

## Datenschutzgesetz

Botschaft und Entwurf der Regierung vom 20. Mai 2008

Inhaltsverzeichnis	Seite
Zusammenfassung.....	1
1. Ausgangslage.....	3
1.1. Bilaterale Abkommen II .....	3
1.1.1. Übersicht.....	3
1.1.2. Schengen-Assoziierungs-Abkommen und Dublin-Assoziierungs-Abkommen.	4
1.1.3. Assoziierungs-Abkommen und Datenschutz .....	5
1.2. Revision des eidgenössischen Datenschutzgesetzes .....	6
1.3. Situation im Kanton St.Gallen.....	6
1.4. Umsetzung der Assoziierungs-Abkommen auf kantonaler Ebene .....	8
2. Bestimmungsfaktoren für den Inhalt des Datenschutzgesetzes .....	9
2.1. Regelung der allgemeinen Datenschutzgrundsätze.....	9
2.2. Einführung eines unabhängigen Kontrollorgans .....	9
3. Bemerkungen zu einzelnen Artikeln .....	10
3.1. Allgemeine Bestimmungen .....	10
3.2. Bestimmungen über die Bearbeitung von Personendaten .....	12
3.3. Bestimmungen über die Bekanntgabe von Personendaten .....	16
3.4. Bestimmungen über die Rechte der betroffenen Person .....	19
3.5. Bestimmungen über die Fachstelle für Datenschutz .....	20
3.5.1. Organisationsbestimmungen.....	20
3.5.2. Zuständigkeitsbestimmungen.....	24
3.5.3. Bestimmungen über das Register über Datensammlungen.....	27
3.6. Schlussbestimmungen .....	28
4. Vernehmlassungsverfahren.....	29
4.1. Grundsätzliche Bemerkungen .....	29
4.2. Vorbehalte und Vorschläge zu einzelnen Artikeln.....	30
4.2.1. Abschnitt I (Allgemeine Bestimmungen).....	30
4.2.2. Abschnitt II (Bearbeitung von Personendaten) .....	32
4.2.3. Abschnitt III (Bekanntgabe von Personendaten) .....	32
4.2.4. Abschnitt IV (Rechte der betroffenen Person) .....	33
4.2.5. Abschnitt V (Fachstelle für Datenschutz).....	33
4.2.6. Abschnitt VI (Register über Datensammlungen).....	34
5. Kostenfolgen .....	34
6. Rechtliches.....	35
7. Antrag .....	35
Entwurf (Datenschutzgesetz) .....	36

## Zusammenfassung

*Die so genannten «Bilateralen II», die zwischen der Schweiz und der Europäischen Union (EU) vereinbart wurden, umfassen neben anderen Verträgen auch das Schengen-Assoziierungs-Abkommen und das Dublin-Assoziierungs-Abkommen. Diese Abkommen sowie der Beitritt der Schweiz zum Zusatzprotokoll zur Europarats-Konvention 108 haben wesentliche Auswirkungen*

auf das Datenschutzrecht des Bundes und der Kantone. Allgemein werden erheblich höhere Anforderungen als bisher an Massnahmen für einen wirksamen Datenschutz gestellt.

Die in den letzten Jahren markant intensivierete polizeiliche Zusammenarbeit zwischen den Staaten veranlasste die Europäische Union (EU), Rechtsnormen mit strengen Massstäben an den Datenschutz zu erlassen. Aufgrund der beiden Assoziierungs-Abkommen tritt die Schweiz deshalb nicht nur dem «Sicherheitsraum Europa», für den das Schengen-Informationssystem (SIS) eine zentrale Rolle spielt, sondern auch dem «Datenschutzraum Europa» bei. Im SIS werden Millionen von Datensätzen, insbesondere auch von Personendaten, gesammelt, weshalb die Gewährleistung eines wirksamen Datenschutzes unumgänglich ist.

Die definitive In-Kraft-Setzung des Schengen-Assoziierungs-Abkommens – und damit auch des auf die Zuständigkeitsregelung bei Asylanträgen ausgerichteten Dublin-Assoziierungs-Abkommens – und der Anschluss an das SIS erfolgen erst dann, wenn die Schweiz ihr innerstaatliches Recht an die Abkommen angepasst und die damit verbundene Rechtsetzungspflicht erfüllt hat. Die In-Kraft-Setzung bedarf eines Beschlusses des Rates der EU. Ein zustimmender Beschluss setzt voraus, dass Bund und Kantone die Vorgaben des EU-Rechts umgesetzt haben.

Nebst hinreichenden datenschutzrechtlichen Bestimmungen über die Rechte von betroffenen Personen wird der Einsatz von Kontrollorganen verlangt, die eine unabhängige und wirksame Datenschutzkontrolle sicherstellen. Da keine Verfassungsgrundlage besteht, die den Bund ermächtigen würde, Datenschutzbestimmungen auch in den kantonalen Zuständigkeitsbereichen zu erlassen, haben die Kantone in ihrer Gesetzgebung die sich aus dem Schengen Assoziierungs-Abkommen ergebenden Vorgaben zu erfüllen.

Der Kanton St.Gallen verfügt über kein Datenschutzgesetz, sondern lediglich über einige wenige Bestimmungen zum Datenschutz im Staatsverwaltungsgesetz. Die Ausführungsbestimmungen finden sich in der Datenschutzverordnung. Das geltende Recht vermag den Anforderungen, wie sie sich aus dem Schengen-Assoziierungs-Abkommen ergeben, nicht zu genügen. Insbesondere ist es unumgänglich, die materiellen Grundregeln des Datenschutzes – namentlich die Grundsätze des Bearbeitens von Personendaten und die Rechte der betroffenen Personen – auf Gesetzesstufe festzuhalten. Auch die organisatorisch-institutionellen Regeln, das heisst insbesondere jene für eine wirksame Datenschutzkontrolle, bedürfen der Grundlage im Gesetz. Es ist unumgänglich, ein Datenschutzgesetz zu erlassen.

Der Entwurf des Datenschutzgesetzes sieht die erforderlichen Bestimmungen über die Bearbeitung von Personendaten durch öffentliche Organe sowie über die Rechte der betroffenen Personen vor. Ferner werden Stellung und Aufgaben der auf kantonaler und kommunaler Ebene einzusetzenden Datenschutzkontrollorgane – als Fachstellen für Datenschutz bezeichnet – gesetzlich normiert. Den Fachstellen, denen Eigenständigkeit im Sinn von Unabhängigkeit von der Verwaltung zukommen muss, sind nach Massgabe der europarechtlichen Vorgaben Beratungsaufgaben sowie Untersuchungs- und Einwirkungsbefugnisse zu übertragen. Ferner sind Führung und Inhalt des Registers über Datensammlungen zu regeln. Dieses bildet eine wichtige Grundlage für die Gewährleistung des im Datenschutz bedeutsamen Transparenzgebotes.

Frau Präsidentin  
Sehr geehrte Damen und Herren

Mit dieser Vorlage unterbreiten wir Ihnen den Entwurf eines Datenschutzgesetzes. Der Entwurf regelt in Berücksichtigung der europarechtlichen Vorgaben einerseits die für die Organe von Kanton und Gemeinden geltenden datenschutzrechtlichen Zuständigkeiten und Pflichten sowie andererseits das auf den Datenschutz bezogene Verhältnis zwischen diesen und den betroffenen Personen.

## 1. Ausgangslage

### 1.1. Bilaterale Abkommen II

#### 1.1.1. Übersicht

Am 26. Oktober 2004 unterzeichneten die Schweiz und die Europäische Union die bilateralen sektoriellen Abkommen, die im allgemeinen Sprachgebrauch mit «Bilaterale II» bezeichnet werden und sich auf die folgenden Bereiche erstrecken:<sup>1</sup>

- Abbau von Zöllen und Exportsubventionen für landwirtschaftliche Verarbeitungserzeugnisse;
- Zusammenarbeit in der Statistik;
- Teilnahme an der Europäischen Umweltagentur und Beteiligung am Umwelt-Netzwerk EIONET;
- Teilnahme der Schweiz an MEDIA-Programmen im Rahmen des europäischen Filmschaffens;
- Vermeidung der Doppelbesteuerung der Pensionen von ehemaligen Beamten von EU-Institutionen;
- Regelung der Zinsbesteuerung;
- Beteiligung an der Schengener Zusammenarbeit über Ausgleichsmassnahmen bei Aufhebung der Personenkontrollen an den Binnengrenzen und an der Dubliner Zusammenarbeit über Behandlung von Asylgesuchen;
- Zusammenarbeit bei der Betrugsbekämpfung.

Die einzelnen Abkommen können unabhängig voneinander in Kraft treten. Bereits in Kraft sind:<sup>2</sup>

- das Abkommen betreffend landwirtschaftliche Verarbeitungszeugnisse (seit 30. März 2005);
- das Abkommen betreffend Statistik (seit 1. Januar 2007);
- das Abkommen betreffend Umwelt (seit 1. April 2006);
- das Abkommen betreffend MEDIA-Programme (seit 1. April 2006);
- das Abkommen betreffend Pensionen (seit 31. Mai 2005);
- das Abkommen betreffend Zinsbesteuerung (seit 1. Juli 2005).

Das Abkommen betreffend Betrugsbekämpfung bedarf der Genehmigung in den einzelnen Mitgliedstaaten und tritt nach Massgabe der zuletzt eingehenden Ratifikations- oder Genehmigungsurkunde in Kraft.

In Bezug auf die Abkommen betreffend Beteiligung an der Schengener und der Dubliner Zusammenarbeit besteht ein Unterschied zwischen In-Kraft-Treten und In-Kraft-Setzung.<sup>3</sup> Das Datum des In-Kraft-Tretens dieser Abkommen ist auf den 1. März 2008 angesetzt worden. Die In-Kraft-Setzung verlangt unter anderem einen Beschluss des Rates der Europäischen Union, wobei jene Staaten, die das Schengener Abkommen anwenden, einstimmig zustimmen müssen. Dem Beschluss liegt die Feststellung zugrunde, dass die Voraussetzungen für die Umsetzung der einschlägigen Bestimmungen von der Schweiz erfüllt sind.

---

<sup>1</sup> Vgl. Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II»), vom 1. Oktober 2004; BBl 2004, 5965 ff., 6033 ff.

<sup>2</sup> Integrationsbüro EDA/EVD: Vorgesehenes In-Kraft-Treten der Bilateralen II (Stand: 1. Februar 2008); <http://www.europa.admin.ch/themen/00500/00507/00527/index.html?lang=de> (PDF-Datei «Zeitplan Bilaterale II»).

<sup>3</sup> Vgl. Integrationsbüro EDA/EVD: Vorgesehenes In-Kraft-Treten der Bilateralen II (Stand: 1. Februar 2008); <http://www.europa.admin.ch/themen/00500/00507/00527/index.html?lang=de> (PDF-Datei «Zeitplan Bilaterale II»).

### 1.1.2. Schengen-Assoziierungs-Abkommen und Dublin-Assoziierungs-Abkommen

Im Zusammenhang mit dem Erlass eines kantonalen Datenschutzgesetzes sind die beiden folgenden Abkommen von ausschlaggebender Bedeutung:<sup>4</sup>

- Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (abgekürzt Schengen-Assoziierungs-Abkommen, SAA);<sup>5</sup>
- Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags (abgekürzt Dublin-Assoziierungs-Abkommen, DAA).<sup>6</sup>

An den beiden Abkommen sind alle Mitgliedstaaten der Europäischen Union beteiligt, Grossbritannien und Irland allerdings nur in Teilbereichen. Mit Norwegen und Island sind auch zwei Staaten Vertragspartei, die nicht Mitglieder der Europäischen Union sind.

Zusammengefasst lässt sich der Inhalt der beiden Assoziierungs-Abkommen wie folgt wiedergeben:<sup>7</sup>

«Im Rahmen der Schengener Zusammenarbeit haben die teilnehmenden Staaten ihre Personenkontrollen an den Binnengrenzen aufgehoben und gleichzeitig zur Stärkung der inneren Sicherheit eine Reihe von Ausgleichsmassnahmen beschlossen. Dazu gehören insbesondere die Verstärkung der Kontrollen an den Aussengrenzen des Schengen-Raums, eine gemeinsame Visumpolitik für Kurzaufenthalte, die Verbesserung der Zusammenarbeit im Bereich der Rechtshilfe in Strafsachen sowie die Intensivierung der grenzüberschreitenden Polizeizusammenarbeit. Zu den wichtigsten Instrumenten dieser Zusammenarbeit gehört das Schengen-Informationen-System (SIS), eine europaweite Fahndungsdatenbank. Die Dubliner Zusammenarbeit ist ein Element des europäischen Asylraums. Es soll sichergestellt werden, dass Asylsuchende ein – aber nur ein – Asylgesuch im Dubliner Raum stellen können. Dublin legt Kriterien fest, gemäss denen der für die Behandlung eines Asylgesuchs zuständige Staat bestimmt wird, und sorgt so für eine ausgewogene Verteilung der Asylsuchenden auf die Dublin-Staaten. Dank der elektronischen Datenbank Eurodac können mehrfach gestellte Asylgesuche systematisch erkannt werden. Die Instrumente der Schengen/Dublin-Zusammenarbeit werden laufend den neuen Anforderungen und technischen Entwicklungen angepasst. Die Schengen/Dublin-Assoziierungsabkommen gewährleisten der Schweiz die umfassende Beteiligung an dieser Zusammenarbeit.»

Die beiden Assoziierungs-Abkommen beziehen sich auch auf Bereiche, die innerstaatlich in der Kompetenz der Kantone liegen oder zu deren Vollzug die Kantone zuständig sind. Dies hat zur Folge, dass die Abkommen rechtlich und organisatorisch nicht nur auf Bundesebene, sondern ebenso auf der Ebene der Kantone umzusetzen sind. Zur rechtlichen Umsetzung gehört der Erlass der aufgrund der Abkommen erforderlichen Rechtsnormen.

---

<sup>4</sup> Die Stimmberechtigten stimmten am 5. Juni 2005 dem Bundesbeschluss vom 17. Dezember 2004 über die Genehmigung und die Umsetzung der bilateralen Abkommen zwischen der Schweiz und der EU über die Assoziierung an Schengen und an Dublin zu; BBl 2005, 5183.

<sup>5</sup> Abkommenstext in: Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II») vom 1. Oktober 2004; BBl 2004, 5965 ff., 6447 ff.

<sup>6</sup> Abkommenstext in: Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II») vom 1. Oktober 2004; BBl 2004, 5965 ff., 6479 ff.

<sup>7</sup> Vgl. Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II»), vom 1. Oktober 2004; BBl 2004, 5965 ff., 5968.

Im Normalfall müssen völkerrechtliche Verträge im Zeitpunkt ihres In-Kraft-Tretens in innerstaatliches Recht umgesetzt sein. Die beiden Assoziierungs-Abkommen sehen hingegen eine besondere Regelung für ihre Umsetzung vor. Die definitive In-Kraft-Setzung des Schengen-Assoziierungs-Abkommens – und dabei vor allem auch der Anschluss an das Schengen-Informationssystem (SIS) – erfolgt erst dann, wenn die Schweiz das Abkommen und die auf dieser Grundlage erlassenen Regelungen ins innerstaatliche Recht übernommen hat. Hierfür ist nach einer entsprechenden Kontrolle die einstimmige Feststellung der bisherigen Mitglieder des Schengen-Raums erforderlich, dass der Bund und die Kantone alle einschlägigen Bestimmungen korrekt umgesetzt haben (vgl. Art. 15 SAA). Das Dublin-Assoziierungs-Abkommen kann nur angewendet werden, wenn auch das Schengen-Assoziierungs-Abkommen in Kraft gesetzt werden kann (Art. 14 Abs. 2 DAA).

Was die Umsetzung der beiden Assoziierungs-Abkommen auf der Ebene des Bundes betrifft, haben die eidgenössischen Räte die Umsetzungsgesetzgebung am 17. Dezember 2004 gleichzeitig mit den Genehmigungsbeschlüssen verabschiedet.<sup>8</sup>

### 1.1.3. *Assoziierungs-Abkommen und Datenschutz*

Die Schengener Polizeizusammenarbeit erfolgt auf der Basis eines umfangreichen Austauschs von Personendaten. Es werden regelmässig Personendaten, darunter häufig auch besonders schützenswerte Personendaten sowie Persönlichkeitsprofile, zwischen den Polizeibehörden der beteiligten Staaten ausgetauscht. Diese intensive Bearbeitung von Personendaten verlangt nach einem entsprechenden Datenschutzstandard. Die Europäische Union hat deshalb nicht bloss die Aufgabenerfüllung umschrieben und wirkungsvolle Informationssysteme bereitgestellt (so das SIS<sup>9</sup> und – für Dublin – die Eurodac<sup>10</sup>), sondern im Bewusstsein, dass solche Systeme auch schwerwiegende Eingriffe in die Persönlichkeitsrechte der betroffenen Personen zur Folge haben können, entsprechende Datenschutzregeln aufgestellt. Staaten, die diese Systeme verwenden, müssen sich an diese Datenschutzregeln halten.<sup>11</sup> Insgesamt sind es im Wesentlichen vier Erlasse, die für das Datenschutzrecht und namentlich auch für die Datenschutzgesetzgebung der Kantone verbindlich sind.

Bedeutsam sind zunächst das Übereinkommen vom 19. Juni 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985<sup>12</sup> (abgekürzt SDÜ) sowie die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24. Oktober 1995<sup>13</sup> (abgekürzt EU-DSRL). Mit Art. 2 Abs. 2 und Abschnitt 5 von Anhang B SAA hat sich die Schweiz verpflichtet, das SDÜ und die EU-DSRL umzusetzen und anzuwenden.

Das SDÜ verlangt im Übrigen die Gewährleistung eines Datenschutzstandards, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (SR 0.235.1; abgekürzt ER-Konv 108), das für die Schweiz am

<sup>8</sup> Bundesbeschluss über die Genehmigung und die Umsetzung der bilateralen Abkommen zwischen der Schweizer und der EU über die Assoziierung an Schengen und an Dublin; BBl 2004, 7149 ff.

<sup>9</sup> Das SIS enthält über 12 Mio. Datensätze über gesuchte und vermisste Personen beziehungsweise verschwundene Gegenstände wie Fahrzeuge oder Waffen. Vgl. Beat Rudin, Datenschutzgesetze – fit für Europa, Europarechtliche Anforderungen an die schweizerischen Datenschutzgesetze; Schriften zum Datenrecht, Band 2, Zürich/Basel/Genf 2007, 11 (nachfolgend zitiert: Beat Rudin, Datenschutzgesetze).

<sup>10</sup> Mit der elektronischen Datenbank «Eurodac» können mehrfach gestellte Asylgesuche systematisch erkannt werden. Beat Rudin, Datenschutzgesetze, a.a.O., 11.

<sup>11</sup> Vgl. zu den einzelnen Erlassen der Europäischen Union: Beat Rudin, Datenschutzgesetze, a.a.O., 12.

<sup>12</sup> Amtsblatt Nr. L 239 vom 22.09.2000, S. 19 ff.; <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:DE:PDF..>

<sup>13</sup> Amtsblatt Nr. L 281 vom 23.11.1995, 31 ff.; <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML..>

1. Februar 1998 in Kraft getreten ist, ergibt.<sup>14</sup> Diesbezüglich existiert ergänzend das Zusatzprotokoll zum Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 8. November 2001 (SR 0.235.11; abgekürzt ZP zur ER-Konv 108). Die eidgenössischen Räte haben am 24. März 2006 parallel zur Revision des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (SR 235.1; abgekürzt eidgDSG) den Bundesbeschluss über den Beitritt der Schweiz zum ZP zur ER-Konv 108 angenommen. Die Referendumsfrist ist am 13. Juli 2006 unbenutzt abgelaufen. Das ZP zur ER-Konv 108 ist am 1. April 2008 in Kraft getreten<sup>15</sup> und damit auch für die Kantone verbindlich geworden.

Zusammenfassend ist festzuhalten, dass die schweizerischen Datenschutzgesetze den Vorgaben von SDÜ, EU-DSRL, ER-Konv 108 und ZP zur ER-Konv 108 genügen müssen, damit das In-Kraft-Setzen der beiden Assoziierungs-Abkommen unter datenschutzrechtlichen Gesichtspunkten möglich ist. Ohne die verlangten gesetzlichen Massnahmen im Bereich des Datenschutzes wird die EU den Anschluss an das SIS nicht freigeben (Art. 15 Abs. 1 SAA, und Art. 117 Abs. 2 SDÜ). Im Rahmen der Kommentierung der einzelnen Artikel in Ziffer 3 dieser Botschaft wird – wo erforderlich – jeweils auf die einzelnen europarechtlichen Grundlagen hingewiesen.

## 1.2. Revision des eidgenössischen Datenschutzgesetzes

Anlass zur Revision des eidgenössischen Datenschutzgesetzes, die am 1. Januar 2008 in Kraft getreten ist, bildeten nicht primär die beiden Assoziierungs-Abkommen, sondern zwei in den Jahren 1999 beziehungsweise 2000 angenommene Motionen,<sup>16</sup> die einerseits eine Verstärkung der Transparenz beim Beschaffen von Daten und andererseits eine formelle gesetzliche Grundlage für Online-Verbindungen zu Datenbanken des Bundes sowie einen Mindestschutz bei der Bearbeitung von Daten durch die Kantone beim Vollzug von Bundesrecht verlangten. Ferner mussten einzelne Bestimmungen des Bundesgesetzes angepasst werden, damit die Schweiz die Vorgaben des ZP zur ER-Konv 108 erfüllt.

Die Teilrevision des eidgenössischen Datenschutzgesetzes verlangt von den Daten bearbeitenden Stellen die aktive Information der betroffenen Person, wenn besonders schützenswerte Daten und Persönlichkeitsprofile beschafft werden. Bei Personendaten, die nicht besonders schützenswert sind und auch kein Persönlichkeitsprofil darstellen, muss für die betroffene Person zumindest erkennbar sein, dass Daten beschafft werden. Die Revision umfasst ausserdem verschiedene Änderungen hinsichtlich der Pflicht zur Meldung von Datensammlungen, und sie stärkt die Rechtsstellung von Personen, die sich der Bearbeitung von sie betreffenden Daten widersetzen. Sie legt ausserdem die Mindestanforderungen fest, denen die Kantone im Bereich des Datenschutzes genügen müssen, wenn sie Bundesrecht vollziehen, und sie verstärkt die Kontrollmöglichkeiten, wenn beim Vollzug von Bundesrecht Personendaten bearbeitet werden.

## 1.3. Situation im Kanton St.Gallen

Im Gegensatz zur überwiegenden Zahl der Kantone verfügt der Kanton St. Gallen noch über kein Datenschutzgesetz, nachdem der Kantonsrat im Jahr 1992 auf den Entwurf eines Datenschutzgesetzes nicht eingetreten war. Aufgrund des In-Kraft-Tretens des eidgenössischen Da-

<sup>14</sup> Art. 117 SDÜ für Datenbearbeitungen im Rahmen des SIS und Art. 126 SDÜ für Datenbearbeitungen ausserhalb des Rahmens des SIS.

<sup>15</sup> AS 2008, 731 ff.

<sup>16</sup> Motion «Erhöhte Transparenz bei der Erhebung von Personendaten» und Motion «Erhöhter Schutz für Personendaten bei Online-Verbindungen»; vgl. Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003, 2101.

tenschutzgesetzes am 1. Juli 1993 sah sich die damals den Entwurf des Staatsverwaltungsgesetzes vorberatende Kommission veranlasst, dem Kantonsrat zu beantragen, die Grundzüge des Datenschutzes in dieses Gesetz aufzunehmen und die Gemeinden mittels einer Bestimmung im Gemeindegesetz zur sachgemässen Anwendung des kantonalen Datenschutzrechts auf kommunaler Ebene zu verpflichten.<sup>17</sup> Der Kantonsrat folgte den Kommissionsanträgen.

Das Staatsverwaltungsgesetz (sGS 140.1; abgekürzt StVG) enthält in Art. 8 und 9 zwei grundsätzliche Bestimmungen über die Bearbeitung und die Bekanntgabe von Personendaten. Art. 10 StVG hält die Rechte der betroffenen Person, insbesondere das Recht auf Auskunft und Einsicht sowie die Berichtigung von Personendaten, fest. Art. 11 StVG verpflichtet die Regierung, ein Kontrollorgan zu bezeichnen, das für die Einhaltung des Datenschutzes sorgt. Art. 9bis des Gemeindegesetzes (sGS 151.2; abgekürzt GG) hält fest, dass die Vorschriften über den Datenschutz in der Staatsverwaltung sachgemäss für die Gemeinden gelten, wobei die Regierung Ausnahmen festlegen kann. In Ausführung der Bestimmungen des Staatsverwaltungsgesetzes erliess die Regierung am 24. Oktober 1995 die Datenschutzverordnung (sGS 142.11; abgekürzt DSV), die am 1. Januar 1996 in Vollzug trat.

Die Staatswirtschaftliche Kommission befasste sich in den Jahren 1998 und 1999 sowie letztmals im Jahr 2004 mit dem Datenschutz in der Staatsverwaltung. In ihrem Bericht 2004 stellte sie einen Rückblick auf die Entwicklung des Datenschutzrechts im Kanton St.Gallen an, sie fasste die dem kantonalen Kontrollorgan zukommenden Aufgaben zusammen und warf verschiedene Fragen zur Umsetzung des Datenschutzrechts auf.<sup>18</sup> Die Schlussfolgerung der zuständigen Subkommission, sie hätte «nach dem Abschluss der Prüfungstätigkeit ... nicht behaupten können, der Datenschutz werde auf kantonomer Stufe optimal umgesetzt», veranlasste die Staatswirtschaftliche Kommission zu folgender Empfehlung:<sup>19</sup>

«Die Staatswirtschaftliche Kommission empfiehlt, die zeitgemässe Umsetzung der kantonalen Bestimmungen über den Datenschutz zu überprüfen, namentlich:

1. die heutige Stellung des kantonalen Kontrollorgans für den Datenschutz;
2. die zur Verfügung stehenden personellen Ressourcen des kantonalen Kontrollorgans für den Datenschutz;
3. die kantonalen Rechtsgrundlagen, insbesondere deren Genügen.»

Aufgrund der zwischenzeitlich eingetretenen Entwicklung in Bezug auf die Umsetzung der Assoziierungs-Abkommen zwischen der Schweiz und der Europäischen Union erachtete es die Regierung als geboten, den Erlass eines Datenschutzgesetzes dann in die Wege zu leiten, wenn der Umsetzungsbedarf konkreter erkennbar ist. Im Hinblick auf die Klärung der offenen Fragen ermächtigte sie die Staatskanzlei, ein Gutachten zur kantonalen Datenschutzgesetzgebung in Auftrag zu geben. Mit der Ausarbeitung des Gutachtens wurde Dr. Beat Rudin, Advokat, Lehrbeauftragter an der Universität Basel sowie Stiftungsrat und Geschäftsführer der Stiftung für Datenschutz und Informationssicherheit, beauftragt. Der Gutachter ist Autor verschiedener Publikationen zum Datenschutz.<sup>20</sup> Er verfasste überdies im Auftrag der Konferenz der Kantonsregierungen (KdK) das als Arbeitsinstrument für den Erlass oder die Anpassung von Datenschutzgesetzen dienende Dokument «Umsetzung Schengen/Dublin in den Kantonen: Datenschutz, Wegleitung» vom 15. März 2006<sup>21</sup> (abgekürzt KdK-Wegleitung).

<sup>17</sup> Vgl. Votum des Präsidenten der vorberatenden Kommission betreffend 22.93.02 Staatsverwaltungsgesetz, in: ProtKR 1992/96 Nr. 414 / 2.

<sup>18</sup> Bericht 2004 der Staatswirtschaftlichen Kommission zur Staatsverwaltung vom 19. August 2004, 8 f.

<sup>19</sup> Bericht 2004 der Staatswirtschaftlichen Kommission zur Staatsverwaltung vom 19. August 2004, 9.

<sup>20</sup> Unter anderem die in dieser Vorlage mehrfach zitierte Publikation «Datenschutzgesetze – fit für Europa. Europarechtliche Anforderungen an die schweizerischen Datenschutzgesetze», Zürich / Basel / Genf 2007.

<sup>21</sup> [http://www.datenschutz.ch/themen/2006\\_kdk\\_schengen\\_dublin\\_datenschutz\\_wegleitung.pdf](http://www.datenschutz.ch/themen/2006_kdk_schengen_dublin_datenschutz_wegleitung.pdf).

Das Gutachten, in das die Wegleitung zuhanden der Konferenz der Kantonsregierungen einbezogen ist, wurde am 28. März 2007 erstattet. In Bezug auf die Erlassstufe wird festgestellt, dass die materiellen Grundregeln des Datenschutzes – insbesondere die Grundsätze des Bearbeitens von Personendaten und die Rechte der betroffenen Personen – sowie die organisatorisch-institutionellen Regeln – insbesondere zur Datenschutzkontrolle – auf Gesetzesstufe zu erlassen sind. Die Bestimmungen im Staatsverwaltungsgesetz und die bestehende umfassende Delegation zum Erlass von Verordnungsrecht genügen nicht.

Mit Blick auf die In-Kraft-Setzung der Assoziierungs-Abkommen aufgrund eines entsprechenden Beschlusses des Rates der Europäischen Union, der sich auf eine einstimmige Zustimmung der Anwenderstaaten des Schengener Abkommens abstützen muss, ist der Erlass eines Datenschutzes dringlich geworden.

#### 1.4. Umsetzung der Assoziierungs-Abkommen auf kantonaler Ebene

In der Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union<sup>22</sup> hält der Bundesrat fest, dass die Assoziierung der Schweiz an Schengen/Dublin auch die Kantone bindet. Je nach Ausgangslage in den Kantonen bestehe im Bereich des Datenschutzes ein kantonaler Umsetzungsbedarf, weil die zum Teil sehr detaillierten Schengener Datenschutzregelungen in ihrem Kompetenzbereich auch von den kantonalen Behörden angewendet werden müssten.<sup>23</sup> Die in den Assoziierungs-Abkommen enthaltenen Verpflichtungen gelten nicht nur im Verhältnis des Bundes zur Europäischen Union, sondern im Rahmen der verfassungsrechtlichen Zuständigkeitsordnung auch für die Kantone. Soweit den Kantonen nach Massgabe von Art. 3 der Bundesverfassung (SR 101; abgekürzt BV) Zuständigkeiten zukommen, sind sie gehalten, für ihre Zuständigkeitsbereiche die im internationalen Recht enthaltenen Vorgaben einzuhalten. Mit anderen Worten: Im jeweiligen Kompetenzbereich müssen die massgebenden internationalen Erlasse auch von den Kantonen umgesetzt und angewendet werden.<sup>24</sup> In Bezug auf den Datenschutz ist bedeutsam, dass die Kantone ein dem europäischen Recht – das heisst insbesondere der EU-DSRL – gleichwertiges Schutzniveau gewährleisten müssen. Das gleichwertige Schutzniveau ist dann gegeben, wenn der betroffenen Person in Bezug auf die Bearbeitung ihrer Daten ein Schutz zuteil wird, der dem Kernbestand der Schutzprinzipien der EU-DSRL im Wesentlichen gerecht wird.<sup>25</sup> Mit dem SIS erhalten die Polizeibehörden für ihre Aufgabenerfüllung Zugriff auf eine Datenbank mit mehreren Millionen Einträgen, und sie können ihre Ausschreibungen von Personen und Sachen in einem Fahndungsraum von 27 Schengen-Staaten (nach Einbindung der neuen EU-Mitglieder) und etwa 450 Millionen Einwohnerinnen und Einwohnern verbreiten. Entsprechend dem Wirkungsgewinn sind die Kantone verpflichtet, ihre Kontrollen im Datenschutzbereich zu verstärken. Dies verlangt nicht bloss die reaktive Beantwortung von Fragen oder Beschwerden von betroffenen Personen, sondern eine wirksame und aktive, das heisst anlassfreie Kontrolle.

<sup>22</sup> Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II») vom 1. Oktober 2004; BBl 2004, 5965 ff.

<sup>23</sup> Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II») vom 1. Oktober 2004; BBl 2004, 5965 ff., 6183. Zur Umsetzung der Datenschutzrichtlinie (EU-DSRL) vgl. a.a.O., 6175 f.

<sup>24</sup> Das eidgenössische Datenschutzgesetz macht den Erlass von kantonalen Datenschutzgesetzen nicht entbehrlich. Dem Bund kommt nämlich keine Kompetenz zu, ein für die Zuständigkeitsbereiche der Kantone geltendes Datenschutzrecht zu erlassen. Art. 37 eidgDSG, der den Kantonen Vollzugsaufgaben im Datenschutz überträgt, gilt nur dann, wenn kantonale Organe Bundesrecht vollziehen, nicht aber, wenn sie im Rahmen eigener Zuständigkeitsbereiche handeln. Vgl. Beat Rudin, Rz. 9 ff. zu Art. 37 eidgDSG, in: Basler Kommentar zum Datenschutzgesetz, hrsg. von Urs Maurer-Lambrou und Nedim Peter Vogt, 2. Aufl., Basel / Genf / München 2006.

<sup>25</sup> Vgl. Botschaft des Bundesrates zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen («Bilaterale II») vom 1. Oktober 2004; BBl 2004, 5965 ff., 6241.

## **2. Bestimmungsfaktoren für den Inhalt des Datenschutzgesetzes**

### **2.1. Regelung der allgemeinen Datenschutzgrundsätze**

Das kantonale Datenschutzgesetz hat die allgemeinen Datenschutzgrundsätze festzuhalten. Der Vergleich zwischen den Anforderungen, wie sie von den erwähnten europarechtlichen Erlassen aufgestellt werden,<sup>26</sup> mit dem geltenden Recht führt – zusammengefasst – zu folgender Beurteilung:

Im geltenden kantonalen Recht fehlen die für die Bearbeitung von Personendaten zentralen Grundsätze der Zweckbindung sowie der Richtigkeit und Vollständigkeit. Ferner fehlen hinreichend konkrete Bestimmungen zur Sicherstellung der Transparenz in den Datenbearbeitungen. Im Weiteren besteht kein gesetzlicher Anspruch auf Unterlassung der Datenbearbeitung oder Beseitigung der Daten, wenn eine Bearbeitung widerrechtlich erfolgt ist. Sodann ist keine Bestimmung über die Voraussetzungen vorhanden, die bei der Bekanntgabe von Personendaten ins Ausland hinsichtlich der Gewährleistung eines angemessenen Schutzes erfüllt sein müssen. Ferner besteht keine Verpflichtung zur Durchführung einer so genannten Vorabkontrolle, was dann erforderlich ist, wenn die Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen verbunden ist.

Die Umsetzung der allgemeinen Datenschutzgrundsätze verlangt den Erlass von Bestimmungen über die Bearbeitung von Personendaten, über die Bekanntgabe von Personendaten und über die Rechte der betroffenen Person.

### **2.2. Einführung eines unabhängigen Kontrollorgans**

Art. 28 EU-DSRL schreibt ein öffentliches Kontrollorgan vor, das seine Aufgaben in «völliger Unabhängigkeit» wahrnimmt. Das ZP zur ER-Konv 108 verlangt, dass Datenbearbeitungen durch eine «völlig unabhängige» Aufsichtsbehörde überwacht werden müssen. Die geforderte «völlige Unabhängigkeit» ist ausdrücklich im Gesetz festzuhalten. Ferner bedarf es institutioneller Sicherungen, welche die Unabhängigkeit garantieren. Es gibt diesbezüglich nicht eine einzige richtige Lösung, sondern es liegt an der Kombination von institutionellen Garantien, die Unabhängigkeit zu gewährleisten.<sup>27</sup> Entscheidend ist, dass die Regelungen in ihrer Gesamtheit Gewähr für die verlangte Unabhängigkeit der Datenschutzaufsicht bieten. Den Garantien ist namentlich Rechnung zu tragen durch:

- Festlegung einer die Unabhängigkeit unterstützenden Zuständigkeit für die Wahl der Leitung des Kontrollorgans;
- die ausschliesslich administrative Zuordnung des Kontrollorgans zur Verwaltung;
- die abschliessende Budgetantragskompetenz des Kontrollorgans;
- eine ausserhalb der Verwaltungsbehörden angesiedelte Aufsichtskompetenz;
- die dem Kontrollorgan zustehende Selbstständigkeit bei der Planung und der Durchführung von Kontrollen;
- Einräumung von Befugnissen mit Einwirkungsmöglichkeiten.

Der vorliegende Gesetzesentwurf (abgekürzt GE) ist auf diese Elemente ausgerichtet. Im nachfolgenden Abschnitt mit den Bemerkungen zu den einzelnen Artikeln des Gesetzesentwurfs wird jeweils bei den einschlägigen Normen auf die Umsetzung der Sicherstellungsgarantien beziehungsweise das Erfordernis der Unabhängigkeit eingegangen.

<sup>26</sup> SDÜ, EU-DSRL, ER-Konv 108 und ZP zur ER-Konv 108.

<sup>27</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O., 73 f.

### 3. Bemerkungen zu einzelnen Artikeln

Im *Ingress* wird festgehalten, dass das Datenschutzgesetz einen Erlass darstellt, der das in Art. 2 Bst. g der Kantonsverfassung (sGS 111.1; abgekürzt KV) erwähnte Grundrecht des Schutzes der Privatsphäre, «einschliesslich Schutz vor Missbrauch persönlicher Daten», ausführt. Die Umsetzung kommt namentlich in den Abschnitten über die Bearbeitung und die Bekanntgabe von Personendaten zum Ausdruck.

#### 3.1. Allgemeine Bestimmungen

Dieser Teil des Erlasses enthält die Umschreibung der für die nachfolgenden Bestimmungen relevanten Begriffe in Gestalt von detailliert formulierten Legaldefinitionen. Ferner legt er den Geltungsbereich des Datenschutzgesetzes fest.

Art. 1 enthält die für das Datenschutzrecht relevanten Begriffe in Gestalt von Legaldefinitionen. Wie bei Art. 3 eidgDSG geht es teils um die Abgrenzung der datenschutzrechtlich verwendeten Begriffe vom allgemeinen Sprachgebrauch und um die Vermeidung von Unklarheiten, teils um die Verkürzung der im Gesetzesentwurf beziehungsweise im künftigen Gesetz enthaltenen Regelungen durch Zusammenfassung mehrerer Tatbestände in einem einzigen Begriff.<sup>28</sup> Letzteres wird – nebst Art. 1 Bst. b, c, e und f – insbesondere auch mit Art. 1 Bst. h angestrebt. Mit dem Begriff «öffentliches Organ» werden sämtliche Organisationseinheiten auf kantonaler und auf Gemeindeebene bezeichnet, die Personendaten bearbeiten oder bekanntgeben oder sonst wie datenschutzrelevant wirken. Als öffentliche Organe gelten auch Private, wenn sie nach Massgabe von Art. 25 Abs. 1 und 3 KV Staatsaufgaben erfüllen.<sup>29</sup>

Aus der Zuordnung der Organe, Behörden und Dienststellen von Gemeinden, selbstständigen öffentlich-rechtlichen Gemeindeunternehmen sowie Gemeindeverbänden und Zweckverbänden unter die als «öffentliches Organ» bezeichneten Normadressaten des vorliegenden Gesetzes geht hervor, dass das Datenschutzgesetz unmittelbar und nicht bloss «sachgemäss» – wie dies für das bestehende Datenschutzrecht in Art. 9bis GG festgehalten wird – auch für die Gemeinden gilt. Dabei besteht keine Differenzierung zwischen politischer Gemeinde und Spezialgemeinde; auch Schulgemeinden, Ortsgemeinden und örtliche Korporationen sind verpflichtet, die Datenschutzbestimmungen dieses Gesetzes zu beachten beziehungsweise anzuwenden, wenn sie im Sinn von Art. 1 Bst. e GE Personendaten bearbeiten.

In institutioneller Hinsicht verlangen die europarechtlichen Anforderungen ein Datenschutzkontrollorgan, dem vorab Aufsichts- und Beratungsbefugnisse, verbunden mit so genannten Einwirkungsmöglichkeiten, zukommen. Im Kanton St.Gallen sollen die Datenschutzkontrollorgane als Fachstellen bezeichnet werden, weil ihr Aufgabenbereich mehr umfasst als die Durchführung von Kontrollen. Der Begriff der Fachstelle für Datenschutz wird mit Art. 1 Bst. j GE eingeführt. Die Bezeichnung «Fachstelle» anstatt «Kontrollorgan» oder «Aufsichtsbehörde» soll verdeutlichen, dass die Tätigkeiten dieser Institution über das Kontrollieren oder Beaufsichtigen hinausgehen und beispielsweise auch die Mitwirkung und die Beratung umfassen. In Bezug auf die Aufgaben ist auf die Art. 30 und 34 ff. GE zu verweisen.

Von besonderer Bedeutung sind Art. 1 Bst. k und l GE. Im Rahmen des Datenschutzrechts spielen das Legalitätsprinzip und dabei namentlich die Differenzierung zwischen formellem Gesetz und anderen Arten von Rechtsgrundlagen eine besondere Rolle. Nach Art. 5 Abs. 1 KV bedürfen staatliche Einschränkungen von Grundrechten nach Massgabe der Bundesverfassung einer gesetzlichen Grundlage. Dieselbe Regelung ist in Art. 36 Abs. 1 erstem Satz BV

<sup>28</sup> Vgl. Georg Müller, *Elemente einer Rechtssetzungslehre*, 2. Aufl., Zürich, Basel, Genf 2006, Fussnote 711 zur Rz. 352.

<sup>29</sup> Unter den Begriff «Staatsaufgaben» fallen nach der Konzeption von Art. 24 ff. KV sowohl die vom Kanton wahrgenommenen Aufgaben (kantonale Aufgaben) wie auch die von den Gemeinden erfüllten Aufgaben (Gemeindeaufgaben).

enthalten, während der zweite Satz von Art. 36 Abs. 1 BV bestimmt, dass schwerwiegende Einschränkungen im Gesetz selbst, das heisst in einem Gesetz im formellen Sinn, vorgesehen sein müssen.<sup>30</sup> Als formelles Gesetz gilt ein Gesetz, das nach Art. 67 Ingress KV vom Kantonsrat mit ausdrücklicher oder stillschweigender Zustimmung der Stimmberechtigten erlassen worden ist. Wenn der Gesetzesentwurf verlangt, dass sich das Handeln eines öffentlichen Organs auf ein «Gesetz» oder eine «gesetzliche Grundlage» abstützen muss, so ist damit ein formelles Gesetz gemeint; wenn demgegenüber eine «Rechtsgrundlage» oder eine «rechtliche Grundlage» für ein bestimmtes datenschutzrelevantes Handeln vorausgesetzt wird, kann diese auch in Form einer Verordnung bestehen. Dem formellen Gesetz sind zwischenstaatliche Vereinbarungen mit Verfassungs- und Gesetzesrang gleichgestellt, weil diese nach Art. 48 Bst. b und Art. 49 Abs. 1 Bst. b KV der ausdrücklichen oder stillschweigenden Zustimmung der Stimmberechtigten unterliegen. Auf kommunaler Ebene entsprechen die Gemeindeordnung sowie die rechtsetzenden Reglemente und die rechtsetzenden Vereinbarungen dem Begriff des formellen Gesetzes, indem diese Erlasse ebenfalls im Verfahren mit ausdrücklicher oder stillschweigender Zustimmung der Stimmberechtigten zustande kommen (Art. 5 in Verbindung mit Art. 35 Abs. 3 Bst. a, Art. 36 Bst. a und b sowie Art. 110 Bst. a und Art. 111 Abs. 1 Bst. a und b GG). Der Verordnung entsprechen auf Gemeindeebene die Vollzugsvorschriften, soweit diese vom fakultativen Referendum ausgenommen worden sind (vgl. Art. 38 Abs. 2 und Art. 99 Abs. 1 Bst. b GG).

Art. 2 umschreibt den Geltungsbereich des Datenschutzgesetzes. Als Grundsatz gilt, dass das Gesetz für die Bearbeitung von Personendaten durch öffentliche Organe, also durch Organe, Behörden und Dienststellen nach Art. 1 Bst. h GE, anzuwenden ist (Art. 2 Abs. 1 GE). Art. 2 Abs. 2 GE enthält in abschliessender Aufzählung die Ausnahmen von diesem Grundsatz.

Keine Anwendung findet das Datenschutzgesetz nach Art. 2 Abs. 2 Bst. a GE, wenn das öffentliche Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt, das heisst, wenn es privatrechtlich tätig ist. In diesem Fall gelten – gleichermassen wie für die privatrechtliche Tätigkeit von Bundesorganen – die Bestimmungen des Datenschutzgesetzes des Bundes für die Bearbeitung von Personendaten durch private Personen (vgl. Art. 23 Abs. 1 eidgDSG).

Im Weiteren ist das Datenschutzgesetz nach Art. 2 Abs. 2 Bst. b GE nicht anzuwenden, wenn Personendaten zum ausschliesslich persönlichen Gebrauch, ohne jegliche Aussenwirkung, bearbeitet werden. Es geht dabei in der Hauptsache um die Verwendung von so genannten höchstpersönlichen Arbeitsmitteln, wie etwa der Agenda, oder um die Anfertigung von nur persönlich gebrauchten (Hand-)Notizen oder Vorgehensskizzen.

In Art. 2 Abs. 2 Bst. c GE wird die Anwendbarkeit des Datenschutzgesetzes in Übereinstimmung mit Art. 2 Abs. 2 Bst. c eidgDSG in Bezug auf Rechtspflege- und Rechtshilfeverfahren ausgeschlossen. Nicht unter den Ausschluss fallen – gleich wie die erstinstanzlichen Verwaltungsverfahren beim Bund nach Art. 2 Abs. 2 Bst. c eidgDSG – das Verwaltungsverfahren sowie das verwaltungsinterne Rechtsmittelverfahren. Deshalb ist in Art. 2 Abs. 2 Bst. c GE die Wendung «gerichtliche Verwaltungsrechtspflege» aufzunehmen.

Art. 2 Abs. 2 Bst. d GE berücksichtigt den Umstand, dass die Archive von Kanton und Gemeinden ebenfalls öffentliche Organe nach Art. 1 Bst. h GE sind. Die für die Tätigkeiten dieser Archive massgebenden datenschutzrechtlichen Vorgaben sind indessen nicht Gegenstand des Datenschutzgesetzes, sondern der Archivgesetzgebung. Würde das Datenschutzgesetz angewendet, würde die Archivierung von Dokumenten der Verwaltungsstellen erheblich behindert, in Teilen gar verunmöglicht. Aus diesem Grund sind die Archive von Kanton und Gemeinden –

---

<sup>30</sup> Vgl. zum Beispiel BGE 130 I 362 mit Hinweisen auf weitere Urteile.

gleich wie in anderen Kantonen<sup>31</sup> – vom Geltungsbereich des Datenschutzgesetzes auszunehmen. Im künftigen Archivgesetz werden Bestimmungen aufzunehmen sein, die den Missbrauch von archivierten Daten verhindern, was namentlich durch das Festschreiben von Schutzfristen zu erfolgen hat.

### 3.2. Bestimmungen über die Bearbeitung von Personendaten

Dieser Abschnitt enthält Bestimmungen über die vom zuständigen öffentlichen Organ zu beachtenden Grundsätze beim Umgang mit Personendaten.

*Art. 3:* Die Pflicht zur Einhaltung der datenschutzrechtlichen Vorgaben bei der Bearbeitung von Personendaten kann nicht einer bestimmten, für diesen Zweck eingerichteten Stelle, insbesondere auch nicht dem Kontrollorgan beziehungsweise – in der Terminologie des vorliegenden Gesetzesentwurfs der Fachstelle für Datenschutz – übertragen oder delegiert werden. Vielmehr hat jedes öffentliche Organ im Sinn von Art. 2 Bst. h GE, das Personendaten bearbeitet oder bearbeiten lässt, die Datenschutzbestimmungen zu befolgen und ist hierfür verantwortlich. Diese Verantwortlichkeit erstreckt sich insbesondere auf die für die Bearbeitung von Personendaten massgebenden Grundsätze von Rechtmässigkeit, Treu und Glauben, Zweckbindung, Verhältnismässigkeit, Richtigkeit und Vollständigkeit sowie Datensicherheit.<sup>32</sup> Die Datenschutzgesetze verschiedener Kantone und das Datenschutzgesetz des Bundes führen diese Grundsätze ausdrücklich auf; in Bezug auf das eidgenössische Datenschutzgesetz ist diesbezüglich namentlich auf Art. 4 eidgDSG hinzuweisen. Es genügt indessen, in Art. 4 GE jene Grundsätze aufzuführen, denen eine für den Datenschutz spezifische Bedeutung zukommt, nachdem bereits Art. 8 KV generell die Grundsätze rechtsstaatlichen Handelns nennt.

Wenn mehrere öffentliche Organe auf der Basis einer Datensammlung, also eines Bestandes von Personendaten nach Art. 2 Bst. g GE, Personendaten bearbeiten, ist eines der beteiligten öffentlichen Organe als für die Einhaltung des Datenschutzrechtes verantwortliche Stelle zu bezeichnen. Welches öffentliche Organ die Verantwortung trägt, bedarf der Abmachung zwischen den beteiligten öffentlichen Organen. Kommt eine Abmachung mangels Einigkeit nicht zustande, hat die kantonale Fachstelle für Datenschutz zu entscheiden. Die Zuordnung dieser Entscheidungsbefugnis an die kantonale Fachstelle berücksichtigt den Sachverhalt, dass Datensammlungen zunehmend staatebenenübergreifend genutzt werden, weshalb von einer differenzierten Regelung, welche die Entscheidung je nach Betroffenheit sowohl der zuständigen Gemeindefachstelle für Datenschutz und der kantonalen Fachstelle für Datenschutz überliesse, abgesehen werden soll.

*Art. 4* auferlegt dem öffentlichen Organ die Verpflichtung, Personendaten im Rahmen des dafür festgelegten Zwecks zu bearbeiten. In Art. 4 Abs. 1 GE wird der Grundsatz der Zweckbindung festgehalten. Die Zweckbindung ist eines der Kernelemente des Datenschutzrechtes. Sie wird in Art. 6 Abs. 1 Bst. b erstem Satz und Bst. c EU-DSRL wie folgt umschrieben (vgl. auch Art. 5 Bst. b und c ER-Konv 108):

«Die Mitgliedstaaten sehen vor, dass personenbezogene Daten:

- b) für festgelegte eindeutige und rechtmässige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. ...
- c) den Zwecken entsprechen, für die sie erhoben und / oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen».

<sup>31</sup> Vgl. zum Beispiel Art. 1 Abs. 5 Bst. b des Datenschutzgesetzes des Kantons Graubünden (Bündner Rechtsbuch, 171.100) und § 3 Abs. 4 des Datenschutzgesetzes des Kantons Basel-Stadt (Gesetzessammlung des Kantons Basel-Stadt, 153.260).

<sup>32</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O., 45.

Der Zweck – oder auch die Rechtfertigung für die Bearbeitung von Personendaten<sup>33</sup> – ergibt sich aus dem Gesetz, ist bei der Beschaffung der Personendaten ausdrücklich angegeben worden oder ist aus den Umständen ersichtlich. «Eine Zweckänderung, also die Verwendung von Personendaten zu einem anderen als dem ursprünglich vorgesehenen und durch die Rechtfertigung abgedeckten Bearbeitungszweck, bedarf einer erneuten Rechtfertigung.»<sup>34</sup>

Art. 4 Abs. 2 GE trägt im ersten Satzteil dem Transparenzgebot Rechnung, das ein weiteres Kernelement des Datenschutzes bildet. Wenn Personendaten beschafft und bearbeitet werden, müssen Beschaffung und Zweck der Bearbeitung für die betroffenen Personen erkennbar sein. Instrumente für die Erkennbarkeit sind im Wesentlichen die Informationspflicht nach Art. 6 GE, das Recht auf Auskunft und Einsicht nach Art. 17 GE sowie die Öffentlichkeit des Registers über Datensammlungen nach Art. 38 Abs. 3 GE.

Art. 4 Abs. 2 GE enthält im zweiten Satzteil die Grundsätze von Richtigkeit und Vollständigkeit der Personendaten. Was die Richtigkeit betrifft, so ist diese hinsichtlich des Datenschutzes Ausfluss aus dem Verhältnismässigkeitsprinzip nach Art. 8 Abs. 2 KV; die Bearbeitung von unrichtigen Personendaten zur behördlichen Aufgabenerfüllung widerspräche dem Grundsatz der Verhältnismässigkeit.<sup>35</sup> Personendaten sind, um dem Erfordernis der Richtigkeit zu genügen, wenn nötig auf den neuesten Stand zu bringen (Art. 6 Abs. 1 Bst. d erster Satzteil EU-DSRL; Art. 5 Bst. d ER-Konv 108). Richtig sind Personendaten zudem erst, wenn sie mit Blick auf die Aufgabe, zu deren Erfüllung sie benötigt werden, vollständig sind. Insofern ist das Vollständigkeitsgebot Teil des Grundsatzes der Richtigkeit der Personendaten.

Art. 4 Abs. 3 GE bezieht sich auf die Datensicherheit und berücksichtigt Art. 17 Abs. 1 EU-DSRL. Darnach müssen geeignete technische und organisatorische Massnahmen durchgeführt werden, «die für den Schutz gegen die zufällige oder unrechtmässige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmässigen Verarbeitung personenbezogener Daten erforderlich sind. Diese Massnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.» Ähnlich lautet Art. 7 ER-Konv 108, der geeignete Sicherungsmassnahmen gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie unbefugten Zugang oder unbefugtes Bekanntgeben der Personendaten fordert.

In Art. 5 wird der Grundsatz der Rechtmässigkeit als Voraussetzung für die Bearbeitung von Personendaten aufgeführt. Die Übernahme dieses allgemein in Art. 8 Abs. 1 KV enthaltenen Grundsatzes in das Gesetz ist im Zusammenhang mit der Differenzierung bei der Bearbeitung von (gewöhnlichen) Personendaten sowie von besonders schützenswerten Personendaten und Persönlichkeitsprofilen erforderlich.

Für die Bearbeitung von Personendaten genügt nach Art. 5 Abs. 1 GE entweder eine Rechtsgrundlage, die auch in Form von Verwaltungsrecht gegeben sein kann (vgl. Art. 2 Bst. k und l GE), oder das Bestehen einer gesetzlich vorgesehenen Aufgabe, zu deren Erfüllung die Bearbeitung von Personendaten erforderlich ist. Ist eine dieser Voraussetzungen erfüllt, handelt das öffentliche Organ rechtmässig im Sinn von Art. 6 Abs. 1 Bst. a EU-DSRL beziehungsweise Art. 5 Bst. a ER-Konv 108.

Handelt es sich um besonders schützenswerte Personendaten, also um solche, die in Art. 1 Bst. b GE in Übereinstimmung mit Art. 8 Abs. 1 EU-DSRL und Art. 6 ER-Konv 108 definiert sind, so ist die Bearbeitung nur zulässig, wenn diese in einem formellen Gesetz vorgesehen

<sup>33</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O., 47.

<sup>34</sup> Beat Rudin, Datenschutzgesetze, a.a.O., 47.

<sup>35</sup> Beat Rudin, Datenschutzgesetze, a.a.O., 49.

oder wenn die Bearbeitung für eine im Gesetz vorgesehene Aufgabe unentbehrlich ist (Art. 5 Abs. 2 Bst. a und b GE).

Besteht keine Rechtsgrundlage in Gestalt eines formellen Gesetzes und ist auch keine Unentbehrlichkeit für die Erfüllung einer gesetzlich vorgesehenen Aufgabe gegeben, dürfen besonders schützenswerte Personendaten und Persönlichkeitsprofile nur mit ausdrücklicher Einwilligung durch die betroffene Person bearbeitet werden (Art. 5 Abs. 2 Bst. c Ziff. 1 GE). Diese Einwilligung kann nicht generell erfolgen; sie muss auf den Einzelfall bezogen sein. Überdies muss die einwilligende Person die Sachlage, das heisst Zweck und Art der vorgesehenen Bearbeitung ihrer Daten, kennen. Hat die betroffene Person ihre besonders schützenswerten Daten bereits allgemein zugänglich gemacht, so ist eine Bearbeitung ohne weiteres möglich (Art. 5 Abs. 2 Bst. c Ziff. 2 GE); weder wird dazu das Bestehen einer gesetzlichen Grundlage gefordert, noch ist es nötig, die Einwilligung der betroffenen Person einzuholen.

*Art. 6* verwirklicht das Transparenzgebot bei der systematischen Beschaffung von Personendaten. Sie überbindet dem öffentlichen Organ in Kanton und Gemeinde dieselbe Verpflichtung, wie sie nach Art. 18 eidgDSG auch für Bundesorgane gilt. Bei der systematischen Beschaffung handelt es sich in der Regel um die Erhebung von Personendaten mit Fragebogen. Führt der Kanton oder eine Gemeinde eine Umfrage durch, die eine systematischen Beschaffung von Personendaten zum Inhalt hat, so ist – in Übereinstimmung mit Art. 4 Abs. 2 GE – über Zweck und Rechtsgrundlage der Bearbeitung zu informieren (Art. 6 Bst. a GE). Ferner ist bekanntzugeben, welche Behörde oder Dienststelle des öffentlichen Organs an der Beschaffung, also beispielsweise an der Erhebung, beteiligt ist und – falls die Beschaffung mündlich durch Befragung erfolgt – wer die dabei handelnden Personen sind (Art. 6 Bst. b GE). Schliesslich ist transparent zu machen, wer in den Besitz der beschafften Personendaten gelangt, also Empfängerin oder Empfänger ist (Art. 6 Bst. c GE). Selbstverständlich fällt nicht jede Befragung beispielsweise von Gemeindeeinschwohnerinnen und Gemeindeeinschwohner unter die Bestimmungen des Datenschutzrechts. Wenn eine Gemeinde im Sinn einer formlosen Umfrage, beispielsweise durch eine Fragebogenaktion, die Meinung der Bevölkerung über eine bestimmte Angelegenheit eruieren will, handelt es sich nicht um ein dem Datenschutz unterstehendes Vorgehen. Die Datenschutzbestimmungen sind erst dann relevant, wenn es um die Beschaffung von Personendaten nach Art. 1 Bst. a und e GE oder um das Anlegen einer Datensammlung nach Art. 1 Bst. g GE geht.

*Art. 7* regelt den Sachverhalt, dass Personendaten über bestimmte oder bestimmbare Personen bearbeitet werden, wobei die Bearbeitung aber nicht auf die Personen als solche ausgerichtet ist, sondern wissenschaftlichen oder statistischen Zwecken oder als Grundlage für Planungstätigkeiten dienen. Hierfür ist keine ausdrückliche spezialgesetzliche Grundlage erforderlich. Das öffentliche Organ ist indessen zu verpflichten, die Daten zu anonymisieren, sobald es der Bearbeitungszweck zulässt (Abs. 1). Ferner hat es bei einer allfälligen Publikation der Ergebnisse sicherzustellen, dass Rückschlüsse auf betroffene Personen ausgeschlossen sind (Abs. 2), und schliesslich hat es Massnahmen zu treffen, damit andere öffentliche Organe oder Dritte, denen es die Bearbeitung überträgt, diese Verpflichtungen ebenfalls einhalten und überdies von einer Weitergabe der Personendaten absehen (Abs. 3).

*Art. 8* beschreibt die von Art. 20 EU-DSRL als «Vorabkontrolle» bezeichnete Tätigkeit des für den Datenschutz eingesetzten Kontrollorgans.<sup>36</sup> Wenn die Bearbeitung von Personendaten aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen, muss sie vorab durch das Datenschutzkontrollorgan geprüft werden. Als Kriterien für die Beurteilung der Risiken gelten beispielsweise die Zahl der erfassten Personen, die Zahl der beteiligten öffentlichen Organe oder die Sensitivität der Personendaten, wobei als Objekte der Vorabkontrolle vor allem Projekte für IT-Systeme, für Datenbanken oder für Register in Frage kommen. Die Pflicht, dem Datenschutzkontrollorgan die Vorabkontrolle zu ermöglichen, muss auf Gesetzesstufe

<sup>36</sup> Vgl. dazu Beat Rudin, Datenschutzgesetze, a.a.O., 60.

normiert werden. Als Datenschutzkontrollorgane werden nach Abschnitt V des vorliegenden Gesetzesentwurfs im Kanton und in den Gemeinden Fachstellen für Datenschutz eingesetzt. Diesen kommt mithin die Aufgabe der Vorabkontrolle nach Art. 8 GE zu.

Nach erfolgter Meldung prüft die Fachstelle für Datenschutz die vorgesehene Bearbeitung. Sie kann empfehlen, die beabsichtigte Bearbeitung zu ändern oder zu unterlassen. Bleibt die Empfehlung wirkungslos, kann die Fachstelle die Anordnung von Massnahmen nach Art. 34 Abs. 1 und Art. 35 Abs. 1 GE beantragen. Die zuständige Behörde, die über den Antrag zu befinden hat, erlässt nach Art. 34 Abs. 2 beziehungsweise Art. 35 Abs. 2 GE gegebenenfalls eine Verfügung, die nach Massgabe des Gesetzes über die Verwaltungsrechtspflege (sGS 951.1; abgekürzt VRP) mit Rekurs beziehungsweise Beschwerde angefochten werden kann.

*Art. 9* berücksichtigt, dass das Outsourcing auch von Datenbearbeitungen zunehmend an Bedeutung gewinnt. Der geltende Art. 18 DSV lässt die Bearbeitung von Personendaten durch Dritte zwar zu, stellt aber keine explizite Regelung dar, unter welchen Voraussetzungen die Bearbeitung durch aussenstehende Dritte möglich ist. Gerade beim Outsourcing besteht aber eine erhöhte Gefahr der Verletzung von Persönlichkeitsrechten von betroffenen Personen, wenn nicht sichergestellt wird, dass sich die Dritten an dieselben gesetzlichen Vorgaben halten müssen, wie sie für das öffentliche Organ gelten.

Nach Art. 9 Abs. 1 GE ist eine Übertragung an Dritte zulässig, wenn nicht ein Gesetz die Übertragung untersagt. Zudem müssen die in Frage kommenden Dritten Gewähr für eine datenschutzrechtlich einwandfreie Bearbeitung bieten. Wie die Übertragung erfolgt, bemisst sich nach dem Einzelfall. Denkbar ist, dass ein Gesetz oder eine andere allgemein verbindliche Rechtsgrundlage die Bearbeitung durch Dritte vorsieht. Eine Übertragung kann ferner durch Verfügung erfolgen. In der Regel wird die Bearbeitung im Rahmen einer Vereinbarung, beispielsweise einer Leistungsvereinbarung, übertragen. Für den Fall einer vorsätzlichen Zuwiderhandlung gegen die im Auftrag zur Datenbearbeitung enthaltenen Bestimmungen ist eine Strafbestimmung in das Gesetz aufzunehmen (vgl. Art. 40 GE).

In Art. 9 Abs. 2 Bst. a und b GE wird festgelegt, dass sich Dritte, denen die Bearbeitung von Personendaten übertragen worden ist, denselben datenschutzrechtlichen Pflichten unterzuordnen haben, wie sie für das öffentliche Organ gelten. Die Übertragung darf also nicht zu einer Lockerung des Datenschutzes führen. Art. 9 Abs. 2 Bst. c GE verlangt zudem, dass die Personendaten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten zu sichern sind. Diese Bestimmung setzt Art. 17 Abs. 2 EU-DSRL um, wonach das öffentliche Organ «einen Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmassnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet». Die Sicherstellung der Einhaltung des Datenschutzes erfolgt – soweit nicht ein Gesetz entsprechende Vorschriften enthält – im Rahmen von Auflagen und Bedingungen, die in die Verfügung oder in die Vereinbarung aufzunehmen sind.

Nach Art. 9 Abs. 3 GE ist das öffentliche Organ, das die Bearbeitung von Personendaten an Dritte übertragen hat, verpflichtet, sich durch geeignete regelmässige Kontrollen zu vergewissern, dass der Datenschutz eingehalten wird. Nötigenfalls hat das öffentliche Organ die Übertragung rückgängig zu machen.

*Art. 10* stellt den Bezug zwischen den beim öffentlichen Organ vorhandenen und nicht mehr ständig benötigten Personendaten und der Archivierung von Akten mit solchen Daten im zuständigen Archiv von Kanton oder Gemeinde her. Dabei beschränkt sich das Datenschutzgesetz auf die Regelung der damit verbundenen Verpflichtungen des öffentlichen Organs, nicht aber auf die Verpflichtungen der zuständigen Archive in Bezug auf die (weitere) Aufbewahrung, Bewirtschaftung und Nutzung der ihnen übergebenen Akten. Diese Sachverhalte sind – wie bereits in Bezug auf Art. 2 Abs. 2 Bst. d GE festgehalten – Regelungsgegenstand des Archivgesetzes. Insofern geht Art. 10 GE materiell nicht weiter als der geltende Art. 16 DSV, enthält aber eine Verdeutlichung hinsichtlich des Vorgehens des öffentlichen Organs.

Art. 10 Abs. 1 GE legt die Anbietepflicht des öffentlichen Organs fest. Diesem obliegt die Pflicht, die Personendaten beziehungsweise die entsprechenden Akten dem zuständigen Archiv des Kantons oder der Gemeinde anzubieten (vgl. Art. 6 der Verordnung über das Staatsarchiv, sGS 271.1, und Art. 154 Abs. 2 GG in Verbindung mit Art. 1 der Verordnung über die Gemeindearchive, sGS 151.57). Dabei bleiben besondere Bestimmungen über die Abgaben von zu archivierenden Akten vorbehalten. Beispielhaft seien in Bezug auf Akten der Rechtspflegeorgane Art. 68ter des Strafprozessgesetzes (sGS 962.1) oder Art. 73 f. der Gerichtsordnung (sGS 941.21) erwähnt.

Art. 10 Abs. 2 GE auferlegt dem öffentlichen Organ die Pflicht zur Vernichtung von Akten, die Personendaten enthalten, wenn das zuständige Archiv die Akten als nicht archivierungswürdig bezeichnet. Die Archivierungswürdigkeit stellt einen Tatbestand dar, der ebenfalls archivgesetzlich zu regeln ist.

Die Vernichtung kann nach Art. 10 Abs. 3 GE unterbleiben, wenn die nicht archivierungswürdigen Akten entweder bereits anonymisierte Personendaten enthalten (Bst. a) oder wenn die Personendaten vom öffentlichen Organ unmittelbar nach der Bewertung des zuständigen Archivs als nicht archivierungswürdig anonymisiert werden (Bst. b).

### **3.3. Bestimmungen über die Bekanntgabe von Personendaten**

Dem Grundrecht des Schutzes vor Missbrauch persönlicher Daten nach Art. 2 Bst. g KV muss ganz besonders beim Bekanntgeben von Personendaten – als besondere Form ihrer Bearbeitung – Rechnung getragen werden. Dieser Abschnitt des Datenschutzgesetzes regelt die Voraussetzungen, die erfüllt sein müssen, damit ein öffentliches Organ Personendaten bekanntgeben darf. Art. 11 und 12 GE regeln die Bekanntgabe von (gewöhnlichen) Personendaten, während Art. 14 GE die Voraussetzungen der Bekanntgabe von besonders schützenswerten Personendaten und von Persönlichkeitsprofilen enthält. Die weiteren Bestimmungen dieses Abschnitts regeln besondere Bekanntgabesachverhalte.

Art. 11 enthält in Abs. 1 eine abschliessende Aufzählung der Voraussetzungen für die Bekanntgabe von gewöhnlichen, das heisst nicht besonders schützenswerten Personendaten. Die Bekanntgabe ist zulässig, wenn eine dieser Voraussetzungen gegeben ist. Keine besonderen Handlungen seitens des öffentlichen Organs sind nötig, wenn die Bekanntgabe nach Art. 11 Abs. 1 Bst. a und b GE in einer Rechtsgrundlage vorgesehen ist oder die betroffene Person ausdrücklich in die Bekanntgabe eingewilligt hat. Anders verhält es sich in den Fällen nach Art. 11 Abs. 1 Bst. c, d und e GE. Liegen weder eine Rechtsgrundlage noch die Einwilligung der betroffenen Person vor, weil letztere nicht eingeholt werden kann, so darf eine Bekanntgabe nur erfolgen, wenn sie im Interesse der betroffenen Person liegt (Art. 11 Abs. 1 Bst. c GE). Dabei hat das öffentliche Organ einerseits festzustellen und gegebenenfalls im Rahmen eines Rekurs- oder Beschwerdeverfahrens nachzuweisen, dass die Bekanntgabe im Interesse der betroffenen Person liegt oder – falls die Bekanntgabe erfolgt ist – gelegen hat; andererseits muss das öffentliche Organ die ihm zumutbaren Handlungen unternehmen beziehungsweise unternehmen haben, die Einwilligung erhältlich zu machen. Bedeutsam ist, dass die Weigerung einer betroffenen Person, in die Datenbekanntgabe einzuwilligen, nicht unter den nach Art. 11 Abs. 1 Bst. c GE geregelten Tatbestand fällt. Vielmehr müssen objektive Hindernisse bestehen, die dazu führen oder geführt haben, dass die Einwilligung nicht eingeholt werden kann oder konnte. Als Beispiel ist der unbekannte Aufenthalt einer nachrichtenlos abwesenden Person zu erwähnen. Die Anwendung von Art. 11 Abs. 1 Bst. d GE ist gegeben, wenn eine Abwägung zwischen dem schutzwürdigen Interesse der betroffenen Person an der Nichtbekanntgabe ihrer Daten und dem öffentlichen Interesse an einer Bekanntgabe erforderlich wird. Eine Bekanntgabe ist dann zulässig, wenn einerseits ein öffentliches Interesse vorliegt und dieses andererseits das schutzwürdige Interesse der betroffenen Person überwiegt. Eine Interessenabwägung ist sodann bei Art. 11 Abs. 1 Bst. e GE erforderlich, wobei hier das schutzwürdige Interesse der Empfängerin oder des Empfängers (vgl. dazu Art. 1 Bst. i GE) an der Aushändigung

der Personendaten dem schutzwürdigen Interesse der betroffenen Person an der Geheimhaltung gegenübersteht.

Art. 11 Abs. 2 GE regelt den Fall der Bekanntgabe von Personendaten an eine Behörde des Bundes, eines anderen Kantons oder einem anderen öffentlichen Organ. Die Bekanntgabe ist zulässig, wenn die Empfängerin oder der Empfänger – also die Behörde des Bundes oder des anderen Kantons oder das andere öffentliche Organ – die Personendaten für die Erfüllung einer gesetzlichen Aufgabe benötigt werden. Trifft dies zu, sind die Personendaten bekanntzugeben, ohne dass eine der Voraussetzungen nach Abs. 1 erfüllt sein müsste.

Art. 12 legt fest, in welchen Fällen das öffentliche Organ die Bekanntgabe von Personendaten einschränken, das heisst beispielsweise auf einzelne Daten begrenzen, oder mit Auflagen verknüpfen muss. Die Bekanntgabe ist nach Art. 12 Bst. a GE einzuschränken, wenn im übergeordneten Recht oder im Rahmen von Spezialgesetzen Datenschutzvorschriften eine Einschränkung in der Bekanntgabe verlangen. Sodann hat das öffentliche Organ nach Art. 12 Bst. b GE die Bekanntgabe gegebenenfalls einzuschränken, wenn die Einschränkung wegen öffentlicher Interessen oder wegen schutzwürdiger privater Interessen geboten ist, wobei schutzwürdige private Interessen auch bei Drittpersonen, also nicht nur bei betroffenen Personen, vorkommen können. Das in Art. 12 Bst. b GE enthaltene Motiv für eine eingeschränkte Bekanntgabe von Personendaten ist auch dann massgeblich, wenn die Bekanntgabe nach Art. 11 GE grundsätzlich zulässig ist. Dabei ist nicht auszuschliessen, dass verschiedene Ausprägungen von öffentlichen Interessen vorliegen. So kann nach Art. 11 Abs. 1 Bst. d GE ein öffentliches Interesse vorhanden sein, das die Bekanntgabe grundsätzlich zulässt; gleichzeitig kann aber auch ein öffentliches Interesse nach Art. 12 Bst. b GE bestehen, das eine Einschränkung, beispielsweise auf einzelne Personendaten, verlangt. Hier ist eine Interessenabwägung erforderlich.

Art. 13 hält die Voraussetzungen für die Bekanntgabe von besonders schützenswerten Personendaten sowie von Persönlichkeitsprofilen fest. Während bei (gewöhnlichen) Personendaten eine Rechtsgrundlage für die Bekanntgabe genügt, bedarf es nach Art. 13 Abs. 1 Bst. a GE der Grundlage in einem Gesetz. Gleichermassen wie bei (gewöhnlichen) Personendaten reicht die Einwilligung einer betroffenen Person aus, um die Bekanntgabe auch von besonders geschützten Personendaten oder von Persönlichkeitsprofilen zuzulassen (Art. 13 Abs. 1 Bst. b GE). Ebenso kann – wie bei (gewöhnlichen) Personendaten – der Fall gegeben sein, dass die Bekanntgabe im Interesse der betroffenen Person liegt, die Einwilligung jedoch nicht eingeholt werden kann (Art. 13 Abs. 1 Bst. c GE). Es gelten hier sachgemäss dieselben Überlegungen, wie sie in den Bemerkungen zu Art. 11 Abs. 1 Bst. c GE enthalten sind. Demgegenüber gibt es bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen keine Interessenabwägungen, wie sie in Art. 11 Abs. 1 Bst. d und e GE vorgesehen sind. Insofern ist auch eine der Bestimmung von Art. 12 GE vergleichbare Regelung in diesem Bereich nicht erforderlich.

Art. 13 Abs. 2 GE ist mit Art. 11 Abs. 2 GE vergleichbar. Bei besonders schützenswerten Personendaten und bei Persönlichkeitsprofilen wird jedoch eine im Vergleich zu (gewöhnlichen) Personendaten qualifiziertere Voraussetzung für die Bekanntgabe der Daten verlangt. Genügt nach Art. 11 Abs. 2 GE der Sachverhalt, dass die Daten für die Erfüllung einer gesetzlichen Aufgaben benötigt werden, ist hier erforderlich, dass einerseits eine von der Empfängerin oder vom Empfänger selbst zu erfüllende gesetzliche Aufgabe vorliegt und andererseits die Bekanntgabe der Daten für die Aufgabenerfüllung unentbehrlich ist.

Für die Regelung in Art. 14 ist kennzeichnend, dass sie konkrete Personendaten abschliessend aufführt. Diese Personendaten dürfen vom öffentlichen Organ bekanntgegeben werden, wenn sie die Empfängerin oder der Empfänger im Hinblick auf die Verwendung für gemeinnützige oder schutzwürdige ideelle Zwecke benötigt. Es geht darum, dass das Datenschutzrecht zum Beispiel die Durchführung von Spendensammlungen (gemeinnütziger Zweck) oder die Werbung für politische Parteien (schutzwürdiger ideeller Zweck) nicht verunmöglicht. Allerdings ist erforderlich, dass die Empfängerin oder der Empfänger Gewähr bietet und sich schriftlich verpflichtet, die genannten Daten nur für den entsprechenden Zweck zu verwenden und sie nicht weiterzugeben.

Art. 15 regelt das so genannte Abrufverfahren. Beim Abrufverfahren werden die Personendaten nicht aktiv vom öffentlichen Organ der Empfängerin oder dem Empfänger bekanntgegeben oder ausgehändigt; vielmehr beschafft sich die Empfängerin oder der Empfänger die Daten selbst («Selbstbedienung»). Wesentlich ist dabei, dass die Beschaffung der Personendaten erfolgen kann, ohne dass die Empfängerin oder der Empfänger sie – beispielsweise unter Bezugnahme auf das Vorliegen eines Interesses nach Art. 11 Abs. 1 Bst. d oder e GE – begründen muss. Um das Risiko eines Missbrauchs von durch ein Abrufverfahren zugänglich gemachten Personendaten auszuschliessen, bedarf diese Form der Datenbekanntgabe einer Rechtsgrundlage beziehungsweise der Grundlage in einem Gesetz, wenn besonderes schützenswerte Personendaten abgerufen werden können.

Bei der Regelung nach Art. 16 geht es darum, dass die Bekanntgabe von Personendaten ins Ausland dann zulässig ist, wenn nicht nur die im vorliegenden Erlass enthaltenen Bekanntgabebestimmungen eingehalten sind, sondern zusätzlich sichergestellt ist, dass der Staat, wo sich die Empfängerin oder der Empfänger der Personendaten befindet, ein adäquates Datenschutzniveau besteht (Art. 25 f. EU-DSRL).<sup>37</sup>

Art. 16 Abs. 1 GE erklärt für den Fall, dass Personendaten ins Ausland bekanntgegeben werden, die Bundesgesetzgebung als sachgemäss anwendbar. Im Wesentlichen handelt es sich um Art. 6 eidgDSG, der wie folgt lautet:

«Grenzüberschreitende Bekanntgabe

Art. 6. Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

- a. hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;
- b. die betroffene Person im Einzelfall eingewilligt hat;
- c. die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;
- d. die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
- e. die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;
- f. die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat;
- g. die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Beauftragte, Art. 26) muss über die Garantien nach Absatz 2 Buchstabe a und die Datenschutzregeln nach Absatz 2 Buchstabe g informiert werden. Der Bundesrat regelt die Einzelheiten dieser Informationspflicht.»

Das öffentliche Organ hat nach Art. 16 Abs. 2 GE in Analogie zu Art. 6 Abs. 2 eidgDSG und Art. 6 der eidgenössischen Datenschutzverordnung (SR 235.11; abgekürzt eidgDSV), das die Information des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten vorsieht, die zuständige Fachstelle für Datenschutz zu informieren, wenn es Personendaten grenzüberschreitend ins Ausland bekanntgeben will. Diese Informationspflicht entfällt jedoch in allen jenen Fällen, in denen der ausländische Staat auf der Liste der Staaten mit angemessener Datenschutzgesetzgebung aufgeführt ist. Diese Liste wird nach Art. 7 eidgDSV vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten geführt und veröffentlicht.

<sup>37</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O., 62 f.

Damit das öffentliche Organ hinreichend Kenntnis über das Vorgehen bei der Bekanntgabe von Personendaten ins Ausland hat, ist es auf entsprechende Informationen angewiesen. Diese sind von der kantonalen Fachstelle für Datenschutz nach Art. 16 Abs. 3 erstem Satz GE beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten zu beschaffen. Die kantonale Fachstelle für Datenschutz informiert alsdann die ihm zugeordneten öffentlichen Organe. Ferner stellt sie die Informationen den Gemeindefachstellen für Datenschutz zur Weiterverbreitung an die diesen zugeordneten öffentlichen Organen zur Verfügung. Es ist also nicht Aufgabe der kantonalen Fachstelle für Datenschutz, die auslandrelevanten Informationen selber aufzuarbeiten; vielmehr soll sie sich auf den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten abstützen, dem nach Art. 31 Abs. 1 Bst. d eidgDSG als Aufgabe die Begutachtung übertragen ist, inwieweit die Datenschutzgesetzgebung im Ausland einen angemessenen Schutz gewährleistet.

### **3.4. Bestimmungen über die Rechte der betroffenen Person**

Der betroffenen Person kommen spezifische datenschutzbezogene Rechte zu. Diese werden in den Art. 17 bis 23 GE geregelt.

Das mit Art. 17 eingeräumte Recht der betroffenen Person auf Auskunft über die Bearbeitung von Personendaten stellt ein Kernelement des Datenschutzrechts dar. Mit dieser Bestimmung werden Art. 12 Bst. a EU-DSRL und Art. 8 Bst. b ER-Konv 108 im kantonalen Datenschutzgesetz umgesetzt. Das Auskunftsrecht bildet die Grundlage für weitere Rechte der betroffenen Person, insbesondere der Anspruch auf Berichtigung, Bereinigung oder Vernichtung von unrichtigen oder widerrechtlich bearbeiteten Personendaten (Art. 20 GE). Für die Wahrnehmung dieser Rechte ist die betroffene Person auf Belege über das Vorhandensein von Personendaten und über deren Bearbeitung angewiesen, weshalb die Auskunft in der Regel schriftlich erfolgen muss (Art. 17 Abs. 1 zweiter Satz GE). Die schriftliche Mitteilung ist in einer für die betroffene Person verständlichen Form zu verfassen, die insbesondere über die vorhandenen Daten, über die Herkunft und über den Gegenstand der Bearbeitung informiert (Art. 12 Bst. a Abs. 2 EU-DSRL). Ergänzend zur oder an Stelle der Auskunft ist der betroffenen Person auf deren Verlangen Einsicht in die Daten zu gewähren (Art. 17 Abs. 2 GE).

Art. 18 bildet die allgemeine gesetzliche Grundlage, auf die sich das öffentliche Organ abstützen hat, wenn es Auskunft und Einsicht ablehnen, einschränken oder mit Auflagen verbinden will. Neben dieser allgemeinen Gesetzesgrundlage können Beschränkungen auch in Spezialerlassen enthalten sein, wenn sie sich auf bestimmte Datensammlungen beziehen.

Voraussetzung für eine Beschränkung der Auskunftserteilung oder der Einsichtgabe nach Art. 18 GE ist ein öffentliches oder ein schutzwürdiges privates Interesse. Als öffentliche Interessen kommen namentlich die Wahrung der öffentlichen Sicherheit sowie Massnahmen zur Verhütung von Straftaten und zur Vermeidung einer Vereitelung der Strafverfolgung in Betracht (vgl. Art. 13 Abs. 1 Bst. c und d EU-DSRL und Art. 9 Abs. 2 Bst. a ER-Konv 108). Sodann können schutzwürdige private Interessen eine Beschränkung in der Auskunftserteilung beziehungsweise in der Einsichtgabe rechtfertigen. Dabei können sich die schutzwürdigen privaten Interessen – gleichermassen wie bei der Beschränkung der Bekanntgabe von Personendaten nach Art. 12 Bst. b GE – sowohl auf Drittpersonen, zu denen auch andere betroffene Personen gehören, wie auch auf die betroffene Person selbst beziehen. Geht es um die betroffene Person selbst, so ist damit deren eigener Schutz oder der so genannte «Selbstschutz der betroffenen Person» gemeint (Art. 13 Abs. 1 Bst. g EU-DSRL und Art. 9 Abs. 2 Bst. b ER-Konv 108). Mit Selbstschutz ist gemeint, dass der betroffenen Person ein schwerer Nachteil – ein so genannter Aufklärungsschaden – droht, was vorab in ihrer Eigenschaft als Patientin oder als Patient denkbar ist.<sup>38</sup>

---

<sup>38</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O. 55.

*Art. 19* regelt die Gebührenerhebung bei Auskunftserteilung oder Einsichtgabe. Als Grundsatz gilt Unentgeltlichkeit. Mit dieser Regelung wird der in Art. 12 Bst. a EU-DSRL und Art. 8 Bst. b ER-Konv 108 enthaltenen Vorgabe Rechnung getragen, wonach Auskunft und Einsicht für die betroffene Person «ohne übermässige Kosten» ermöglicht werden muss.

*Art. 20* räumt der betroffenen Person Ansprüche bei Vorliegen von unrichtigen oder bei widerrechtlich bearbeiteten Personendaten ein. Nach Art. 20 Abs. 1 erstem Satz GE kann die betroffene Person verlangen, dass unrichtige Personendaten berichtigt werden. Kann weder die Richtigkeit noch die Unrichtigkeit vom öffentlichen Organ oder von der betroffenen Person bewiesen werden, indem beispielsweise Personendaten vorliegen, die von ihrer Natur her nicht bewiesen werden können, wie etwa Werturteile, so sind diese nicht zu berichtigen, sondern mit einem entsprechenden Vermerk zu versehen. Ein solcher Vermerk kann dahingehend lauten, dass die betroffene Person die Richtigkeit bestreitet (Bestreitungsvermerk).<sup>39</sup>

Art. 20 Abs. 2 GE bezieht sich auf widerrechtlich bearbeitete Personendaten. Es geht bei dieser Bestimmung um die Rechtmässigkeit der Bearbeitung von Personendaten, unabhängig davon, ob die Personendaten richtig sind oder nicht. Sobald eine widerrechtliche Bearbeitung – auch von richtigen Daten – vorliegt, kann die betroffene Person verlangen, dass die Bearbeitung unterbleibt und dass bereits bearbeitete Personendaten vernichtet werden.

Nach Art. 20 Abs. 3 GE hat das öffentliche Organ die Empfängerinnen und Empfänger von unrichtigen oder widerrechtlich bearbeiteten Personendaten über die getroffenen Massnahmen zu informieren. Je nach Sachverhalt ist über die Berichtigung der Personendaten, über das Anbringen eines Vermerks, über die Unterlassung der Bearbeitung oder über die Vernichtung von Personendaten zu informieren.

*Art. 21* legt den Anspruch der betroffenen Person auf Sperrung der Bekanntgabe ihrer Personendaten fest. Die Sperrung ist vorzunehmen, wenn die betroffene Person ein schutzwürdiges Interesse nachweist und nicht einer der Gründe nach Art. 22 GE vorliegt.

*Art. 22* ermöglicht die Bekanntgabe von Personendaten trotz einer von der betroffenen Person verlangten Sperrung. Die Bekanntgabe ist nach Art. 22 GE zulässig, wenn dazu eine Rechtspflicht besteht, wenn sonst die Erfüllung einer gesetzlichen Aufgabe verunmöglicht würde oder wenn die Sperrung rechtsmissbräuchlich erwirkt wurde. Im konkreten Einzelfall (insbesondere nach Bst. c) ist zu beachten, dass sich aus dem Anspruch auf rechtliches Gehör (Art. 29 Abs. 2 BV) ergeben kann, dass der betroffenen Person vor der Bekanntgabe Gelegenheit zur Stellungnahme zu geben ist.

*Art. 23* enthält die Rechtsweggarantie im Datenschutz. Damit die betroffene Person ihre Rechte im Rahmen eines Rechtsmittelverfahrens durchsetzen kann, ist das öffentliche Organ zu verpflichten, eine Verfügung zu erlassen, wenn es das Gesuch einer betroffenen Person abweist. Verweigert es beispielsweise die Einsichtnahme in eine Datensammlung, hat es die Abweisung des entsprechenden Gesuchs unter Angabe der Gründe in eine Verfügung zu kleiden. Der Erlass der Verfügung und deren Anfechtung richten sich nach den Bestimmungen des Gesetzes über die Verwaltungsrechtspflege. Dieses gilt namentlich auch für den Instanzenweg beim Anfechten von Verfügungen und von Entscheiden über Verfügungen.

### **3.5. Bestimmungen über die Fachstelle für Datenschutz**

#### *3.5.1. Organisationsbestimmungen*

Dieser Abschnitt enthält die Bestimmungen über Organisation und Zuständigkeit des mit Fachstelle für Datenschutz bezeichneten Kontrollorgans im Kanton und in den Gemeinden.

---

<sup>39</sup> Beat Rudin, Datenschutzgesetze, a.a.O., 57.

Art. 24 verpflichtet den Kanton und die Gemeinden – gemeint sind sowohl die politischen wie auch die Spezialgemeinden –, eine Fachstelle für Datenschutz einzusetzen. Der Wirkungsbereich der kantonalen Fachstelle erstreckt sich über die Staatsverwaltung und die selbstständigen öffentlich-rechtlichen Anstalten des Kantons sowie – nach Art. 2 Bst. b des Gerichtsgesetzes (sGS 941.1; abgekürzt GerG) in der Fassung gemäss Art. 42 GE – über die Justizverwaltung. Die Gemeindefachstelle für Datenschutz ist nach Art. 24 Abs. 2 erstem Satz GE für die Gemeindeverwaltung sowie für die nach Art. 197 ff. GG bestehenden selbstständigen öffentlich-rechtlichen Gemeindeunternehmen zuständig.

Errichtung und administrative Führung der Gemeindefachstelle für Datenschutz sind auf dreifache Art möglich: Die erste Möglichkeit besteht darin, dass die Gemeinde im Sinn von Art. 24 Abs. 2 erstem Satz GE für ihren Zuständigkeitsbereich eine eigene Fachstelle führt. Es widerspricht jedoch den Grundsätzen einer wirksamen und wirtschaftlichen Aufgabenerfüllung, wenn jede Gemeinde eine eigene Fachstelle für Datenschutz einsetzen würde. Als zweite Möglichkeit steht es einer Gemeinde deshalb zu, mit einer anderen Gemeinde zu vereinbaren, dass deren Fachstelle die Aufgaben übernimmt (Art. 24 Abs. 2 zweiter Satz GE). Damit verwirklichen die beteiligten Gemeinden im Bereich des Datenschutzes die in Art. 203 Abs. 1 Bst. a GG vorgesehene Zusammenarbeitsform, wonach Gemeinden durch Vereinbarung Einrichtungen einer anderen Gemeinde zur Verfügung stellen können. Eine solche Zusammenarbeit muss sich nicht auf bloss zwei Gemeinden beschränken; denkbar ist vielmehr auch, dass sich mehrere Gemeinden zusammenschliessen und die Gemeindefachstelle einer einzigen – grossen oder grösseren – Gemeinde als für alle beteiligten Gemeinden zuständig erklären. Die dritte Möglichkeit, nämlich die Errichtung einer gemeinsamen Gemeindefachstelle von mehreren Gemeinden, ist in Art. 25 GE geregelt, und entspricht der Zusammenarbeitsform nach Art. 203 Abs. 1 Bst. b GG über die Schaffung gemeinsamer Einrichtungen.

Art. 25 sieht in Abs. 1 vor, dass die Gemeinden durch Vereinbarung gemeinsame Fachstellen einsetzen können. Dabei besteht nicht die Meinung, dass die gemeinsame Fachstelle auf Gemeinden derselben Art – also je separat auf politische Gemeinden, Schulgemeinden, Ortsgemeinden und örtliche Korporationen – ausgerichtet sein müsste. Vielmehr kann dem Grundsatz der wirtschaftlichen Aufgabenerfüllung dann am ehesten entsprochen werden, wenn einer Gemeindefachstelle alle Gemeinden – politische *und* Spezialgemeinden – der von den Gemeinden festzulegenden Region angeschlossen sind. Denkbar und mit erheblichen wirtschaftlichen Vorteilen verbunden wäre eine Lösung, bei der die Gemeinden die in Art. 37 Abs. 1 KV vorgegebenen Wahlkreise heranziehen und für sämtliche sich auf dem Gebiet des Wahlkreises befindlichen Gemeinden eine einzige Fachstelle einrichten. Für die administrative Führung der Fachstelle ist nach Art. 25 Abs. 1 zweitem Satz Bst. a GE eine Sitzgemeinde zu bezeichnen. Deren Rat ist Wahlinstanz in Bezug auf die Leiterin oder den Leiter der Fachstelle (vgl. Art. 29 Abs. 2 GE). Neben der Sitzgemeinde ist nach Art. 25 Abs. 1 zweitem Satz Bst. b GE der Schlüssel für die Finanzierung der Ausgaben der gemeinsamen Fachstelle zu bestimmen. Den Gemeinden werden von Gesetzes wegen keine Vorgaben gemacht, nach welchen Kriterien sie diesen Schlüssel festzulegen haben. Sie können diesen nach der Zahl der Einwohnerinnen und Einwohner, nach der Zahl vorhandener Datensammlungen oder nach anderen Bestimmungsgrössen festlegen.

Art. 25 Abs. 2 GE ermächtigt die Regierung, eine gemeinsame Gemeindefachstelle für Datenschutz einzurichten, wenn keine entsprechende Vereinbarung zustande kommt, eine wirksame Aufgabenerfüllung und ein wirtschaftlicher Mitteleinsatz es jedoch verlangen. In einem ersten Schritt bezeichnet die Regierung die beteiligten Gemeinden (Art. 25 Abs. 1 erster Satz GE). Wenn sich die zur Zusammenarbeit verpflichteten Gemeinden nicht auf die Bestimmung einer Sitzgemeinde oder auf den Finanzierungsschlüssel einigen können, legt die Regierung in einem zweiten Schritt auch diese Zusammenarbeitsgrundsätze fest.

Art. 25 Abs. 3 GE bezeichnet die zuständige Gemeindefachstelle für Datenschutz bei Bestehen eines Gemeindeverbandes oder eines Zweckverbandes. Zuständig ist jene Fachstelle, welche für die Mitgliedgemeinde handelt, die Sitz des Verbandes ist.

Art. 26 legt in Übereinstimmung mit Abs. 2 der Präambel des ZP zur ER-Konv 108 und Art. 28 Abs. 1 zweitem Satz EU-DSRL den Grundsatz des unabhängigen und selbstständigen Handelns der Fachstelle für Datenschutz fest. Im Wesentlichen bringt dieser Grundsatz zum Ausdruck, dass die Fachstelle ihre Aufgaben weisungsungebunden erfüllt. Ihre Zugehörigkeit zur Staats- beziehungsweise zur Gemeindeverwaltung kann demzufolge nur eine administrative Zuordnung sein, was in Art. 26 Abs. 2 GE festgehalten wird. Auf kantonaler Ebene entscheidet die Regierung durch Verordnung – vorzugsweise im Rahmen des Geschäftsreglementes der Regierung und der Staatskanzlei (sGS 141.3) – über die Zuordnung, wobei in Anwendung von Art. 34 StVG in Verbindung mit Art. 33 Bst. h StVG neben der Zuordnung an ein Departement auch eine solche an die Staatskanzlei möglich ist. Die Gemeindefachstelle für Datenschutz ist administrativ dem Rat der Gemeinde beziehungsweise – bei Bestehen einer gemeinsamen Fachstelle für mehrere Gemeinden – der Sitzgemeinde zugeordnet.

Art. 27 regelt die Aufsicht über die Tätigkeit der Fachstelle. Die Unabhängigkeit nach Art. 27 GE bedeutet nicht, dass die Aufgabenerfüllung durch die Fachstelle nicht einer Aufsicht unterstellt sein soll. Die Aufsicht muss indessen ebenfalls dem Grundsatz der Unabhängigkeit der Fachstelle Rechnung tragen, weshalb sie ausserhalb der Verwaltungsorgane anzusiedeln ist. Audits durch die Exekutive oder im Auftrag der Exekutive sind unzulässig. Auf kantonaler Ebene ist die für die Aufsicht über Regierung und Verwaltung zuständige Kommission des Kantonsrates als Aufsichtsorgan zu bezeichnen. Die Aufsicht obliegt demgemäss nach Art. 15 des Geschäftsreglementes des Kantonsrates (sGS 131.11; abgekürzt GeschKR) der Staatswirtschaftlichen Kommission. In Bezug auf die Gemeindefachstellen für Datenschutz soll die kantonale Fachstelle Aufsichtsinstanz sein.

Die Prüfung des administrativ-finanziellen Gebarens erfolgt für die kantonale Fachstelle für Datenschutz durch die Finanzkontrolle (vgl. Art. 42b Abs. 1 Bst. b<sup>bis</sup> StVG in der Fassung gemäss Art. 41 GE). Auf kommunaler Ebene besteht dieselbe Aufsicht wie für Dienststellen der Gemeinde, also einerseits durch die Geschäftsprüfungskommission in Gemeinden mit Bürgerversammlung beziehungsweise durch die mit der Geschäftsprüfung betraute parlamentarische Kommission in Gemeinden mit Parlament nach Art. 105 GG und andererseits durch das für die Gemeindeaufsicht zuständige Departement.

Art. 28 stellt die für das Personal der Fachstelle massgebende Bestimmung dar.

Art. 28 Abs. 1 und 2 GE bezeichnen das für die Wahl der Leiterin oder den Leiter der Fachstelle zuständige Wahlorgan. Aufgrund der europarechtlichen Vorgaben, die eine «völlige Unabhängigkeit» der Kontrollstelle verlangen, sind institutionelle Sicherungen vorzusehen, die diese Unabhängigkeit gewährleisten. Eine dieser Sicherungen besteht bei der Festlegung der Wahlinstanz, allenfalls verbunden mit der Festlegung einer für das Kontrollorgan geltenden Amtsdauer. In dieser Hinsicht sieht die KdK-Wegleitung drei Varianten vor:

- *Variante A:* Wahl durch das Parlament auf eine Amtsdauer von vier bis sechs Jahren (mit der Möglichkeit der Wiederwahl);
- *Variante B:* Wahl durch die Exekutive mit Vorbehalt der Genehmigung durch das Parlament auf eine Amtsdauer von sechs bis acht Jahren (mit der Möglichkeit der Wiederwahl);
- *Variante C:* Wahl durch die Exekutive auf eine Amtsdauer von acht oder mehr Jahren (mit der Möglichkeit der Wiederwahl).

Für den Kanton St.Gallen soll auf kantonaler Ebene die Regierung (Art. 28 Abs. 1 GE), auf Gemeindeebene der Rat (Art. 28 Abs. 2 GE) Wahlinstanz sein. Eine Mitwirkung durch das kantonale oder das Gemeindeparlament und – parallel dazu in Gemeinden mit Bürgerversammlung – durch die ausserhalb der Gemeindeverwaltung stehende Geschäftsprüfungskommission ist nicht erforderlich, wenn anderweitige institutionelle Garantien für das vom europäischen Recht geforderte unabhängige Wirken der Fachstelle bestehen. Solche sind im vorliegenden Gesetzesentwurf dadurch vorgesehen, dass die Fachstelle lediglich administrativ einer Verwaltungsbehörde zugeordnet ist (Art. 26 Abs. 2 GE). Hinzu kommt, dass die Fachstelle nach Art. 27 GE unter einer verwaltungsexternen Aufsicht steht. Ferner kommt ihr das Recht

auf eigenständige Erstellung des Voranschlags zu (Art. 29 GE). Sodann legt die Fachstelle nach Art. 30 Abs. 1 Bst. a GE ihr Prüfprogramm für die Einhaltung des Datenschutzrechts autonom und ohne Mitwirkung anderer Behörden fest. Im Weiteren ist bedeutsam, dass der Fachstelle eine Einwirkungsmöglichkeit in Form eines an die obersten zuständigen Verwaltungsbehörden zu richtenden Antrags auf Anordnung von Massnahmen zukommen soll, wenn ihren Empfehlungen nicht oder nicht in allen Teilen Rechnung getragen werden sollte (Art. 34 Abs. 1 und Art. 35 Abs. 1 GE). Schliesslich ist massgebend, dass der Fachstelle das Recht auf Einreichung von Rekursen beziehungsweise Beschwerden gegen Verfügungen über die Anordnung von Massnahmen und Entscheide über solche Verfügungen zustehen soll; sie hat mithin Parteistellung (Art. 34 Abs. 3 zweiter Satz und Art. 35 Abs. 3 zweiter Satz GE).

Mit Blick auf die Gewährleistung von institutionellen Garantien für die Unabhängigkeit der Fachstelle ist bei vorgesehener Wahl durch ein Exekutivorgan – Regierung auf kantonaler Ebene, Rat auf Gemeindeebene – die Meinung vertreten worden, dass im Gegenzug zur Wahlkompetenz der Exekutive die Wahl auf eine vergleichsweise lange Amtsdauer von acht oder mehr Jahren erfolgen soll.<sup>40</sup> Dem ist entgegenzuhalten, dass dem st.gallischen Recht die Wahl auf Amtsdauer mit Ausnahme der Behörden von Kanton und Gemeinden im Sinn von Art. 55 Abs. 1 KV fremd ist. Nachdem die Kantonsverfassung überdies das Beamtenverhältnis und damit die Wahl von Mitarbeitenden auf Amtsdauer abgeschafft hat – was allerdings noch des Nachvollzugs auf Gesetzesstufe bedarf –, ist ein Wahlmodus mit einer Wahl auf Amtsdauer nicht gerechtfertigt. Die Wahl der Leiterin oder des Leiters der Fachstelle für Datenschutz auf eine wie auch immer ausgestaltete Amtsdauer wäre nach der geltenden verfassungsrechtlichen Ordnung als systemfremd zu beurteilen.

Art. 28 Abs. 3 GE ermächtigt die Fachstelle für Datenschutz zur Anstellung des Personals. Allerdings kann sie Anstellungen nur im Rahmen der ihr im Voranschlag eingeräumten Kredite vornehmen. Mit der Festlegung der Anstellungskompetenz erhält die Fachstelle eine weitere institutionelle Garantie für die unabhängige Aufgabenerfüllung. Sie stellt die Mitarbeitenden aufgrund des von ihr nach Massgabe des Gesetzes aufzustellenden Anforderungsprofils an.

Heute ist die juristische Mitarbeiterin im Rechtsdienst der Staatskanzlei, welche die Funktionen als kantonale Datenschutzbeauftragte ausübt, im Ausmass von 30 Stellenprozenten für den Datenschutz tätig. Mit diesem Pensum lassen sich – mit gewissen Einschränkungen – die an die Datenschutzbeauftragte gerichteten Anfragen beantworten sowie höchstens eine bis zwei Datenschutz-Visitationen durchführen. Weitere Aufgaben, wie die Begleitung von Projekten oder die Stellungnahme zu Erlassen mit Datenschutzrelevanz, können nicht oder nur in sehr geringem Ausmass wahrgenommen werden. Mit der Umsetzung des Schengen-Assoziierungs-Abkommens nehmen die Aufgaben des Kontrollorgans, wie sie in Art. 16, 30, 33 f. und 36 GE festgelegt sind, gegenüber heute merklich zu. Von besonderer Bedeutung sind in diesem Zusammenhang folgende Tätigkeitsbereiche:

- **Auskünfte:** Die Erfahrungen der Staaten im Schengen-Raum zeigen, dass die Anfragen betroffener Personen erheblich zunehmen werden, dies namentlich aufgrund des Umstandes, dass es vielfach um die Einspeisung von Daten in europaweit abrufbare Datenbanken geht. Dies tangiert und interessiert die Bevölkerung wesentlich stärker als die bisherigen vorab lokal auf St. Gallen bezogenen polizeilichen Systeme. Zu bedenken ist auch, dass es sich bei SIS-Daten nicht nur um Angaben über mögliche Straftäter handelt, sondern auch Daten von Personen erfasst werden, die Opfer oder Zeugen einer Straftat sind.
- **Kontrollen:** Die Aufsicht muss künftig den von den Schengen-Staaten etablierten internationalen Standards entsprechen, was zeitaufwendigere Begutachtungen von Datensammlungen bewirkt. Ein erhöhter Zeitbedarf ergibt sich aufgrund der Zunahme von Zahl und Umfang der Visitationen.

---

<sup>40</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O., 74.

- Aufsicht: Dem kantonalen Kontrollorgan, also der kantonale Fachstelle für Datenschutz, obliegt neu die Aufsicht über die Kontrollorgane, das heisst die Fachstellen, der Gemeinden. Ferner kommt der kantonalen Fachstelle die Beratung der kommunalen Fachstellen zu. Diese Aufgaben bedeuten eine wesentliche Erweiterung der Tätigkeitsbereiche der kantonalen Fachstelle.
- Beratung und Schulung: Insbesondere die Mitarbeitenden der Polizei, die über einen Zugang zum SIS verfügen, bedürfen der spezifisch auf ihre Bedürfnisse zugeschnittenen Beratung und Schulung.
- Öffentlichkeitsarbeit: Die Ausweitung der Aufgabenfelder des Kontrollorgans verlangt ein verstärktes Engagement im Bereich der Öffentlichkeitsarbeit. Auch ist davon auszugehen, dass die Medienanfragen zunehmen werden.
- Empfehlungen und Massnahmen, einschliesslich Rechtsmittelverfahren: Die in Art. 33 ff. GE vorgesehenen Instrumente der so genannten Einwirkung führen zu einer grösseren Arbeitsbelastung des Kontrollorgans, namentlich auch unter Berücksichtigung der Abklärungen, die im Vorfeld eines an die zuständige Behörde gerichteten Antrags auf Anordnung von Massnahmen einzuhalten sind.

Insgesamt ist davon auszugehen, dass der personelle Ressourcenbedarf für die Gewährleistung des sich aus den Assoziierungs-Abkommen ergebenden Datenschutzniveaus bei 150 Stellenprozent liegt. Dieser Grössenordnung liegt die Meinung zu Grunde, dass die Aufgaben auch im Rahmen des merklich erweiterten Tätigkeitsbereichs des Datenschutzkontrollorgans pragmatisch und unkompliziert wahrgenommen werden. In Bezug auf die Gemeindefachstellen lassen sich keine schlüssigen Angaben machen. Bestimmend werden die Organisation dieser Fachstellen und namentlich die Verwirklichung der interkommunalen Zusammenarbeit sein.

Art. 28 Abs. 4 GE legt fest, dass für das Dienstverhältnis der Leiterin oder des Leiters sowie der Mitarbeitenden der kantonalen Fachstelle die Bestimmungen des Staatsverwaltungsgesetzes anzuwenden sind. Für die Gemeindefachstellen gilt das Dienstrecht der Gemeinde beziehungsweise der Sitzgemeinde.

Art. 29 räumt der Fachstelle für Datenschutz das Recht ein, den sie betreffenden Abschnitt des Voranschlags selbstständig zu erstellen und direkt dem für die Beschlussfassung über den Voranschlagsentwurf zuständigen Organ, das heisst der Regierung oder dem Rat, vorzulegen. Das Budget der Fachstelle sollte nebst den üblichen Aufwendungen für personelle und sachliche Ressourcen (Büro, Büromaterial, PC, Telefon etc.) auch einen Betrag aufweisen, der es dem Kontrollorgan erlaubt, externe Fachspezialisten beizuziehen oder – für den Fall, dass Massnahmen aufgrund von komplexen Sachverhalten beantragt werden müssen – rechtskundige Beratung anzufordern. Wenn die Regierung beziehungsweise der Rat im Voranschlagsentwurf zuhanden des Kantonsrates beziehungsweise des Gemeindeparlamentes oder der Bürgerversammlung von den Kreditanträgen der Fachstelle abweicht, ist dies in der Budgetvorlage zu erwähnen und die Abweichungen sind zu begründen.

### 3.5.2. Zuständigkeitsbestimmungen

Art. 30 legt – zusammen mit Art. 33 bis 35 GE – die nach Art. 1 ZP zur ER-Konv 108 und Art. 28 EU-DSRL vorgegebenen und durch das innerstaatliche Recht zu konkretisierenden Aufgaben und Befugnisse des Datenschutzkontrollorgans, das heisst in der Terminologie des vorgesehenen st.gallischen Rechts der Fachstelle für Datenschutz, fest. Im Zentrum stehen die Kontroll- und die Beratungsaufgaben.

In Art. 30 Abs. 1 Bst. a GE ist die Kontroll- beziehungsweise Aufsichtsfunktion festgehalten. Die Fachstelle überwacht einerseits nach einem eigenen, von ihr aufgestellten Programm die Einhaltung des Datenschutzrechts; andererseits wird sie auf Anzeige von betroffenen Personen tätig. Da der Fachstelle für Datenschutz nach Massgabe der verfassungsrechtlich geordneten Staatsorganisation keine dem Kantonsrat und der Regierung beziehungsweise dem Gemein-

deparlament und dem Rat übergeordnete Stellung zukommen kann, sind diese Behörden von der Aufsicht auszunehmen.

Ein wichtiges Merkmal für Unabhängigkeit der Fachstelle für Datenschutz liegt darin, dass diese ihr Prüfprogramm im Rahmen des gesetzlichen Auftrages autonom aufstellt. Sie muss über umfassende Untersuchungsbefugnisse (ungeachtet allfälliger Geheimhaltungspflichten), wirksame Einwirkungsbefugnisse und eine Klage-/Anzeigebefugnis verfügen, und sie muss die Kompetenz haben, Sonderaufträge zur Prüfung abzulehnen, wenn diese die Realisierung des Prüfprogramms gefährden würden.

Art. 30 Abs. 1 Bst. b GE verpflichtet die Fachstelle für Datenschutz zur Beratungstätigkeit zu Gunsten der öffentlichen Organe und betroffener Personen. Sodann kann sie nach Art. 30 Abs. 1 Bst. c GE den Erlass von Weisungen über technische und organisatorische Massnahmen zur Gewährleistung des Datenschutzes beantragen. Im Gegensatz zum geltenden Art. 28 Abs. 1 Bst. e DSV, der dem Kontrollorgan das Recht einräumt, Richtlinien über technische und organisatorische Massnahmen zu erlassen, sieht das künftige Gesetz ein entsprechendes Antragsrecht vor. Diese Änderung ist geboten, nachdem die zu erlassende Weisung als aufsichtsrechtliche Massnahme zu qualifizieren ist, die vom für die Aufsicht über die Dienststellen zuständigen Organ getroffen werden muss. Von einer entsprechenden Rechtsetzungskompetenz der Fachstelle ist abzusehen.

Art. 30 Abs. 1 Bst. d GE steht im Zusammenhang mit der Beratungsfunktion nach Bst. b. Zur Beratung gehört die Stellungnahme zu datenschutzrelevanten Erlassentwürfen. Gleichermassen ist die Mitwirkung in Projekten, die den Datenschutz betreffen oder zu diesem in einer Beziehung stehen, Teil der Beratungsfunktionen der Fachstelle (Art. 30 Abs. 1 Bst. e GE).

Der kantonalen Fachstelle kommt nach Art. 30 Abs. 2 GE die zusätzliche Aufgabe der Beratung der Fachstellen für Datenschutz der Gemeinden zu.

Art. 31 ist zusammen mit Art. 32 darauf ausgerichtet, der Fachstelle eine wirksame Aufgabenerfüllung zu ermöglichen. Art. 31 GE räumt der Fachstelle ein Einsichtsrecht in die Datensammlungen ein, während Art. 32 Abs. 1 GE die vom öffentlichen Organ zu erbringenden Unterstützungshandlungen in einer nicht abschliessenden Aufzählung auflistet. Mit diesen beiden Bestimmungen werden die Instrumente festgelegt, mit welchen die Fachstelle die nach Art. 28 Abs. 3 erstem Abschnitt EU-DSRL verlangten Untersuchungsbefugnisse ausüben kann. In Bezug auf Art. 32 Abs. 1 Bst. e GE ist festzuhalten, dass unter Fachinformationen Auskünfte fallen können, die nicht einen konkreten datenschutzrelevanten Sachverhalt zum Gegenstand haben, sondern der Vermittlung von Wissen dienen, das die Fachstelle für die Erfüllung ihrer Aufgaben benötigt. Wenn beispielsweise im geltenden Art. 28 Abs. 2 DSV festgehalten ist, dass das Kontrollorgan für die Aufsicht über elektronische Datenverarbeitungen den Dienst für Informatikplanung beiziehen kann, so wird eine solche Unterstützung künftig nach Art. 32 Abs. 1 Bst. e GE zu erbringen sein. Die generell-abstrakte gesetzliche Regelung schafft die Möglichkeit, Fachinformationen bei allen hiezu geeigneten Dienststellen einzuholen.

Erst die Entbindung vom Amtsgeheimnis gegenüber der Fachstelle gibt letzterer die Möglichkeit, die für die Aufgabenerfüllung notwendigen Unterstützungsleistungen bei den Dienststellen anzufordern. Die für die Entbindung vom Amtsgeheimnis erforderliche Gesetzesgrundlage wird mit Art. 32 Abs. 2 GE geschaffen.

Art. 33 sowie Art. 34 und Art. 35 bilden die massgebende Bestimmungen über die so genannten Einwirkungsbefugnisse, die dem Kontrollorgan nach Art. 28 Abs. 3 zweitem Abschnitt EU-DSRL eingeräumt werden müssen. Diese Bestimmung lautet wie folgt:

«Jede Kontrollstelle verfügt insbesondere über:

- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20, vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben<sup>41</sup> und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;»

Die Bedeutung dieser Bestimmung liegt darin, dass sich die Befugnis des Kontrollorgans nicht darauf beschränken darf, die vorgesetzte Behörde des öffentlichen Organs im Rahmen einer aufsichtsrechtlichen Anzeige, die keine rechtlich verbindliche Wirkung entfaltet, aufzufordern, Massnahmen zu ergreifen; eine solche Befugnis genügt den Anforderungen an wirksame Einwirkungsbefugnisse nicht. Vielmehr muss die Möglichkeit geschaffen werden, dass die datenschutzrechtlichen Anliegen des Kontrollorgan – oder in der Terminologie des st.gallischen Rechts: der Fachstelle für Datenschutz – «Eingang in ein förmliches rechtliches Verfahren finden».<sup>42</sup>

Die vorgeschlagene Regelung sieht zwei der Fachstelle einzuräumende Instrumente vor, die in einem zweistufigen Verfahren eingesetzt werden.

Das erste Instrument, das in *Art. 33* geregelt ist, besteht in Form der Empfehlung, welche die Fachstelle gegenüber dem öffentlichen Organ abgeben kann. Die Fachstelle verbindet die Empfehlung mit der Aufforderung gegenüber dem öffentlichen Organ, hierzu innert einer anzusetzenden Frist schriftlich Stellung zu nehmen. Eine Empfehlung ist abzugeben, wenn die Fachstelle Mängel bei der Bearbeitung von Personendaten feststellt (Bst. a) oder wenn es sich um die beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für den Grundrechtsschutz handelt, über welche das öffentliche Organ nach *Art. 8 GE* die Fachstelle im Voraus zu informieren hat (Bst. b). Nachdem die Fachstelle und das öffentliche Organ nach *Art. 30 Abs. 1 Bst. b GE* im Rahmen der Beratungsfunktion der Fachstelle zusammenarbeiten, wird das Instrument der Empfehlung in der Regel ausreichend sein, um das öffentliche Organ in die Lage zu versetzen, datenschutzrechtlich korrekt zu handeln.

*Art. 34* und *Art. 35*: Sollte das Verfahren der Empfehlung in einzelnen Fällen nicht genügen, indem das öffentliche Organ den Empfehlungen nicht oder bloss teilweise Nachachtung schenken will oder sich zu den Empfehlungen nicht äussert, so soll das zweite Instrument anwendbar sein. Die Fachstelle hat diesfalls die Möglichkeit, bei der zuständigen Behörde die Anordnung von Massnahmen zu beantragen (*Art. 34 Abs. 1* und *Art. 35 Abs. 1 GE*). Zuständige Behörde ist auf kantonaler Ebene das zuständige Departement oder die Staatskanzlei. Zuständig ist jenes Departement, zu dessen Geschäftsbereich sachinhaltlich eine Beziehung zu den datenschutzrechtlichen Handlungen besteht. Liegt eine von einer Dienststelle der Staatskanzlei zu erfüllende Aufgabe mit Datenschutzrelevanz vor, ist die Staatskanzlei zuständig. Die Regierung ist in jenen Fällen zuständige Behörde, bei denen ein Departement oder die Staatskanzlei nach *Art. 1 Bst. h Ziff. 1 GE* oder eine selbstständige öffentlich-rechtliche Anstalt des Kantons nach *Art. 1 Bst. h Ziff. 2 GE* als öffentliches Organ handelt. Auf Gemeindeebene ist der Rat Adressat der Anträge der Gemeindefachstelle für Datenschutz. Wenn er selber öffentliches Organ nach *Art. 1 Bst. h Ziff. 3 GE* ist, oder wenn ein selbstständiges öffentlich-rechtliches Gemeindeunternehmen, ein Gemeinde- oder ein Zweckverband als öffentliches Organ tätig ist und Anlass zu Empfehlungen gegeben hat, so hat die Gemeindefachstelle ihre Anträge an das zuständige Departement zu richten. Auch hier ergibt sich die Zuständigkeit nach Massgabe des in Frage stehenden Aufgabenbereichs. Mit der Bezeichnung der für den Erlass von Massnahmen zuständigen Organe wird gewährleistet, dass ein förmliches rechtliches Verfahren in Gang gesetzt werden kann.

<sup>41</sup> Gemeint ist damit die Vorabkontrolle; vgl. *Art. 9 GE*.

<sup>42</sup> Beat Rudin, *Datenschutzgesetz*, a.a.O., 68.

Die in Art. 34 Abs. 1 und Art. 35 Abs. 1 GE festgelegten Organe erlassen gestützt auf ihre Sachverhaltsfeststellungen und ihre Beurteilung der Situation gegebenenfalls eine Verfügung (Art. 34 Abs. 2 und Art. 35 Abs. 2 GE), in welcher sie das öffentliche Organ zu einem bestimmten Tun oder Unterlassen verpflichten. Vom Erlass einer Verfügung ist indessen – zwecks Vermeidung von Doppelspurigkeiten – abzusehen, wenn das öffentliche Organ eine Verfügung gegenüber der betroffenen Person erlässt, indem es zum Beispiel ein Gesuch um Berichtigung abweist.

Die zuständige Fachstelle für Datenschutz hat nach Art. 34 Abs. 3 GE beziehungsweise Art. 35 Abs. 3 GE die Möglichkeit, die Verfügung – je nach verfügender Instanz – mit Rekurs oder mit Beschwerde nach Massgabe des Gesetzes über die Verwaltungsrechtspflege anzufechten. Wesentlich ist mit Blick auf die Unabhängigkeit der Fachstelle für Datenschutz, dass diese ein förmliches Verfahren in Gang setzen kann und damit über Parteirechte verfügt. Letztlich beurteilt das Verwaltungsgericht die verfügten Massnahmen.

Art. 36 ist Ausfluss von Art. 28 Abs. 5 EU-DSRL, wonach die Kontrollstelle regelmässig einen Bericht über die Aufgabenerfüllung vorzulegen hat. Der Bericht ist nach Art. 36 Abs. 1 Ingress GE dem Wahlorgan zuzuleiten. Er enthält namentlich die in Bst. a bis c aufgeführten Teile.

Art. 36 Abs. 2 GE sieht ausdrücklich davon ab, dass der Bericht integral der Öffentlichkeit zugänglich gemacht wird. Vielmehr soll sich die Information der Öffentlichkeit darauf beschränken, dass sie über die Feststellungen der Fachstelle für Datenschutz, die Fälle von allgemeinem Interesse betreffen, in Kenntnis gesetzt wird. Auf diese Weise erhält der Bericht mehr Aufmerksamkeit als bei einer ausführlichen Darlegung der in Abs. 1 Bst. a bis c erwähnten und vorab die Wahlorgane interessierenden Aspekte. Eine Information der Öffentlichkeit ist jedenfalls in Bezug von Personendaten ausgeschlossen, die dem Amtsgeheimnis unterstehen.

Für die kantonale Fachstelle für Datenschutz besteht nach Art. 36 Abs. 3 GE überdies die Verpflichtung, dem Kantonsrat jährlich über ihre Tätigkeit Bericht zu erstatten. Diese Berichterstattung bildet unter anderem die Grundlage für die Wahrnehmung der Aufsichtsfunktionen durch die Staatswirtschaftliche Kommission nach Art. 27 Bst. a GE. Dem Bericht an den Kantonsrat kommt dieselbe Stellung zu, wie dem Geschäftsbericht der Regierung nach Art. 5a StVG in der Fassung gemäss dem vom Kantonsrat am 16. April 2008 erlassenen IV. Nachtrag zum Staatsverwaltungsgesetz.<sup>43</sup> Der Kantonsrat nimmt vom Bericht Kenntnis.

### 3.5.3. Bestimmungen über das Register über Datensammlungen

Mit den Bestimmungen über das Register über Datensammlungen werden Art. 8 Bst. a ER-Konv 108 sowie Art. 18 f. und 21 EU-DSRL umgesetzt. Das Register über Datensammlungen bildet ein Mittel für die Verwirklichung des Transparenzgebots bei der Bearbeitung von Personendaten. Es dient den betroffenen Personen als Grundlage für die Geltendmachung ihrer Rechte und ist zudem Basis für die Kontrolltätigkeit der Fachstellen.<sup>44</sup> Die Führung des Registers über Datensammlungen bildet gegenüber heute keine Neuerung, indem nach geltendem Art. 22 DSV bereits ein öffentliches Register zu führen ist.

Nach Art. 37 führt die Fachstelle für Datenschutz das Register über die in ihrem Zuständigkeitsbereich vorhandenen Datensammlungen. Der Zuständigkeitsbereich bemisst sich nach Art. 24 und 25 GE. Insbesondere ist die Organisation der kommunalen Fachstellen bestimmend für den jeweiligen Zuständigkeitsbereich auf Gemeindeebene.

<sup>43</sup> Referendumsvorlage zum IV. Nachtrag zum Staatsverwaltungsgesetz, vom Kantonsrat erlassen am 16. April 2008, in: ABI 2008, 1556 ff.

<sup>44</sup> Beat Rudin, Datenschutzgesetze, a.a.O., 61 f.

Eine Besonderheit ergibt sich, wenn Private Staatsaufgaben erfüllen. In diesem Fall ist nach Art. 37 Abs. 2 GE massgebend, ob kantonale Aufgaben oder ob Aufgaben der Gemeinden zur Erfüllung an Private übertragen worden sind.

Art. 38 listet die Bestandteile des Registers auf. Diese ergeben sich aufgrund der erwähnten Zwecke, die dem Register zugedacht sind. Die Aufzählung von Art. 38 Abs. 1 GE ist nicht abschliessend; sie kann je nach Bedarf erweitert, nicht jedoch verkürzt werden.

Das Register ist nach Art. 38 Abs. 2 GE wenigstens jährlich zu aktualisieren. Dem Transparenzgebot entsprechend und damit es als Grundlage für die Geltendmachung der Rechte von betroffenen Personen dienen kann, ist das Register öffentlich (Art. 38 Abs. 3 GE).

Art. 39 auferlegt dem öffentlichen Organ Meldepflichten, damit die Fachstelle für Datenschutz über die für die Führung und die Aktualisierung des Registers erforderlichen Informationen verfügt.

### 3.6. Schlussbestimmungen

Art. 40: Nach Art. 24 EU-DSRL müssen Sanktionen bei Verstössen gegen das Datenschutzgesetz vorgesehen werden. Möglich sind Strafbestimmungen für Amtsgeheimnisverletzungen oder für die auftragswidrige Verwendung oder Bekanntgabe von Personendaten durch Dritte bei einer Datenbearbeitung im Auftrag.<sup>45</sup> Das Amtsgeheimnis wird durch Art. 320 des Strafgesetzbuches (SR 311.0; abgekürzt StGB) genügend geschützt. So wird die Verletzung der datenschutzrechtlichen Schweigepflicht durch eine Amtsperson der kantonalen oder der kommunalen Verwaltung fast immer schon durch diese Bestimmung erfasst.<sup>46</sup> Es erübrigt sich daher, Strafbestimmungen für Amtsgeheimnisverletzungen in das kantonale Recht aufzunehmen. Nicht unter den Tatbestand von Art. 320 StGB fällt hingegen die Datenbearbeitung durch Personen, die von einer Behörde zur Datenbearbeitung beauftragt wurden. Neu ist deshalb die auftragswidrige Bearbeitung von Daten unter Strafe zu stellen. Damit wird auf jene Fälle Bezug genommen, in denen öffentliche Organe des Kantons oder der Gemeinden nach Art. 9 GE die Bearbeitung von Daten an externe Dritte ausgelagert haben.

Mit Art. 41 wird das Staatsverwaltungsgesetz geändert. Es sind die geltenden Bestimmungen über den Datenschutz in Art. 8 bis 11 StVG aufzuheben. In Bezug auf die finanzielle Aufsicht ist die kantonale Finanzkontrolle als Aufsichtsorgan einzusetzen, was eine entsprechende Anpassung von Art. 42b Abs. 1 StVG nötig macht. Sodann ist die für den Datenschutz festgelegte Ermächtigung zum Erlass von Verordnungsrecht in Art. 95 Bst. d StVG aufzuheben.

Art. 42 führt zur Aufhebung von Art. 9bis GG, wonach die Vorschriften über den Datenschutz in der Staatsverwaltung, d.h. die entsprechenden Bestimmungen des Staatsverwaltungsgesetzes und der Datenschutzverordnung, sachgemäss für die Gemeinden gelten.

Art. 43 sieht eine Ergänzung des Sozialhilfegesetzes (sGS 381.1; abgekürzt SHG) vor. Nach Art. 1 Bst. b Ziff. 3 GE gelten Leistungen und Massnahmen der sozialen Hilfe als besonders schützenswerte Personendaten. Was die Amts- und Verwaltungshilfe im Sozialversicherungsrecht betrifft, gilt Art. 32 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechtes (SR 830.1). Im Bereich der Leistungen der Sozialhilfe fehlt eine analoge allgemeine Regelung.<sup>47</sup> Um den diesbezüglichen Bedürfnissen hinreichend Rechnung tragen zu können, ist in das Sozialhilfegesetz ein neuer Art. 6bis aufzunehmen. Für die mit dem Vollzug des Sozialhilfegesetzes betrauten Behörden und für die weiteren Behörden, wie Polizei, Betrei-

<sup>45</sup> Vgl. Beat Rudin, Datenschutzgesetze, a.a.O., 64 f.

<sup>46</sup> Franz Riklin, Rz. 8 zum 7. Abschnitt des eidgDSG, in: Basler Kommentar zum Datenschutzgesetz, hrsg. von Urs Maurer-Lambrou und Nedim Peter Vogt, 2. Aufl., Basel / Genf / München 2006.

<sup>47</sup> Es gibt einzelne sachbezogene Regelungen, die auch für die Sozialhilfe massgebend sind (z.B. Art. 91 Abs. 5 des Bundesgesetzes über Schuldbetreibung und Konkurs [SR 281.1], nicht jedoch eine allgemein gültige Amtshilfebestimmung.

bungsämter, Steuerämter oder Gerichte, soll eine formell-gesetzliche Grundlage für die Amtshilfe in Form des Informationsaustauschs geschaffen werden. Dabei sollen nur diejenigen Informationen vermittelt werden, die für die Erfüllung der Aufgaben geeignet und erforderlich sind (Abs. 1), und mit Abs. 2 soll den zuständigen Behörden das Recht eingeräumt werden, relevante Informationen zur Prüfung und Ahndung allfälliger Sozialhilfemissbräuche an die Sozialhilfebehörden zu melden.

Mit *Art. 44* werden der in Art. 37 des Polizeigesetzes (sGS 451.1; abgekürzt PolG) festgelegten Auskunfts- und Berichtigungsanspruch sowie das in Art. 39 Bst. c PolG erwähnte Auskunfts- und Berichtigungsverfahren aufgehoben. Für bei den Polizeiorganen vorhandene Daten gelten neu die Bestimmungen des Datenschutzgesetzes.

*Art. 45* sieht Änderungen im Gesetz über die Niederlassung der Schweizer (sGS 453.1; abgekürzt NG) vor. Die für das Einwohneramt geltende Datenschutzbestimmung von Art. 13 NG ist aufzuheben; Einwohnerämter sind öffentliche Organe nach Art. 1 Bst. h Ziff. 3 GE und mithin dem Datenschutzgesetz unterstellt. Auskünfte an Private werden in aller Regel Anwendungsfälle von Art. 11 Abs. 1 Bst. c oder e GE sein. Hinzu kommt, dass Art. 13 NG insofern unvollständig ist, als die Bestimmung keine Regelung über die Bekanntgabe von Daten an Dienststellen enthält. In Art. 16 Bst. b zweitem Satzteil wird die Regierung ermächtigt, die zum Vollzug des NG notwendigen Verordnungsvorschriften über den Datenschutz zu erlassen. Diese Ermächtigungsklausel wird mit dem Datenschutzgesetz hinfällig.

*Art. 46* ändert Art. 2 GerG. In Konkretisierung von Art. 1 Bst. h und Art. 2 Abs. 2 Bst. c GE wird im neuen Abs. 3 von Art. 2 GerG die Anwendbarkeit des Datenschutzgesetzes für die Justiz festgehalten. Unter anderem wird damit die Rechtsgrundlage geschaffen, dass die kantonale Fachstelle für Datenschutz ihre Funktionen auch im Bereich der Justizverwaltung ausübt.

*Art. 47* ermächtigt die Regierung, das Datum des Vollzugsbeginns des Datenschutzgesetzes festzulegen.

## **4. Vernehmlassungsverfahren**

### **4.1. Grundsätzliche Bemerkungen**

Mit Beschluss der Regierung vom 4. März 2008 wurden das Sicherheits- und Justizdepartement sowie die Staatskanzlei ermächtigt, über den Entwurf des Datenschutzgesetzes (Vernehmlassungsentwurf; abgekürzt VLE) ein Vernehmlassungsverfahren durchzuführen. Dieses wurde am 5. März 2008 eröffnet. Innert der bis zum 30. April 2008 verlängerten Vernehmlassungsfrist haben die CVP, die SVP, die SP, die FDP, die Vereinigung St.Galler Gemeindepräsidentinnen und Gemeindepräsidenten (VSGP), das Netzwerk St.Galler Gemeinden, der Verband St.Gallischer Ortsgemeinden, das Kantonsgericht, das Verwaltungsgericht, die Industrie- und Handelskammer (IHK), das KMU Forum sowie der Kantonale Gewerkschaftsbund Stellung genommen. In grundsätzlicher Hinsicht wurde – insbesondere mit Blick auf die beiden Assoziierungs-Abkommen von Schengen und Dublin sowie der damit einhergehenden europarechtlichen Vorgaben namentlich im Sicherheitsbereich – durchwegs Zustimmung signalisiert. Der Entwurf wurde als pragmatisch, überzeugend, auf den Kanton St.Gallen zugeschnitten und ausgereift bezeichnet. Verschiedentlich kam zum Ausdruck, dass der Rechtsanwendung grosse Bedeutung zukommen werde, nachdem viele Bestimmungen Ermessensspielräume enthielten. Dabei werde es unabdingbar sein, den Vollzug so zu gestalten, dass die Zusammenarbeit sowohl unter den Behörden derselben staatlichen Ebene wie auch zwischen dem Kanton und den Gemeinden nicht beeinträchtigt werden darf.

Angesichts der zustimmenden Grundhaltung zum Gesetzesentwurf beschränken sich die erhobenen Vorbehalte und die eingegangenen Vorschläge auf einzelne konkrete Bestimmungen. Dabei kann einer Reihe von Anregungen namentlich aus drei Gründen nicht Rechnung getragen werden:

- Der für die Schweiz aufgrund des Schengen- und des Dublin-Assoziierungs-Abkommens Gültigkeit erlangende Datenschutzstandard, wie er sich insbesondere aus den Bestimmungen von SDÜ, EU-DSRL, ER-Konv 108 und ZP zur ER-Konv 108 ergibt,<sup>48</sup> lässt Änderungen im Gesetzesentwurf nicht zu.
- Spezialgesetzliche Regelungen des Datenschutzes, wie zum Beispiel im Strafverfahrensrecht, gehen dem Datenschutzgesetz vor, weshalb in verschiedenen Vernehmlassungen angeregte Ergänzungen im Gesetzesentwurf unberücksichtigt bleiben.
- Es wird übersehen, dass der Regelungsumfang des Datenschutzgesetzes auf die datenschutzrelevante Bearbeitung von Personendaten im Sinn von Art. 1 Bst. e und f in Verbindung mit Art. 1 Bst. a und b GE beschränkt ist; nicht jeder Daten- oder Informationsaustausch zwischen den Behörden und nicht jedes Einholen von Informationen beziehungsweise Verbreiten von Informationen fallen unter das Datenschutzrecht.

Nachfolgend wird auf einzelne Bestimmungen eingegangen, die aufgrund des Vernehmlassungsverfahrens zu besonderen Bemerkungen Anlass geben.

## 4.2. Vorbehalte und Vorschläge zu einzelnen Artikeln

### 4.2.1. Abschnitt I (Allgemeine Bestimmungen)

Zu Art. 1 Bst. b Ziff. 3 VLE wurde bemerkt, dass es keine «Massnahmen der Sozialhilfe» gäbe; die Bestimmung sei zu streichen. Der Wortlaut dieser Bestimmung ist praktisch identisch mit Art. 3 Bst. c Ziff. 3 eidgDSG, wonach «Massnahmen der sozialen Hilfe» zu den besonders schützenswerten Personendaten gehören. In Art. 1 Bst. b Ziff. 3 GE wird nunmehr die Wendung «Leistungen und Massnahmen der sozialen Hilfe» verwendet, dies einerseits mit Blick auf das Sozialhilfegesetz, das im Bereich der persönlichen Sozialhilfe «Leistungen» vorsieht, sowie andererseits aufgrund der als «Massnahmen» zu bezeichnenden Instrumente der sozialen Hilfe, wie etwa Vormundschaftsmassnahmen oder der fürsorgerische Freiheitsentzug.<sup>49</sup>

In Bezug auf Art. 1 Bst. d GE wurde angeregt, den Begriff «Persönlichkeitsprofil» wegzulassen und an dessen Stelle die entsprechend geschützten Daten zu definieren. Der Begriff ist datenschutzrechtlich von Relevanz und allgemein gebräuchlich. Er wird auch in Art. 3 Bst. d eidgDSG verwendet. In der Botschaft des Bundesrates vom 23. März 1988 zum Bundesgesetz über den Datenschutz<sup>50</sup> wird Folgendes ausgeführt:

«Ein besonderer Schutz muss auch gewährt werden, wenn Persönlichkeitsprofile erstellt, ausgewertet oder an Dritte bekanntgegeben werden. Ein Persönlichkeitsprofil ist eine Zusammenstellung einer grösseren Zahl von Daten über die Persönlichkeitsstruktur, die beruflichen Fähigkeiten und Aktivitäten oder auch die ausserberuflichen Beziehungen und Tätigkeiten, die ein Gesamtbild oder ein wesentliches Teilbild der betreffenden Person ergibt. Persönlichkeitsprofile können zum Beispiel bei Sicherheitsüberprüfungen oder im Rahmen eines Anstellungsverhältnisses entstehen. Aber auch Datensammlungen über das Konsumverhalten oder über schulische und berufliche Qualifikationen sind geeignet, mindestens ein Teilbild der betroffenen Personen zu ergeben. Entscheidend ist, dass auch durch die systematische Zusammenstellung von an sich nicht besonders schützenswerten Daten (z. B. über Lesegewohnheiten, Reise- und Freizeitaktivitäten) sensitive Bereiche einer Person, z. B. ihre Weltanschauung, erschlossen werden können. Durch die Auswertungsmöglichkeiten der automatischen Datenverarbeitung und durch die Verknüpfung automatisierter Datenbestände ist die Erstellung von Persönlichkeitsprofilen leichter und häufiger geworden. Die Betroffenen haben oft keine Kenntnis vom Bestehen eines Profils und können so dessen Richtigkeit und Verwendung nicht kontrollieren.

<sup>48</sup> Vgl. Ziff. 1.1.3. dieser Botschaft.

<sup>49</sup> Vgl. Urs Belser, Rz. 17 zu Art. 3 eidgDSG, in: Basler Kommentar zum Datenschutzgesetz, hrsg. von Urs Maurer-Lambrou und Nedim Peter Vogt, 2. Aufl., Basel / Genf / München 2006.

<sup>50</sup> BBl 1988 II 413 ff.

Einmal erstellt, können aber Persönlichkeitsprofile den Betroffenen der Freiheit berauben, sich so darzustellen, wie er will. Sie vermögen mithin die Entfaltung der Persönlichkeit ganz wesentlich zu beeinträchtigen. Deshalb sollen sie, gleich wie besonders schützenswerte Daten, nur unter bestimmten Voraussetzungen erstellt und bearbeitet werden dürfen.»<sup>51</sup>

Der Begriff «Persönlichkeitsprofil» ist aus diesen Gründen zu belassen.

Im Zusammenhang mit der Definition des Begriffs «Gesetz» in Art. 1 Bst. k VLE und des Begriffs «Rechtsgrundlage» in verschiedenen Bestimmungen wurde die Zweckmässigkeit der Differenzierung zwischen den beiden Rechtsetzungsformen hinterfragt. Diese Differenzierung ist erforderlich, weil in bestimmten Fällen ein erhöhter datenschutzrechtlicher Standard gefordert wird, der dadurch erreicht wird, dass diesbezügliche Sachverhalte in einem formellen Gesetz zu regeln sind (Beispiel: Sachverhalte über besonders schützenswerte Personendaten). Demgegenüber genügt in vielen Fällen eine von der Erlassform unabhängige Rechtsgrundlage. Diese kann zwar ebenfalls in eine formell-gesetzliche Bestimmung gekleidet sein; zulässig sind aber auch Verordnungsbestimmungen. Die Differenzierung ist mithin beizubehalten. Zur Verdeutlichung ist Art. 1 Bst. k in den GE aufgenommen worden. (Art. 1 Bst. k VLE wurde zu Art. 1 Bst. I GE).

Art. 2 Abs. 2 Bst. a VLE sah vor, dass das Datenschutzgesetz keine Anwendung findet, wenn das öffentliche Organ archivierte Daten bearbeitet, deren Alter die Verletzung von schutzwürdigen privaten Interessen bei der Bearbeitung ausschliesst. Aufgrund des Vernehmlassungsverfahrens hat sich gezeigt, dass diese Regelung Rechtsunsicherheit schaffen würde sowie erheblich auslegungsbedürftig und kaum praktikabel wäre. Sie wurde deshalb nicht in den GE übernommen. Hingegen hat sich ergeben, dass Personendaten, die von den zuständigen Archiven des Kantons und der Gemeinden dauerhaft archiviert werden, nicht dem Geltungsbereich des Datenschutzgesetzes zu unterstellen sind. Hierfür wird das künftige Archivgesetz mit der Aufnahme von Schutzfristen datenschutzbezogene Massnahmen in Form von spezialgesetzlichen Bestimmungen vorsehen.

Im Zusammenhang mit Art. 2 Abs. 2 Bst. c GE wurde angeregt, alle – nicht nur die hängigen – Rechtspflegeverfahren vom Geltungsbereich der Datenschutzgesetzes auszunehmen. Die Nichtunterstellung der hängigen Verfahren deckt sich mit Art. 2 Abs. 2 Bst. c eidgDSG. Hierzu äusserte sich der Bundesrat in seiner Botschaft zum Datenschutzgesetz vom 23. März 1988 wie folgt:<sup>52</sup>

«Rechtsprechungsverfahren folgen genauen Regeln, die in den Prozessgesetzen festgehalten sind. Zweck verschiedener Prozessbestimmungen ist es dabei, die Persönlichkeit der in ein Verfahren Einbezogenen zu schützen. Dies gilt namentlich für die Bestimmungen über die Anhörungs-, Akteneinsichts- und Mitwirkungsrechte der Betroffenen. Prozessgesetze enthalten aber auch eigentliche Bestimmungen über die Informationsbearbeitung, indem sie etwa festlegen, wie der Prozessstoff gesammelt und gewürdigt wird. Im Prozessrecht werden auch die Interessen des Richters und der Parteien an einer Information gegenüber dem Geheimhaltungsinteresse derjenigen Person, welche die Angaben machen könnte, abgewogen, so bei der Regelung des Zeugnisverweigerungsrechts. Prozessrecht ist deshalb in einem gewissen Sinne immer auch Datenschutzrecht. Fände nun das Datenschutzgesetz auch auf Rechtsprechungsverfahren Anwendung, so würden sich zwei Gesetze mit zum Teil gleicher Zielrichtung überlagern. Das aber würde zu Rechtsunsicherheiten, zu Koordinationsproblemen und schliesslich zu Verfahrensverzögerungen führen. Die Ausnahmeklausel ... soll dies verhindern.»

In Bezug auf die abgeschlossenen Verfahren treffen diese Überlegungen nicht zu. Die Bearbeitung von Personendaten aus abgeschlossenen Verfahren soll deshalb nach den daten-

---

<sup>51</sup> BBl 1988 II 446 f.

<sup>52</sup> BBl 1988 II 442 f.

schutzgesetzlichen Bestimmungen erfolgen, zumal das geltende Recht diesbezüglich nur rudimentäre Regelungen kennt.

#### 4.2.2. *Abschnitt II (Bearbeitung von Personendaten)*

Art. 3 Abs. 2 VLE sah vor, dass jedes öffentliche Organ nach Massgabe der von ihm zu erfüllenden Aufgaben für die Einhaltung des Datenschutzes verantwortlich ist, wenn mehrere öffentliche Organe Personendaten einer Datensammlung bearbeiten. Im Vernehmlassungsverfahren wurde vorgeschlagen, die Datenherrschaft klar zu definieren. Dieser Vorschlag ist berechtigt, denn eine Aufteilung der Verantwortung auf alle beteiligten Organe ist wenig praktikabel und bei einer Vielzahl von öffentlichen Organen kaum durchführbar. Art. 3 Abs. 2 GE sieht deshalb die Bezeichnung eines einzigen öffentlichen Organs vor, das für ein datenschutzrechtlich korrektes Vorgehen verantwortlich ist.

Sodann wurde zu Art. 4 VLE angeregt, die Aufzählung der Grundsätze zu erweitern und namentlich auch den Grundsatz der Verhältnismässigkeit und den Grundsatz von Treu und Glauben bei der Bearbeitung von Personendaten festzuschreiben. Diesem Anliegen wird in Art. 4 GE insofern nicht gefolgt, weil es der st.gallischen Gesetzgebungspraxis widerspricht, verfassungsrechtliche Normen auf Gesetzesstufe zu wiederholen. Deshalb beschränkt sich der Gehalt von Art. 4 GE auf die einschlägigen datenschutzrelevanten Grundsätze.

In Bezug auf Art. 5 Abs. 3 VLE, der die Bekanntgabe von besonders schützenswerten Personendaten für zulässig erklärte, wenn die betroffene Person hierzu im Einzelfall ihre Einwilligung gegeben hat, wurde angeregt, eine Veröffentlichung zuzulassen, wenn die betroffene Person eine Bearbeitung nicht ausdrücklich untersagt hat. Dem steht entgegen, dass keine praktikable und umsetzbare Möglichkeit besteht, festzustellen zu können, ob jemand die Bearbeitung ausdrücklich untersagt hat. Abgesehen davon dient es dem Datenschutz mehr, wenn die betroffene Person «im Einzelfall» und «ausdrücklich» einzuwilligen hat und dabei auch über «Zweck und Art der vorgesehenen Bearbeitung» in Kenntnis gesetzt werden muss. Art. 5 Abs. 3 VLE ist im Übrigen zwecks Klärung, dass es dabei um die Kategorie der besonders schützenswerten Personendaten geht, im Sinn einer weiteren Anregung im Vernehmlassungsverfahren mit Art. 5 Abs. 2 VLE zusammengefasst und als Art. 5 Abs. 2 GE formuliert worden.

Zu Art. 9 VLE wurde angeführt, dass die Übertragung der Bearbeitung von Personendaten an Dritte problematisch sei und davon abgesehen werden sollte. Nachdem in Übereinstimmung mit Art. 24 Abs. 2 KV Aufgaben von öffentlichem Interesse von Privaten wahrgenommen werden können, wobei nach Art. 25 Abs. 3 KV das Gesetz die Voraussetzungen für die Übertragung der Erfüllung von Staatsaufgaben an Private zu regeln hat, ist es folgerichtig, dass den Privaten auch die Bearbeitung von Personendaten übertragen werden können. Vielfach setzt die Aufgabenerfüllung die Bearbeitung von Personendaten zwingend voraus. Allerdings ist aufgrund einer weiteren Anregung Art. 9 Abs. 1 GE dahingehend ergänzt worden, dass die Übertragung der Bearbeitung von Personendaten an Dritte nur erfolgen darf, wenn diese Gewähr für ein datenschutzrechtlich einwandfreies Handeln bieten.

#### 4.2.3. *Abschnitt III (Bekanntgabe von Personendaten)*

Dem Vorschlag zu Art. 11 Abs. 2 VLE und Art. 13 Abs. 2 VLE, davon abzusehen, dass öffentliche Organe beim gegenseitigen Austausch von Personendaten verpflichtet sind, den Nachweis zu erbringen, dass sie bestimmte Personendaten benötigen, wurde Rechnung getragen. Es genügt, wenn öffentliche Organe Personendaten für die Aufgabenerfüllung benötigen (Art. 11 Abs. 2 GE) beziehungsweise die Personendaten für die Aufgabenerfüllung unentbehrlich sind (Art. 13 Abs. 2 GE). Es ist der Praxis zu überlassen, in welcher Form das Bestehen dieser Voraussetzungen festgestellt wird; in vielen Fällen wird schon aufgrund des Gesetzes, in dem die Aufgabe festgehalten ist, offensichtlich sein, dass Personendaten benötigt werden beziehungsweise unentbehrlich sind. Die in den GE aufgenommene Regelung berücksichtigt das Erfordernis, dass das Datenschutzrecht die Zusammenarbeit von Behörden sowohl innerhalb der gleichen staatlichen Ebene wie auch staatsebenenübergreifend nicht behindern darf.

Im Vernehmlassungsverfahren wurde angeregt, die in Art. 14 VLE vorgesehene Möglichkeit der Bekanntgabe von bestimmten Personendaten für gemeinnützige und schutzwürdige ideelle Zwecke zu streichen. Es bestehe kein Anlass, bestimmte gesellschaftliche oder politische Gruppierungen bevorzugt zu behandeln. Diesem Einwand ist entgegenzuhalten, dass es nicht um die Privilegierung von Organisationen oder Institutionen geht, sondern um die Unterstützung der Erfüllung von gemeinnützigen und schutzwürdigen ideellen Aufgaben. Die mannigfachen Formen von ehrenamtlicher Tätigkeit, die im öffentlichen Interesse geleistet wird, soll nicht durch datenschutzrechtliche Beschränkungen behindert werden.

#### 4.2.4. *Abschnitt IV (Rechte der betroffenen Person)*

Art. 20 Abs. 1 zweiter Satz VLE sah vor, dass das öffentliche Organ, das die Datensammlung führt, die Beweislast für die Richtigkeit der Daten trägt. Dieser Regelung wurde mit dem Hinweis opponiert, dass damit von einer Mitwirkungspflicht der betroffenen Person an der Feststellung der Richtigkeit von Personendaten abgesehen werde, was ungerechtfertigt sei. Dieser Überlegung ist zuzustimmen, weshalb Art. 20 Abs. 1 zweiter Satz GE lediglich den Sachverhalt des Beweises der Richtigkeit oder der Unrichtigkeit und nicht mehr die Zuordnung der Beweisspflicht festhält. Damit wird eine dem Art. 25 Abs. 2 eidgDSG analoge Regelung getroffen.

#### 4.2.5. *Abschnitt V (Fachstelle für Datenschutz)*

Zu diesem Abschnitt wurden grundsätzliche Bemerkungen zu zwei Regelungsbereichen, nämlich einerseits zur organisatorischen Ausgestaltung der Fachstellen für Datenschutz (Art. 24 ff. VLE) und andererseits zu den formellen Einwirkungsmöglichkeiten der Fachstellen (Art. 34 VLE), angebracht.

In Bezug auf die organisatorische Ausgestaltung wurde die Schaffung einer einzigen kantonalen Fachstelle, die auch für die Gemeinden tätig sein soll, vorgeschlagen. Art. 24 GE sieht von der Übernahme dieses Vorschlages ab. Zu berücksichtigen ist namentlich, dass der Datenschutz und das Datenschutzrecht eine enge Verbindung zur Erfüllung der Staatsaufgaben aufweisen. Der Datenschutz geht mit der Aufgabenerfüllung einher; er ist Bestandteil des auf die Aufgabenerfüllung ausgerichteten Handelns der öffentlichen Organe von Kanton und Gemeinden. Die unmittelbare Aufsicht über die Einhaltung des Datenschutzes und die damit verbundenen Supportleistungen insbesondere im Bereich der Beratung sollen deshalb nach Massgabe der Aufgabenzuteilung auf Kanton und Gemeinden je separat für die kantonalen und die kommunalen öffentlichen Organe ausgerichtet sein. Die mit der vorliegenden Regelung anvisierte Nähe der Fachstelle zu den zuständigen öffentlichen Organen trägt zu einer sachgerechten und effizienten Wahrnehmung der Aufsichts- und Beratungstätigkeiten nach Art. 30 GE bei.

Ein weiterer Vorschlag ging dahin, die Aufgaben der Fachstelle an aussenstehende Dritte, beispielsweise an Personen, die rechtsanwaltlich oder im Universitätsbereich tätig sind, zu übertragen. Dieser Vorschlag entspricht nicht den europarechtlichen Vorgaben. Art. 28 Abs. 1 EU-DSRL legt fest, dass «eine oder mehrere öffentliche Stellen» zu beauftragen sind, «die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen», und nach Art. 1 Abs. 1 ZP zur EU-Konv 108, der mit dem Randtitel «Aufsichtsbehörden» versehen ist, sieht jede Vertragspartei «mindestens eine Behörde vor, die dafür zuständig ist, die Einhaltung jener innerstaatlichen Rechtsvorschriften zu gewährleisten, durch die die in Kapitel II und III des Übereinkommens bzw. in diesem Protokoll festgelegten Grundsätze umgesetzt werden.» Damit wird allerdings nicht ausgeschlossen, dass beispielsweise eine rechtsanwaltlich tätige Person nach Art. 28 Abs. 2 GE zur Leiterin oder zum Leiter der Gemeindefachstelle für Datenschutz und damit als Aufsichtsbehörde im Sinn der EU-DSRL und des ZP zur EU-Konv 108 gewählt wird und in einer nebenamtlichen Anstellung die Funktionen der Gemeindefachstelle erfüllt.

Sodann wurde angeregt, den Gemeinden im Gesetz lediglich die Verpflichtung zu überbinden, eine unabhängige Fachstelle für Datenschutz einzurichten, wobei sie diese durch Leistungsvereinbarung einsetzen können. Dieser Anregung kann nicht Rechnung getragen werden. So-

weit die Leistungsvereinbarung mit Dritten abgeschlossen würde, stünden die erwähnten europarechtlichen Regelungen entgegen. Wird die Leistungsvereinbarung mit einer öffentlich-rechtlichen Körperschaft – beispielsweise mit einer bestimmten Gemeinde – abgeschlossen, bedürfte es dennoch gesetzlicher Vorgaben, welche die geforderte Unabhängigkeit definieren und gewährleisten.

Aufgrund des Vernehmlassungsverfahrens hat sich ergeben, dass die im Vernehmlassungsentwurf vorgesehene Regelung, der Verwaltungsrekurskommission Verfügungsbefugnisse zur Anordnung von datenschutzrechtlichen Massnahmen zuzuerkennen, aus Gründen der Gewaltenteilung verfassungswidrig und überdies unter dem Gesichtspunkt der st.gallische Rechtspflegeordnung systemfremd wäre. Art. 34 und 35 GE sehen deshalb ein Verfahren vor, dass die jeweils oberste Verwaltungsbehörde zur Anordnung von Massnahmen zuständig erklärt, worauf die entsprechende Verfügung mit Rekurs beziehungsweise Beschwerde angefochten werden kann. Um die geforderte Unabhängigkeit der Fachstellen für Datenschutz zu gewährleisten, werden ihnen Parteirechte eingeräumt. Insbesondere sind sie berechtigt, Verfügungen und Entscheide über Verfügungen auf dem Rechtsmittelweg anzufechten.

#### 4.2.6. *Abschnitt VI (Register über Datensammlungen)*

Im Vernehmlassungsverfahren ist gewünscht worden, dass für die Einsicht in die Register ein besonderes Interesse – ähnlich der Einsicht in das Grundbuch nach Art. 970 Abs. 1 des Schweizerischen Zivilgesetzbuches (SR 210; abgekürzt ZGB) – bestehen sollte. Dieses Anliegen kann nicht berücksichtigt werden, weil jede Person zwecks Prüfung, ob und welche Personendaten bearbeitet werden, zur Einsicht berechtigt sein muss, um alsdann ihre Rechte nach Art. 17 und 20 f. GE wahrnehmen zu können.

## 5. **Kostenfolgen**

Die Schätzung des jährlichen Aufwandes der kantonalen Fachstelle für Datenschutz ergibt bei einer Besetzung mit 150 Stellenprozenten (Leiterin oder Leiter mit juristischer Qualifikation sowie Sachbearbeiterin oder Sachbearbeiter) einen Personalaufwand von rund 208'100 Franken.<sup>53</sup> Hinzu kommt der Sachaufwand (umfassend Bürokosten und Drucksachen sowie Informatikbetriebskosten und Spesenentschädigungen sowie Kosten für Aufträge an Dritte), der aufgrund von Erfahrungswerten mit rund 40'000 Franken zu veranschlagen ist. Es resultieren somit jährlich wiederkehrende Ausgaben von rund 250'000 Franken. Wird der Personal- und Sachaufwand des bereits bestehenden kantonalen Kontrollorgans für Datenschutz mitberücksichtigt, ergibt sich durch die Schaffung der im vorliegenden Gesetzesentwurf vorgesehenen kantonalen Fachstelle eine Erhöhung des jährlichen Aufwandes von rund 175'000 Franken.

Die einmaligen Investitionskosten für Einrichtung und Ausstattung der Räume liegen je Arbeitsplatz und Büro gemäss Erfahrungswerten bei rund 12'000 Franken beziehungsweise bei rund 24'000 Franken für zwei Arbeitsplätze.

Die jährlichen Aufwendungen der Gemeinden lassen sich nicht beziffern, weil sie von der organisatorischen Ausgestaltung der Gemeindefachstellen abhängig sind (vgl. Art. 24 Abs. 2 und Art. 25 GE).

---

<sup>53</sup> Jahresbesoldung (einschliesslich 13. Monatslohn) für Leiterin oder Leiter zuzüglich Arbeitgeberbeiträge: 149'000 Franken; Jahresbesoldung (einschliesslich 13. Monatslohn) für Sachbearbeiterin oder Sachbearbeiter zuzüglich Arbeitgeberbeiträge, Ansatz 50 Prozent: 57'400 Franken. Was die Leitungsstelle betrifft, sind rund 70 Prozent des Betrags neue Ausgaben, nachdem das bereits bestehende kantonale Kontrollorgan für Datenschutz im Ausmass von 30 Prozent besetzt ist.

## **6. Rechtliches**

Die jährlich wiederkehrenden Ausgaben erreichen die in Art. 7 Abs. 1 des Gesetzes über Referendum und Initiative (sGS 125.1; abgekürzt RIG) festgelegte Grenze einer Jahresausgabe von Fr. 300'000.– nicht. Das Datenschutzgesetz untersteht nach Art. 5 RIG dem fakultativen Gesetzesreferendum.

## **7. Antrag**

Wir beantragen Ihnen, Frau Präsidentin, sehr geehrte Damen und Herren, auf den Entwurf des Datenschutzgesetzes einzutreten.

Im Namen der Regierung,  
Die Präsidentin:  
Kathrin Hilber

Der Staatssekretär:  
Martin Gehrer

## Datenschutzgesetz

Entwurf der Regierung vom 20. Mai 2008

Der Kantonsrat

hat von der Botschaft der Regierung vom 20. Mai 2008<sup>54</sup> Kenntnis genommen und erlässt

in Ausführung von Art. 2 Bst. g der Kantonsverfassung vom 10. Juni 2001<sup>55</sup>

als Gesetz:

### I. Allgemeine Bestimmungen

#### *Begriffe*

*Art. 1.* In diesem Erlass bedeuten:

- a) Personendaten: Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;
- b) besonders schützenswerte Personendaten: Angaben über:
  - 1. religiöse, weltanschauliche sowie politische Ansichten und Tätigkeiten. Ausgenommen sind Angaben über die Mitgliedschaft bei einer Religionsgemeinschaft, einer Organisation oder einer politischen Partei, wenn die betroffene Person diese selbst bekannt gegeben hat oder für ein öffentliches Amt kandidiert;
  - 2. Gesundheit, Intimsphäre und Rassenzugehörigkeit;
  - 3. Leistungen und Massnahmen der sozialen Hilfe;
  - 4. strafrechtliche sowie disziplinarische Verfahren und Sanktionen;
- c) betroffene Person: natürliche oder juristische Person sowie Personengemeinschaften, über die Personendaten bearbeitet werden;
- d) Persönlichkeitsprofil: Zusammenstellung von Personendaten, welche die Beurteilung der Persönlichkeit einer natürlichen Person erlaubt;
- e) Bearbeitung von Personendaten: Umgang mit Personendaten, insbesondere Beschaffung, Aufbewahrung, Verwendung, Bekanntgabe, Veränderung oder Vernichtung;
- f) Bekanntgabe von Personendaten: Zugänglichmachen von Personendaten sowie Gewährung von Einsicht, Weitergabe und Veröffentlichung;
- g) Datensammlung: Bestand von Personendaten, der nach Personen erschlossen oder erschliessbar ist;
- h) öffentliches Organ: Organ, Behörde oder Dienststelle von:
  - 1. Kanton;
  - 2. selbstständiger öffentlich-rechtlicher Anstalt des Kantons;
  - 3. Gemeinde;
  - 4. selbstständigem öffentlich-rechtlichem Gemeindeunternehmen;
  - 5. Gemeindeverband und Zweckverband.Dem öffentlichen Organ sind Private gleichgestellt, wenn sie Staatsaufgaben erfüllen.

<sup>54</sup> ABI 2008, ●●.

<sup>55</sup> sGS 111.1.

- i) Empfängerin oder Empfänger: natürliche oder juristische Person, die vom öffentlichen Organ Personendaten erhält;
- j) Fachstelle für Datenschutz: von Kanton und Gemeinde eingesetztes Organ für Aufsicht und Beratung im Datenschutz;
- k) Rechtsgrundlage: Erlass mit allgemein verbindlichen Bestimmungen, insbesondere Gesetz und Verordnung. Der Verordnung sind vom fakultativen Referendum ausgenommene Vollzugsvorschriften von Gemeinden gleichgestellt;
- l) Gesetz: Erlass, der nach Art. 67 der Kantonsverfassung vom 10. Juni 2001<sup>56</sup> von den Stimmberechtigten ausdrücklich oder stillschweigend angenommen wurde, sowie zwischenstaatliche Vereinbarungen, denen nach Massgabe ihres Inhalts Verfassungs- oder Gesetzesrang zukommt. Dem Gesetz sind die Gemeindeordnung sowie das rechtsetzende Reglement und die rechtsetzende Vereinbarung gleichgestellt.

#### *Geltungsbereich*

*Art. 2.* Dieser Erlass regelt die Bearbeitung von Personendaten durch öffentliche Organe.

Er wird nicht angewendet:

- a) wenn das öffentliche Organ am wirtschaftlichen Wettbewerb teilnimmt und dabei nicht hoheitlich handelt;
- b) auf Personendaten, die von einer im Dienst- oder Auftragsverhältnis mit dem öffentlichen Organ stehenden natürlichen Person zum ausschliesslich persönlichen Gebrauch bearbeitet werden und anderen Personen weder ausgehändigt werden noch ihnen zugänglich sind;
- c) in hängigen Verfahren der Zivil-, der Straf- und der gerichtlichen Verwaltungsrechtspflege sowie in hängigen Rechtshilfeverfahren;
- d) auf Personendaten, die das zuständige Archiv von Kanton und Gemeinde dauerhaft aufbewahrt.

## **II. Bearbeitung von Personendaten**

#### *Verantwortlichkeit*

*Art. 3.* Wer Personendaten bearbeitet oder bearbeiten lässt, ist für die Einhaltung des Datenschutzes verantwortlich.

Bearbeiten mehrere öffentliche Organe Personendaten einer Datensammlung, bezeichnen sie das für Einhaltung des Datenschutzes verantwortliche Organ. Bei Uneinigkeit entscheidet die kantonale Fachstelle für Datenschutz.

#### *Grundsätze*

*Art. 4.* Das öffentliche Organ bearbeitet Personendaten nach Massgabe des Zwecks, der in der Rechtsgrundlage festgelegt ist, bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich ist.

Es stellt sicher, dass die Beschaffung der Personendaten und der Zweck ihrer Bearbeitung für die betroffene Person erkennbar und die Personendaten richtig und, nach Massgabe der Verwendung, vollständig sind.

Es trifft angemessene organisatorische und technische Massnahmen zur Sicherung der Daten vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten.

---

<sup>56</sup> sGS 111.1.

### *Voraussetzungen*

*Art. 5.* Die Bearbeitung von Personendaten ist zulässig, wenn eine Rechtsgrundlage besteht oder die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist.

Die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen ist zulässig, wenn:

- a) das Gesetz die Bearbeitung vorsieht oder
- b) die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe unentbehrlich ist oder
- c) die betroffene Person:
  - 1. im Einzelfall ausdrücklich sowie in Kenntnis von Zweck und Art der vorgesehenen Bearbeitung eingewilligt hat oder
  - 2. ihre Daten allgemein zugänglich gemacht hat.

### *Besondere Fälle a) Systematische Beschaffung*

*Art. 6.* Das öffentliche Organ gibt bei einer systematischen Beschaffung von Personendaten durch Fragebogen oder andere Formen von Umfragen bei einer Vielzahl von Personen bekannt:

- a) Zweck und Rechtsgrundlage der Bearbeitung;
- b) an der Beschaffung beteiligte Behörde oder Dienststelle und für diese handelnde Personen;
- c) Empfängerinnen und Empfänger der beschafften Personendaten.

### *b) Bearbeitung für nicht personenbezogenen Zweck*

*Art. 7.* Das öffentliche Organ anonymisiert Personendaten, die es für einen nicht personenbezogenen Zweck, insbesondere für Statistik, Planung und Forschung, bearbeitet, sobald der Zweck der Bearbeitung die Anonymisierung zulässt.

Es stellt sicher, dass bei Bekanntgabe des Ergebnisses Rückschlüsse auf betroffene Personen ausgeschlossen sind.

Es kann Personendaten einem anderen öffentlichen Organ oder Dritten zur Bearbeitung für einen nicht personenbezogenen Zweck überlassen, wenn die Empfängerin oder der Empfänger Gewähr bietet und sich schriftlich verpflichtet:

- a) die Verpflichtungen nach Abs. 1 und 2 dieser Bestimmung zu erfüllen;
- b) die Personendaten nicht weiterzugeben.

### *c) Bearbeitung mit besonderen Risiken für den Grundrechtesschutz*

*Art. 8.* Das öffentliche Organ meldet der Fachstelle für Datenschutz im Voraus die Bearbeitung von Personendaten, wenn damit besondere Risiken für den Schutz der Grundrechte der betroffenen Personen, insbesondere des Rechts auf persönliche Freiheit und des Schutzes der Privatsphäre, verbunden sein könnten.

### *Bearbeitung durch Dritte*

*Art. 9.* Das öffentliche Organ kann die Bearbeitung von Personendaten an Dritte übertragen, wenn die Übertragung nicht durch Gesetz ausgeschlossen ist und die beauftragten Dritten Gewähr für die datenschutzrechtlich einwandfreie Bearbeitung bieten.

Es stellt die Einhaltung des Datenschutzes sicher und legt insbesondere fest, dass die Personendaten:

- a) nur so bearbeitet werden, wie das öffentliche Organ es selbst tun dürfte;
- b) nach den für das öffentliche Organ geltenden gesetzlichen Bestimmungen bearbeitet werden;
- c) vor Verlust und Entwendung sowie unbefugter Kenntnisnahme und unbefugtem Bearbeiten gesichert werden.

Es prüft durch geeignete regelmässige Kontrollen, ob der Datenschutz eingehalten wird. Stellt es die Nichteinhaltung von Auflagen nach Abs. 2 dieser Bestimmung oder Verstösse gegen andere Datenschutzvorschriften fest, macht es die Übertragung rückgängig.

#### *Archivierung und Vernichtung*

*Art. 10.* Das öffentliche Organ bietet dem zuständigen Archiv von Kanton oder Gemeinde die Personendaten an, die es nicht mehr ständig benötigt. Vorbehalten bleiben besondere Bestimmungen über die Archivierung.

Das öffentliche Organ vernichtet die vom zuständigen Archiv als nicht archivierungswürdig bezeichneten Personendaten.

Auf die Vernichtung kann verzichtet werden, wenn die Personendaten:

- a) anonymisiert sind;
- b) vom öffentlichen Organ unmittelbar nach Mitteilung des zuständigen Archivs anonymisiert werden.

### **III. Bekanntgabe von Personendaten**

#### *Personendaten a) Grundsatz*

*Art. 11.* Die Bekanntgabe von Personendaten ist zulässig, wenn:

- a) eine Rechtsgrundlage besteht oder
- b) die betroffene Person eingewilligt hat oder
- c) die Bekanntgabe im Interesse der betroffenen Person liegt und deren Einwilligung nicht eingeholt werden kann oder
- d) ein öffentliches Interesse besteht, welches das schutzwürdige Interesse der betroffenen Person an der Geheimhaltung der Personendaten überwiegt, oder
- e) Empfängerin oder Empfänger ein schutzwürdiges Interesse glaubhaft macht, welches das schutzwürdige Interesse der betroffenen Person an der Geheimhaltung der Personendaten überwiegt.

Das öffentliche Organ gibt Personendaten einer Behörde des Bundes, eines anderen Kantons oder einem anderen öffentlichen Organ bekannt, wenn die Empfängerin oder der Empfänger die Personendaten zur Erfüllung einer gesetzlichen Aufgabe benötigt.

#### *b) Einschränkung der Bekanntgabe*

*Art. 12.* Das öffentliche Organ schränkt die Bekanntgabe von Personendaten ein oder verbindet sie mit Auflagen, wenn:

- a) besondere Bestimmungen über den Datenschutz es verlangen oder
- b) öffentliche Interessen oder schutzwürdige private Interessen es verlangen.

*Besonders schützenswerte Personendaten und Persönlichkeitsprofile*

Art. 13. Die Bekanntgabe von besonders schützenswerten Personendaten und Persönlichkeitsprofilen ist zulässig, wenn:

- a) das Gesetz die Bekanntgabe vorsieht oder
- b) die betroffene Person eingewilligt hat oder
- c) die Bekanntgabe im Interesse der betroffenen Person liegt und deren Einwilligung nicht eingeholt werden kann.

Das öffentliche Organ gibt besonders schützenswerte Personendaten und Persönlichkeitsprofile einer Behörde des Bundes, eines anderen Kantons oder einem anderen öffentlichen Organ bekannt, wenn die Personendaten für die Empfängerin oder den Empfänger zur Erfüllung einer ihr oder ihm übertragenen gesetzlichen Aufgabe unentbehrlich sind.

*Besondere Fälle a) Bekanntgabe für gemeinnützige und schutzwürdige ideelle Zwecke*

Art. 14. Das öffentliche Organ gibt auf Anfrage Name, Vorname, Geburtsdatum, Adresse sowie Zuzug in den Kanton oder die Gemeinde und Wegzug aus dem Kanton oder der Gemeinde bekannt, wenn die Empfängerin oder der Empfänger Gewähr bietet und sich schriftlich verpflichtet, die Personendaten ausschliesslich für gemeinnützige oder schutzwürdige ideelle Zwecke zu verwenden und nicht weiterzugeben.

*b) Abrufverfahren*

Art. 15. Die Bekanntgabe von Personendaten im Abrufverfahren ist zulässig, wenn dieses in einer Rechtsgrundlage vorgesehen ist.

Die Bekanntgabe von besonders schützenswerten Personendaten im Abrufverfahren ist zulässig, wenn dieses im Gesetz vorgesehen ist.

*c) Bekanntgabe ins Ausland*

Art. 16. Die Bekanntgabe von Personendaten ins Ausland richtet sich sachgemäss nach den Bestimmungen der Bundesgesetzgebung über den Datenschutz.

Das öffentliche Organ informiert vor der Bekanntgabe die zuständige Fachstelle für Datenschutz über die von der Bundesgesetzgebung geforderten Garantien, wenn der Staat nicht auf der von der oder vom eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten veröffentlichten Liste der Staaten mit angemessener Datenschutzgesetzgebung aufgeführt ist.

Die kantonale Fachstelle für Datenschutz beschafft bei der oder beim eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten Informationen über den Datenschutz im Ausland. Sie stellt die Informationen zur Verfügung:

- a) den öffentlichen Organen in ihrem Zuständigkeitsbereich;
- b) den Fachstellen der Gemeinden zur Weiterleitung an die öffentlichen Organe in deren Zuständigkeitsbereich.

## **IV. Rechte der betroffenen Person**

*Auskunft und Einsicht a) Grundsatz*

Art. 17. Das öffentliche Organ erteilt der betroffenen Person auf Gesuch und gegen Ausweis über die Identität Auskunft, welche Personendaten über sie bearbeitet werden. Die Auskunft erfolgt in der Regel schriftlich.

Es gewährt auf Verlangen der betroffenen Person Einsicht in die Personendaten.

*b) Beschränkung*

*Art. 18.* Das öffentliche Organ lehnt Auskunft und Einsicht ab, schränkt sie ein oder verbindet sie mit Auflagen, soweit öffentliche Interessen oder schutzwürdige private Interessen überwiegen.

*c) Gebühr*

*Art. 19.* Die Behandlung des Gesuchs um Auskunft und Einsicht ist in der Regel unentgeltlich.

*Unrichtige und widerrechtlich bearbeitete Personendaten*

*Art. 20.* Die betroffene Person hat Anspruch darauf, dass das öffentliche Organ unrichtige Personendaten berichtigt. Kann weder Richtigkeit noch Unrichtigkeit bewiesen werden, bringt das öffentliche Organ bei den Personendaten einen entsprechenden Vermerk an.

Die betroffene Person hat Anspruch darauf, dass das öffentliche Organ:

- a) die widerrechtliche Bearbeitung von Personendaten unterlässt;
- b) widerrechtlich bearbeitete Personendaten vernichtet.

Das öffentliche Organ informiert Empfängerinnen und Empfänger von unrichtigen oder widerrechtlich bearbeiteten Personendaten über die getroffenen Massnahmen.

*Sperrung a) Grundsatz*

*Art. 21.* Das öffentliche Organ sperrt auf Gesuch die Bekanntgabe von Personendaten, wenn die betroffene Person ein schutzwürdiges Interesse hat.

*b) Bekanntgabe trotz Sperrung*

*Art. 22.* Das öffentliche Organ gibt Personendaten trotz Sperrung bekannt, wenn:

- a) eine Rechtspflicht zur Bekanntgabe besteht oder
- b) die Erfüllung einer gesetzlichen Aufgabe verunmöglicht würde oder
- c) die Empfängerin oder der Empfänger glaubhaft macht, dass die Sperrung rechtsmissbräuchlich erwirkt wurde.

*Verfügung des öffentlichen Organs*

*Art. 23.* Das öffentliche Organ erlässt eine Verfügung, wenn es ein zur Durchsetzung ihrer Rechte eingereichtes Gesuch der betroffenen Person abweist.

## **V. Fachstelle für Datenschutz**

### **1. Organisation**

*Fachstelle für Datenschutz in Kanton und Gemeinden*

*Art. 24.* Der Kanton setzt die kantonale Fachstelle für Datenschutz ein, die für die Staatsverwaltung und für die selbstständigen öffentlich-rechtlichen Anstalten tätig ist.

Die Gemeinde setzt die Gemeindefachstelle für Datenschutz ein, die für die Verwaltungsstellen der Gemeinde und die selbstständigen öffentlich-rechtlichen Gemeindeunternehmen tätig ist.

Sie kann durch Vereinbarung mit einer anderen Gemeinde deren Gemeindefachstelle für Datenschutz als für sie zuständig bezeichnen.

#### *Gemeinsame Fachstelle für Datenschutz für mehrere Gemeinden*

Art. 25. Die Gemeinde kann durch Vereinbarung mit anderen Gemeinden eine gemeinsame Gemeindefachstelle einsetzen. Die Vereinbarung bestimmt:

- a) die für die administrative Zuordnung zuständige Sitzgemeinde;
- b) den Schlüssel für die Finanzierung der Ausgaben der Gemeindefachstelle.

Die Regierung kann Gemeinden verpflichten, eine gemeinsame Gemeindefachstelle einzusetzen, wenn eine wirksame Aufgabenerfüllung und ein wirtschaftlicher Mitteleinsatz es verlangen. Sie legt die Sitzgemeinde und den Schlüssel für die Finanzierung der Ausgaben der Gemeindefachstelle fest, wenn sich die Gemeinden nicht einigen.

Für den Gemeindeverband oder den Zweckverband ist die Gemeindefachstelle der Mitgliedsgemeinde zuständig, in der sich der Verbandssitz befindet.

#### *Unabhängigkeit*

Art. 26. Die Fachstelle für Datenschutz erfüllt ihre Aufgaben unabhängig und selbstständig.

Sie ist administrativ zugeordnet:

- a) im Kanton dem von der Regierung durch Verordnung bezeichneten Departement oder der Staatskanzlei;
- b) in der Gemeinde dem Rat der Gemeinde oder der Sitzgemeinde.

#### *Aufsicht*

Art. 27. Die Aufsicht übt aus:

- a) die für die Aufsicht von Regierung und Staatsverwaltung zuständige Kommission des Kantonsrates über die kantonale Fachstelle für Datenschutz;
- b) die kantonale Fachstelle für Datenschutz über die Gemeindefachstelle für Datenschutz.

#### *Personal*

Art. 28. Die Regierung wählt die Leiterin oder den Leiter der kantonalen Fachstelle für Datenschutz.

Der Rat wählt die Leiterin oder den Leiter der Gemeindefachstelle für Datenschutz. Haben mehrere Gemeinden eine gemeinsame Gemeindefachstelle eingesetzt, wählt der Rat der Sitzgemeinde nach Anhörung der Räte der beteiligten Gemeinden.

Die Leiterin oder der Leiter der Fachstelle für Datenschutz stellt im Rahmen des Vorschlags die Mitarbeitenden an und erlässt die das Dienstverhältnis betreffenden Verfügungen.

Das Dienstverhältnis der Leiterin oder des Leiters sowie der Mitarbeitenden der kantonalen Fachstelle für Datenschutz richtet sich nach dem Staatsverwaltungsgesetz vom 16. Juni 1994.<sup>57</sup>

---

<sup>57</sup> sGS 140.1.

### *Voranschlag*

Art. 29. Die Fachstelle für Datenschutz erstellt ihren Abschnitt des Voranschlags selbstständig.

Die Regierung, in der Gemeinde der Rat, gibt im Voranschlagsentwurf zuhanden des Kantonsrates, in Gemeinden zu Handen des Gemeindeparlamentes oder der Bürgerversammlung, bekannt, ob der von der Fachstelle für Datenschutz erstellte Voranschlag unverändert übernommen wurde. Abweichungen werden begründet.

## **2. Zuständigkeit**

### *Aufgaben*

Art. 30. Die Fachstelle für Datenschutz:

- a) überprüft auf Anzeige betroffener Personen und nach dem von ihr aufgestellten Prüfprogramm die Einhaltung der Bestimmungen über den Datenschutz. Kantonsrat und Regierung sowie Gemeindeparlament und Rat sind von der Aufsicht ausgenommen;
- b) berät öffentliche Organe und betroffene Personen in Fragen des Datenschutzes;
- c) kann der Regierung, in Gemeinden dem Rat, den Erlass von Weisungen über technische und organisatorische Massnahmen zur Gewährleistung des Datenschutzes beantragen;
- d) nimmt Stellung zum Entwurf von Erlassen, die:
  1. Bestimmungen über den Datenschutz enthalten;
  2. datenschutzerhebliche Sachverhalte regeln;
- e) wirkt in Projekten mit, die den Datenschutz betreffen oder Bezüge zum Datenschutz aufweisen.

Die kantonale Fachstelle für Datenschutz berät die Gemeindefachstellen für Datenschutz.

### *Einsicht in Daten*

Art. 31. Die Fachstelle für Datenschutz ist berechtigt, die für die Erfüllung ihrer Aufgaben unentbehrlichen Daten einschliesslich besonders geschützter Personendaten aus den Datensammlungen des öffentlichen Organs einzusehen.

### *Unterstützung durch Dienststellen*

Art. 32. Das öffentliche Organ unterstützt die Fachstelle für Datenschutz bei der Erfüllung ihrer Aufgaben, indem es auf deren Verlangen insbesondere:

- a) Auskünfte erteilt;
- b) Unterlagen vorlegt und Einsicht in Unterlagen gewährt;
- c) das Vorgehen bei der Bearbeitung von Personendaten erläutert;
- d) die Bearbeitung von Personendaten vorführt;
- e) Fachinformationen vermittelt.

Es ist vom Amtsgeheimnis entbunden.

### *Empfehlungen*

Art. 33. Die Fachstelle für Datenschutz gibt Empfehlungen ab und unterbreitet diese dem öffentlichen Organ zur schriftlichen Stellungnahme:

- a) wenn sie Mängel bei der Bearbeitung von Personendaten feststellt;
- b) bei beabsichtigter Bearbeitung von Personendaten mit besonderen Risiken für den Grundrechtsschutz.

### *Massnahmen a) im Kanton*

*Art. 34.* Die kantonale Fachstelle für Datenschutz kann beim zuständigen Departement oder bei der Staatskanzlei die Anordnung von Massnahmen beantragen, wenn das öffentliche Organ die Empfehlungen nicht oder nur teilweise umsetzen will oder innert angesetzter Frist keine Stellungnahme abgibt. Handelt das zuständige Departement, die Staatskanzlei oder eine selbstständige öffentlich-rechtliche Anstalt des Kantons als öffentliches Organ, ist der Antrag an die Regierung zu richten.

Das zuständige Departement, die Staatskanzlei oder die Regierung verfügt Massnahmen, ausgenommen in Fällen, in denen das öffentliche Organ eine Verfügung gegenüber der betroffenen Person erlässt.

Der Rechtsschutz richtet sich nach der Gesetzgebung über die Verwaltungsrechtspflege. Die kantonale Fachstelle für Datenschutz ist beschwerdeberechtigt.

### *b) in der Gemeinde*

*Art. 35.* Die Gemeindefachstelle für Datenschutz kann beim Rat die Anordnung von Massnahmen beantragen, wenn das öffentliche Organ die Empfehlungen nicht oder nur teilweise umsetzen will oder innert angesetzter Frist keine Stellungnahme abgibt. Handelt der Rat, ein Gemeinde- oder Zweckverband oder ein selbstständiges öffentlich-rechtliches Gemeindeunternehmen als öffentliches Organ, ist der Antrag an das zuständige Departement zu richten.

Der Rat oder das zuständige Departement verfügt Massnahmen, ausgenommen in Fällen, in denen das öffentliche Organ eine Verfügung gegenüber der betroffenen Person erlässt.

Der Rechtsschutz richtet sich nach der Gesetzgebung über die Verwaltungsrechtspflege. Die Gemeindefachstelle für Datenschutz ist rekurs- und beschwerdeberechtigt.

### *Berichterstattung*

*Art. 36.* Die Fachstelle für Datenschutz erstattet der Regierung, in Gemeinden dem Rat oder bei der gemeinsam eingesetzten Gemeindefachstelle den beteiligten Räten, jährlich Bericht über:

- a) die Anwendung des Datenschutzrechts und die Einhaltung des Datenschutzes;
- b) Umfang und Schwerpunkte der Prüftätigkeit;
- c) Feststellungen und deren Beurteilung.

Die Fachstelle kann in Fällen von allgemeinem Interesse die Öffentlichkeit über ihre Feststellungen informieren. Ausgenommen ist die Veröffentlichung von Personendaten, die dem Amtsgeheimnis unterstehen.

Die kantonale Fachstelle für Datenschutz berichtet dem Kantonsrat jährlich über ihre Tätigkeit. Der Kantonsrat nimmt vom Bericht Kenntnis.

## **VI. Register über Datensammlungen**

### *Führung*

*Art. 37.* Die Fachstelle für Datenschutz führt das Register über die in ihrem Zuständigkeitsbereich vorhandenen Datensammlungen.

Für die Führung des Registers über Datensammlungen bei Privaten, die Staatsaufgaben erfüllen, ist zuständig:

- a) die kantonale Fachstelle für Datenschutz bei Erfüllung von kantonalen Aufgaben;
- b) die Gemeindefachstelle für Datenschutz bei Erfüllung von Gemeindeaufgaben.

#### *Inhalt*

Art. 38. Das Register informiert insbesondere über:

- a) Rechtsgrundlage und Zweck;
- b) Mittel der Bearbeitung;
- c) Art und Herkunft der Personendaten;
- d) Dritte, die Daten eingeben und verändern dürfen;
- e) regelmässige Empfängerinnen und Empfänger.

Das Register über Datensammlungen ist periodisch, mindestens jedoch jährlich zu aktualisieren.

Es ist öffentlich.

#### *Meldung von Änderungen*

Art. 39. Das öffentliche Organ meldet der zuständigen Fachstelle für Datenschutz Änderungen:

- a) im Bestand der von ihm geführten Datensammlungen;
- b) von für den Inhalt des Registers massgeblichen Sachverhalten.

Es meldet:

1. neue Datensammlungen vor deren Eröffnung;
2. übrige Änderungen jährlich auf Beginn des nächsten Kalenderjahres.

## **VII. Schlussbestimmungen**

#### *Strafbestimmung*

Art. 40. Wer Personendaten im Auftrag des öffentlichen Organs bearbeitet und sich dabei vorsätzlich auftragswidrig verhält, wird auf Antrag mit Busse bestraft.

#### *Änderung bisherigen Rechts a) Staatsverwaltungsgesetz*

Art. 41. Das Staatsverwaltungsgesetz vom 16. Juni 1994<sup>58</sup> wird wie folgt geändert:

*Art. 8 bis 11 werden aufgehoben.*

#### *Aufsichtsbereich*

Art. 42b. Der Finanzaufsicht durch die Finanzkontrolle unterliegen vorbehältlich besonderer gesetzlicher Vorschriften:

- a) der Kantonsrat;
- b) die Staatsverwaltung;
- b<sup>bis</sup>) **die kantonale Fachstelle für Datenschutz;**
- c) die Gerichte und andere Justizbehörden;
- d) die selbstständigen öffentlich-rechtlichen Anstalten des Kantons.

---

<sup>58</sup> sGS 140.1.

Die Finanzkontrolle übt die Finanzaufsicht auch dort aus, wo nach Gesetz oder Statuten eine eigene Revisionsstelle beauftragt ist. Sie stimmt ihre Tätigkeit mit anderen Organen ab, die Prüfungsaufgaben wahrnehmen.

Die Finanzkontrolle kann bei Organisationen und Personen, die Staatsbeiträge empfangen oder denen Staatsaufgaben übertragen sind, in Absprache mit dem zuständigen Departement Prüfungen durchführen.

*Art. 95 Bst. d wird aufgehoben.*

*b) Gemeindegesetz*

*Art. 42.* Das Gemeindegesetz vom 23. August 1979<sup>59</sup> wird wie folgt geändert:

*Art. 9bis wird aufgehoben.*

*c) Sozialhilfegesetz*

*Art. 43.* Das Sozialhilfegesetz vom 27. September 1998<sup>60</sup> wird wie folgt geändert:

**Amtshilfe**

**Art. 6bis (neu).** Die Verwaltungs- und Rechtspflegebehörden von Kanton und Gemeinden geben den mit dem Vollzug dieses Gesetzes betrauten Organen auf schriftliche und begründete Anfrage im Einzelfall kostenlos Daten bekannt, die erforderlich sind für:

- a) Festsetzung, Änderung oder Rückforderung von Sozialhilfeleistungen;**
- b) Verhinderung ungerechtfertigter Bezüge von Sozialhilfeleistungen.**

**Sie sind berechtigt, den Organen der Sozialhilfe Wahrnehmungen mitzuteilen, die auf einen unberechtigten Bezug von Sozialhilfeleistungen schliessen lassen.**

*d) Polizeigesetz*

*Art. 44.* Das Polizeigesetz vom 10. April 1980<sup>61</sup> wird wie folgt geändert:

*Art. 37 und Art. 39 Bst. c werden aufgehoben.*

*e) Gesetz über die Niederlassung der Schweizer*

*Art. 45.* Das Gesetz über die Niederlassung der Schweizer vom 5. April 1979<sup>62</sup> wird wie folgt geändert:

*Art. 13 wird aufgehoben.*

---

<sup>59</sup> sGS 151.2.

<sup>60</sup> sGS 381.1.

<sup>61</sup> sGS 451.1.

<sup>62</sup> sGS 453.1.

*Randtitel*

**Art. 16. Die Regierung** erlässt die zum Vollzug dieses Gesetzes erforderlichen Vorschriften, insbesondere über:

- a) die Registerführung;
- b) die Erhebung von Daten \_\_\_\_.

*g) Gerichtsgesetz*

**Art. 46.** Das Gerichtsgesetz vom 2. April 1987<sup>63</sup> wird wie folgt geändert:

*Andere Gesetze*

**Art. 2.** Die Zuständigkeit der Gerichte, die Verfahrensarten und ergänzende Vorschriften zu diesem Erlass sind Gegenstand des Bundesgesetzes über den Gerichtsstand in Zivilsachen vom 24. März 2000 sowie der Gesetzgebung über die Zivil-, die Straf- und die Verwaltungsrechtspflege.

Organisation, Zuständigkeit und Verfahren der Untersuchungs- und Anklagebehörden richten sich nach der Gesetzgebung über die Strafrechtspflege.

**Das Datenschutzgesetz vom ●● wird sachgemäss angewendet auf:**

- a) rechtskräftig abgeschlossene Verfahren der Zivil-, Straf- und Verwaltungsrechtspflege;**
- b) die Justizverwaltung;**
- c) die Aufsicht über die Gerichte.**

*Vollzugsbeginn*

**Art. 47.** Die Regierung bestimmt den Vollzugsbeginn dieses Erlasses.

---

63 sGS 941.1.