

## § 9 Gesetz über den Schutz von Personendaten

(Datenschutzgesetz)

### 1. Grundlagen

#### 1.1. Memorialsantrag auf Erlass eines Gesetzes über den Datenschutz

Vor dem Hintergrund und anbetrachts der Möglichkeiten der elektronischen Datenverarbeitung reichte die Freisinnig-Demokratische Partei des Kantons Glarus im August 1984 einen Memorialsantrag zuhanden der Landsgemeinde 1987 auf Erlass eines Gesetzes über den Datenschutz ein, das für den öffentlichen Bereich des Kantons Glarus gelten sollte. Die Landsgemeinde stimmte dem Memorialsantrag 1985 zu. Die anschließende Vernehmlassung zu einem vom Regierungsrat erstellten Entwurf förderte ein kontroverses Bild über die in Aussicht genommenen Vorschriften zu Tage. Dieses Ergebnis und dasjenige der Vernehmlassung des Bundes zu einem Bundesgesetz über den Datenschutz sowie die Wünschbarkeit einer Harmonisierung der kantonalen Regelungen führte zu einem Verschiebungsantrag; vor allem sei der Erlass eines eidgenössischen Datenschutzgesetzes abzuwarten. Die Landsgemeinde 1987 stimmte dem Verschiebungsantrag zu.

#### 1.2. Rechtsvergleichender Ueberblick

Die Kantonsverfassung (KV) von 1988 gewährt jedermann Schutz vor Missbrauch der ihn betreffenden Daten als Teilgehalt des Grundrechts auf persönliche Freiheit (Art. 5 Abs. 1 KV).

Am 1. Juli 1993 trat das Bundesgesetz über den Datenschutz (DSG) in Kraft, das vor allem für die Organe des Bundes sowie die privaten Personen gilt. Auf die Behörden des Kantons und der Gemeinden ist das Bundesgesetz nur anwendbar, soweit diese Bundesrecht vollziehen und der Kanton keine eigenen Datenschutzvorschriften kennt (Art. 37 Abs. 1 DSG). Seit dem Inkrafttreten des Bundesgesetzes erliessen die meisten Kantone Vorschriften über den Datenschutz. Eigentliche Datenschutzgesetze kennen 20 Kantone, vier stützen sich auf Datenschutzrichtlinien bzw. Weisungen oder fragmentarische Datenschutzbestimmungen in Gesetzen über die Staats- und Verwaltungsorganisation ab und ein Kanton schuf ein Gesetz über das Oeffentlichkeitsprinzip und den Datenschutz. Nur noch zwei Kantone (NW und GL) verfügen über keine materiellen eigenen Datenschutzbestimmungen, so dass für sie – zumindest beim Vollzug von Bundesrecht – Artikel 37 DSG subsidiär zum Tragen kommt.

Momentan ist eine Teilrevision des Bundesgesetzes über den Datenschutz in Vorbereitung. Angesichts der grossen Unsicherheit über den Fortgang dieser Teilrevision wurde auf eine Berücksichtigung der darin enthaltenen Vorschläge verzichtet.

### 2. Zur Vorlage des Regierungsrates

#### 2.1. Rechtliche Grundlagen

Das Erheben, Aufbewahren und Bearbeiten von Personendaten stellt nach bundesgerichtlicher Rechtssprechung einen Eingriff in das Verfassungsrecht der persönlichen Freiheit dar und berührt somit den Schutzbereich von Artikel 8 Ziffer 1 der Europäischen Menschenrechtskonvention. Der Datenschutz ist zudem sowohl kraft Bundesverfassung (Art. 13 Abs. 2 BV) wie auch kraft Kantonsverfassung als Grundrechtsanspruch ausgestaltet. Damit die Bearbeitung von Personendaten als verfassungsmässig erkannt werden kann, bedarf es unter anderem einer entsprechenden Rechtsgrundlage, die den Eingriff demokratisch legitimiert.

Die kantonalen Vorschriften müssen zudem einem Mindeststandard genügen, ansonsten das eidgenössische Datenschutzgesetz als subsidiäres Recht direkt zur Anwendung kommt. Der kantonale Gesetzgeber hat sich deshalb an den Grundsätzen des Bundesgesetzes zu orientieren, um nicht der Gefahr drohender Rechtsunsicherheit infolge Kollision von kantonalem und eidgenössischem Recht Vorschub zu leisten.

#### 2.2. Notwendigkeit einer Regelung

Die staatlichen Organe sind für die Wahrnehmung der ihnen übertragenen hoheitlichen Aufgaben oft auf Sammlungen von Personendaten angewiesen. Die nach wie vor rasch fortschreitende Entwicklung im Bereich der Informatik und der Vernetzung (inner- und ausserhalb der öffentlichen Verwaltung) eröffnet neue Möglichkeiten der Datensammlung und Bearbeitung. Das Sammeln und Bearbeiten dieser Informationen steht in einem erheblichen Spannungsverhältnis zur Privatsphäre der betroffenen Personen. Diesen fehlt in der Regel die Uebersicht, welche Daten der Staat über sie besitzt und welchen Gebrauch er davon macht, ob er diese beispielsweise Dritten gegen Entgelt zur Verfügung stellt. Die Zunahme der öffentlichen Aufgaben und der damit verbundene Einsatz moderner Informationstechnologien verlangen, dass die

Datenverarbeitung der öffentlichen Hand rechtlich geordnet wird, womit dem Grundrecht auf Schutz vor Missbrauch von Personendaten Nachachtung verschafft wird. Insbesondere darf jedermann bei der Bearbeitung seiner Daten Schutz vor unzulässigen und unnötigen Eingriffen erwarten. Im Umfeld der elektronischen Verwaltung wird das Vertrauen in die öffentlichen Organe nur dann gewährleistet werden können, wenn für den Einzelnen transparent ist, was mit seinen Daten geschieht, und wie von Staats wegen sichergestellt wird, dass seine Daten nicht anderen Zwecken als den von Rechts wegen bestimmten zugeführt werden. Darüber hinaus wird die Akzeptanz, dem Staat persönliche Daten zur Verfügung zu stellen, durch den Schutz der Integrität der Daten gestärkt. Die Schweiz kommt zudem zunehmend aufgrund von EU-Recht unter Druck, weil das Fehlen von Datenschutzgesetzen in einigen Kantonen kritisiert wird.

Das vorliegende Datenschutzgesetz ermöglicht eine moderne, wirksame und praktikable Regelung des Datenschutzes im Kanton Glarus. Es lehnt sich an das DSG an, wird aber auch den Besonderheiten und Bedürfnissen des Kantons gerecht. Es beschränkt sich materiell auf die wesentlichen Grundzüge und regelt einlässlich die Aufsicht über die Einhaltung des Datenschutzes in Nachachtung des übergeordneten Rechts (Art. 37 Abs. 2 DSG). Weiter schafft es Rechtssicherheit und erfüllt die Anforderungen von Artikel 8 der Europäischen Menschenrechtskonvention sowie weiterem internationalem Recht.

Anlässlich der Vorarbeiten für ein nicht mehr weiter verfolgtes Staatsverwaltungsgesetz wurde der Wechsel vom Prinzip des Amtsgeheimnisses zum Öffentlichkeitsprinzip mit Geheimnisvorbehalt (wie es die Kantone Bern und Solothurn kennen; der Bund prüft dessen Einführung) verworfen. Dieser Grundsatzentscheid für die Beibehaltung der Vertraulichkeit der Verwaltung liegt dem Datenschutzgesetz zugrunde und es wurde auf einen Systemwechsel betreffend des Zugangs zu Informationen der öffentlichen Hand verzichtet.

### 2.3. Erlassstufe

Der Schutz vor einem Missbrauch persönlicher Daten stellt ein Grundrecht dar. Einschränkungen von Grundrechten dürfen nur im Rahmen der Verfassung und aufgrund eines Gesetzes erfolgen. Vorbehalten werden einzig Fälle ernster, unmittelbarer und offensichtlicher Gefahr. Eingriffe in Grundrechte dürfen nicht weiter gehen, als es ein zulässiger Zweck und ein überwiegendes öffentliches Interesse erfordern (Art. 2 Abs. 3 und 4 KV). Die wesentlichen Grundsätze und Leitlinien für die Bearbeitung von Personendaten seitens des Staates sind deshalb in einem Gesetz im formellen Sinne zu regeln. Dies hat zumindest für solche Eingriffe in Personendaten zu gelten, die als schwerwiegend zu erachten sind.

### 2.4. Vernehmlassung

Der Regierungsrat unterzog den Vorentwurf einem Vernehmlassungsverfahren. Zudem waren die Erkenntnisse aus der Vernehmlassung zum Staatsverwaltungsgesetz, welches ebenfalls eine kantonale Regelung des Datenschutzes enthielt, in den Entwurf eingeflossen. Das Spektrum der 35 eingegangenen Vernehmlassungen erwies sich als breit und reichte von vorbehaltloser Unterstützung seitens einer grossen Zahl von Vernehmlassenden bis zu einem Antrag auf Rückweisung. Einzelne Einschätzungen und Aenderungsbegehren liefen sich – je nach politischem Standpunkt und Interessenlage – diametral entgegen. Einzelne verlangten die ausdrückliche zusätzliche Regelung spezieller Sachverhalte, während andere einen noch kürzeren Erlass wünschten. Einige Gemeindevorsteherschaften stellten zutreffend fest, dass es sich bei dieser Vorlage um eine komplexe und abstrakte Angelegenheit handle. Diesem Umstand wird nach der Verabschiedung des Gesetzes insoweit Rechnung zu tragen sein, als für die Anwender vor dem Inkrafttreten des Datenschutzgesetzes Einführungs- und Instruktionsveranstaltungen organisiert werden sollen sowie allenfalls ein Leitfaden zur Verfügung zu stellen ist.

### 2.5. Finanzielle Auswirkungen

Die Anwendung des Datenschutzgesetzes wird Mehraufwendungen bringen. Die finanziellen Auswirkungen abzuschätzen ist ausserordentlich schwierig, weil die Schutzmassnahmen jeweils aufgrund laufender Analyse angepasst werden müssen und sich die Verhältnisse bei den Gemeinden in Bezug auf den Standard der Informatisierung erheblich unterscheiden. Die Kosten werden auch durch die noch zu erlassenden Ausführungsvorschriften beeinflusst.

Die Funktion der kantonalen Aufsichtsstelle ist wie bisher durch einen Datenschutzbeauftragten, der aus dem Mitarbeiterstab der Regierungskanzlei rekrutiert wird, zu versehen, so dass an sich mit keinen zusätzlichen direkten Personal- und Infrastrukturkosten zu rechnen ist. Immerhin wird sich die zusätzliche Arbeit auf die Möglichkeit der Erledigung anderer Aufgaben auswirken. Der zeitliche Aufwand des kantonalen Datenschutzbeauftragten dürfte etwa einem Stellenpensum von 15 bis 20 Prozent entsprechen (ohne Aufbau des zentralen Registers).

### 3. Erläuterungen zum Entwurf

#### 3.1. Einleitende Bestimmungen (Art. 1–3)

##### *Artikel 1; Zweck*

Datenschutz dient dem Schutz der Persönlichkeitsrechte des Bürgers, den die Kantonsverfassung als grundrechtlichen Anspruch garantiert. Dabei wird nicht eine Verhinderung jeglicher Bearbeitung von Personendaten bezweckt, sondern die Bekämpfung des Missbrauchs. Ein Missbrauch von Personendaten liegt namentlich dann vor, wenn deren Bearbeitung den Bestimmungen des Datenschutzgesetzes widerspricht. Der einleitende Zweckartikel soll als Auslegungshilfe bei der Rechtsanwendung im Einzelfall dienen.

##### *Artikel 2; Geltungsbereich*

Schwergewichtig betrifft das Datenschutzgesetz die *Kantonale Verwaltung* (inkl. die regierungsrätlich bestellten Kommissionen im Sinne von Art. 104 Abs. 2 KV) sowie die Exekutive als oberste vollziehende Behörde des Kantons. Keine Anwendung finden die Vorschriften des Datenschutzgesetzes jedoch dann, wenn Personendaten vom Regierungsrat anlässlich eines Rechtsmittelverfahrens bearbeitet werden. Hingegen gelten die Vorschriften für das nichtstreitige Verfahren, werden doch vor allem von den sachlich zuständigen Amtsstellen erster Instanz (häufig relativ formlos) Daten gesammelt und verwaltet, so dass dort Bedarf nach lenkenden Vorschriften besteht.

Für die *Gerichte und Rekurskommissionen* (z.B. die Landesschatzungskommission) sowie die übrigen *staatlichen Justizbehörden* (Vermittler, Schlichtungsstellen, Jugendamt und Jugendanwalt, Verhörrichter, Staatsanwalt usw.) gilt das kantonale Datenschutzrecht ebenfalls, insbesondere im Bereich der Justizverwaltung. Das Datenschutzgesetz wird jedoch auf die hängigen Zivilprozesse und Strafverfahren nicht angewendet, weil die entsprechenden Verfahrensgesetze Bestimmungen enthalten, welche ebenfalls die Persönlichkeitsrechte der in ein staatliches Verfahren einbezogenen Personen zu schützen bezwecken. Dies gilt vor allem für Bestimmungen über die Anhörungs-, Akteneinsichts- und Mitwirkungsrechte. Prozessrecht stellt so gesehen auch Datenschutzrecht dar. Die Ausklammerung hängiger Strafverfahren umfasst auch die *polizeilichen Untersuchungen* innerhalb von Ermittlungsverfahren. Die Polizei ist bei der Sicherung von Spuren und der Ermittlung darauf angewiesen, möglichst rasch und unkompliziert zu sachdienlichen Informationen zu kommen (Art. 2 Abs. 2 Bst. c). Für die übrigen Bereiche der Polizeiarbeit (z. B. Präventivmittlung [= Datenbearbeitung im Vorfeld einer konkreten Gefahr], Erkennungsdienst, Erstellen von Erhebungsberichten usw.) untersteht das Polizeikorps jedoch grundsätzlich dem Gesetz. Sollen also beispielsweise anlässlich der Verfolgung einer Straftat erhobene Daten nach Abschluss des Verfahrens zum Zwecke künftiger Gefahrenabwehr oder Strafverfolgung gespeichert oder sonstwie verarbeitet werden, so ist das Datenschutzgesetz zumindest als subsidiäres Recht zu beachten.

Ebenfalls unterstellt sind dem Grundsatz nach die *kantonalen öffentlich-rechtlichen Anstalten und Körperschaften*. Damit wird das Datenschutzgesetz für die beiden Landeskirchen oder für das Kantonsspital gelten. Die Grundrechte und damit der Schutz vor Missbrauch von Personendaten stellen wichtige Grundsätze der staatlichen Ordnung dar, an die sich auch die Kirchen als vom Kanton anerkannte Körperschaften (mit daraus resultierender besonderer Rechtsstellung) halten sollen, namentlich, wenn sie vom Staat Informationen über Personen zu kirchlichen Zwecken einholen und verwenden wollen. Von Verfassungen wegen ausgeschlossen ist lediglich eine staatliche Einflussnahme in den Bereich der *inneren Angelegenheiten der Kirchen* (vgl. den Vorbehalt in Art. 2 Abs. 2 Bst. e) worunter unter anderem die Verkündung des Wortes Gottes, die Seelsorge oder das Spenden der Sakramente zu zählen sind.

Sinnvollerweise werden auch die *Gemeinden* mit einbezogen; gerade auf kommunaler Ebene werden etwa im Schul- und Fürsorgebereich viele und teils recht heikle Informationen über Personen verarbeitet. Infolge der Quantität der auf Stufe Gemeinde gesammelten Daten sowie des von denselben bereits früher geäußerten Wunsches nach einer einzigen Aufsichtsstelle im Kanton, drängt sich deren Unterstellung auf.

Ebenfalls dem Datenschutzgesetz unterstellt werden *private Personen und Organisationen*, soweit sie *öffentliche Aufgaben erfüllen*, die ihnen gesetzlich oder durch öffentlich-rechtlichen Vertrag (z. B. anlässlich einer Auslagerung [Outsourcing] zwecks Bereitstellung spezifischer Dienstleistungen oder Produkte für die öffentliche Hand) übertragen worden sind. Gerade dieser Anwendungsfall zeigt, dass es für den Geltungsbereich vor allem auf die Art der Tätigkeit und nicht auf die Organisationsform ankommt.

In Artikel 2 Absatz 2 werden jene Fälle geregelt, bei denen das Gesetz keine Anwendung findet. So gilt das Datenschutzgesetz namentlich für die *Glarner Kantonalbank* nicht (obwohl sie eine kantonale öffentlich-rechtliche Anstalt ist), weil sie am wirtschaftlichen Wettbewerb teilnimmt, dabei nicht hoheitlich auftritt und ihr jegliche Verfügungskompetenz abgeht. Hinsichtlich der *Kantonalen Sachversicherung* ist zu differenzieren: Wo diese im Rahmen des kantonalen Monopols als Gebäudeversicherer oder beispielsweise als «Fachstelle für Brandschutz und Feuerwehr» auftritt, untersteht sie dem Datenschutzgesetz. Wo sie jedoch mit privaten Versicherungsgesellschaften in Konkurrenz tritt, gelangt nicht das kantonale, sondern das Bundesgesetz über den Datenschutz zur Anwendung.

Aus rechtspolitischen Gründen unterstehen *Landrat* und landrätliche Kommissionen den Bestimmungen des Datenschutzgesetzes nicht. Hätte der Landrat (insbesondere die Geschäftsprüfungskommission) das Datenschutzgesetz zu beachten (namentlich die Beschränkungen bei der Weitergabe von Personendaten), so könnte er seine Pflicht zur Wahrnehmung der Oberaufsicht über Regierungsrat, Verwaltung und Gerichte (Art. 82 Abs. 2 KV) kaum oder nur unter erschwerten Bedingungen erfüllen. Ausserdem sind die Beratungen des Landrates in aller Regel öffentlich (Art. 85 Abs. 2 KV).

Sobald Personendaten an das Landesarchiv oder andere Archive der öffentlichen Hand (vor allem der Gemeinden) übergegangen sind, werden ausschliesslich die Bestimmungen über die *Archivierung* angewendet. Dabei wirkt sich der Datenschutz insoweit aus, als die archivierten Personendaten nicht mehr verändert werden dürfen und die Urheberin und abliefernde Stelle die Daten weiterhin unbeschränkt einsehen und vom Archiv wieder herausverlangen darf.

### *Artikel 3; Begriffe*

Den Schutz des Gesetzes geniessen nicht alle vom Staat bearbeiteten Informationen, sondern lediglich die Personendaten. Als solche gelten alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, und zwar ungeachtet, ob es sich um eine Tatsachenfeststellung oder ein Werturteil handelt und ob die Personendaten mit Hilfe der Informatik oder manuell bearbeitet werden. Unerheblich ist auch, ob eine Aussage als Zeichen (z. B. digital, numerisch), Wort, Bild, Ton oder Kombinationen aus diesen besteht und auf welcher Art Datenträger die Information (Papier, Film, Festplatte) gespeichert ist. Den Datenschutzbegriffen sind grundsätzlich nur Daten unterstellt, die sich auf eine bestimmte oder bestimmbare Person beziehen, wohingegen rein sachbezogene Daten ihnen nicht unterliegen. Sachdaten sind jedoch immer dann auch Personendaten, wenn sie mit einer Person in Verbindung gebracht werden können: Da jedes Grundstück einen Eigentümer und jedes immatrikulierte Auto einen Halter hat, sind Informationen über Grundstücke und Autos zwangsläufig ebenfalls Personendaten. Der Begriff «Personendaten» erweist sich somit als sehr weit.

Unter den Personendaten gibt es neben eher unsensiblen Angaben (z. B. Name, Adresse) auch heikle Daten, deren Verwendung zu einer schwerwiegenden Beeinträchtigung der Persönlichkeit führen kann, und die deshalb als besonders schützenswert erscheinen. Vor allem die Polizei- und Strafverfolgungsbehörden oder die Behörden des Gesundheits- und Vormundschaftswesens bearbeiten häufig solche Personendaten. Hinsichtlich der religiösen Anschauung gehen Bundesgesetzgeber und etliche Kantone von einem besonders schützenswerten Personenidentifikator aus. Die praktische Bedeutung der Klassifizierung liegt in den strengeren Anforderungen, welche entsprechende Bearbeitungen erfüllen müssen (z. B. hinsichtlich der gesetzlichen Grundlage). Der Katalog von besonders schützenswerten Personendaten ist nicht abschliessend.

Unter den Begriff der Datensammlung fallen nicht nur Karteien und Sammlungen, die nach den betroffenen Personen gegliedert sind, sondern auch solche, die nach bestimmten Personen erschlossen werden können.

## **3.2. Bearbeiten von Personendaten (Art. 4–12)**

### *Artikel 4; Grundsätze*

Artikel 4 hält die das kantonale Datenschutzrecht überspannenden Leitlinien fest, an denen jede Bearbeitung von Personendaten zu messen ist. Die Bearbeitung von Informationen über Personen muss sich mindestens mittels Auslegung der Vorschriften über die wahrzunehmenden öffentlichen Aufgaben ableiten lassen. Umgekehrt ist nicht für jede Datensammlung eine formell-gesetzliche Rechtsgrundlage zu verlangen, will der Datenschutz nicht überdehnt und die von Verfassungen wegen verlangte Wirksamkeit und Wirtschaftlichkeit der Verwaltungstätigkeit nicht übermässig erschwert werden. Dem Gesetzmässigkeitsprinzip entsprechend darf eine Bearbeitung von Personendaten grundsätzlich nur dann erfolgen, wenn sie sich auf eine Rechtsgrundlage beziehen kann. In Absatz 1 werden die Voraussetzungen zur Bearbeitung umrissen.

Jede Bearbeitung verlangt grundsätzlich eine Rechtsgrundlage. In Ausnahmefällen genügt die Rückführung auf eine rechtlich klar definierte Staatsaufgabe, zu deren Verwirklichung die Bearbeitung unentbehrlich ist. Auch der Bundesgesetzgeber hat sich an denselben Begriff angelehnt. Je sensibler die bearbeiteten Personendaten sind, desto höhere Anforderungen sind an die Normstufe zu stellen. Im Weiteren genügt die Einwilligung der betroffenen Person, die freiwillig und nach gehöriger Aufklärung zu erfolgen hat.

In Konkretisierung des Verhältnismässigkeitsgrundsatzes wird in Absatz 2 festgehalten, dass der Staat nur ein Recht zur Beschaffung und Bewirtschaftung von Personendaten hat, soweit er sie für die Erfüllung der staatlichen Aufgaben benötigt und sie sich als dafür tauglich erweisen. In Absatz 1 geht es primär um das «Ob», in Absatz 2 dagegen um die Frage nach dem «Wie weit».

Der Staat soll ausschliesslich richtige Daten bearbeiten (Abs. 3) und damit dazu beitragen, dass Betroffenen aus der Bekanntgabe ihrer Daten an Dritte keine vermeidbaren Unannehmlichkeiten erwachsen. Einwohner wie Behörden haben gleichermassen ein Interesse an richtigen und vollständigen Daten.

#### *Artikel 5; Besonders schützenswerte Personendaten*

Wo ein grundrechtlicher Eingriff sehr intensiv ist, sind an die gesetzlichen Grundlagen erhöhte Anforderungen zu stellen. Für die Bearbeitung von *besonders schützenswerten Personendaten* bedarf es einer von der Landsgemeinde verabschiedeten Gesetzesvorschrift (Abs. 1).

Der Verfassungsgrundsatz von Treu und Glauben staatlichen Handelns verlangt, dass die von einer Datenbearbeitung betroffenen Personen wissen, wozu ihre Daten bearbeitet werden (Abs. 2). Der Bearbeitungszweck soll erkennbar sein. Personendaten werden dem Staat in der Regel nicht voraussetzungslos und freiwillig, sondern im Hinblick auf einen bestimmten Bearbeitungszweck geliefert. Das kann dazu führen, dass eine kantonale Amtsstelle oder eine Abteilung einer Gemeinde Personendaten selber erheben muss, obwohl eine andere Amtsstelle oder Abteilung bereits über die benötigten Daten verfügt (Grundsatz der informationellen Trennung innerhalb von Verwaltungseinheiten). Immerhin hat das gesetzliche Zweckbindungsgebot nur für die besonders schützenswerten Personendaten Geltung. Mit dieser Missbrauchsschranke soll das Vertrauensverhältnis zwischen Bürger und Behörden gestärkt werden. Als Korrektiv dieser im gesamtschweizerischen Vergleich recht grosszügigen und verwaltungsfreundlichen Regelung wird für die Bekanntgabe von Personendaten im Abrufverfahren (Online), bei der eine Vielzahl von Datenstämmen betroffen sein kann, eine rechtlichen Grundlage verlangt (s. dazu Art. 10).

#### *Artikel 6; Verantwortlichkeiten, Auslagerung*

Namentlich bei der automatisierten Datenverarbeitung verwenden öffentliche Organe aus praktischen Gründen Personendaten oft aus derselben Datensammlung (Datenbank). Die Hauptverantwortung für den Bestand der Daten und die Einhaltung des Datenschutzes liegt beim Inhaber der Datensammlung. Es können jedoch auch die Mitbenutzer für ihren Bereich zur Verantwortung gezogen werden. Bei gemeinsamer Nutzung von Datenbanken kann der hauptverantwortliche Inhaber der Datensammlung die Einhaltung der Datenschutzbestimmungen durch die Mitbenutzer kontrollieren (Abs. 1).

Wird die Bearbeitung von Personendaten an verwaltungsexterne Dritte ausgelagert, z. B. an ein Rechenzentrum oder einen Betreiber einer privaten Datenbank, hat die auslagernde Stelle mit flankierenden Massnahmen und Kontrollen sicherzustellen, dass die Daten nicht missbraucht werden. Infolge des erheblichen Missbrauchspotenzials ist der Grundsatzentscheid über eine Auslagerung im Gesetz zu verankern (Abs. 2 und 3).

#### *Artikel 7; Beschaffen von Personendaten*

Dieser Artikel verhindert, dass sich die staatlichen Stellen der Einfachheit halber die Daten bei einer anderen kantonalen oder kommunalen Stelle besorgen. Für die erstmalige Erhebung von Personendaten haben sie sich in der Regel an die betroffene Person zu halten, die bestimmen und erkennen können soll, ob, wem und zu welchem Zweck ihre Daten zugänglich gemacht werden. Damit wird zudem dem Gebot der Richtigkeit der Personendaten am ehesten Rechnung getragen (Abs. 1). Das Wissen, dass von der Einwohnerkontrolle erhobene Daten auch andern Verwaltungsstellen zugänglich gemacht bzw. bekannt gegeben werden, kann vorausgesetzt werden. Aus Gründen der Transparenz wird die Einwohnerkontrolle aber künftig gut daran tun, die Anmeldungspflichtigen (z. B. mittels einem vorbereiteten Formular) zu orientieren, welchen Zwecken die Personendaten zugeführt werden, und sich die Kenntnisnahme und Zustimmung unterschriftlich bestätigen zu lassen. Eine möglichst grosse Transparenz ist auch bei Umfragen oder ähnlichem (Fragebogen) zu gewährleisten (Abs. 2).

Die Betroffenen sollen aber nochmals angefragt werden, wenn besonders schützenswerte Daten zu einem völlig anderen als dem ursprünglichen Zweck bearbeitet werden wollen. Ist eine Beschaffung bei ihnen nicht möglich oder unverhältnismässig, so können unter Beachtung der Grundsätze von Artikel 4 ausnahmsweise verwaltungsinterne oder -externe Dritte angegangen werden (Abs. 3).

#### *Artikel 8; Datensicherheit*

Die Betreiber von Datenbanken werden angesichts des Missbrauchspotenzials bei der informatikgestützten Datenbearbeitung verpflichtet, durch baulich-technische und organisatorische Massnahmen unberechtigte Zugriffe zu unterbinden oder möglichst einzuschränken. Insbesondere in Bereichen, in denen besonders schützenswerte Personendaten über das Internet oder andere öffentliche Netze übermittelt werden, dürfte um eine Verschlüsselung nicht mehr herumzukommen sein. Solche Vorkehrungen werden als verhältnismässig

bezeichnet werden müssen. Auch dem Bereich des Virenschutzes und vergleichbaren Gefahren ist mit griffigen Massnahmen zu begegnen. Die Sicherheitsvorkehrungen sollen aber in einem angemessenen Verhältnis von Nutzen und Kosten stehen (Abs. 1).

Der Regierungsrat wird ermächtigt, flexibel und rasch, insbesondere bei Neuerungen, die nötigen Massnahmen und Mindestanforderungen vorzuschreiben (Abs. 2).

#### *Artikel 9; Allgemeine Einschränkung der Bekanntgabe von Personendaten*

Im Einzelfall kann aus öffentlichen (z. B. im strafrechtlichen Ermittlungsverfahren) oder schutzwürdigen privaten Interessen (z. B. Krankengeschichten des Kantonsspitals, Fürsorgeabhängigkeiten) die Bekanntgabe von Personendaten abgelehnt werden, wenn die Interessen des Nachfragers wenig schutzwürdig sind. Erscheint eine Verweigerung der Datenbekanntgabe als unverhältnismässig, kann sie unter Auflagen erteilt oder eingeschränkt gewährt werden (Abs. 1). Vorbehalten bleiben besondere Geheimhaltungsvorschriften, die als Spezialrecht den kantonalen Datenschutzbestimmungen vorgehen (Abs. 2).

Da der grenzüberschreitende Datenverkehr unter der Aegide des Bundes ausgehandelt zu werden pflegt und die diesbezüglichen Vorschriften erfahrungsgemäss periodisch den neuesten Staatsverträgen angepasst werden, ist es gerechtfertigt, die entsprechenden Bestimmungen des Bundesgesetzes über den Datenschutz (als eigenständiges kantonales Recht) für anwendbar zu erklären (Abs. 3).

#### *Artikel 10; Bekanntgabe von Personendaten*

Die Weitergabe von Personendaten ist ein besonders kritischer Teil des Bearbeitungsprozesses und bedarf deshalb einlässlicher Regelung. Detailliert wird in Artikel 10 festgelegt, unter welchen Voraussetzungen eine Bekanntgabe von Personendaten an Dritte (Behörden und Private) stattfinden darf. Selbst wenn die Bedingungen von Artikel 10 erfüllt sind, ist das angefragte öffentliche Organ trotzdem nicht verpflichtet, die Daten ohne Wenn und Aber bekannt zu geben. Es muss sich vielmehr vergewissern, ob auch die anderen Bestimmungen des Gesetzes (vor allem die allgemeinen Grundsätze) eingehalten sind und beispielsweise die Sicherheit der Datenübermittlung gewährleistet ist (Abs. 1 Bst. a).

Eine Bekanntgabe ist namentlich zulässig, wenn jemand (in aller Regel wird es ein öffentliches Organ sein) glaubhaft zu machen vermag, dass er ohne die Information eine gesetzliche Aufgabe nicht wahrnehmen kann (Abs. 1 Bst. b).

Verweigert eine Privatperson, einzig um einer Rechtspflicht zu entgehen (Alimentenzahlungen, Sozialversicherungsbeiträge, Schuldbetreibung usw.), die Bekanntgabe der sie betreffenden Daten, darf eine Bekanntgabe erfolgen. Die betroffene Person ist jedoch in der Regel zu informieren und ihr Gelegenheit zur Stellungnahme zu gewähren (rechtliches Gehör). Das angefragte öffentliche Organ sollte von dieser gesetzlich vorgesehenen Ausnahme bloss mit Zurückhaltung Gebrauch machen (Abs. 1 Bst. c).

Eine Bekanntgabe darf selbstverständlich gestützt auf eine ausdrückliche oder eine stillschweigende Einwilligung der Betroffenen erfolgen. Eine blindlings erteilte Globalemächtigung würde aber nicht genügen. Wenn die Bekanntgabe besonders schützenswerte Personendaten betrifft, ist eine ausdrückliche Einwilligung durch eine über ihre Rechte und die Zweckbestimmung der Daten aufgeklärte Person erforderlich. Von der nach den Umständen vorauszusetzenden Einwilligung ist mit Zurückhaltung Gebrauch zu machen. Nur wenn es sich als unmöglich oder schwierig erweist, die Einwilligung der betroffenen Person einzuholen, darf diese Spielart einer Einwilligung in Erwägung gezogen werden. Auf jeden Fall haben die Umstände erkennen zu lassen, dass die Person die Bekanntgabe gutgeheissen hätte, weil diese in ihrem offensichtlichen Interesse liegt (Abs. 1 Bst. d).

Wenn die betroffene Person selbst die sie betreffenden Daten allgemein zugänglich gemacht hat, namentlich durch deren Veröffentlichung in einem Buch oder in einer Zeitung, so ist die Bekanntgabe zulässig. Auch bereits im Amtsblatt publizierte Personendaten dürfen bekannt gegeben werden, weil sich die Veröffentlichung ja ebenfalls auf einen gesetzlichen Auftrag abstützte. Die entsprechende Information ist jedoch grundsätzlich bei dem öffentlichen Organ in Erfahrung zu bringen, das den Auftrag zur Publikation erteilt hat (Abs. 1 Bst. e).

Der Datenhunger privater Datennachfrager ist enorm. Zulässig ist die Bekanntgabe von Personendaten über die vorstehend genannten Fälle hinaus für ideelle und politische Zwecke. So kann einem Jahrgängerverein zwecks glaubhaft gemachter Organisation eines Klassentreffens eine Liste mit den ehemaligen Schulkameraden bekannt gegeben werden (Abs. 2). Der Bekanntgabe gleichgestellt ist die Meldung von Personendaten aufgrund gesetzlicher Verpflichtungen, wie sie in der kantonalen Zivilstandsverordnung zahlreich vorgesehen sind, unter anderem die Bestattungsbewilligung an die zuständigen Pfarrämter oder die Mitteilungen der Strafbehörden an die Fremdenpolizei über rechtskräftige Strafmandate und Strafurteile.

Sollen Personendaten in einem Abrufverfahren (Online-Zugriff, automatisiertes Verfahren) zugänglich gemacht werden, bedarf es dazu einer ausdrücklichen Vorschrift, welche dies gestattet. Dabei müssen mindestens das Abrufverfahren, zugriffsberechtigte Stellen sowie Umfang der abrufbaren Daten festgeschrieben sein. Handelt es sich um besonders schützenswerte Personendaten, muss eine formell-gesetzliche Regelung vorhanden sein (Abs. 3).

Wenig sensible Personendaten wie Name, Vorname, Adresse, Geburtsdatum und Heimatort dürfen in Übereinstimmung mit den Vorschriften für die Einwohnerkontrollen erleichtert bekannt gegeben werden. Diese Personendaten gelten als mehr oder weniger allgemein bekannt und ermöglichen primär die Identifikation von Personen. Es kann daraus aber nicht abgeleitet werden, dass es sich um freie Daten handelt. Auch der Name oder die Adresse kann im Zusammenhang mit besonders schützenswerten Personendaten (z. B. Angaben aus einer Datensammlung des Asyl- oder Polizeiwesens) zu einer unter Umständen heiklen Bekanntgabe führen (Abs. 4).

Grundsätzlich kann es nicht Aufgabe des Staates sein, Daten für die Privatwirtschaft bereit zu stellen. Die Bearbeitung von Personendaten hat sich auf die Erfüllung der hoheitlichen Aufgaben zu beschränken. Die öffentliche Hand kann aber ein legitimes fiskalisches Interesse haben, dass der grosse Aufwand, den die Erhebung von Daten zur Einrichtung von Datensammlungen mit sich bringt, verringert wird und die Kosten von privaten, nutznussenden Dritten mitgetragen werden. Zu denken ist beispielsweise an die Oeffnung einer eventuell für die kantonale Verwaltung einzuführenden Datenbank für Gebietsinformationen (GIS) gegen Entrichtung einer Gebühr. Immerhin soll aber das Stimmvolk, dessen Daten der Oeffentlichkeit preisgegeben werden, das letzte Wort haben (Abs. 5).

#### *Artikel 11; Datenbearbeitung für nicht personenbezogene Zwecke*

Die Bearbeitung von Personendaten für Zwecke der Statistik, Planung oder wissenschaftlichen Forschung genießt datenschutzrechtlich weitgehende Privilegien, weil die betroffene Person nicht als individuelle Persönlichkeit, sondern lediglich anonym, als statistische Einheit, fungiert. Das verantwortliche öffentliche Organ hat sich aber zu vergewissern, dass keine Vorschriften bestehen, die eine Bekanntgabe in diesen Fällen ausschliessen, und dass die für eine bestimmte Untersuchung nötigen Daten so weitergegeben werden, dass Rückschlüsse auf Personen möglichst erschwert sind (z. B. durch Unkenntlichmachen des Familiennamens und der Adresse, durch Anonymisieren oder Pseudonymisieren). Von praktischem Interesse ist in diesem Zusammenhang die Bearbeitung von Entscheiden und Urteilen der Rechtspflegeorgane zur Veröffentlichung in Entscheidungssammlungen (Abs. 1).

#### *Artikel 12; Vernichten und Archivieren*

Personendaten, soweit sie von den öffentlichen Organen für die ursprüngliche Zweckbestimmung oder zu Sicherungs- und Beweiszwecken nicht mehr benötigt werden, sind in ein Archiv (z. B. Landesarchiv, Gemeindearchive, Kirchenarchive) zu überführen oder dann zu vernichten (physische Vernichtung oder ≠Löschen elektronischer Daten unter gleichzeitiger Erstellung eines Vernichtungsprotokolls) oder zu anonymisieren. Auch rechtmässig beschaffte Daten dürfen nicht während beliebig langer Zeit bearbeitet werden. Es gibt einen Anspruch auf Vergessen; nach Verstreichen einer gewissen Zeitspanne sind die Daten aus dem öffentlichen Gedächtnis des Staates zu eliminieren. Auch praktische Ueberlegungen sprechen gegen ein Horten von ständig wachsenden und im Laufe der Zeit veraltenden Datenbeständen.

### **3.3. Rechte der betroffenen Personen (Art. 13–19)**

#### *Artikel 13; Register*

Die zu erstellenden Register haben in erster Linie der Oeffentlichkeit gegenüber transparent zu machen, wo überall der Staat Daten über sie speichert. Sie soll sich darüber informieren können, welche Daten zu welchem Zweck bearbeitet und wem sie zugänglich gemacht werden. Damit können Personen die ihnen zustehenden weiteren Rechte auf Auskunft, Berichtigung, Sperrung usw. geltend machen. Jedes dem Datenschutzgesetz unterstehende öffentliche Organ führt deshalb ein Register über alle von ihm angelegten Datensammlungen. Der dazu erforderliche Aufwand soll aber angesichts der Vielzahl verschiedenster Datensammlungen in Grenzen gehalten werden (Abs. 1).

Sollen die Register ihre zugeordnete Funktion erfüllen, braucht es eine Meldepflicht, damit die kantonale Aufsichtsbehörde ihr der Oeffentlichkeit zugängliches Zentralregister in einem aktuellen, ein einigermaßen getreues Abbild vermittelnden Zustand unterhalten kann. Im Weiteren dient das Register als Kontrollinstrument für die Aufsichtsstelle. Diese soll zur Gewährleistung einer gewissen Harmonisierung der Register im Einzelfall oder generell Weisungen über die Registerführung erteilen dürfen (Abs. 2).

#### *Artikel 14; Einsichts- und Auskunftsrecht*

Absatz 1 statuiert das Recht einer betroffenen Person, Auskunft über und Einsicht in ihre eigenen, sie betreffenden Daten und das zentral von der kantonalen Aufsichtsstelle zu führende öffentliche Register zu erhalten. Diese Rechte des Betroffenen stellen die bedeutendsten Instrumente des Datenschutzrechts dar. Beim Auskunftsrecht handelt es sich um ein höchstpersönliches Recht, auf das sich auch eine urteilsfähige unmündige Person berufen kann. Erst die ausdrückliche Erwähnung eines Anspruches auf Einsicht erlaubt Betroffenen die wirksame Durchsetzung der Abwehrrechte. Nur wenn sie erfahren, welche Daten über sie bearbeitet werden, können sie die ihnen zustehenden weiteren Rechte und Ansprüche (z. B. auf Berichtigung oder Unterlassung) wahrnehmen (Abs. 1).

Das öffentliche Organ erteilt grundsätzlich nur Auskunft über Personendaten, welche in einer von ihr geführten Datensammlung enthalten sind und die Gesuch stellende Person betreffen. Eine Drittperson kann die Auskunft nur bei gesetzlicher oder mittels Ermächtigung belegter Stellvertretung verlangen. Die Auskunftserteilung erfolgt mündlich oder schriftlich nach Ueberprüfung der Berechtigung der Gesuch stellenden Person. Mit der Verpflichtung, die Auskunft in allgemeinverständlicher Form zu erteilen, wird vermieden, dass die betroffene Person mit unverständlichen Fachausdrücken oder mit EDV-Codes abgespiesen wird (Abs. 2).

Die Einschränkung des Auskunfts- und Einsichtsrechts darf grundsätzlich nur aus gesetzlichen Gründen erfolgen. Vorbehalten bleiben übergesetzliche Schranken wie das Missbrauchsverbot. Eine Beschränkung des Rechts auf Einsichtnahme ist insbesondere zulässig, wenn bei umfangreichem Aktenbestand, der auch Personendaten Dritter enthält, die nicht einfach abgedeckt werden können, der Aufwand des öffentlichen Organs in keinem Verhältnis stünde zum Interesse der Gesuch stellenden Person. Ausserdem soll diese in solchen Fällen die voraussichtlich zu überbindenden Kosten (zumindest teilweise) bevorschussen müssen. Praktisch handelt es sich dabei um eine Missbrauchsschranke. Im Uebrigen sollen die Betroffenen ausnahmsweise mit einem schriftlichen Auszug vorlieb nehmen müssen (Abs. 3).

Es gibt Daten, namentlich im Bereich des Gesundheitswesens, die der betroffenen Person in ihrem eigenen Interesse besser nicht oder allenfalls bloss einer Person ihres Vertrauens (z. B. Hausarzt) erteilt werden (Abs. 4).

#### *Artikel 15; Recht auf Berichtigung*

Das Prinzip, wonach Personendaten richtig sein müssen, gilt als Grundanforderung für jede Bearbeitung von Personendaten. Das Datenschutzgesetz sieht deshalb einen selbstständigen Anspruch des oder der Betroffenen auf Berichtigung unrichtiger Personendaten vor. Die Richtigkeit von Personendaten ist zwar mit Rücksicht auf die vielfältigen Bearbeitungsvorgänge und Bearbeitungszwecke ein relativer Begriff. Einer betroffenen Person kann deshalb kein absoluter Anspruch auf Berichtigung eingeräumt werden. Insbesondere für den Fall der bestrittenen Richtigkeit von Personendaten obliegt die Beweislast primär dem öffentlichen Organ. Kann die Richtigkeit nicht erstellt werden, hat die betroffene Person Anspruch auf die Beifügung eines Vermerks über die Bestreitung. Gewisse Personendaten (z. B. Wertungen über eine bestimmte Person) können allerdings einer Beurteilung auf die Richtigkeit entzogen sein: Auch in solchen Fällen soll bei einer Bestreitung ein Vermerk oder eine kurze Darstellung aus Sicht der betroffenen Person angebracht werden. Einschränkungen des Rechts auf Berichtigung bestehen bei Gerichtsakten; sie haben nach Abschluss des Verfahrens die «prozessuale Wahrheit» wiederzugeben, was einer nachträglichen Abänderung entgegensteht.

#### *Artikel 16; Unterlassungs-, Beseitigungs- und Feststellungsansprüche*

Dieser Artikel garantiert der betroffenen Person weitere Abwehrrechte. Betroffene können sich gegen alle Arten widerrechtlicher oder unzulässiger Bearbeitung wehren. Widerrechtlich kann eine Bearbeitung von Personendaten dann sein, wenn sie auf einer ungenügenden Rechtsgrundlage beruht, gegen eine Geheimhaltungsvorschrift verstösst, unverhältnismässig oder bei besonders schützenswerten Personendaten zu einem Zweck erfolgt, der mit dem Zweckbindungsgebot nicht vereinbar ist. Der Unterlassungsanspruch kann sich namentlich auf die Weitergabe von Daten an Dritte beziehen und ist bereits dann zuzulassen, wenn eine widerrechtliche Bearbeitung ernstlich zu befürchten ist. Die Beseitigung der Folgen einer unzulässigen Datenbearbeitung ist manchmal nur mehr in beschränktem Umfang möglich, namentlich wenn Dritte schon Kenntnis von einer Information erhalten haben. Widerrechtlich bearbeitete Daten sind grundsätzlich zu vernichten. Auch die blosser Feststellung der Widerrechtlichkeit einer Datenbearbeitung kann von Bedeutung sein. Die betroffene Person hat damit einen Rechtstitel in Händen, der es ihr ermöglicht, bei nachträglich auftauchenden Folgen widerrechtlicher Bearbeitung unverzüglich einzuschreiten.

### *Artikel 17; Sperrung*

Jede Person hat das Recht, die Weitergabe ihrer Personendaten an Private bei Daten bearbeitenden öffentlichen Organen sperren zu lassen, und zwar ohne Angabe von Gründen. Es sind Fälle denkbar, in denen die betroffene Person ein Interesse daran hat, dass selbst ihr Name und ihre Adresse nicht bekannt gegeben werden; zu denken ist an getrennt lebende Frauen, die sich vor Repressionen ihres Mannes schützen wollen, oder an politisch verfolgte Flüchtlinge, die auf schwarzen Listen ihres Heimatlandes stehen (Abs. 1).

Das Sperrrecht findet dort seine Schranken, wo ein gesetzlicher Auftrag (Mitteilungspflichten) vereitelt und die Rechtsordnung bzw. der Gesetzgeber selber eine Interessenabwägung vorgenommen und sich für eine Bekanntgabe entschieden hat, die dem individuellen Sperrrecht vorgeht. Auch soll die missbräuchliche Ausübung des Sperrrechts keinen Schutz finden. Macht beispielsweise ein Gläubiger dem öffentlichen Organ glaubhaft, dass der Schuldner die Sperrung seiner Adressdaten nur veranlasst hat, um sich einer Betreuung zu entziehen, so können dem Gläubiger trotz des Sperrvermerks die zum Auffinden des Schuldners notwendigen Daten zugänglich gemacht werden (Abs. 2).

### *Artikel 18; Rechtsschutz*

Auf Verlangen eines Betroffenen hat das öffentliche Organ einen Entscheid (Verfügung) zu erlassen, der gemäss den allgemeinen Bestimmungen des Verwaltungsrechtspflegegesetzes mit Beschwerde angefochten und dem Verwaltungsgericht zur Beurteilung unterbreitet werden kann (Abs. 1).

Auch wenn die Hauptverantwortung für die Durchsetzung ihrer Rechtsansprüche bei den betroffenen Personen selber bleiben und es in ihrem Belieben liegen soll, ob sie ihre Rechte wahrnehmen wollen, ist zugunsten der kantonalen Aufsichtsstelle ein Beschwerderecht vorzusehen, soweit und sobald das Daten bearbeitende öffentliche Organ eine Verfügung erlassen hat (Abs. 2).

Weil die Gerichte und übrigen staatlichen Justizbehörden in weiten Teilen nicht dem Verwaltungsrechtspflegegesetz unterstehen, drängt sich für diese eine andere Regelung auf. Gestützt auf das bestehende Recht über die Gerichtsorganisation können sich betroffene Personen gegen widerrechtliche Bearbeitungen seitens der Justiz nur aufsichtsrechtlich wehren (Abs. 3).

Ueber Beschwerden gegen letztinstanzliche kantonale Entscheide, die aufgrund des kantonalen Datenschutzrechts ergangen sind, sich aber richtigerweise auf Datenschutzrecht des Bundes hätten stützen müssen, entscheidet die eidgenössische Datenschutzkommission und letztlich das Bundesgericht.

### *Artikel 19; Schlichtungsverfahren*

Absatz 1 stellt den betroffenen Personen ein fakultatives Schlichtungsverfahren bei der kantonalen Aufsichtsstelle zur Verfügung, bevor die Parteien in ein förmliches Verfahren gezwungen werden. Mit der Vermittlung zwischen den öffentlichen Organen und den betroffenen Personen können Letztere versuchen, ihre Rechte ohne Rückgriff auf ein förmliches Verfahren einzufordern. Die Aufsichtsstelle soll dabei pragmatische und lösungsorientiert eine Einigung zu erreichen versuchen, vergleichbar etwa der Tätigkeit einer Ombudsstelle oder der Schlichtungsbehörde in Mietsachen. Im Falle eines Scheiterns kann die betroffene Person immer noch eine Verfügung verlangen, die sie dann rechtsmittelweise anfechten kann.

## **3.4. Aufsicht und Gebühren (Art. 20–22)**

### *Artikel 20; Aufsichtsstelle*

Artikel 20 verschafft der Forderung von Artikel 37 Absatz 2 DSG Nachachtung, wonach der Kanton ein Kontrollorgan einzusetzen hat, das beim Vollzug von Bundesrecht über die Einhaltung der Datenschutzvorschriften wacht. Wie die Erfahrung in anderen Kantonen zeigte, kann ein befriedigender und wirksamer Datenschutz nur gewährleistet werden, wenn eine unabhängige Kontrollinstanz seine Verwirklichung überwacht. Auch von Bundesrechts wegen ist das Erfordernis der Unabhängigkeit der Aufsichtsstelle unabdingbar; es ist damit nicht abhängig von einer kantonalrechtlichen Umsetzung. Unabhängigkeit bedeutet in diesem Zusammenhang mindestens Weisungsungebundenheit (Abs. 1).

In den anderen Kantonen haben sich als Lösungen die Einsetzung eines Datenschutzbeauftragten oder einer Datenschutzkommission herausgebildet. Eine Datenschutzkommission tagt periodisch und behandelt vorbereitete Themen; sie kommt in der Regel nicht ohne zusätzliche Ausstattung aus. Ein Datenschutzbeauftragter ist demgegenüber meist permanent ansprechbar und relativ unabhängig in der Gestaltung seiner Agenda. Die Sachkompetenz und Flexibilität wird bei einem Datenschutzbeauftragten höher sein als bei einem Mehrpersonengremium; demgegenüber dürfte das politische Gewicht sowie die Akzeptanz bei einer Datenschutzkommission grösser sein. Seit dem Inkrafttreten des DSG wurden die Aufsichtsaufgaben im Kanton Glarus durch einen nebenamtlichen Datenschutzbeauftragten wahrgenommen, der in einem kantonalen Dienstverhältnis steht (zuerst durch den Direktionssekretär der Polizeidirektion, seit dem 1. Januar 1998 durch einen juristischen Mitarbeiter der Regierungskanzlei).

Die Gemeinden sollen keine eigenen Aufsichtsstellen für den kommunalen Bereich vorsehen müssen. Dieser Verzicht hat zur Folge, dass die kantonale Aufsichtsstelle eine erhebliche Mehrbelastung erfährt, weil zur kantonalen Verwaltung noch die Gemeinden in regelmässigen Abständen Inspektionen zu unterziehen sein werden.

Auch wenn der Regierungsrat sowie teilweise die Gerichte dem Geltungsbereich des Datenschutzgesetzes unterliegen, werden die obersten Behörden – selbst in diesem eingeschränkten Bereich – nicht einer Superaufsichtsbehörde unterstellt. Sollten sich bei den genannten Behörden Anzeichen auf Missstände zeigen, müssten diese über die rechtlich vorgesehenen Mittel der politischen Aufsicht zu beheben versucht werden, allenfalls veranlasst durch die Berichtgabe der kantonalen Aufsichtsstelle an den Landrat im Amtsbericht (Abs. 3).

#### *Artikel 21; Aufgaben und Befugnisse der kantonalen Aufsichtsstelle*

Die gesetzliche Ausgestaltung zeigt, dass nicht nur an die nachträgliche Kontrolle gedacht worden ist. Vorgesehen ist unter anderem eine unterstützende, im Vorfeld von Konflikten beratende und vermittelnde Tätigkeit. Kontrollen bleiben aber nichtsdestotrotz unerlässlich und müssen insbesondere dort durchgeführt werden können, wo eine grosse Anzahl von Personen gravierend beeinträchtigt zu werden droht. Die Aufsicht verfolgt demnach zwei Stossrichtungen: einerseits Beratung und Information, andererseits Kontrolle und Ueberwachung. Notfalls ist es der Aufsichtsstelle in Einzelfällen gestattet, für gewisse Belange Experten beizuziehen. Dem kantonalen wird aber genauso wenig wie dem eidgenössischen Datenschutzbeauftragten eigentliche Entscheidkompetenz zukommen (Abs. 1 und 2).

Weil die Aufsichtsstelle zur Abklärung des rechtserheblichen Sachverhalts über weitreichende Kompetenzen verfügt und sie dadurch Einsicht in sensible Personendaten erhalten kann, wird sie einer Verpflichtung zur Verschwiegenheit unterstellt (Abs. 3).

#### *Artikel 22; Gebühren*

Dieser Artikel garantiert den Betroffenen im Grundsatz, dass sie ihre im Gesetz garantierten Rechte ohne die abschreckende oder behindernde Wirkung eines Kostenrisikos wahrnehmen können (Abs. 1).

Immerhin soll die Staatsverwaltung aber dann nicht auf eine Entschädigung ihres unter Umständen erheblichen Aufwandes verzichten müssen, wenn z. B. Personen ohne Unterlass oder in rechtsmissbräuchlicher Weise ihre Rechte geltend machen. In Anlehnung an die vom Bundesrat erlassene Datenschutzverordnung werden zwei generell geltende Ausnahmen im Gesetz vorgesehen. Der «grosse Aufwand» ist aber nicht bereits dann gegeben, wenn lediglich ein Dossier hervorgeholt und kopiert werden muss. Anwendung finden dürfte die Ausnahmebestimmung bei erforderlichen langwierigen Nachforschungen, insbesondere wenn eine Datensammlung manuell geführt ist oder auf mehrere Dossiers verweist. Der andere Fall betrifft namentlich schikanöse Begehren. Droht dem Gesuchsteller eine Kostenbeteiligung, ist er vorher darauf aufmerksam zu machen, damit er sein Begehren innert einzuräumender Frist zurückziehen kann. Im Uebrigen soll der Regierungsrat die Kompetenz erhalten, im Nachgang an allfällig auftauchende Problemfälle von ähnlicher Bedeutung weitere Ausnahmen von der Kostenlosigkeit vorzusehen.

### **3.5. Uebergangs- und Schlussbestimmungen (Art. 23–25)**

#### *Artikel 23; Uebergangsbestimmungen*

Der letzte Abschnitt enthält diejenigen Bestimmungen, welche ein möglichst reibungsloses Anpassen der bestehenden Personendatensammlungen an die neuen Vorschriften ermöglichen. Da es dazu eines erheblichen Aufwandes bedürfen wird und allenfalls bereichsspezifische Rechtsgrundlagen geschaffen werden müssen, rechtfertigt sich die Einräumung einer angemessenen Frist. Die unterschiedlichen Fristen erklären sich aus dem Umstand, dass der Aufsichtsstelle ebenfalls Zeit für den Aufbau ihres zentralen öffentlichen Registers einzuräumen ist.

#### *Artikel 24; Ausführungsbestimmungen*

Der Regierungsrat wird beauftragt bzw. ermächtigt, weitere ausführende Bestimmungen zu erlassen. Es werden vor allem die Anforderungen in Sachen Datensicherheit näher zu umschreiben sein.

#### *Artikel 25; Inkrafttreten*

Das neue Datenschutzgesetz tritt auf den 1. Januar 2003 in Kraft.

#### 4. Beratung der Vorlage im Landrat

Eine landrätliche Kommission unter dem Vorsitz von Landrat Otto Fischli, Näfels, nahm sich dieser Vorlage an. Eintreten auf die Vorlage war unbestritten. Nebst einigen redaktionellen Korrekturen beantragte die Kommission restriktivere Fassungen von Artikel 7 (Beschaffung von Personendaten) und Artikel 10 Absatz 4 (Umfang der Bekanntgabe von allgemein zugänglichen Personendaten).

Im Landrat war die Vorlage grundsätzlich unbestritten. Einzig in Bezug auf Artikel 10 Absatz 4 ergaben sich Meinungsdivergenzen, welche mit einem Kompromiss zwischen der regierungsrätlichen und der restriktiveren Kommissionsfassung bereinigt wurden.

In der Schlussabstimmung wurde der bereinigte Entwurf einstimmig zuhanden der Landsgemeinde verabschiedet.

#### 5. Antrag

*Gestützt auf vorstehende Ausführungen beantragt der Landrat der Landsgemeinde, den Memorialsantrag betreffend Erlass eines Datenschutzgesetzes aus dem Jahr 1985 als erledigt abzuschreiben und nachstehendem Gesetzesentwurf zuzustimmen:*

## Gesetz über den Schutz von Personendaten

(Datenschutzgesetz)

(Erlassen von der Landsgemeinde am ..... Mai 2002)

### I. Einleitende Bestimmungen

#### Art. 1

##### Zweck

Dieses Gesetz dient dem Schutz des Grundrechts jeder Person vor dem Missbrauch der sie betreffenden Daten, welche die öffentlichen Organe des Kantons bearbeiten.

#### Art. 2

##### Geltungsbereich

<sup>1</sup> Die Bestimmungen dieses Gesetzes gelten, unabhängig von den dabei angewandten Mitteln und Verfahren, für jedes Bearbeiten von Personendaten durch öffentliche Organe; als solche gelten:

- a. der Regierungsrat, die regierungsrätlichen Kommissionen sowie die kantonale Verwaltung,
- b. die Gerichte, Rekurskommissionen und die übrigen staatlichen Justizbehörden, soweit sie Verwaltungsaufgaben versehen,
- c. die Gemeinden,
- d. die weiteren öffentlich-rechtlichen Körperschaften und Anstalten von Kanton und Gemeinden,
- e. Private, soweit ihnen öffentliche Aufgaben übertragen sind.

<sup>2</sup> Das Gesetz ist nicht anwendbar auf:

- a. das nicht hoheitliche Handeln öffentlicher Organe anlässlich der Teilnahme am wirtschaftlichen Wettbewerb;
- b. den Landrat und dessen Kommissionen;
- c. hängige Zivilprozesse und Strafverfahren, eingeschlossen die polizeilichen Untersuchungen im Rahmen von Ermittlungsverfahren;
- d. hängige Verfahren der Staats- und Verwaltungsrechtspflege, mit Ausnahme der nichtstreitigen Verwaltungsverfahren;
- e. die öffentlich-rechtlich anerkannten Landeskirchen und die Kirchgemeinden im Bereich ihrer inneren Angelegenheiten;
- f. die öffentlichen Register, mit Ausnahme der in Artikel 13 dieses Gesetzes vorgesehenen Register;
- g. Personendaten, die einem Archiv der öffentlichen Hand zugeführt worden sind.

<sup>3</sup> Abweichende und ergänzende Bestimmungen in anderen Gesetzen bleiben vorbehalten, sofern sie den Schutz vor widerrechtlicher Bearbeitung von Personendaten im Sinne dieses Gesetzes sicherstellen.

### **Art. 3**

#### *Begriffe*

Die folgenden Ausdrücke bedeuten:

- a. Personendaten: alle Angaben, die sich auf eine bestimmte oder bestimm-  
bare natürliche oder juristische Person oder eine Personengesellschaft  
des Handelsrechts beziehen;
- b. besonders schützenswerte Personendaten: namentlich Angaben über  
religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten  
und Tätigkeiten, über die Gesundheit und die Intimsphäre, die ethnische  
Herkunft, über Massnahmen der Sozialhilfe sowie über strafrechtliche  
oder administrative Verfolgungen und Sanktionen;
- c. Bearbeiten: jeder Umgang mit Personendaten, insbesondere das Be-  
schaffen, Erheben, Aufzeichnen, Sammeln, Aufbewahren, Verwenden,  
Berichtigen, Umarbeiten, Bekanntgeben, Veröffentlichen, Zugänglichma-  
chen, Archivieren oder Vernichten von Personendaten;
- d. Datensammlung: jeder Bestand von Personendaten, der so aufgebaut ist,  
dass die Daten nach den betroffenen Personen erschliessbar sind;
- e. Inhaber einer Datensammlung: öffentliche Organe, die über den Zweck,  
den Inhalt und die Verwendung der Datensammlung entscheiden.

## **II. Bearbeiten von Personendaten**

### **Art. 4**

#### *Grundsätze*

<sup>1</sup> Personendaten dürfen bearbeitet werden,

- a. wenn dafür eine Rechtsgrundlage besteht, oder
- b. wenn es zur Erfüllung einer auf einer Rechtsgrundlage beruhenden Auf-  
gabe unentbehrlich ist, oder
- c. wenn und soweit die betroffene Person eingewilligt hat.

<sup>2</sup> Die Bearbeitung von Personendaten muss verhältnismässig sein. Sie hat sich insbesondere auf die notwendigen und geeigneten Personendaten zu beschränken.

<sup>3</sup> Personendaten müssen richtig, und soweit es der Zweck des Bearbeitens verlangt, vollständig und aktuell sein.

### **Art. 5**

#### *Besonders schützenswerte Personendaten*

<sup>1</sup> Besonders schützenswerte Personendaten dürfen unter Vorbehalt einer ausdrücklichen Zustimmung der betroffenen Person nur bearbeitet werden, wenn es in einem formellen Gesetz vorgesehen oder zur Erfüllung einer in einem formellen Gesetz vorgesehenen Aufgabe unentbehrlich ist.

<sup>2</sup> Sie dürfen nicht für Zwecke bearbeitet werden, die sich mit dem ursprünglichen Beschaffungszweck nicht vereinbaren lassen, die für die betroffene Person aus den Umständen nicht erkennbar waren oder mit denen die betroffene Person nicht rechnen musste.

### **Art. 6**

#### *Verantwortlichkeiten, Auslagerung*

<sup>1</sup> Bearbeiten mehrere öffentliche Organe Personendaten aus einer gemeinsamen Datensammlung, trägt in erster Linie der Inhaber der Datensammlung die Verantwortung; jede Behörde bleibt aber für ihren Bereich verantwortlich. Dem Inhaber der Datensammlung ist die Durchführung von Kontrollen über die Einhaltung der Datenschutzbestimmungen bei den andern öffentlichen Organen zu gestatten.

- <sup>2</sup> Das Bearbeiten von Personendaten darf an Dritte ausgelagert werden,
- wenn es in einem formellen Gesetz vorgesehen ist, und
  - wenn das den Auftrag vergebende öffentliche Organ dafür sorgt, dass die Daten nur so bearbeitet werden, wie es ihm selbst erlaubt ist, und
  - wenn keine Geheimhaltungspflichten entgegenstehen.
- <sup>3</sup> Die Einhaltung der Bestimmungen über den Datenschutz und die Datensicherheit seitens des beauftragten Dritten ist mittels Weisungen, Kontrollrechten, Auflagen, Vereinbarungen oder mit andern geeigneten Mitteln sicherzustellen. Der Beauftragte darf die zur Verfügung gestellten Personendaten nur dem Auftraggeber bekannt geben und nicht in eigenem Ermessen bearbeiten, unter Vorbehalt anderslautender Vereinbarung.

## Art. 7

### *Beschaffen von Personendaten*

- <sup>1</sup> Die Beschaffung von Personendaten hat grundsätzlich bei den betroffenen Personen selbst in einer für sie erkennbaren Weise zu erfolgen.
- <sup>2</sup> Bei systematischen Erhebungen, namentlich mit Fragebogen, gibt das öffentliche Organ den Zweck, die Rechtsgrundlage der Datenbeschaffung und allfällige weitere Empfänger der Daten an. Es weist darauf hin, ob eine Auskunftspflicht besteht und welche Folgen eine Verweigerung der Auskunft haben kann.
- <sup>3</sup> Im Uebrigen können Personendaten bei Dritten beschafft werden, wenn eine direkte Erhebung bei der betroffenen Person insbesondere unverhältnismässig oder nicht möglich ist und die Grundsätze der Bearbeitung von Personendaten gemäss Artikel 4 beachtet werden.

## Art. 8

### *Datensicherheit*

- <sup>1</sup> Wer Personendaten bearbeitet, sorgt durch angemessene organisatorische und technische Vorkehren für ihre Sicherung vor Verlust sowie vor unbefugter Bearbeitung oder Kenntnisnahme.
- <sup>2</sup> Der Regierungsrat erlässt hinsichtlich einzuhaltender Mindestanforderungen nach Anhörung insbesondere der Abteilung für Informatik und Organisation EDV sowie des Landesarchivs ausführende Vorschriften.

## Art. 9

### *Allgemeine Einschränkung der Bekanntgabe von Personendaten*

- <sup>1</sup> Die Bekanntgabe von Personendaten kann aus überwiegenden öffentlichen oder aus schutzwürdigen privaten Interessen eingeschränkt, mit Auflagen verbunden oder verweigert werden.
- <sup>2</sup> Vorbehalten bleiben gesetzliche Geheimhaltungsvorschriften oder besondere Datenschutzvorschriften.
- <sup>3</sup> Die Bekanntgabe von Personendaten ins Ausland richtet sich sinngemäss nach den Bestimmungen des Bundesgesetzes über den Datenschutz.

## Art. 10

### *Bekanntgabe von Personendaten*

- <sup>1</sup> Personendaten dürfen nur dann von einem öffentlichen Organ im Einzelfall oder im Rahmen einer Listenauskunft bekannt gegeben werden, wenn alternativ
- dafür eine Rechtsgrundlage besteht;
  - der Gesuchsteller glaubhaft macht, dass die Personendaten zur Erfüllung einer ihm obliegenden gesetzlichen Aufgabe unentbehrlich sind;
  - der Gesuchsteller glaubhaft macht, dass die betroffene Person die Zustimmung verweigert, um die Durchsetzung von Rechtsansprüchen oder die Wahrnehmung anderer schutzwürdiger Interessen zu vereiteln; unter Vorbehalt von dringenden, bedeutsamen Gesuchen ist der betroffenen Person vor einer Bekanntgabe Gelegenheit zur Stellungnahme zu geben;
  - die betroffene Person zugestimmt hat oder ihr mutmassliches Einverständnis aufgrund der Interessenlage und der Umstände des Einzelfalles vorausgesetzt werden darf;

e. die Daten von der betroffenen Person allgemein zugänglich gemacht worden sind oder aus allgemein zugänglichen amtlichen oder amtlich bewilligten Veröffentlichungen stammen.

<sup>2</sup> Zusätzlich können Personendaten einem privaten Gesuchsteller im Einzelfall bekannt gegeben werden, wenn er schutzwürdige, insbesondere ideelle oder politische Zwecke verfolgende Interessen an den Personendaten glaubhaft machen kann. Besonders schützenswerte Personendaten dürfen nur mit schriftlicher Einwilligungserklärung der betroffenen Person bekannt gegeben werden.

<sup>3</sup> Personendaten dürfen ohne Anfrage gemeldet oder im Abrufverfahren (Online-Betrieb) bekannt gegeben werden, wenn dies in einem Rechtssatz ausdrücklich vorgesehen ist. Für besonders schützenswerte Personendaten bedarf es einer formell-gesetzlichen Grundlage.

<sup>4</sup> Name, Vorname, Adresse, Geburtsdatum und Heimatort dürfen auch dann bekannt gegeben werden, wenn die vorstehenden Voraussetzungen nicht erfüllt sind.

<sup>5</sup> Die Bekanntgabe von systematisch aufbereiteten Personendaten für wirtschaftliche Zwecke, insbesondere die Veräusserung von Personendaten an gewerbsmässig tätige Unternehmungen, ist zulässig, wenn sie in einem formellen Gesetz vorgesehen ist.

#### **Art. 11**

##### *Datenbearbeitung für nicht personenbezogene Zwecke*

<sup>1</sup> Für nicht personenbezogene Zwecke, insbesondere für Forschung, Planung und Statistik, können Personendaten auch dann bearbeitet werden, wenn die Voraussetzungen der vorstehenden Artikel nicht erfüllt sind; dabei ist jedoch sicherzustellen, dass

- a. die Daten anonymisiert werden, sobald es der Zweck des Bearbeitens erlaubt, und
- b. die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind.

<sup>2</sup> Vorbehalten bleiben besondere Vorschriften, insbesondere im Bereich der medizinischen Forschung.

#### **Art. 12**

##### *Vernichten und Archivieren*

<sup>1</sup> Die öffentlichen Organe müssen die Personendaten, die sie zur Erfüllung ihrer Aufgaben oder zu Sicherheits- oder Beweis Zwecken voraussichtlich nicht mehr benötigen, einem Archiv der öffentlichen Hand zur Ablieferung anbieten.

<sup>2</sup> Werden zur Archivierung angebotene Personendaten als nicht archivwürdig bezeichnet, sollen sie vernichtet werden, ausser wenn

- a. sie anonymisiert sind;
- b. sie zu Beweis- oder Sicherheitszwecken aufbewahrt werden müssen;
- c. die Löschung aufgrund einer erfolgten Vernetzung von Datensammlungen die Integrität anderer Datenstämme gefährdet und sich dies technisch nicht verhindern lässt.

<sup>3</sup> Ueber die Vernichtung von Personendaten ist ein Protokoll zu erstellen.

### **III. Rechte der betroffenen Personen**

#### **Art. 13**

##### *Register*

<sup>1</sup> Die öffentlichen Organe im Sinne von Artikel 2 führen, soweit sie dem Gesetz unterstehen, über ihre Datensammlungen ein Register. Wesentliche Änderungen haben sie der Aufsichtsstelle innert 30 Tagen zu melden. Die Aufsichtsstelle kann den öffentlichen Organen über die Führung der Register Weisungen erteilen.

<sup>2</sup> Die Aufsichtsstelle führt ein zentrales öffentliches Register, das auf den Registern nach Absatz 1 beruht.

<sup>3</sup> Die Register enthalten für jede Datensammlung zumindest Angaben über die Bezeichnung des Inhabers der Datensammlung, die Rechtsgrundlage und den Zweck der Bearbeitung, die Herkunft der bearbeiteten Personendaten sowie die Empfänger, denen Personendaten durch ein Abrufverfahren oder ohne Anfrage gemeldet werden.

<sup>4</sup> Nicht registriert werden müssen Datensammlungen, die nicht regelmässig und nicht auf Dauer geführt werden oder die rechtmässig veröffentlicht worden sind.

#### **Art. 14**

##### *Einsichts- und Auskunftsrecht*

<sup>1</sup> Jede betroffene Person kann Einsicht in das öffentliche, zentrale Register der Datensammlungen der Aufsichtsstelle verlangen.

<sup>2</sup> Jede betroffene Person, die sich über ihre Identität ausweist, erhält auf Verlangen Auskunft über und Einsicht in ihre von einem öffentlichen Organ geführten Personendaten, soweit keine Geheimhaltungsvorschriften und keine wichtigen öffentlichen oder schutzwürdigen privaten Interessen entgegenstehen. Bestehen nur für einen Teil der Daten Hinderungsgründe, so wird das Auskunfts- und Einsichtsrecht nur betreffend diesen Teils eingeschränkt. Die Auskunft wird in allgemein verständlicher Form und auf Verlangen schriftlich erteilt.

<sup>3</sup> Würde das Einsichtsbegehren für das öffentliche Organ zu einem unverhältnismässigen Verwaltungsaufwand führen, kann die Einsichtnahme ausnahmsweise vom Nachweis eines erheblichen schutzwürdigen Interesses und von der Bevorschussung der voraussichtlichen Gebühr nach Artikel 22 abhängig gemacht oder auf einen schriftlichen Auszug beschränkt werden.

<sup>4</sup> Kann die Kenntnisnahme von Personendaten zu einer schwerwiegenden Belastung der betroffenen Person führen, so erteilt der Inhaber der Datensammlung die Auskunft einer von der betroffenen Person bezeichneten Vertrauensperson.

#### **Art. 15**

##### *Recht auf Berichtigung*

<sup>1</sup> Jede betroffene Person kann vom öffentlichen Organ verlangen, dass unrichtige Daten über die eigene Person berichtigt oder ergänzt werden.

<sup>2</sup> Bestreitet das öffentliche Organ die Unrichtigkeit, obliegt ihm der Beweis für die Richtigkeit. Die betroffene Person hat bei der Abklärung mitzuwirken.

<sup>3</sup> Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten bewiesen werden, insbesondere von solchen, die eine Wertung menschlichen Verhaltens enthalten, kann die betroffene Person die Aufnahme einer kurzen Gegendarstellung oder eines Vermerks über die bestrittene Richtigkeit verlangen.

#### **Art. 16**

##### *Unterlassungs-, Beseitigungs- und Feststellungsansprüche*

Wer ein schutzwürdiges Interesse hat, kann bezüglich der eigenen Daten vom öffentlichen Organ verlangen, dass

- a. ein widerrechtliches Bearbeiten der Daten unterlassen wird;
- b. die Folgen eines widerrechtlichen Bearbeitens soweit als möglich beseitigt werden;
- c. die Widerrechtlichkeit einer Bearbeitung festgestellt wird.

#### **Art. 17**

##### *Sperrung*

<sup>1</sup> Jede betroffene Person kann von einem öffentlichen Organ mit schriftlichem Gesuch verlangen, dass es bestimmte sie betreffende Personendaten Privaten nicht bekannt gibt.

<sup>2</sup> Das öffentliche Organ verfügt die Bekanntgabe im Einzelfall trotz der Sperre oder hebt sie auf, wenn

- a. eine Rechtspflicht zur Bekanntgabe besteht oder
- b. die gesuchstellende Person glaubhaft macht, dass die Sperre sie in der Durchsetzung von schutzwürdigen, eigenen Rechtsansprüchen gegenüber der betroffenen Person erheblich behindert.

#### **Art. 18**

##### *Rechtsschutz*

<sup>1</sup> Das öffentliche Organ erlässt einen beschwerdefähigen, begründeten Entscheid, wenn eine gesuchstellende Person oder eine betroffene Drittperson es verlangt.

<sup>2</sup> Die kantonale Aufsichtsstelle ist ebenfalls berechtigt gegen den Entscheid des öffentlichen Organes, der auch ihr zu eröffnen ist, Beschwerde zu führen.

<sup>3</sup> Im Uebrigen richten sich das Verfahren und der Rechtsschutz nach dem Verwaltungsrechtspflegegesetz und nach dem Gerichtsorganisationsgesetz.

#### **Art. 19**

##### *Schlichtungsverfahren*

<sup>1</sup> Jede in eigenen Rechten betroffene Person kann der kantonalen Aufsichtsstelle einen Antrag auf Schlichtung stellen, wenn sie eine Verletzung von Datenschutzvorschriften rügt.

<sup>2</sup> Kommt eine Einigung zustande, hält die Aufsichtsstelle dies schriftlich fest; das Verfahren gilt damit als erledigt.

<sup>3</sup> Scheitert der Schlichtungsversuch, gibt die Aufsichtsstelle dem öffentlichen Organ bei festgestellter Rechtsverletzung eine schriftliche Empfehlung ab.

### **IV. Aufsicht und Gebühren**

#### **Art. 20**

##### *Kantonale Aufsichtsstelle*

<sup>1</sup> Der Regierungsrat wählt eine unabhängige und fachlich selbstständige kantonale Aufsichtsstelle, die auf Anzeige oder Gesuch hin oder von Amtes wegen über die Einhaltung des Datenschutzrechts wacht.

<sup>2</sup> Die dem Datenschutzgesetz unterstehenden öffentlichen Organe sind verpflichtet, die Aufsichtsstelle bei der Erfüllung ihrer Aufgaben sowie der Feststellung des Sachverhalts zu unterstützen. In Aussicht genommene Erlasse und Projekte, die Aspekte des Datenschutzes berühren können, sind der Aufsichtsstelle unaufgefordert zur allfälligen Stellungnahme zu unterbreiten.

<sup>3</sup> Der Regierungsrat und die kantonalen Gerichte sind von der Aufsicht durch die Aufsichtsstelle ausgenommen.

#### **Art. 21**

##### *Aufgaben und Befugnisse der kantonalen Aufsichtsstelle*

<sup>1</sup> Die kantonale Aufsichtsstelle

- a. überwacht die Anwendung der Datenschutzvorschriften;
- b. bringt dem öffentlichen Organ oder dessen Aufsichtsbehörde Mängel bei der Bearbeitung von Personendaten zur Kenntnis und empfiehlt nötigenfalls Massnahmen;
- c. berät in Zusammenarbeit mit den zuständigen Fachstellen der Verwaltung, insbesondere mit der Abteilung für Informatik und Organisation EDV und dem Landesarchiv, die öffentlichen Organe in Fragen des Datenschutzes und der Datensicherheit;
- d. erteilt den betroffenen Personen Auskunft über ihre Rechte;
- e. vermittelt zwischen betroffenen Personen und öffentlichen Organen und führt auf Verlangen das Schlichtungsverfahren gemäss Artikel 19 durch;
- f. führt nach eigenem Ermessen Beschwerde gegen Verfügungen der öffentlichen Organe;
- g. erstattet auf behördliches Gesuch hin schriftliche Amtshilfe;
- h. nimmt Stellung zu Erlassen und Projekten, die Aspekte des Datenschutzes berühren können;

- i. sorgt für die Führung des zentralen Registers und erteilt nötigenfalls Weisungen über die Führung der andern auf diesem Gesetz beruhenden Register;
- k. erstattet dem Landrat jährlich Bericht über ihre Tätigkeit;
- l. arbeitet mit dem eidgenössischen Datenschutzbeauftragten und den Aufsichtsstellen der andern Kantone zusammen.

<sup>2</sup> Zur Wahrnehmung ihrer Aufgaben kann die kantonale Aufsichtsstelle bei den öffentlichen Organen, ungeachtet allfälliger Geheimhaltungsvorschriften, Auskünfte über das Bearbeiten von Personendaten einholen, Einsicht in Datensammlungen, Unterlagen und Akten nehmen und sich Bearbeitungen von Personendaten vorführen lassen. Sie kann für einzelne Aufgaben externe Experten beiziehen.

<sup>3</sup> Die kantonale Aufsichtsstelle untersteht denselben Geheimhaltungsvorschriften wie das Personendaten bearbeitende öffentliche Organ, auch nach der Beendigung der Amtsausübung.

## **Art. 22**

### *Gebühren*

<sup>1</sup> Die öffentlichen Organe sowie die kantonale Aufsichtsstelle behandeln die Gesuche von betroffenen Personen, welche die ihnen gemäss diesem Gesetz zustehenden Rechte geltend machen, in der Regel kostenlos.

<sup>2</sup> Nach vorgängig erfolgtem Hinweis kann jedoch vom Gesuchsteller eine angemessene Verwaltungsgebühr von höchstens 500 Franken verlangt werden, insbesondere wenn

- a. die Behandlung eines Gesuches einen grossen Aufwand erfordert;
- b. die Gesuch stellende Person wiederholt ohne schutzwürdiges Interesse oder in rechtsmissbräuchlicher Weise die gleichen Begehren bei demselben öffentlichen Organ stellt.

<sup>3</sup> Der Regierungsrat kann für begründete Fälle weitere Ausnahmen von der Kostenlosigkeit vorsehen.

## **V. Uebergangs- und Schlussbestimmungen**

### **Art. 23**

#### *Uebergangsbestimmungen*

<sup>1</sup> Innert drei Jahren nach Inkrafttreten dieses Gesetzes haben die dem Gesetz unterstehenden öffentlichen Organe ihre bestehenden Datensammlungen dem neuen Recht anzupassen und ihre Register zu erstellen. Die Aufsichtsstelle richtet das kantonale Register der Datensammlungen innert vier Jahren nach Inkrafttreten des Gesetzes ein.

<sup>2</sup> Datensammlungen, die bei Inkrafttreten dieses Gesetzes bestehen, dürfen während drei Jahren benützt werden, auch wenn die Voraussetzungen des Gesetzes nicht erfüllt sind. Der Regierungsrat kann die Frist aus wichtigen Gründen für einzelne Datensammlungen erstrecken.

### **Art. 24**

#### *Ausführungsbestimmungen*

Der Regierungsrat erlässt die notwendigen Ausführungs- und Vollzugsbestimmungen.

### **Art. 25**

#### *Inkrafttreten*

Das Gesetz tritt auf den 1. Januar 2003 in Kraft.