) und «bei der Wahrnehmung ihrer Aufgaben völlig unabhängig» sind (Art. 1 Ziff. 3). Das Gesetz muss diesen Grundsatz ausdrücklich festhalten.

Die Unabhängigkeit der Datenschutzaufsicht setzt geeignete organisatorische «Sicherungen» voraus. Mit einer adäquaten Regelung der Bestellung und der Rechtsstellung der verantwortlichen Personen sowie der administrativen Zuordnung der Aufsichtsstelle ist sicherzustellen, dass die mit der Aufsicht betrauten Personen von der kontrollierten Verwaltung so unabhängig sind, dass sie nicht beispielsweise mit der Drohung einer Entlassung an der Ausübung ihrer Aufgaben gehindert werden können. In Bezug auf die konkrete Umsetzung dieser Vorgabe bestehen verschiedene Lösungsmöglichkeiten. Entscheidend ist, dass die Regelungen in ihrer Gesamtheit Gewähr für die verlangte «völlige Unabhängigkeit» der Datenschutzaufsicht bieten. Was in dieser Hinsicht angezeigt ist, richtet sich unter anderem danach, wie die Aufsichtsstelle selbst organisatorisch ausgestaltet ist.

2.3.2 Organisatorische Ausgestaltung der kantonalen Aufsichtsstelle

Entgegen dem Antrag des Regierungsrats im Entwurf für das KDSG von 1985, die kantonale Aufsichtsstelle für Datenschutz als Kommission auszugestalten, entschied sich der Grosse Rat auf Antrag der vorberatenden Kommission dafür, die Aufsicht einem Datenschutzbeauftragten zu übertragen. Diese Lösung hat sich in der Praxis bewährt. Nach Ansicht des Regierungsrats besteht kein Anlass, auf den damaligen Beschluss des Grossen Rates zurückzukommen. Den seinerzeit für eine Kommission ins Feld geführten Argumenten kommt heute im Licht der europäischen Vorgaben nur noch beschränktes Gewicht zu. Angesichts der neuen zwingenden Aufgaben im Bereich der Datenschutzaufsicht (vgl. hinten Ziff. 2.4) wird eine kostengünstige

«Milizkommission» nicht mehr möglich sein. Das erforderliche Fachwissen kann, soweit die oder der Datenschutzbeauftragte nicht selbst darüber verfügt, im Rahmen des heutigen Systems bedürfnisgerecht bei Dritten beschafft werden. Gegen die Ausgestaltung als Kommission spricht nicht zuletzt die Schwerfälligkeit dieser Lösung. Eine Kommission wird weniger rasch als eine einzelne Person reagieren können, was negative Auswirkungen auf die Erledigung vor allem der Tagesgeschäfte hätte.

Es besteht auch kein Grund, die Aufsichtsstelle neu als Verwaltungseinheit auszugestalten. Die mit einer oder einem Datenschutzbeauftragten verbundene «Personifizierung» erscheint mindestens in psychologischer Hinsicht günstiger, weil sich Betroffene mit einer Einzelperson eher identifizieren können und den Zugang zu einer solchen eher finden werden als zu einer «anonymen» Verwaltungseinheit. Die Bildung einer eigentlichen Verwaltungseinheit erschiene auch angesichts des begrenzten Umfangs bezüglich Tätigkeit und Ressourcen unverhältnismässig; in diesem Punkt lässt sich die Datenschutzaufsicht beispielsweise nicht mit der kantonalen Finanzkontrolle vergleichen.

Das heutige System mit einer oder einem kantonalen Datenschutzbeauftragten soll deshalb beibehalten werden. Dieses System entspricht einer verbreiteten Regelung im In- und Ausland und namentlich auch der durch den Bund gewählten Lösung (Art. 26 ff. DSG). Es schliesst nicht aus, dass sich im Rahmen der mit dem Vorschlag bewilligten Mittel unter Umständen weitere Personen mit besonderen Kenntnissen (Recht, Informatik) mit Datenschutzfragen befassen, die ihre Aufgaben allerdings unter der Verantwortung der oder des Datenschutzbeauftragten wahrnehmen werden.

2.3.3 Institutionelle Sicherungen der Unabhängigkeit

a) Wahl/Ernennung der oder des kantonalen Beauftragten

Heute wird die oder der kantonale Datenschutzbeauftragte durch den Regierungsrat gewählt (Art. 32 Abs. 1 KDSG). Diese Regelung erscheint im Licht der europäischen Vorgaben zwar grundsätzlich möglich, ist aber nicht unproblematisch, weil eine Wahl oder Ernennung ausschliesslich durch die Exekutive eine Wahl der Kontrollierenden durch die Kontrollierten darstellt. Sie kann gemäss der KdK-Wegleitung «unter dem Aspekt der verlangten völligen Unabhängigkeit allerhöchstens dann genügen, wenn dieses offensichtliche Manko» durch «andere Sicherungen in höchster Qualität», insbesondere durch eine verhältnismässig lange Amtsdauer (die Wegleitung geht von einer Amtsdauer von acht oder mehr Jahren aus), kompensiert wird. Im Interesse der Unabhängigkeit wurde eine förmliche Wahl der für die Datenschutzaufsicht verantwortlichen Person durch den Grossen Rat bereits anlässlich der Schaffung des Datenschutzgesetzes durch die damalige Justizdirektion vorgeschlagen. Vor allem im Licht der neuen europäischen Vorgaben sprechen gute Gründe für diese Lösung, namentlich die folgenden:

- Die Unabhängigkeit der Datenschutzaufsicht von Regierung und Verwaltung wird bereits anlässlich der Bestellung der Aufsichtsstelle gewahrt. Damit wird den

europarechtlichen Vorgaben optimal Rechnung getragen; der Kanton ist mit dieser Lösung «auf der sicheren Seite».

- Rechtsunsicherheiten werden vermieden. Erfolgte die Wahl, wie heute, durch den Regierungsrat, müsste die Regelung durch «andere Sicherungen in höchster Qualität» ergänzt werden, von denen nicht klar ist, worin sie im Einzelnen bestehen müssen.
- Aus politischer Sicht erscheint es wünschenswert, dass bereits der blosser Anschein einer Abhängigkeit von Exekutive und Verwaltung vermieden wird. Eine Wahl durch den Grossen Rat vermeidet auch diesen Anschein.

Für die Beibehaltung der Wahl durch den Regierungsrat könnte demgegenüber sprechen, dass der Regierungsrat dank der Kenntnisse der Verwaltung eher in der Lage ist, die fachliche Eignung der in Frage stehenden Personen zu beurteilen. Diesem Umstand kann dadurch Rechnung getragen werden, dass der Grosse Rat die Person auf Antrag des Regierungsrats wählt. Die förmliche Wahl durch den Grossen Rat erscheint aber aus den erwähnten rechtlichen und politischen Gründen angezeigt. Für den Grossen Rat ist damit kein ins Gewicht fallender Mehraufwand verbunden, weil eine Wahl in der Regel nur auf eine neue Amtsdauer vorzunehmen sein wird (vgl. sogleich Ziff. 2.3.3 b).

b) Amtsdauer

Das Datenschutzgesetz enthält keine besonderen Vorschriften über die Rechtsstellung des Datenschutzbeauftragten, womit die betreffende Person nach den Art. 37 ff. des Personalgesetzes vom 16. September 2004 (PG)¹⁵⁾ in einem unbefristeten, kündbaren öffentlich-rechtlichen Anstellungsverhältnis steht. Zur Sicherung der verlangten «völligen Unabhängigkeit» wird die oder der Datenschutzbeauftragte in Zukunft auf eine feste Amtsdauer zu wählen sein. Üblich sind im Kanton Bern Amtsdauern von vier Jahren. In einzelnen Fällen, so beispielsweise für Geistliche¹⁶⁾ sowie für die Mitglieder des Obergerichts¹⁷⁾ und des Verwaltungsgerichts¹⁸⁾, gilt eine Amtsdauer von sechs Jahren. Angesichts der hohen demokratischen Legitimation aufgrund der hier vorgeschlagenen Wahl durch den Grossen Rat erscheint die im Kanton übliche vierjährige Amtsdauer angemessen.

Eine Amtszeitbeschränkung mag zwar der Gefahr vorbeugen, dass die oder der Datenschutzbeauftragte im Lauf der Zeit eine allzu grosse (persönliche) Nähe zu den kontrollierten Stellen aufweist. Andererseits sind im Bereich der Datenschutzaufsicht Fachkompetenz und damit auch eine gewisse Erfahrung unabdingbar. Auf eine gesetzliche Amtszeitbeschränkung wird deshalb verzichtet, womit die oder der Datenschutzbeauftragte grundsätzlich unbeschränkt wiederwählbar ist.

¹⁵⁾ BSG 153.01

¹⁶⁾ Art. 32 Abs. 1 des Gesetzes vom 6. Mai 1945 über die bernischen Landeskirchen (BSG 410.1)

¹⁷⁾ Art. 4 Abs. 1 des Gesetzes vom 14. März 1995 über die Organisation der Gerichtsbehörden in Zivil- und Strafsachen (GOG; BSG 161.1)

¹⁸⁾ Art. 120 Abs. 1 VRPG, Fassung vom 14. März 1995

c) Ressourcen

Die Unabhängigkeit der Datenschutzaufsicht ist nur gewährleistet, wenn die zu kontrollierende Verwaltung die Planung und Durchführung der Kontrolltätigkeit nicht dadurch verhindern oder beeinflussen kann, dass sie der Aufsichtsstelle die erforderlichen Ressourcen vorenthält. In der Praxis zeigten sich in dieser Hinsicht denn auch durchaus Probleme. So hielt die Geschäftsprüfungskommission zum Verwaltungsbericht 2000 fest, der gesetzliche Auftrag des Datenschutzes werde chronisch untererfüllt. Die Kommission empfahl dem Regierungsrat, die erforderlichen Ressourcen bereitzustellen. Der Regierungsrat setzte diese Empfehlung in drei Regierungsratsbeschlüssen um (Einsetzen externer Kontrollstellen; Einsetzen der Rechtsdienste als Anlaufstellen für Datenschutzfragen der Verwaltung; Verpflichtung, zu Informatikprojekten Datenschutzkonzepte zu erstellen). Der Regierungsrat nahm zur Kenntnis, dass die Datenschutzaufsichtsstelle 120 Geschäfte unerledigt zu den Akten legte. Nicht ohne Grund verlangen daher die europäischen Vorgaben ausdrückliche gesetzliche «Sicherungen». Nach diesen Vorgaben muss die Aufsichtsstelle über einen eigenen Voranschlag für die benötigten Personal- und Sachressourcen verfügen, welcher dem für den Beschluss zuständigen Organ, d.h. dem Grossen Rat, «ohne Regierungsintervention» unterbreitet wird. Die für die Datenschutzaufsicht verantwortliche Person oder Stelle muss auch die Möglichkeit haben, das für die Erfüllung ihrer Aufgaben benötigte weitere Personal im Rahmen des Voranschlags selbst anstellen zu können. Dies entspricht der geltenden Regelung beispielsweise für die Finanzkontrolle oder für gerichtliche Instanzen. Die Aufsichtsstelle muss auch in Bezug auf die weitere Verwendung der Mittel frei sein und beispielsweise die Möglichkeit haben, im Fall von Kapazitätsproblemen externe Spezialistinnen und Spezialisten beizuziehen.

d) Administrative Zuordnung

Heute ist die kantonale Aufsichtsstelle für Datenschutz administrativ der Justiz-, Gemeinde- und Kirchendirektion angegliedert (Art. 32 Abs. 2 KDSG). Die Datenschutzaufsicht wurde jedenfalls zu Beginn vorab als «Spezialdienst» verstanden, der sich vor allem mit juristischen Fragestellungen beschäftigt. Eine eigentliche Eingliederung der Aufsichtsstelle in die Verwaltung im Sinn einer hierarchischen Unterstellung unter eine Direktion wurde aber bereits beim Erlass des Datenschutzgesetzes verworfen, weil die Unabhängigkeit der Datenschutzaufsicht damit in Frage gestellt worden wäre. Eine derartige Eingliederung genügt insbesondere den Anforderungen von Schengen/Dublin nicht, welche für die Datenschutzaufsicht «völlige Unabhängigkeit» verlangen. Grundsätzlich möglich ist demgegenüber auch im Licht der europarechtlichen Vorgaben eine rein administrative Zuordnung zu einer Direktion. Denkbar ist ebenso eine Zuordnung zum Büro des Grossen Rates oder zur Staatskanzlei.

Die KdK-Wegleitung empfiehlt, die Aufsichtsstelle für Datenschutz im Fall der Wahl durch das Parlament der «Geschäftsleitung des Parlaments», im vorliegenden Fall also dem Büro des Grossen Rates, zuzuordnen. Diese Zuordnung erscheint aus Sicht des Regierungsrats allerdings sachfremd. Die oder der Datenschutzbeauftragte

muss zwar vom Regierungsrat und von der Verwaltung unabhängig sein, erfüllt aber keine parlamentarische, sondern eine Verwaltungsfunktion. Die Unabhängigkeit wird durch die vorgeschlagene Wahl durch den Grossen Rat und die feste Amtsdauer hinreichend gewährleistet. Die Aufsichtsstelle muss auch keinen laufenden Kontakt zum Grossen Rat pflegen, sondern, wie der Regierungsrat und z.B. die Finanzkontrolle auch, dem Grossen Rat nur periodisch berichten (vgl. Art. 37 Abs. 1 KDSG). Eine Zuordnung der Aufsichtsstelle zum Büro des Grossen Rates erscheint deshalb nicht angezeigt.

Die Zuordnung zu einer Direktion mag, theoretisch und aus einer Aussensicht, zumindest den Anschein einer gewissen Abhängigkeit von der Direktionsspitze erwecken. Dies darf allerdings angesichts der zur Gewährleistung der Unabhängigkeit vorgesehenen anderweitigen «Sicherungen» (vorne Ziff. 2.3.3 a–c) nicht überbewertet werden. Tatsächlich hat die Zuordnung zur JGK bisher in der Praxis unter dem Gesichtspunkt der Unabhängigkeit der Datenschutzaufsicht nicht zu grösseren Problemen geführt. Im Sinne einer pragmatischen Anpassung des Datenschutzgesetzes sieht der Entwurf deshalb vor, dass die kantonale Aufsichtsstelle für Datenschutz in administrativer Hinsicht wie bisher der Justiz-, Gemeinde- und Kirchendirektion zugeordnet wird.

2.3.4 Datenschutzaufsicht über Leistungserbringer gemäss Spitalversorgungsgesetz

In Bezug auf die Organisation der Datenschutzaufsicht stellt sich ein besonderes Problem hinsichtlich der Aufsicht über Leistungserbringer im Sinn des Spitalversorgungsgesetzes vom 5. Juni 2005 (SpVG)¹⁹⁾. Nach Art. 77 SpVG kann der Regierungsrat durch Verordnung die Leistungserbringer, die kantonale Aufgaben erfüllen, zur Bezeichnung einer eigenen Aufsichtsstelle für Datenschutz verpflichten; die kantonale Aufsichtsstelle im Sinn von Art. 32 KDSG übt in diesen Fällen die Oberaufsicht aus. Die bisherigen Spitalverbände waren als gemeinderechtliche Körperschaften verpflichtet, eine eigene Datenschutzaufsichtsstelle zu führen. Mit Art. 77 SpVG sollte sichergestellt werden, dass die entsprechenden Ressourcen auch nach der Kantonalisierung der öffentlichen Spitäler zur Verfügung stehen würden.

Der Regierungsrat hat von seiner Kompetenz Gebrauch gemacht und die Erbringer von Spital- und Rettungsleistungen, die kantonale Aufgaben erfüllen und nicht Teil der Kantonsverwaltung sind, mit Art. 110 der Spitalversorgungsverordnung vom 30. November 2005 (SpVV)²⁰⁾ verpflichtet, eine gemeinsame, fachlich unabhängige Aufsichtsstelle für Datenschutz zu bezeichnen. Diese Stelle besteht zur Zeit noch nicht. Im Licht der Vorgaben von Schengen/Dublin erscheint es fraglich, ob diese Bestimmung beibehalten werden soll. Für eine zentrale Datenschutzaufsicht, auch im Bereich der Spitäler, sprechen die Komplexität der Fragen, insbesondere auch im Zusammenhang mit Klinikinformationssystemen (elektronische Führung der Behandlungsdokumentationen), und die damit verbundenen hohen Anforderungen an

die Fachkompetenz der verantwortlichen Personen. Mit einer Zentralisierung würde die Datenschutzaufsicht auch in dem Sinn vereinfacht, als eine einheitliche Aufsicht über die drei kantonalen psychiatrischen Kliniken als Teil der Kantonsverwaltung und die übrigen Spitäler bestünde und die Oberaufsicht des kantonalen Datenschutzauftragten über die Aufsichtsstelle der Spitäler entfielen. Diese Lösung läge schliesslich auch in der Linie der mit dem SpVG erfolgten Kantonalisierung der Spitäler. Der Regierungsrat zieht aus diesen Gründen eine Revision oder Streichung von Art. 110 SpVV im Sinn einer Übertragung der Datenschutzaufsicht über die Spitäler an den kantonalen Beauftragten in Erwägung. Noch näher abzuklären wird sein, wie die Finanzierung dieser Tätigkeit durch die Leistungserbringer nach SpVG erfolgen kann.

Die in die Zuständigkeit des Grossen Rates fallende gesetzliche Regelung wird durch eine allfällige Änderung der SpVV allerdings nicht berührt. Art. 77 SpVG enthält lediglich eine Kannvorschrift im Sinn einer Ermächtigung an den Regierungsrat. Die Bestimmung kann auch dann beibehalten werden, wenn der kantonale Datenschutzauftragte die Aufsicht über die Spitäler wahrnimmt.

2.3.5 Datenschutzaufsicht in den Gemeinden

Für die Gemeinden und andern gemeinderechtlichen Körperschaften gilt das Datenschutzgesetz grundsätzlich in gleicher Weise wie für den Kanton. Auf die gemeinderechtlichen Körperschaften anwendbar sind namentlich die Bestimmungen über die Unabhängigkeit der Datenschutzaufsicht sowie die Zuständigkeiten und insbesondere über die unter Ziffer 2.4 näher zu erörternden Aufgaben und Befugnisse der Aufsichtsstelle. An die organisatorische Ausgestaltung und Fachkompetenz der kommunalen Aufsichtsstellen werden somit hohe Anforderungen gestellt. Im Licht dieser Anforderungen sprechen zwar durchaus auch Argumente für eine Kantonalisierung der Datenschutzaufsicht in den Gemeinden. Vor allem für kleinere gemeinderechtliche Körperschaften dürfte es mitunter schwierig sein, eine Aufsichtsstelle mit der nötigen Fachkompetenz ins Leben zu rufen.

Im Rahmen der vorliegenden Revision werden, entsprechend den erwähnten Leitideen (vorne Ziff. 1.4), nur Anpassungen vorgeschlagen, die aufgrund der europäischen Vorgaben oder aus andern Gründen mehr oder weniger zwingend erscheinen. Zwingender Änderungsbedarf im Sinn einer Kantonalisierung der Datenschutzaufsicht in den Gemeinden besteht nicht. Das europäische Recht schreibt keine Zentralisierung der Datenschutzaufsicht vor; kommunale Aufsichtsstellen sind mit Schengen/Dublin grundsätzlich vereinbar. Mit Rücksicht auf die verfassungsrechtliche Gewährleistung der Gemeindeautonomie und der Verpflichtung des Kantons, den Gemeinden «einen möglichst weiten Handlungsspielraum» zu gewähren (Art. 109 Abs. 2 KV), erscheint es sachgerecht, das heutige System der gemeindeeigenen Datenschutzaufsichtsstellen beizubehalten. Dies gilt nicht zuletzt deshalb, weil die Gemeinden im Bereich des für Schengen/Dublin zentralen Bereichs der Polizei mit der Umsetzung von Police Bern nur noch beschränkte Zuständigkeiten wahrnehmen werden; wirklich «Schengen/Dublin-relevante» Datenbearbeitungen werden die Gemeinden kaum mehr vorzunehmen haben. Zu beachten ist

¹⁹⁾ BSG 812.11

²⁰⁾ BSG 812.112

auch, dass die kommunalen Stellen der Oberaufsicht durch die kantonale Aufsichtsstelle unterstehen (Art. 33 Abs. 2 KDSG).

Den europäischen Vorgaben, insbesondere dem Zusatzprotokoll, ist dadurch Rechnung zu tragen, dass das Datenschutzgesetz auch für die kommunalen Aufsichtsstellen in allgemeiner Weise vorschreibt, dass diese ihre Aufgaben in völliger Unabhängigkeit wahrnehmen müssen und dass die Gemeinden entsprechende organisatorische bzw. institutionelle Sicherungen zur Gewährleistung dieser Unabhängigkeit vorsehen müssen. Wie die Gemeinden diese zwingenden Vorgaben umsetzen, ist ihnen im Rahmen ihrer Organisationsautonomie überlassen. Sie sollen immerhin durch eine adäquate Information über die rechtlichen Anforderungen an die Datenschutzaufsicht und insbesondere an deren Unabhängigkeit und Einwirkungsmöglichkeiten, beispielsweise im Rahmen einer BSIG-Information oder eines aktualisierten Muster-Datenschutzreglements, unterstützt und begleitet werden. Gemeinderechtliche Körperschaften, welchen den europarechtlichen Anforderungen nicht entsprechen, werden aufzufordern sein, die erforderlichen Verbesserungen auszulösen. Als rechtlich heikel dürften nach dem unter Ziffer 2.3.3 Ausgeführten kommunale Lösungen zu beurteilen sein, wonach die Aufsichtsstelle in einem kommunalen Rechtsdienst integriert ist oder in einem Auftragsverhältnis zur Gemeinde steht, das von der Gemeindeexekutive jederzeit aufgelöst werden kann.

2.4. Aufgaben und Befugnisse der Aufsichtsstellen

2.4.1 Behandlung von Eingaben

Nach Art. 28 Abs. 4 EU-Datenschutzrichtlinie können sich die Betroffenen «an jede Kontrollstelle mit einer Eingabe wenden», wobei die betroffene Person darüber zu informieren ist, «wie mit der Eingabe verfahren wurde». Ein Anspruch auf Überprüfung des Anliegens besteht da, wo das Auskunftsrecht in den Bereichen Polizei, Strafverfolgung und Staatsschutz aufgrund besonderer Vorschriften eingeschränkt ist. Das geltende Datenschutzgesetz statuiert keine Pflicht zur Behandlung von Eingaben betreffend die Bearbeitung ihrer Personendaten, verweist aber in Art. 26 KDSG für das Verfahren in allgemeiner Weise auf das VRPG. Nach Art. 101 VRPG kann die Person, welche eine aufsichtsrechtliche Anzeige einreicht, Auskunft über die Erledigung der Anzeige verlangen; ein Anspruch auf materielle Behandlung und Erledigung des Begehrens besteht nicht. Diese Regelung genügt den erwähnten Vorgaben des europäischen Rechts nicht vollständig, weil sie eine Pflicht zur Auskunft über die Behandlung aufsichtsrechtlicher Eingaben nur auf Verlangen statuiert. Soweit in den Bereichen Polizei, Strafverfolgung und Staatsschutz das Recht auf Einsicht in eigene Personendaten eingeschränkt ist, ist eine solche Pflicht somit generell zu statuieren.

2.4.2 Untersuchungsbefugnisse, Vorabkontrollen

Art. 28 Abs. 3 EU-Datenschutzrichtlinie verlangt, dass die Aufsichtsstelle über «Untersuchungsbefugnisse» verfügt. Gemäss Art. 35 Abs. 2 KDSG kann die Auf-

sichtsstelle bei Behörden, ungeachtet allfälliger Geheimhaltungspflichten, schriftliche oder mündliche Auskünfte einholen, Einsicht in alle Unterlagen von bestimmten Bearbeitungen nehmen, Besichtigungen durchführen und sich Bearbeitungen vorführen lassen. Die verantwortlichen Behörden sind verpflichtet, die Aufsichtsstelle in der Erfüllung ihrer Aufgaben zu unterstützen (Art. 35 Abs. 1 KDSG). Mit dieser Regelung werden der Aufsichtsstelle umfassende Untersuchungsbefugnisse zugestanden, womit den europäischen Anforderungen unter diesem Gesichtspunkt Genüge getan ist.

Regelungsbedarf besteht indes im Hinblick auf den besonderen Fall so genannter Vorabkontrollen. Art. 20 Abs. 1 EU-Datenschutzrichtlinie verpflichtet die Mitgliedstaaten dazu, festzulegen, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, und dafür Sorge zu tragen, dass diese Verarbeitungen vor ihrem Beginn geprüft werden. Abs. 2 dieser Bestimmung schreibt vor: «Solche Vorabprüfungen nimmt die Kontrollstelle nach Empfang der Meldung des für die Verarbeitung Verantwortlichen vor, oder sie erfolgen durch den Datenschutzbeauftragten, der im Zweifelsfall die Kontrollstelle konsultieren muss». Derartige Vorabkontrollen sind im Kanton Bern bisher nicht gesetzlich geregelt. Für gemeinderechtliche Körperschaften bestehen überhaupt keine Vorgaben. Für die kantonale Verwaltung sieht ein Regierungsratsbeschluss vom 9. April 2003 vor, dass die Projektverantwortlichen ein Datenschutzkonzept ausarbeiten müssen, wenn ein Informatikprojekt Kosten von mehr als 100 000 Franken auslöst. Dieses Datenschutzkonzept muss der Aufsichtsstelle vor dem Ausgabenbeschluss zur Prüfung unterbreitet werden. Gleiches gilt, wenn der Kanton an Dritte, etwa an Spitäler, Beiträge an Informatikprojekte ausrichtet. Ein vorprüfungsähnliches Instrument umschreibt Art. 52 Abs. 5 des Polizeigesetzes vom 8. Juni 1997 (PolG)²¹⁾, der für Informatiksysteme der Kantonspolizei das Erfordernis einer Betriebsbewilligung des Regierungsrats statuiert; eine Stellungnahme der Aufsichtsstelle für Datenschutz ist zwar in der Praxis jeweils eingeholt worden, gesetzlich aber nicht vorgeschrieben.

Der Regierungsrat plant, unabhängig von Schengen/Dublin, die Einführung eines differenzierten Vorgehens bei der Einführung neuer Informatikprojekte des Kantons, in dessen Rahmen auch der Vorprüfung aus datenschutzrechtlicher Sicht das gebührende Gewicht beigemessen werden soll. Dieses Vorgehen genügt, für die kantonale Verwaltung und für Beiträge des Kantons, den europäischen Vorgaben, muss aber in einem Gesetz verankert werden. Gesetzlich vorzuschreiben sind überdies Vorabkontrollen für Informatiksysteme der gemeinderechtlichen Körperschaften.

2.4.3 Einwirkungsbefugnisse

Art. 28 Abs. 3 EU-Datenschutzrichtlinie verlangt «wirksame Einwirkungsbefugnisse» der Aufsichtsstelle und zählt beispielhaft auf, was darunter etwa zu verstehen ist. Dazu können etwa die Befugnis zur geeigneten Veröffentlichung der Stellungnahmen, zur Anordnung der Sperrung, Löschung oder Vernichtung von Daten oder des

²¹⁾ BSG 551.1

endgültigen Verbots einer Datenbearbeitung, zur Verwarnung oder Ermahnung der Verantwortlichen oder zur Befassung des Parlaments oder anderer politischen Institutionen gezählt werden. Ein bestimmter «Minimalsatz» an Einwirkungsbefugnissen wird nicht ausdrücklich vorgeschrieben. Erforderlich ist aber, dass die Aufsichtsstelle mit den gesetzlich festgelegten Einwirkungsbefugnissen in ihrer Gesamtheit tatsächlich Wirksamkeit entfalten kann. Die Aufsichtsstelle muss deshalb in der Lage sein, die datenschutzrechtlichen Vorgaben im Notfall auch gegen den Willen einer widerstrebenden Behörde durchzusetzen.

Diesem Erfordernis entspricht die geltende Regelung nicht. Die Aufsichtsstelle hat heute grundsätzlich nur die Möglichkeit, die Beseitigung von Verstössen und Mängeln zu empfehlen und Vorschläge zur Verbesserung des Datenschutzes zu unterbreiten (Art. 35 Abs. 3 KDSG; vgl. zur – praktisch allerdings bedeutungslosen – Verfügungsbefugnis nach Art. 27 hinten Ziff. 3.1, Bemerkungen zu Art. 27). Folgt die für die Datenbearbeitung verantwortliche Stelle einer Empfehlung nicht, hat die Aufsichtsstelle keine Möglichkeit, verbindliche Anordnungen zu erlassen und ihre Haltung gegen den Willen der betroffenen Stelle durchzusetzen. Sie kann lediglich die verantwortliche oder die vorgesetzte Behörde zum Ergreifen von Massnahmen auffordern (Art. 35 Abs. 4 KDSG) und die Öffentlichkeit informieren (Art. 37 Abs. 2 KDSG) und dadurch Druck ausüben.

Der Vorgabe wirksamer Einwirkungsbefugnisse kann auf verschiedene Arten Rechnung getragen werden. Namentlich bestehen folgende Optionen:

Variante a)

Die Aufsichtsstelle entscheidet im Bedarfsfall selbst. Sie erlässt ihre Empfehlungen in Form einer verbindlichen Anweisung an die betroffene Behörde, welcher die gleiche Wirkung wie einer Verfügung nach Art. 49 VRPG gegenüber Privaten zukommt.

Variante b)

Die Aufsichtsstelle hat grundsätzlich die Befugnisse nach geltendem Recht. Sie kann aufgrund ihrer umfassenden Auskunfts- und Prüfungsrechte den Daten bearbeitenden Behörden Empfehlungen abgeben, wie die geplante oder getätigte Datenbearbeitung rechts- und datenschutzkonform auszugestaltet ist. Sie kann in diesem Rahmen selbst grundsätzlich keine verbindlichen Anordnungen treffen, aber für den Fall, dass der Empfehlung nicht gefolgt wird, verlangen, dass die Daten bearbeitende Behörde die umfassende oder teilweise Ablehnung der Empfehlungen mittels einer Verfügung im Sinn von Art. 49 VRPG oder – in Verfahren, für welche die ZPO oder das StrV zur Anwendung kommt – eines anderweitigen verbindlichen Beschlusses eröffnet. Dieser Entscheid kann durch die Aufsichtsstelle mittels Behördenbeschwerde bei den zuständigen Rechtspflegeinstanzen angefochten werden. Die Aufsichtsstelle hat damit die Möglichkeit, ein verbindliches Urteil über die Rechtmässigkeit der umstrittenen Datenbearbeitung zu erwirken.

Variante c)

Eine teilweise mit Variante b) vergleichbare weitere Option sieht das Bundesrecht in Art. 27 Abs. 4–6 DSG vor: Die Aufsichtsstelle gibt, wie im Fall der Variante b), eine Empfehlung ab. Sie orientiert darüber das zuständige Departement oder die Bundeskanzlei. Wird eine Empfehlung nicht befolgt oder abgelehnt, kann die Aufsichtsstelle die Angelegenheit dem Departement oder der Bundeskanzlei zur Entscheid vorlegen. Gegen den Entscheid dieser Stellen kann sie Beschwerde erheben.

Die Variante c) hat den Nachteil, dass bereits vor dem Erlass einer verbindlichen Anordnung drei Stellen in das Verfahren involviert sind. Sie ist somit verhältnismässig kompliziert und dürfte zu entsprechenden Verzögerungen führen, weist aber gegenüber der Variante b) keinen nennenswerten Vorteil auf. Sie fällt deshalb für den Regierungsrat ausser Betracht. Demgegenüber lassen sich sowohl für die Variante a) als auch für die Variante b) gewisse Argumente anführen. Aus der Sicht des Regierungsrats überwiegen insgesamt die Vorteile der Variante b) deutlich. Zugunsten dieser Variante sprechen namentlich die folgenden Gründe:

- Die Variante b) entlastet die Datenschutzaufsichtsstelle und schont deren Ressourcen. Der Aufwand für eine Empfehlung wird deutlich kleiner sein als für den Erlass einer förmlichen Verfügung. Verbindliche Anordnungen müssten in inhaltlicher Hinsicht wesentlich solider geprüft werden und verursachen auch in verfahrensrechtlicher Hinsicht Mehraufwand (z.B. rechtliches Gehör). Folgt die angesprochene Behörde der Empfehlung, ist die Sache erledigt.
- Die Variante b) entspricht dem Grundsatz, dass für die gesetzeskonforme Datenbearbeitung die Behörde verantwortlich ist, welche die Daten bearbeitet (Art. 8 Abs. 1 KDSG). Mit der Möglichkeit zwangsweiser Anordnungen der Aufsichtsstelle würde diese Verantwortung verwässert.
- Mit der Variante b) kommt gewissermassen das «Verursacherprinzip» zur Anwendung. Die Daten bearbeitende Behörde entscheidet selbst, wie sie ihre Aufgaben wahrnimmt. Sie muss aber in Kauf nehmen, dass ihr im Fall der Nichtbefolgung einer Empfehlung der Aufsichtsstelle Mehraufwand entstehen kann, indem sie ihre Rechtsauffassung in Verfügungsform bestätigen und ausführlich begründen sowie allenfalls auch in einem Rechtsmittelverfahren vertreten muss. Der Aufwand zur Beilegung von Differenzen wird damit der Partei auferlegt, die behauptet, hinreichende Gründe zu haben, um einer Empfehlung nicht zu folgen.
- Die direkte zwangsweise Anordnung von Massnahmen nach der Variante a) widerspräche der schweizerischen Auffassung einer Datenschutzaufsichtsstelle, die vorab beratend und begleitend tätig werden soll.
- Im Fall der Variante b) besteht immer die Möglichkeit, dass die Daten bearbeitende Stelle und die Datenschutzaufsichtsstelle zunächst das Gespräch suchen und eine einvernehmliche Lösung finden. Dadurch wird nicht zuletzt die Rolle der Aufsichtsstelle als beratendes und unabhängiges Organ gestärkt.
- Schliesslich weist die Variante b) auch verfahrensrechtliche Vorteile auf. Die heute bereits bestehenden Rechtsmittelzüge nach den jeweils anwendbaren verfahrensrechtlichen Bestimmungen gemäss dem VRPG, der ZPO, dem StrV oder allenfalls der Spezialgesetzgebung können unverändert zur Anwendung

kommen. Die Datenschutzaufsichtsstelle kann die in Frage stehende Verfügung oder den in Frage stehenden Beschluss wie eine Privatperson im entsprechenden, bereits heute gesetzlich vorgesehenen Verfahren anfechten.

Es erscheint aus diesen Gründen angezeigt, im Sinn der Variante b) am Instrument der Empfehlung festzuhalten, dieses Instrument aber mit der Möglichkeit der Aufsichtsstelle zu ergänzen, die Behörde zum Erlass einer ablehnenden Verfügung oder eines ablehnenden Beschlusses zu veranlassen. Auch auf diesem Weg kann im Bedarfsfall nach den anwendbaren verfahrensrechtlichen Vorschriften (VRPG, allenfalls ZPO oder StrV) ein verbindliches gerichtliches Urteil erwirkt werden. Die möglichen Argumente zugunsten der Variante a) vermögen die Vorteile der Variante b) aus der Sicht des Regierungsrats nicht aufzuwiegen. Dass nach der Variante b) einer allfälligen gerichtlichen Überprüfung im Fall der Anwendbarkeit des VRPG ein verwaltungsinternes Beschwerdeverfahren vorgeschaltet ist, stellt keinen ins Gewicht fallenden Nachteil dar. Die Gefahr, dass die verantwortliche Behörde zwar auf den Erlass einer ablehnenden Verfügung verzichtet und die Empfehlung scheinbar akzeptiert, aber dann die empfohlene Anordnung dennoch nicht umsetzt, kann zwar nicht ausgeschlossen werden, dürfte aber nach den bisherigen Erfahrungen weit gehend theoretischer Natur sein. Gegen behördliche Untätigkeit könnte im Bedarfsfall Rechtsverweigerungs- bzw. Rechtsverzögerungsbeschwerde erhoben werden (vgl. insbesondere Art. 49 Abs. 2 VRPG).

2.4.4 Klage- und Anzeigebefugnis, Sanktionen

Art. 28 Abs. 3 EU-Datenschutzrichtlinie verlangt «das Klagerecht oder eine Anzeigebefugnis» der Datenschutzaufsichtsstelle bei Verstössen gegen die Vorschriften zur Umsetzung dieser Richtlinie. Erforderlich ist kein eigentliches «Recht zur Klage», sondern das Recht, bei einem Verstoss gegen das Datenschutzgesetz eine Anzeige einzureichen und diesen dadurch zur strafrechtlichen Sanktionierung zu bringen. Es genügt mithin, wenn die Aufsichtsstelle die Möglichkeit hat, bei der Strafverfolgungsbehörde eine Anzeige einzureichen. Dieses Erfordernis ist erfüllt. Erhält die Datenschutzaufsichtsstelle Kenntnis von einer von Amtes wegen zu verfolgenden Straftat, ist sie nach Art. 199 und 201 StrV berechtigt oder sogar verpflichtet, bei der Polizei oder einer andern Strafverfolgungsbehörde Strafanzeige einzureichen. Überdies hat sie bei festgestellten oder vermuteten Verstössen gegen das Datenschutzgesetz, unabhängig von der Strafbarkeit der in Frage stehenden Handlung, stets die Möglichkeit, Empfehlungen abzugeben (Art. 35 Abs. 3 KDSG) oder eine aufsichtsrechtliche Anzeige einzureichen (Art. 101 VRPG).

Art. 24 EU-Datenschutzrichtlinie verlangt, dass Verstösse gegen die Datenschutzgesetzgebung mit Sanktionen geahndet werden. Gegen Verletzungen des Amtsgeheimnisses durch die Daten bearbeitenden Behörden bietet Art. 320 des Schweizerischen Strafgesetzbuchs vom 21. Dezember 1937 (StGB) strafrechtlichen Schutz. Dritte, die Personendaten im Auftrag einer Behörde bearbeiten, unterstehen dem Amtsgeheimnis ebenfalls (Art. 16 KDSG). Soweit beauftragte Dritte Personendaten auftragswidrig bekannt geben, dürfte der Tatbestand der Amtsgeheimnisverletzung erfüllt sein, weshalb für diesen Fall die bestehende Regelung des StGB

genügt. Indes sind auch Verstösse gegen das Datenschutzgesetz durch Daten bearbeitende Behörden selbst oder beauftragte Dritte denkbar, die nicht unter den Tatbestand der Amtsgeheimnisverletzung fallen. So dürfen gemäss Art. 5 Abs. 4 KDSG Personendaten nicht für einen Zweck bearbeitet werden, der nach Treu und Glauben mit dem Zweck unvereinbar ist, für den sie ursprünglich beschafft oder der Behörde bekannt gegeben worden sind. In solchen Fällen kann heute lediglich die Widerrechtlichkeit der Handlung festgestellt werden, ohne dass die Möglichkeit einer strafrechtlichen Sanktion besteht. Eine solche Möglichkeit erscheint zwar grundsätzlich wünschbar, doch dürfte dieses Problem vorab im Rahmen einer bundesrechtlichen Regelung im StGB zu lösen sein; der Erlass einer besonderen Strafbestimmung im kantonalen Recht erscheint nicht opportun.

2.4.5 Amtshilfe

Art. 28 Abs. 6 EU-Datenschutzrichtlinie und Art. 1 Ziff. 5 Zusatzprotokoll verpflichten die Datenschutzaufsichtsstellen, zur Erfüllung ihrer Kontrollaufgaben zusammenzuarbeiten und Amtshilfe zu leisten. In Betracht kommt eine Zusammenarbeit sowohl mit Aufsichtsstellen anderer Kantone und des Bundes als auch mit entsprechenden Stellen im Ausland. Weil der Kanton Bern auch kommunale Aufsichtsstellen kennt, muss auch die Pflicht zur Zusammenarbeit innerhalb des Kantons geregelt werden.

Das geltende Recht enthält zwar Bestimmungen über die Zusammenarbeit. Art. 36a Abs. 1 KDSG erlaubt es der kantonalen Aufsichtsstelle im Sinn einer Kannvorschrift, zur Erfüllung ihrer Aufgaben mit Datenschutzaufsichtsorganen anderer öffentlich-rechtlicher Körperschaften zusammenzuarbeiten, wobei Art und Umfang der Zusammenarbeit in einer schriftlichen Vereinbarung umschrieben werden (Art. 36a Abs. 2 KDSG). Diese Regelung wurde im Zusammenhang mit dem Gesetz vom 5. Juni 2002 über die Aktiengesellschaft Bedag Informatik (Bedag-Gesetz, BIG)²²⁾ in das Datenschutzgesetz aufgenommen und sollte im Zusammenhang mit der Beteiligung des Kantons Waadt an der Bedag gemeinsame Inspektionshandlungen der kantonalen Aufsichtsstellen von Bern und Waadt ermöglichen. Die eigentliche Amtshilfe im Sinne von Art. 28 Abs. 6 EU-Datenschutzrichtlinie ist nicht Gegenstand der Bestimmung. Auch die allgemeinen Vorschriften über die Zusammenarbeit von Bund und Kantonen in Art. 44 BV und über die Rechtshilfe der Verwaltungs- und Verwaltungsjustizbehörden in Art. 10 VRPG erscheinen, insbesondere im Hinblick auf die Zusammenarbeit mit ausländischen Aufsichtsstellen, nicht als hinreichende Regelung.

2.4.6 Weitere Punkte

Die vorliegende Teilrevision wird schliesslich zum Anlass genommen, um die praktisch bedeutungslose Bestimmung über die Verfügungsbefugnis der Aufsichts-

²²⁾ BSG 152.031.2

stelle zu streichen und deren Rechenschaftspflicht teilweise neu zu regeln (vgl. dazu hinten Ziff. 3.1, Erläuterungen zu Art. 27 und 37 KDSG).

3. Bemerkungen zu einzelnen Bestimmungen

3.1 Datenschutzgesetz

Artikel 4: Geltungsbereich

Entsprechend der bundesrechtlichen Regelung (Art. 2 Abs. 2 Bst. c DSG) wird der Anwendungsbereich des Datenschutzgesetzes mit Art. 4 Abs. 2 Bst. c KDSG auf Verwaltungsverfahren, d.h. auf Verfahren auf Erlass einer Verfügung (Art. 49–59 VRPG), ausgedehnt (vgl. dazu vorne Ziff. 2.2.1). Für Verwaltungsjustizverfahren einschliesslich des verwaltungsinternen Beschwerdeverfahrens gelten demgegenüber ausschliesslich die Bestimmungen des VRPG. Die Änderung bedingt eine entsprechende Anpassung von Art. 23 VRPG (vgl. hinten Ziff. 3.2).

Artikel 14a (neu): Bekanntgabe von Daten ins Ausland

Mit dem neuen Art. 14a wird die verlangte Regelung der grenzüberschreitenden Datenbekanntgabe in das Gesetz aufgenommen. Die Bestimmung orientiert sich weitgehend an der bundesrechtlichen Regelung in Art. 6 des revidierten DSG, mit welchem der Bund sein Recht an die Vorgaben gemäss Zusatzprotokoll angepasst hat.

Abs. 1 entspricht wörtlich Art. 6 Abs. 1 rev. DSG. Abs. 2 sieht verschiedene Voraussetzungen vor, unter denen vom Grundsatz nach Abs. 1 abgewichen werden kann. Wie sich aus dem Wort «oder» am Ende von Bst. e ergibt, handelt es sich um alternative Möglichkeiten. Für die Zulässigkeit der Bekanntgabe genügt es mithin, wenn eine der genannten Voraussetzungen erfüllt ist. Andererseits ist die Aufzählung aber abschliessend, womit mindestens eine der in Abs. 2 genannten Situationen gegeben sein muss, sofern eine Gefährdung im Sinn von Abs. 1 anzunehmen ist. Vorbehalten bleiben allfällige spezialgesetzliche Vorschriften, die eine Bekanntgabe in weiteren Fällen erlauben. Abs. 2 entspricht, abgesehen vom Zusatz «oder» in Bst. e, wörtlich der Regelung in Art. 6 Abs. 2 rev. DSG, wobei Bst. f dieser Bestimmung nicht aufgenommen worden ist. Art. 6 Abs. 2 Bst. f rev. DSG erlaubt die Bekanntgabe auch dann, wenn die betroffene Person die Daten der Allgemeinheit zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Unter dieser Voraussetzung ist die Bekanntgabe nach eidgenössischem Recht auch im Inland zulässig (Art. 17 Abs. 2 Bst. c DSG). Das KDSG regelt die Bekanntgabe im Inland in den Art. 10 und 11 einschränkender. Die Aufnahme von Art. 6 Abs. 2 Bst. f DSG in das kantonale Gesetz hätte zur Folge, dass derartige Daten ins Ausland ohne weiteres, in der Schweiz aber nur im engeren Rahmen von Art. 10 und 11 Abs. 2 KDSG bekannt gegeben werden dürften. Die Empfänger in der Schweiz würden damit schlechter gestellt als diejenigen im Ausland. Diese stossende Konsequenz wird vermieden, indem der zwar für das Bundesrecht

angezeigte, für das KDSG aber nicht passende Art. 6 Abs. 2 Bst. f DSG nicht in das kantonale Recht übernommen wird.

Im Interesse der betroffenen Personen muss die Aufsichtsstelle für Datenschutz im Fall einer Bekanntgabe gemäss Abs. 2 Bst. a prüfen können, ob die «anderen hinreichenden Garantien» tatsächlich einen angemessenen Schutz für die beabsichtigte Datenübermittlung gewährleisten. Um dieser Obliegenheit nachkommen zu können, muss sie über die Garantien informiert werden. Abs. 3 hält diesen Grundsatz fest. Die Regelung orientiert sich wiederum an Art. 6 Abs. 3 rev. DSG, präzisiert aber zusätzlich, dass die Information rechtzeitig, mithin vor der Bekanntgabe der Daten ins Ausland, erfolgen muss. Damit hat die Aufsichtsstelle im Bedarfsfall die Möglichkeit, vor der Datenbekanntgabe durch die Abgabe einer förmlichen Empfehlung (vgl. vorne Ziff. 2.4.3) oder – was die Regel sein dürfte – auch nur informell zu reagieren. Auf eine explizite Delegation für die Regelung der Einzelheiten wird verzichtet (vgl. dazu Art. 38 KDSG).

Artikel 17a (neu): Vorabkontrolle

Im neuen Art. 17a wird in Abs. 1 und 2 im Wesentlichen die bestehende Praxis für kantonale Informatikvorhaben gesetzlich festgeschrieben. Die Bestimmung enthält aber nur die Grundsätze und unbestimmte Rechtsbegriffe («grössere Zahl betroffener Personen», «besondere Risiken», «wesentliche Änderungen»), welche der Regierungsrat im Rahmen der vorgesehenen Ausführungsbestimmungen noch zu präzisieren haben wird (vgl. Erläuterungen zu Art. 38).

Abs. 1 zählt verschiedene alternative Voraussetzungen auf, unter denen die Aufsichtsstelle zu konsultieren ist. Mit besonderen Geheimhaltungspflichten (Bst. c) sind besondere gesetzliche Pflichten, beispielsweise solche nach der Sozialversicherungsgesetzgebung, und nicht freiwillig vereinbarte vertragliche Pflichten gemeint. Das Ergebnis der Vorabkontrolle und damit auch die Stellungnahme der Aufsichtsstelle haben grundsätzlich nicht den Charakter einer verbindlichen Anordnung. Soweit nötig bilden sie einen Vorschlag zur Verbesserung des Datenschutzes. Folgt die verantwortliche Behörde dem Vorschlag nicht, kann die Datenschutzaufsichtsstelle nach der Inbetriebnahme der Informatikanwendung eine Empfehlung abgeben. Wird diese abgelehnt, steht das Verfahren nach Art. 35 Abs. 4 offen.

Informatikvorhaben sind in der Regel mit beträchtlichen Kosten verbunden. Das Verfahren nach Art. 35 Abs. 4 soll deshalb in bestimmten Fällen, nämlich dann, wenn dies die verantwortliche Behörde wünscht, nach Abs. 3 auch bereits im Rahmen der Vorabkontrolle, d.h. vor der Inbetriebnahme einer geplanten Bearbeitung, zur Anwendung kommen. Damit können allfällige Differenzen zwischen der verantwortlichen Behörde und der Aufsichtsstelle im Bedarfsfall bereits frühzeitig, bevor unter Umständen unnötige Kosten anfallen, verbindlich geklärt werden.

Die Vorabkontrolle nach Art. 17a gilt für sämtliche Datenbearbeitungen im Sinn dieser Bestimmung und damit insbesondere auch für die Datenbearbeitungssysteme der Kantonspolizei. In Art. 52 PolG ist das Verhältnis dieser Kontrolle zur Erteilung der Betriebsbewilligung für derartige Systeme zu regeln (vgl. den

vorgeschlagenen neuen Art. 52 Abs. 6 PolG). Nicht ausgeschlossen ist, dass auch medizinische Forschungsprojekte einer Vorabkontrolle nach Art. 17a unterstellt sind. Die mit einer allfälligen Bewilligung nach Art. 321^{bis} StGB verbundenen Auflagen zur Sicherung des Datenschutzes und weiteren Rahmenbedingungen werden bei der Vorabkontrolle zu berücksichtigen sein.

Artikel 18: Register der Datensammlungen

Nach heute geltendem Recht liegt die Verantwortung für die Führung des Registers grundsätzlich ausschliesslich bei der Aufsichtsstelle (Art. 34 Bst. a). Die Verpflichtung der verantwortlichen Behörden beschränkt sich auf die Anmeldung der Datensammlungen (Art. 18 Abs. 1). Tatsächlich ist die Aufsichtsstelle aber kaum in der Lage, diese Verantwortung in vollem Umfang wahrzunehmen, weil primär die verantwortliche Behörde und nicht die Aufsichtsstelle weiss, welche Datensammlungen jeweils bestehen oder erheblich verändert werden (vgl. auch vorne Ziff. 2.2.4). Der neu gefasste Art. 18 will diesem Umstand Rechnung tragen und gleichzeitig die Registrierung der Datensammlungen etwas umfassender und präziser als heute regeln.

Die betroffenen Personen werden bei der Wahrung ihrer Rechte wie des Rechts auf Einsichtnahme in Datensammlungen, Berichtigung oder Löschung von Personendaten durch verlässliche und leicht zugängliche Angaben über den Bestand von Datensammlungen unterstützt. Abs. 1 sieht deshalb neu ausdrücklich vor, dass die Aufsichtsstelle das Register über Internet veröffentlicht und in diesem Sinn führt. Die Veröffentlichung des Registers ist nach heutigem Recht nicht ausdrücklich vorgeschrieben, aber aus den genannten Gründen und angesichts des Umstands, dass jede Person Einsicht in das Register nehmen kann (Art. 20), grundsätzlich angezeigt. Sie wird in zeitgemässer Weise über Internet zu erfolgen haben. Mit «Aufsichtsstelle» sind, wie immer im Gesetz, sowohl die kantonale Aufsichtsstelle als auch die kommunalen Aufsichtsstellen gemeint. Wie Abs. 1 zum Ausdruck bringt, werden in dem durch die kantonale Aufsichtsstelle veröffentlichten Register die Datensammlungen der kantonalen Behörden und in den Registern der kommunalen Aufsichtsstellen die in der betreffenden Gemeinde oder gemeinderechtlichen Körperschaft angelegten Datensammlungen zu veröffentlichen sein.

Der neue Abs. 4 regelt Einzelheiten im Zusammenhang mit der Führung des Registers. Die Pflicht zur «Bewirtschaftung», d.h. zur Erstellung und Nachführung des Registers, obliegt neu primär den verantwortlichen Behörden. Die eigentliche «Führung» des Registers obliegt aber, entsprechend Art. 21 Abs. 2 EU-Datenschutzrichtlinie, nach wie vor der Aufsichtsstelle, indem diese das Register über Internet veröffentlicht. Die Aufsichtsstelle wird den verantwortlichen Behörden zur Gewährleistung verlässlicher Informationen über die bestehenden Datensammlungen gewisse Vorgaben im Hinblick auf die Erstellung und Nachführung der einzelnen Teile des Registers zu machen haben, beispielsweise in dem Sinn, dass sie entsprechende EDV-Masken zur Verfügung stellt. Dieses System wird heute beispielsweise im Kanton Zürich angewendet. Soweit sich dies als erforderlich erweisen

sollte, werden Einzelheiten der Registrierung in den Ausführungsbestimmungen nach Art. 38 geregelt werden können.

Die Regelung in Abs. 1 und Abs. 4 gilt jedenfalls für den Kanton und die durch ihn beauftragten Körperschaften, Anstalten und Privaten im Sinn von Art. 2 Abs. 5 Bst. b. Mit Rücksicht auf die (Organisations-)Autonomie der Gemeinden und insbesondere auf die Bedürfnisse kleiner gemeinderechtlicher Körperschaften erlaubt es Abs. 5 Bst. a den Gemeinden und andern gemeinderechtlichen Körperschaften, in ihren organisationsrechtlichen Bestimmungen von Abs. 4 abweichende Regelungen zu treffen und beispielsweise der Aufsichtsstelle nach wie vor die umfassende Verantwortung für das Register zuzuweisen. Regelt eine Gemeinde die Zuständigkeiten nicht abweichend, gilt Abs. 4 auch für sie. Aus den genannten Gründen sollen die Gemeinden nach Abs. 5 Bst. b auch die Möglichkeit haben, von der Veröffentlichung des Registers über Internet abzusehen; vor allem kleinere gemeinderechtliche Körperschaften, die über keine eigene Homepage verfügen, dürften mit einer strikten Regelung im Sinn von Abs. 1 überfordert sein. Anders als Bst. a spricht Bst. b nicht von «regeln», womit ein Verzicht auf die Veröffentlichung im Internet auch durch einfachen Beschluss erfolgen kann.

Die Aufsichtsstelle wird mit der Neuregelung in Abs. 4 entlastet. Es macht unter diesen Umständen kaum mehr Sinn, dass ihr die Datensammlungen gemeldet werden müssen, die nach Abs. 3 nicht registriert werden müssen. Abs. 3 wird entsprechend angepasst.

Artikel 26: Anwendbare Bestimmungen

Art. 26 verweist in der geltenden Fassung einzig auf das VRPG und das Gemeindegesetz vom 16. März 1998 (GG)²³⁾. Anordnungen im Bereich des Datenschutzes stellen zwar in der Regel Verfügungen nach Art. 49 VRPG dar, die im Verwaltungsbeschwerdeverfahren anzufechten sind. Erfolgt die Bearbeitung der Daten im Rahmen eines abgeschlossenen Verfahrens der Zivil- oder Strafrechtspflege oder im Rahmen von Art. 49 Abs. 2 PolG durch die Polizei, wird ein Beschluss im Sinn von Art. 134 Abs. 3 ZPO oder Art. 83 Abs. 2 oder Art. 217 Abs. 4 StrV erlassen, der – entsprechend dem Grundsatz, dass sich die (datenschutzrechtliche) Rechtswegzuständigkeit nach derjenigen der «Hauptsache» (Zivil- oder Strafrecht) richtet – nach dem anwendbaren Verfahrensrecht (ZPO, StrV) anzufechten ist. Art. 26 wird in diesem Sinn präzisiert.

Artikel 27: Beschwerden gegen die Aufsichtsstelle

Das geltende Gesetz erwähnt eine förmliche Verfügungsbefugnis der Aufsichtsstelle einzig in Art. 27, wobei die Aufsichtsstelle aber «praktisch ausschliesslich im Zusammenhang mit Registrierungen verfügungsberechtigt» wäre (Vortrag der Justizdirektion an den Regierungsrat zuhänden des Grossen Rates des Kantons Bern vom 26. Juni 1985 betreffend das Datenschutzgesetz, Bemerkungen zu Art. 27). Tatsächlich ist Art. 27 allerdings toter Buchstabe geblieben; soweit ersichtlich haben die

²³⁾ BSG 170.11

Aufsichtsstellen von dieser Befugnis überhaupt nie Gebrauch gemacht. Angesichts der in Art. 18 neu geregelten Verantwortung für das Datenschutzregister und der besonderen Einwirkungsbefugnisse der Aufsichtsstelle nach Art. 35 ist es angezeigt, diese praktisch bedeutungslose Bestimmung ersatzlos zu streichen. Im Zusammenhang mit den Einwirkungsbefugnissen wird bewusst auf eine förmliche Verfügungsbefugnis der Aufsichtsstelle verzichtet (vgl. vorne Ziff. 2.4.3); die Beibehaltung von Art. 27 wäre deshalb auch systemwidrig.

Artikel 31: Gebühren für Einsichtnahme und Auskunft

Der durch die europarechtlichen Vorgaben verlangte Grundsatz der Kostenlosigkeit der Einsichtnahme und von Auskünften gilt heute wohl in der Praxis, ist aber im geltenden Recht nicht ausdrücklich festgehalten. Art. 31 ist deshalb, entsprechend der tatsächlich gehandhabten Praxis, anzupassen. Das Entgelt für die Einsicht und Auskünfte stellt rechtlich eine (Verwaltungs-)Gebühr dar, weshalb in Art. 31, wie bereits heute, von Gebühren die Rede ist. Der Grundsatz der Gebührenfreiheit gilt nach Abs. 1 für die Einsichtnahme und für Auskünfte nach Art. 20 und 21. Im Fall von Rechtsmittelverfahren ist nicht ausgeschlossen, dass einer unterliegenden Partei Verfahrenskosten nach Massgabe des VRPG auferlegt werden. Gebühren können aber auf jeden Fall nur erhoben werden, soweit die dafür erforderlichen Rechtsgrundlagen bestehen.

Abs. 2 ermächtigt den Regierungsrat, für den Kanton Ausnahmen vom Grundsatz der Gebührenfreiheit vorzusehen. Bereits heute werden die Gebühren auf Verordnungsstufe, nämlich in der Verordnung vom 22. Februar 1995 über die Gebühren der Kantonsverwaltung (Gebührenverordnung; GebV)²⁴⁾, geregelt. Art. 31 GebV sieht vor, dass die Einsichtnahme in das Register der Datensammlungen gebührenfrei ist. Nach Art. 32 GebV sind Auskünfte und Dateneinsicht gemäss Art. 21 KDSG grundsätzlich gebührenfrei. Ausnahmsweise kann eine Gebühr verlangt werden, wenn die ersuchende Person in den vorangehenden zwölf Monaten die gewünschte Auskunft bereits erhalten hat und kein schutzwürdiges Interesse an einer erneuten Auskunftserteilung nachgewiesen werden kann oder wenn die Auskunftserteilung mit einem besonders grossen Arbeitsaufwand verbunden ist. Die GebV entspricht somit der neuen Regelung im Datenschutzgesetz und wird deshalb nicht angepasst werden müssen.

Der Grundsatz der Gebührenfreiheit gilt sowohl für den Kanton als auch für die Gemeinden. Der Regierungsrat regelt die Ausnahmen nach Abs. 2 nur für den Kanton. Für die Gemeinden und anderen gemeinderechtlichen Körperschaften sieht Abs. 3 mit Rücksicht auf die Gemeindeautonomie lediglich in allgemeiner Weise die Möglichkeit von Ausnahmeregelungen vor. Soweit bestehende kommunale Regelungen dem Grundsatz der Gebührenfreiheit gemäss Abs. 1 widersprechen, werden sie angepasst werden müssen.

Artikel 32: Kantonale Aufsichtsstelle für Datenschutz

Art. 32 Abs. 1 sieht neu vor, dass die oder der kantonale Datenschutzbeauftragte auf Antrag des Regierungsrats durch den Grossen Rat gewählt wird (zur Begründung dieser Regelung vorne Ziff. 2.3.3 a). Angesichts der erweiterten Aufgaben und Befugnisse (vgl. Art. 34 und 35) dürfte eine nebenamtliche Tätigkeit dieser Person kaum mehr in Betracht fallen. Diese Möglichkeit wird deshalb nicht mehr explizit erwähnt, ist aber damit auch nicht prinzipiell ausgeschlossen. Hingegen wird neu bereits in Abs. 1 ausdrücklich präzisiert, dass Gegenstand der Regelung in Art. 32 nur die kantonale Aufsichtsstelle ist.

Die oder der Beauftragte wird nach Abs. 2 neu auf eine Amtsdauer von vier Jahren gewählt (vgl. zur Begründung vorne Ziff. 2.3.3 b). Die rechtliche Stellung dieser Person richtet sich nach den Art. 37 ff. des Personalgesetzes und ist somit vergleichbar mit derjenigen von Mitgliedern richterlicher Behörden oder von Geistlichen. Eine Entlassung während der Amtsdauer kommt nur bei schwer wiegenden Amtspflichtverletzungen in Betracht (vgl. Art. 41 f. PG) und könnte gerichtlich überprüft werden. Die neue personalrechtliche Stellung der oder des Beauftragten erfordert Anpassungen des Personalgesetzes (vgl. hinten Ziff. 3.2).

Die kantonale Aufsichtsstelle wird, wie bisher, administrativ der Justiz-, Gemeinde- und Kirchendirektion zugeordnet. Es handelt sich um eine rein administrative Zuordnung. Die Unabhängigkeit der Aufsichtsstelle in Bezug auf Ressourcen und auf ihre Tätigkeit muss auf jeden Fall gewahrt bleiben (vgl. Ziff. 2.3.3 d). Der Grundsatz der Unabhängigkeit wird aber nicht mehr in Art. 33, sondern neu und ausführlicher im neuen Art. 33a geregelt.

Artikel 33a (neu): Unabhängigkeit der Datenschutzaufsicht

Angesichts ihrer zentralen Bedeutung wird die Unabhängigkeit der Aufsichtsstelle neu in einem besonderen Artikel geregelt. Art. 33a hält, entsprechend den europarechtlichen Vorgaben, zunächst in Abs. 1 den Grundsatz der Unabhängigkeit als solchen fest. «Aufsichtsstelle» im Sinn dieser Bestimmung sind sowohl die kantonale Stelle als auch die Aufsichtsstellen der Gemeinden und anderen gemeinderechtlichen Körperschaften. Satz 2 dieser Bestimmung ist in Anlehnung an die Regelung für die kantonale Finanzkontrolle in Art. 4 Abs. 2 des Gesetzes vom 1. Dezember 1999 über die Finanzkontrolle (Kantonales Finanzkontrollgesetz; KFKG)²⁵⁾ formuliert. Unabhängigkeit der Aufsichtsstelle bedeutet beispielsweise, dass die Stelle das Prüfprogramm selbst und ohne Einflussnahme von Regierung oder Verwaltung bestimmt und dass sie die ihr zustehenden Untersuchungs- und Einwirkungsbefugnisse nach Art. 35 sowie ihre Klage- bzw. Anzeigebefugnis (vorne Ziff. 2.4.4) frei ausüben kann. Sie muss insbesondere auch die Möglichkeit haben, besondere Aufträge der Exekutive oder der Verwaltung abzulehnen, wenn diese die unabhängige Durchführung des Prüfprogramms gefährden würden.

Aufgrund der Vorgaben von Schengen/Dublin muss die Aufsichtsstelle, wie ausgeführt (vorne Ziff. 2.3.3 c), auch über einen eigenen Voranschlag verfügen, auf

²⁴⁾ BSG 154.21

²⁵⁾ BSG 622.1

welchen Regierung und Verwaltung keinen Einfluss nehmen dürfen. Das Budget für die Datenschutzaufsicht wird indes in den gesamten Voranschlag des Kantons integriert werden müssen, was in administrativer Hinsicht durch die Verwaltung erfolgen muss. Abs. 2 verdeutlicht zunächst, dass die Gesetzgebung über die Steuerung von Finanzen und Leistungen grundsätzlich auch für die Aufsichtsstelle gilt. Abs. 3 hält die NEF-Grundsätze der Leistungs- und Kostenorientierung fest und regelt das Verfahren der Erstellung von Aufgaben- und Finanzplan und Voranschlag, sieht aber zusätzlich vor, dass der Regierungsrat den Voranschlag zuhanden des Grossen Rates kommentieren kann. Der Grosse Rat entscheidet schliesslich im Rahmen seiner Budgethoheit, ob er die beantragten Mittel für die Datenschutzaufsicht zur Verfügung stellt. Abs. 4 stellt klar, dass die Aufsichtsstelle selbst über die mit dem Voranschlag bewilligten Mittel verfügt. Diese Mittel können sowohl zur Anstellung von Personal als auch für andere Zwecke, beispielsweise für den «Einkauf» von Leistungen spezialisierter Personen, verwendet werden. Explizit verzichtet wird in diesem Zusammenhang auf das Erfordernis der Leistungsvereinbarung, wie sie beispielsweise in Art. 10 KFKG festgehalten ist. Eine solche Leistungsvereinbarung würde dem Grundsatz der Unabhängigkeit der Datenschutzaufsicht widersprechen.

Der Grundsatz der Unabhängigkeit der Datenschutzaufsicht nach Abs. 1 gilt sowohl für den Kanton als auch für die Gemeinden und anderen gemeinderechtlichen Körperschaften. Demgegenüber sind die Abs. 2 bis 4 spezifisch auf den Kanton zugeschnitten und auf die Gemeinden nicht *tel quel* anwendbar. Dass auch die Aufsichtsstellen der Gemeinden in Bezug auf die Ressourcen unabhängig sein müssen, wird in Abs. 5 in allgemeiner Weise vorgeschrieben. Die Gemeinden selbst werden die Unabhängigkeit ihrer Datenschutzaufsicht durch geeignete Regelungen zu gewährleisten haben. Denkbar ist eine nähere kantonale Regelung auf Verordnungsstufe, beispielsweise in dem Sinn, dass die kommunalen Aufsichtsstellen über die gleichen Ausgabenbefugnisse wie ein Rechnungsprüfungsorgan verfügen, wenn die Gemeinden dies nicht ausdrücklich anders regeln²⁶⁾.

Die Unabhängigkeit der Datenschutzaufsicht darf nicht dazu führen, dass die Aufsichtsstelle ihrerseits zu einer unkontrollierten «vierten Gewalt» oder gar zu einem «Staat im Staat» wird. Diese Gefahr besteht indes nicht. Die kantonale Aufsichtsstelle untersteht einer adäquat ausgestalteten Aufsicht (vgl. hinten Ziff. 3.2, Bemerkungen zu Art. 38 und 41 PG) und muss nach Art. 37 Abs. 1 und 2 auch Rechenschaft über ihre Tätigkeit ablegen. Die Rechenschaftspflicht der kommunalen Stellen richtet sich nach den gemeindeeigenen Regelungen (vgl. Art. 37 Abs. 3). Das administrativ-finanzielle Gebaren der Aufsichtsstellen wird im Rahmen der Rechnungsprüfung überprüft.

²⁶⁾ Vgl. dazu die Regelung in Art. 127 der Gemeindeverordnung von 16. Dezember 1998 (GV; BSG 170.111)

Artikel 34: Aufgaben der Aufsichtsstelle

Art. 34 Abs. 1 listet in konzentrierter Form Aufgaben der Aufsichtsstelle auf. Auch diese Bestimmung gilt sowohl für die kantonale als auch für die kommunale Datenschutzaufsicht. Bst. *a* ist neu gefasst, Bst. *k* stellt eine Erweiterung des bisherigen Bst. *g* dar. Bst. *c*, *d* und *n* sind neu. Bst. *g* und *h* entsprechen dem bisherigen Bst. *e*. Die übrigen Bestimmungen in Bst. *b*, *e*, *f*, *i*, *l* und *m* entsprechen wörtlich der bisherigen Regelung (Bst. *b*, *c*, *d*, *f*, *h* und *l*).

Bst. *a* ist auf Art. 18 Abs. 1 abgestimmt, wonach die Registrierung der Datensammlungen neu geregelt wird. Die Wendung «führt im Sinn von Artikel 18» weist darauf hin, dass in diesem Zusammenhang nicht nur der Aufsichtsstelle, sondern auch den verantwortlichen Behörden Pflichten obliegen (vgl. die diesbezüglichen Bemerkungen zu Art. 18). Bst. *c* verweist auf die in Art. 17a neu geregelten Vorabkontrollen. Bst. *d* hält den an sich bereits geltenden Grundsatz fest, dass Eingaben von Betroffenen als aufsichtsrechtliche Anzeigen im Sinn von Art. 101 VRPG zu behandeln sind. Diese ausdrückliche Regelung ist vor allem im Hinblick auf den neuen Abs. 2 aufgenommen worden. Der neu formulierte Bst. *k* erfasst neu nicht nur Erlasse, sondern auch andere Massnahmen wie beispielsweise Vorkehren zur Sicherstellung der Informatiksicherheit, Umfragen, Aus- und Umgestaltung von Prozessen wie etwa die Ausstellung von elektronischen Zertifikaten etc. Bst. *n* hält schliesslich die Pflicht zur Zusammenarbeit mit andern Aufsichtsstellen und zur Amtshilfe (dazu vorne Ziff. 2.4.5) fest.

Der neue Abs. 2 schreibt vor, dass die Aufsichtsstelle die Betroffenen in den da genannten Fällen auch dann über die erfolgte Überprüfung aufgrund von Eingaben gemäss Abs. 1 Bst. *d* orientiert, wenn diese nicht ausdrücklich eine entsprechende Auskunft verlangen. Die Regelung geht, entsprechend den Vorgaben von Schengen/Dublin (vorne Ziff. 2.4.1), über die allgemeine Regelung in Art. 101 Abs. 2 VRPG hinaus, wonach über die Erledigung einer aufsichtsrechtlichen Anzeige nur auf Verlangen Auskunft gegeben werden muss.

Artikel 35: Arbeitsweise der Aufsichtsstelle und Verfahren

Art. 35 regelt im erweiterten Abs. 3 und in den neuen Abs. 4 und 5 die Einwirkungsbefugnisse der Aufsichtsstelle im Sinn der vorne unter Ziffer 2.4.3 erläuterten Lösung nach der Variante b). Abs. 6 entspricht dem bisherigen Abs. 4.

Abs. 3 entspricht der bisherigen Regelung, mit dem Zusatz, dass die Aufsichtsstelle ihre Empfehlung in Form eines mit einer Begründung versehenen Antrags abgeben muss. Damit kann die Aufsichtsstelle auch ohne förmliche Verfügungsbefugnis (die bisher bestehende Befugnis zum Erlass eigener Verfügungen im Zusammenhang mit Registrierungen wird gestrichen; vgl. Bemerkungen zu Art. 27) im Wesentlichen selbst festlegen, was Gegenstand der allenfalls durch die verantwortliche Behörde zu erlassenden Verfügung (Abs. 4) und einer allfälligen späteren rechtlichen Auseinandersetzung in einem Beschwerdeverfahren nach Abs. 5 sein soll. Diese Regelung verhindert, dass die verantwortlichen Behörden, denen in Bezug auf die Umsetzung der Empfehlung ein gewisses Ermessen zusteht, das datenschutzrechtliche Anliegen verwässern können. Gleichzeitig können Antrag und Begrün-

dung, namentlich für in Verwaltungsverfahren wenig erfahrene Stellen, eine willkommene Hilfe im Hinblick auf eine allenfalls zu erlassende Verfügung sein. Die Aufsichtsstelle wird ihre Empfehlung so begründen müssen, dass die angesprochene Stelle auch ohne einschlägige Erfahrung in der Lage ist, die Frage zu prüfen und gegebenenfalls innert der Frist nach Abs. 4 die (teilweise) Ablehnung von Empfehlungen zu verfügen.

Folgt die Daten bearbeitende Behörde dem begründeten Antrag der Aufsichtsstelle nicht, muss sie nach Abs. 4 einen entsprechenden anfechtbaren Entscheid erlassen. Dieser Entscheid wird in der Regel eine Verfügung im Sinn von Art. 49 VRPG darstellen. Erfolgt die Bearbeitung der Daten indes im Rahmen eines abgeschlossenen Verfahrens der Zivil- oder Strafrechtspflege oder im Rahmen von Art. 49 Abs. 2 PolG durch die Polizei, wird, entsprechend der heutigen Regelung für Gesuche um Akteneinsicht, ein Beschluss im Sinn von Art. 134 Abs. 3 ZPO oder Art. 83 Abs. 3 oder Art. 217 Abs. 4 StrV zu erlassen sein. Eine angemessene gesetzliche Frist für den anfechtbaren Entscheid erscheint angezeigt, weil eine widerstrebende Behörde andernfalls die Möglichkeit hätte, das Verfahren über Gebühr zu verzögern. Abs. 4 sieht die für Verwaltungsverfahren übliche Frist von 30 Tagen vor. Mit dieser Regelung besteht die Gewähr, dass allfällige Differenzen innert nützlicher Frist durch einen verbindlichen Entscheid erledigt werden können.

Abs. 5 ermächtigt die Aufsichtsstelle zur Anfechtung des Entscheids. Das Verfahren richtet sich nach dem anwendbaren Verfahrensrecht (vgl. Art. 26 und Bemerkungen dazu), wobei in allen Fällen die Möglichkeit besteht, dass im Bedarfsfall eine gerichtliche Instanz über allfällige bleibende Differenzen entscheidet. Im Fall der Anwendbarkeit des VRPG bedeutet dies, dass, wie bei einer entsprechenden Beschwerde einer Privatperson, im Verwaltungsbeschwerdeverfahren grundsätzlich auch die Angemessenheit der Verfügung überprüft werden kann (Art. 66 Abs. 1 Bst. c VRPG). Die Beschwerdeinstanz wird sich in diesem Punkt allerdings regelmässig Zurückhaltung auferlegen müssen, im Fall kommunaler Verfügungen namentlich mit Blick auf die Gemeindeautonomie. Zu berücksichtigen ist auch, dass die Aufsichtsstelle nach Abs. 3 nur die «Beseitigung von Verstössen und Mängeln» beantragen und damit zum Gegenstand eines Rechtsmittelverfahrens machen kann. An sich taugliche Massnahmen, die möglicherweise noch etwas optimiert werden könnten, stellen keinen Verstoß oder Mangel im Sinn von Abs. 3 dar. Bloss Vorschläge zur Verbesserung sind, wie der neu formulierte Art. 34 Abs. 1 Bst. g zum Ausdruck bringt, Teil der allgemeinen Beratung der Aufsichtsstelle, die in der Regel nicht zu einer förmlichen Empfehlung im Sinn von Art. 35 Abs. 4 führen wird. In der Praxis wird der Überprüfung der blossen Angemessenheit von Verfügungen nach Abs. 4 damit beschränkte Bedeutung zukommen.

Artikel 37: Rechenschaftspflicht

Neu erwähnt wird in Art. 37 insbesondere die Berichterstattung an den Regierungsrat. Der Grosse Rat und der Regierungsrat werden vom Bericht der Aufsichtsstelle vor allem Kenntnis zu nehmen haben. Massnahmen werden sie nur im Rahmen ihrer Zuständigkeiten, beispielsweise im Hinblick auf eine allfällige Neu-

regelung im Gesetz oder in der Verordnung (Art. 38), treffen können. Eine direkte Einwirkung auf die Tätigkeit der oder des Datenschutzbeauftragten widerspräche dem Gebot der völligen Unabhängigkeit der Datenschutzaufsicht.

Artikel 38: Ausführungsbestimmungen

Art. 38 ermächtigt, wie bereits die heutige Regelung, den Regierungsrat in allgemeiner Weise zum Erlass von Ausführungsbestimmungen. Zu denken ist unter anderem an allfällige Einzelheiten der Registrierung von Datensammlungen (Art. 18) und an nähere Vorschriften über die Vorabkontrolle im Sinn von Art. 17a. Geplant ist, die heute durch regierungsrätlichen Beschluss geregelten Vorgaben für Informatikvorhaben in generell-abstrakter Weise durch Verordnung zu regeln. Der Bereich der Informatiksicherheit ist allerdings einem raschen technischen Wandel unterworfen. Es erscheint deshalb angezeigt, dass der Regierungsrat die Regelung einzelner Materien im Bedarfsfall auch an untergeordnete Stellen delegieren kann. Art. 38 enthält die dafür nach Art. 69 Abs. 3 KV erforderliche gesetzliche Grundlage. Er entspricht inhaltlich der allgemeinen Regelung in Art. 43 des Gesetzes vom 20. Juni 1995 über die Organisation des Regierungsrates und der Verwaltung (Organisationsgesetz, OrG)²⁷⁾. Nach Art. 43 Abs. 2 OrG können die Ämter nicht zum Erlass von Verordnungen im Rechtssinn, sondern lediglich zum Erlass so genannter Verwaltungsverordnungen, d.h. von verwaltungsintern geltenden Anweisungen, ermächtigt werden.

3.2 Weitere Erlasse

Artikel 38 und 41 Personalgesetz

Die oder der kantonale Beauftragte für Datenschutz ist aufgrund der Wahl auf eine feste Amtsdauer (Art. 32 Abs. 2 KDSG) nicht mehr Angestellte oder Angestellter im Sinn von Art. 3 Abs. 2 PG. Sie oder er erfüllt die Aufgaben nach Art. 33a Abs. 1 KDSG selbständig und unabhängig und darf deshalb in personalrechtlicher Hinsicht nicht der Aufsicht einer hierarchisch vorgesetzten Verwaltungsstelle unterstellt werden. Andererseits darf es aus rechtsstaatlichen Gründen keine gänzlich unkontrollierte Stelle geben. Zu regeln sind deshalb, unter Berücksichtigung der erforderlichen Selbständigkeit, die Aufsicht und insbesondere die Zuständigkeit zu einer allfälligen Abberufung.

Die rechtliche Stellung der oder des Beauftragten für Datenschutz lässt sich mit derjenigen der Staatsschreiberin oder des Staatsschreibers und der Ratssekretärin oder des Ratssekretärs des Grossen Rates vergleichen, die als hauptamtliche Behördenmitglieder im Sinn von Art. 3 Abs. 4 PG ebenfalls durch den Grossen Rat auf eine feste Amtsdauer gewählt werden. Die Aufsicht über die Beauftragte oder den Beauftragten wird deshalb in Übereinstimmung mit der für diese Personen geltenden Lösung geregelt. Aufsichtsbehörde ist somit nach Art. 38 Abs. 1 Bst. c PG die Oberaufsichtskommission, welche nach Art. 41 Abs. 4 Bst. c PG gegebenenfalls auch Antrag auf Abberufung stellt. Der Entscheid über die Abberufung liegt in der

²⁷⁾ BSG 152.01

Zuständigkeit des Verwaltungsgerichts (Art. 41 Abs. 1 und 2 PG). Mit dieser Regelung ist dem Erfordernis der Unabhängigkeit der Datenschutzaufsichtsstelle von Regierung und Verwaltung Rechnung getragen.

Artikel 23 Verwaltungsrechtspflegegesetz: Akteneinsicht

Aufgrund der Ausweitung des Geltungsbereichs des Datenschutzgesetzes auf hängige Verwaltungsverfahren in Art. 4 Abs. 2 Bst. c KDSG ist Art. 23 Abs. 3 VRPG entsprechend anzupassen. Die Formulierung «ist *überdies* das Datenschutzgesetz vom 19. Februar 1986 anwendbar» bringt zum Ausdruck, dass auf diese Verfahren selbstverständlich auch das VRPG Anwendung findet, soweit nicht der spezifische Bereich der Datenbearbeitung betroffen ist (vgl. Art. 1 VRPG). Demgegenüber ist der Hinweis auf die bisher in Art. 23 Abs. 3 VRPG erwähnten abgeschlossenen Verfahren gestrichen worden. Das VRPG gilt nur für hängige Verfahren und regelt dementsprechend abgeschlossene Verfahren grundsätzlich nicht, womit auf diese Verfahren auch nach heute geltendem Recht einzig das Datenschutzgesetz Anwendung findet. Auf die bisherige Regelung kann damit im VRPG selbst verzichtet werden. An der materiellen Rechtslage in Bezug auf abgeschlossene Verfahren ändert sich mit dieser Streichung nichts.

Artikel 52 Polizeigesetz: Datenbearbeitungssysteme der Kantonspolizei

Auch wenn für Informatiksysteme der Kantonspolizei künftig die Vorabkontrolle nach Art. 17a KDSG im Vordergrund stehen soll, erscheint es gerechtfertigt, das bestehende Instrument der Betriebsbewilligung in Art. 52 PolG beizubehalten. Damit wird der Regierungsrat in die Gesamtverantwortung für die polizeilichen Datenbearbeitungssysteme eingebunden. Die Verfahren der datenschutzrechtlichen Vorabkontrolle und der Betriebsbewilligung müssen jedoch zur Vermeidung von Doppelspurigkeiten koordiniert werden. Der neue Art. 52 Abs. 6 PolG sieht deshalb vor, dass die Vorabkontrolle der Betriebsbewilligung vorgeschaltet wird.

Artikel 39a Gesundheitsgesetz: Recht auf Einsicht in und Herausgabe von Akten

Das Gesundheitsgesetz (GesG)²⁸⁾ sieht heute in Art. 39a Absatz 2 vor, dass bei der Einsichtnahme in Behandlungsunterlagen für die Anfertigung von Kopien eine kostendeckende Gebühr erhoben werden kann. Diese Möglichkeit wird in Zukunft die Ausnahme bleiben müssen, weshalb auch diese Bestimmung anzupassen ist. Der Verweis auf die «anwendbare Gesetzgebung, insbesondere über den Datenschutz» ist allgemein gehalten, weil sich der Geltungsbereich des GesG auf die Behandlung von Patientinnen und Patienten sowohl in öffentlichen als auch in privaten Institutionen sowie durch privat praktizierende Gesundheitsfachpersonen erstreckt, womit je nachdem sowohl das kantonale Datenschutzrecht als auch die bundesrechtliche Regelung oder eine allfällige weitere gesetzliche Vorschrift zur Anwendung kommen kann.

4. Auswirkungen

4.1 Finanzielle und personelle Auswirkungen

Die finanziellen und personellen Auswirkungen der Revision sind nicht einfach abzuschätzen. Zur Zeit wird die kantonale Aufsichtsstelle für Datenschutz durch einen vollzeitlich angestellten Beauftragten (Lohnklasse 24) geführt. Für Sekretariatsarbeiten kann der Beauftragte für Datenschutz auf das Sekretariat von Rechtsamt und Generalsekretariat der JGK zurückgreifen, dies im Umfang von ca. 20 bis 40 Stellenprozenten. Zusätzlich besteht die Möglichkeit, der Rechtskandidatin oder dem Rechtskandidaten über das Rechtsamt der JGK Aufträge zu erteilen. Für externe Datenschutzprüfungen in seinem Einflussbereich setzt der Regierungsrat jährlich einen Betrag von 130 000 Franken (ein Promille der jährlichen Informatikbetriebskosten) ein.

Auch nach der Revision des Datenschutzgesetzes soll die Beratung kantonaler Stellen in erster Linie durch verwaltungseigene Anlaufstellen, vorab durch die Rechtsdienste der Direktionen, erfolgen. Die oder der Beauftragte für Datenschutz wird nach der Neuregelung aber trotzdem erweiterte Aufgaben und Befugnisse wahrzunehmen haben. Zu zusätzlichem Aufwand werden namentlich die im revidierten Art. 35 KDSG geregelten Untersuchungs- und Einwirkungsbefugnisse führen. Erforderlich wird ebenso eine zusätzliche Unterstützung der Aufsichtsstellen gemeinderechtlicher Körperschaften sein. Die kantonale Aufsichtsstelle wird so ausgestattet werden müssen, dass sie zu den vorgeschriebenen wirksamen Kontrollhandlungen und Interventionen auch in der Lage ist. Sie wird unter anderem die Datenbearbeitung im Rahmen des Polizeiinformationssystems SIS II, das von 28 europäischen Staaten mit insgesamt 450 Millionen Einwohnern betrieben wird, zu begleiten haben, was entsprechendes juristisches und Informatikwissen voraussetzt. Die entsprechenden Mittel werden, wie erwähnt, im Rahmen eines separat ausgewiesenen Voranschlags zu bewilligen sein. Aufgrund der zusätzlichen Anforderungen durch Schengen/Dublin werden damit in Zukunft sicher höhere Aufwendungen anfallen. Nach heutigem Kenntnisstand dürfte mit einem zusätzlichen Bedarf in der Grössenordnung von 80 bis 100 Stellenprozenten für eine wissenschaftliche Mitarbeiterin oder einen wissenschaftlicher Mitarbeiter sowie von 50 Stellenprozenten für das Sekretariat zu rechnen sein, was eine Erhöhung des Personalaufwands in der Grössenordnung von 250 000 Franken zur Folge hätte (zur Finanzierung der für die Übertragung der Datenschutzaufsicht über die Spitäler an den kantonalen Beauftragten erforderlichen Stelle vgl. vorne Ziff. 2.3.4). Für das Veröffentlichen des Registers der Datensammlungen auf Internet werden einmalige Kosten von schätzungsweise 60 000 Franken für das Anschaffen der erforderlichen Informatikmittel anfallen. Die wiederkehrenden Kosten für den Betrieb des Registers werden unter 10 000 Franken jährlich betragen. Bei diesen Kosten handelt es sich genau genommen nicht um zusätzliche Kosten. Das in Kraft stehende Datenschutzgesetz enthält bereits einen Auftrag zur Registerführung. Dieser Auftrag wurde aber bis heute de facto nicht umgesetzt.

²⁸⁾ BSG 811.01

4.2 Auswirkungen auf die Gemeinden

Der vorgeschlagene Verzicht auf eine Kantonalisierung der Datenschutzaufsicht führt dazu, dass die Organisationsautonomie der Gemeinden in dieser Hinsicht nicht berührt wird. Die aufgrund der Assoziierung mit Schengen/Dublin und des Zusatzprotokolls erhöhten Anforderungen an die Unabhängigkeit und Tätigkeit der Datenschutzaufsicht führt aber zu Regelungsbedarf und zu gewissen Mehraufwendungen. In Bezug auf die Umsetzung der rechtlichen Vorgaben sollen die Gemeinden, wie erwähnt, in geeigneter Form (BSIG-Mitteilungen, Anpassung des Muster-Datenschutzreglements) unterstützt werden.

5. Ergebnis des Vernehmlassungsverfahrens

Zur vorliegenden Gesetzesvorlage wurde von Anfang März bis Anfang Juni 2007 eine Vernehmlassung durchgeführt. Insgesamt sind 43 Vernehmlassungseingaben eingegangen. Grundsätzlich wird die Notwendigkeit einer Revision des Datenschutzgesetzes nicht bestritten, und insgesamt ist die Vorlage auf ein positives Echo gestossen. Dementsprechend wurde die Vorlage aufgrund des Vernehmlassungsverfahrens nurmehr geringfügig angepasst.

Für die SP geht die Vorlage in einigen Punkten, namentlich in Bezug auf den Datenschutz in den Gemeinden, zu wenig weit. Die Vorstellungen gehen allerdings über das im Rahmen einer pragmatischen Anpassung an die Vorgaben der EU Notwendige hinaus und sollen deshalb erst im Rahmen einer allfälligen künftigen umfassenden Revision des Datenschutzrechts geprüft werden. Die FDP beurteilt demgegenüber die vorgesehene Finanz- und Budgetierungskompetenz des Datenschutzbeauftragten als zu weitgehend. Der Klarheit halber wird im Vortrag präzisiert, dass die Budgethoheit des Grossen Rates bestehen bleibt und keine Pflicht zur unveränderten Übernahme des Voranschlags und Finanzplans besteht.

Hinsichtlich Art. 14a (Datenaustausch mit dem Ausland) haben verschiedene Vernehmlassungsteilnehmende (FDP, SVP, Jungfreisinnige und Finanzdirektion) die Abweichungen vom Bundesrecht kritisiert. Dieser Einwand ist berechtigt, da insbesondere in diesem Bereich eine bundesrechtskonforme Lösung von Vorteil erscheint. Art. 14a ist somit noch verstärkt in Anlehnung an Art. 6 EDSG formuliert worden. Was Abs. 3 von Art. 14a betrifft (Pflicht zur Information vor Bekanntgabe der Daten ins Ausland), wird an der ursprünglichen Fassung festgehalten, da dies nicht nur im Interesse der betroffenen Person, sondern auch im Interesse der zuständigen Behörde liegt.

Zu Art. 31 stellen einige Vernehmlassungsteilnehmende (FDP, Jungfreisinnige, Gemeinde Ittigen) den Grundsatz der Gebührenfreiheit in Frage. Eine gegenteilige Regelung dürfte im Lichte der EU-Vorgaben vor der Evaluation durch die EU allerdings kaum Bestand haben.

Betreffend Art. 33a (Unabhängigkeit der Aufsichtsstelle) haben verschiedene Vernehmlassungen klarere Vorgaben gewünscht. Die Gemeinden werden über eine BSIG-Meldung umfassend und rechtzeitig über die neuen Anforderungen informiert werden.

Weiter haben die Kommunalverbände und die Stadt Langenthal verlangt, dass die Kognition im Beschwerdeverfahren auf die Rechtmässigkeit kommunaler Entscheide zu beschränken sei (Art. 35 Abs. 5). Hier ist insbesondere zu berücksichtigen, dass die Aufsichtsstelle nur die «Beseitigung von Verstössen und Mängeln» (Abs. 3) zum Gegenstand eines Rechtsmittelverfahrens machen kann. An sich taugliche Massnahmen, die möglicherweise noch etwas optimiert werden könnten, stellen keinen Verstoß oder Mangel im Sinn von Art. 35 Abs. 3 dar. In der Praxis wird der Überprüfung der blossen Angemessenheit von Verfügungen nach Abs. 4 damit lediglich beschränkte Bedeutung zukommen. Der Vortrag ist entsprechend präzisiert worden.

Die vorliegende Vorlage enthält schliesslich eine in der Vernehmlassungsvorlage noch nicht enthaltene Änderung des Personalgesetzes, mit welcher die Aufsicht über die kantonale Beauftragte oder den kantonalen Beauftragten für Datenschutz mit Rücksicht auf die verlangte Unabhängigkeit der Datenschutzaufsicht neu geregelt wird.

6. Antrag

Der Regierungsrat beantragt dem Grossen Rat, den vorliegenden Änderungen zuzustimmen.

Bern, 17. Oktober 2007

Im Namen des Regierungsrates

Der Präsident: *Gasche*

Der Staatsschreiber: *Nuspliger*

Nachtrag zum Vortrag des Regierungsrates vom 17. Oktober 2007 betreffend Änderung des Datenschutzgesetzes

Artikel 85a des Gesetzes über die Steuerung von Finanzen und Leistungen

Da die Datenschutzaufsichtsstelle keine Leistungsvereinbarung mit dem Regierungsrat abschliesst, erfüllt sie nicht sämtliche Voraussetzungen eines NEF-Betriebes und führt demzufolge eine Besondere Rechnung gemäss Artikel 36 Absatz 1 FLG. Wegen des Verbotes der Einflussnahme durch die Regierung ist es jedoch nicht statthaft, dass die Art und Weise der Rechnungsführung der Datenschutzaufsichtsstelle durch Verordnung des Regierungsrates geregelt wird; Artikel 36 Absatz 2 ist demzufolge nicht anwendbar. Analog zur Regelung bei den Gerichtsbehörden (Art. 85) ist deshalb im Gesetz eine Bestimmung aufzunehmen, wonach der Grosse Rat die Regelung der Rechnungsführung in einem Dekret regeln wird.

Bern, 30. Januar 2008

Im Namen des Regierungsrates

Der Präsident: *Gasche*

Der Staatsschreiber: *Nuspliger*