KANTON
LUZERN

Botschaft des Regierungsrates
an den Grossen Rat B 38

zum Entwurf eines Informatikgesetzes

27. Januar 2004

Übersicht

Der Regierungsrat unterbreitet dem Grossen Rat den Entwurf eines Informatikgesetzes zum Beschluss.

Die Informatik hat für die staatliche Aufgabenerfüllung in verhältnismässig kurzer Zeit eine zentrale Bedeutung erlangt. In der Verwaltung des Kantons und der Gemeinden sowie bei den Gerichten ist die Informatik nicht nur das oftmals wichtigste Arbeitsinstrument, sondern darüber hinaus immer wichtiger werdendes Kommunikations- und Informationsmittel (E-Mail, E-Government, Internet).

Die rasche und intensive Verbreitung der Informatik hat in verschiedener Hinsicht zu Problemen geführt:

- *Das aus wirtschaftlicher Sicht erwünschte Zusammenführen von Datensammlungen verschiedener Organe, beispielsweise im Steuerbereich die des Kantons und der Gemeinden, bringt datenschutzrechtliche Probleme mit sich.*
- *Dasselbe gilt für die Einrichtung von Abrufverfahren, wie sie etwa zwischen der Kantonspolizei und den Einwohnerregistern der Gemeinden angewendet werden.*
- *Im heutigen rechtlichen Rahmen ist die immer bedeutender werdende Auslagerung (Outsourcing) von Informatikdienstleistungen problematisch. Hier besteht die Gefahr, dass bei einem allfälligen Ausfall des Auftragnehmers die Erfüllung der staatlichen Tätigkeit nicht mehr gewährleistet sein könnte.*
- *Ungeklärt ist die Zulässigkeit von Techniken, die geeignet sind, aus nicht besonders schützenswerten Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen (z. B. data mining oder Rasterfahndung).*
- *Die wirtschaftliche Bedeutung der Informatik für den Kanton ist ein wesentlicher Aspekt; insbesondere können durch eine effiziente Informatikorganisation bedeutende Einsparungen erzielt werden.*
- *Die Informatiksicherheit sollte gewährleistet werden. Dazu gehört, dass die Benutzerinnen und Benutzer von Informatikmitteln diese richtig und nicht missbräuchlich einsetzen. Die dazu erforderlichen Überwachungsmassnahmen können einen Eingriff in die Grundrechte bedeuten (Informationsfreiheit), was eine gesetzliche Grundlage erfordert.*

Die Regelung dieser Problemfelder der Informatik bedarf einer zeitgemässen Rechtsgrundlage. Damit sollen folgende Ziele erreicht werden:

- *Die Rechtsunsicherheiten bei der Einrichtung zentraler Datenbanken verschiedener Organe und bei Abrufverfahren werden beseitigt.*
- *Beim Auslagern von Informatikdienstleistungen wird die Erfüllung der staatlichen Aufgaben auch bei einem allfälligen Ausfall des Auftragnehmers sichergestellt.*
- *Der zulässige Einsatz von Techniken, die geeignet sind, aus nicht besonders schützenswerten Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen, wird geregelt.*
- *Das Verwaltungshandeln soll vereinfacht und gleichzeitig der Datenschutz gestärkt werden.*
- *Es soll die Grundlage für einen rationellen, sicheren und effizienten Informatikeinsatz geschaffen werden.*

– *Zur Stärkung der Gemeindeautonomie wird den Gemeinden weitgehende Freiheit belassen. Das Gesetz gilt für sie daher nur hinsichtlich der zentralen Datenbanken und der Abrufverfahren sowie des Einsatzes von Techniken, die geeignet sind, aus nicht besonders schützenswerten Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen; im Übrigen gilt es für die Gemeinden nur dann, wenn sie Informatikmittel des Kantons benutzen.*

Der Gesetzesentwurf ist in sechs Teile gegliedert:

– *Im ersten Teil des Entwurfs werden der Zweck des Gesetzes umschrieben und Grundsätze der Informatik aufgestellt. Der Geltungsbereich wird abgesteckt, Begriffe werden definiert.*
– *Im zweiten Teil werden die Voraussetzungen für die Einrichtung zentraler Datenbanken und Abrufverfahren geregelt. Dazu ist der Abschluss einer Leistungsvereinbarung zwischen den angeschlossenen Organen und dem Betreiber erforderlich; diese muss durch die zuständige Behörde des Kantons oder der Gemeinden genehmigt werden. Enthält die zentrale Datenbank keine besonders schützenswerten Personendaten, so ist das Informatikgesetz selber die gesetzliche Grundlage; enthält sie besonders schützenswerte Personendaten oder Persönlichkeitsprofile, so ist eine gesetzliche Grundlage in einem Spezialgesetz erforderlich. Dringliche Projekte sollen unter bestimmten Voraussetzungen während fünf Jahren auch ohne solche spezialgesetzliche Grundlage realisiert werden können. Geregelt werden die Verantwortlichkeiten des Betreibers, die Zugriffsverwaltung sowie Besonderheiten bei der Erhebung der Personendaten für zentrale Datenbanken, bei der Führung der Register zentraler Datenbanken und bei den Kontrollrechten der betroffenen Person. Werden Personendaten dauerhaft in zentralen Datenbanken gespeichert, ist für solche Datenbanken eine Publikationspflicht im Kantonsblatt vorgesehen.*
– *Im dritten Teil des Entwurfs werden die Voraussetzungen für die Auslagerung von Informatikdienstleistungen geregelt. Im Zentrum steht hier die Gewährleistung der staatlichen Aufgabenerfüllung, die durch eine Vereinbarung mit Mindestinhalt sowie durch organisatorische und technische Massnahmen sichergestellt werden soll.*
– *Der vierte Teil enthält eine verbesserte Rechtsgrundlage für die Informatikorganisation auf der Ebene des Kantons, welche in der Informatikverordnung (SRL Nr. 39) geregelt ist.*
– *Der fünfte Teil enthält die Rechtsgrundlage für den Erlass einer Informatiksicherheitsverordnung durch den Regierungsrat sowie eine verbesserte Rechtsgrundlage für die Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz (SRL Nr. 38c).*
– *Der sechste Teil enthält Strafbestimmungen sowie Anpassungen zweier Gesetze: Einerseits soll in das Datenschutzgesetz ein Verweis auf das Informatikgesetz eingefügt werden; andererseits soll anstelle einer bereits in Kraft stehenden Verordnungsbestimmung im Gesetz über die Kantonspolizei eine formellgesetzliche Grundlage für die Einrichtung von Abrufverfahren bei den Einwohnerkontrollen geschaffen werden.*

Der Regierungsrat des Kantons Luzern an den Grossen Rat

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen mit dieser Botschaft den Entwurf für ein Informatikgesetz.

I. Ausgangslage

1. Allgemeines

Die Informatik hat für die staatliche Aufgabenerfüllung in verhältnismässig kurzer Zeit eine zentrale Bedeutung erlangt. In der Verwaltung des Kantons und der Gemeinden sowie bei den Gerichten ist die Informatik nicht nur das oftmals wichtigste Arbeitsinstrument, sondern darüber hinaus ein immer wichtiger werdendes Kommunikations- und Informationsmittel (E-Mail, E-Government, Internet).

Diese rasche und intensive Verbreitung der Informatik hat in verschiedener Hinsicht zu rechtlichen Problemen geführt. So bringt etwa das aus wirtschaftlicher Sicht erwünschte Zusammenführen von Datenbanken verschiedener Organe, beispielsweise im Steuerbereich von Seiten des Kantons und der Gemeinden, datenschutzrechtliche Probleme mit sich. Sodann wird auch die Auslagerung (auch Outsourcing genannt) von Informatikdienstleistungen immer bedeutender. Hier besteht die Gefahr, dass bei einem allfälligen Ausfall des Auftragnehmers die Erfüllung der staatlichen Tätigkeit nicht mehr gewährleistet ist. Nicht geklärt ist ferner die Zulässigkeit von Techniken, die geeignet sind, aus nicht besonders schützenswerten Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen (z. B. data mining oder Rasterfahndung). Ein wesentlicher Aspekt der Informatik ist weiter ihre wirtschaftliche Bedeutung für den Kanton; insbesondere können durch eine effiziente Informatikorganisation bedeutende Einsparungen erzielt werden. Gewährleistet werden sollte sodann die Informatiksicherheit. Dazu gehört auch, dass die Benutzerinnen und Benutzer von Informatikmitteln diese richtig und nicht missbräuchlich einsetzen. Dies sicherzustellen kann einen Eingriff in die Grundrechte bedeuten (Informationsfreiheit), was eine gesetzliche Grundlage erfordert.

2. Kanton Luzern

Die Informatik stützt sich im Kanton Luzern auf verschiedene rechtliche Grundlagen (vgl. die nachfolgende Zusammenstellung). Eine formelle gesetzliche Grundlage für die Informatik fehlt jedoch. Mit dem Informatikgesetz soll eine einheitliche Rechtsgrundlage für Informatik-Belange im Kanton entstehen. Insbesondere sollen die Or-

ganisation der Informatik bestimmt und der Einsatz der Informatikmittel unter Einbezug des Datenschutzes geregelt werden.

Die heutigen Rechtsgrundlagen sind mangelhaft. Der rasche technische Fortschritt der Informatik eröffnet der Verwaltung und den Gerichten, aber auch den Gemeinden, ständig neue Möglichkeiten. So bietet sich die Datenhaltung in gemeinsamen Datenbanken an. Online-Abrufverfahren können eingerichtet werden. Informatikdienstleistungen können aber auch ausgelagert werden. Der Datenaustausch und die Informationsbeschaffung erfolgen immer häufiger auf elektronischem Weg. Mit dieser Entwicklung geht die Notwendigkeit der Schaffung klarer organisatorischer Strukturen einher. Die Sicherheit der Datenhaltung sowie der Austauschprozesse muss gewährleistet werden. Synergien sollen genutzt werden.

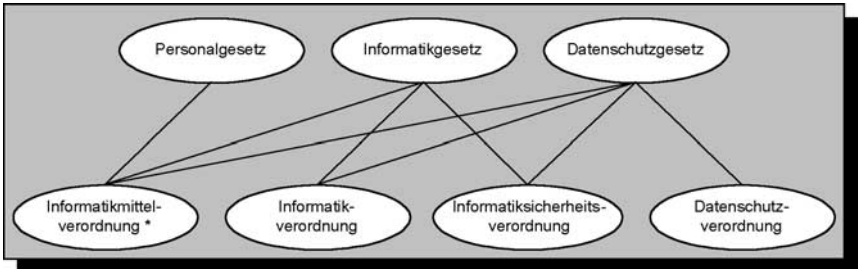
Erste zentrale Datenbanken und Abrufverfahren sind bereits eingerichtet worden (Datenpool mit Steuerdaten des Kantons und der Gemeinden, Zugriff der Kantonspolizei auf Einwohnerregisterdaten, landwirtschaftliches Informationssystem). Weitere sollen folgen (Datenwarenhaus / data warehouse mit Steuerdaten). Die entsprechenden Rechtsgrundlagen sind entweder lückenhaft oder ungenügend, oder sie fehlen ganz.

Die wichtigsten, heute bestehenden rechtlichen Grundlagen für die Informatik sind:

- Informatikverordnung vom 10. Dezember 2002 (SRL Nr. 39),
- Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz vom 10. Dezember 2002 (SRL Nr. 38c),
- Verordnung über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches vom 23. April 1996 (SRL Nr. 39b),
- Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990 (SRL Nr. 38),
- Verordnung zum Datenschutzgesetz vom 26. Februar 1991 (SRL Nr. 38b),
- Gesetz über das Archivwesen (Archivgesetz) vom 16. Juni 2003 (SRL Nr. 585; G 2003 275).

3. Systematik

Wir streben mit dem vorliegenden Entwurf die Schaffung eines zusammenhängenden Informatikrechts an. Wir wollen Lücken schliessen und zweifelhafte durch genügende Rechtsgrundlagen ersetzen. Dies wollen wir grundsätzlich auf der Basis der geltenden Erlasse tun. Das nachfolgende Schema verdeutlicht die systematische Stellung des Informatikgesetzes im Verhältnis zu den in diesem Zusammenhang wichtigsten Erlassen. Wir weisen darauf hin, dass die Verordnung über die Sicherheitsgrundsätze und das Bewilligungsverfahren im Bereich des elektronischen Datenaustausches (SRL Nr. 39b) durch eine Informatiksicherheitsverordnung gemäss § 19 des Entwurfs ersetzt werden soll.



* Vollständige Bezeichnung: Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz

4. Andere Kantone und Bund

Es findet sich sowohl beim Bund als auch bei den Kantonen eine Vielfalt von Lösungen, sowohl bezüglich der Erlassstufe (Gesetz, Verordnung) als auch hinsichtlich der materiellen Regelungen. Einige Kantone und auch der Bund stellen Regeln über die Informatiksicherheit auf (BS, FR, ZH). Bemerkenswert ist die Regelung des Kantons Zürich über die Auslagerung von Informatikdienstleistungen auf Gesetzesstufe (ZH LS 172.71). Die zentralen Datenbanken und Abrufverfahren sollen auf der Ebene des Bundes eine Regelung erfahren, welche über eine Änderung des Datenschutzgesetzes des Bundes angestrebt wird – dieses gilt allerdings für die Kantone nicht (BBl 2003, S. 2101 ff.). Organisationsrechtlich ist auf die Bundesinformatikverordnung (SR 172.010.58) hinzuweisen. Höchst unterschiedlich fällt jeweils auch die Regelungsdichte aus. Eine zusammenhängende Lösung, wie wir sie vorliegend anstreben, wird wohl mancherorts als wünschenswert erachtet, wurde aber noch nirgendwo realisiert. Der einzige als Informatikgesetz betitelte Erlass findet sich im Kanton Genf, ist aber veraltet (Loi sur les informations traitées automatiquement par ordinateur du 17.12.1981; RSG B 4 35).

II. Hauptziele des Informatikgesetzes

Ziel des Gesetzesentwurfs ist die Schaffung einer einheitlichen und zusammenhängenden Rechtsgrundlage für den Einsatz der Informatik im öffentlich-rechtlichen Bereich des Kantons Luzern. Die Gemeinden sind vom Geltungsbereich weitgehend ausgenommen: Das Gesetz gilt für sie nur hinsichtlich der zentralen Datenbanken und Abrufverfahren sowie des Einsatzes von Techniken, die geeignet sind, aus nicht besonders schützenswerten Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen; im Übrigen gilt es nur dann für die Gemeinden, wenn sie Informatikmittel des Kantons benutzen.

Mit der Regelung über zentrale Datenbanken und Abrufverfahren soll die effiziente und zeitgemässe Datenhaltung und -bewirtschaftung gefördert werden. Der bei solchen Bestrebungen oftmals als Behinderung empfundene Datenschutz soll auf solche Projekte hin konkretisiert und damit gleichzeitig gestärkt werden. Der Zielkonflikt zwischen effizientem, flexiblem und damit auch raschem Verwaltungshandeln einerseits und dem Erfordernis gesetzlicher Grundlagen für die Bearbeitung von Personendaten und dem damit verbundenen verhältnismässig langen Zeitraum eines Gesetzgebungsverfahrens andererseits soll entschärft werden.

Auch die Auslagerung (das Outsourcing) von Informatikdienstleistungen soll ermöglicht werden, um die aus wirtschaftlichen Gründen erforderliche Handlungsfreiheit des Staates zu gewährleisten. Dabei soll aber der Gefahr begegnet werden, dass die staatliche Aufgabenerfüllung gefährdet werden könnte, falls der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt. Zudem ist auch hier die Sicherstellung des Datenschutzes ein wichtiges Anliegen.

Der Gefahr des Datenverlusts, aber auch der Lahmlegung der Verwaltungstätigkeit durch unsichere Informatikmittel soll durch einheitliche Massnahmen im Bereich der Informatiksicherheit begegnet werden. Dafür soll eine gesetzliche Grundlage geschaffen werden.

Das formale Ziel des neuen Gesetzes besteht darin, die Grundsätze des Umgangs mit der Informatik auf Gesetzesstufe zu heben, während sie bislang bloss auf Verordnungsstufe festgehalten waren. Zudem soll eine bessere Rechtsgrundlage für die beiden bestehenden Verordnungen, nämlich die Informatikverordnung vom 10. Dezember 2002 (SRL Nr. 39) und die Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz vom 10. Dezember 2002 (SRL Nr. 38c), geschaffen werden.

Schliesslich kann das Informatikgesetz als Gefäss für künftigen Regelungsbedarf dienen. Dieser könnte etwa in der Regelung der Kommerzialisierung von Daten bestehen.

III. Vernehmlassungsverfahren

Wir haben in den Monaten Juli bis September 2003 zum Entwurf des Informatikgesetzes ein Vernehmlassungsverfahren durchgeführt. Wir haben alle Departemente, die Staatskanzlei, das Obergericht, das Verwaltungsgericht, den Verband Luzerner Gemeinden, alle Luzerner Gemeinden sowie alle im Grossen Rat vertretenen politischen Parteien zur Vernehmlassung eingeladen. Ausdrücklich auf eine Vernehmlassung verzichtet haben die Luzerner Pensionskasse und die Gemeinden Büron und Winikon. Das Gesundheits- und Sozialdepartement, die Steuerverwaltung sowie die Gemeinden Adligenswil, Mauensee und Rothenburg haben die Vorlage ohne weitere Bemerkungen begrüsst. Einlässlich zum Entwurf geäussert haben sich das Bildungs- und Kulturdepartement, das Justiz- und Sicherheitsdepartement, das Obergericht und das Verwaltungsgericht in einer gemeinsamen Stellungnahme, die FDP-Frauen, die SP, die Stadt Luzern, die Interessengemeinschaft Gemeindeinformatik (IGGI), deren Stellungnahme sich Dierikon, Hildisrieden und Kriens angeschlossen haben,

die Gemeinden Meggen, Rain, Root und Wolhusen, welche die Stellungnahme der EDV-ERFA Nest Kanton Luzern übernommen haben, sowie die Organisations- und Informatikdienste (OID). Als einzige Vernehmlassungsadressatin hielt die Gemeinde Buttisholz das neue Gesetz für nicht nötig, weil damit der Staatsapparat auf allen Ebenen aufgebläht werde.

Die in den Vernehmlassungen vorgebrachten Hinweise und Anregungen wurden sorgfältig geprüft und führten zu einer Überarbeitung des Entwurfs. Folgende Hauptdiskussionspunkte haben zu Änderungen an der Vernehmlassungsvorlage geführt:

– Von der im Vernehmlassungsentwurf vorgesehenen gesetzlichen Verankerung eines Informatikorgans, nämlich der Informatikkommission, wurde abgesehen und die entsprechende Verordnungskompetenz dem Regierungsrat übertragen.
– Die Genehmigung der Leistungsvereinbarungen zwischen den an einer zentralen Datenbank angeschlossenen Organen und dem Betreiber soll nicht wie im Vernehmlassungsentwurf vorgesehen durch ein Informatikorgan der kantonalen Verwaltung erfolgen, sondern durch die zuständige Behörde sei es des Kantons, sei es der Gemeinde, welcher das betreffende Organ zugehört. Der Regierungsrat soll die zuständige Behörde des Kantons bestimmen; auf Gemeindeebene soll diese Kompetenz dem Gemeinderat übertragen werden.
– Angesichts des in der Praxis häufig verwendeten englischen Begriffs folgen wir der Anregung des Obergerichts und des Verwaltungsgerichts, den englischen Begriff für «Datenwarenhaus» in Klammern anzuführen (data warehouse). Beim Begriff «Datendrehscheibe» wird darauf verzichtet, weil hier die Begrifflichkeit im Englischen uneinheitlich ist und daher mit einem englischen Begriff mehr Verwirrung gestiftet als zur Klarheit beigetragen würde. Im Interesse des einheitlichen kantonalen Sprachgebrauchs verzichten wir auch darauf, im Gesetzestext den englischen Begriff für die Auslagerung (outsourcing) in Klammern anzuführen.
– Die Umschreibung des Geltungsbereichs wurde vereinfacht; die Formulierung lehnt sich an den Vorschlag der Stadt Luzern an.
– Die in § 9 Absatz 2 der Vernehmlassungsvorlage vorgesehene ausdrückliche Einführung eines Äusserungsrechts des Datenschutzbeauftragten zur Datenschutzfreundlichkeit von Technologien, welche für zentrale Datenbanken beschafft werden sollen, wurde gestrichen. Eine solche Norm erübrigt sich angesichts der §§ 23 und 24 des Datenschutzgesetzes.
– Auf Anregung des Justiz- und Sicherheitsdepartementes sowie des Ober- und des Verwaltungsgerichtes wurde der Aspekt der Archivierung in verschiedenen Bestimmungen integriert. Das Archivgesetz wurde während der Vernehmlassungsfrist von Ihrem Rat beschlossen.

In den folgenden Hauptkritikpunkten haben wir aus folgenden Gründen am Entwurf festgehalten:

– Im Sinn der Einheit der Materie sollte die Informatik in einem eigenständigen Gesetz geregelt werden. Dies empfiehlt sich auch deshalb, weil es sich um eine Querschnittmaterie handelt, deren Bedeutung weiter wächst. Der Erlass eines neuen Gesetzes ist der bessere Weg als die Aufsplitterung der Materie: Die ebenfalls denkbare Normierung der Informatik in verschiedenen bestehenden Geset-

zen (z.B. Organisationsgesetze, Datenschutzgesetz, Personalgesetz) würde ein unübersichtliches Flickwerk ergeben. Insbesondere sollte das Datenschutzgesetz als Rahmengesetz mit seinen grundlegenden Bestimmungen in seiner Übersichtlichkeit und Klarheit erhalten werden: Die Konkretisierung der darin enthaltenen Bestimmungen hinsichtlich bestimmter Sachbereiche erfolgt nämlich in der Rechtsordnung in zahlreichen anderen Gesetzen (z. B. Teil V «Datenschutz» im Personalgesetz; SRL Nr. 51). Die Konkretisierung des Datenschutzes im Bereich der Informatik soll im Informatikgesetz erfolgen.

- Das Justiz- und Sicherheitsdepartement sowie die SP haben angeregt, nicht ein Informatik-, sondern ein Informationsgesetz vorzulegen. Gewollter Regelungsgegenstand ist jedoch nicht die Information allein, sondern es werden auch Informatiksysteme (samt darin enthaltener Information) erfasst. Nicht informatikbezogene Formen der Information dagegen (z. B. Öffentlichkeitsarbeit [vgl. Informationsrichtlinien, SRL Nr. 28], Publikation [vgl. Publikationsgesetz, SRL Nr. 27]) werden nicht erfasst. Ein Informations- statt eines Informatikgesetzes würde somit einerseits die angestrebte Regelungsmaterie nicht zutreffend bezeichnen und andererseits zu einer unerwünschten Verlagerung des Schwerpunktes führen. Wir halten daher am Namen «Informatikgesetz» für den vorliegenden Entwurf fest.
- Mit Rücksicht auf die Gemeindeautonomie, insbesondere die Organisationskompetenz der Gemeinden, verzichten wir darauf, die Gemeinden in die Bestimmungen über die Auslagerung und über die Informatiksicherheit mit einzubeziehen. Dies wurde von der Stadt Luzern gewünscht. Damit bleiben die Gemeinden frei, in diesen Gebieten eigene Bestimmungen zu erlassen. Sie sind dabei jedoch an das geltende Datenschutzrecht gebunden.
- Der Detaillierungsgrad wurde vom Justiz- und Sicherheitsdepartement als zu hoch kritisiert. Angesichts der rasanten Entwicklung in der Informatik sei zu befürchten, dass ein detailliertes Gesetz mit grosser Wahrscheinlichkeit schon bald wieder revisionsbedürftig werde. Diese Befürchtung teilen wir nicht, weil der Entwurf nicht technik-, sondern systembezogen aufgebaut ist. Damit werden auch künftige Entwicklungen, soweit zum heutigen Zeitpunkt in irgendwelcher Weise vorstellbar, vom Entwurf erfasst. Zudem erweist sich ein minimaler Detaillierungsgrad als unumgänglich: er orientiert sich an jenem des Luzerner Datenschutzgesetzes, was den Abschnitt über die zentralen Datenbanken betrifft, und am zürcherischen Gesetz über die Auslagerung von Informatikdienstleistungen, was den entsprechenden Abschnitt betrifft. Im Vergleich mit dem Entwurf des revidierten Datenschutzgesetzes des Bundes betreffend Abrufverfahren kann der vorliegende Entwurf eines Informatikgesetzes als schlank bezeichnet werden.
- Der Anregung einiger Vernehmlasser zu folgen, die Bestimmungen des Teils II nicht nur für zentrale, sondern auch für dezentrale beziehungsweise lokale Datenbanken anwendbar zu erklären, erübrigt sich. Solche Datenbanken gelten, unabhängig davon, wo sie sich befinden, als Datensammlungen im Sinne des Datenschutzgesetzes, und es sind die entsprechenden Bestimmungen anwendbar. Erst wenn Datensammlungen verschiedener Organe zusammengeführt werden, gelten sie als zentrale Datenbank. Auch diesfalls ist es unerheblich, wo sich die Daten befinden.

– Das Justiz- und Sicherheitsdepartement, die IGGI und die Gemeinden, welche sich der Stellungnahme der IGGI angeschlossen haben (Dierikon, Hildisrieden, Kriens) regen in ihrer Stellungnahme an, die Kommerzialisierung von Daten zu regeln. Wir nehmen diese Anregung auf. Das Informatikgesetz kann als Gefäss dafür dienen. Weil dazu einerseits einlässliche Diskussionen notwendig sind und andererseits der Erlass des vorliegenden Informatikgesetzes nicht verzögert werden sollte, wird diese Anregung zur Regelung in einem späteren Zeitpunkt aufgenommen. Im spezifischen Bereich der Geoinformationsdaten ist die Frage in den §§ 7 und 34 des Geoinformationsgesetzes (SRL Nr. 29) geregelt.
– Die IGGI und die Gemeinden, welche sich der Stellungnahme der IGGI angeschlossen haben (Dierikon, Hildisrieden, Kriens), schlagen die gesetzliche Verankerung eines gemeinsamen Informatik-Strategie-Organs des Kantons und der Gemeinden vor. Wir begrüssen dieses Organ, wollen es aber nicht auf Gesetzesstufe verankern. Bei der gesetzlichen Verankerung von Organen ist Zurückhaltung geboten.
– Die von der SP vorgeschlagene Einschränkung der Auslagerung auf öffentlichrechtliche Auftragnehmer lehnen wir aus wirtschaftlichen Überlegungen ab. Zudem wäre eine solche Einschränkung auch aus der Sicht des öffentlichen Beschaffungswesens problematisch, und zwar insbesondere wegen den Verpflichtungen, die sich aus dem Bundesgesetz über den Binnenmarkt und aus GATT/WTO ergeben.

Auf weitere inhaltliche Vorbringen kommen wir bei den Ausführungen zu den einzelnen Bestimmungen zurück (vgl. Kap. VI).

IV. Finanzielle und personelle Auswirkungen

Zentrale Datenbanken und Abrufverfahren dienen der rationellen Datenhaltung und dem effizienten Verwaltungshandeln. Dies gilt auch für die Auslagerung von Informatikdienstleistungen: Sie wird in der Regel nur in Frage kommen, wenn für den Staat ein wirtschaftlich günstigeres Resultat zu erwarten ist als ohne Auslagerung. Die im vorliegenden Entwurf vorgesehenen Regeln über zentrale Datenbanken, Abrufverfahren und die Auslagerung sollen solche Vorhaben rechtlich ermöglichen, indem sie für zulässig erklärt und die zu erfüllenden Voraussetzungen klar festgehalten werden. Auch die vorgesehene Zulässigkeit von Pilotprojekten dient der Förderung solcher Vorhaben. Die vorgeschlagenen Genehmigungsverfahren sind einfach ausgestaltet und führen zu keinem nennenswerten Mehraufwand. Dagegen führt der Gewinn an Rechtssicherheit und die eigentliche Ermöglichung solcher Projekte zu einem insgesamt geringeren Aufwand für die Verwaltungstätigkeit und somit schliesslich zu Einsparungen.

Geringerer finanzieller und personeller Aufwand resultiert auch – und zwar gestützt auf die Informatikverordnung bereits heute – aus der klaren Regelung der Aufgaben und Zuständigkeiten in der Informatikorganisation des Kantons. Mit der Konzern-Informatik kann für departementsübergreifende Aufgaben zentral die beste Lösung getroffen werden, und Skaleneffekte können genutzt werden.

Die Informatiksicherheit kann zwar finanziellen und personellen Mehraufwand nach sich ziehen. Dem stehen jedoch die Kosten gegenüber, die durch unsichere Informatiksysteme entstehen können. Daher ist die Gewährleistung der Informatiksicherheit eine Aufgabe, die schon heute in der Praxis bei der Umsetzung von Informatikvorhaben berücksichtigt wird. Insofern ist nicht mit zusätzlichen Kosten zu rechnen. Mit der vorgesehenen Regelung der Informatiksicherheit sollen einerseits die Sicherheitsmassnahmen besser koordiniert und andererseits das Sicherheitsrisiko minimiert werden; mittelbar wird dies zu Einsparungen führen, insbesondere auch im Zusammenhang mit der Informatikorganisation (Konzern-Aufgaben). Mit der vorgesehenen Regelung der Informatiksicherheit sollen mögliche Sicherheitsrisiken aufgedeckt und entsprechender Handlungsbedarf aufgezeigt werden. Sie können über den Aufwand von Informatiksicherheitsvorkehren auf dem Weg der ordentlichen Budgetierung befinden. Auch soll das Verhältnismässigkeitsprinzip auf Verordnungsstufe ausdrücklich verankert werden: Nicht jede erdenkliche Sicherheitsmassnahme soll realisiert werden, sondern nur solche, die in einem vernünftigen Verhältnis zum Aufwand stehen. Bezifferbar wird der Aufwand erst zwei Jahre nach Inkrafttreten der vorgesehenen Informatiksicherheitsverordnung sein: In dieser Zeitspanne werden die Dienststellen und Gerichte ihren Handlungsbedarf evaluieren und ordentlich budgetieren können. Während dieser Zeit werden für diese Evaluation vermehrt personelle Ressourcen gebunden sein. Im Hinblick auf den Zweck der Informatiksicherheit, nämlich die Risikominimierung, ist die vorgesehene Regelung insgesamt als kostendämpfend zu beurteilen.

V. Grundzüge und Gliederung des Erlasses

Das Informatikgesetz ist in sechs Teile gegliedert. Im ersten Teil des Entwurfs werden der Zweck des Gesetzes umschrieben und die Grundsätze der Informatik aufgestellt. Der Geltungsbereich wird abgesteckt, und Begriffe werden definiert. Im zweiten Teil werden die Voraussetzungen für die Einrichtung zentraler Datenbanken und Abrufverfahren geregelt. Dazu ist der Abschluss einer Leistungsvereinbarung zwischen den angeschlossenen Organen und dem Betreiber erforderlich; diese muss durch die zuständige Behörde des Kantons oder der Gemeinde genehmigt werden. Enthält die zentrale Datenbank keine besonders schützenswerten Personendaten, ist das Informatikgesetz selber die gesetzliche Grundlage; enthält sie besonders schützenswerte Personendaten oder Persönlichkeitsprofile, ist eine gesetzliche Grundlage in einem Spezialgesetz erforderlich. Dringliche Projekte sollen unter bestimmten Voraussetzungen während fünf Jahren auch ohne solche spezialgesetzliche Grundlage realisiert werden können. Geregelt werden die Verantwortlichkeiten des Betreibers, die Zugriffsverwaltung sowie Besonderheiten bei der Erhebung der Personendaten, bei der Führung der Register und bei den Kontrollrechten der betroffenen Person. Werden Personendaten dauerhaft in einem Datenwarenhaus gespeichert, ist für solche Datenbanken eine Publikationspflicht im Kantonsblatt vorgesehen. Im dritten Teil des Entwurfs werden die Voraussetzungen für die Auslagerung von Informatikdienstleistun-

gen geregelt. Die Regelung orientiert sich am zürcherischen Gesetz über die Auslagerung von Informatikdienstleistungen. Im Zentrum steht hier die Gewährleistung der staatlichen Aufgabenerfüllung, die durch eine Vereinbarung mit Mindestinhalt sowie durch organisatorische und technische Massnahmen sichergestellt werden soll. Der vierte Teil des Entwurfs enthält eine verbesserte Rechtsgrundlage für die Informatikorganisation des Kantons, welche in der Informatikverordnung (SRL Nr. 39) geregelt ist. Der fünfte Teil enthält die Rechtsgrundlage für den Erlass einer Informatiksicherheitsverordnung durch den Regierungsrat sowie eine verbesserte Rechtsgrundlage für die Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz (SRL Nr. 38c). Der sechste Teil enthält Strafbestimmungen sowie die Anpassung zweier Gesetze: Einerseits soll in das Datenschutzgesetz ein Verweis auf das Informatikgesetz eingefügt werden; andererseits soll anstelle einer bereits in Kraft stehenden Verordnungsbestimmung im Gesetz über die Kantonspolizei eine formellgesetzliche Grundlage für die Einrichtung von Abrufverfahren bei den Einwohnerkontrollen geschaffen werden.

VI. Die Gesetzesbestimmungen im Einzelnen

§ 1
Die zu regelnde Materie lässt sich unter den Begriffen der Organisation der Informatik und des Einsatzes der Informatikmittel zusammenfassen; auch etwa die Informatiksicherheit wird in diesem Sinn als Teil der Informatikorganisation verstanden. Die Begriffe Informatik und Informatikmittel werden in § 3 definiert. Der Hinweis auf den Datenschutz verdeutlicht die systematische Stellung des Informatikgesetzes. Die Gemeinden Meggen, Rain, Root und Wolhusen, welche die Stellungnahme der ERFA-Nest übernommen haben, schlagen vor, nicht auf den Datenschutz, sondern auf das Datenschutzgesetz zu verweisen. Dieser Anregung folgen wir nicht, denn dies würde eine Einschränkung darstellen: Nicht nur das Datenschutzgesetz, sondern auch die Datenschutzverordnung, die zahlreichen, in der gesamten Rechtsordnung verstreuten datenschutzrechtlichen Bestimmungen sowie die entsprechende Praxis sollen berücksichtigt werden.

§ 2
Soweit das Informatikgesetz Organisationsrecht und personalrechtliche Elemente enthält, soll es nur auf kantonaler, nicht jedoch auf Gemeindeebene gelten. Eine Ausnahme gilt dann und der Geltungsbereich wird entsprechend erweitert, wenn Gemeinden oder andere Stellen Informatikmittel des Kantons benutzen. Diesfalls sollen insbesondere die Informatiksicherheitsvorschriften, aber auch die Bestimmungen über die Informatikorganisation und über die Benutzung von Informatikmitteln am Arbeitsplatz Anwendung finden. Soweit entspricht der Geltungsbereich also jenem der Informatikverordnung bzw. der Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz.

Derselbe Geltungsbereich wird mit Rücksicht auf die Stärkung der Gemeindeautonomie auch für die Informatiksicherheit und die Auslagerung von Informatikdienstleistungen definiert, obwohl diese Regelungsbereiche beachtliche datenschutzrechtliche Aspekte enthalten.

Die Regelungen über die zentralen Datenbanken und Abrufverfahren dagegen werden wegen ihres stark datenschutzrechtlichen Charakters auch für die Gemeinden und die anderen vom Gesetz und vom Regierungsrat bezeichneten Stellen als anwendbar erklärt. Der Geltungsbereich entspricht diesbezüglich weitgehend jenem des Datenschutzgesetzes.

In § 3 Absatz 2 der Informatikverordnung hat der Regierungsrat Anlagen der Haustechnik und solche, die ausschliesslich der Steuerung technischer Prozesse dienen, von der Begriffsdefinition der Informatik (vgl. Bemerkungen zu § 3 Absätze 2 und 3) ausgenommen. Dem Regierungsrat soll in *Absatz 3* die Möglichkeit eingeräumt werden, solche und ähnliche Anlagen vom Geltungsbereich der Informatikgesetzgebung weiterhin auszuschliessen.

§ 3

Die in *Absatz 1* genannten Begriffe entstammen dem Datenschutzrecht, weshalb darauf verwiesen wird.

Absätze 2 und 3 entsprechen § 3 Absätze 1 und 3 der Informatikverordnung. Sie haben sich bewährt und treffen auch auf Gesetzesstufe zu. Sie werden daher übernommen. Auf Anregung des Obergerichts und des Verwaltungsgerichts wurde in Absatz 3 auch die Archivierung aufgenommen.

In *den Absätzen 4–7* werden jene Begriffe definiert, die im Teil II über zentrale Datenbanken und Abrufverfahren Verwendung finden (vgl. dazu die Ausführungen zu diesem Teil). Dazu ist zu bemerken, dass diese naturgemäss noch junge Begrifflichkeit in der Praxis häufig unterschiedlich verwendet wird. Deshalb ist es besonders wichtig, die Begriffe im Gesetz so zu definieren, wie sie im gesetzgeberischen Zusammenhang zu verstehen sind. In diesem Sinn werden die Begriffe nicht in technischer, sondern in funktionaler Weise umschrieben. Dies hat den Vorteil einer gewissen Zeitlosigkeit: Die in der Informatik ständig wechselnden und neu aufkommenden Begriffe können so unter die gesetzlichen Kategorien subsumiert werden. Beispielsweise stellen die gegenwärtig aktuellen Begriffe «Data Marts» und «Data Cubes» Datenwarenhäuser (data warehouses) im Sinn des Informatikgesetzes dar. Die Anregung des Justiz- und Sicherheitsdepartementes und der SP, von «Datenbanken» statt von «zentralen Datenbanken» zu sprechen, weil es sich beim Gegenstück um «dezentrale Datenbanken» handeln würde, übernehmen wir nicht. «Dezentrale Datenbanken», also Datensammlungen einzelner Organe, unterliegen nämlich der abschliessenden Regelung des Datenschutzgesetzes. Nur dann, wenn solche «dezentralen» oder «lokalen» Datensammlungen zusammengeführt werden, handelt es sich um «zentrale Datenbanken», wie sie vorliegend definiert werden. Der gewählte Begriff soll gerade den Umstand illustrieren, dass es sich nicht um die Datensammlung eines einzelnen, sondern um jene mehrerer Organe handelt.

Hinsichtlich der verschiedenen Rechenzentren der Gemeinden (z. B. IGGI, ERFA-Nest, RZ Littau) bedeutet diese Begriffsdefinition, dass diese Rechenzentren

so lange keine zentralen Datenbanken im Sinn des Gesetzes darstellen, als die Datenhaltung für jede Gemeinde separat betrieben wird. Erst dann, wenn die Datensammlungen verschiedener Gemeinden verschmolzen werden, ist von einer zentralen Datenbank auszugehen. Dies ist beispielsweise dann der Fall, wenn verschiedene Gemeinden auf denselben Datensatz (file) einer Person oder Teile davon Zugriff haben.

Absatz 8 bestimmt den Begriff der Auslagerung im Sinn dieses Gesetzes. Zudem wird sichergestellt, dass Dienstleistungen, die etwa die Organisations- und Informatikdienste für die kantonale Verwaltung und die Gerichte erbringen, keine Auslagerung darstellen (vgl. dazu die Ausführungen zum Teil III).

§ 4

Absatz 1 orientiert sich an § 4 der Informatikverordnung. Diesem Grundsatz kommt Gesetzesrang zu. Auf Anregung der SP und der OID wird gegenüber jener Formulierung der Zusatz «in den Schulen» weggelassen. Wir teilen die Ansicht, dass nicht nur Lernprozesse in den Schulen, sondern auch etwa in der Verwaltung unterstützungswürdig sind.

Absatz 2 orientiert sich an § 5 der Informatikverordnung. Dieser Vorschrift kommt ebenfalls Gesetzesrang zu. Auf Anregung der IGGI und der Gemeinden, die sich ihrer Stellungnahme angeschlossen haben (Dierikon, Hildisrieden, Kriens), wird nicht auf die Bedürfnisse der Dienststellen und Gerichte, sondern allgemeiner auf die Erfüllung der öffentlichen Aufgaben als Anknüpfungspunkt abgestellt.

Absatz 3: Als Techniken, die geeignet sind, aus Daten oder Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen, gelten etwa das Data Mining oder die diesem verwandte Rasterfahndung. Data Mining ist eine interdisziplinäre Wissenschaft, welche zum Gegenstand hat, mit verschiedenen hochkomplexen Verfahren und Methoden der Datenanalyse in grossen Datenbeständen bisher unbekannte Informationen zu entdecken. Es werden dabei verschiedene Algorithmen eingesetzt, die selbständig grosse Datenbestände nach unbekannten Auffälligkeiten, Zusammenhängen, Regeln, Trends, Mustern und Relationen zwischen den einzelnen Daten durchforsten. In der Wirtschaft wird diese Möglichkeit zur Ermittlung von Käufer- und Konsumentenprofilen genutzt. Aus datenschutzrechtlicher Sicht eröffnen solche Techniken unter Umständen die Möglichkeit, aus einfachen Personendaten besonders schützenswerte Personendaten oder gar Persönlichkeitsprofile zu generieren[1]. Ausgangsmaterial solcher Prozesse können also durchaus nicht besonders schützenswerte Personendaten sein, weshalb gestützt auf das geltende Datenschutzrecht dafür keine gesetzliche Grundlage erforderlich ist. Weil jedoch durch solche Prozesse aus grossen Mengen nicht besonders schützenswerter Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile hergestellt werden können, wird vorgesehen, dass für den Einsatz solcher Techniken die Voraussetzungen für das Bearbeiten von besonders schützenswerten Personendaten gemäss § 5 Absatz 2 des Datenschutzgesetzes erfüllt sein müssen; dabei steht das Vorhandensein einer gesetzlichen Grundlage im Vordergrund. Die Widerhandlung gegen diese Vorschrift stellt gemäss § 23 Absatz 1 einen Straftatbestand dar.

[1] Vgl. Alex Schweizer, Data mining, data warehousing, Zürich 1999.

Vorbemerkungen zu den Bestimmungen über zentrale Datenbanken und Abrufverfahren

a. Allgemeines

Zentrale Datenbanken und Abrufverfahren gewinnen auch in der Verwaltung und in den Gerichten rasch an Bedeutung. Aktuelle Beispiele sind etwa die Steuerdaten (Datenpool)[2] und das Zivilstandswesen. Sowohl in der Praxis als auch in der Lehre geht damit eine erhebliche Unsicherheit hinsichtlich des Umgangs mit Fragen des Datenschutzes einher[3]. Damit hat sich im Kanton Luzern eine Arbeitsgruppe befasst und ihre Erkenntnisse in einem Bericht festgehalten. Dieser ist Ausgangspunkt für die Arbeiten einer weiteren, von unserem Rat eingesetzten Arbeitsgruppe, insbesondere betreffend die Problematik zentraler Datenbanken. Lösungen dieser auch in anderen Kantonen, beim Bund und im Ausland sowie in der Lehre bekannten Problematik sind bisher allerdings noch nicht gefunden worden. Immerhin sieht der Entwurf des revidierten Datenschutzgesetzes des Bundes eine Regelung der Abrufverfahren vor. Der vorliegende Entwurf orientiert sich daran, ist aber einfacher ausgestaltet. In diesem Zusammenhang sei die Motion M 869 von Rico De Bona (am 23. Juni 2003 als Postulat erheblich erklärt) erwähnt, welche die Revision des Datenschutzgesetzes in einem pragmatischen Sinn verlangt.

b. Problematik

In einer zentralen Datenbank werden Datensammlungen verschiedener Organe an einem beliebigen Ort zusammengeführt. Dabei müssen den Organen der unveränderte Zugriff auf die Daten und die Bearbeitungsrechte erhalten bleiben. Diese Rechte dürfen andererseits auch nicht erweitert werden. Damit entsteht aus datenschutzrechtlicher Sicht etwas grundsätzlich Neues, was sich von «Datensammlungen» im herkömmlichen Sinn unterscheidet: Es handelt sich gewissermassen um eine Sammlung von Datensammlungen.

Keine zentralen Datenbanken in diesem Sinn stellen die verschiedenen gemeinsamen Rechenzentren der Gemeinden, wie etwa jenes der IGGI, das Rechenzentrum Littau oder das EDV-ERFA-Nest dar. In diesen Rechenzentren werden nämlich die Datensammlungen der Gemeinden nicht in einer gemeinsamen Datenbank zusammengeführt, sondern weiter getrennt betrieben.

Ein wesentlicher Unterschied zu Datensammlungen besteht darin, dass es – im Unterschied zu den Datensammlungen, für welche jeweils ein «Inhaber» vorgesehen wird – einen «Inhaber einer zentralen Datenbank» nicht gibt. Diese «Inhaber-Denkweise» stammt aus den Zeiten, als in den Büros noch Kasten und Kästchen mit Karteikarten standen und der zuständige Dienststellenleiter die Verantwortung für diese Karteikarten trug (in der Botschaft aus dem Jahr 1989 zum geltenden Datenschutzge-

[2] Vgl. die Motion M 445 von Louis Schelbert über die Errichtung eines zentralen Steuerregisters innerhalb der kantonalen Verwaltung (am 20. November 2001 teilweise erheblich erklärt als Postulat).

[3] Ausführlich: Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern / Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Data-Warehouse und Datenschutz, in: Tätigkeitsbericht 2000 LDA Brandenburg, S. 166 ff.

setz ist von «Kartotheken», nicht aber von Informatik die Rede). Diese Denkweise liess sich zwar noch auf die dezentralen Informatik-Datenbanken übertragen, nicht jedoch auf den Tatbestand, dass Datenbanken verschiedener Verwaltungseinheiten an einem beliebigen Ort zusammengeführt werden. Der Grund liegt darin, dass mit dieser Zentralisierung des «Aufbewahrungsortes» keine Zentralisierung der beteiligten Verwaltungseinheiten einhergeht; diesbezüglich bleibt die dezentrale Struktur erhalten.

In § 6 Absatz 3 des Datenschutzgesetzes hat der Gesetzgeber zwar daran gedacht, dass mehrere Organe Personendaten aus einer Datensammlung bearbeiten können, und er hat die Verantwortung «in erster Linie» dem Inhaber der Datensammlung zugewiesen, also unter den damaligen Verhältnissen jenem Organ, in dessen Räumlichkeiten die Kartothek steht. Daran, dass eine zentrale Datenbank aber auch woanders stehen könnte als in den Räumlichkeiten des Organs, welches die Daten bearbeiten darf, respektive daran, dass der Standort der Daten hinsichtlich ihres Bearbeitungsortes einmal unerheblich sein würde, hat der Gesetzgeber im Jahr 1989 wohl noch nicht gedacht. Interessant ist aber immerhin die Bestimmung, dass «jedes Organ für seinen Bereich mitverantwortlich bleibt» (§ 6 Absatz 3 DSG). Damit greift der Gesetzgeber – trotz des Konstrukts des Inhabers der Datensammlung als des Hauptverantwortlichen – zurück auf den in § 6 Absatz 1 DSG verankerten Grundsatz, dass derjenige die Verantwortung trägt, der die Daten bearbeitet. Sinnvollerweise sollte an diesem Grundsatz auch hinsichtlich zentraler Datenbanken festgehalten werden.

Insgesamt wird also *niemand* den «entscheidenden Einfluss auf Zweck und Bestand» (§ 6 Absatz 3 DSG) der zentralen Datenbank haben und somit «Inhaber der zentralen Datenbank» sein, denn die Datenbearbeitung erfolgt, wie ausgeführt, dezentral.

Es ist aber auch gar nicht nötig, einen «Inhaber einer zentralen Datenbank» zu definieren. Der erwähnte, in § 6 Absatz 1 DSG verankerte Grundsatz, wonach für den Datenschutz verantwortlich ist, wer Personendaten bearbeitet oder bearbeiten lässt, kann nämlich auch bei der Einrichtung von zentralen Datenbanken ohne weiteres aufrechterhalten und sogar gestärkt werden, wie nachfolgend gezeigt wird.

c. Lösung

Betrachtet man die Funktionen des «Inhabers einer Datensammlung» im Datenschutzrecht, so beschränken sich diese, abgesehen vom vorstehend besprochenen § 6 Absatz 3 DSG, auf das Verfahren betreffend Einsicht, Auskunft und Berichtigung. Diese Elemente gilt es also für zentrale Datenbanken zu ordnen.

Dabei ist zunächst davon auszugehen, dass sich die Zugriffs- und Bearbeitungsberechtigungen der beteiligten Organe nicht ändern sollen. Dies ist so festzuhalten. Sodann ist der wesentliche Umstand zu beachten, dass sich eine zentrale Datenbank an einem beliebigen Ort befinden kann und dort technisch betrieben wird: sei es bei einem beteiligten Organ, sei es bei einem kantonsinternen Betreiber (insbesondere OID) oder einem Auslagerungs-Partner. Um die technische Funktionsfähigkeit der zentralen Datenbank sicherzustellen, braucht der Betreiber entsprechende Zugriffs- und Bearbeitungsrechte. Diese Rechte sind durch die Aufgaben des Betreibers, nämlich die Sicherstellung der technischen Funktionsfähigkeit, begrenzt. Darüber hinaus-

gehende Zugriffs- oder Bearbeitungsrechte stehen dem Betreiber nicht zu. Zusammenfassend ist also der *Betreiber* der Akteur, welcher aus datenschutzrechtlicher Sicht neu zum Inhaber einer Datensammlung, zum Organ und zur betroffenen Person hinzutritt. Struktur und Aufbau zentraler Datenbanken einerseits sowie das bestehende Datenschutzrecht andererseits lassen es als sinnvoll erscheinen, als neuen Akteur den Betreiber einzusetzen.

d. Kontrollrechte der betroffenen Person

Damit ist auch die Frage, wer auskunftspflichtiger Datenherr eines Datenwarenhauses (data warehouse) ist, einfach zu beantworten. Es ist davon auszugehen, dass jede Person nach Datenschutzrecht das Recht haben muss, zu erfahren, welche Daten über sie in einem Datenwarenhaus gespeichert sind. Sodann hat jedes Organ nur auf jene Daten Zugriff, die es gestützt auf eine gesetzliche Grundlage bearbeiten darf. Der an und für sich mögliche Ansatz, eine zentrale Anlaufstelle (z. B. Datenschutzbeauftragter oder Betreiber) zu schaffen, welche Zugriff auf sämtliche in einem Datenwarenhaus gespeicherten Daten einer Person hätte und über alle diese Daten Auskunft geben würde, ist jedoch zu verwerfen: Dies wäre nämlich nicht zweckdienlich, weil zum Beispiel ein Ausdruck dieser oftmals abstrakten Daten ohne Kommentar des zugriffsrespektive bearbeitungsberechtigten Organs der betroffenen Person möglicherweise wenig nützen würde. Dennoch soll auch die betroffene Person von den Vorteilen der zentralen Datenhaltung profitieren können und nicht «blind» bei allen möglichen Dienststellen das Vorhandensein von Personendaten über sie nachfragen müssen. Es soll deshalb zwar eine zentrale Stelle geschaffen werden, welche die Berechtigung hat, in allen Datenwarenhäusern, an welchen ein Gemeinwesen beteiligt ist – darüber wird ein Register geführt – nachzuprüfen, ob Personendaten über die betroffene Person gespeichert sind, und welches Organ Zugriffs- oder Bearbeitungsrechte dazu hat. Als Anlaufstelle bietet sich die zuständige Aufsichtsstelle für den Datenschutz an. Diese klärt mit Unterstützung des Betreibers ab, ob im fraglichen Datenwarenhaus Personendaten über die betroffene Person vorhanden sind und welche Organe Zugriffs- oder Bearbeitungsrechte dafür haben. Dies wird die zuständige Aufsichtsstelle für den Datenschutz der betroffenen Person mitteilen, worauf sich diese im ordentlichen Verfahren an die entsprechenden Organe wenden kann. Die zuständige Aufsichtsstelle für den Datenschutz darf diese Auskunft aus überwiegenden öffentlichen Interessen oder überwiegenden privaten Interessen Dritter oder der betroffenen Person einschränken, mit Auflagen versehen oder verweigern (analog § 16 DSG). Im Sinn eines Dienstes am Bürger sehen wir vor, dass die zuständige Aufsichtsstelle für den Datenschutz das Verfahren bei den entsprechenden Organen direkt einleitet. Dies kann helfen, Schwellenängste abzubauen, und verleiht der Anfrage einer betroffenen Person mehr Gewicht, womit der Datenschutz gestärkt wird. Am weiteren Verfahren ist die zuständige Aufsichtsstelle für den Datenschutz aber nicht mehr beteiligt, dieses spielt sich direkt zwischen der betroffenen Person und den Organen gemäss den im Datenschutzgesetz vorgesehenen Regeln ab.

§ 5

In *Absatz 1* wird eine generelle Erlaubnis für die Errichtung zentraler Datenbanken statuiert. Der Vorbehalt des Datenschutzrechtes geht insbesondere dahin, dass zentrale Datenbanken, in welchen besonders schützenswerte Personendaten oder Persönlichkeitsprofile gespeichert werden, einer formellen gesetzlichen Grundlage in der Spezialgesetzgebung bedürfen. Eine solche besteht zum Beispiel bereits in § 135 des Steuergesetzes. Umgekehrt bedeutet dies, dass zentrale Datenbanken, die bloss einfache Personendaten enthalten, keiner formellen gesetzlichen Grundlage bedürfen, sondern sich lediglich an die vorliegenden Vorschriften des Informatikgesetzes zu halten haben. Dieser Ansatz kann als ausgesprochen praxisnah bezeichnet werden und ist daher in der Form der ausdrücklichen Erlaubnis gesetzlich zu verankern.

Der Vorbehalt des Datenschutzrechtes bezieht sich selbstverständlich auch auf die datenschutzrechtlichen Grundsätze. So dürfen beispielsweise Personendaten gemäss § 4 Absatz 4 DSG nicht für einen Zweck bearbeitet werden, der nach Treu und Glauben mit dem Zweck unvereinbar ist, für den sie ursprünglich beschafft oder der Behörde bekannt gegeben worden sind. Das Bearbeiten von Personendaten muss zudem gemäss § 4 Absatz 3 DSG verhältnismässig sein. Sodann sind Personendaten, sofern es der Zweck des Bearbeitens zulässt (wissenschaftliche Forschung, Führung von Statistiken und dergleichen), gemäss § 4 Absatz 5 DSG so zu anonymisieren, dass die betroffene Person nicht mehr bestimmt oder bestimmbar ist. All dies gilt ohne weiteres auch für die elektronische Bearbeitung von Personendaten und somit für zentrale Datenbanken und Abrufverfahren. Die Umsetzung dieser Prinzipien ist eine organisatorische und technische Frage.

Absatz 2: Wie bereits zu Absatz 1 erwähnt, bedürfen zentrale Datenbanken, welche bloss einfache Personendaten enthalten, keiner formellen gesetzlichen Grundlage. Um dennoch einen angemessenen Schutz dieser Personendaten zu gewährleisten, wird hier eine Leistungsvereinbarung gefordert, die mindestens die im Gesetz aufgeführten Punkte regeln soll. Die zuständige Behörde genehmigt diese Leistungsvereinbarung. Die zuständige Behörde wird gemäss § 21 vom Regierungsrat bestimmt; die Gemeinden bestimmen ihre zuständige Behörde selber. Sind mehrere Organe beteiligt, gilt diese Vorschrift für jedes Organ. Ein solches Verfahren ist wesentlich einfacher und rascher durchführbar als die Errichtung einer formellen gesetzlichen Grundlage. Weil es sich um einfache Personendaten handelt, vermag es in datenschutzrechtlicher Hinsicht dennoch zu genügen. Die Vorschrift gilt aber selbstverständlich auch für zentrale Datenbanken, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthalten.

Mit *Absatz 3* wird die Grundlage geschaffen, zentrale Datenbanken, welche besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthalten, während einer befristeten Testphase *ohne formelle gesetzliche Grundlage* zu betreiben. Damit wird einem in der Praxis verbreiteten Bedürfnis entsprochen, kollidiert doch die Notwendigkeit effizienten Verwaltungshandelns häufig mit der relativ langen Dauer eines Gesetzgebungsverfahrens. Als Voraussetzungen gefordert werden *(Unterabs. a)* eine formelle gesetzliche Grundlage für die zu erfüllende Aufgabe, *(Unterabs. b)* ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen und *(Unterabs. c)* die Dringlichkeit der Testphase. Die Vorschrift stellt gemessen am

geltenden Recht eine Erleichterung für die Verwaltung dar, wobei die Anliegen des Datenschutzes angemessen berücksichtigt werden; sie orientiert sich am Entwurf für die Revision des Datenschutzgesetzes des Bundes, ist aber einfacher ausgestaltet. Sofern nur Organe des kantonalen Gerichtswesens an der zentralen Datenbank beteiligt sind, ist gemäss *Unterabsatz d* die Bewilligungskompetenz des Regierungsrates unter Beachtung des Gewaltenteilungsprinzips von der Zustimmung des betreffenden obersten Gerichtes abhängig.

§ 6

Mit dieser Vorschrift werden dem Betreiber einer zentralen Datenbank die sachgerechten Rechte eingeräumt und entsprechende Pflichten auferlegt. Diese beschränken sich grundsätzlich auf den technischen Betrieb und die technische Sicherheit; dies im Gegensatz zu den inhaltlichen Aspekten der Datensammlung, wofür die jeweiligen Inhaber der Datensammlung verantwortlich bleiben *(Abs. 1; vgl. Vorbemerkungen, Kap. c)*. Dabei ist unerheblich, ob der Betreiber ein an der zentralen Datenbank beteiligtes Organ ist oder nicht *(Abs. 2)*. Zugriffs- und Bearbeitungsrechte stehen dem Betreiber nur insoweit zu, als er sie für die Aufrechterhaltung des technischen Betriebs und der technischen Sicherheit benötigt. Um zu verhindern, dass sich in einer einzigen Person eine allzu grosse Macht über die zentrale Datenbank konzentriert, wird mit der Trennung der Systemadministration und der Zugriffsverwaltung das Vieraugenprinzip stipuliert *(Abs. 3)*. Der damit verbundene Mehraufwand, auf den die Gerichte hinweisen, rechtfertigt sich durch das grosse Gefahrenpotenzial; er dürfte sich zudem insofern in Grenzen halten, als Betreiber zentraler Datenbanken in der Regel über genügend Personal verfügen dürften, um das Vieraugenprinzip ohne nennenswerten Aufwand umzusetzen. Der Betreiber und seine Hilfspersonen sind zur Verschwiegenheit verpflichtet *(Abs. 4)*. Gemäss § 23 Absatz 1 stellt eine diesbezügliche Pflichtverletzung einen Straftatbestand dar.

Absatz 5: Die hier vorgeschlagene Lösung kollidiert mit § 6 Absatz 3 DSG (vgl. Vorbemerkungen Kap. b–d). Diese Norm ist daher für zentrale Datenbanken ausser Kraft zu setzen. Dennoch sind Konstellationen, in denen diese Norm zur Anwendung gelangt, nach wie vor denkbar. Sie sollte daher beibehalten werden.

§ 7

Absatz 1: Weil eine zentrale Datenbank die Datensammlungen verschiedener Organe enthält, besteht die Gefahr, dass ein beteiligtes Organ auf Daten zugreifen und diese bearbeiten könnte, die es zur Erfüllung seiner Aufgaben nicht benötigt. Die Vorschrift stellt sicher, dass die Zugriffs- und Bearbeitungsberechtigungen der Organe auch nach der Zusammenführung der Datensammlungen in einer zentralen Datenbank unverändert bleiben. Damit ist auch klar, dass nach wie vor jedes Organ, das Personendaten bearbeitet oder bearbeiten lässt, für den Datenschutz verantwortlich bleibt (§ 6 Absatz 1 DSG). Vorbehalten bleibt die Zugriffs- und Bearbeitungsberechtigung des Betreibers, welche sich auf den technischen Betrieb und die technische Sicherheit beschränkt (vgl. Ausführungen zu § 6).

Absatz 2: Datenwarenhäuser bergen die Gefahr, dass Personendaten gespeichert bleiben, obwohl der Zweck ihrer Bearbeitung hinsichtlich aller an dem Datenwaren-

haus beteiligten Organe dahingefallen ist. Um zu verhindern, dass auf diese Weise ungerechtfertigterweise riesige Ansammlungen von Personendaten entstehen, sollten diese Daten aus datenschutzrechtlichen Gründen gelöscht werden. Dies muss speziell geregelt werden, weil sich § 13 DSG auf ganze Datensammlungen, nicht jedoch auf einzelne Daten bezieht und dazu auch den Umstand nicht berücksichtigt, dass ein anderes am Datenwarenhaus beteiligtes Organ die Personendaten noch benötigen könnte. In Einklang mit dem neuen Archivgesetz[4] (§§ 6, 8), welches am 1. Januar 2004 in Kraft trat, dürfen die Daten allerdings nur dann gelöscht werden, wenn sie dem zuständigen Archiv angeboten und von diesem als nicht archivwürdig eingestuft worden sind.

§ 8

Das Vorgehen bei der Erhebung von Personendaten ist in § 8 DSG geregelt. Um zu verhindern, dass verschiedene Organe dieselben Daten erheben müssen, die dann doch im selben Datenwarenhaus gespeichert werden, sieht diese Vorschrift – im Sinn des wirtschaftlichen Einsatzes staatlicher Mittel – vor, dass die verschiedenen Organe die Daten auch gemeinsam erheben können. Dabei ist allerdings die Transparenz gegenüber den betroffenen Personen zu wahren: Sie müssen – zusätzlich zu den in § 8 DSG vorgesehenen Anforderungen – auf die Speicherung der Daten in einem Datenwarenhaus und auf die daran beteiligten Organe hingewiesen werden.

In der Praxis ist etwa bei einem Datenwarenhaus für Steuerdaten des Kantons und der Gemeinden ein Aufdruck auf der Steuererklärung denkbar: «Die mit vorliegender Steuererklärung erhobenen Daten werden im kantonalen Datenpool gespeichert. Am kantonalen Datenpool sind die Steuerverwaltungen des Kantons Luzern und der Gemeinden (...) beteiligt.» In der heutigen Ausgestaltung stellt der Datenpool für Steuerdaten des Kantons und der Gemeinden allerdings kein Datenwarenhaus dar, sondern eine Datendrehscheibe. Der § 8 des Informatikgesetzes braucht daher vorläufig nicht beachtet zu werden. Dies wird sich ändern, sobald der «Datenpool» eine Ausgestaltung als Datenwarenhaus im Sinn dieses Gesetzes erfährt.

§ 9

Um den Anliegen des Datenschutzes möglichst entgegenzukommen, soll die Datenschutzfreundlichkeit der Technologien bei der Beschaffung von Informatikmitteln für zentrale Datenbanken berücksichtigt werden. Es handelt sich dabei um eine Verstärkung des ohnehin geltenden Grundsatzes, dass Informatikmittel nicht zur Verletzung des Datenschutzes führen dürfen. Eine solche Regelung rechtfertigt sich angesichts der erhöhten Gefährdung der Persönlichkeitsrechte durch zentrale Datenbanken. Der Einbezug der Angemessenheit bedeutet, dass der Datenschutz bei der Beschaffung von Informatikmitteln nicht das einzige, sondern eines von mehreren Kriterien ist und dass dieser Grundsatz insbesondere im Rahmen der verfügbaren Mittel zu berücksichtigen ist. Die gesetzliche Regelung bezweckt nicht zuletzt, die Anbieter zu motivieren, datenschutzfreundliche Technologien zu entwickeln.

[4] SRL Nr. 585, G 2003 275 ff.

Technologien werden im Allgemeinen als datenschutzfreundlich gelten, wenn sie die Grundsätze und Ziele des Datenschutzes nicht nur einhalten, sondern aktiv unterstützen. Dazu gehören insbesondere die Datensicherheit, die Verhältnismässigkeit und Zweckgebundenheit des Bearbeitens, die Zugriffs- und Bearbeitungsberechtigungen, die Anonymisierung sowie die Archivierung beziehungsweise Löschung nicht mehr benötigter Daten (vgl. Erläuterungen zu § 7).

§ 10

Absatz 1: Entsprechend der Bedeutung von Datenwarenhäusern wird eine Publikationspflicht im Kantonsblatt mit den wichtigsten Angaben gefordert. Dabei wird der Betreiber in die Pflicht genommen. Die Missachtung dieser Bestimmung stellt einen Straftatbestand gemäss § 23 dar. Zweck ist die Information der Bevölkerung sowie die in Absatz 2 normierte Aufklärung über deren Kontrollrechte gemäss § 11 des Entwurfs (dazu nachstehend) sowie den §§ 14 ff. DSG. Die Begriffe «Organ» und «Datensammlung» richten sich nach dem Datenschutzgesetz.

Absatz 3: Gemäss § 14 DSG führt jedes Gemeinwesen über seine Datensammlungen ein Register. Entsprechend der Bedeutung von Datenwarenhäusern wird hier vorgesehen, dass die zuständige Aufsichtsstelle für den Datenschutz ein Register über die Datenwarenhäuser des Kantons und der Gemeinden führt. Dieses gilt als Anknüpfungspunkt für die Kontrollrechte der betroffenen Person gemäss § 11 des Informatikgesetzes. Die zuständige Aufsichtsstelle für den Datenschutz ist der kantonale Datenschutzbeauftragte für jene Datenwarenhäuser, an welchen sich der Kanton beteiligt. Er ist aber auch zuständig für die Führung des Registers von Datenwarenhäusern, an welche sich die Gemeinden angeschlossen haben, sofern diese keine eigene Aufsichtsstelle für den Datenschutz gemäss § 22 Absatz 3 DSG geschaffen haben.

§ 11

Die Kontrollrechte der betroffenen Person richten sich grundsätzlich nach den §§ 14 ff. DSG. Sie werden hier sachgemäss auf die Datenwarenhäuser ausgedehnt (vgl. Vorbemerkungen, Kap. d). Sachgemäss und bürgernah wird als Anlaufstelle – wie für die Registerführung gemäss § 10 Absatz 3 – die zuständige Aufsichtsstelle für den Datenschutz bestimmt.

Wer der in *Absatz 2* genannte Informatikverantwortliche ist, richtet sich nach der Linie innerhalb eines am Datenwarenhaus angeschlossenen Organs. Auf der Ebene des Kantons ist dies in der Informatikverordnung geregelt.

Hinsichtlich *Absatz 4* schlägt die SP im Sinn der Bürgerfreundlichkeit vor, dass der Zugriff unterstützt werden müsse und wenn möglich zentral erfolgen sollte. Diese Anregung wird jedoch nicht aufgenommen, denn technisch würde dies eine Einbindung des Betreibers bedeuten. Dies würde dem Bürger und der Bürgerin aber weniger helfen als die Einbindung jener Organe, welche die Personendaten der betroffenen Person bearbeiten.

§ 12

Bei Abrufverfahren werden nicht, wie in zentralen Datenbanken, die Datensammlungen verschiedener Organe zusammengeführt, sondern es handelt sich um automatisierte Verfahren, welche es Dritten ermöglichen, Personendaten ohne Intervention

des bekannt gebenden Organs zu bearbeiten (§ 3 Abs. 7). In der Praxis sind Abrufverfahren von zentralen Datenbanken jedoch insofern kaum zu unterscheiden, als sie diesen technisch und organisatorisch oft sehr nahe kommen. Dies gilt entsprechend für ihr Gefährdungspotenzial bezüglich Persönlichkeitsrechten. Abrufverfahren sollen daher in der rechtlichen Behandlung den zentralen Datenbanken gleichgestellt werden. Wegen des im Vergleich mit Datenwarenhäusern insgesamt doch geringeren Gefährdungspotenzials rechtfertigt sich der Aufwand der Registerführung und der Publikation im Kantonsblatt jedoch nicht.

Vorbemerkungen zu den Bestimmungen über die Auslagerung

Wie in der Privatwirtschaft kann es auch in der Verwaltung gestützt auf den Grundsatz des effizienten und kostengünstigen Verwaltungshandelns angezeigt sein, Informatikdienstleistungen auszulagern. Das Erbringen von Informatikdienstleistungen innerhalb der Verwaltung fällt grundsätzlich unter das allgemeine Verwaltungshandeln. Indessen handelt es sich um eine Unterstützung der Verwaltungstätigkeit, die nicht direkt an Individuen gerichtet ist. Insofern können Informatikdienstleistungen ohne weiteres ausgelagert werden. Insoweit Informatikdienstleistungen also nur mittelbar der Erfüllung öffentlicher Aufgaben dienen, ist für deren Auslagerung eine formelle gesetzliche Grundlage nicht erforderlich. Hingegen begibt sich die Verwaltung mit der Auslagerung gegebenenfalls in ein Abhängigkeitsverhältnis zu einem Auslagerungspartner. Daraus ergibt sich eine mögliche Gefährdung der ordentlichen Aufgabenerfüllung durch das auslagernde Organ. Problematisch kann aber auch etwa der Umgang mit Amts- und Spezialgeheimnissen und mit dem Datenschutz sein, insbesondere auch hinsichtlich der Kontrollrechte der betroffenen Personen. Der Umgang mit Daten kann Private in ihren Rechten verletzen. Der Entscheid darüber, wer mit Daten umgehen kann, bedarf einer genügenden demokratischen Legitimation[5]. Zudem sind Auslagerungsvorhaben meist für die Informatikorganisation des Kantons bedeutsam oder gar kantonsweit von strategischem Interesse. Diese Problemkreise erfordern, dass die Auslagerung von Informatikdienstleistungen einheitlichen Regeln unterworfen wird[6].

Der Entwurf orientiert sich, bei allerdings geringerer Regelungsdichte, an der Regelung des Kantons Zürich, der sich in der Praxis bewährt hat[7]. Die Bestimmungen über die Auslagerung sind nur auf die kantonale Verwaltung und die Gerichte anwendbar (§ 2 des Entwurfs). Dass die Zulässigkeit der Auslagerung von der unterschiedlichen Sensibilität der Daten abhängig gemacht werden soll, wie die IGGI und jene Gemeinden, die sich ihrer Stellungnahme angeschlossen haben, vorschlagen, erscheint uns nicht zweckmässig, weil mit unterschiedlicher Sensibilität der Daten auch die Anforderungen an die Sicherheit entsprechend steigen.

[5] Tobias Jaag, Dezentralisierung und Privatisierung öffentlicher Aufgaben, Zürich 2000, S. 40.

[6] Ausführlich: Rolf H. Weber, Outsourcing von Informatikdienstleistungen in der Verwaltung, in: ZBl. 2/1999; ders., IT-Outsourcing: Praxis und Rechtsfragen, in: Jusletter vom 23. März 2003.

[7] Gesetz über die Auslagerung von Informatikdienstleistungen vom 23. August 1999; Allgemeine Geschäftsbedingungen des Kantons Zürich über die Geheimhaltung, den Datenschutz und die Daten- und Informationssicherheit bei der Erbringung von Informatikdienstleistungen vom September 2001.

§ 13
Absatz 1 stellt klar, dass die Auslagerung von Informatikdienstleistungen nebst vorliegendem Entwurf keiner formellen gesetzlichen Grundlage bedarf. Allerdings werden die datenschutzrechtlichen sowie die Regelungen dieses Gesetzes vorbehalten, also insbesondere auch jene über die Informatiksicherheit sowie gegebenenfalls jene über die zentralen Datenbanken, die Abrufverfahren und die Informatikorganisation. Beachtlich bleiben auch die finanzrechtlichen Bestimmungen.

Absatz 2 verpflichtet die Auslagerungspartner zur Regelung der wichtigsten Punkte (vgl. Vorbemerkungen).

Absatz 3 geht davon aus, dass trotz Auslagerung die Verantwortung für die Erfüllung ihrer Aufgabe grundsätzlich beim auslagernden Organ verbleibt. Dieses hat mit organisatorischen und technischen Massnahmen dafür zu sorgen, dass etwa ein Konkurs oder allfälliges regelwidriges Verhalten des Auftragnehmers nicht dazu führen kann, dass die Erfüllung seiner Aufgaben dadurch wesentlich beeinträchtigt wird. Denkbar sind etwa die Hinterlegung des Quellcodes einer Softwarelösung bei einem Dritten und ähnliche Massnahmen.

§ 14
Auslagerungsvorhaben sind für die kantonale Informatikorganisation regelmässig von Interesse und sind daher der gemäss § 21 zuständigen Behörde zu melden. Übergeordnete oder strategische Auslagerungsvorhaben sind auf Stufe der Konzern-Informatik (vgl. § 17) anzusiedeln und sollten, analog der Zuweisung bestimmter Aufgaben zur Konzern-Informatik gemäss Informatikverordnung, vom Regierungsrat genehmigt werden.

§ 15
Absatz 1: Um die Einhaltung der Amts-, Berufs- und Geheimhaltungspflichten sowie die Einhaltung der datenschutzrechtlichen Bestimmungen und jener über die Informatiksicherheit sicherzustellen, ist deren Anwendungsbereich von Gesetzes wegen auf die Auftragnehmer auszudehnen. Die Missachtung dieser Bestimmung stellt gemäss § 23 Absatz 1 einen Straftatbestand dar.

Absatz 2: Damit die Einhaltung der Verpflichtungen des Auftragnehmers kontrolliert werden kann, muss für das auslagernde Organ, die zuständige Behörde für den Datenschutz sowie die Finanzkontrolle der Zugang zu dessen Räumen und Anlagen gewährleistet sein, und es müssen ihnen die erforderlichen Zugriffsrechte gewährt werden. Der Auftragnehmer hat sie dabei zu unterstützen. Die Unterstützung muss angemessen sein, was bedeutet, dass sie sich in Art und Umfang am tatsächlichen Bedarf zu orientieren hat.

§ 16
Absatz 1 schreibt vor, dass die Verantwortung für den Datenschutz beim auslagernden Organ verbleibt und somit nicht an den Auftragnehmer übertragen werden kann. Nichtsdestotrotz wird der Auftragnehmer gemäss § 15 Absatz 1 verpflichtet, die datenschutzrechtlichen Bestimmungen einzuhalten.

Absatz 2: Entsprechend dem in Absatz 1 verankerten Grundsatz bleibt das auslagernde Organ Ansprechpartner für betroffene Personen bei der Ausübung ihrer Kontrollrechte. Der Auftragnehmer hat sich jeder materiellen Behandlung der Begehren zu enthalten.

§ 17

Mit dieser Vorschrift wird eine bessere gesetzliche Grundlage für die Informatikverordnung (SRL Nr. 39) geschaffen, deren Grundzüge sie enthält. Dem Regierungsrat verbleibt ein angemessener Handlungsspielraum für seine Verordnungskompetenz.

Absatz 1: Gemäss § 7 Absatz 1 der Informatikverordnung sind die Departemente, die Staatskanzlei, das Obergericht und das Verwaltungsgericht für die Informatik verantwortlich («Departements-Informatik»). Gemäss § 7 Absatz 2 in Verbindung mit § 10 der Informatikverordnung weist der Regierungsrat Aufgaben von übergeordnetem oder strategischem Interesse der Konzern-Informatik zu. Dieses Interesse kann verschiedener Natur sein. Im Vordergrund stehen einheitliche Lösungen, welche regelmässig erhebliches Einsparungspotenzial bergen und durch Kompatibilität die Kommunikation und den Datenaustausch erleichtern. Auch die Informatiksicherheit kann zentral besser gesteuert werden. Alle Belange, die der Regierungsrat nicht in diesem Sinn der Konzern-Informatik zugewiesen hat, fallen unter die Departements-Informatik.

In *Absatz 2* erhält der Regierungsrat die Organisationskompetenz für die Informatikorganisation. Diese ist in der Informatikverordnung geregelt. Danach sind Informatikorgane insbesondere die Informatikkommission, der oder die Informatikgesamtverantwortliche, die Organisations- und Informatikdienste, die Organisations- und Informatikbeauftragten, die Dienststellen und die Gerichte sowie die Informatik-Kompetenzzentren. Weil sich diese Organisation auf Belange der als Ressource verstandenen Informatik beschränkt, wird die Gewaltenteilung davon nicht berührt; die Unabhängigkeit der Gerichte bleibt gewahrt.

Absatz 3: Das Obergericht und das Verwaltungsgericht weisen zu Recht darauf hin, dass der Ausdruck «Departements-Informatik» im Grunde genommen falsch ist, weil auch die Gerichte unter diesen Begriff fallen. Die korrekte Bezeichnung wäre «Departements- und Gerichtsinformatik». Allerdings wird dieser Begriff seiner Länge wegen in der Praxis nicht verwendet. Aus diesem Grund wurde auch in der geltenden Informatikverordnung der Begriff «Departements-Informatik» verwendet. Im Informatikgesetz halten wir an dieser Terminologie fest. Allerdings soll mit dieser Norm klargestellt werden, dass innerhalb der Departements-Informatik die Organisation den Departementen und den Gerichten selbst obliegt. Damit wird auch den Anliegen der FDP-Frauen Rechnung getragen, die auf die eigene Organisationskompetenz der Gerichte hinweisen.

Vorbemerkung zu den Bestimmungen über die Informatiksicherheit

Diese Bestimmungen gelten für die Gemeinden und andere Stellen nur, soweit sie Informatikmittel des Kantons benutzen (§ 2).

§ 18

Mit dieser Norm werden die Inhaber von Datensammlungen sowie die Betreiber zentraler Datenbanken hinsichtlich der Informatiksicherheit in die Pflicht genommen. Sie werden dabei von den Organen der Informatik unterstützt. Im Gegensatz zu § 20, wo die Anwendungsverantwortung geregelt wird, geht es hier um Systemschutz. Gegenstand der Sicherheitsvorkehren sind die Informatikmittel – und damit die darin enthaltenen Daten – hinsichtlich der Gefahren des Verlustes und unerwünschter Einwirkungen und Personendaten hinsichtlich unbefugten Zugriffs und Bearbeitens.

§ 19

Absatz 1: Das vorgesehene dreistufige Verfahren (Klassifizierung der Daten und der Informatikmittel; Festlegen der Schutzziele; Erstellen eines Massnahmenplans) stellt einen pragmatischen Ansatz zur Verwirklichung der Informatiksicherheit dar, welcher auch in der privatwirtschaftlichen Praxis Verwendung findet. Die im Kanton Zürich getroffene Lösung verfolgt einen ähnlichen Ansatz.

Die Klassifizierung der Daten und der Informatikmittel kann etwa nach den Kriterien Vertraulichkeit, Datenschutz, Integrität und Authentizität, Archivierung, Verfügbarkeit, Wert und Wiederbeschaffung erfolgen. Dabei werden diese Kriterien nach Stufen gegliedert. Gestützt darauf werden die Schutzziele festgelegt. Der Massnahmenplan schliesslich enthält die zu treffenden Massnahmen unter Berücksichtigung der verfügbaren Mittel, die Verantwortlichkeiten sowie die Umsetzungsschritte und die Termine.

Absatz 2: Um die Informatiksicherheit zu gewährleisten, sind periodische Kontrollen notwendig. Dabei kann es sich um interne oder externe Kontrollen handeln. Die Periodizität der Kontrollen soll sich nach dem Einzelfall richten und wird deshalb offen gelassen.

Absatz 3: Auf Gesetzesstufe sollen nur die Grundzüge der Informatiksicherheit verankert werden.

§ 20

Mit dieser Bestimmung soll eine bessere gesetzliche Grundlage für die seit 1. Januar 2003 in Kraft stehende Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz (SRL Nr. 38c) geschaffen werden, deren Grundzüge sie enthält. Die Überwachungsmassnahmen können einen Eingriff in das Recht der Persönlichkeit darstellen (Informationsfreiheit) und bedürfen einer gesetzlichen Grundlage. Dem Regierungsrat verbleibt ein angemessener Handlungsspielraum hinsichtlich seiner Verordnungskompetenz. Die missbräuchliche Verwendung von Informatikmitteln am Arbeitsplatz stellt gemäss § 23 Absatz 1 einen Straftatbestand dar. Dieser Thematik fehlt es nicht an Aktualität (vgl. Anfrage A 751 von Gerhard Klein über Kinderpornografie im Internet).

§ 21

In § 5 Absatz 2 wird die Leistungsvereinbarung, welche die an einer zentralen Datenbank angeschlossenen Organe mit dem Betreiber abzuschliessen haben, von der Genehmigung der zuständigen Behörde abhängig gemacht. Dasselbe gilt für die Verein-

barung, die anlässlich der Auslagerung einer Informatikdienstleistung vom auslagernden Organ mit dem Auftragnehmer abzuschliessen ist (§ 14 Abs. 2). Wer diese zuständige Behörde ist, bestimmt der Regierungsrat. Auf Gemeindeebene wird vorgesehen, dass der Gemeinderat die zuständige Behörde bestimmen soll; dies im Einklang mit dem Entwurf eines neuen Gemeindegesetzes, insbesondere § 10 Unterabsatz b Ziffer 3.

§ 22

Datenschutzgesetz: Die Vorschriften im Datenschutzgesetz über die Kontrollrechte der betroffenen Person sollten um einen Verweis auf die entsprechenden Spezialbestimmungen erweitert werden, um dem Rechtsuchenden eine Orientierungshilfe zu bieten. Die materielle Regelung der Kontrollrechte hinsichtlich zentraler Datenbanken sollte dagegen im Informatikgesetz und nicht im Datenschutzgesetz erfolgen, um die Bestimmungen über die zentralen Datenbanken nicht zu verzetteln.

Gesetz über die Kantonspolizei: Das Justiz- und Sicherheitsdepartement regt in seiner Stellungnahme die Änderung des Gesetzes über die Kantonspolizei an. Damit soll die formelle gesetzliche Grundlage für ein Abrufverfahren gemäss § 12 des Entwurfs geschaffen werden. Die vorgeschlagene Regelung entspricht im Wortlaut dem § 6a der Vollziehungsverordnung zum Gesetz über das Niederlassungswesen vom 1. Dezember 1948 (SRL Nr. 6), welchen wir durch Änderung vom 2. September 2003, in Kraft seit dem 1. Oktober 2003 (G 2003 293), in diese Verordnung eingefügt haben. Wir übernehmen diese Anregung, da die genannte Verordnungsbestimmung aus rechtsstaatlichen Gründen bloss als Übergangslösung taugt.

Es gibt diverse Situationen, in denen die Dienst tuenden Polizistinnen und Polizisten ausserhalb der Öffnungszeiten der Einwohnerkontrollen auf Personalien von Bürgerinnen und Bürgern dringend angewiesen sind. Diese Situationen sind auch massgebend dafür, welche Personendaten für die Polizei online einsehbar sein sollen. Es handelt sich bei diesen Situationen vorwiegend um Vorfälle (z.B. Unfälle, Festnahmen, Anhalten verwirrter Personen), in denen möglichst rasch Angehörige oder z. T. auch Dolmetscher benachrichtigt oder herbeigezogen werden müssen. Es kann aber auch darum gehen, an den Schweizer Grenzen eine Alarmfahndung auszulösen, wenn ein ausländischer Straftäter über die Grenze in sein Heimatland zu flüchten versucht. Heute erhält die Kantonspolizei diese Daten von den Gemeinden aus den Karteien, wobei deren Aktualität und Verwaltung immer wieder zu Problemen und vor allem telefonischen Nachfragen führt. Diese Situation ist für die Gemeinden wie für die Polizei mit personellem Aufwand verbunden. Im Rahmen eines Pilotversuchs besteht zurzeit bei gewissen Gemeinden für die Polizei die Möglichkeit der elektronischen Datenabfrage. Verschiedene Gemeinden haben grössere Investitionen getätigt, damit die Polizei die Daten elektronisch abfragen kann und nicht mehr auf die Gemeindeangestellten angewiesen ist.

§ 23

Absatz 1: Die Missachtung zentraler Bestimmungen dieses Gesetzes, die ein hohes Potenzial an Gefährdungen der Persönlichkeitsrechte, des Amts- oder Berufsgeheimnisses oder anderer Geheimnisse oder der staatlichen Aufgabenerfüllung enthalten, stellt einen Straftatbestand dar (vgl. die Ausführungen zu den betreffenden Bestim-

mungen). Der Strafrahmen orientiert sich an vergleichbaren Tatbeständen im Verwaltungsstrafrecht. Gemäss Artikel 335 StGB sind die Kantone zum Erlass von Verwaltungsstrafrecht befugt.

Absatz 2: Die detaillierte Umschreibung des strafbaren Verhaltens bei der Benutzung von Informatikmitteln am Arbeitsplatz würde den gesetzlichen Rahmen sprengen. Dies wird daher dem Regierungsrat als Verordnungsgeber zu dieser Thematik überlassen (vgl. die Ausführungen zu § 20 und die Verordnung über die Benutzung von Informatikmitteln am Arbeitsplatz, SRL Nr. 38c). Eine analoge Delegation der Rechtsetzungsbefugnis im Bereich von Strafrechtsnormen findet sich etwa im Volksschulbereich (§ 63 des Gesetzes über die Volksschulbildung [SRL Nr. 400a] und § 18 der Verordnung zum Gesetz über die Volksschulbildung [SRL Nr. 405]).

Absatz 3: An die Stelle der Strafe kann als Massnahme Datenschutzunterricht treten. Weil zu erwarten ist, dass die damit verfolgten spezialpräventiven Ziele nur erreicht werden können, wenn die Fehlbaren in die Massnahme einwilligen, wird dies gesetzlich verankert.

Absatz 4: Angesichts der beschränkten Ressourcen des oder der Beauftragten für den Datenschutz wird die Möglichkeit vorgesehen, dass der Datenschutzunterricht durch Dritte erteilt wird. Dass es sich dabei um ausgewiesene Fachpersonen handeln muss, ist selbstverständlich und braucht nicht erwähnt zu werden.

Absatz 5: Gemäss dieser Bestimmung steht der Straftatbestand gemäss Absatz 1 in Idealkonkurrenz zu anderen Straftatbeständen. In Frage kommen etwa Delikte gegen Amts- und Berufspflichten, insbesondere die Verletzung von Geheimhaltungspflichten, aber auch Computerdelikte, Ehrverletzungsdelikte, Vermögensdelikte sowie Delikte gegen die Sittlichkeit oder den Datenschutz.

Sehr geehrter Herr Präsident, sehr geehrte Damen und Herren, wir beantragen Ihnen, dem Entwurf des Informatikgesetzes zuzustimmen.

Luzern, 27. Januar 2004

Im Namen des Regierungsrates
Der Schultheiss: Kurt Meyer
Der Staatsschreiber: Viktor Baumeler

Nr. 26

Informatikgesetz

vom

Der Grosse Rat des Kantons Luzern,

nach Einsicht in die Botschaft des Regierungsrates vom 27. Januar 2004,

beschliesst:

I. Allgemeine Bestimmungen

§ 1 *Zweck*

Dieses Gesetz legt die Organisation der Informatik fest und regelt den Einsatz der Informatikmittel unter Einbezug des Datenschutzes.

§ 2 *Geltungsbereich*

[1] Das Gesetz gilt für die kantonale Verwaltung (einschliesslich Spitäler und kantonaler Schulen) und für die Gerichte. Ausgenommen sind die Ausgleichskasse Luzern, die IV-Stelle Luzern, die Arbeitslosenkasse, die Gebäudeversicherung, die Luzerner Pensionskasse, die im Rahmen eines Konkordats geführten Hochschulen und Fachhochschulen sowie die Universität.

[2] Für die Gemeinden, die in Absatz 1 ausgenommenen Stellen und andere vom Regierungsrat durch Verordnung bezeichnete Stellen gelten die Teile I, II, und VI. Der Teil V ist für sie anwendbar, soweit sie Informatikmittel des Kantons Luzern benutzen.

[3] Der Regierungsrat kann bestimmte Anlagen vom Geltungsbereich dieses Gesetzes ausnehmen.

§ 3 *Begriffe*

[1] Die Begriffe «Personendaten», «besonders schützenswerte Personendaten», «betroffene Person», «Bearbeiten von Personendaten», «Datensammlung», «Inhaber einer Datensammlung» sowie «Organ» richten sich nach dem kantonalen Datenschutzgesetz.

[2] Der Begriff der Informatik umfasst die Steuerung, Planung und Einführung sowie den Betrieb und Unterhalt von Prozessen und Techniken, welche der maschinellen oder maschinell unterstützten Bearbeitung von Informationen aller Art dienen.

[3] Informatikmittel sind Geräte, Einrichtungen und Dienste, wie insbesondere Computersysteme, Computerprogramme, Kommunikationsdienste, die der elektronischen Erfassung, Verarbeitung, Speicherung, Übermittlung, Auswertung, Archivierung oder Vernichtung von Informationen dienen.

[4] Zentrale Datenbanken bestehen aus Datensammlungen verschiedener Organe. Sie können sich an einem beliebigen Ort befinden. Datenwarenhäuser und Datendrehscheiben sind zentrale Datenbanken.

[5] Datenwarenhäuser (data warehouses) dienen der dauerhaften Speicherung von Daten.

[6] In Datendrehscheiben stehen Daten für den Datenaustausch vorübergehend zur Verfügung.

[7] Abrufverfahren sind automatisierte Verfahren, welche es Dritten ermöglichen, Personendaten ohne Intervention des bekannt gebenden Organs zu bearbeiten.

[8] Eine Auslagerung ist das Zurückgreifen eines Organs auf Informatikmittel Dritter zur Erfüllung seiner Aufgaben. Organe innerhalb eines Gemeinwesens gelten nicht als Dritte.

§ 4 *Grundsätze*

[1] Die Informatik unterstützt die Wirtschaftlichkeit und die Wirksamkeit von Geschäfts- und von Lernprozessen.

[2] Der Informatikeinsatz muss wirtschaftlich sein, der Erfüllung der öffentlichen Aufgaben dienen und den Bedürfnissen der Benutzerinnen und Benutzer entsprechen.

[3] Techniken, die geeignet sind, aus Daten oder Personendaten besonders schützenswerte Personendaten oder Persönlichkeitsprofile herzustellen, dürfen nur dann eingesetzt werden, wenn die Voraussetzungen gemäss § 5 Absatz 2 des Datenschutzgesetzes erfüllt sind.

II. Zentrale Datenbanken und Abrufverfahren

§ 5 *Zulässigkeit zentraler Datenbanken*

[1] Die Errichtung und der Betrieb zentraler Datenbanken sind zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden.

[2] Die Errichtung und der Betrieb zentraler Datenbanken setzen eine zwischen den angeschlossenen Organen und dem Betreiber abgeschlossene und durch die zuständigen Behörden genehmigte Leistungsvereinbarung voraus, die mindestens folgende Punkte regelt:

a. Struktur der zentralen Datenbank,
b. Inhalt der Datenbank insbesondere in Bezug auf Personendaten,
c. verwendete Techniken, einschliesslich Entwicklung und Wartung,
d. Zugriffsverwaltung,
e. Sicherheitskonzept,
f. Standort der Hardware,
g. Kontrollrechte und -pflichten,
h. Verantwortlichkeiten,
i. Publikation gemäss § 10.

[3] Der Regierungsrat kann, nachdem er die Stellungnahme des oder der Beauftragten für den Datenschutz eingeholt hat, vor Inkrafttreten eines formellen Gesetzes eine zentrale Datenbank mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen während einer einmaligen befristeten Zeitspanne von höchstens fünf Jahren bewilligen, wenn

a. die Aufgaben, die diese Bearbeitung erforderlich machen, in einem formellen Gesetz geregelt sind,
b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden,
c. die praktische Umsetzung einer Datenbearbeitung vor Inkrafttreten eines formellen Gesetzes zwingend eine Testphase erfordert und
d. die Zustimmung des zuständigen obersten Gerichtes vorliegt für den Fall, dass an der zentralen Datenbank ausschliesslich Organe des kantonalen Gerichtswesens beteiligt sind.

§ 6 *Betreiber*

[1] Der Betreiber einer zentralen Datenbank ist für den technischen Betrieb und die technische Sicherheit zuständig und verantwortlich.

[2] Betreiber kann ein an der zentralen Datenbank beteiligtes Organ, ein Organ der Informatik gemäss § 17 Absatz 2 oder, unter Vorbehalt der Bestimmungen über die Auslagerung, ein Dritter sein.

[3] Dem Betreiber stehen die für die Erfüllung seiner Aufgaben erforderlichen Zugriffs- und Bearbeitungsrechte auf die gespeicherten Personendaten zu. Die Systemadministration und die Zugriffsverwaltung dürfen nicht derselben Person übertragen werden.

[4] Er und jede von ihm mit Aufgaben des Betriebs betraute Person ist über die von ihm wahrgenommenen Personendaten zur Verschwiegenheit verpflichtet.

[5] § 6 Absatz 3 des Datenschutzgesetzes ist auf zentrale Datenbanken nicht anwendbar.

§ 7 *Zugriffsverwaltung und Löschung der Personendaten*

[1] Der Umfang der Zugriffs- und Bearbeitungsberechtigung von Organen auf Personendaten einer zentralen Datenbank bestimmt sich nach Massgabe des Datenschutzgesetzes und ist technisch und organisatorisch auf geeignete Weise sicherzustellen. § 6 Absatz 3 bleibt vorbehalten.

[2] Werden die in einem Datenwarenhaus gespeicherten Personendaten von keinem beteiligten Organ mehr benötigt, sind sie dem zuständigen Archiv zur Übernahme anzubieten. Werden sie vom Archiv als nicht archivwürdig eingestuft, sind sie zu löschen.

§ 8 *Erhebung von Personendaten*

[1] Personendaten, welche in einem Datenwarenhaus gespeichert werden sollen, können für mehrere Organe gemeinsam erhoben werden.

[2] Werden Personendaten, welche in einem Datenwarenhaus gespeichert werden sollen, für mehrere Organe gemeinsam erhoben, so ist die betroffene Person anlässlich der Erhebung auch auf die Speicherung ihrer Personendaten im Datenwarenhaus und auf die daran beteiligten Organe hinzuweisen.

§ 9 *Datenschutzfreundliche Technologien*

Bei der Beschaffung von Informatikmitteln für zentrale Datenbanken ist die Datenschutzfreundlichkeit der Technologien angemessen zu berücksichtigen.

§ 10 *Publikation und Register*

[1] Die Errichtung von Datenwarenhäusern ist vom Betreiber im Kantonsblatt zu publizieren. In der Publikation sind für jedes Datenwarenhaus die daran beteiligten Organe und die entsprechenden Datensammlungen sowie der Betreiber aufzuführen. Ferner hat die Publikation für jede Datensammlung Auskunft zu geben über die Rechtsgrundlage, den Zweck, die Mittel und Verfahren des Bearbeitens, die Art und Herkunft der Personendaten und deren regelmässige Empfänger sowie über das Vorhandensein und den Aufbewahrungsort von Kopien.

[2] In der Publikation sind ferner die Kontrollrechte jeder Person gemäss diesem und dem Datenschutzgesetz anzugeben.

[3] Die zuständige Aufsichtsstelle für den Datenschutz führt ein Register über die Datenwarenhäuser. Das Register enthält die Angaben gemäss Absatz 1.

§ 11 *Kontrollrechte der betroffenen Person*

[1] Jede Person kann bei der zuständigen Aufsichtsstelle für den Datenschutz Auskunft verlangen
a. über den Inhalt des Registers,
b. ob über sie in einem Datenwarenhaus Personendaten gespeichert sind; sie hat sich dabei über ihre Identität auszuweisen.

[2] Die zuständige Aufsichtsstelle für den Datenschutz und der oder die zuständige Informatikverantwortliche prüfen gemeinsam, ob über die betroffene Person im Datenwarenhaus Personendaten gespeichert sind und welchen Organen dafür Zugriffs- oder Bearbeitungsrechte zustehen. Der zuständigen Aufsichtsstelle für den Datenschutz und dem oder der Informatikverantwortlichen stehen die dazu erforderlichen Zutrittsrechte zu den Räumen und Anlagen des Betreibers sowie die erforderlichen Zugriffs- und Bearbeitungsrechte auf im Datenwarenhaus gespeicherte Personendaten zu. Der Betreiber hat ihnen alle für die Prüfung notwendige Unterstützung zu leisten.

[3] Die zuständige Aufsichtsstelle für den Datenschutz gibt der betroffenen Person Auskunft darüber, welche am Datenwarenhaus beteiligten Organe über eine Zugriffs- oder Bearbeitungsberechtigung auf ihre Personendaten verfügen. Die zuständige Aufsichtsstelle für den Datenschutz darf diese Auskunft aus überwiegenden öffentlichen Interessen oder überwiegenden privaten Interessen Dritter oder der betroffenen Person einschränken, mit Auflagen versehen oder verweigern.

[4] Das Verfahren betreffend Auskunft über die über eine betroffene Person vorhandenen Personendaten sowie betreffend Einsicht, Berichtigung und anderen Ansprüchen richtet sich nach dem Datenschutzgesetz. Auf Begehren der betroffenen Person leitet die zuständige Aufsichtsstelle für den Datenschutz bei den Organen, welche über eine Zugriffs- oder Bearbeitungsberechtigung auf ihre Personendaten verfügen, das Verfahren ein.

[5] Die Aufsichtsstellen für den Datenschutz und die Informatikverantwortlichen sind über die von ihnen wahrgenommenen Personendaten zur Verschwiegenheit verpflichtet.

§ 12 *Abrufverfahren*

Teil II dieses Gesetzes ist auf die Errichtung und den Betrieb von Abrufverfahren sinngemäss anwendbar. Vorbehalten bleiben die Vorschriften über Publikation und Register.

III. Auslagerung

§ 13 *Zulässigkeit*

[1] Die Auslagerung von Informatikdienstleistungen ist zulässig, sofern die Vorschriften über den Datenschutz sowie die Bestimmungen dieses Gesetzes eingehalten werden. Die finanzrechtlichen Vorschriften bleiben vorbehalten.

[2] Die Auslagerung setzt eine schriftliche Vereinbarung voraus, die mindestens folgende Punkte regelt:
a. Inhalt der Dienstleistung,
b. Wahrung des Amtsgeheimnisses sowie besonderer Geheimhaltungspflichten,
c. Verantwortlichkeiten,
d. verwendete Techniken, einschliesslich Entwicklung und Wartung,
e. Zugriffs- und Zutrittsrechte,
f. Sicherheitskonzept,
g. Standorte der Hardware und der Datenbearbeitung,
h. Kontrollrechte,
i. Beizug von Dritten,
j. Archivierung.

[3] Das auslagernde Organ stellt durch organisatorische oder technische Massnahmen sowie vertraglich sicher, dass die staatliche Aufgabenerfüllung auch dann ohne wesentliche Beeinträchtigung gewährleistet ist, wenn der Auftragnehmer Abmachungen nicht einhält oder die Geschäftstätigkeit einstellt.

§ 14 *Genehmigungs- und Meldepflicht*

[1] Die Auslagerung von Informatikdienstleistungen von übergeordnetem oder strategischem Interesse bedarf der Genehmigung des Regierungsrates.

[2] Die übrigen Auslagerungsvorhaben sind vorgängig der zuständigen Behörde zu melden.

§ 15 *Pflichten des Auftragnehmers*

[1] Der Auftragnehmer einschliesslich dessen Mitarbeitende und Hilfspersonen muss diejenigen Amts-, Berufs- und besonderen Geheimhaltungspflichten übernehmen sowie die Bestimmungen über den Datenschutz und die Informatiksicherheit einhalten, an welche das auslagernde Organ gebunden ist.

[2] Er hat dem auslagernden Organ, der zuständigen Behörde für den Datenschutz sowie der Finanzkontrolle Zutritt zu den Räumen und Anlagen sowie die erforderlichen Zugriffsrechte auf die entsprechenden Daten zu gewähren und sie angemessen zu unterstützen.

§ 16 *Kontrollrechte der betroffenen Person*

[1] Als Inhaber der Datensammlung gilt das auslagernde Organ.

[2] Werden beim Auftragnehmer Kontrollrechte gemäss Datenschutzrecht geltend gemacht, hat dieser die betroffene Person an das auslagernde Organ zu verweisen und eine materielle Bearbeitung der Begehren zu unterlassen.

IV. Informatikorganisation

§ 17 *Organisationsstruktur*

[1] Die Informatikorganisation des Kantons Luzern besteht aus der Konzern-Informatik und der Departements-Informatik.

[2] Der Regierungsrat bezeichnet die Organe der Informatik und bestimmt deren grundsätzliche Aufgaben, Funktionen und Zuständigkeiten.

[3] Die Departements-Informatik ist Sache der Departemente, der Staatskanzlei sowie der obersten Gerichte.

V. Informatiksicherheit

§ 18 *Zuständigkeit*

[1] Die Informatikmittel sind durch den Inhaber einer Datensammlung beziehungsweise den Betreiber einer zentralen Datenbank gegen Verlust und unerwünschte Einwirkungen zu sichern. Personendaten sind vor unbefugtem Zugriff und unbefugtem Bearbeiten zu schützen.

[2] Die Organe der Informatik unterstützen die Inhaber von Datensammlungen und die Betreiber von zentralen Datenbanken bei der Festlegung und der Umsetzung von Sicherheitsmassnahmen.

§ 19 *Grundsätze*

[1] Die Dienststellen und die Gerichte sowie die Gemeinden und die andern gemäss § 2 Absatz 2 dem Geltungsbereich unterliegenden Stellen klassifizieren die Daten und die Informatikmittel und legen gestützt darauf die Schutzziele fest. Sie erstellen einen Massnahmenplan zur Erreichung der Schutzziele.

[2] Schutzziele und Massnahmenplan sind periodisch zu überprüfen.

[3] Der Regierungsrat regelt das Nähere.

§ 20 *Benutzung von Informatikmitteln am Arbeitsplatz*

[1] Alle Anwenderinnen und Anwender sind für die Benutzung der Informatikmittel im Rahmen der geltenden Rechtsordnung und dieses Gesetzes persönlich verantwortlich. Informatikmittel dürfen nicht in missbräuchlicher Weise benutzt werden.

[2] Der Regierungsrat regelt die Benutzung der Informatikmittel am Arbeitsplatz und bezeichnet die Fälle der missbräuchlichen Benutzung.

[3] Für Kontroll- und Überwachungsmassnahmen gelten die folgenden Grundsätze:
a. Kontroll- und Überwachungsmassnahmen dienen in erster Linie der Überprüfung und der Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit und der Verfügbarkeit der Informatikmittel.
b. Sämtliche Internetzugriffe und der gesamte E-Mail-Verkehr der Anwenderinnen und Anwender werden aufgezeichnet (protokolliert). Der Inhalt der E-Mails darf ohne Zustimmung der betroffenen Anwenderinnen und Anwender nicht gelesen werden.
c. Protokolldaten sind in anonymisierter Form auszuwerten.
d. Personenbezogene Auswertungen sind ausnahmsweise zulässig, sofern die technische Sicherheit, die Funktionsfähigkeit oder die Verfügbarkeit der Informatikmittel ernsthaft gefährdet sind und dies zur Störungsbehebung unumgänglich ist, oder bei begründetem Verdacht auf Missbrauch von Informatikmitteln nach schriftlicher Ankündigung.
e. Technische Überwachungs- und Kontrollinstrumente sowie Filtersperren sind mit Ausnahme so genannter Spionageprogramme zulässig.

[4] Der Regierungsrat regelt das Nähere, insbesondere das Kontrollverfahren. Er kann insbesondere vorsehen, anonymisierte Plausibilitätskontrollen über eine jeweils beschränkte Benutzungsdauer durchführen zu lassen.

VI. Schlussbestimmungen

§ 21 *Zuständige Behörde*

[1] Der Regierungsrat bestimmt die zuständige Behörde gemäss § 5 Absatz 2 und § 14 Absatz 2.

[2] In den Gemeinden bestimmt der Gemeinderat die zuständige Behörde.

§ 22 *Änderung von Erlassen*

Folgende Erlasse werden gemäss Anhang geändert:
a. Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990,
b. Gesetz über die Kantonspolizei vom 27. Januar 1998.

§ 23 *Strafen und Massnahmen*

[1] Wer die Vorschriften der §§ 4 Absatz 3, 6 Absatz 4, 10 Absatz 1 und 15 Absatz 1 verletzt, wird mit Haft oder Busse bis 5000 Franken bestraft.

[2] Der Regierungsrat kann durch Verordnung für Verstösse gegen die Vorschriften von § 20 oder gegen Verordnungsbestimmungen, die gestützt auf diese Bestimmung erlassen werden, Bussen bis zu 3000 Franken vorsehen.

[3] An die Stelle der Strafe kann eine Massnahme treten, sofern der Fehlbare einwilligt. Diese besteht aus einem Datenschutzunterricht auf Kosten des Fehlbaren.

[4] Der oder die Beauftragte für den Datenschutz organisiert den Datenschutzunterricht. Dieser kann durch Dritte erteilt werden.

[5] Vorbehalten bleiben die Bestimmungen des Schweizerischen Strafgesetzbuches.

§ 24 *Inkrafttreten*

Das Gesetz tritt am 1. Januar 2005 in Kraft. Es unterliegt dem fakultativen Referendum.

Luzern,

Im Namen des Grossen Rates
Der Präsident:
Der Staatsschreiber:

Änderung von Erlassen im Zusammenhang mit dem Informatikgesetz (§ 22)

a. Datenschutzgesetz (SRL Nr. 38)

Das Gesetz über den Schutz von Personendaten (Datenschutzgesetz) vom 2. Juli 1990 wird wie folgt geändert:

§ 15 *Absatz 5 (neu)*

[5] Die Kontrollrechte hinsichtlich der in zentralen Datenbanken gespeicherten Personendaten richten sich nach dem Informatikgesetz vom

b. Gesetz über die Kantonspolizei (SRL Nr. 350)

Das Gesetz über die Kantonspolizei vom 27. Januar 1998 wird wie folgt geändert:

§ 4a *Abrufverfahren (neu)*

[1] Die Gemeinden können der Kantonspolizei mit öffentlich-rechtlichem Vertrag das Recht einräumen, die für die Erfüllung ihrer Aufgaben erforderlichen Daten bei der Einwohnerkontrolle elektronisch abzurufen.

[2] Der Zugriff kann auf folgende Daten eingeräumt werden:

a. Name,
b. Vorname,
c. Geschlecht,
d. Beruf,
e. Adresse,
f. Zivilstand,
g. Staatsangehörigkeit,
h. Heimat- und Geburtsort,
i. Angaben zum Zuzug und Wegzug (Datum, Ort),
j. Geburtsdatum,
k. zivilrechtliche Handlungsfähigkeit,
l. Name der Eltern, des Ehegatten und der Kinder,
m. Name des Arbeitgebers oder der Arbeitgeberin.

[3] Folgende Suchkriterien sind zulässig:
a. Name,
b. Name und Vorname,
c. Name und Geburtsdatum,
d. Adresse,
e. Haushaltsübersicht,
f. Suche nach Strassenzügen.

[4] Die Abrufung von Daten wird unter Angabe des Zweckes protokolliert.