Regierungsrat des Kantons Basel-Stadt

An den Grossen Rat **08.0637.01**

JD/P080637
Basel, 11. Februar 2009

Regierungsratsbeschluss
vom 10. Februar 2009

Ratschlag

betreffend

Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz)

Den Mitgliedern des Grossen Rates des Kantons Basel-Stadt zugestellt am 13. Februar 2008

Inhaltsverzeichnis

Zusammenfassung

Bisher gilt für die Behörden von Kanton und Gemeinden der Geheimhaltungsgrundsatz. Nur ausnahmsweise gibt das Verfassungs- und Gesetzesrecht einen Anspruch auf Zugang zu Informationen. Es liegt weitgehend im Ermessen der Behörden, ob und wie weit sie Informationen über ihre Tätigkeit zugänglich machen. Die Einführung des Öffentlichkeitsprinzips bringt den Wechsel vom traditionellen Geheimhaltungsgrundsatz neu zum Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt.

Die beiden Kantone Basel-Stadt und Basel-Landschaft haben gemeinsam eine gesetzliche Regelung ausgearbeitet. Es würde kaum verstanden werden, wenn auf derart kleinem Raum grundsätzlich unterschiedliche Regelungen für den Zugang zu Informationen gelten würden. Aufgrund der höheren zeitlichen Dringlichkeit in unserem Kanton wird das Geschäft nicht (mehr) als partnerschaftliches Geschäft behandelt.

Weil Datenschutz und Öffentlichkeitsprinzip beide die Fragen von Informationszugang und -nichtzugang behandeln und Personendaten auch Informationen sind, soll ein kombiniertes Informations- und Datenschutzgesetz geschaffen werden, das Information und Informationsbearbeitung in den Mittelpunkt stellt. Das ermöglicht auch die lückenlose Abstimmung der beiden Regelungsbereiche aufeinander.

Das Gesetz regelt den Umgang der öffentlichen Organe mit Informationen im Allgemeinen und – als Unterfall – mit Personendaten im Besonderen; es bezweckt einerseits, das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern sowie letztlich die Kontrolle des staatlichen Handelns zu erleichtern (Öffentlichkeitsprinzip), und anderseits die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten

Das geltende Datenschutzrecht wird weitgehend unverändert übernommen; Anpassungen erfolgten hauptsächlich an die technologische Entwicklung, z.B. mit der Einführung des Prinzips der Datenvermeidung und Datensparsamkeit bei IT-Systemen.

Neu ist der «Informationsteil»: Neben der bisher schon bestehenden Verpflichtung der Behörden zur (pro-)aktiven Informationstätigkeit wird neu jeder Person ein durchsetzbarer Anspruch auf Zugang zu den bei den öffentlichen Organen vorhandenen Informationen eingeräumt. Das Recht auf Zugang zu amtlichen Informationen besteht, ohne dass besondere Interessen geltend gemacht werden müssen. Es muss aber zum Schutz überwiegender öffentlicher oder privater Interessen eingeschränkt, aufgeschoben oder verweigert werden können. Die Gründe, die eine Beschränkung, einen Aufschub oder eine Verweigerung der Zugangsgewährung zu Informationen erlauben, werden im Gesetz exemplarisch aufgezählt. So liegen etwa überwiegende öffentliche Interessen vor, wenn die freie Meinungs- und Willensbildung einer Behörde durch eine vorzeitige Bekanntgabe amtlicher Informationen beeinträchtigt oder wenn durch den Zugang zu amtlichen Informationen die innere oder äussere Sicherheit der Schweiz gefährdet würde. Da transparentes Verwaltungshandeln das Ziel ist und nicht die gläserne Bürgerin oder der gläserne Bürger, wird der Zugang zu Personenda-

ten nur in anonymisierter Form gewährt. Auch weitere überwiegende private Interessen (zum Beispiel Berufs-, Geschäfts- oder Fabrikationsgeheimnisse) führen zur Einschränkung des Zugangs. Spezialgesetzliche Geheimnisse (zum Beispiel das Steuergeheimnis) bleiben weiterhin ausdrücklich vorbehalten.

Das Verfahren auf Zugang zu amtlichen Informationen ist einfach, rasch und grundsätzlich kostenlos. Für besonderen Aufwand (beispielsweise umfangreiche Anonymisierung von Informationen) sowie für die Abgabe von Fotokopien und anderen Datenträgern wird eine Gebühr erhoben. Zieht ein öffentliches Organ in Betracht, den Zugang zu Informationen nicht oder nicht im beantragten Umfang zu gewähren oder ihn entgegen den ablehnenden Stellungnahmen von betroffenen Drittpersonen zu gewähren, können sich die gesuchstellende Person oder die betroffene Drittperson an die Ombudsstelle wenden. Kommt im dortigen Schlichtungsverfahren keine Einigung zustande, wird auf Verlangen eine Verfügung erlassen.

Die Kontroll- und Beratungsfunktion wird der unter dem Namen «Informationszugangs- und Datenschutzbeauftragte(r)» fungierenden Aufsichtsstelle übertragen. So lassen sich wertvolle Synergien nutzen.

In den Kantonen, die das Öffentlichkeitsprinzip bereits eingeführt haben, hat der Vollzug des Öffentlichkeitsgesetzes keine nennenswerte Mehrbelastung mit entsprechenden Mehrkosten zur Folge gehabt. Da in unserem Kanton bereits heute eine offene Informationspolitik und Auskunftstätigkeit betrieben wird, kann davon ausgegangen werden, dass auch hier die Entwicklung ähnlich verlaufen wird. Eine Ausnahme bildet das Schlichtungsverfahren: Mit erfolgreicher Schlichtung können langwierige Rechtsmittelverfahren vermieden werden. Das ist aber nur möglich, wenn die für die Durchführung nötigen Ressourcen bereitgestellt werden.

I. Ausgangslage

Das Öffentlichkeitsprinzip wurde in der neuen Kantonsverfassung vom 23. März 2005 (KV, SG 111.100) verankert. § 75 KV legt fest, dass die Einzelheiten auf Gesetzesstufe zu regeln sind. Auch im Kanton Basel-Landschaft muss infolge eines parlamentarischen Vorstosses ein Informationsgesetz geschaffen werden.

Im Anschluss an die erfolgten Abklärungen und Vorbereitungsarbeiten in den Kantonen beider Basel beschlossen das Justizdepartement BS und die Justiz-, Polizei- und Militärdirektion BL (jetzt: Sicherheitsdirektion BL) zu Beginn des Jahres 2006, den Entwurf für ein gemeinsames Informationsgesetz zu erarbeiten. Im Herbst 2006 wurde in den beiden Kantonen ein Mitberichtsverfahren zu einem ersten Entwurf durchgeführt. Der Gesetzesentwurf wurde grundsätzlich gut aufgenommen; Handlungsbedarf zeigte sich hingegen bei der Abstimmung mit dem Datenschutzgesetz.

Informationszugang und Nichtzugang sind zwei Seiten derselben Medaille. Schon bisher regelt das Datenschutzgesetz sowohl Zugang als auch Nichtzugang zu Personendaten. Das Informationsgesetz wiederum muss ebenfalls Zugang und Nichtzugang regeln, generell für alle Informationen, welche bei den Behörden von Kanton und Gemeinden sowie bei den juristischen Personen des kantonalen und kommunalen öffentlichen Rechts vorhanden sind. Dabei entstehen zwangsläufig Berührungspunkte, weil Personendaten auch Informationen sind. Öffentlichkeitsprinzip und Datenschutz müssen sorgfältig aufeinander abgestimmt sein, damit nicht Doppelspurigkeiten oder Lücken entstehen. Aus diesem Grund werden in letzter Zeit vermehrt Informations- und Datenschutzgesetze geschaffen, welche die beiden Seiten in einem Gesetz integrieren und damit die Abstimmung erleichtern.

Aus diesen Überlegungen beschlossen das Justizdepartement BS und die Justiz-, Polizei- und Militärdirektion BL anfangs 2007, gemeinsam einen neuen Entwurf für eine Kombination von Informations- und Datenschutzgesetz zu erarbeiten und darin den im Mitberichtsverfahren positiv aufgenommenen Entwurf zu einem Informationsgesetz zu integrieren.

Beim Gesetzesentwurf handelt es sich um ein Vorhaben von allgemeiner Tragweite im Sinne von § 53 KV, weshalb ein externes Vernehmlassungsverfahren durchgeführt wurde. Dieses fand in den beiden Kantonen von Mitte Juni bis Mitte September 2008 statt. Einige Anregungen fanden Eingang in die neue Vorlage.

Aufgrund der höheren zeitlichen Dringlichkeit wird das Geschäft nicht (mehr) als partnerschaftliches Geschäft behandelt.

II. Vom traditionellen Geheimhaltungsgrundsatz zum Öffentlichkeitsprinzip

1. Bisher: Geheimhaltungsgrundsatz mit Öffentlichkeitsvorbehalt

Bisher gilt für die kantonale Verwaltung und für die Gemeindeverwaltungen der **Geheimhaltungsgrundsatz**. Zwar ist dies im kantonalen Recht nirgends ausdrücklich festgeschrieben,

ergibt sich aber gemäss bundesgerichtlicher Rechtsprechung[1] aus der gesetzlichen Pflicht der Verwaltungsmitarbeitenden zur Verschwiegenheit über Angelegenheiten, die ihrer Natur nach oder gemäss besonderer Vorschrift geheimzuhalten sind.[2] Die Verletzung dieses so genannten Amtsgeheimnisses ist denn auch unter Strafe gestellt.[3]

Der Geheimhaltungsgrundsatz bedeutet nicht, dass die Behörden passiv bleiben dürfen. § 8 Organisationsgesetz (OG, SG 153.100) verpflichtet die Behörden, die Öffentlichkeit über ihre Tätigkeit zu informieren. Diesen Auftrag zur **aktiven Informationstätigkeit** erfüllen der Regierungsrat, die Departemente und die Dienststellen durch regelmässige Medienmitteilungen, Pressekonferenzen und den Versand von Unterlagen, aber auch und in zunehmendem Mass durch den Auftritt im Internet. Allerdings verfügen die Bürgerinnen oder Bürger über kein generelles Recht, Informationen über die gesamte Verwaltungstätigkeit zu erhalten und sich so ein eigenes Bild zu verschaffen. Die in Art. 16 BV und § 11 Abs. 1 lit. l KV verankerte **Informationsfreiheit** garantiert lediglich den Anspruch, sich aus allgemein zugänglichen Quellen zu informieren. Nur in bestimmten Fällen gewährt das Akteneinsichtsrecht als Ausfluss des Rechts auf rechtliches Gehör bestimmten Personen einen Zugang zu amtlichen Dokumenten. Darüber hinaus liegt es aber weitgehend im Ermessen der Behörden, ob sie Informationen oder Dokumente über ihre Tätigkeit zugänglich machen oder nicht.

2. Künftig: Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt

Information wird in unserer modernen Gesellschaft immer wichtiger. Die technologische Entwicklung, insbesondere das Internet, erlaubt es heute, sich auf einfache Art zu fast allen Lebensbereichen Informationen zu beschaffen. Das stellt eine Herausforderung auch für die Gemeinwesen dar: Es reicht zur Förderung des Vertrauens der Bevölkerung in die staatlichen Institutionen nicht mehr aus, allein den Behörden zu überlassen, zu welchem Zeitpunkt über welchen Gegenstand in welcher Art und Weise die Öffentlichkeit über die staatlichen Tätigkeiten informiert wird. Vielmehr soll der Bürgerin oder dem Bürger auch ermöglicht werden, sich selbst Informationen zu beschaffen.

Nun stellen ja – wie erwähnt – Behörden seit Jahren Informationen über das Internet zur Verfügung. Diese neuere Art der aktiven Informationstätigkeit ändert aber eines nicht: Immer noch entscheiden die Behörden darüber, worüber informiert werden soll. Das Öffentlichkeitsprinzip kehrt das bis zu einem gewissen Grad um: Die Bürgerinnen und Bürger, aber auch wirtschaftliche Unternehmen und die Medien erhalten einen durchsetzbaren Anspruch auf Zugang zu Informationen, welche die staatlichen Stellen besitzen. Die Einführung des Öffentlichkeitsprinzips bedeutet so gesehen keine Revolution, sondern eher eine Evolution der bisherigen Informationspolitik, indem diese nochmals erweitert wird.

Mit diesem Anspruch als Kern des Öffentlichkeitsprinzips wird der **Zweck** verfolgt, das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern sowie letztlich die Kontrolle

---

1 BGE 104 Ia 88 bestätigt und präzisiert in BGE 107 Ia 304, siehe auch BGE 113 Ia 309.
2 § 19 Personalgesetz (SG 162.100).
3 Art. 320 Schweizerisches Strafgesetzbuch (StGB, SR 311.0).

des staatlichen Handelns zu erleichtern. Kurz: Die **Transparenz des Verwaltungshandelns** ist angestrebt – wenn auch nicht uneingeschränkt. Es braucht Ausnahmen zum Schutz überwiegender öffentlicher Interessen, um das Funktionieren der Verwaltung sicherzustellen, also etwa den behördlichen Meinungsbildungsprozess zu schützen.

Die transparente Verwaltung, **nicht** aber die **gläserne Bürgerin oder** der **gläserne Bürger** ist das Ziel. Es geht nicht darum, dass über das Öffentlichkeitsprinzip Informationen zugänglich gemacht werden, welche die Bürgerinnen und Bürger kraft gesetzlicher Verpflichtung den Behörden zur Verfügung stellen müssen. Es wäre eine das Vertrauen gefährdende Fehlentwicklung und würde zu Recht den Widerstand der Betroffenen herausfordern. Aus diesem Grund sind Personendaten, zu welchen Zugang gewährt werden soll, zu **anonymisieren**.

3. Zunehmende Verbreitung des Öffentlichkeitsprinzips

Schweden hat das Öffentlichkeitsprinzip bereits vor 240 Jahren (1766) eingeführt, inzwischen sind auch Australien, Belgien, Dänemark, Finnland, Frankreich, Irland, Italien, Kanada, Neuseeland, Norwegen, Südafrika, Ungarn sowie die USA und fast alle ihrer Bundesstaaten diesem Beispiel gefolgt.

Auch in der Schweiz hat das Öffentlichkeitsprinzip in den vergangenen Jahren zunehmende Akzeptanz erfahren. Seit 1. Juli 2006 ist das neue Öffentlichkeitsgesetz des Bundes (BGÖ, SR 152.3) in Kraft. Bereits zuvor hatten die Kantone Bern (1995), Genf (2002), Solothurn, Waadt und Jura (alle 2003) das Öffentlichkeitsprinzip gesetzlich eingeführt. Die Informations- und Datenschutzgesetze der Kantone Aargau, Zürich und Schwyz traten am 1. Juli, am 1. Oktober bzw. am 1. November 2008 in Kraft und in weiteren Kantonen sind Gesetzesvorlagen zur Einführung des Öffentlichkeitsprinzips in Arbeit (Kantone Freiburg, Neuenburg, St. Gallen und Wallis).

III. Verhältnis zwischen Öffentlichkeitsprinzip und Datenschutz

1. Überschneidungen

Wie bereits erwähnt, überschneiden sich Öffentlichkeitsprinzip und Datenschutz mehrfach, da es bei beiden um die Frage des Zugangs oder Nichtzugangs zu Informationen geht. Dem Gesetzgeber der Kantone Solothurn, Zürich, Aargau und Schwyz erschien es daher sinnvoll, das Öffentlichkeitsprinzip und den Datenschutz in einem einzigen Gesetz zu behandeln. Anders macht es der Bund, was aber daher kommt, dass die beiden Gesetze unterschiedliche Geltungsbereiche haben: Das Öffentlichkeitsgesetz gilt nur für Bundesorgane, das Datenschutzgesetz aber daneben auch für private Datenbearbeiterinnen und Datenbearbeiter.

Die Kombination wurde zum Teil derart vorgenommen, dass gleichsam einfach ein Informationsgesetz und ein Datenschutzgesetz zusammen in ein einziges Gesetz gepackt worden

sind. Einen anderen Weg ist der Kanton Zürich gegangen: Er hat das Recht auf Zugang zu Informationen der Verwaltung in seinem Gesetz erstmals in einer Gesamtansicht mit dem Datenschutz geregelt, stellt also die **Information und den Informationsprozess in den Mittelpunkt**. Der vorliegende Entwurf orientiert sich an diesem integrierenden Modell.

2. Gesamtsicht: Information und Informationsprozess im Mittelpunkt

Das bedeutet, dass Regeln für den Umgang der Behörden mit Informationen im Zentrum stehen; der Zugang jeder Person zu diesen Informationen ist dabei ein wichtiges, aber nicht das einzige Element. Die Zugänglichkeit von Informationen ist auch im alltäglichen Betrieb der Verwaltung, bei der Erfüllung der von Verfassung und Gesetz übertragenen Aufgaben immer entscheidender. Ein geordneter Umgang mit Informationen kommt nicht nur den interessierten Personen, wirtschaftlichen Unternehmen und Medien zugute, sondern auch der staatlichen Aufgabenerfüllung generell – nicht zuletzt auch dem Parlament.

Es wäre möglich, den Informationsprozess vollumfänglich – von der Erhebung von Informationen über die Verwendung zur Aufgabenerfüllung bis hin zur Frage der Aufbewahrung für Zwecke des kollektiven Gedächtnisses – zum Gegenstand einer einzigen und einheitlichen Regelung zu machen, also wie im Kanton Aargau auch die **Archivierung** im gleichen Gesetz zu regeln. Da die Archivgesetze der beiden Basler Halbkantone beide eher jüngeren Datums sind und vor allem unterschiedlichen Konzepten folgen, wird auf eine Integration verzichtet und auf die jeweilige Archivgesetzgebung verwiesen. In der Bestimmung zur Änderung bisherigen Rechts werden aber die nötigen Anpassungen vorgeschlagen (§ 53).

3. Anpassung des Datenschutzrechts an die technologische Entwicklung

Gleichzeitig sollen im Datenschutzteil dringend notwendige Anpassungen an die technologische Entwicklung vorgenommen werden. Dieses Anliegen kommt insbesondere bei der Einführung des Prinzips der **Datenvermeidung und Datensparsamkeit** bei IT-Systemen (§ 14), der stärkeren Betonung von **technischen Möglichkeiten zur Wahrung der Persönlichkeitsrechte** (Stichwort «Privacy Enhancing Technologies» wie beispielsweise Anonymisierung und Pseudonymisierung) (§ 14 Abs. 2 und § 17 Abs. 4) sowie der Schaffung einer Grundlage für **Auditierungen und Zertifizierungen** (§ 19) zum Ausdruck.

IV. Entwurf eines Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz)

1. Vorweg: Das Zusammenwirken von formellem und materiellem Datenschutzrecht

In den Vernehmlassungen hat es sich gezeigt, dass eine Vorbemerkung zum Zusammenwirken von formellem und materiellem Datenschutzrecht notwendig ist, damit verständlich ist, welches Datenschutzrecht für welche Datenbearbeiter anwendbar ist.

Als **formelles Datenschutzrecht** erscheinen die Datenschutz*gesetze*. Sie regeln nicht das konkrete Datenbearbeiten (z.B. der Polizei, der Schul-, Sozialhilfe- oder Steuerbehörden), sondern setzen – gleichsam zwischen Verfassung und Gesetz geschoben – die verfassungsrechtlich vorgegebenen rechtsstaatlichen Anforderungen an staatliches Handeln (Gesetzmässigkeit, Verhältnismässigkeit, Handeln nach Treu und Glauben[4]) um, indem sie die Voraussetzungen und Anforderungen für staatliches Datenbearbeiten (gesetzliche Grundlage bzw. ausdrückliche Grundlage in einem Gesetz im formellen Sinn für das Bearbeiten von besonders schützenswerten Personendaten, Verhältnismässigkeit, Treu und Glauben, Richtigkeit und Vollständigkeit) und die Rechte der betroffenen Personen festlegen.

Als **materielles Datenschutzrecht** erscheinen die generell-abstrakten Regelungen, die ein bestimmtes Datenbearbeiten erlauben oder ganz oder teilweise verbieten; sie sind in der Regel als sog. **bereichsspezifisches Datenschutzrecht** in den entsprechenden Sachgesetzen zu finden (also z.B. im Polizeigesetz für polizeiliches Datenbearbeiten, im Bildungsgesetz für die Schule, im Sozialhilfegesetz für die Sozialhilfebehörden, im Steuergesetz für die Steuerbehörden usw.). Es erscheint dort als die Erlaubnis, Verpflichtung oder Verbot, bestimmte Daten oder Datenkategorien zu bearbeiten, sie an bestimmte Empfänger oder Empfängerkategorien bekannt zu geben, als Einschränkungen der Rechte der betroffenen Personen usw.

Die Kompetenz zum Erlass des *formellen Datenschutzrechts* ergibt sich aus der **Organisationsautonomie** von Bund und Kantonen. Soweit es um das Datenbearbeiten durch *Bundesorgane* geht, kommt damit dem **Bund** kraft seiner Organisationsautonomie die Kompetenz zum Erlass formellen Datenschutzrechts zu. Als Bundesorgane gelten auch Private, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind,[5] also beispielsweise die Verbandsausgleichskassen, welche das AHV-Gesetz des Bundes vollziehen, oder die privatrechtlichen Krankenkassen, welche die obligatorische Krankenpflegeversicherung gemäss Krankenversicherungsgesetz des Bundes vollziehen. Der Bund hat diese Kompetenz zum Erlass formellen Datenschutzrechts durch die Schaffung des Bundesdaten-schutzgesetzes, insb. durch die Art. 1-11*a* und 16-25bis DSG, wahrgenommen. Ausserdem ist der Bund gestützt auf Art. 122 BV zuständig für den Erlass des formellen Datenschutzrechts für das Datenbearbeiten durch *Private*, was er durch die Schaffung des Bundesdatenschutzgesetzes, insb. durch die Art. 1-11*a* und 12-15 DSG, wahrgenommen hat. Die **Kantone** haben aufgrund ihrer Organisationsautonomie formelles Datenschutzrecht zu erlassen, soweit es das Bearbeiten von Personendaten durch *kantonale und kommunale öffentliche Organe* sowie durch Private, denen die Erfüllung öffentlicher Aufgaben des Kantons oder der Gemeinden übertragen werden, betrifft.

Die Kompetenz zum Erlass des *materiellen Datenschutzrechts* ist ein Ausfluss der **Aufgabenkompetenz**. Das Gemeinwesen, das die Kompetenz zur Rechtsetzung in einer bestimmten Materie innehat, besitzt auch die Kompetenz, materielles Datenschutzrecht bezüglich dieser Materie zu setzen, also den Datenschutz materiell sicherzustellen beim Vollzug dieses Rechts. Wenn beispielsweise der Bund zuständig ist für die Rechtsetzung auf dem Gebiet der Kranken- und Unfallversicherung (Art. 117 BV), dann darf er auch festlegen, wel-

4 Art. 5 BV (bzw. bei der Einschränkung von Grundrechten: Art. 36 BV); § 5 (bzw. § 13) KV.
5 Art. 3 lit. h DSG-Bund.

che Daten dafür bearbeitet werden dürfen, welche Daten welchen anderen öffentlichen Organen oder Privaten bekannt gegeben werden dürfen oder müssen, von welchen anderen öffentlichen Organen oder Privaten die mit dem Vollzug betrauten Stellen welche Daten erhalten dürfen usw. Diese Vorschriften gelten dann unabhängig davon, ob Bundesorgane oder kantonale (oder kommunale) öffentliche Organe dieses Bundesrecht vollziehen, also auch für das materielle Datenbearbeiten durch kantonale Organe, z.B. die öffentlichrechtlichen Spitäler als Organe, welche den mit dem Vollzug betrauten Stellen Daten bekannt geben müssen. Wo der Bund keine Rechtsetzungskompetenz besitzt, sind die Kantone zuständig zum Erlass des materiellen Datenschutzrechts.

Daraus folgt: Erstens unterstehen die öffentlichrechtlichen Körperschaften und Anstalten des Kantons und der Gemeinden dem *kantonalen Datenschutzgesetz* (mit den Ausnahmen des § 2 Abs. 2), und zwar unabhängig davon, ob sie kommunales, kantonales oder Bundesrecht vollziehen. Zweitens gilt das *materielle Datenschutzrecht* (die rechtlichen Grundlagen für das konkrete Datenbearbeiten in einem Sachgesetz, für den Bereich der obligatorischen Krankenpflegeversicherung z.B. im Krankenversicherungsgesetz des Bundes [KVG]) für alle, die in den Geltungsbereich dieses Gesetzes fallen, und zwar unabhängig davon, ob sie Private (Privatspitäler), Bundesorgane (im Krankenpflegebereich etwa [früher noch] das Militärspital Novaggio), kantonale Organe (die Universitäts-, Kantons- und Bezirksspitäler) oder kommunale Organe (Gemeindespitäler) sind. Dass damit, wenn es um den Vollzug von Bundesrecht geht, unterschiedliche Datenschutz*gesetze* zur Anwendung gelangen – das Bundesdatenschutzgesetz, soweit Bundesorgane oder Private den Vollzug besorgen, das jeweilige kantonale Datenschutzgesetz, soweit kantonale (und kommunale) öffentliche Organe mit dem Vollzug betraut sind – ist nicht problematisch, weil die entscheidenden Regeln für das konkrete Datenbearbeiten gar nicht in den Datenschutzgesetzen, sondern im *materiellen* Datenschutzrecht (also beispielsweise eben im KVG des Bundes) enthalten sind und für alle Datenbearbeiter gleichermassen gelten – auch beispielweise im Hinblick auf die Einführung von Fallkostenpauschalen (DRG).

2. Gliederung des Gesetzesentwurfs

Das Gesetz ist wie folgt gegliedert:

- Es beginnt im Abschnitt I. mit den **allgemeinen Bestimmungen** zum Regelungsgegenstand und zum Geltungsbereich, gefolgt von den nötigen Begriffsdefinitionen.

- Die beiden folgenden Abschnitte II. und III. legen die Grundsätze **für den Umgang mit Informationen** fest: Der zweite Abschnitt enthält die allgemeinen Grundsätze für den Umgang mit **Informationen** generell. Der dritte Abschnitt beinhaltet die besonderen Grundsätze für den Umgang mit **Personendaten**.

- Es folgen im Abschnitt IV. die Regeln für die **Bekanntgabe von Informationen im Zusammenhang mit der behördlichen Aufgabenerfüllung**, einerseits für die (pro-)

aktive Informationstätigkeit von Amtes wegen, dann aber vor allem auch für die **Bekanntgabe von Personendaten**.

- Der Abschnitt V. fasst die **Rechtsansprüche** zusammen. Es beginnt zuallererst mit dem **Informationszugangsrecht**, also dem Recht **jeder Person** auf Zugang zu Informationen. Anschliessend folgen die Rechtsansprüche der **betroffenen Personen**.

- Der Abschnitt VI. enthält gemeinsame Bestimmungen für die Bekanntgabe von und den Zugang zu Informationen, nämlich die Vorschriften über die **Einschränkungen** im Einzelfall.

- Im Abschnitt VII. erfolgt die Regelung des **Verfahrens auf Zugang zu Informationen**.

- Es folgen im Abschnitt VIII. die Bestimmungen zu der oder dem **Informationszugangs- und Datenschutzbeauftragten**, von der Wahl und Stellung über die Aufgaben, Kontroll- und Einwirkungsbefugnisse bis hin zur Schweigepflicht.

- Der Abschnitt IX. behebt eine Schwäche des bisherigen Datenschutzgesetzes und führt eine **Strafbestimmung** ein für vertragswidriges Bearbeiten von Personendaten durch externe Auftragnehmerinnen und –nehmer (Outsourcing) bzw. Empfängerinnen und Empfänger von Personendaten zum Bearbeiten zu nicht personenbezogenen Zwecken (Wissenschaft und Forschung).

- In den Abschnitten X. und XI. sind schliesslich die erforderlichen **Aufhebungen/Änderungen bisherigen Rechts** sowie die **Schlussbestimmungen** enthalten.

3. Eckpunkte des Gesetzesentwurfs

Das Gesetz regelt den Umgang der öffentlichen Organe mit Informationen im Allgemeinen und mit Personendaten im Besonderen; es bezweckt einerseits, das Handeln der öffentlichen Organe transparent zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern sowie letztlich die Kontrolle des staatlichen Handelns zu erleichtern (Öffentlichkeitsprinzip), und anderseits die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten (§ 1).

Der Geltungsbereich entspricht weitgehend demjenigen des bisher geltenden Datenschutzgesetzes: Das Informations- und Datenschutzgesetz gilt für alle öffentlichen Organe des Kantons und der Gemeinden, für die Körperschaften und Anstalten des kantonalen und kommunalen öffentlichen Rechts sowie für Private, die mit öffentlichern Aufgaben des Kantons oder der Gemeinden betraut sind (§ 2). Das Gesetz verwendet wie bisher den Begriff des «öffentlichen Organs» und knüpft damit an einem funktionalen, d.h. aufgabenbezogenen Behördenbegriff an. Der klassische Behördenbegriff, wie er in der Verfassung verwendet wird, knüpft an der Organisation an und ist damit zwar nicht in allen, aber doch in vielen Fällen ungeeignet.

Das Gesetz spricht von «Informationen» und meint damit alle Aufzeichnungen, welche die Erfüllung einer öffentlichen Aufgabe betreffen, unabhängig von ihrer Darstellungsform und ihrem Informationsträger (§ 3). Es verwendet nicht den Begriff «amtliche Akten» oder «amtliche Dokumente», weil es nicht um die Datenträger, sondern letztlich um den Informationsgehalt geht. Es verwendet nicht den Begriff «amtliche Informationen», weil es selbstredend nur um Informationen geht, über die ein öffentliches Organ verfügt. Personendaten sind eine Unterkategorie von Informationen, besondere Personendaten eine Unterkategorie der Personendaten.

Das Gesetz stellt die Information und den Informationsprozess in den Mittelpunkt. Es schreibt deshalb generell für den Umgang mit Informationen den öffentlichen Organen vor, die Prozesse so zu gestalten, dass das Organ rasch, umfassend und sachlich informieren kann (§ 4). Für die Verwaltung von Informationen wird auf das Archivgesetz verwiesen, wo bereits – damit verwandt – die Grundlage für ein Dokumentenmanagement gelegt ist (§ 5). Wie bisher im Datenschutzgesetz ist dasjenige öffentliche Organ für den Umgang mit Informationen verantwortlich, das die Informationen zur Erfüllung seiner gesetzlichen Aufgabe bearbeitet (§ 6). Gleichzeitig wird – was bisher nur im Datenschutzgesetz, also nur für Personendaten, gegeben war – eine Grundlage für das Bearbeiten im Auftrag (Outsourcing, § 7) und für die Informationssicherheit (§ 8) geschaffen.

Für das Bearbeiten von Personendaten übernimmt das Gesetz weitgehend die bisher im Datenschutzgesetz enthaltenen Voraussetzungen (Gesetzmässigkeit, Treu und Glauben und Verhältnismässigkeit, Richtigkeit und Zweckbindung, Erkennbarkeit der Beschaffung, Vernichtung, §§ 9 bis 12 und §§ 15 und 16), sowie die mit der Revision des Datenschutzgesetzes aufgrund der Assoziierung der Schweiz an Schengen/Dublin[6] eingeführte Vorabkontrolle (§ 13). Neu werden zwei weitere Gegenstände geregelt: das Prinzip der Datenvermeidung und Datensparsamkeit bei IT-Systemen (§ 14) und die Grundlage für die Einführung marktwirtschaftlicher Instrumente zur Qualitätssicherung (Zertifizierungen) (§ 19).

Das baselstädtische Gesetz übernimmt ausserdem (im Unterschied zum Baselbieter Gesetz) die bisher in § 6a DSG geregelten besonderen Voraussetzungen für die Videoüberwachung, modifiziert sie aber (§§ 17 und 18).

In Bezug auf die Bekanntgabe von Informationen im Zusammenhang mit der Aufgabenerfüllung – in Abgrenzung zur Gewährung des Zugangs zu Informationen aufgrund des individuellen Informationszugangsrechts – legt das Gesetz die Grundlage für die (pro-)aktive Informationstätigkeit der Behörden (§ 20). Damit erhalten Medienorientierungen, Publikationen wie der Staatskalender und – heute immer wichtiger – der Webauftritt von Kanton und Gemeinden ihre gesetzliche Grundlage. Für die Bekanntgabe von Personendaten und besonderen Personendaten werden die bisher im Datenschutzgesetz enthaltenen Grundsätze übernommen (§ 21). Ausserdem werden hier die Bestimmungen für die Bekanntgabe von Personendaten zum nicht personenbezogenen Bearbeiten (wie Statistik, Planung, Wissenschaft und Forschung) und die mit der Schengen/Dublin-Revision eingeführte Bestimmung zur grenzüberschreitenden Bekanntgabe von Personendaten aufgenommen (§§ 22 und 23).

---

[6] Nachfolgend: Schengen/Dublin-Revision (vgl. Grossratsbeschluss Nr. 08/16/16G vom 16. April 2008).

Schliesslich wird das bisherige zentrale Verzeichnis der Datensammlungen durch dezentrale Verzeichnisse der Informationsbestände, die Personendaten enthalten, abgelöst (§ 24).

Im fünften Abschnitt werden die Rechtsansprüche Privater zusammengefasst. Das Gesetz beginnt mit dem neu jeder Person zustehenden voraussetzungslosen Recht auf Zugang zu Informationen (§ 25). Selbstverständlich hat die betroffene Person – wie schon bisher nach dem Datenschutzgesetz – das Recht auf Zugang zu den eigenen Personendaten, also zu den bei einem öffentlichen Organ über sie vorhandenen Informationen (§ 26). Ebenso stehen ihr wie bisher weitere Rechtsansprüche zu: das Recht auf Zugang zu den eigenen Personendaten, auf Berichtigung unrichtiger Personendaten, Unterlassungs-, Beseitigungs- und Feststellungsansprüche sowie das Recht auf Sperrung (§§ 27 und 28).

Der Zugang zu Informationen ist nicht schrankenlos: Verlangt eine Person Zugang zu Informationen, so muss das öffentliche Organ den Zugang ganz oder teilweise verweigern oder aufschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht besteht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht (§ 29). Das Gesetz umschreibt nicht abschliessend die in Frage kommenden öffentlichen und privaten Interessen, die gegenüber den Interessen an der Bekanntgabe von oder am Zugang zu Informationen überwiesen können (§ 29 Abs. 2 und 3). Personendaten, zu denen Zugang gewährt werden soll, sind vorgängig zu anonymisieren (§ 30).

Das Verfahren auf Zugang zu Informationen beginnt mit einem Gesuch der ihr Recht auf Zugang geltend machenden Person (§ 31). Das öffentliche Organ prüft das Gesuch. Es tritt nicht darauf ein, wenn sich ein Gesuch ausschliesslich auf bereits öffentlich zugängliche Informationen bezieht; soweit Drittinteressen im Spiel sind, holt das öffentliche Organ in der Regel die Stellungnahmen der betroffenen Personen oder öffentlichen Organe ein (§ 32). Anschliessend gewährt es der gesuchstellenden Person entweder den Zugang oder teilt ihr mit, dass es das Gesuch abzulehnen gedenkt; gegebenenfalls teilt es den Drittinteressen geltend machenden Personen oder Organen mit, dass es den Zugang entgegen ihren Stellungnahmen zu gewähren gedenkt. Die gesuchstellende Person oder die Drittperson können anschliessend innert 30 Tagen den Erlass einer anfechtbaren Verfügung oder die Durchführung eines Schlichtungsverfahrens durch die Ombudsstelle verlangen (§ 33). Das Schlichtungsverfahren wird nur durchgeführt, wenn keine der beteiligten Parteien den Erlass einer Verfügung verlangt hat (§ 34). Der Zugang zu Informationen erfolgt durch Aushändigung, Einsichtgewährung oder mündliche Mitteilung (§ 35). Eine Frist von 30 Tagen bis zur Gewährung des Zugangs oder der Mitteilung im Sinne von § 33 Abs. 2 verhindert zu lange Verzögerungen; in begründeten Fällen ist eine Überschreitung der Frist zulässig (§ 36). Das Verfahren ist in der Regel kostenlos; Ausnahmen sind vorgesehen bei aufwändigen Verfahren, für die Erstellung von Kopien und generell bei Informationen, die zur gewerblichen Nutzung geeignet sind, in keinem Fall jedoch, wenn es sich um den Zugang zu den eigenen Personendaten handelt (§ 37).

Im Anschluss an die Verfahrensregelungen folgen die Bestimmungen zu der oder dem Informationszugangs- und Datenschutzbeauftragten (§§ 38 bis 51). Sie übernehmen die mit der Schengen/Dublin-Revision beschlossenen Regelungen, gliedern sie aber neu. Die Wahl erfolgt durch den Grossen Rat (§ 40 Abs. 2).

Weil bis anhin die Sanktionsmöglichkeiten bei einer Datenschutzverletzung in Outsourcing-Verträgen und bei der Bekanntgabe von Personendaten zur Bearbeitung zu nicht personenbezogenen Zwecken zu schwach waren, sieht das Gesetz neu die Möglichkeit vor, vertragswidriges Bearbeiten von Persondaten mit einer Busse zu sanktionieren (§ 52).

Die beiden letzten Abschnitte X. und XI. enthalten die notwendigen Änderungen anderer Gesetze (§ 53), die Aufhebung des bisherigen Datenschutzgesetzes (§ 54), setzen eine Übergangsfrist (§ 55) und regeln das Inkrafttreten des neuen Gesetzes (§ 56).

4. Ergebnis des Vernehmlassungsverfahrens

Der Entwurf für ein Informations- und Datenschutzgesetz wurde von Mitte Juni bis Mitte September 2008 in die Vernehmlassung gegeben. Zur Vernehmlassung waren insbesondere die Parteien, Verbände, Departemente, Gerichte und Gemeindebehörden eingeladen.

18 Stellungnahmen sind eingegangen. Alle Teilnehmerinnen und Teilnehmer an der Vernehmlassung haben grundsätzlich den Gesetzesentwurf begrüsst. Auf einhellige Zustimmung stiess die Verbindung des Öffentlichkeitsprinzips mit dem Datenschutz. Hingegen haben SP, BastA! und DJS das partnerschaftliche Vorgehen mit dem Kanton Basel-Landschaft und die Zusammenlegung der beiden Datenschutzaufsichtsstellen für unnötig erachtet, während CVP und JFBS das Streben nach gemeinsamen institutionellen Regelungen befürwortet haben. Die CVP hätte sogar den Einbezug weiterer Kantone begrüsst.

Die zu den einzelnen Bestimmungen gemachten Bemerkungen werden im Detail in den Erläuterungen zu den einzelnen Bestimmungen (unten IV.5.) vorgestellt. Hier soll nur auf die wichtigsten Vorbringen hingewiesen werden:

- Die Gerichte haben die Befürchtung geäussert, dass der Zugang zu heiklen Personendaten aus Gerichtsakten gewährt werden muss, wenn das Öffentlichkeitsprinzip die rechtskräftig abgeschlossenen Gerichtsverfahren (§ 2 Abs. 2 lit. b und c) erfasst (siehe dazu nun die Erläuterungen zu § 29 Abs. 3).

- SP, BastA! und DJS haben die Befürchtung geäussert, dass der in der Vernehmlassungsvorlage noch enthaltene § 2 Abs. 2 lit. d (Ausnahme vom Geltungsbereich für persönliche Aufzeichnungen, die als persönliche Arbeitsmittel dienen) zu einer «doppelten Buchhaltung» führe, weil dann Verwaltungsangestellte beginnen könnten, «persönliche Dossiers» zu führen (siehe dazu nun die Erläuterungen zu § 2 Abs. 2).

- SP, BastA!, DJS und die Bürgergemeinde der Stadt Basel stören sich an der Verwendung des Begriffs der «Rassenzugehörigkeit» (§ 3 Abs. 4 lit. a Ziff. 2), weil es keine unterschiedlichen Menschenrassen, sondern nur eine Spezies Mensch gebe (siehe dazu nun die Erläuterungen zu dieser Bestimmung).

- Die Gemeinde Riehen hält den Begriff «Informationsverwaltung» in § 5 für nicht aussagekräftig, da er im Zusammenhang mit öffentlichen Organen eine andere Bedeutung habe; es brauche letztlich ein Dokumentenmanagementsystem (siehe dazu nun die Erläuterungen zu § 5).

- Die SP, die Gemeinde Riehen und das Erziehungsdepartement haben geltend gemacht, der in der Vernehmlassungsvorlage noch enthaltene § 9 Abs. 2 lit. c, wonach besondere Personendaten bearbeitet werden dürfen, wenn die betroffene Person die Daten allgemein zugänglich gemacht und ihre Bearbeitung nicht ausdrücklich untersagt hat, aufzuheben sei, da das öffentliche Organ nur Daten bearbeiten dürfe, die der Erfüllung einer dem öffentlichen Organ zugeordneten Aufgabe dienen (siehe dazu nun die Erläuterungen zu § 9 Abs. 2).

- Das Wirtschafts- und Sozialdepartement hat die Aufnahme einer Statistiknorm angeregt (siehe nun § 10 und § 22 Abs. 3 und die Erläuterungen dazu).

- SP, BastA! und DJS haben beantragt, dass nicht mehr benötigte, als nicht archivwürdig beurteilte Personendaten zu vernichten seien. Die in der Vernehmlassungsvorlage noch vorgesehene Möglichkeit der Anonymisierung sei zu streichen (vgl. nun § 16 und die Erläuterungen dazu).

- Auf divergierende Kritik stiess die Bestimmung über die Videoüberwachung. Am weitesten ging die Forderung von BastA!: Sie verlangte ein gesetzliches Verbot der Videoüberwachung. Die vorgeschlagene Verlängerung der Aufbewahrungsdauer von bisher 24 Stunden auf eine Woche wurde teilweise begrüsst (SP, BastA! für den Fall, dass Videoüberwachung nicht verboten wird, DJS, CVP), teilweise wurde eine Verlängerung auf drei Monate oder 100 Tage (Gerichte) verlangt. Die Streichung der Autorisierung durch die oder den Informationszugangs- und Datenschutzbeauftragten im Interesse der Klärung der Verantwortlichkeiten wurde ebenfalls teilweise begrüsst (SP, BastA!), aber es wurde auch dafür plädiert, an einer Bewilligungspflicht festzuhalten (BastA!); und schliesslich wurde der Einsatz von technischen Datenschutzmassnahmen (SP) verlangt (siehe nun die Neukonzipierung der Videoüberwachungsregelung in §§ 17 und 18 und die Erläuterungen dazu).

- Für die SP geht die Bestimmung über die Qualitätssicherung (Datenschutzzertifizierung) zu wenig weit (siehe die Erläuterungen zu § 19).

- Die Gemeinde Riehen und die Bürgergemeinde der Stadt Basel haben beantragt, dass die Regelung der Informationstätigkeit für die kommunale Verwaltung der Exekutive übertragen werden – analog zur Regelung für die kantonale Verwaltung (siehe nun § 20 Abs. 5 und die Erläuterungen dazu).

- Die SP und die Gemeinde Riehen kritisieren die Übernahme der bisher geltenden Regelung, wonach die Einrichtung von Online-Abrufverfahren durch die Datenschutzaufsichtsstelle autorisiert werden müsse, da dadurch Verantwortlichkeiten verwischt würden; die Gemeinde Riehen macht ausserdem geltend, dass sich ein Widerspruch zur Organisationsautonomie der Gemeinden ergebe, wenn die Gemeinden aufgrund der

hohen Anforderungen an die Unabhängigkeit und Wirksamkeit der Datenschutzaufsicht die Aufsicht an den Kanton zurückdelegieren müssten; dann müsste ein kantonales Organ über die Online-Zugriffe auf kommunaler Ebene entscheiden (siehe nun § 21 Abs. 3 und die Erläuterungen dazu).

- Die SP und die Gemeinde Riehen haben sich für die Einführung der sog. Listenauskunft ausgesprochen. Wie in den meisten Kantonen solle es der Einwohnerkontrolle künftig erlaubt sein, ausschliesslich für ideelle Zwecke Familiennamen, Vornamen, Geburtsdatum und Adresse von Personen, die in der Gemeinde wohnen, bekannt zu geben (siehe nun § 30 Abs. 5 (Variante 1) bzw. Abs. 6 (Variante 2) Aufenthaltsgesetz in der Fassung der Änderung gemäss § 53 Ziff. 1).

- Das Appellationsgericht hat die Aufnahme einer Regelung vorgeschlagen, wonach richterliche Behörden den in einem kantonalen Anwaltsregister eingetragenen Anwältinnen und Anwälten zum Zweck der Berufsausübung Urteile samt Personendaten bekannt geben dürfen, wenn sie die gleichen Garantien abgeben wie Private, denen Personendaten zu nicht einem personenbezogenen Zweck bekannt gegeben werden (siehe nun § 22 Abs. 5 und die Erläuterungen dazu).

- SP, BastA!, DJS und die Bürgergemeinde der Stadt Basel haben die Befürchtung geäussert, dass bei einem dezentralen Verzeichnis der Informationsbestände, die Personendaten enthalten, die Transparenz für die betroffenen Personen leidet (siehe dazu nun die Erläuterungen zu § 24).

- BastA! und die Bürgergemeinde der Stadt Basel haben die Befürchtung geäussert, dass die Regelung, wonach kein Zugangsrecht bestehe zu Aufzeichnungen, die nicht fertig gestellt sind, dazu führen könnte, dass mit der absichtlichen Nichtfertigstellung das Öffentlichkeitsprinzip unterlaufen werden könne, während für das Baudepartement der Ausschluss des Zugangs zu Arbeitsnotizen und Vorentwürfen für ein reibungsloses und effizientes Funktionieren der Verwaltung zentral ist (siehe dazu nun die Erläuterungen zu § 25 Abs. 1).

- Verschiedentlich wurde die Regelung der Einschränkungen bei der Bekanntgabe von und dem Zugang zu Informationen wegen überwiegender öffentlicher oder privater Interessen kritisch kommentiert (SP, BastA!, DJS, Gemeinde Riehen, Gerichte, Baudepartement). Der Schutz der zielkonformen Durchführung staatlicher Massnahmen wurde etwa als vage beurteilt. Die SP schlug vor, anstelle der Interessenabwägung im Anwendungsfall in einer Verordnung konkret die nicht-öffentlichen Akte zu bezeichnen, weil sonst der Ermessensspielraum so gross sei, dass das Öffentlichkeitsprinzip unterlaufen werden könne (siehe dazu nun die erweiterten Erläuterungen zu § 29).

- Die Einrichtung eines Schlichtungsverfahrens wird einheitlich begrüsst. SP, DJS und die Gemeinde Riehen haben aber geltend gemacht, die oder der Informationszugangs- und Datenschutzbeauftragte sei nicht die geeignete Instanz für die Durchführung von Schlichtungsverfahren, weil er/sie vorher allenfalls das öffentliche Organ und die betroffene Person schon beraten und nachher die Anwendung der Bestimmungen über den Umgang mit Informationen durch das öffentliche Organ zu kontrollieren habe.

Damit fehle ihr/ihm die erforderliche Neutralität im Verfahren (siehe nun § 33 Abs. 4 lit. b und § 34 sowie die Erläuterungen dazu). Das Appellationsgericht könnte sich sogar ein obligatorisches Schlichtungsverfahren vorstellen.

- Die Gemeinde Riehen, SP und DJS befürworten die Streichung der Bestimmung, wonach die kantonale Aufsichtsstelle gemeinsam mit anderen Kantonen geführt werden kann, während CVP und JFBS die Benennung eines Informationszugangs- und Datenschutzbeauftragten für mehrere Kantone begrüssen würden (siehe dazu nun die Erläuterungen zu § 38 Abs. 2).

- Die SP verlangt schliesslich die Prüfung der Frage, ob die Zuordnung der/des Informationszugangsbeauftragten zum Grossen Rat richtig sei, d.h. ob Beratung und Kontrolle bezüglich des Informationszugangs *und* des Datenschutzes in einer Stelle, die dem Büro des Grossen Rates zugeordnet ist, zusammengefasst werden soll, oder ob die/der dem Grossen Rat zugeordnete Aufsichtsstelle nur für den Bereich des Datenschutzes zuständig sein soll (siehe dazu nun die Erläuterungen vor § 38).

5. Erläuterungen zu den einzelnen Gesetzesbestimmungen

I. Allgemeine Bestimmungen

§ 1 Gegenstand und Zweck

Abs. 1 umschreibt den **Gegenstand** des Gesetzes: Es regelt den Umgang der öffentlichen Organe mit Informationen. Die Begriffe «öffentliches Organ» und «Information» finden sich als Legaldefinitionen in § 3 Abs. 1 und 2. Das Wort «Umgang» ist bewusst offen gewählt.

Abs. 2 umschreibt den **Gesetzeszweck**. Mit dem Informations- und Datenschutzgesetz (IDG) soll letztlich zusätzliches Vertrauen in die staatlichen Behörden geschaffen werden. Deshalb bezweckt es zweierlei: Erstens das Handeln der öffentlichen Organe noch transparenter als bisher zu gestalten und damit die freie Meinungsbildung und die Wahrnehmung der demokratischen Rechte zu fördern, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen (vgl. § 75 Abs. 2 KV), (lit. a) und zweitens die Grundrechte von Personen zu schützen, über welche die öffentlichen Organe Personendaten bearbeiten (lit. b). Das IDG verbindet damit eine demokratische Funktion (Förderung der freien Meinungsbildung und der Wahrnehmung demokratischer Rechte) mit einer rechtsstaatlichen Funktion (Kontrolle staatlichen Handelns und Schutz der Grundrechte, vor allem der informationellen Selbstbestimmung, aber auch der Entfaltung der Persönlichkeit und wirtschaftlicher Tätigkeiten).

§ 2 Geltungsbereich

Abs. 1: Die Umschreibung des **persönlichen Geltungsbereichs** des Informations- und Datenschutzgesetzes deckt sich erstens – trotz geänderter Formulierung – mit dem Geltungsbereich des Datenschutzgesetzes (DSG, SG 153.260) und entspricht zweitens jenem der meisten kantonalen Informations- oder Öffentlichkeitsgesetze. Der Begriff des öffentlichen Organs wird in § 3 Abs. 1 definiert.

In Abs. 2 werden die **Ausnahmen vom Geltungsbereich** geregelt.

Das Gesetz findet erstens keine Anwendung, wenn ein öffentliches Organ am **wirtschaftlichen Wettbewerb** teilnimmt und dabei privatrechtlich handelt. Der in § 3 Abs. 3 DSG enthaltene Begriff «nicht hoheitlich», wird durch «privatrechtlich» ersetzt, da er in der Praxis immer wieder zu Diskussionen Anlass gab und letzterer viel klarer ist (vgl. auch Art. 23 DSG-Bund, SR 235.1). Mit «privatrechtlich» ist – wie bisher – gemeint als Anbieter in Konkurrenz zu anderen Anbietern, wie z.B. die Basler Kantonalbank zu anderen Banken oder die Gebäudeversicherung ausserhalb des Monopolbereichs, wie bei der Wasserschaden-Zusatzversicherung. Handelt ein öffentliches Organ (z.B. die Kantonalbank) nur privatrechtlich, ist sie immer «Private». Das Bearbeiten von Personendaten durch solche Organe fällt in den Geltungsbereich des Bundesdatenschutzgesetzes (DSG-Bund), und es besteht keine Veranlassung, diesen Organen andere Transparenzpflichten aufzuerlegen als ihren Konkurrenten. Handelt ein öffentliches Organ teils hoheitlich, teils privatrechtlich (z.B. die Gebäudeversicherung öffentlich-rechtlich im Monopolbereich und privatrechtlich bei der Anstellung der Mitarbeitenden und bei Versicherungsprodukten ausserhalb des Monopolbereichs), dann untersteht es für das jeweilige Handeln dem kantonalen Recht bzw. als Private dem Bundesdatenschutzgesetz.

Eine zweite Ausnahme betrifft die **hängigen Verfahren der Zivil- und Strafrechtspflege (lit. b) sowie der Verfassungs- und Verwaltungsgerichtsbarkeit (lit. c)**: Das Informations- und Datenschutzgesetz findet keine Anwendung, sobald und solange das entsprechende Prozessrecht gilt und dieses den Umgang mit Informationen spezifisch für diese Verfahren regelt. Damit wird von der bisherigen Regelung abgewichen. § 4 Abs. 2 DSG (auch nach der Fassung der Schengen/Dublin-Revision) nimmt diese gerichtlichen Verfahren nicht von der Geltung aus, sondern behält bloss die Bestimmungen der entsprechenden Verfahrensordnungen über den Personendatenschutz vor. Dies hat zur Folge, dass – anders als bei den Ausnahmen vom Geltungsbereich – beispielsweise das Datenschutzkontrollorgan auch in diesen hängigen Verfahren zur Aufsicht berufen ist, was unüblich ist. Andere Informationsgesetze sehen vor, dass die Justizbehörden nur soweit dem Informations- und Datenschutzgesetzen unterstehen, als sie Verwaltungsaufgaben erfüllen.[7] Diese Ausnahme ist nicht sachgerecht, denn es entsteht eine problematische Lücke: Die Prozessordnungen gelten nur während der Hängigkeit der Verfahren, das Informations- und Datenschutzgesetz nur im Bereich der Justizverwaltung. Das bedeutet, dass bei einer solchen Lösung die Tätigkeiten ausserhalb der Justizverwaltung vor und nach Hängigkeit der Verfahren nicht geregelt sind. Die Unterstellung unter das IDG heisst aber natürlich nicht, dass deshalb nach dem

[7] § 2 Abs. 1 Informations- und Datenschutzgesetz ZH (LS 170.4), § 2 Abs. 2 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen AG (SAR 150.700).

rechtskräftigen Verfahrensabschluss unbegrenzt Zugang zu den Gerichtsakten zu gewähren wäre (vgl. dazu die Ausführungen zu § 29).

Die in der Vernehmlassungsvorlage noch vorgeschlagene vierte Ausnahme («wenn eine Person Informationen bearbeitet, um ausschliesslich für sich selbst über ein persönliches Arbeitsmittel zu verfügen»), ist im Entwurf nicht mehr enthalten. Die Regelung entstammte § 2 Abs. 2 lit. b des Datenschutzgesetzes BL. Das geltende Basler Datenschutzgesetz kennt die Ausnahme nicht, einzig § 8 Abs. 3 lit. d DSG nimmt persönliche Aufzeichnungen, die als persönliche Arbeitsmittel dienen, von der Registrierpflicht aus. Die Ausnahme wurde wieder gestrichen, nachdem in der Vernehmlassung die Befürchtung geäussert wurde, sie führe zu einer «doppelten Buchhaltung», weil dann Verwaltungsangestellte beginnen könnten, «persönliche Dossiers» zu führen.

Abs. 3: Nach den allgemeinen Kollisionsregeln geht **bereichsspezifisches Datenschutzrecht** des Kantons (z.B. spezifische Geheimhaltungsbestimmungen, Bekanntgabeermächtigungen oder –pflichten in einem Sachgesetz) als lex specialis dem allgemeineren Datenschutzgesetz vor – diejenigen des Bundes aufgrund des Vorrangs des Bundesrechts ohnehin. Entsprechend hält dieser Absatz fest, dass abweichende und ergänzende Bestimmungen in anderen Gesetzen vorbehalten bleiben. Dies gilt z.B. für das Archivgesetz, weshalb § 3 Abs. 4 DSG, wonach die im Staatsarchiv oder in einem Gemeindearchiv archivierten Personendaten vom Geltungsbereich des Datenschutzgesetzes ausgenommen sind, gestrichen werden kann. Abs. 3 stellt allerdings – wie schon § 4 Abs. 1 DSG – eine **qualitative Anforderung** auf: Nicht jede Abweichung ist möglich, nur diejenige, die – angepasst an den bereichsspezifischen Kontext – einen angemessenen Schutz im Sinne des Informations- und Datenschutzgesetzes sicherstellt. Diese Regelung geht zwar weniger weit als § 4 Abs. 1 DSG, welcher vorschreibt: «Besondere Bestimmungen über den Schutz von Personendaten sind anwendbar, soweit sie strengere Voraussetzungen für das Bearbeiten von Personendaten enthalten oder dieses Gesetz näher ausführen». Eine so hohe Hürde ist jedoch in der Kombination von Informationszugangs- und Datenschutz-Regeln schwer umsetzbar. Zudem war bisher fraglich, wie wirksam die Regelung in Wirklichkeit ist, mindestens dann, wenn das abweichende Recht ebenfalls auf Gesetzesstufe steht. Es zeigte sich hier eine Schwäche des Datenschutzrechts, das als Querschnittsrecht auf Gesetzesstufe steht: Es ist für die bereichsspezifischen Regelung der Datenbearbeitungen auf Recht auf Gesetzesstufe angewiesen, wird aber im Kollisionsfall durch eben dieses Recht auch gefährdet.

Abs. 4: Auf Datenbearbeitungen durch **interkantonale Institutionen** sind die kantonalen Datenschutzgesetze nicht unmittelbar anwendbar. Das Beispiel der Liste der pädophilen Lehrkräfte der Bildungsdirektorenkonferenz hat das Problem sichtbar gemacht. Es ist daher wichtig, dass die bisher in § 3 Abs. 2 DSG enthaltene Bestimmung, wonach der Regierungsrat dafür zu sorgen hat, dass interkantonale Institutionen mit baselstädtischer Beteiligung einen gleichwertigen Datenschutz gewährleisten, beibehalten wird. Eine griffigere Lösung, wie sie im Vernehmlassungsverfahren gewünscht wurde, erscheint kaum umsetzbar; mehr als ein Datenschutz, der seiner gesetzlichen Regelung gleichwertig ist, kann ein Kanton ja kaum verlangen.

§ 3 Begriffe

Das Gesetz enthält, soweit es für die Anwendbarkeit notwendig ist, **Legaldefinitionen** der wichtigsten verwendeten Begriffe.

Abs. 1: Der Gesetzesentwurf verwendet, wie bereits vorne unter IV.2. erwähnt, den funktional definierten Begriff des «öffentlichen Organs». **Öffentliche Organe** sind Organisationseinheiten des Kantons und der Gemeinden, die eine öffentliche Aufgabe erfüllen (lit. a), und der juristischen Personen des kantonalen und kommunalen öffentlichen Rechts, die eine öffentliche Aufgabe erfüllen (lit. b), sowie die Privaten, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist (lit. c). Dies entspricht inhaltlich der Definition von § 2 Abs. 5 DSG. Das bedeutet, dass eine kleine Dienststelle des Kantons, die eine einzige Aufgabe erfüllt, auch gleich als gesamtes ein öffentliches Organ darstellt. Eine grössere Dienststelle, welche in verschiedene organisatorische Untereinheiten unterteilt verschiedene Aufgaben erfüllt, bildet mehrere öffentliche Organe. Als öffentliche Organe können nach lit. c auch Private gelten, jedoch nur soweit als sie im Sinne der «Aufgabenübertragung» tätig sind, wie z.B. der Verein Opferhilfe beider Basel oder zum Teil Alters- und Pflegeheime. Nicht gemeint ist «das Bearbeiten im Auftrag des Kantons» (vgl. § 7 und die dort erwähnten Beispiele).

Abs. 2: Einer der Kernbegriffe des Informations- und Datenschutzgesetzes ist der Begriff der «**Information**». Die Information muss aufgezeichnet, also irgendwie verkörpert sein, ohne dass es eine Rolle spielt, in welcher Form und auf welchem Informationsträger dies geschieht. Über die Verwaltungstätigkeit kann keine allgemeine Auskunft verlangt werden, die nicht irgendwie verkörpert ist. Solche Informationen sind zu wenig erhärtet, als dass sie Gegenstand eines gerichtlich durchsetzbaren Rechts sein könnten. Die Aufzeichnung kann in Akten, Schriftstücken, auf Magnetbändern, Disketten, Filmen, Fotos, Tonbändern, in Plänen, Diagrammen, Bildern oder Karten erfolgt sein. Entscheidend ist nur, aber immerhin, dass die Informationen mit der Erfüllung einer öffentlichen Aufgabe zusammenhängen; keine Informationen im Sinne des Gesetzes sind deshalb private Dokumente, welche eine Mitarbeiterin oder ein Mitarbeiter in einem Ordner im Büro stehen hat, oder private E-Mails, die an ihre oder seine Geschäftsadresse gesandt worden sind. Der Begriff Informationen umfasst auch Personendaten und besondere Personendaten; sie sind «Teilmengen» der Informationen im Sinne des Gesetzes. Unerheblich ist es, ob die Informationen vor oder nach dem Inkrafttreten des Gesetzes verfasst oder dem öffentlichen Organ zugestellt worden sind.

Abs. 3: Die Definition der **Personendaten** ist aus § 2 Abs. 1 DSG übernommen. Personendaten sind eine Unterkategorie der Informationen, nämlich all jene, die einen Personenbezug aufweisen.

Abs. 4: Unter dem Begriff der **besonderen Personendaten** werden mit den lit. a und b neu zwei Kategorien zusammengefasst: die sog. besonders schützenswerten Personendaten (§ 2 Abs. 2 DSG) und neu die Persönlichkeitsprofile.

Der bisher verwendete Begriff der «besonders schützenswerten Personendaten» ist eine Wertung, die in der Praxis regelmässig zum Missverständnis führt, die anderen («gewöhnlichen») Personendaten seien nicht schützenswert. Es ist daher vorteilhaft, wie im neuen In-

formations- und Datenschutzgesetz des Kantons Zürich,[8] den Ausdruck «besondere Personendaten» zu verwenden und die Besonderheit, nämlich die besondere Gefahr der Grundrechtsverletzung, auch zu erwähnen, weil die anschliessende Aufzählung wie bisher nicht abschliessend ist. Der Kanton Basel-Landschaft hat seine Terminologie im Rahmen der Schengen/Dublin-Revision bereits angepasst.

Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt, womit die Gefahr der Grundrechtsverletzung besteht wie bei den besonderen Personendaten. Die Eidgenössische Datenschutzkommission hat in einem Entscheid dazu festgehalten: «Der Begriff des Persönlichkeitsprofils kann nicht generell formuliert werden», «[…] Menge und Inhalt der personenbezogenen Daten sind ausschlaggebend. Daten, die über einen längeren Zeitraum zusammengetragen werden und so ein biografisches Bild ergeben (Längsschnitt), sind eher als Persönlichkeitsprofil zu qualifizieren als solche, die eine blosse Momentaufnahme darstellen (Querprofil)»[9]. § 2 DSG enthält keine Legaldefinition der Persönlichkeitsprofile, womit diese bisher anders als die besonders schützenswerten Personendaten behandelt werden. Damit liegt eine für die betroffenen Personen spürbare Lücke im Persönlichkeitsschutz vor: Der erhöhten Gefahr einer Persönlichkeitsverletzung, die dadurch entsteht, dass ein öffentliches Organ über eine Person viele, für sich genommen zwar eher harmlose, in ihrer Gesamtheit aber heikle Daten bearbeitet, wird nicht angemessen Rechnung getragen. Diese Lücke wird nun geschlossen.

Die beiden Kategorien werden materiell immer gleich behandelt; es macht deshalb Sinn, sie unter einem Begriff zusammenzufassen, damit nicht im ganzen Gesetz jeweils umständlich von «besonderen Personendaten und Persönlichkeitsprofilen»[10] gesprochen werden muss, was die Lesbarkeit beeinträchtigen würde. Inhaltlich ergibt sich keine Änderung daraus.

In der Vernehmlassung wurde der Begriff der «Rassenzugehörigkeit» (§ 3 Abs. 4 lit. a Ziff. 2) als störend bezeichnet; es gebe keine unterschiedlichen Menschenrassen, sondern nur eine Spezies Mensch. Unzweifelhaft gibt es keinen wissenschaftlich haltbaren Begriff der «Rasse»; doch wird der Begriff in den Diskriminierungsverboten der Bundesverfassung (Art. 8 Abs. 2 BV) und der Basler Kantonsverfassung (§ 8 Abs. 2 KV) verwendet. Der alternativ vorgeschlagene Begriff «rassistische Zuordnung» ist auf jeden Fall keine Lösung, denn genau dies ist verboten; der Vorschlag «ethnische Zugehörigkeit» ist nicht viel schärfer. Der Regierungsrat schlägt deshalb vor, den Begriff der Rassenzugehörigkeit im Gesetzestext zu belassen (in Übereinstimmung mit § 5 Abs. 1^{bis} lit. b Datenschutzgesetz BL und Art. 3 lit. c DSG-Bund).

Abs. 5 übernimmt für den Begriff des **Bearbeitens** die Definition aus dem § 2 Abs. 3 und § 3 Abs. 1 DSG.

Abs. 6 übernimmt für den Begriff der **Bekanntgabe** die Definition aus dem § 5 Abs. 4 Datenschutzgesetz BL; schon bisher wurde im DSG die Bekanntgabe von Personendaten aus-

8 § 3 Informations- und Datenschutzgesetz ZH (LS 170.4).
9 Urteil vom 27.01.2000, VPB 65.48.
10 Wie z.B. im Bundesdatenschutzgesetz (SR 235.1), vgl. nur etwa Art. 4 Abs. 5, Art. 17 Abs. 2, Art. 17a Abs. 2 lit. c, Art. 18 Abs. 2, Art. 19 Abs. 3.

führlich geregelt (§§ 10-12 DSG), aber ohne dass der Begriff der Bekanntgabe definiert gewesen wäre. Es ist wichtig festzuhalten, dass jedes Zugänglichmachen und nicht nur das (absichtliche) Weitergeben eine Bekanntgabe darstellt.

Nicht mehr ins IDG übernommen zu werden braucht der Begriff der Datensammlung. Neu müssen die öffentlichen Organe ein Verzeichnis der Informationsbestände öffentlich zugänglich machen (§ 24).

II. Allgemeine Grundsätze für den Umgang mit Informationen

Die §§ 4 bis 8 regeln grundsätzlich den **Umgang** der öffentlichen Organe **mit Informationen**. Im folgenden Abschnitt III. ist der Umgang mit Personendaten im Besonderen geregelt.

§ 4 Transparenzprinzip

Im Umgang mit Informationen soll **Transparenz** herrschen. Das öffentliche Organ hat seinen Umgang mit Informationen so zu gestalten, dass es rasch, umfassend und sachlich informieren kann. Diese Gestaltung ist einerseits die Voraussetzung dafür, dass die Informationen zur Aufgabenerfüllung genutzt werden können, anderseits aber auch dafür, dass der Zugang zu Informationen gewährleistet werden kann. Das Transparenzprinzip verdeutlicht den **Systemwechsel** vom «Geheimhaltungsprinzip mit Öffentlichkeitsvorbehalt» neu zum «Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt», und zwar nicht nur gegen aussen (Private, wirtschaftliche Unternehmen, Medien), sondern auch gegen innen.

§ 5 Informationsverwaltung

Transparenz setzt eine geeignete **Informationsverwaltung** voraus. Die Akten sind so anzulegen und zu verwalten, dass die Informationen auffindbar und nachvollziehbar sind (Kategorisierung, Datierung von Informationen, Angaben zur Urheberin oder zum Urheber usw.). Das Gesetz verweist hiefür auf die Regelungen des Archivgesetzes, das die Grundlage für die Regelung der Aktenführung in der Registratur- und Archivierungsverordnung (SG 153.610) stellt.[11] Für grössere Verwaltungseinheiten braucht es letztlich ein Dokumentenmanagementsystem, wodurch der Dossierverlauf für Dritte nachvollziehbar wird. Das öffentliche Organ muss die im Archivierungsrecht enthaltenen Grundsätze in Zusammenarbeit mit dem zuständigen Archiv in Form von Organisationsvorschriften konkretisieren; zu regeln sind dabei die Geschäftsrelevanz von Unterlagen, die Archivrelevanz, Zuständigkeiten, Verantwortungen, Zugriffskonzepte, Ordnungssysteme usw. Es wird jedoch darauf verzichtet, solche Konkretisierungen hier verbindlich festzulegen.

§ 6 Verantwortung

Abs. 1: Wie schon nach § 7 Abs. 1 DSG für das Bearbeiten von Personendaten muss unverändert dasjenige öffentliche Organ die **Verantwortung** für den Umgang mit Informatio-

[11] § 18 Abs. 1 Archivgesetz (SG 153.600).

nen übernehmen, das diese bearbeitet. Die Verantwortung für die Informationsbearbeitung durch beauftragte Dritte ist in § 7 Abs. 2 («Outsourcing-Bestimmung») geregelt.

Abs. 2: Zunehmend werden in der Verwaltung Datenpools geschaffen, indem **mehrere verschiedene Stellen** zu unterschiedlichen Zwecken dieselben Informationen bearbeiten. Soweit dabei Personendaten bearbeitet werden, ist eine gesetzliche Grundlage erforderlich (§ 9). Auf jeden Fall zu klären ist aber die Verantwortung, insbesondere für die Aktenanlage und –verwaltung, die Pflege oder die Bekanntgabe der Informationen oder auch für den Betrieb von elektronischen Informationsbeständen. § 6 Abs. 2, der im Wesentlichen § 7 Abs. 2 DSG entspricht, legt die entsprechende Pflicht fest. Es ist an den öffentlichen Organen oder allenfalls an ihren vorgesetzten Stellen, diese Verantwortung zu regeln. So hat z.B. ein Amt, welches Informationen in einen gemeinsam bearbeiteten Informationsbestand liefert, dafür zu sorgen, dass die Daten rechtmässig erhoben und richtig sind; ein anderes Amt, welches den Datenbestand verwaltet, sorgt für die Gewährleistung der Informationssicherheit, wie den Vollzug der Zugriffsberechtigung. Im Falle der Unmöglichkeit einer Zuordnung der Verantwortung wegen Uneinigkeit zwischen den beiden Amtsstellen, hat die gemeinsame nächsthöhere Stelle (Amtsstellenleitung, Departement, Regierungsrat) darüber zu entscheiden. Hierzu ist keine bestimmte Form erforderlich. Möglich ist eine Lösung im Gesetz, in einer Verordnung, in einem Bearbeitungsreglement zu einem bestimmten Vorhaben oder durch Absprache zwischen den involvierten Amtsstellen. Für die Öffentlichkeit wird die Verteilung der Verantwortung bei den Informationsbeständen, die Personendaten enthalten, transparent über das Verzeichnis der Informationsbestände nach § 24.

§ 7 Bearbeiten im Auftrag

Abs. 1: Bereits heute lässt § 16 Abs. 1 DSG die **Bearbeitung von Personendaten** durch (externe, das heisst dem Gesetz nicht unterstehende) **Dritte** zu; der Datenschutz ist dabei durch Auflagen, Vereinbarung oder auf andere Weise sicherzustellen. Anwendungsbeispiele sind der IT-Support durch ein externes IT-Unternehmen, IT-Audits im Bereich Informatiksicherheit, Revisionen durch private Treuhandgesellschaften, die Spitalseelsorge, die Administration Gesetzessammlung/Kantonsblatt/Staatskalender oder Bevölkerungsumfragen. Es geht also hier um Externe, welche Daten im Auftrag eines öffentlichen Organs **zur Erfüllung der Aufgabe dieses Organs** bearbeiten. Davon klar zu unterscheiden ist das Datenbearbeiten durch Private zur Erfüllung einer ihnen (das heisst: diesen Privaten) übertragenen öffentlichen Aufgabe (z.B. an den Verein Opferhilfe beider Basel); Private, denen die Erfüllung einer öffentlichen Aufgabe übertragen ist, werden gemäss § 3 Abs. 1 lit. c zu einem öffentlichen Organ und unterstehen deshalb dem IDG.

Es ist sinnvoll, diese Regelung für das Bearbeiten durch Dritte generell für den Umgang mit Informationen in dieses Gesetz zu übernehmen. Gleichzeitig sind die Voraussetzungen festzuhalten: Eine Übertragung des Bearbeitens auf eine dritte Person ist – analog zu Art. 10a DSG-Bund – nur zulässig, wenn keine rechtliche Bestimmungen (z.B. ein Berufsgeheimnis) oder vertragliche Vereinbarungen entgegenstehen (lit. a) und sichergestellt wird, dass die Informationen nur so bearbeitet werden, wie es das öffentliche Organ tun dürfte (lit. b).

Abs. 2: Die **Verantwortung** bleibt – wie nach § 7 Abs. 1 DSG – beim öffentlichen Organ, das die Informationen für seine Aufgabenerfüllung bearbeiten lässt. Die Verantwortung beinhaltet insbesondere auch die sorgfältige Auswahl, Instruktion und Kontrolle des oder der beauftragten Dritten. Weil die bisherigen Erfahrungen gezeigt haben, dass es bisweilen schwer fällt, angemessene Konventionalstrafen zu vereinbaren, soll eine strafrechtliche Sanktionierungsmöglichkeit eingeführt werden (vgl. unten zu § 52 Abs. 1). Dies kennt etwa der Kanton Zürich[12] schon lange, kürzlich wurde sie auch im Kanton Aargau[13] eingeführt.

§ 8 Informationssicherheit

Weil **Informationssicherheit**, wie sie bisher im § 17 DSG festgelegt war, nicht nur Personendaten, sondern generell Informationen schützen soll, wird diese Bestimmung mit dem Auftrag, eine Informationssicherheitsverordnung zu erlassen, übernommen (Abs. 1, 3 und 4). Eine solche Verordnung besteht bereits in Bezug auf die Informatik mit der Verordnung zur Informatiksicherheit (ISV) vom 9. April 2002[14]. Sie regelt aber die Aufgaben, Kompetenzen und Verantwortlichkeiten zur Wahrung der Informatiksicherheit nur bei den Informatiksystemen, für welche der Kanton verantwortlich ist; für den kommunalen Bereich hat deshalb der Gemeinderat die entsprechende Regelung zu treffen (Abs. 4).

Neu werden in Abs. 2 auf Wunsch der Informatikkonferenz die Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Nachvollziehbarkeit) aufgenommen.

III. Besondere Grundsätze für den Umgang mit Personendaten

Die §§ 9 bis 19 regeln grundsätzlich den **Umgang** der öffentlichen Organe **mit Personendaten und mit besonderen Personendaten**. Weil Personendaten eine Unterkategorie von Informationen sind, gelten die im Abschnitt II. festgelegten Grundsätze auch für den Umgang mit Personendaten.

§ 9 Voraussetzungen für das Bearbeiten von Personendaten

§ 9 übernimmt die bereits im § 5 DSG für das (personenbezogene) Bearbeiten von Personendaten festgelegten Grundsätze der **Gesetzmässigkeit**, von **Treu und Glauben** und der **Verhältnismässigkeit**. Für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck siehe § 10.

Abs. 1: Die aus dem verfassungsrechtlichen Legalitätsprinzip[15] abgeleitete Voraussetzung der gesetzlichen Grundlage wird hier für Personendaten allgemein statuiert. Diese Regelung entspricht materiell der Bundes-[16] und der bisherigen Regelung (§ 5 Abs. 1 DSG).

---

12 § 26 des per 1. Oktober 2008 ausser Kraft gesetzten kantonalzürcherischen Gesetzes vom 6. Juni 1993 über den Schutz von Personendaten (Datenschutzgesetz ZH); übernommen als § 40 ins neue Informations- und Datenschutzgesetz ZH (LS 170.4).

13 § 41 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen AG (SAR 150.700).

14 SG 153.320.

15 Art. 5 Abs. 1 und Art. 36 Abs. 1 BV (SR 101); § 5 Abs. 1 und 13 Abs. 1 KV (SG 111.100).

16 Art. 17 Abs. 1 im Vergleich zu Art. 17 Abs. 2 DSG-Bund (SR 235.1).

Abs. 2: Auch diese Regelung entspricht weitgehend dem bisherigen § 6 DSG. Es wurden jedoch drei geringfügige Anpassungen vorgenommen.

Zu lit. a: Die Bearbeitung von besonderen Personendaten ist eine schwerwiegende Einschränkung des verfassungsmässigen Rechts auf informationelle Selbstbestimmung. Grundrechtseinschränkungen bedürfen nach Art. 36 Abs. 1 Satz 1 BV und nach § 13 Abs. 1 Satz 1 KV einer gesetzlichen Grundlage, schwerwiegende Einschränkungen müssen nach Art. 36 Abs. 1 Satz 2 BV und nach § 13 Abs. 1 Satz 2 KV im Gesetz selbst vorgesehen sein. Aus der unterschiedlichen Formulierung (gesetzliche Grundlage – im Gesetz selber) ist zu schliessen, dass im zweiten Fall ein Gesetz im formellen Sinn verlangt ist (vgl. Ulrich Häfelin/Walter Haller/Helen Keller, Schweizerisches Bundesstaatsrecht, 6. Auflage, Zürich 2008, Rz. 310). Damit stimmt auch die Regelung in Art. 17 DSG-Bund überein – und § 21 Abs. 2 lit. a des Gesetzesentwurfs. Dies entspricht auch der bisherigen Praxis. Der bisher in § 6 lit. a DSG vorgesehene Grossratsbeschluss ist jedoch nach § 83 KV kein Gefäss mehr für die Rechtsetzung (vgl. auch § 13 Abs. 1 KV). Aus diesem Grund wurde der Grossratsbeschluss als Grundlage für die Bearbeitung von besonderen Personendaten gestrichen.

Zu lit. b: Hier erfolgt lediglich die Klarstellung, dass es sich um eine gesetzliche Aufgabe handeln muss.

Gemäss § 6 lit. c DSG setzt ein Datenbearbeiten entweder die Einwilligung der betroffenen Person oder ein Zugänglichmachen der Daten voraus. Öffentliche Organe müssen die Daten bearbeiten dürfen, welche für die Erfüllung ihrer gesetzlichen Aufgabe erforderlich sind. Das öffentliche Organ hat – umgekehrt – keine Daten zu bearbeiten, die nicht der Erfüllung einer dem öffentlichen Organ zugeordneten Aufgabe dienen. Bereits im Vernehmlassungsentwurf war deshalb festgehalten, dass die im DSG noch erwähnte *Einwilligung* der betroffenen Person zu einer solchen nicht zur Aufgabenerfüllung gehörenden Bearbeitung keine Rechtfertigung abzugeben vermag. Zu Recht wurde in Vernehmlassungen auch geltend gemacht, dass die im Vernehmlassungsentwurf noch vorgesehene Regelung, dass besondere Personendaten auch bearbeitet werden dürfen, wenn die betroffene Person die Daten *allgemein zugänglich gemacht* und ihre Bearbeitung nicht ausdrücklich untersagt hat (lit. c), keine Datenbearbeitung zu rechtfertigen vermag. Deshalb wird keine lit. c mehr vorgeschlagen.

Abs. 3 legt entsprechend dem verfassungsrechtlichen Prinzip[17] fest, dass das Bearbeiten von Personendaten nach Treu und Glauben erfolgen und verhältnismässig sein muss.

§ 10 Voraussetzungen für das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck

Im Vernehmlassungsentwurf war das Bearbeiten von Personendaten zu einem nicht personenbezogenen Zweck, also insbesondere für Statistik, Planung, Wissenschaft und Forschung, als Spezialfall der Zweckbindung in § 11 Abs. 2 vorgesehen. Das Wirtschafts- und Sozialdepartement und das Statistische Amt legen demgegenüber Wert auf eine Regelung in einem eigentlichen «Statistikparagraphen». Eine gesetzliche Regelung ist erforderlich, weil das Bearbeiten von Personendaten durch das Statistische Amt eine Zweckänderung

[17] Art. 5 Abs. 2 BV (SR 101), § 5 Abs. 2 KV (SG 111.100).

darstellt, welche im Sinne von § 12 rechtfertigungsbedürftig ist. Das kann – wie zum Beispiel im Kanton Basel-Landschaft[18] – in Form eines Statistikgesetzes mit spezifischen Datenschutzvorschriften sowie Regelungen über die Datenbeschaffung, über die statische Bearbeitung, über die Datenverbreitung und über ein Statistikgeheimnis geschehen. Die Minimallösung besteht darin, hier eine generelle Ermächtigung für alle öffentlichen Organe – inkl. des Statistischen Amtes – zu statuieren und die Bekanntgabevorschrift (§ 22) durch einen Absatz für das Statistische Amt (Abs. 3) zu ergänzen.

Abs. 1 übernimmt die Regelung des geltenden Datenschutzgesetzes (§ 15 Abs. 1 DSG). Danach darf ein öffentliches Organ Personendaten (inkl. besondere Personendaten), die es i.S.v. § 9 rechtmässig bearbeitet, auch für einen nicht personenbezogenen Zweck, namentlich für Statistik, Planung, Wissenschaft oder Forschung, bearbeiten – mit bestimmten Auflagen: Die für einen nicht personenbezogenen Zweck bearbeiteten Daten dürfen nicht mehr für personenbezogene Zwecke bearbeitet werden (lit. a); diese Daten müssen, sobald es der Bearbeitungszweck zulässt, anonymisiert oder mindestens pseudonymisiert werden (lit. b), und aus den bekanntgegebenen Ergebnissen der Bearbeitung (aus der Statistik, aus den Planungsunterlagen, aus der wissenschaftlichen Arbeit oder aus den Forschungsergebnissen) dürfen keine Rückschlüsse auf die betroffenen Personen mehr möglich sein (lit. c). Wenn die Daten für die konkrete nicht personenbezogene Bearbeitung nicht mit anderen Daten verknüpft werden müssen, muss von allem Anfang an mit anonymisierten Daten gearbeitet werden.

Abs. 2: Das AHV-Gesetz des Bundes[19] legt in Art. 50*e* Abs. 2 fest, dass die Versichertennummer (die neue Sozialversicherungsnummer, die anstelle der alten AHV-Nummer tritt) von folgenden Stellen und Institutionen, die mit dem Vollzug von kantonalem Recht betraut sind, für die Erfüllung ihrer gesetzlichen Aufgaben systematisch verwendet werden darf: mit dem Vollzug der Prämienverbilligung in der Krankenversicherung betraute Stellen (lit. a), mit dem Vollzug der Sozialhilfe betraute Stellen (lit. b), mit dem Vollzug der Steuergesetzgebung betrauten Stellen (lit. c) und die Bildungsinstitutionen (lit. d). Andere Stellen und Institutionen, die mit dem Vollzug von kantonalem Recht betraut sind, dürfen die Versichertennummer zur Erfüllung ihrer Aufgaben systematisch nur verwenden, wenn ein kantonales Gesetz dies vorsieht. Aus diesem Grund legt Abs. 2 fest, dass das Statistische Amt – nicht aber andere öffentliche Organe ausser den oben erwähnten im Bundesgesetz genannten – die Versichertennummer zum Zweck der Verknüpfung von Personendaten (inkl. besonderen Personendaten) verwenden darf.

§ 11 Richtigkeit

§ 11 übernimmt das bereits im § 5 Abs. 4 DSG enthaltene Prinzip der **Richtigkeit** der Personendaten. Personendaten müssen richtig und, soweit es der Bearbeitungszweck erfordert, vollständig sein. Daraus abgeleitet wird – analog der Regelung von Art. 5 Abs. 1 DSG-Bund – die Pflicht, sich über die Richtigkeit der erhobenen Daten zu vergewissern. Die betroffene Person kann die Berichtigung unrichtiger Daten verlangen (§ 27 Abs. 1 lit. a).

---

[18] Kantonales Statistikgesetz vom 21. Februar 2008 (SGS 164).

[19] Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG, SR 831.10).

§ 12 Zweckbindung

§ 12 übernimmt den bereits im § 5 Abs. 3 DSG für das Bearbeiten von Personendaten festgelegten Grundsatz der **Zweckbindung**, eine der Kernbestimmungen des Datenschutzrechts. Der Zweck ergibt sich aus der gesetzlichen Grundlage; er besteht in der Erfüllung der gesetzlichen Aufgabe. Bearbeitungen innerhalb dieses Zweckes sind damit gerechtfertigt. Eine Bearbeitung über diesen Zweck hinaus bedarf einer erneuten Legitimation, entweder durch eine gesetzliche Grundlage oder durch die Einwilligung der betroffenen Person. Die bisherige Formulierung in § 5 Abs. 3 DSG meint, allerdings sprachlich missverständlich, nichts anderes.

Eine wichtige Zweckänderung wird – schon bisher – durch das Archivgesetz[20] gesetzlich legitimiert: Mit der Archivierung werden als archivwürdig beurteilte Unterlagen der öffentlichen Organe über den Zweck hinaus, zu dem die Informationen ursprünglich erhoben worden sind, für einen neuen Zweck – die retrospektive Bearbeitung mit dem Ziel, staatliches Handeln rückblickend nachvollziehen, verstehen und kontrollieren zu können («kollektives Gedächtnis») – aufbewahrt. Zur Aufgabenerfüllung nicht mehr benötigte Personendaten, die von der gemäss Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt werden, sind hingegen zu vernichten (§ 16).

Der in der Vernehmlassungsvorlage noch enthaltene Abs. 2 wird ersetzt durch den eigenständigen Statistikparagraphen (§ 10) und den zusätzlichen Absatz 3 in § 22.

§ 13 Vorabkontrolle

Mit der Schengen/Dublin-Revision des Datenschutzgesetzes wurde die **Vorabkontrolle** eingeführt (vgl. § 18a DSG). Dieses Instrument, mit welchem die Berücksichtigung der Datenschutz-Anliegen frühzeitig gefördert werden soll, wird in § 13 übernommen: Das öffentliche Organ muss eine beabsichtigte Bearbeitung von Personendaten, die aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen (z.B. grosse Informatikprojekte), vorab der oder dem Informationszugangs- und Datenschutzbeauftragten zur Kontrolle unterbreiten. Das Ergebnis erfolgt in Form einer Empfehlung gemäss § 48.

§ 14 Datenvermeidung und Datensparsamkeit bei IT-Systemen

Das Datenschutzgesetz von 1992 folgt dem Konzept, das anfangs der 1980er Jahre als Antwort auf die in den 1970er Jahren erkannten Gefährdungen der informationellen Selbstbestimmung durch die Informationstechnologie entwickelt wurde. Die damaligen Erwartungen (oder Befürchtungen) wurden von der Entwicklung weit überholt.

Problematisch ist etwa, dass bei informationstechnologischen Systemen (IT-Systemen) oft systembedingt Personendaten bearbeitet werden: Für technische Vorgänge fallen Daten an, die anschliessend – obwohl für die behördliche Aufgabenerfüllung nicht erforderlich – nicht aus dem System entfernt werden. Es geht um «Randdaten», die für das technische Funktio-

[20] Gesetz vom 11. September 1996 über das Archivwesen (Archivgesetz, SG 153.600).

nieren von Datenbearbeitungssystemen und -programmen notwendig sind, wie Verbindungsdaten und Protokollierungen. Angesichts dieser fortschreitenden technologischen Entwicklung reicht es nicht mehr, für das (nachträgliche) Bearbeiten Regeln aufzustellen. Es ist notwendig, die Wirkung des gesetzgeberischen Entscheides früher einsetzen zu lassen, bei der Gestaltung von IT-Systemen nämlich: Datenschutz muss bereits in die Systeme «eingebaut» werden.

Moderne Datenschutzgesetze im In- und Ausland[21] statuieren deshalb **das Prinzip der Datenvermeidung und Datensparsamkeit**. Dieses Prinzip ist mehr, als was das Verhältnismässigkeitsprinzip bereits vorschreibt. Datenvermeidung und Datensparsamkeit «sind als gezielte Restriktion der Verwendung personenbezogener Daten entstanden, sollten also auch und gerade klarstellen, dass die Verarbeitung personenbezogener Angaben stets als begründungsbedürftige Ausnahme gesehen und behandelt werden muss.»[22]

Abs. 1: Das **Prinzip der Datenvermeidung und Datensparsamkeit** soll zu einem Umdenken führen, indem die Technologie den Anforderungen des Rechts zu folgen hat und nicht umgekehrt. Die IT-Systeme sind so zu gestalten, dass keine oder so wenig personenbezogene und personenbeziehbare Daten wie möglich anfallen. Es wird dabei bewusst nicht der Begriff «Personendaten» verwendet, da es eben darum geht, nicht nur Personendaten (wie sie zum Zweck der Aufgabenerfüllung durch die Steuerverwaltung, die Polizei, die Sozialhilfe Basel, die Einwohnerkontrolle usw. bearbeitet werden) nicht anfallen zu lassen, sondern grundsätzlich jede Information, die sich auf eine Person beziehen lässt (wie eben die zuvor erwähnten «Randdaten», also Verbindungsdaten und Protokollierungen, die nicht zur behördlichen Aufgabenerfüllung, sondern nur für das technische Funktionieren von Informatik- und Telekommunikationssystemen nötig sind) a priori zu vermeiden.

Abs. 2: Ist es systembedingt unvermeidbar, dass personenbezogene oder personenbeziehbare Daten erhoben werden, sollen «Privacy Enhancing Technologies» (PET, datenschutzfreundliche Technologien) zum Einsatz kommen, das heisst, die Daten sollen **anonymisiert oder pseudonymisiert** werden, sobald und soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Anonymisierung bedeutet, dass der Personenbezug irreversibel aufgehoben wird und keine Rückschlüsse auf Personen mehr möglich sind. Unter Pseudonymisierung versteht man die Aufhebung des Personenbezugs, wobei ein bestimmter Schlüssel zur Re-Personifizierung der Informationen erhalten bleibt. Werden Daten pseudonymisiert, sind die Bedingungen zu regeln, unter denen eine Person identifiziert werden darf. Wenn der «Einbau» solcher Routinen von Anfang an vorgesehen ist, ist der Aufwand erheblich geringer, als wenn nachträglich solche Vorkehren getroffen werden müssen. Insbesondere kann durch frühzeitige Kooperation des IT-Bereichs mit dem Staatsarchiv und dem Datenschutz vermieden werden, dass irreversible Eingriffe an Daten vorgenommen werden. Aus diesem Grund wird diese Bestimmung vor al-

---

[21] Vgl. nur etwa § 4 des Schleswig-Holsteinischen Gesetzes vom 9. Februar 2000 zum Schutz personenbezogener Informationen; § 3a des (deutschen) Bundesdatenschutzgesetzes (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I 66); § 5a des (Berliner) Gesetzes zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz, BlnDSG); § 11 Informations- und Datenschutzgesetz ZH (LS 170.4); § 9 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen AG (SAR 150.700).

[22] SPIROS SIMITIS, Auf dem Weg zu einem neuen Datenschutzkonzept: Die zweite Novellierungsstufe des BDSG, DuD 12/2000, 727 ff.

lem beim Aufbau neuer Systeme oder bei der Ablösung bestehender Systeme zur Geltung kommen.

Datenschutzfreundliche Technologie soll ausserdem neu Anwendung finden bei der Videoüberwachung (vgl. § 17 Abs. 4).

§ 15 Erkennbarkeit der Beschaffung

Die betroffene Person muss **erkennen** können, welche Personendaten über sie beschafft und zu welchem Zweck sie bearbeitet werden. Dieses in § 9 Abs. 1 DSG[23] festgehaltene Prinzip wird samt Ausnahme und Präzisierung für die systematische Datenerhebung in § 15 in die Absätze 1 und 2 übernommen. Es reicht für die Ausnahme nicht jede noch so geringe Gefährdung; die Beschaffung darf nur dann nicht erkennbar bleiben, wenn die Aufgabenerfüllung ernsthaft gefährdet wird. Präzisierend wird festgehalten, dass nicht nur die Erhebung per Fragebogen auf Papier eine systematische Erhebung darstellt, sondern dass Onlineerfassungen ihr gleichgestellt sind (z.B. Erhebung von Personendaten mit Onlineformularen auf einer Website). Ergänzt wird das Prinzip der Erkennbarkeit um eine **qualifizierte Transparenzpflicht** bei der Beschaffung besonderer Personendaten, wie sie auch das Bundesdatenschutzgesetz für alle Datenbearbeiterinnen und Datenbearbeiter, Private wie Bundesorgane, vorschreibt (vgl. auch § 9 Abs. 2 DSG): Werden besondere Personendaten beschafft, ist die betroffene Person zu informieren (Abs. 3). Sollen also beispielsweise Daten über den Gesundheitszustand einer Person oder ein Strafregisterauszug beschafft werden, dann ist die betroffene Person darüber zu informieren, falls nicht – die generelle Einschränkung von Abs. 1 gilt auch hier – gerade durch die Information die Erfüllung der gesetzlichen Aufgabe ernsthaft gefährdet wird. Für die Information reicht ein deutlicher Hinweis beispielsweise auf einem Formular, mit welchem die betroffene Person eine Dienstleistung beantragt; die Erfüllung der Transparenzpflicht erfordert deshalb in weiten Bereichen der staatlichen Verwaltung keine zusätzlichen Umsetzungsmassnahmen.

§ 16 Vernichtung

Die im § 18 DSG noch angesprochene Archiv-Anbietepflicht muss nicht ins neue Gesetz übernommen werden, da das Archivgesetz (§ 7 Abs. 1) sie bereits enthält. Festzuhalten ist hingegen, was mit Personendaten zu geschehen hat, welche zur Aufgabenerfüllung nicht mehr benötigt werden und von der nach dem Archivgesetz zuständigen Stelle als nicht archivwürdig beurteilt worden sind: Sie sind – wie bisher (§ 18 DSG) – vom öffentlichen Organ zu **vernichten.** Die in der Vernehmlassungsvorlage noch vorgesehene Alternative zur Vernichtung – die Anonymisierung – wurde verschiedentlich kritisiert und deshalb gestrichen.

§ 17 Besondere Voraussetzungen für den Einsatz von Videoüberwachung

§ 6a DSG wurde 2004 aufgrund eines parlamentarischen Vorstosses im Grossen Rat ins Datenschutzgesetz aufgenommen. Die grundsätzlichen Überlegungen aus dem damaligen Ratschlag des Regierungsrates (Nr. 9277) und die ergänzenden Ausführungen der grossrätlichen Kommission gelten heute nach wie vor unverändert. Der Einsatz von Videoüberwa-

[23] In der Fassung der Schengen/Dublin-Revision.

chung muss weiterhin an Bedingungen geknüpft werden, wie sie im vorliegenden Entwurf für ein Informations- und Datenschutzgesetz generell für Datenbearbeitungen enthalten sind. Im Laufe der Vorbereitung, im Mitberichts- und im Vernehmlassungsverfahren wurden aber sehr *widersprüchliche Stellungnahmen* zu den jeweiligen Vorschlägen (§ 15a in den entsprechenden Vorlagen) formuliert. Die Forderungen reichen von einem gesetzlichen Verbot der Videoüberwachung bis zur Schaffung einer generellen Grundlage dafür (anstelle des Vorbehalts spezialgesetzlicher Grundlagen); es wurde die Verlängerung der Aufbewahrungsdauer von bisher 24 Stunden auf eine Woche begrüsst oder gar eine Verlängerung auf drei Monate oder 100 Tage verlangt; die Streichung der Autorisierung durch die oder den Informationszugangs- und Datenschutzbeauftragten im Interesse der Klärung der Verantwortlichkeiten wurde begrüsst, aber es wurde auch dafür plädiert, an einer Bewilligungspflicht festzuhalten; und schliesslich wurde der Einsatz von technischen Datenschutzmassnahmen verlangt.

Viele der Unterschiede der Anschauungen rühren daher, dass unter «Videoüberwachung» *sehr verschiedene Einsatzformen* verstanden werden können und dass eine einheitliche Regelung an Grenzen stösst. Eine sehr kurze Aufbewahrungsdauer ist gerechtfertigt, wo kurze Zeit nach der Überwachung feststeht, dass die Aufnahmen nicht mehr benötigt werden, also wenn etwa Vandalismus im Tram erfasst werden soll: Wenn keine Wände versprayt und keine Sitzpolster aufgeschlitzt sind und somit keine Vandalen überführt werden müssen, werden die Aufnahmen sofort nicht mehr benötigt und können vernichtet werden. Wenn aber der Zweck eines staatlich betriebenen Videoüberwachungssystems darin besteht, Privaten als Opfer eines Delikts im öffentlichen Raum ein Beweismittel zur Verfügung zu stellen, dann wird die Zweckerreichung durch eine sehr kurze Aufbewahrungsdauer vereitelt, weil die Beweismittel in dem Moment, wo ein Strafantrag noch möglich ist, bereits vernichtet sind. Die Beispiele zeigen, dass es eben **entscheidend** auf die **konkrete Zweckbestimmung** eines Videoüberwachungssystems ankommt. Diese Zweckbestimmung ist jeweils kritisch zu prüfen: Nicht jede staatliche Videoüberwachung wird dazu eingerichtet, Beweismittel für Private in straf- und zivilrechtlichen Verfahren zu generieren, weshalb sich auch die generelle Verlängerung auf die in einem abstrakten Normkontrollverfahren vor Bundesgericht als zulässig beurteilte Frist von 100 Tagen (BGE 133 I 77) verbietet. Je länger eine Aufbewahrungsdauer wird, umso wichtiger ist es, durch rechtliche, organisatorische und technische Massnahmen dafür zu sorgen, dass in der Zwischenzeit für die erfassten Personen keine Persönlichkeitsrechtsverletzung entsteht.

Um die verschiedenen Einwendungen und Forderungen sachgerecht zu berücksichtigen, wurde die Bestimmung nach der Vernehmlassung neu konzipiert. Die wichtigsten Elemente der Änderung sind:

- Es wird nicht mehr eine (spezial-)gesetzliche Grundlage verlangt, sondern die Bestimmung im IDG stellt die aus rechtsstaatlichen Gründen erforderliche gesetzliche Grundlage dar.

- Für jedes Videoüberwachungssystem muss vor der Inbetriebnahme ein Reglement erlassen werden; das Reglement ist zeitlich zu befristen und vor der Verlängerung muss die Wirksamkeit evaluiert werden.

- Im Mittelpunkt der Regelung eines Videoüberwachungssystems steht die Festlegung des konkreten Zwecks, der mit dem Einsatz des Systems erreicht werden soll.

- Es wird nicht mehr zwingend eine einheitliche Löschungsfrist festgelegt; sie kann im Reglement, wenn es der konkrete Zweck des Videoüberwachungssystems erfordert, über die «Regellänge» von einer Woche verlängert werden.

Die Videoüberwachungs-Regelung wird wegen ihrer Länge auf zwei Paragraphen aufgeteilt; der erste regelt allgemein den Einsatz von Videoüberwachung (§ 17), der zweite das erforderliche Reglement (§ 18).

Abs. 1: Im Vergleich zur bisherigen Regelung wird nicht nur Videoüberwachung an öffentlichen und allgemein zugänglichen Orten (§ 6a Abs. 1 DSG) erfasst, sondern auch an öffentlichen, aber nicht allgemein zugänglichen Orten. Dies entspricht der Ausweitung des Geltungsbereichs durch § 1 Abs. 2 der Videoüberwachungsverordnung[24]. Der bisher verwendete Begriff «technische Überwachung mittels Bildübermittlungs- und Bildaufzeichnungsgeräten (Videoüberwachung)» (Überschrift von § 6a DSG) kann vereinfacht werden, da die Kurzform «Videoüberwachung» heute allgemein verständlich ist.

Neu muss ausdrücklich festgehalten sein, dass es bei der Regelung nur um Videoüberwachungssysteme geht, bei denen **Personen identifiziert** werden können, nicht aber um solche, bei denen aufgrund des Kamerastandortes und der Kameraeinstellungen eine Identifikation ausgeschlossen ist (etwa bei Kameras entlang der Autobahn, die bloss zur Erkennung der allgemeinen Verkehrssituation dienen). Das war bisher klar, da das Datenschutzgesetz nur die Bearbeitung von Personendaten regelt; das neue Informations- und Datenschutzgesetz gilt aber auch für den Umgang mit Nicht-Personendaten. Die Beschränkung ist angemessen, da «nicht-identifizierende» Überwachungssysteme deutlich geringere Risken für die Persönlichkeitsrechte der betroffenen Personen bergen. Die massgebliche Identifizierbarkeit kann beispielsweise durch die Aufnahme des Gesichtes der erfassten Person oder anderer Merkmale (beispielsweise des Polizeikennzeichens bei Motorfahrzeugen, über welche auf die Halterin oder den Halter geschlossen werden kann) gegeben sein.

Im Unterschied zur bisherigen Regelung ist der *Schutz* von Personen und Sachen *vor strafbaren Handlungen (Prävention)* nicht mehr der einzige **zulässige Zweck**; streng genommen hätte in diesem Fall nämlich eine Videoaufnahme nicht mehr verwendet werden dürfen, sobald eine strafbare Handlung erfolgt ist, weil die Verwendung nicht mehr der Prävention dient. Deshalb wird richtigerweise neu auch die *Verfolgung von strafbaren Handlungen* gegen Personen und Sache als zulässige Zweckbestimmung erwähnt.

Neu wird wie erwähnt nicht mehr auf die Voraussetzung einer (spezial-)gesetzlichen Grundlage verwiesen (bisheriger Verweis auf die Voraussetzungen des § 5 DSG in § 6a Abs. 1 DSG), sondern § 17 selber stellt die **gesetzliche Grundlage** für den Einsatz von Videoüberwachungssystemen dar. Schon nach der bisherigen Praxis wurde in aller Regel keine formellgesetzliche Grundlage vorausgesetzt; bei den Sportanlagen beispielsweise wurde vom Datenschutzbeauftragten, der bisher jedes Videoüberwachungssystem zu autorisieren

[24] SG 153.290.

hatte (§ 6a Abs. 1 DSG), die Regelung in einem Benutzungsreglement als genügend angesehen. Mit der neu vorgeschlagenen Regelung wird deshalb die rechtliche Erfassung trotz des formellen Verzichts auf die (spezial-)gesetzliche Grundlage eher verdichtet als verdünnt.

Abs. 2 konkretisiert – wie bisher § 6a Abs. 2 Satz 2 DSG – das **Verhältnismässigkeitsprinzip** (§ 9 Abs. 3) für die Videoüberwachung, und zwar *in räumlicher wie zeitlicher Hinsicht*: Es dürfen nur die Orte erfasst werden, die zur Erreichung des konkreten Zwecks erforderlich sind, und auch die Betriebszeiten müssen auf das zur Zweckerreichung Notwendige beschränkt werden. Ganz generell darf aufgrund des Verhältnismässigkeitsprinzips Videoüberwachung nur dann vorgesehen werden, wenn der Zweck mit anderen, milderen Massnahmen (z.B. bessere Beleuchtung, unregelmässige Kontrolle durch das Personal, Videoüberwachung, bei welcher Personen nicht identifiziert werden können, usw.) nicht erreicht werden kann. Im Rahmen der Vorabkontrolle (§ 18 Abs. 3) sind die entsprechenden Nachweise zu erbringen.

Abs. 3 konkretisiert – wie bisher § 6a Abs. 3 DSG – für die Videoüberwachung die Pflicht von § 15 (**Erkennbarkeit** der Beschaffung).

Abs. 4 regelt, wie lange Videoüberwachungsaufzeichnungen **aufbewahrt** werden dürfen. Die bisherige Frist von 24 Stunden (§ 6a Abs. 1 DSG) wird – wie in der Vernehmlassungsvorlage vorgeschlagen – auf **eine Woche** verlängert; diese Frist gilt in der Regel. Im Reglement kann **ausnahmsweise** eine **längere Frist** festgelegt werden, wenn kumulativ:

- der *konkrete Zweck*, der mit dem Einsatz der Videoüberwachung erreicht werden soll, dies erfordert; das kann der Fall sein, wenn im Reglement ausdrücklich angegeben wird, Zweck des Videoüberwachungssystems sei es, Privaten als Opfer eines Delikts Beweismittel zur Verfügung zu stellen;

- das Risiko einer Persönlichkeitsverletzung durch *technische und organisatorische Vorkehren* minimiert wird; das kann also beispielsweise durch sog. Privacy-Filter erfolgen, welche Menschen und Gesichter auf den Aufnahmen durch «Verpixelung» unkenntlich machen, wobei die Verpixelung unter vorgegebenen Voraussetzungen rückgängig gemacht werden kann (Anwendungsfall von Privacy Enhancing Technologies).

Abs. 5 regelt – wie bisher § 6a Abs. 4 Satz 2 und 3 DSG – die **Verwendung** für ein straf- oder zivilrechtliches Verfahren. Im Vordergrund stehen logischerweise von öffentlichen Organen eingeleitete strafrechtliche Verfahren; unzulässig wäre etwa die Verwendung einer Videoaufzeichnung in einem arbeitsrechtlichen Verfahren, um zu beweisen, dass eine Arbeitnehmerin oder ein Arbeitnehmer zu einer bestimmten Zeit an einem bestimmten Ort (statt an der Arbeit) war.

§ 18 Reglement für das Videoüberwachungssystem

Abs. 1 legt fest, dass für jedes Videoüberwachungssystem vor seiner Inbetriebnahme ein **Reglement** zu erlassen ist. Das Reglement muss insbesondere den Zweck, die Verantwortlichkeit und die Löschungsfrist festlegen. Zum weiteren Inhalt des Reglements siehe die Erläuterungen zu Abs. 5.

Ein **Videoüberwachungssystem** ist eine technische Anlage zur Bilderfassung und zur Bildübermittlung und/oder Bildaufzeichnung, welche zur Überwachung von Orten und/oder Personen benützt wird. Es ist also unerheblich, ob beim konkreten System eine «Echtzeitauswertung» stattfindet oder ob die Bilder erst später (generell oder bei Bedarf) ausgewertet werden, ob die Bilder bei der Anlage bleiben oder an einen anderen Ort (z.B. eine Überwachungszentrale) übermittelt werden, ob die Bilder (die technischen Signale) aufgezeichnet werden oder nicht, ob das System immer oder nur zu bestimmten Zeiten in Betrieb ist. Erfasst von der Regelung werden Systeme, die im Verantwortungsbereich von öffentlichen Organen im öffentlichen Raum, nicht aber solche, die von Privaten im privaten Raum eingesetzt werden. Nicht Gegenstand dieser Regelung ist ausserdem der Einsatz von Videoüberwachungssystemen durch die Polizei im Sinne von §§ 58 f. des Polizeigesetzes[25]. Ein *System* kann aus mehreren Kameras bestehen, die zusammenhängend dem gleichen Zweck dienen (z.B. ein System von mehreren Kameras, welche die Umgebung und die Zugänge zu einer bestimmten Einrichtung wie einem Tramdepot erfassen), oder an mehreren Orten einen identischen Zweck verfolgen (z.B. alle Kameras in Tramanhängern).

Abs. 2 legt fest, wer für den Erlass des erforderlichen Reglements **zuständig** ist:

- die Departemente bei Systemen im Verantwortungsbereich kantonaler öffentlicher Organe (lit. a);

- der Gemeinderat bei Systemen im Verantwortungsbereich kommunaler öffentlicher Organe (lit. b);

- das Appellationsgericht bei Systemen im Verantwortungsbereich von Gerichten (lit. c);

- die Direktion selbständiger Anstalten und Körperschaften des öffentlichen Rechts bei Systemen in ihrem Verantwortungsbereich.

Abs. 3: Die **Befristung** entspricht der bisherigen Regelung in § 2 Abs. 4 der Videoüberwachungsverordnung. Neu eingeführt wird die Pflicht, die Wirksamkeit zu **evaluieren**; dazu sind während des Einsatzes die nötigen Daten zu erfassen. Wenn beispielsweise der Zweck im Schutz vor Vandalismus (Gewalt gegen Sachen) bestand und sich die Lage trotz des Einsatzes von (erst nachträglich ausgewerteter) Videoüberwachung nicht bessert, wird das Reglement nicht unverändert verlängert werden können, sondern es ist beispielsweise eine Echtzeitauswertung vorzusehen.

Abs. 4: Anstelle der bisherigen Autorisierung durch die Datenschutzaufsichtsstelle (§ 6a Abs. 1 DSG) tritt neu die (mit der Schengen/Dublin-Revision des Datenschutzgesetzes eingeführte) **Vorabkontrolle** durch die oder den Informationszugangs- und Datenschutzbeauftragten (§ 18a DSG, § 13 des vorliegenden Entwurfs). Damit wird die Verwischung der Verantwortlichkeiten, die der bisherigen Lösung anhaftet, beseitigt.

---

[25] SG 510.100.

Abs. 5 sieht vor, dass das Nähere bezüglich der Reglemente durch **Verordnung** zu regeln ist. So wird insbesondere festzulegen sein, welche Regelungen das Reglement zu enthalten hat. Es werden dies die folgenden Punkte sein:

- Beschreibung des Systems,
- verantwortliches öffentliches Organ,
- konkreter Zweck der Videoüberwachung,
- von der Videoüberwachung erfasste Bereiche und Personen,
- Betriebszeiten,
- Aufzeichnung (nie, immer, situativ nach welchen Kriterien),
- Auswertung (in Echtzeit oder nachträglich),
- Personen, welche Zugriff haben auf die aufgezeichneten Daten,
- Aufbewahrungsdauer (in der Regel 1 Woche, in Ausnahmefällen nach § 17 Abs. 4 länger),
- Massnahmen zum Schutz vor unbefugter Bearbeitung und
- Massnahmen zum Schutz der erfassten Personen.

Der Zweck des Einsatzes von Videoüberwachung wird damit stärker in den Mittelpunkt gestellt. An ihm ist die Verhältnismässigkeit zu messen, insbesondere bezüglich des örtlichen und zeitlichen Einsatzes (§ 17 Abs. 2) und der Aufbewahrungsdauer allfälliger Aufzeichnungen (§ 17 Abs. 4), aber auch bei der Frage nach der Wirksamkeit, die bei der Verlängerung zu prüfen ist (§ 18 Abs. 3). Die Zweckbeschreibung muss dementsprechend möglichst konkret sein.

Die Verordnungsregelung ist für die kantonale Verwaltung durch den Regierungsrat zu erlassen. Für die Gerichte, die Gemeinden und die selbständigen Anstalten und Körperschaften gilt die Verordnungsregelung sinngemäss. Es ist nicht notwendig, in dem relativ formalen Bereich von diesen separate Regelungen zu verlangen; insbesondere würde es auch kaum Sinn machen, vom Gemeinderat zu verlangen, in einer allgemeinen Form zu regeln, was er selber in Form des Reglements anschliessend umzusetzen hat.

§ 19 Qualitätssicherung

Die zunehmende Komplexität von Gesellschaft, Wirtschaft, Politik, aber auch der Verwaltung und der Rechtspflege verlangt, dass die einzelnen Bereiche systematisch(er) gelenkt werden. So wurden etwa **Qualitätsmanagementsysteme** entwickelt, bei welchen eine Lenkung und Beschreibung der Abläufe zu qualitätssichernden und –verbessernden Massnahmen führen. Die Grundsätze von Managementsystemen lassen sich auch auf Informationsbear-

beitungen übertragen. Mit der Entwicklung und Anwendung von Datenschutzmanagementsystemen können die Datenbearbeitungen systematisch und umfassend gelenkt und damit ein gesetzeskonformer Umgang mit den Personendaten sichergestellt werden. Als durchaus gewünschter Nebeneffekt lassen sich Kosten sparen, indem unnötige Datenbearbeitungen vermieden werden. Auf dem Markt haben sich bereits erste Datenschutzmanagementsysteme herausgebildet. Allerdings fehlt es noch weitgehend an Kriterien, nach welchen sich solche Systeme zu richten haben. Der Bund hat mit der Revision seines Datenschutzgesetzes vom 24. März 2006 die gesetzliche Grundlage für solche **Auditierungen und Zertifizierungen** durch anerkannte unabhängige Zertifizierungsstellen eingeführt (vgl. Art. 11 DSG-Bund). Am 28. September 2007 hat der Bundesrat die dazu gehörende Datenschutzzertifizierungsverordnung[26] erlassen.

Auch für den Kanton Basel-Stadt mit unzähligen grossen Informatiksystemen sind solche Managementsysteme bzw. Auditierungs- und Zertifizierungsverfahren geeignete Massnahmen, die den Umgang mit Personendaten für die öffentlichen Organe vereinfachen. Auf gesetzlicher Ebene soll – wie im Bundesdatenschutzgesetz – der allgemeine Grundsatz statuiert werden; die Konkretisierung hat zu gegebener Zeit in einer Verordnung zu erfolgen. § 16 des Gesetzesentwurfs soll das Bemühen um eine solche Qualitätssicherung fördern, aber nicht vorschreiben.

IV. Bekanntgabe von Informationen

Die §§ 20 bis 24 regeln die **Bekanntgabe von Informationen** (inklusive Personendaten) **zur Erfüllung der gesetzlichen Aufgaben** – in Abgrenzung zum Zugang zu Informationen gestützt auf das Informationszugangsrecht, wo Informationen nicht zugänglich gemacht werden, weil dies zur Erfüllung der gesetzlichen Aufgabe des öffentlichen Organs erforderlich wäre, sondern weil eine private Person, ein wirtschaftliches Unternehmen oder die Medien ihr Recht auf Zugang zu Informationen geltend machen; jener Zugang zu Informationen ist Gegenstand der Regelung in den nächsten Abschnitten (§§ 25 ff.).

§ 20 Informationstätigkeit von Amtes wegen

Die **Informationstätigkeit**[27] nach dem Öffentlichkeitsprinzip umfasst zwei Aspekte: einerseits das Informieren von Amtes wegen und anderseits auf Anfrage. Informieren von Amtes wegen meint die Pflicht der öffentlichen Organe, die Öffentlichkeit von sich aus (pro-)aktiv ausreichend über ihre Tätigkeit von allgemeinem Interesse zu informieren. Informieren auf Anfrage meint die (reaktive) Pflicht der öffentlichen Organe zur Informationstätigkeit, wenn eine Person ihr Recht auf Zugang zu Informationen (§§ 25 ff.) geltend macht. Die beiden Aspekte hängen aber auch direkt zusammen: Je mehr ein öffentliches Organ von sich aus informiert und je mehr es dadurch die Informationsbedürfnisse der Öffentlichkeit abdeckt, umso geringer wird erstens die Zahl der Informationszugangsgesuche ausfallen und umso geringer wird zweitens der Aufwand bei der Informationstätigkeit auf Anfrage – einerseits

[26] Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (VDSZ, SR 235.13).

[27] Es ist terminologisch klar zu unterscheiden zwischen «Information» (die Aufzeichnungen im Sinne von § 3 Abs. 2) und «Informationstätigkeit» bzw. «informieren» (das Vermitteln von Informationen).

wegen der geringeren Gesuchsanzahl, anderseits auch wegen der Möglichkeit, auf Gesuche um Zugang zu bereits öffentlich zugänglichen Informationen unter Verweis auf die Quelle nicht eintreten zu müssen (§ 32 Abs. 1).

Abs. 1: Die hier statuierte Pflicht zur **Informationstätigkeit von Amtes wegen** ist nicht neu; sie konkretisiert die naturgemäss allgemein gehaltene Grundsatzbestimmung der Kantonsverfassung, wonach die Behörden die Öffentlichkeit über ihre Tätigkeit informieren (§ 75 Abs. 1 KV). Auch wenn die heutige Informationspolitik der öffentlichen Organe in unserem Kanton schon in diesem Sinn wahrgenommen wird, ist sie dennoch auf Gesetzesstufe zu verankern.[28] Eine offene Informationspolitik schafft Transparenz und Vertrauen in den Staat und seine Organe. Sinn und Zweck der verfassungsrechtlich festgeschriebenen Informationspflicht bestehen indes nicht darin, dass ein öffentliches Organ über sämtliche Geschäfte informiert, mit denen es sich befasst. Das wäre weder praktikabel noch entspräche eine solche Interpretation der Intention des Verfassungsgebers. Vielmehr muss ein allgemeines Interesse an der Information bestehen.

Abs. 2: Von **allgemeinem Interesse** sind Informationen, die Belange von öffentlichem Interesse betreffen und für die Meinungsbildung über das Geschehen im Kanton respektive in der Gemeinde und zur Wahrung der demokratischen Rechte der Bevölkerung von Bedeutung sind. Zu den Tätigkeiten und Angelegenheiten von allgemeinem Interesse zählen Beschlüsse, wichtige Geschäfte, bedeutende Entscheide und Massnahmen, Ziele, Lagebeurteilungen, Planungen usw. Für die (pro-)aktive Informationstätigkeit der öffentlichen Organe lassen sich folgende Leitlinien formulieren: Das Informieren von Amtes wegen hat rasch (unmittelbar nach einem Entscheid oder Ereignis), umfassend (mit allen zum Verständnis notwendigen Angaben) sowie sachlich (unvoreingenommen und frei von Propaganda) zu erfolgen. Die Mittel der Informationstätigkeit von Amtes wegen sind einerseits die Medienarbeit (Medienmitteilungen, -orientierungen), aber auch amtliche Publikationen (Kantonsblatt, Broschüren, Merkblätter) und zunehmend das Internet. Zu beachten ist, dass der Veröffentlichung einer bestimmten Information im Einzelfall überwiegende öffentliche oder private Interessen entgegenstehen können (§ 29).

Abs. 3: Die Information über den **Aufbau** eines öffentlichen Organs, über seine **Zuständigkeiten** und über die **Ansprechpersonen** für bestimmte Anliegen ist ein wesentlicher Teil der Informationstätigkeit von Amtes wegen, heute schon weitgehend wahrgenommen durch die Veröffentlichung im Staatskalender, in Behördenverzeichnissen der Gemeinden und auf den Websites von Kanton und Gemeinden. Diese Information ist aber – vor allem im Zusammenhang mit dem Verzeichnis der Informationsbestände (§ 24) – von Bedeutung für den individuellen Zugang zu den eigenen Personendaten (§ 26). Ausserdem ist diese Bestimmung die gesetzliche Grundlage für die Veröffentlichung von Personendaten über Amtsträgerinnen und Amtsträger (Name, dienstliche Adresse, Angaben zur dienstlichen Erreichbarkeit wie Telefonnummer und E-Mail-Adresse, Funktion und Zuständigkeit).

Abs. 4 regelt eine Frage, die immer wieder zu Diskussionen Anlass gibt: das **Informieren über hängige Verfahren**. Das öffentliche Organ soll über hängige Verfahren des Verwal-

[28] Nur vereinzelt bestehen ausdrückliche gesetzliche Grundlagen, zum Beispiel für die Polizei in § 12 Polizeigesetz (SG 510.100).

tungs- und Verwaltungsrekursverfahrens (hängige Verfahren der Straf- und Zivilrechtspflege sowie der Verfassungs- und Verwaltungsgerichtsbarkeit sind infolge von § 2 Abs. 2 lit. b und c aus dem Geltungsbereich des IDG ausgeschlossen) informieren dürfen, wenn dies zur Berichtigung oder Vermeidung falscher Meldungen erforderlich ist oder wenn es in einem besonders schweren oder Aufsehen erregenden Fall angezeigt ist, unverzüglich zu informieren. Die Bestimmung überlässt dem öffentlichen Organ richtigerweise einen gewissen Handlungsspielraum. Dabei ist klar, dass spezialgesetzliche Vorschriften vorgehen (also beispielsweise bei Vorhaben, die von Gesetzes wegen öffentlich aufgelegt werden müssen, etwa in Planauflageverfahren).

Abs. 5: Der Regierungsrat soll – wie bisher – die Informationstätigkeit der kantonalen Verwaltung regeln. Die gesetzliche Delegation lässt absichtlich offen, wie der Regierungsrat dies regeln soll (z.B. durch Verordnung, Beschluss oder Absprache). Für die kommunale Verwaltung regelt der Gemeinderat die Informationstätigkeit.

§ 21 Bekanntgabe von Personendaten

Die **Bekanntgabe von Personendaten** ist ein Bearbeiten von Personendaten, aber ein besonderes, weil die Personendaten damit den Bereich verlassen, für den sie ursprünglich erhoben wurden, womit fast immer eine Zweckänderung – und damit eine Verletzung der Zweckbindung (§ 12) – erfolgt. Deshalb regeln die Datenschutzgesetze dieses Bearbeiten regelmässig separat. § 21 übernimmt die Regeln der §§ 10 und 11 DSG; allerdings wird nicht mehr nach den Datenempfängerinnen oder –empfängern (also öffentliche Organe und Private) gegliedert. Denn die Voraussetzungen für die Bekanntgabe von (besonderen) Personendaten an öffentliche Organe und an Private sind die gleichen. Entscheidend ist jeweils die Frage, ob die konkrete materiellgesetzliche Grundlage (das Steuergesetz, das Sozialhilfegesetz usw.) eine Bekanntgabe nur an öffentliche Organe oder auch an Private oder weder noch zulässt, oder ob es zur Erfüllung der konkreten gesetzlichen Aufgabe erforderlich ist, dass Personendaten an öffentliche Organe oder allenfalls auch an Private bekannt gegeben werden. Im Unterschied zur Vernehmlassungsvorlage, in welcher noch zwei (fast gleichlautende) Paragraphen die Bekanntgabe von Personendaten allgemein (§ 18) bzw. die Bekanntgabe von besonderen Personendaten (§ 19) geregelt haben, werden die Bekanntgabevoraussetzungen für beide Personendatenkategorien in einer einzigen Bestimmung zusammengefasst – so wie auch § 9 die Bearbeitungsvoraussetzungen für beide Kategorien enthält.

Abs. 1 nennt die **Voraussetzungen** für die Bekanntgabe von Personendaten generell: eine gesetzliche Grundlage für die Bekanntgabe (lit. a)[29], die Erforderlichkeit zur Erfüllung einer gesetzlichen Aufgabe (lit. b)[30] oder – im Einzelfall – die Einwilligung der betroffenen Person (lit. c)[31]. Als gesetzliche Bestimmung (lit. a) kann für das Bearbeiten von Personendaten – im Gegensatz zum Bearbeiten von besonderen Personendaten (§ 21 Abs. 2) – eine Bestim-

[29] § 5 Abs. 1 DSG.
[30] § 10 DSG.
[31] § 11 Abs. 1 lit. a DSG; im Unterschied zu dieser Regelung wird der Satz umgestellt: Entweder liegt eine Einwilligung vor oder es wird – wenn nicht – geprüft, ob die Bekanntgabe im Interesse der betroffenen Person liegt und ihre Einwilligung in guten Treuen vorausgesetzt werden darf. Hat die betroffene Person eingewilligt, braucht nicht noch extra geprüft zu werden, ob die Datenbekanntgabe in ihrem Interesse liegt. Der neue Wortlaut nimmt damit die betroffene Person ernster als der alte.

mung in einer kompetenz- und delegationskonform erlassenen Verordnung (= Gesetz im materiellen Sinn) genügen.

Abs. 2 legt die **qualifizierten Voraussetzungen** für die **Bekanntgabe von besonderen Personendaten** fest, analog zu den qualifizierten Voraussetzungen für die Bearbeitung von besonderen Personendaten (§ 9 Abs. 2, materiell weitgehend übereinstimmend mit § 10 DSG). Im Unterschied zu § 21 Abs. 1 braucht es als Grundlage für das Bearbeiten von besonderen Personendaten (lit. a) eine Bestimmung in einem formellen Gesetz, da es sich um eine schwerwiegende Grundrechtseinschränkung handelt (vgl. § 13 Abs. 1 KV und Art. 36 Abs. 2 BV). Da es nicht angehen kann, dass das Weitergebendürfen von Personendaten unter weniger strengen Voraussetzungen zulässig sein soll als generell das Bearbeiten durch das erhebende Organ (vgl. § 9), ist die Weitergabe von besonderen Personendaten gemäss Abs. 1 lit. b nur zulässig, wenn dies zur Erfüllung einer klar umschriebenen gesetzlichen Aufgabe zwingend notwendig ist. Schliesslich erfolgt eine Bekanntgabe von besonderen Personendaten auch mit Zustimmung der betroffenen Person oder in gutem Treuen in ihrem Interesse liegend (lit. c).

Abs. 3 regelt die Datenbekanntgabe in einem **Online-Abrufverfahren**, wenn also wegen der Einrichtung der Online-Zugriffsmöglichkeit das Daten bekannt gebende öffentliche Organ künftig nicht mehr prüfen kann, ob die Voraussetzungen für die Bekanntgabe im konkreten Fall erfüllt sind, sondern das Daten abrufende öffentliche Organ direkt die Daten aus einer Datenbank beziehen kann. Der Vernehmlassungsentwurf übernahm die bisherige Regelung von § 10 Abs. 2 DSG: Das Autorisierungsverfahren wurde also beibehalten. In der Vernehmlassung wurde aber die Streichung dieses Absatzes verlangt, weil dadurch die Verantwortlichkeiten verwischt würden (SP, Riehen). Die oder der Informationszugangs- und Datenschutzbeauftragte solle zur Frage des Online-Zugriffs eine Empfehlung abgeben und die Zugriffsgewährung kontrollieren können; das öffentliche Organ habe aber über die Gewährung des Online-Zugriffs zu entscheiden und diesen Entscheid zu verantworten. Die Mehrzahl der Departemente will aber am Autorisierungsverfahren, das sich in der Vergangenheit bewährt habe, festhalten. Die Gemeinde Riehen macht geltend, dass sich ein Widerspruch zur Organisationsautonomie der Gemeinden (§§ 59 und 65 KV) ergebe, wenn die Gemeinden aufgrund der hohen Anforderungen an die Unabhängigkeit und Wirksamkeit der Datenschutzaufsicht die Aufsicht an den Kanton zurückdelegieren müssten; dann müsste ein kantonales Organ (die oder der Informationszugangs- und Datenschutzbeauftragte) über Online-Zugriffe auf kommunaler Ebene entscheiden. Riehen beantragt deshalb, dass die Autorisierung nur für die Einrichtung von Online-Zugriffen auf Personendaten in kantonalen Datenbanken vorausgesetzt werden solle; die Gemeinde würde es allerdings begrüssen, wenn auf das Autorisierungsverfahren überhaupt verzichtet würde, da es wegen des neuen Instruments der Vorabkontrolle (§ 13) nicht mehr nötig sei.

Der Regierungsrat schliesst sich der Argumentation der Vernehmlassungen an und verzichtet darauf vorzuschlagen, das Autorisierungsverfahren beizubehalten, weil neu das Verfahren der Vorabkontrolle (§ 13) zur Verfügung steht und dadurch die Berücksichtigung der datenschutzrechtliche Anforderungen gewährleistet werden kann.

Die Vernehmlassungsvorlage enthielt noch einen weiteren Absatz, der dem heutigen § 11 Abs. 2 DSG entsprach: Der Regierungsrat hatte danach die Befugnis, die Bekanntgabe von

Personendaten für Druckerzeugnisse im allgemeinen Interesse (beispielsweise das Basler Adressbuch) zu bewilligen. Nachdem bereits auf gesetzlicher Stufe festgelegt ist, dass die Einwohnerdienste Basel-Stadt befugt sind, die nötigen Datenangaben zur Herausgabe des Basler Adressbuches zu machen (§ 30 Abs. 2 Aufenthaltsgesetz[32]), ist eine Delegation an den Regierungsrat nicht mehr erforderlich. Der Regierungsrat hat seine bestehende Befugnis für andere Nachschlagewerke als das Basler Adressbuch bisher nicht wahrgenommen. Zum laut gewordenen Bedürfnis nach einer Internet-Ausgabe des Basler Adressbuchs ist zu bemerken, dass das Ergebnis dieses Ansinnens einem Quantensprung im Angebot entspräche, würden doch dadurch unzählige Möglichkeiten geschaffen, die publizierten Daten auf einfache elektronische Art und Weise zu kopieren und zu verschiedensten Zwecken, insbesondere auch kommerziellen, zu nutzen. Die Publikation des Adressbuches im Internet wäre mit den allgemeinen Zielen des Daten- und Persönlichkeitsschutzes für das Individuum nicht mehr in Einklang zu bringen. Ein Datenmissbrauch wäre jederzeit ohne grossen Aufwand möglich. Mit der Regelung im Aufenthaltsgesetz beschränkt sich die Zulässigkeit der Datenbekanntgabe klar auf Druckerzeugnisse klassischer Art, d.h. in Papierform, also entsprechend dem heutigen Adressbuch. Die Herausgabe des derzeitigen Inhaltes des Adressbuches via Internet oder ein anderes elektronisches Medium ist damit ausgeschlossen. Auszüge aus dem Handelsregister sind ohnehin, da im Wesentlichen öffentlich, im Internet bereits heute abrufbar bzw. gegen Entgelt voraussetzungslos bestellbar. Auch Teile des Grundbuches sind heute elektronisch unter bestimmten Voraussetzungen allgemein zugänglich.

§ 22 Bekanntgabe von Personendaten für einen nicht personenbezogenen Zweck

§ 15 DSG behandelt bisher die nicht personenbezogene Bearbeitung von Personendaten und die Bekanntgabe von Personendaten zu nicht personenbezogenen Zwecken an andere öffentliche Organe und an Private nicht sehr klar strukturiert in einem Paragraphen. Dieses Gesetz regelt nun die Bearbeitung von Personendaten zu einem nicht personenbezogenen Zweck durch das öffentliche Organ, das sie zu personenbezogenen Zwecken erhoben hat, in § 10 und die **Bekanntgabe von Personendaten zu nicht personenbezogenen Zwecken** an andere öffentliche Organe und an Private hier in § 22.

Grundsätzlich ist anzustreben, keine Personendaten, sondern bloss anonymisierte Daten herauszugeben. Es kann aber sein, dass der Bearbeitungszweck mit bereits anonymisierten Daten nicht erreicht werden kann, wenn etwa bei einem Forschungsprojekt Daten zu einzelnen Personen aus verschiedenen Quellen zueinander in Bezug gebracht werden müssen; das ist nicht mehr möglich, sobald der Personenbezug entfernt ist. Hier ist es erforderlich, «scharfe» Personendaten zur Verfügung zu stellen, allerdings mit der Auflage, dass sie zu anonymisieren oder zu pseudonymisieren sind, sobald es der Bearbeitungszweck erlaubt (Abs. 2 lit. a), und dass die Veröffentlichung so erfolgt, dass keine Rückschlüsse auf die betroffenen Personen mehr möglich sind (Abs. 2 lit. b). Pseudonymisierung bedeutet, dass die identifizierenden Angaben zur Person vom übrigen Datensatz getrennt aufbewahrt werden, wobei beide Teile mit einem Schlüsselcode versehen werden, der die Wiederherstellung der Originaldaten bei Bedarf ermöglicht.

[32] SG 122.200.

Neu eingefügt wird ein Abs. 3, der die Bekanntgabe von Personendaten (inkl. besonderen Personendaten) an das Statistische Amt regelt. Wo ein Statistikgesetz besteht, regelt dieses üblicherweise auch das Recht des kantonalen Statistischen Amtes, von anderen öffentlichen Organen für die Erstellung von kantonalen Statistiken die Bekanntgabe von Personendaten zu verlangen beziehungsweise die Pflicht der öffentlichen Organe, dem Statistischen Amt die verlangten Daten bekannt zu geben. Mangels eines Statistikgesetzes soll diese Regelung hier untergebracht werden. Aufgrund der anlässlich der Regierungs- und Verwaltungsreform 2009 bei den notwendigen Gesetzesänderungen eingeführten Sprachregelung wird im Gesetzestext das Statistische Amt nicht explizit erwähnt, sondern der Begriff „Das zuständige Departement„ verwendet. Dennoch soll die erwähnte Kompetenz nur dem Statistischen Amt zukommen.

Abs. 4: Bei der Bekanntgabe von Personendaten an private Datenempfängerinnen und -empfängern werden, weil diese dem Gesetz nicht unterstehen, in Abs. 4 zusätzliche Sicherungen eingebaut: Erstens dürfen ihnen nicht anonymisierte Personendaten nur zur Bearbeitung für Zwecke der *Wissenschaft und Forschung* bekanntgegeben werden (also nicht für Planung und Statistik), und müssen sie sich zusätzlich *verpflichten*, die Daten nicht für andere Zwecke zu bearbeiten (Abs. 4 lit. a), sie nicht an Dritte weiterzugeben (Abs. 4 lit. b) und für die Informationssicherheit zu sorgen (Abs. 4 lit. c). Das bekannt gebende öffentliche Organ hat – wie bei anderen Bekanntgaben auch – selber dafür zu sorgen, dass die gesetzlichen Voraussetzungen erfüllt sind. Zur Verstärkung der Verpflichtungserklärung nach Abs. 4 soll die privilegierte Person, die – anders als beim allgemeinen Zugang nach § 25 i.V.m. § 30 – Personendaten in nicht anonymisierter Form erhält, einer strafrechtlichen Sanktion unterliegen, falls sie die Personendaten vertragswidrig bearbeitet, sie also für andere (z.B. eigene) Zwecke bearbeitet oder sie an Dritte weitergibt (§ 52 Abs. 2).

Abs. 5: Auf Vorschlag des Appellationsgerichts soll neu ausdrücklich festgehalten werden, dass richterliche Behörden den in einem kantonalen Anwaltsregister nach dem Anwaltsgesetz des Bundes[33] eingetragenen Advokatinnen und Advokaten zum Zweck der Berufsausübung Urteile samt Personendaten unter den gleichen Voraussetzungen wie in Abs. 4 bekannt geben können. Hier geht es nicht um die Verfahren, in welchen diese Advokatinnen und Advokaten die Parteien vertreten – dort gelten die Prozessordnungen –, sondern um die Entscheide in anderen, rechtskräftig abgeschlossenen Gerichtsverfahren. Den Gerichten fehlen die Ressourcen für die (nachträgliche) Anonymisierung aller Entscheide, zumal die Beantwortung entsprechender Anfragen von Anwältinnen und Anwälten wegen laufender Fristen häufig zeitlich dringlich ist. Auf der anderen Seite unterstehen die eingetragenen Advokatinnen und Advokaten der Disziplinaraufsicht nach dem Bundes-Anwaltsgesetz, so dass eine Gewähr für die Einhaltung der Auflagen besteht.

§ 23 Grenzüberschreitende Bekanntgabe von Personendaten

Mit der Schengen/Dublin-Revision des Datenschutzgesetzes wurden Regeln für die **grenzüberschreitende Bekanntgabe von Personendaten** in § 14 Abs. 3 DSG eingefügt. § 23

[33] Art. 5 des Bundesgesetzes vom 23. Juni 2000 über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA, SR 935.61).

übernimmt diese Regelung. Lediglich lit. d wird analog zu § 21 Abs. 1 lit. c[34] und Abs. 2 lit. c formuliert, d.h. der Satz wird im Vergleich zur Formulierung gemäss der Schengen/Dublin-Revision umgestellt: Entweder liegt eine Einwilligung vor oder es wird – wenn nicht – geprüft, ob die Bekanntgabe im Interesse der betroffenen Person liegt und ihre Einwilligung in guten Treuen vorausgesetzt werden darf. Dieser neue Wortlaut nimmt die betroffene Person ernster als der alte: Hat sie eingewilligt, braucht nicht auch noch geprüft zu werden, ob die Datenbekanntgabe in ihrem Interesse liegt.

§ 24 Verzeichnis der Informationsbestände mit Personendaten

Abs. 1: Gemäss § 8 Abs. 1 DSG führen Kanton und Gemeinden ein zentrales Register der Datensammlungen, die dem Gesetz unterstehen. Diese Lösung leidet vor allem daran, dass das Datenschutzkontrollorgan, welches das Register führt (§ 28 lit. g DSG), in keiner Weise für die Vollständigkeit und Richtigkeit des Registerinhalts verantwortlich sein kann. Es ist auch vom durch die Assoziierung an Schengen/Dublin anwendbar werdenden Recht her keine zentrale Führung eines Registers erforderlich. Deshalb geht der Trend klar in Richtung dezentraler Verzeichnisse.[35] Der Kanton Basel-Landschaft hat bereits mit der Schengen/Dublin-Revision die Schaffung von **dezentralen Verzeichnissen** anstelle des zentralen Registers eingeführt. Dementsprechend sieht § 24 Abs. 1 neu vor, dass die verantwortlichen öffentlichen Organe (§ 6) ein vollständiges Verzeichnis über ihre Informationsbestände, die Personendaten enthalten, führen. Es wird bewusst nicht von «Personendatensammlungen» gesprochen, da dieser Begriff sonst im IDG nicht mehr verwendet wird.

Der Aufwand für die neu zur Verzeichnisführung verpflichteten Behörden wird gegenüber der heutigen Rechtslage (Meldepflicht) nicht verändert und kann zusätzlich durch IT-Unterstützung (Datenbanklösung für alle Dienststellen/Departementen, Zugänglichkeit übers Internet) reduziert werden. Für die Veröffentlichung der Verzeichnisse wird in § 55 Abs. 1 eine angemessene Übergangsfrist festgelegt.

Abs. 2: Die nach Abs. 1 geführten Verzeichnisse sind leicht zugänglich zu machen. Sie dienen als Grundlage für die Wahrnehmung der datenschutzrechtlichen Ansprüche – Recht auf Zugang zu den eigenen Personendaten (§ 26), Ansprüche auf Berichtigung (§ 27 Abs. 1 lit. a), Unterlassungs-, Beseitigungs- und Feststellungsansprüche (§ 27 Abs. 1 lit. b bis d) und Recht auf Sperrung (§ 28).

In der Vernehmlassung wurde mehrfach gefordert, dass die Dezentralisierung nicht zu einer Verschlechterung der Transparenz für die betroffenen Personen führen dürfe. Es ist – im Interesse der Bürgerfreundlichkeit wie auch aus verwaltungsökonomischen Gründen – anzustreben, die Verzeichnisse so einfach zugänglich zu machen, dass die interessierten Personen nicht bei jedem Organ vorstellig werden müssen. Die *Führung* der Verzeichnisse wird dezentralisiert, aber für die *Einsicht* soll eine für den Kanton bzw. für die Gemeinden je zentrale Web-Lösung angeboten werden, so dass Interessierte möglichst einfach zu den entsprechenden Verzeichnissen finden. Für EDV-mässig nicht besonders stark aufgerüstete Gemeinden kann die Web-Lösung durchaus aus einem Verzeichnis in PDF-Form bestehen.

---

34 Siehe dazu auch die Fussnote 31.

35 Vgl. z.B. § 13 Abs. 4 Informations- und Datenschutzgesetz ZH (LS 170.4).

Eine zentrale nicht-elektronische Einsichtsmöglichkeit zu schaffen ist nicht nötig, nachdem bisher die bestehende Möglichkeit nach Auskunft des Datenschutzbeauftragten praktisch nicht genutzt wurde.

Es wird mit der Formulierung «insbesondere durch öffentliche Datennetze» nicht verlangt, dass jedes einzelne dem Gesetz unterstellte öffentliche Organ (§ 3 Abs. 1: auch zum Beispiel Kirchgemeinden und Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist) eine entsprechende Website schaffen muss; es ist dem Regierungsrat und den Gemeinden überlassen festzulegen, wie die Veröffentlichung erfolgt, ob dezentral bei jedem öffentlichen Organ, halbzentral bei den Departementen oder zentral für den ganzen Kanton oder die ganze Gemeinde.

Abs. 3: Der erforderliche Inhalt der Verzeichnisse sowie die Ausnahmen von der Veröffentlichungspflicht sind einheitlich für alle öffentlichen Organe durch den Regierungsrat in einer Verordnung zu regeln. Die Regelung dürfte inhaltlich weitgehend mit dem bisher geltenden § 8 Abs. 2 und 3 DSG übereinstimmen, weshalb der Aufwand für die öffentlichen Organe sicher nicht grösser wird als bisher.

V. Informationszugangsrecht und andere Rechtsansprüche

Dieser Abschnitt fasst die verschiedenen **Rechtsansprüche** zusammen: den aus dem Öffentlichkeitsprinzip entspringenden Anspruch jeder Person auf Zugang zu Informationen einerseits (§ 25), die aus dem Datenschutzgesetz herrührenden Ansprüche der von behördlicher Datenbearbeitung betroffenen Personen anderseits (§§ 26-28).

§ 25 Zugang zu Informationen

Abs. 1: Entsprechend der Idee des Öffentlichkeitsprinzips soll jeder Person ohne Nachweis eines Interesses ein **Anspruch auf Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen** zukommen. Indem der Zugang «jeder Person» gewährt wird, garantiert das Öffentlichkeitsprinzip eine kollektive Information: Wird der Zugang zu einer amtlichen Information einer Person gewährt, ist er allen zu gewähren («access to one – access to all»). Dieser Anspruch wird hier festgeschrieben – mit zwei Einschränkungen: Erstens betrifft der Anspruch nur Informationen bei öffentlichen Organen im Sinne von § 3 Abs. 1 lit. a und b dieses Gesetzes, also nicht bei Privaten, denen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist und die nach § 3 Abs. 1 lit. c deswegen als öffentliche Organe gelten; in diesen Fällen ist das Zugangsgesuch auf die aufgabenübertragende Behörde zu richten. Zweitens beschlägt der Anspruch auf Zugang zu Informationen nicht Aufzeichnungen, die nicht fertig gestellt sind.[36] Dieser Ausschluss ist unter dem gleichen Aspekt wie der Schutz der freien Meinungs- und Willensbildung einer Behörde (vgl. unten zu § 29) zu beurteilen: Der Verwaltung muss erlaubt sein, sich vorerst möglichst ungestört eine Meinung zu bilden. So können auch Missverständnisse, Unklarheiten und andere Risiken vermieden werden, die sich aus der Veröffentlichung einer Information mit provisori-

[36] Vgl. auch Art. 5 Abs. 3 Bundesöffentlichkeitsgesetz (SR 152.3), § 3 Informations- und Datenschutzgesetz ZH (LS 170.4) zum Begriff Informationen (Satz 2).

schem Charakter ergeben könnten. Als Beispiele für nicht fertig gestellte Informationen können genannt werden: Ein handschriftlich oder elektronisch aufgezeichneter Text mit Streichungen oder Anmerkungen vor einer Schlusskorrektur, eine zusammenfassende Übersicht in Bearbeitung, eine provisorische Fassung eines Berichts, informelle Arbeitsnotizen, der Vorentwurf eines Textes usw. Die Bestimmung soll aber nicht dazu führen, dass Informationen dem Zugang entzogen werden, indem die Aufzeichnungen systematisch nicht fertig gestellt werden. Die in der Vernehmlassung vorgeschlagene Lösung, wonach die öffentlichen Organe Verfahren oder Fristen festzulegen haben, innerhalb derer die Aufzeichnungen fertig gestellt werden, ist aber im Verwaltungsalltag untauglich. Sollte ein solches systematisches Verzögern der Fertigstellung festgestellt werden, wäre eine aufsichtsrechtliche Anzeige an die vorgesetzte Stelle der richtige Weg.

Abs. 2: Während in hängigen Verfahren der Verfassungs- und Verwaltungsgerichtsbarkeit sowie der Zivil- und Strafrechtspflege das Informations- und Datenschutzgesetz nicht gilt (§ 2 Abs. 2 lit. b und c), fallen die **Verwaltungsverfahren und verwaltungsinternen Rekursverfahren** in den Geltungsbereich des Informations- und Datenschutzgesetzes. Für den Informationszugang während der Hängigkeit solcher Verfahren verweist das IDG auf die geltenden Normen; es gilt also weiterhin § 38 Abs. 2 OG, wonach insbesondere die (durch § 12 lit. b KV auch verfassungsrechtlich garantierten) Grundsätze der Akteneinsicht und des rechtlichen Gehörs zu gewährleisten sind.

§ 26 Zugang zu den eigenen Personendaten

Jede Person hat – wie nach § 19 Abs. 1 DSG – **Anspruch auf Zugang zu** den bei einem öffentlichen Organ vorhandenen **eigenen Personendaten**. Dieser Anspruch ist eines der Kernelemente des Grundrechts auf informationelle Selbstbestimmung.[37] Ausdrücklich hält dies die Charta der Grundrechte der Europäischen Union in Art. 8 Abs. 2 Satz 2 fest: «Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.» Der Anspruch bezieht sich auf zweierlei: Erstens auf die Auskunft, ob bei einem öffentlichen Organ über sie Personendaten vorhanden sind, und zweitens auf den Zugang zu diesen eigenen Personendaten. Obwohl das in der Formulierung der Vernehmlassungsvorlage («Anspruch auf Zugang zu den bei einem öffentlichen Organ vorhandenen eigenen Personendaten») mitverstanden war, wird es im neu vorgeschlagenen Gesetzestext noch ausgeführt. Der Zugang darf – wie das Recht auf Auskunft und Einsicht schon gemäss § 20 Abs. 1 DSG – nur eingeschränkt werden unter den Voraussetzungen von § 29 Abs. 1: Er ist ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere gesetzliche Geheimhaltungspflicht oder ein überwiegendes öffentliches oder privates Interesse entgegensteht, also beispielsweise aus überwiegenden Interessen einer Drittperson.[38]

[37] Art. 13 Abs. 2 BV (SR 101); § 11 Abs. 1 lit. j KV (SG 111.100).

[38] Wenn es sich überhaupt um «eigene Personendaten» handelt und nicht um Personendaten über jene Drittperson. Die Unterscheidung ist bei Dossiers mit mehreren Beteiligten (zum Beispiel Disziplinaruntersuchungen zu Vorfällen in einer Schule, wo mehrere Tatverdächtige beteiligt sind, bei der Betreuung von Familien durch einen Sozialdienst usw.) oft nicht einfach.

§ 27 Schutz der eigenen Personendaten

Abs. 1: Aus den §§ 21 und 22 DSG übernommen werden auch die folgenden **Rechtsansprüche**:

- auf **Berichtigung** unrichtiger Personendaten (lit. a),
- auf **Unterlassung** des widerrechtlichen Bearbeitens von Personendaten (lit. b),
- auf **Beseitigung** der Folgen widerrechtlichen Bearbeitens von Personendaten (lit. c) und
- auf **Feststellung** der Widerrechtlichkeit des Bearbeitens von Personendaten (lit. d).

Abs. 2: Die bisher in § 21 Abs. 2 und 3 DSG enthaltenen konkretisierenden Regelungen sind in die **Verordnung** zu übernehmen, nämlich die Regelungen, dass die Beweislast für die Richtigkeit der Daten beim öffentlichen Organ liegt und dass die betroffene Person vom öffentlichen Organ die Aufnahme einer Gegendarstellung verlangen kann, wenn nach der Natur der Daten weder die Richtigkeit noch die Unrichtigkeit von Personendaten bewiesen werden kann, insbesondere von solchen, die eine Wertung menschlichen Verhaltens enthalten.

§ 28 Sperrung der Bekanntgabe von Personendaten

Schliesslich ist aus § 13 DSG (in der Fassung der Schengen/Dublin-Revision) auch das **Recht auf Sperrung** der Bekanntgabe von Personendaten samt der Ausnahme ins Informations- und Datenschutzgesetz zu übernehmen. Im Vergleich zu jener Fassung wird die Bestimmung formell anders formuliert, was aber materiell nicht zu einem anderen Resultat führt: Statt ein (anscheinend) umfassendes Sperrrecht mit zwei Ausnahmen, die das behördliche Datenbearbeiten praktisch gleich wieder erlauben, wird neu präziser festgehalten, wo das Sperrrecht überhaupt besteht, nämlich dort, wo ein öffentliches Organ aufgrund einer spezialgesetzlichen Bestimmung Personendaten *an Private voraussetzungslos bekanntgeben* darf, was etwa der Fall ist bei den Einwohnerkontrollen[39]. Nicht darunter fallen somit die Fälle, in denen das öffentliche Organ die Daten aufgrund einer spezialgesetzlichen Bestimmung nicht bloss voraussetzungslos bekannt geben *kann*, sondern bekannt geben *muss*, weshalb die diesbezüglichen (alten) Ausnahmen von § 13 lit. a und b DSG nicht mehr nötig sind. Wenn also beispielsweise das Krankenversicherungsgesetz des Bundes die Leistungserbringer (also die öffentlichrechtlichen Spitäler ebenso wie Privatspitäler) dazu verpflichtet, den mit der obligatorischen Krankenpflegeversicherung betrauten Versicherern bestimmte Daten bekanntzugeben, dann ist das aus zweierlei Gründen kein Anwendungsfall für § 28: weil erstens eine gesetzliche Bekanntgabepflicht existiert und weil zweitens die Krankenkassen im KVG-Bereich Bundesorgane sind. Im Interesse der Rechtssicherheit wird neu verlangt, dass das Sperrbegehren schriftlich zu stellen ist.

---

[39] *[Bei Variante 1 in § 53 Ziff. 1]* § 12 DSG; vgl. dazu die Änderung des Aufenthaltsgesetzes gemäss § 53 Ziff. 1 (betreffend § 30 Abs. 3 und 4 Aufenthaltsgesetz).
[Bei Variante 2 in § 53 Ziff. 1] § 12 DSG; vgl. dazu die Änderung des Aufenthaltsgesetzes gemäss § 53 Ziff. 1 (betreffend § 30 Abs. 5 und 6 Aufenthaltsgesetz).

VI. Einschränkungen bei der Bekanntgabe von und beim Zugang zu Informationen

§ 29 Verweigerung oder Aufschub

Bereits in § 14 Abs. 1 DSG ist vorgesehen, dass die Bekanntgabe von Personendaten eingeschränkt oder mit Auflagen versehen werden kann. Dieser Vorbehalt muss auch weiterhin gelten, nicht nur für die Bekanntgabe von und den Zugang zu Personendaten, sondern generell für alle Informationen. Allerdings sollen die Voraussetzungen für die **Einschränkungen** präziser gefasst werden: Die Ausnahmen dürfen nicht allzu offen formuliert sein, sonst droht das Öffentlichkeitsprinzip unwirksam zu werden.

Abs. 1 hält den Grundsatz fest: Das öffentliche Organ hat die Bekanntgabe von oder den Zugang zu Informationen im Einzelfall ganz oder teilweise zu verweigern oder aufzuschieben, wenn eine besondere **gesetzliche Geheimhaltungspflicht** oder ein **überwiegendes öffentliches oder privates Interesse** entgegensteht. Was als entgegenstehende überwiegende öffentliche oder private Interessen in Frage kommt, zählen die Abs. 2 und 3 nicht abschliessend auf.[40] Aus Gründen der Rechtssicherheit und zur Vermeidung von Rekursverfahren werden überwiegende öffentliche Interessen beispielhaft aufgezählt. Eine nicht abschliessende Liste möglicher Zugangsbeschränkungen zu Informationen hat den Vorteil, dass sie erlaubt, den Besonderheiten des Einzelfalls sowie unvorhergesehenen Situationen Rechnung zu tragen. Dieser Vorteil überwiegt die Befürchtung, die Verwaltung könnte das Öffentlichkeitsprinzip über Gebühr einschränken. Für die effektive Tragweite des Öffentlichkeitsprinzips ist massgebend, welche Anforderungen an die überwiegenden Geheimhaltungsinteressen gestellt werden, und ob in der einzelfallbezogenen Interessenabwägung auch die öffentlichen oder privaten Interessen am Informationszugang berücksichtigt werden.

Die **besonderen gesetzlichen Geheimhaltungspflichten** waren schon in § 14 Abs. 2 und § 15 Abs. 2 lit. a DSG bei der Bekanntgabe von Personendaten vorbehalten. Die Einführung des Öffentlichkeitsprinzips bezweckt nicht, sie aufzuheben. Als solche Geheimhaltungspflichten erscheinen im kantonalen Recht etwa das Steuergeheimnis[41], die Schweigepflicht der Sozialhilfeorgane[42], das Wahl- und Abstimmungsgeheimnis[43] oder andere gesetzliche Vorschriften im Bundesrecht[44]. Diese besonderen gesetzlichen Geheimhaltungspflichten werden durch den Erlass des IDG nicht angetastet, und die in der Vernehmlassung geforderte Schaffung eines öffentlichen Steuerregisters würde nach geltendem Verfassungsrecht schon an § 75 Abs. 3 KV scheitern, wonach die Vertraulichkeit der Steuerdaten gewährleistet bleibt.

---

40 Wie etwa auch die entsprechenden Regelungen in den Kantonen Bern, Genf, Solothurn und Zürich.

41 § 138 Steuergesetz (SG 640.100).

42 § 28 Sozialhilfegesetz (SG 890.100).

43 § 43 Abs. 3 KV (SG 111.100).

44 Etwa die Schweigepflicht der Opferhilfestellen (Art. 4 des Opferhilfegesetzes des Bundes, OHG, SR 312.5) oder der Personen, die an der Durchführung sowie der Kontrolle oder der Beaufsichtigung der Durchführung der Bundessozialversicherungsgesetze beteiligt sind (Art. 33 des Bundesgesetzes vom 6. Oktober 2000 über den Allgemeinen Teil des Sozialversicherungsrechts, ATSG, SR 830.1).

Abs. 2 umschreibt nicht abschliessend, in welchen Fällen **öffentliche Interessen** gegenüber den Interessen an der Bekanntgabe von oder am Zugang zu Informationen überwiegen können. In der Vernehmlassung wurde vorgeschlagen, anstelle der Abs. 2 und 3 in einer Verordnung konkret nicht-öffentliche Akte zu bezeichnen, weil sonst der Ermessensspielraum so gross sei, dass das Öffentlichkeitsprinzip unterlaufen werden könne (SP). Die Gemeinde Riehen fände es hilfreich, wenn die öffentlichen Organe verpflichtet würden, in Zusammenarbeit mit dem zuständigen Archiv eine entsprechende Auflistung von grundsätzlich nicht-öffentlichen Aufzeichnungen (z.B. Personaldossiers, spezielle Geschäftsleitungsdossiers, Sozialhilfedossiers usw.) bzw. von öffentlichen Aufzeichnungen vorzunehmen. Diese beispielhafte Aufzählung zeigt aber: Keine Regelung kommt ohne Generalklauseln oder unbestimmte Rechtsbegriffe aus, und mit jeder scheinbar konkreteren Regelung würden vermutlich generell weite Bereiche ausgeschlossen werden, die – bei der Abwägung im Einzelfall – durchaus öffentlich sein könnten. Es ist aber davon auszugehen, dass sich in der Praxis «Faustregeln» entwickeln werden, die aber immer im Lichte der konkretisierenden Ausführungen der Absätze 2 und 3 überprüft werden können.

In folgenden Fällen können öffentliche Interessen gegenüber den Interessen an der Bekanntgabe von oder am Zugang zu Informationen überwiegen:

- **Gefährdung der Sicherheit des Staates oder der öffentlichen Sicherheit** (lit. a): Diese Ausnahme ermöglicht es, Massnahmen zum Erhalt der Handlungsfähigkeit der Regierung in ausserordentlichen Lagen oder zur Sicherstellung der wirtschaftlichen Landesversorgung, oder Informationen, deren Zugänglichmachung zur Beeinträchtigung der Sicherheit wichtiger Infrastrukturen oder gefährdeter Personen führen würde, geheim zu halten.

- **Beeinträchtigung der Aussenbeziehungen** zu einem anderen Kanton, zum Bund oder zum Ausland (lit. b): Beeinträchtigt die Bekanntgabe von Informationen das Verhältnis zu einem anderen Kanton, zum Bund oder zum Ausland, besteht ein überwiegendes öffentliches Interesse an deren Geheimhaltung. Nach Ansicht des Bundesrates[45] ermöglicht diese Ausnahme zudem, der anerkannten Staatenpraxis Rechnung zu tragen, nach der Informationen, die ein ausländischer Staat oder eine internationale Organisation als intern oder vertraulich übergibt, vom Empfängerstaat grundsätzlich nur mit Zustimmung des Absenders an die Öffentlichkeit weiter gegeben werden. Unter diesen Umständen erscheint eine Einschränkung des Zugangs gerechtfertigt, da bei Bekanntgabe der Information damit gerechnet werden muss, dass künftig entsprechende Informationen nicht mehr bekannt gegeben werden.

- **Beeinträchtigung des freien Meinungs- und Willensbildungsprozesses** der öffentlichen Organe (lit. c): Diese Einschränkung soll verhindern, dass öffentliche Organe – nicht nur dasjenige, das die Informationen zugänglich machen soll – durch eine verfrühte Bekanntgabe von Informationen (beispielsweise Arbeitspapiere, Entwürfe, Gutachten, Stellungnahmen) während eines Entscheidungsprozesses unter allzu starken Druck der Öffentlichkeit geraten, wodurch die freie Meinungs- und Willensbildung verhindert werden könnte. Die frühzeitige Bekanntgabe bestimmter Positionen kann je

[45] Vgl. die Botschaft des Bundesrates zum Bundesöffentlichkeitsgesetz (Bundesblatt 2003 2011).

nach den Umständen die öffentliche Auseinandersetzung vorzeitig blockieren. Generell ist festzuhalten, dass nicht jede noch so geringe Beeinträchtigung eine Verweigerung zu begründen vermag. Verwaltungsinterne Mitberichte sollen aber weder vorgängig noch nachträglich dem Zugang offen stehen: Würden solche Mitberichte öffentlich, würde das Kollegialitätsprinzip erheblich gefährdet werden.

- **Beeinträchtigung der Position in Verhandlungen** (lit. d): Keine Verhandlung kann wirkungsvoll geführt werden, wenn eine Partei ihre Karten uneingeschränkt offen legen muss. Würde die Bekanntgabe von Informationen die Position in Verhandlungen beeinträchtigen, muss darauf verzichtet werden. Dem Zugang entzogen sind allerdings nur Informationen, deren Bekanntgabe tatsächlich die Verhandlungsposition des betreffenden öffentlichen Organs schwächen würde, denn nur dort kann ein schützenswertes Geheimhaltungsinteresse angenommen werden. Im Gegensatz zum DSG-Bund ist lediglich die Rede von Verhandlungen anstatt von Vertragsverhandlungen, da im Einzelfall nicht immer ersichtlich ist, ob es um Vertragsverhandlungen geht. Zudem sind mit «Verhandlungen» auch vorvertragliche Verhandlungen gemeint.

- **Beeinträchtigung der zielkonformen Durchführung konkreter behördlicher, insbesondere polizeilicher Massnahmen** (lit. e): Diese Einschränkung ermöglicht die Geheimhaltung von Informationen, die der Vorbereitung konkreter behördlicher Massnahmen wie Untersuchungs-, Kontroll- oder Aufsichtsmassnahmen und Inspektionen dienen. Müssten solche Informationen auf Gesuch hin bekannt gegeben werden, wäre die Massnahmenumsetzung in vielen Fällen zumindest in Frage gestellt. Zu denken ist insbesondere etwa an polizeitaktische Informationen und Strategien, an die Einsatzdispositive für Einsätze der Polizei im sogenannten unfriedlichen Ordnungsdienst, an die periodischen Testkäufe zur Kontrolle des Alkohol- oder Tabakverkaufs an Jugendliche unter 16 Jahren, an den Einsatzplan für Verkehrskontrollen oder für Kontrollen bei Alkoholverkaufsstellen. In der Vernehmlassung wurde diese Bestimmung als vage und unbestimmt gerügt (SP, BastA!, DJS). Es liegt wohl in der Natur der Sache, dass generell-abstrakte Formulierungen mit unbestimmten Gesetzesbegriffen die konkret notwendige Interessenabwägung eben nicht vorwegnehmen und auch nicht eng einfassen kann, da die Interessenabwägung ja eben gerade offen bleiben soll. Selbst die Einschränkung auf eine «erhebliche Beeinträchtigung» könnte die Wertung im Einzelfall nicht ersetzen.

Abs. 3 umschreibt nicht abschliessend, in welchen Fällen **private Interessen** gegenüber den Interessen an der Bekanntgabe von oder am Zugang zu Informationen überwiegen können:

- wenn die Bekanntgabe von oder der Zugang zu Informationen den Schutz der **Privatsphäre** beeinträchtigen würde (lit. a). Der Begriff «Privatsphäre» entstammt der privatrechtlichen Dreisphärentheorie, ist hier aber im Sinne des grundrechtlichen Schutzes der Persönlichkeit/auf informationelle Selbstbestimmung zu verstehen. Insbesondere relevant ist ein solcher Schutz im Hinblick auf § 30, da Sachverhalte denkbar sind, bei welchen die Anonymisierung zum Persönlichkeitsschutz nicht ausreichen würde (z.B. psychiatrische Gutachten in heiklen abgeschlossenen Verwaltungs- oder in Strafverfahren). Bei den **besonderen Personendaten** i.S.v. § 3 Abs. 4 ist immer davon aus-

zugehen, dass das private Interesse der betroffenen Personen gegenüber dem Interesse am Zugang überwiegt; das ist beispielsweise von Bedeutung bei Gerichtsakten zu Verfahren der Unfall-, Kranken- und Invalidenversicherung (§ 3 Abs. 4 lit. a Ziff. 2: Angaben über die Gesundheit), der Sozialhilfe (§ 3 Abs. 4 lit. a Ziff. 3: Angaben über Massnahmen der sozialen Hilfe) oder des Strafrechts (§ 3 Abs. 4 lit. a Ziff. 4: Angaben über administrative oder strafrechtliche Verfolgungen und Sanktionen). Privatinteressen können aber nicht nur bei besonderen Personendaten überwiegen und die Zugangsgewährung verbieten: Auch bei «gewöhnlichen» Personendaten kann das der Fall sein; zu denken ist etwa an Personendaten aus Urteilen in familienrechtlichen Gerichtsverfahren.

- wenn durch die Bekanntgabe von oder den Zugang zu Informationen **Berufs-, Fabrikations- oder Geschäftsgeheimnisse** offenbart oder Urheberrechte verletzt würden (lit. b): Berufs-, Geschäfts- und Fabrikationsgeheimnisse müssen trotz Öffentlichkeitsprinzip geheim gehalten werden können. Solche Geheimnisse können einem öffentlichen Organ etwa in Submissionsverfahren oder im Rahmen einer gesetzlichen Kontrollaufgabe zur Kenntnis gelangen. Das Vertrauen, das durch Berufsgeheimnisse geschützt werden soll, darf nicht verletzt werden. Der Wettbewerb zwischen Marktteilnehmern darf durch das Informationszugangsrecht nicht verzerrt werden, weshalb Fabrikations- und Geschäftsgeheimnisse zu schützen sind. Ebenso kann die Herausgabe von copyright-geschützten Werken Urheberrechte verletzen. Es ist allerdings darauf hinzuweisen, dass nicht jedes Copyright den Zugang verhindern kann. Wenn sich die Verwaltung das Recht, z.B. ein Gutachten zu verwenden, übertragen lässt, kann mit dem vielleicht auf dem Gutachten noch vermerkten © der Zugangsanspruch nicht abgewehrt werden (aber vielleicht mit den Ausnahmen des Meinungsbildungsprozesses oder der Beeinträchtigung von Verhandlungen).

- wenn die Bekanntgabe von oder der Zugang zu Informationen verlangt wird, die dem öffentlichen Organ von Dritten **freiwillig mitgeteilt** worden sind und deren **Geheimhaltung** es **zugesichert** hat (lit. c). Private wären kaum mehr bereit, den Behörden freiwillig Informationen zu liefern, wenn diese Informationen trotz Zusicherung der Geheimhaltung jedermann bekannt gegeben werden könnten. Allerdings bleibt – wie heute schon – die grundsätzliche Frage auch weiterhin unbeantwortet, inwiefern ein öffentliches Organ überhaupt verbindlich Geheimhaltung zusagen kann.

Abs. 4: Der Zugang zu den eigenen Personendaten kann ausserdem eingeschränkt werden, wenn der betroffenen Person durch die Zugangsgewährung offensichtlich ein schwerer Nachteil droht (sog. Offenbarungsschaden). In der Vernehmlassung wurde die aus dem geltenden § 20 Abs. 1 DSG übernommene Regelung als paternalistisch bezeichnet. Es versteht sich von selbst, dass diese Ausnahme nur sehr restriktiv angewandt werden darf, was durch die Begriffe «offensichtlich» und «schwerer Nachteil» unterstrichen wird. Eine Alternative wäre die Übernahme der Regelung aus Art. 8 Abs. 3 DSG-Bund, wonach Daten über die Gesundheit der betroffenen Person über eine Ärztin oder einen Arzt ihres Vertrauens offengelegt werden können.

Die von SP, BastA! und DJS in der Vernehmlassung verlangte generelle Umkehrung des Zugangssystems – Zugang gewähren, wenn auch zu anonymisierten Personendaten, und

nur Verweigerung des Zugangs, falls dies nicht möglich ist – wäre aus Sicht der betroffenen Personen mit grossen Risiken verbunden. Am Beispiel von sehr sensitiven Personen in psychiatrischen Gutachten etwa in Sozialversicherungs- oder strafgerichtlichen Dossiers illustriert: Es kann in solchen Fällen mit einer Anonymisierung nicht sicher ausgeschlossen werden, dass Personen dank einem Zusatzwissen die betroffene Person identifizieren können und damit in Kenntnis von äusserst sensitiven Informationen kommen. Deshalb kann nicht die Anonymisierung die Regel und der Entscheid über die ganze oder teilweise Einschränkung des Zugangs ausnahmsweise die Alternative sein. Eine Umkehr ist aber auch nicht nötig, weil – das ist schliesslich nochmals ausdrücklich festzuhalten – alle *Einschränkungen nur zulässig* sind, wenn und soweit die tangierten öffentlichen oder privaten Geheimhaltungsinteressen das Interesse am Informationszugang respektive an der Transparenz der Verwaltung überwiegen (Abs. 1). Wo den Geheimhaltungsinteressen mit einer teilweisen Einschränkung Genüge getan werden kann, darf nicht der Zugang insgesamt verweigert werden. Eine teilweise Einschränkung des Zugangs kann beispielsweise durch Abdeckung von geheimzuhaltenden Teilen erfolgen – die Lösung, die für Personendaten ausdrücklich vorgeschrieben wird (§ 30).

§ 30 Anonymisierung von Personendaten

Eine der grossen Herausforderungen bei der Einführung des Öffentlichkeitsprinzips ist die Austarierung zwischen den hinter dem Öffentlichkeitsprinzip stehenden Interessen einerseits und den Interessen der Personen, über welche öffentliche Organe Daten bearbeiten, anderseits. Es ist verfassungsrechtlich unbestreitbar, dass der Schutz der Grundrechte der von behördlichem Datenbearbeiten betroffenen Person dazu führen *muss*, dass der Zugang zu Personendaten eingeschränkt werden muss – es geht wie gesagt um eine transparente Verwaltung, nicht um die gläserne Bürgerin oder den gläsernen Bürger.

Abs. 1: Das geschieht einerseits dadurch, dass der Zugang zu den gewünschten Personendaten über Drittpersonen gemäss § 29 Abs. 1 und 3 aus überwiegenden privaten Interessen ganz oder teilweise zu verweigern ist. Wo das nicht schon der Fall ist, sind zum Schutz der Grundrechte der betroffenen Drittpersonen die Personendaten **vor der Zugangsgewährung** zu **anonymisieren** (zum Begriff der Anonymisierung vgl. die Erläuterungen zu § 14 Abs. 2). Eine übereinstimmende Lösung hat der Bund getroffen: Art. 9 Bundesöffentlichkeitsgesetz gewährt grundsätzlich Zugang zu Informationen, legt aber fest, dass amtliche Dokumente, welche Personendaten enthalten, nach Möglichkeit zu anonymisieren sind; ist dies nicht möglich, richtet sich die Bekanntgabe nach den Regeln des Datenschutzgesetzes.

Abs. 2: Der Zugang zu **Personendaten über Drittpersonen in nicht anonymisierter Form** – für den Fall, dass die gesuchstellende Person nicht anonymisierte Personendaten erhalten will oder die Anonymisierung nicht möglich ist – richtet sich wie im Bund nach den datenschutzrechtlichen Regeln über die Bekanntgabe von Personendaten, also nach den §§ 21 ff. Eine Bekanntgabe von Personendaten ist demnach zulässig aufgrund einer gesetzlichen Grundlage, wenn es zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist oder mit der Einwilligung der betroffenen Person (nach § 21 Abs. 1 bzw. – für die Bekanntgabe von besonderen Personendaten – nach den qualifizierten Voraussetzungen von § 21 Abs. 2).

VII. Verfahren auf Zugang zu Informationen

Ein wesentliches Element für die erfolgreiche Implementierung des Öffentlichkeitsprinzips ist das Verfahren. Ein kompliziertes Verfahren vermag auf der einen Seite Gesuchstellerinnen und Gesuchsteller nicht zufrieden zu stellen, und auf der anderen Seite erhöht es auch den Aufwand auf Verwaltungsseite. Es stellt sich die grundsätzliche Frage, ob nur ein **einfaches Zugangsverfahren** vorgesehen oder zusätzlich die Möglichkeit eines **Schlichtungsverfahrens** geschaffen werden soll.

Wie der Bund[46] und ein Teil der Kantone[47] sieht der Gesetzesentwurf ein **Schlichtungsverfahren** vor. Es gelangt zur Anwendung, wenn das um Informationszugang ersuchte öffentliche Organ beabsichtigt, das Gesuch teilweise oder vollständig abzuweisen. In diesem Fall hat die gesuchstellende Person die Möglichkeit, innert eines Monats die Durchführung des Schlichtungsverfahrens zu verlangen. Das Schlichtungsverfahren ist allerdings nicht obligatorisch, sondern es ist der gesuchstellenden Person freigestellt, ob sie es beanspruchen will oder nicht. Mit einem erfolgreichen Schlichtungsverfahren können zeit- und kostenintensive Rechtsmittelverfahren vermieden werden. Wie viele Schlichtungsverfahren durchzuführen sein werden, kann nicht vorausgesagt werden. Immerhin kann aus der Erfahrung in Kantonen mit dem Öffentlichkeitsprinzip, wonach die Einführung des Prinzips keine Flut von Informationszugangsgesuchen verursacht hat, auch geschlossen werden, dass auch nicht viele Schlichtungsverfahren durchgeführt werden müssen. Sollte sich diese Erwartung nicht bewahrheiten, wäre die Zuteilung von zusätzlichen Ressourcen bei der Ombudsstelle zu prüfen. Denn wenn die Verfahren nicht speditiv durchgeführt werden können, wird die Gefahr von Rechtsmittelverfahren eher zu- als abnehmen.

Ein zweites entscheidendes Element ist die **Gebührenordnung**. Die freizügigste Zugangsregelung schafft nicht wirklich Transparenz, wenn der Zugang durch eine prohibitive Gebührenregelung praktisch vereitelt wird.[48] Wenn die Einführung des Öffentlichkeitsprinzips zu mehr Vertrauen in die staatlichen Organe führen soll, muss der Zugang grundsätzlich kostenlos sein. Nur in aufwändigen Verfahren, für die Anfertigung von Kopien und sonstigen Datenträgern und dort, wo sich Informationen für eine gewerbliche Nutzung eignen, darf vom Prinzip der Kostenlosigkeit abgewichen werden (§ 37).

§ 31 Gesuch

Abs. 1 hält fest, dass das Verfahren um Zugang zu Informationen gemäss §§ 25 und 26 mit einem hinreichend genau formulierten **Gesuch** über die gewünschte Information eingeleitet wird. Das Gesuch kann mündlich oder schriftlich (dies erscheint v.a. bei komplexen Sachverhalten im Interesse einer effizienten Abwicklung angebrachter) gestellt werden. Es muss,

---

46 Art. 13 Bundesöffentlichkeitsgesetz (SR 152.3).

47 § 36 Informations- und Datenschutzgesetz SO; § 37 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen AG (SAR 150.77); Loi sur l'information VD (Verweis auf Arrêté concernant le bureau cantonal de médiation administrative) (RSV 170.21).

48 Grundsätzlich keine Gebühren werden – wie in den USA, in Frankreich und in Schweden – im Kanton Aargau erhoben (§ 40 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen AG, SAR 150.700). Grundsätzlich gebührenpflichtig sind die Verfahren im Bund (Art. 17 Abs. 1 Bundesöffentlichkeitsgesetz, SR 152.3) und im Kanton Zürich (§ 29 Abs. 1 Informations- und Datenschutzgesetz ZH, LS 170.4).

da das Gesetz den Anspruch auf Zugang zu Informationen voraussetzungslos gewährt, nicht begründet werden.

Abs. 2: Eine Sonderregelung besteht für den **Zugang zu den eigenen Personendaten**. Hier muss die Identität der gesuchstellenden Person zweifelsfrei festgestellt werden, was entweder schon gegeben ist, weil die zuständige Sachbearbeiterin oder der zuständige Sachbearbeiter die Person kennt (wie zum Beispiel der Vormund das Mündel kennt), oder durch die Vorlage eines amtlichen Ausweises erfolgen kann. Eine Stellvertretung ist deshalb nicht ausgeschlossen: In diesem Fall braucht es erstens einen Identitätsnachweis der vollmachtgebenden Person, die Zugang zu den eigenen Personendaten verlangt (Ausweiskopie zur Vollmacht), und zweitens muss sich die bevollmächtigte Person vor der Zugangsgewährung identifizieren.

§ 32 Prüfung

Das öffentliche Organ hat das Gesuch zu prüfen.

Abs. 1: Bezieht sich das Gesuch ausschliesslich auf **Informationen, die bereits öffentlich sind** und auf angemessene Weise zur Verfügung stehen – etwa weil sie im Rahmen der Informationstätigkeit von Amtes wegen gemäss § 20 schon öffentlich zugänglich gemacht worden und beispielsweise auf der Website des Kantons oder einer Gemeinde abrufbar sind –, so tritt das öffentliche Organ unter Verweis auf die Quelle nicht auf das Gesuch ein. In diesem Sinne ist Eintretensvoraussetzung, dass sich das Gesuch auf nicht bereits veröffentlichte und angemessen zugängliche Informationen bezieht.

Abs. 2: Sobald Interessen von Drittpersonen (im Sinne von § 29 Abs. 3) oder von anderen öffentlichen Organen (im Sinne von § 29 Abs. 2) betroffen sind, hat das öffentliche Organ **rechtliches Gehör** zu gewähren und den betroffenen Personen oder Organen Gelegenheit zur **Stellungnahme** zu geben, ausser wenn es auch ohne Stellungnahme klar ist, dass der Zugang ganz oder teilweise verweigert werden muss, und setzt dafür eine angemessene Frist. Ohne (externe) Stellungnahme berücksichtigt das öffentliche Organ die Einschränkungen durch besondere gesetzliche Geheimhaltungsvorschriften oder aufgrund «seiner» öffentlichen Interessen.

§ 33 Entscheid

Abs. 1: Ergibt die Prüfung, dass der Gewährung des verlangten Zugangs zu Informationen nichts entgegensteht, gewährt das öffentliche Organ den **Zugang** (zur Form der Zugangsgewährung vgl. § 35).

Abs. 2: Wenn das öffentliche Organ aufgrund seiner Prüfung des Gesuchs oder aufgrund der nach § 32 Abs. 2 eingeholten Stellungnahmen in Betracht zieht, das Gesuch ganz oder teilweise abzuweisen, dann hat es dies der gesuchstellenden Person **mitzuteilen**.

Abs. 3: Wenn das öffentliche Organ in Betracht zieht, dem Gesuch entgegen den nach § 32 Abs. 2 eingeholten Stellungnahmen zu entsprechen, dann hat es dies den betroffenen Drittpersonen oder den betroffenen anderen öffentlichen Organen **mitzuteilen**.

Abs. 4: Mit der Mitteilung im Sinne der Absätze 2 und 3 beginnt eine dreissigtägige Frist zu laufen. Innert dieser Frist können einerseits die Person, deren Gesuch nicht entsprochen werden soll, oder die Drittperson, entgegen deren Stellungnahme dem Gesuch entsprochen werden soll, entweder beim öffentlichen Organ den Erlass einer **anfechtbaren Verfügung** (lit. a) oder bei der Ombudsstelle die Durchführung eines **Schlichtungsverfahrens** verlangen (lit. b). Diese Möglichkeiten stehen einem anderen öffentlichen Organ nicht offen; es ist Sache des um Zugang ersuchten Organs, öffentliche Interessen, die einer Zugangsgewährung entgegenstehen, in seinem Entscheid angemessen zu berücksichtigen. Allenfalls kann das andere öffentliche Organ, entgegen dessen Stellungnahme dem Gesuch entsprochen werden soll, die nächsthöhere gemeinsame vorgesetzte Instanz anrufen.

§ 34 Schlichtungsverfahren

Abs. 1: Die Durchführung des **Schlichtungsverfahrens** obliegt der Ombudsstelle, falls ein solches nach § 33 Abs. 4 lit. b von der gesuchstellenden Person und/oder einer Drittperson verlangt wird. In der Vernehmlassungsvorlage war noch vorgesehen, dass die oder der Informationszugangs- und Datenschutzbeauftragte das Schlichtungsverfahren durchführen soll. Zu Recht wurde in verschiedenen Vernehmlassungen geltend gemacht, dass die oder der Informationszugangs- und Datenschutzbeauftragte nicht die geeignete Instanz dafür ist (Gemeinde Riehen, SP, DJS), weil er/sie vorher allenfalls das öffentliche Organ und die betroffene Person schon beraten hat (§ 45 lit. c und d) und nachher die Anwendung der Bestimmungen über den Umgang mit Informationen durch das öffentliche Organ zu kontrollieren hat (§ 45 lit. a). Damit fehlt ihr/ihm die erforderliche Neutralität im Verfahren. Wenn an der Einrichtung eines Schlichtungsverfahrens festgehalten werden soll, dann drängt es sich auf, die Ombudsstelle mit dessen Durchführung zu betrauen, weil nicht eine neue Schlichtungsstelle (wie etwa die staatliche Schlichtungsstelle für Mietstreitigkeiten) eingerichtet werden soll.

Die Anrufung der Schlichtungsinstanz hat schriftlich zu erfolgen. Aus dem Begehren muss hervorgehen, dass sich die Ombudsstelle mit der Angelegenheit befassen soll. Die Frist ist eingehalten, wenn das schriftliche Schlichtungsbegehren innert 30 Tagen nach Empfang der Mitteilung des öffentlichen Organs eingereicht wird. Der Erlass einer Verfügung schliesst aber die Durchführung eines Schlichtungsverfahrens aus, weil dann offensichtlich eine betroffene Partei nicht schlichtungsbereit ist. Kommt im Schlichtungsverfahren eine Einigung zustande, so ist damit das Verfahren erledigt (Abs. 2). Kommt keine Einigung zustande, gibt die Ombudsstelle eine Empfehlung an das öffentliche Organ ab (Abs. 3); die nach § 33 Abs. 4 berechtigten Personen können den Erlass einer anfechtbaren Verfügung und gegebenenfalls per Rekurs eine Überprüfung verlangen (vgl. §§ 41 ff. OG) oder die Nicht-Erledigung des Verfahrens (ausdrücklich oder formlos) akzeptieren.

§ 35 Gewährung des Zugangs

Abs. 1: Die **Zugangsgewährung** erfolgt, indem die Informationen schriftlich, in Form von Kopien oder auf Datenträgern ausgehändigt werden (lit. a). Wenn die gesuchstellende Person einverstanden ist, kann ihr auch vor Ort Einsicht in die Informationen gewährt oder die Information mündlich mitgeteilt werden (lit. b). Werden Informationen vor Ort eingesehen, untersagt der Gesetzesentwurf nicht, dass die gesuchstellende Person sie selber vervielfäl-

tigt, etwa handschriftlich abschreibt, fotografiert, fotokopiert, scannt oder auf andere Weise eine Kopie anfertigt. Stellt die Verwaltung den Einsichtnehmenden Kopierapparate zur Verfügung, ist sie gestützt auf § 37 berechtigt, für deren Benutzung Gebühren zu erheben.

Abs. 2: Wurde das Zugangsgesuch mündlich gestellt, dann hat das öffentliche Organ im Interesse einer rationellen Erledigung auch ohne das Einverständnis der gesuchstellenden Person das Recht, die Informationen ebenfalls mündlich mitzuteilen.

§ 36 Fristen

Da der Gehalt der Information von deren Aktualität lebt, darf das Verfahren nicht verzögert werden. Ausländische Beispiele zeigen, dass für die seriöse Behandlung von Gesuchen zwischen 15 Tagen und vier Wochen benötigt werden. Aus diesem Grund sieht das Gesetz eine dreissigtägige **Frist** ab Gesuchseingang vor. Innert dieser Frist hat das öffentliche Organ

- entweder der gesuchstellenden Person **Zugang** zu gewähren (lit. a),
- ihr eine **Mitteilung** im Sinne von § 33 Abs. 2 (Abweisung des Gesuches wird in Betracht gezogen) zukommen zu lassen (lit. b), oder
- ihr, falls die Frist nicht eingehalten werden kann, unter Angabe der Gründe **mitzuteilen**, bis wann der Entscheid vorliegen wird (lit. c).

Eine Fristverlängerung nach lit. c kann etwa nötig werden, wenn Interessen von Drittpersonen oder anderen öffentlichen Organen betroffen sind und nach § 32 Abs. 2 deren Stellungnahmen einzuholen sind. Die vom öffentlichen Organ gemäss lit. c zu nennende zweite Frist muss angemessen sein; andernfalls kann sich die gesuchstellende Person wegen Rechtsverzögerung beschweren. Allenfalls muss es dem öffentlichen Organ möglich sein, diese zweite Frist nochmals zu verlängern, da es rechtlich keine Handhabe hat, die nach § 32 Abs. 2 gesetzte Frist gegenüber Privaten oder einem anderen öffentlichen Organ durchzusetzen.

§ 37 Gebühren

Abs. 1: Für das Verfahren auf Zugang zu Informationen nach § 25 werden in der Regel **keine Gebühren** erhoben. Soll das Öffentlichkeitsprinzip sein Ziel erreichen, dürfen nicht über Gebühren hohe Hürden aufgestellt werden. Allerdings gilt die Kostenlosigkeit nicht ausnahmslos.

Abs. 2: Eine angemessene Gebühr nach Aufwand kann erhoben werden:

- bei **aufwändigen Verfahren**, insbesondere bei komplizierten Verhältnissen oder bei umfangreichen Anonymisierungen von Informationen (lit. a), und
- für die Anfertigung v**on Kopien** oder sonstigen Datenträgern (lit. b).

Wird einer Person Zugang zu den eigenen Personendaten (§ 26) gewährt, dürfen in keinem Fall Gebühren erhoben werden. Nur der Vollständigkeit halber sei darauf hingewiesen, dass

die Bekanntgabe von Personendaten an Private zu einem nicht personenbezogenen Zweck nach § 20 Abs. 4 (Wissenschaft und Forschung) nicht in den Geltungsbereich von § 35 betreffend Gebühren für den Zugang zu Informationen fällt, weshalb dafür auch nicht nach Abs. 2 eine Gebühr erhoben werden darf.

Als nicht aufwändig im Sinne von Abs. 2 lit. a gilt ein Aufwand von unter einer Stunde, wie es bisher schon der Praxis entspricht.

Abs. 3: Es darf nicht sein, dass das öffentliche Organ einen grossen Aufwand (im Sinne von Abs. 2 lit. a) generiert und hinterher der gesuchstellenden Person einfach die Rechnung zustellt (zum Beispiel die verlangten Informationen per Nachnahme zustellt[49]). Aus diesem Grund ist die gesuchstellende Person **auf die erheblichen Kostenfolgen hinzuweisen**, *bevor* das öffentliche Organ den entsprechenden Aufwand treibt; damit kann die gesuchstellende Person ihr Gesuch zurückziehen oder – in Kenntnis der Kostenfolge – daran festhalten. Auf Verlangen ist die Mitteilung in eine Verfügung zu kleiden, welche dann von der gesuchstellenden Person angefochten werden kann.[50] Dem öffentlichen Organ ist es unbenommen, vor der weiteren Gesuchsbearbeitung einen Kostenvorschuss zu verlangen; unter Umständen empfiehlt sich das sogar, weil mit der Reaktion der gesuchstellenden Person darauf ihr Wille, am Gesuch festzuhalten oder es zurückzuziehen, klar zum Ausdruck kommt. Diese Regelung ist eine Ausnahme von der Regelung von § 14a der Verordnung über die Verwaltungsgebühren, welche einen Kostenvorschuss nur in «besonderen Fällen» zulässt.[51] Sie ist jedoch zulässig, denn die Aufzählung in dieser Bestimmung ist nicht abschliessend.

Abs. 4: Wie erwähnt, wird der Zugang zu Informationen voraussetzungslos gewährt. Es ist durchaus möglich, dass solche Informationen auch zu **kommerziellen Zwecken** verwendet werden (zum Beispiel geographische Daten, die der Produktion von topographischen Karten dienen, oder statistische Daten für Marktuntersuchungen). Lässt sich aus den zugänglich gemachten Informationen ein wirtschaftlicher Nutzen ziehen, ist es sachlich nicht mehr gerechtfertigt, auf eine Gebührenerhebung zu verzichten. Der Gesetzestext stellt dafür auf die *Eignung* der Informationen ab. Eine andere Lösung – etwa das Abstellen darauf, ob die Informationen der gewerblichen Nutzung *dienen* – würde das Prinzip des voraussetzungslosen Zugangs durchbrechen, indem dann bei jedem Gesuch ein Verwendungszweck anzugeben wäre. Ausserdem müsste möglicherweise ein Kontrollverfahren eingerichtet werden, um herauszufinden, ob Informationen nicht entgegen dem angegebenen Verwendungszweck doch für gewerbliche Zwecke genutzt werden.

Abs. 5: Für die Festlegung der Höhe der Gebühren nach Abs. 2 und 4 ist der Regierungsrat zuständig.

---

[49] So hat die Eidgenössische Datenschutzkommission (bis Ende 2006 das Bundes-Datenschutzgericht) festgestellt, dass die Zusendung der verlangten Akten zusammen mit der Verfügung betreffend die Kostenbeteiligung per Nachnahme gegen Art. 2 Abs. 2 Verordnung zum Bundesdatenschutzgesetz (VDSG, SR 235.11) verstösst (VPB 65.50 E. 4 a).

[50] §§ 38 ff. Organisationsgesetz (SG 153.100).

[51] § 15 Abs. 2 Gesetz über die Verwaltungsgebühren (SG 153.800) i.V.m. § 14a Verwaltungsgebührenverordnung (SG 153.810).

VIII. Die oder der Informationszugangs- und Datenschutzbeauftragte

Für den Datenschutzbereich ist zwingend ein **unabhängiges Kontrollorgan** einzusetzen.[52] Angesichts der Überschneidungen zwischen Zugang und Nichtzugang zu Informationen, die zur Schaffung eines kombinierten Informations- und Datenschutzgesetzes führen, ist es auch zweckmässig, ein **einziges Organ** für die Kontroll- und Beratungsaufgaben in beiden Bereichen einzusetzen.

Von der SP wurde in der Vernehmlassung eine vertiefte Auseinandersetzung gewünscht zur Frage, ob der Informationszugang der Datenschutzaufsichtsstelle «angehängt» werden soll. Es gibt Gründe für und gegen eine solche Zusammenlegung:

- Gegen eine Zusammenlegung wird die Befürchtung angeführt, dass die oder der Informationszugangs- und Datenschutzbeauftragte in eine Doppelrolle käme und die Datenschutz-Rolle als «Fürsprecher» für die Persönlichkeitsrechte der betroffenen Personen nicht in der gleichen «Reinheit» ausüben könnte.

- Für die Zusammenlegung spricht die Tatsache, dass die oder der Datenschutzbeauftragte schon heute genau diese Abwägung vornehmen muss: Die Frage, ob ein öffentliches Organ Personendaten bearbeiten, insbesondere erheben oder an Dritte (Private oder andere öffentliche Organe) bekannt geben darf oder eben nicht, verlangt genau die Auslegung der (spezial-)gesetzlichen Bestimmungen, die der Datenbearbeitung zugrunde liegen (z.B. im Sozialhilfe-, Polizei- oder Steuergesetz), und der entgegenstehenden Interessen.

Wenn die Funktionen der oder des Informationszugangsbeauftragten und der oder des Datenschutzbeauftragten getrennt sind, entfällt eine wichtige Funktion zur Unterstützung der öffentlichen Organe bei der Abwägung beim Zugang zu Personendaten: Wenn jede dieser Stellen nur zuständig ist für die Beantwortung der Frage auf «ihrer» Seite, bekommt das öffentliche Organ, das sich im Interesse der richtigen Rechtsanwendung an die beratenden Stellen wendet, genau für den schwierigsten Teil, nämlich die Abwägung zwischen den jeweils geltend gemachten Interessen, keine Unterstützung. Im Gegenteil: es ist möglich, dass die gleiche (spezial-)gesetzliche Bestimmung durch die beiden beratenden Stellen im Zusammenhang mit dem Zugang zu Informationen (nach dem Öffentlichkeitsprinzip) anders ausgelegt wird als im Zusammenhang mit der Bearbeitung oder Bekanntgabe der Personendaten zur Aufgabenerfüllung. Aus diesem Grund schlägt der Regierungsrat weiterhin vor, die beiden Funktionen in einer Stelle, derjenigen der oder des Informationszugangs- und Datenschutzbeauftragten zusammenzulegen. Entschärft wird die Problematik ausserdem, weil das Schlichtungsverfahren neu nicht durch die oder den Informationszugangs- und Datenschutzbeauftragten, sondern durch die Ombudsstelle durchgeführt wird (§ 34). Im interkan-

[52] Art. 37 Abs. 2 DSG-Bund (SR 235.1); Art. 1 des Zusatzprotokolls vom 8. November 2001 zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Übermittlung (Zusatzprotokoll zur Europarats-Konvention 108, SR 0.235.11); für den Anwendungsbereich Schengen/Dublin: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutzrichtlinie), Amtsblatt der Europäischen Gemeinschaften Nr. L 281 vom 23/11/1995, 0031-0050.

tonalen Vergleich: Im Kanton Bern und im Kanton Zürich gibt es nur einen Datenschutzbeauftragten; im Kanton Bern wurden Datenschutz und Öffentlichkeitsprinzip zu unterschiedlichen Zeitpunkten (1986 bzw. 1993) in zwei unterschiedlichen Gesetzen geregelt; in Zürich ist nicht nachvollziehbar, weshalb in der Parlamentsvorlage die in der Vernehmlassungsvorlage noch vorgesehene Doppelzuständigkeit nicht mehr enthalten war. Im Bund, im Kanton Solothurn, im Kanton Aargau und im Kanton Schwyz ist jeweils eine Stelle für beiden Themen zuständig.

In den §§ 38-51 werden materiell die Regelungen von §§ 26-29 DSG in der Fassung der Schengen/Dublin-Revision übernommen. Die Gliederung und Formulierung lehnen sich aber an § 4 des Finanzkontrollgesetzes vom 17. September 2003 (FKG, SG 610.200) an, da der oder dem Datenschutzbeauftragten eine ähnliche Stellung wie der Leitung der Finanzkontrolle zukommt.

§ 38 Kantonale Aufsichtsstelle

Abs. 1: Der Kanton führt eine kantonale Aufsichtsstelle. Sie tritt unter dem Namen «**Die oder der Informationszugangs- und Datenschutzbeauftragte**» auf. In der Rechtspraxis im deutschsprachigen Raum hat sich der Begriff der oder des Datenschutzbeauftragten längst eingebürgert, und zwar sowohl für die Institution wie auch für die Leiterin oder den Leiter der Institution; so heisst die entsprechende Stelle im Bund «Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter».[53] Einzig in Bestimmungen, bei denen es um die Person der Leiterin oder des Leiters geht (Wahl: § 40; Personalrecht: § 42; Verschwiegenheit: § 50), wird von «der Beauftragten oder dem Beauftragten» gesprochen. Informations*zugangs*- und Datenschutzbeauftragte soll die Funktion heissen, damit nicht der Anschein erweckt wird, sie sei die oder der Beauftragte für die (pro-)aktive Information (Informationsbeauftragte im Sinne der heute schon existierenden Kommunikationsbeauftragten der Departemente, Gemeinden usw.).

Abs. 2: Die Regierungen der beiden Basel haben 2004/5 beschlossen, die Schaffung einer **gemeinsamen Aufsichtsstelle beider Basel** zu prüfen. In der Zwischenzeit ist klar geworden, dass die zu erwartenden Synergien nicht sehr gross wären, da sich die beiden Kantone in ihrer Organisation und bezüglich der materiellen Gesetzesgrundlagen, welche das Datenbearbeiten durch öffentliche Organe konkret regeln (z.B. Bildungs-, Bau- und Planungsrecht, Polizeirecht usw.), zu stark unterscheiden. Dementsprechend haben die Vorsteherin der Sicherheitsdirektion des Kantons Basel-Landschaft und der Vorsteher des Justizdepartements Basel-Stadt bei der Präsentation der Vernehmlassungsvorlage erklärt, dass das Projekt einer Zusammenlegung nicht mehr weiterverfolgt werde. In der Vernehmlassung haben die Gemeinde Riehen, SP und DJS die Streichung von Abs. 2 verlangt; CVP und JFBS begrüssen demgegenüber die Benennung eines Informations- und Zugangsbeauftragten für mehrere Kantone. Der Regierungsrat will mit § 38 Abs. 2 die Möglichkeit offenhalten, allenfalls in fernerer Zukunft mit anderen Kantonen die Schaffung einer gemeinsamen Aufsichtsstelle ins Auge zu fassen. Eine solche partnerschaftliche Lösung müsste durch Staatsvertrag getroffen werden. Gelöst werden müsste dabei das Problem, dass eine Wahl durch die Parlamente, wie es die beiden Basel kennen, kaum mehr möglich wäre.

[53] Vgl. nur etwa den fünften Abschnitt (Art. 26 ff.) im DSG-Bund (SR 235.1).

§ 39 Stellung

Abs. 1: Als Verdeutlichung der in § 38 Abs. 1 bereits erwähnten **Unabhängigkeit** wird – wie mit der Schengen/Dublin-Revision des Datenschutzgesetzes (§ 26 Abs. 2) beschlossen – festgehalten, dass die oder der Informationszugangs- und Datenschutzbeauftragte die Aufgaben weisungsunabhängig erfüllt; das heisst insbesondere, dass keine Instanz die Vornahme bestimmter Kontrollen verbieten oder die Stellungnahme inhaltlich vorschreiben kann.

Abs. 2 übernimmt die organisatorische Zuordnung der/des Informationszugangs- und Datenschutzbeauftragten von § 26 Abs. 4 DSG in der Fassung der Schengen/Dublin-Revision.

Abs. 3 nimmt neu die Mitglieder des Grossen Rates und den Grossen Rat als Behörde (lit. a) und den Regierungsrat als Behörde (lit. b) aus dem Kontrollbereich der oder des Informationszugangs- und Datenschutzbeauftragten.

Zur Kontrollzuständigkeit gegenüber der Fachgruppe 9 der Staatsanwaltschaft vgl. die Erläuterungen zu § 45.

§ 40 Leitung

Abs. 1: Die Bestimmung entspricht weitgehend § 26a Abs. 3 DSG in der Fassung der Schengen/Dublin-Revision. Es wird lediglich noch zusätzlich analog zu § 4 Abs. 1 FKG festgehalten, dass die Leitung der Aufsichtsstelle durch eine in Datenschutzfragen ausgewiesene Fachperson erfolgen soll.

Abs. 2: Diese Bestimmung enthält die mit der Schengen/Dublin-Revision des Datenschutzgesetzes beschlossene **Wahlregelung**, ergänzt – analog § 4 Abs. 2 Satz 3 FKG – durch die Erwähnung der Wiederwahlmöglichkeit.

Abs. 3: Das Amt der oder des Beauftragten kann auf zwei Personen mit max. 100 Stellenprozenten aufgeteilt werden. Damit wurde § 26a Abs. 3 DSG in der Fassung der Schengen/Dublin-Revision übernommen.

Abs. 4: In Analogie zu § 4 Abs. 3 FKG wird festschrieben, dass die oder der Beauftragte bei schwerwiegender Amtspflichtverletzung oder bei fachlichem Ungenügen vom Grossen Rat mit Zweidrittelsmehrheit vor Ablauf der Amtsdauer abgewählt werden kann.

§ 41 Unvereinbarkeit

Diese Regelung entspricht § 26a Abs. 3 DSG in der Fassung der Schengen/Dublin-Revision.

§ 42 Personal

Abs. 1 hält zur Klarstellung fest, dass das **Personalrecht** des Kantons auf die Beauftragte oder den Beauftragten und das weitere Personal anwendbar ist, soweit das Gesetz nichts anderes vorsieht. Diese Bestimmung entspricht § 26a Abs. 2 DSG in der Fassung der Schengen/Dublin-Revision.

Abs. 2 übernimmt die mit der Schengen/Dublin-Revision des Datenschutzgesetzes beschlossene Regelung von § 26a Abs. 6, wonach die oder der Beauftragte im Rahmen des vom Grossen Rat genehmigten Budgets für die Einstellungen der **weiteren Mitarbeitenden** zuständig ist. Dies gehört zur Unabhängigkeit der Aufsichtsstelle.

§ 43 Budget

§ 43 übernimmt die zur Sicherstellung der Unabhängigkeit dienende Regelung von § 26 Abs. 3 DSG in der Fassung der Schengen/Dublin-Revision: Die oder der Informationszugangs- und Datenschutzbeauftragten hat ein **eigenes Budget**.

§ 44 Kommunale Aufsichtsstelle

Die Absätze 1, 2 und 4 der Bestimmung übernehmen materiell unverändert die Regelung über die **kommunalen Aufsichtsstellen** aus der mit der Schengen/Dublin-Revision beschlossenen Regelung von § 27 DSG. Ausserdem statuiert Abs. 3 neu die Unvereinbarkeit des kommunalen Beauftragten und seiner Mitarbeiter mit anderen behördlichen Funktionen in der Gemeinde. Die CVP erkennt keine Notwendigkeit für einen zusätzlichen kommunalen Informationszugangs- und Datenschutzbeauftragten der Landgemeinden. Es spricht jedoch kaum etwas dafür, hier die verfassungsrechtliche Organisationsautonomie der Gemeinden ohne zwingenden Grund zu beschneiden; es ist den Gemeinden selbstverständlich unbenommen, keine eigene Aufsichtsstelle zu schaffen (oder die bestehende Datenschutzkommission abzuschaffen).

§ 45 Aufgaben

§ 45 übernimmt den eigentlichen **Aufgaben**teil aus dem mit der Schengen/Dublin-Revision beschlossenen § 28 lit. a, b, c, e, f und h DSG:

- **Kontrolle** nach einem autonom aufzustellenden Prüfprogramm (lit. a);
- Durchführung von **Vorabkontrollen** gemäss § 13 (lit. b);
- **Beratung** der öffentlichen Organe (lit. c);
- **Beratung** der betroffenen Personen (lit. d);
- **Vermittlung** zwischen betroffenen Personen und öffentlichen Organen (lit. e);
- **Stellungnahme** zu Erlassen, die für den Umgang mit Informationen oder den Datenschutz erheblich sind (lit. f).

Im Vergleich zur bisherigen Regelung verwendet die Aufzählung der Aufgaben in § 45 eine andere Reihenfolge. Es wird die logischere Abfolge des Datenschutzgesetzes Basel-Landschaft übernommen, wo im Rahmen der Schengen/Dublin-Revision bereits eine umfassendere Anpassung des Aufgabenkatalogs vorgenommen wurde.[54] Die in der Vernehmlas-

[54] § 24 DSG BL.

sungsvorlage noch enthaltene Aufgabe, das Schlichtungsverfahren durchzuführen, ist hinfällig geworden (§ 34).

In ihrer Vernehmlassung hat die SP eine Rechtsgrundlage zur **Aufsicht und Kontrolle über die Fachgruppe 9** der Staatsanwaltschaft, die im Rahmen von Art. 6 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)[55] für den Vollzug jenes Gesetzes im Kanton zuständig ist, verlangt. Soweit es um das Bearbeiten von Personendaten durch die Fachgruppe 9 geht, ist die oder der Informationszugangs- und Datenschutzbeauftragte aufgrund des ohne Weiteres zur Kontrolle zuständig. In diesem Gesetz braucht es deshalb keine Ergänzung. Die umstrittene Frage ist vielmehr, ob die gestützt auf das BWIS erlassene Bundesverordnung (VWIS)[56] die Kontrollbefugnis des kantonalen Kontrollorgans zu Recht – vor allem nur im dem durch das BWIS vorgegebenen Rahmen – einschränkt. Diese Frage kann hier im Informations- und Datenschutzgesetz nicht beantwortet werden; der Regierungsrat wird aber zu gegebener Zeit die allenfalls nötigen kantonalen Rechtsgrundlagen schaffen.

Die Pflichten der oder des Informationszugangs- und Datenschutzbeauftragten (Pflicht zur Zusammenarbeit, zur Verschwiegenheit und zur Berichterstattung, § 28 lit. d und i DSG in der Fassung der Schengen/Dublin-Revision und § 30 DSG) werden selbständig in den §§ 49 bis 51 geregelt. Ebenfalls nicht mehr im Aufgabenkatalog enthalten ist die Führung des zentralen Registers (§ 28 lit. g DSG), da dieses durch eine dezentrale Führung von Verzeichnissen ersetzt wurde (§ 24).

§ 46 Kontrollbefugnisse

Abs. 1 übernimmt die **Kontrollbefugnisse** aus dem mit der Schengen/Dublin-Revision beschlossenen § 29 Abs. 2-3 DSG. In Abs. 2 wird ergänzend präzisiert, worin die Unterstützung der öffentlichen Organe und der beauftragten Dritten bestehen soll.

In der Vernehmlassungsvorlage war hier, nach § 46 und vor der Bestimmung zu den Empfehlungen der oder des Informationszugangs- und Datenschutzbeauftragten, ein Paragraph zum Instrument der «Aufforderung» vorgesehen. Er entsprach inhaltlich dem § 29 Abs. 5 DSG (in der Fassung vor der Schengen/Dublin-Revision). Da diese Bestimmung durch die Schengen/Dublin-Revision wegfiel, werden die «Aufforderungen» hier auch nicht mehr vorgeschlagen.

§ 47 Empfehlungen

Hier ist die **Empfehlung** geregelt, eine Einwirkungsbefugnis, die mit der Schengen/Dublin-Revision (§ 29 Abs. 4 DSG) beschlossen wurde.

---

[55] Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120).

[56] Verordnung vom 27. Juni 2001 über Massnahmen zur Wahrung der inneren Sicherheit (VWIS, SR 120.2).

§ 48 Weisungen zum Bearbeiten von Personendaten

Diese Bestimmung enthält die mit der Schengen/Dublin-Revision des Datenschutzgesetzes (§ 29 Abs. 5-7) beschlossene Befugnis der oder des Informationszugangs- und Datenschutzbeauftragten, abgelehnte oder nicht befolgte Empfehlungen oder Teile davon als **Weisung in Form einer Verfügung** zu erlassen, wenn das Interesse an der Durchsetzung schwer wiegt (lit. b). Diese Weisungsbefugnis bleibt eingeschränkt auf die Bearbeitung von Personendaten (lit. a) und gilt nicht gegenüber dem Appellationsgericht, das zum Entscheid über Weisungsanfechtungen berufen ist (Abs. 2). Neu wird allerdings geregelt, dass die oder der Informationszugangs- und Datenschutzbeauftragte direkt eine Weisung erlassen kann, wenn absehbar ist, dass das öffentliche Organ eine Empfehlung ablehnen oder ihr keine Folgen leisten wird (Abs. 3). Auch weiterhin kann die oder der Informationszugangs- und Datenschutzbeauftragte die Einstellung oder Einschränkung der Bearbeitung anordnen, wenn schutzwürdige Interessen offensichtlich oder schwerwiegend verletzt werden (Abs. 4), und kann das öffentliche Organ, an welches die Weisung gerichtet ist, die Weisung mit **Rekurs** beim Appellationsgericht anfechten (Abs. 5).

§ 49 Zusammenarbeit

Dieser Paragraph übernimmt die mit der Schengen/Dublin-Revision des Datenschutzgesetzes beschlossene Pflicht der oder des Informationszugangs- und Datenschutzbeauftragten, zur Erfüllung ihrer oder seiner Aufgaben mit den Informations- und/oder Datenschutzbeauftragten anderer Kantone, des Bundes und des Auslandes **zusammenzuarbeiten** (§ 28 lit. i).

§ 50 Verschwiegenheit

Hier wird die bereits im § 30 DSG enthaltene **Schweigepflicht**bestimmung, terminologisch angepasst an die Regelung in § 19 Personalgesetz, übernommen.

§ 51 Berichterstattung

§ 51 übernimmt die bereits im § 28 lit. e DSG enthaltene **Berichterstattung**spflicht der oder des Informationszugangs- und Datenschutzbeauftragten, ergänzt um die Pflicht, sich – im Sinne der Wirkungsorientierung staatlichen Handelns – auch zur Wirkung des Gesetzes zu äussern.

IX. Strafbestimmungen

§ 52 Vertragswidriges Bearbeiten von Personendaten

Mit strafrechtlicher Sanktionierung von Datenschutzverletzungen soll auch in Zukunft sparsam umgegangen werden. Wie erwähnt waren bis anhin in zwei Fällen die Sanktionsmöglichkeiten bei einer Datenschutzverletzung zu schwach, weil die Personendaten den Bereich verlassen, der durch personalrechtliche Sanktionierungsmöglichkeiten gesichert ist: in **Outsourcing-Verträgen** (nach § 7) und bei der Bekanntgabe von Personendaten an Private zum **Bearbeiten zu einem nicht personenbezogenen Zweck** (nach § 22 Abs. 4). Die Er-

fahrungen zeigen, dass es bisweilen schwerfällt, angemessene Konventionalstrafen zu vereinbaren. Deshalb sieht das Gesetz neu die Möglichkeit vor, vertragswidriges Bearbeiten von Personendaten im Zusammenhang mit Outsourcing-Verträgen mit einer Busse zu sanktionieren (Abs. 1). Der Kanton Zürich[57] kennt diese Verstärkung des Datenschutzes schon lange und der Kanton Aargau[58] hat sie vor kurzem auch eingeführt. Die gleiche Sanktionierungsmöglichkeit soll gegenüber Privaten bestehen, welche von einem öffentlichen Organ Personendaten in nicht anonymisierter Form zum Bearbeiten zu nicht personenbezogenen Zwecken erhalten haben und diese Personendaten entgegen der Verpflichtung gemäss § 22 Abs. 4 lit. a und b für andere Zwecke bearbeitet oder an Dritte weitergeben (Abs. 2). Es handelt sich in beiden Fällen um Übertretungstatbestände, auf die das kantonale Übertretungsstrafgesetz[59] anwendbar ist; dieses legt insbesondere auch den Bussenrahmen fest. In der Vernehmlassungsvorlage war das Bearbeiten für andere Zwecke noch nicht enthalten; es ist aber nicht zu rechtfertigen, die eine der Arten, im Outsourcing-Verhältnis anvertraute Daten vertragswidrig zu bearbeiten, unter Strafe zu stellen und die andere nicht.

X. Änderung und Aufhebung bisherigen Rechts

§ 53 Änderung bisherigen Rechts

Ziff. 1: Aufenthaltsgesetz (SG 122.200)

Die Herausgabe von Personendaten durch die zuständigen Behörden, geregelt in § 30 des Aufenthaltsgesetzes, richtet sich neu nach den Vorschriften des Informations- und Datenschutzgesetzes. Die bisher in § 12 DSG enthaltene Bekanntgabebefugnis der Einwohnerkontrolle wird damit ins relevante Sachgesetz transferiert, so wie auch in den anderen Bereichen staatlicher Tätigkeit die konkreten, aufgabenbezogenen Datenbearbeitungsbefugnisse der öffentlichen Organe in den entsprechenden Sachgesetzen und nicht im (Informations- und) Datenschutzgesetz niedergelegt sind.

Da das Aufenthaltsgesetz zur Zeit ebenfalls revidiert wird und zeitlich nicht abgeschätzt werden kann, welche Vorlage zuerst verabschiedet wird, werden folgend zwei Varianten der Änderung von § 53 des Aufenthaltsgesetzes vorgestellt. Dabei baut die Variante 1 auf die geltende Fassung des Aufenthaltsgesetzes auf und Variante 2 berücksichtigt die laufende Revision des Aufenthaltsgesetzes.

Die Herausgabe von Personendaten durch die zuständigen Behörden, geregelt in § 30 des Aufenthaltsgesetzes, richtet sich neu nach den Vorschriften des Informations- und Datenschutzgesetzes. Die bisher in § 12 DSG enthaltene Bekanntgabebefugnis der Einwohnerkontrolle wird damit ins relevante Sachgesetz transferiert (Variante 1: Abs. 3 und 4; Variante 2: Abs. 4 und 5), so wie auch in den anderen Bereichen staatlicher Tätigkeit die konkreten, aufgabenbezogenen Datenbearbeitungsbefugnisse der öffentlichen Organe in den entspre-

[57] § 26 Datenschutzgesetz ZH (ausser Kraft gesetzt per 1. Oktober 2008); übernommen als § 40 ins Informations- und Datenschutzgesetz ZH (LS 170.4).
[58] § 41 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen AG (SAR 150.700).
[59] Insbesondere § 1 Übertretungsstrafgesetz (SG 253.100).

chenden Sachgesetzen und nicht im (Informations- und) Datenschutzgesetz niedergelegt sind.

Neu soll, wie in der Vernehmlassung von der Gemeinde Riehen und der SP verlangt, die Möglichkeit der sog. **Listenauskunft** eingeführt werden. Wie in den meisten Kantonen (z.B. in § 10 Abs. 3 Datenschutzgesetz BL) soll es der Einwohnerkontrolle künftig erlaubt sein, *ausschliesslich für schützenswerte ideelle Zwecke* Familiennamen, Vornamen, Geburtsdatum und Adresse von Personen, die in der Gemeinde wohnen, bekanntzugeben (Variante 1: Abs. 5; Variante 2: Abs. 6). Als ideelle Zwecke erscheinen etwa die Mitgliederwerbung für politische Parteien, Kultur- oder Sportvereine, für Spendenaufrufe von gemeinnützigen Organisationen wie Pro Infirmis; ausgeschlossen ist die Verwendung für kommerzielle Zwecke. Die Einwohnerkontrolle hat deshalb entsprechende Gesuche genau zu prüfen und sich von den Datenempfängerinnen und -empfängern eine Erklärung unterzeichnen zu lassen, worin diese sich verpflichten, jede andere Verwendung als die im Gesuch genannte zu unterlassen[60]. Diese Verpflichtungserklärung kann durch die Androhung der Ungehorsamstrafe nach Art. 292 Strafgesetzbuch verstärkt werden. Natürlich können die Daten nicht nach einem beliebigen Kriterium (z.B. steuerbares Einkommen über CHF 500'000) geordnet bekannt gegeben werden; das Gesetz hat deshalb die Kriterien, nach denen geordnet Daten bekanntgegeben werden dürfen, aufzuzählen: Alter (z.B. nur unter 18-Jährigen für einen Jugendsportverein), Geschlecht (z.B. nur Einwohnerinnen für den Damenturnverein), Adresse (z.B. nur die in bestimmten Strassen wohnhaften Personen für einen Quartierverein), Stimmberechtigung (z.B. für politische Parteien) und Zuzug (z.B. Mitgliederwerbung aller Vereine bei Neuzuzügerinnen und –zuzügern). § 30 Abs. 5 Aufenthaltsgesetz stellt im Sinne von § 26 IDG eine spezialgesetzliche Bestimmung dar, welche die voraussetzungslose Bekanntgabe von Personendaten erlaubt; jede betroffene Personen kann deshalb nach § 26 die Bekanntgabe ihrer Daten ohne Angaben von Gründen sperren lassen.

Ziff. 2: Organisationsgesetz (SG 153.100)

Zur Vermeidung von Missverständnissen wird in § 8 OG auf die Anwendbarkeit des Informations- und Datenschutzgesetzes hingewiesen.

Ziff. 3: Archivgesetz (SG 153.600)

- § 2 Abs. 1 lit. c und § 5 Abs. 6 verweisen neu auf das Informations- und Datenschutzgesetz.

- § 10 Abs. 7: Für amtliche Informationen soll das Informations- und Datenschutzgesetz gelten, unabhängig davon, ob sich diese bei der ursprünglichen Dienststelle befinden oder – gemäss Archivgesetz – ins Staatsarchiv gelangten. Aus diesem Grund wird in § 10 Abs. 7 neu festgehalten, dass die Schutzfristen der Absätze 1 und 2 nicht für Archivgut gelten, soweit es vor der Übergabe an das Staatsarchiv nach dem Informations- und Datenschutzgesetz zugänglich war. Mit «zugänglich war» ist die rechtliche Zugänglichkeit gemäss Informations- und Datenschutzgesetz gemeint, unabhängig

[60] Vgl. etwa die Musterverpflichtungserklärung der Baselbieter Datenschutzbeauftragten: <http://www.basel land.ch/prak-003-htm.289389.0.html#body-over>

davon, ob irgendjemand je konkret Zugang zu diesen amtlichen Informationen verlangt und erhalten hat.

Ziff. 4: Personalgesetz (SG 162.100)

Die neue Formulierung von § 19 Abs. 1 stellt klar, dass die Geheimhaltungspflicht neu im Rahmen des Informations- und Datenschutzgesetzes gilt. Die Tragweite der Geheimhaltungspflicht wird also durch die Einführung des Öffentlichkeitsgrundsatzes neu definiert. Durch das Inkrafttreten des Informations- und Datenschutzgesetzes wird die Geltung der Geheimhaltungspflicht auf Informationen beschränkt, die nach dem Informations- und Datenschutzgesetz nicht zugänglich oder die nach einer spezialgesetzlichen Vorschrift geheim zu halten sind. Es braucht daher nicht mehr geregelt zu werden, dass keine Geheimhaltungspflicht besteht in Fällen, in denen die Gesetzgebung die Aussage- oder Publikationspflicht vorsieht. Abs. 3 ist somit obsolet geworden.

Ziff. 5: Steuergesetz (SG 640.100)

§ 141a Abs. 4 verweist neu auf das Informations- und Datenschutzgesetz.

Ziff. 6: Das Einführungsgesetz zum Bundesgesetz über die Invalidenversicherung für eine IV-Stelle Basel-Stadt (SG 832.500)

In der Vernehmlassungsvorlage war vorgesehen, den in § 6 dieses Gesetzes enthaltenen Verweis auf das Datenschutzgesetz durch einen Verweis auf das Informations- und Datenschutzgesetz zu ersetzen. Das Sozialversicherungsgericht hat in seiner Vernehmlassung darauf hingewiesen, dass dieser Verweis («Der Datenschutz richtet sich nach dem kantonalen Gesetz …») nicht notwendig sei, weil dies ohnehin für kantonale öffentliche Organe gelte; andernfalls wäre es angebracht, ihn auch in den vergleichbaren Gesetzen[61] aufzunehmen. Weil unnötige Bestimmungen vermieden werden sollen, wird in § 6 der bisherige Absatz 2 gelöscht und der Titel dem verbleibenden Inhalt angepasst.

Die in der Vernehmlassungsvorlage noch vorgesehene Anpassung des Tagesbetreuungsgesetzes ist durch die am 25. Juni 2008 beschlossene Änderung jenes Gesetzes hinfällig geworden.

§ 54 Aufhebung bisherigen Rechts

Mit dem Inkrafttreten des Informations- und Datenschutzgesetzes wird das geltende Datenschutzgesetz aufgehoben.

[61] Einführungsgesetz zum Bundesgesetz über die Alters- und Hinterlassenenversicherung vom 5. Juni 1991 (SG 832.200); Gesetz betreffend Einführung des Bundesgesetzes vom 25. Juni 1982 über die obligatorische Arbeitslosenversicherung und die Insolvenzentschädigung vom 27. September 1984 (SG 835.100); Gesetz über die Einführung des Bundesgesetzes über die Ergänzungsleistungen zur Alters-, hinterlassenen- und Invalidenversicherung sowie über die Ausrichtung von kantonalen Beihilfen vom 11. November 1987 (SG 832.700).

XI. Schlussbestimmungen

§ 55 Fristen

Das Informations- und Datenschutzgesetz braucht eine spezifische Übergangsfrist, da § 22 nicht ohne Weiteres im Zeitpunkt des Inkrafttretens umsetzbar ist. Es ist deshalb festzuhalten, dass innerhalb zweier Jahre ab Inkrafttreten dieses Gesetzes die Verzeichnisse der Informationsbestände mit Personendaten (§ 24) zu veröffentlichen sind (Abs. 1). Auf begründetes Gesuch hin kann der Regierungsrat die Frist um ein Jahr verlängern (Abs. 2).

§ 56 Inkrafttreten

Wie üblich soll der Regierungsrat ermächtigt werden, das Gesetz in Kraft zu setzen.

V. Finanzielle und personelle Auswirkungen

Der Vollzug des Informations- und Datenschutzgesetzes erfolgt einerseits durch alle öffentlichen Organe von Kanton und Gemeinden und anderseits durch die Informationszugangs- und Datenschutzbeauftragte oder den Informationszugangs- und Datenschutzbeauftragten.

Die öffentlichen Organe haben wie bis anhin die datenschutzrechtlichen Bestimmungen umzusetzen. Daran wird sich durch das Informations- und Datenschutzgesetz nichts ändern. Welchen Aufwand die Umsetzung der informationsrechtlichen Bestimmungen verursachen wird, lässt sich im Voraus nicht exakt abschätzen. Er hängt in erster Linie von der Anzahl der eingereichten Zugangsgesuche und der allenfalls folgenden Rechtsmittelverfahren ab. Allerdings kann darauf hingewiesen werden, dass die Einführung des Öffentlichkeitsprinzips in der Staatsverwaltung des Kantons Bern, der inzwischen über eine 10-jährige Erfahrung damit verfügt, nur geringe Kosten verursacht hat[62]. Auch in den anderen Kantonen mit Öffentlichkeitsprinzip haben sich entsprechende Befürchtungen als unbegründet erwiesen. Da unser Kanton schon seit langem eine offene und aktive Informationspolitik sowie Auskunftstätigkeit betreibt, dürfte auch hier mit keiner anderen Entwicklung zu rechnen sein. Daher ist davon auszugehen, dass ein allfälliger Mehraufwand bei den öffentlichen Organen ohne zusätzliche Stellen und Ressourcen bewältigt werden kann. Das gilt insbesondere, wenn mit der Einrichtung eines Schlichtungsverfahrens (§ 34) einvernehmliche Lösungen gefunden und damit Rechtsmittelverfahren vermieden werden können.

Die Ombudsstelle wird neu für die Durchführung eines allfälligen Schlichtungsverfahrens zuständig sein. Obwohl keine Flut von Informationszugangsgesuchen und damit auch nicht von Schlichtungsgesuchen erwartet wird, ist im heutigen Zeitpunkt schlicht nicht abschätzbar, wie gross die zusätzliche Belastung der Ombudsstelle durch diese neue Funktion sein wird.

---

62 Vgl. KURT NUSPLIGER, 10 Jahre Öffentlichkeitsprinzip im Kanton Bern, in: Datenschutzbeauftragter des Kantons Zürich (Hrsg.), Herausforderung Datenschutz, 10 Jahre Datenschutzgesetz – eine Zwischenbilanz, digma-Schriften Band 1, Zürich/Basel/Genf 2005, 56 ff. (Ziff. 6 und 7).

Falls aber daraus längerfristig ein Bedarf nach zusätzlichen personellen Mitteln entstehen sollte, wird die Ombudsstelle dies in den Budgetprozess einfliessen lassen müssen.

Die oder der Informationszugangs- und Datenschutzbeauftragte hat wie bis anhin die Aufsicht über die Umsetzung der Datenschutzbestimmungen zu gewährleisten. Mit der stärkeren Betonung der Unabhängigkeit im Rahmen der Schengen/Dublin-Revision des Datenschutzgesetzes wurde festgelegt, dass die kantonale Aufsichtsstelle über ein eigenes Budget verfügt, dessen Entwurf sie selbständig erstellt. Gemäss dem derzeitigen Datenschutzbeauftragten ist für eine wirksame Datenschutzaufsicht mit folgenden Kosten zu rechnen:

a) Personalkosten: Mindestens 300 Stellenprozente, nämlich 1 Beauftragte(r) und 2 Mitarbeitende, was gegenüber heute Mehrkosten von CHF 300'000 ausmacht. Zusätzliche Ressourcen werden im Bereich der IT-Revision (ca. 30-50 Stellenprozente) erforderlich sein, die jedoch als externe Dienstleistung eingekauft werden können (CHF 50'000-80’000).

b) Mobiliar: Es wird einen neuen Standort geben. Kosten für drei Arbeitsplätze werden sich aufgrund von Angaben des Baudepartements auf CHF 30'000 belaufen.

c) IT-Ausrüstung: Hard- und Software für drei Arbeitsplätze betragen rund CHF 13'000. Dazu kommen noch Telefoneinrichtungen für drei Personen = CHF 2'000 und allenfalls noch eine neue fachspezifische Applikation für Autorisierungen.

d) Offen sind: Kosten für IT-Projekte, Dezentralisierung Zentrales Register, Kosten für den Umzug, Miete neuer Standort, evtl. Anschluss DANEBS (je nach Standort), Unterstützungs- und Umlagekosten, Sachkosten für Büromaterial, Kosten Unterhalt Büroräumlichkeiten und generell laufende Betriebskosten.

Im Rahmen des Wahlverfahrens hat die Wahlvorbereitungskommission auf Vorschlag des jetzigen Datenschutzbeauftragten einen Entwurf für das erstmalige Budget 2009 ausgearbeitet[63].

Es ist davon auszugehen, dass mit der Einführung des Öffentlichkeitsprinzips anfänglich eine erhöhte Nachfrage nach Beratung entstehen wird. Falls daraus längerfristig ein Bedarf nach zusätzlichen personellen Mitteln entstehen sollte, hat die oder der Informationszugangs- und Datenschutzbeauftragte dies in den Budgetprozess einfliessen zu lassen. Zum Vergleich: Im Kanton Basel-Landschaft war die Datenschutzaufsichtsstelle schon vor der Schengen/Dublin-Anpassung und ohne Aufgaben im Zusammenhang mit dem Öffentlichkeitsprinzip mit 200 Stellenprozenten dotiert (plus eine Volontärsstelle); mit der Schengen/Dublin-Revision werden zusätzliche 50-100 Stellenprozente dazugegeben[64]. Im Kanton Zürich verfügt die kantonale Datenschutzaufsicht über 720 Stellenprozente (ohne Aufsicht im Bereich des Öffentlichkeitsprinzips), wobei die grössten Gemeinden verpflichtet sind, zu-

[63] Bericht Nr. 08.5271.01 der Wahlvorbereitungskommission an den Grossen Rat zur Wahl eines Datenschutzbeauftragten des Kantons Basel-Stadt (Amtsdauer 2009-2014), Ziff. 1.3; Budget 2009 des Regierungsrates (Beilage zum Bericht Nr. 08.0039.02 des Regierungsrates), 276 f.

[64] Landratsvorlage 2007-173, 35 f.

sätzlich eigene Aufsichtsstellen einzurichten (Stadt Zürich z.B. mit zusätzlichen 250 Stellenprozenten).

VI. Antrag an den Grossen Rat

Aufgrund der vorstehenden Ausführungen beantragt der Regierungsrat dem Grossen Rat, dem vorgelegten Entwurf des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz) zuzustimmen.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Guy Morin	Barbara Schüpbach
Präsident	Staatsschreiberin

Beilagen:

- Entwurf des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz)
- Synopse zwischen dem IDG-Entwurf und den mit der Schengen/Dublin-Revision geänderten Bestimmungen des Datenschutzgesetzes