Bericht der Aufsichtsstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Die datenbearbeitenden Stellen hatten im Berichtsjahr erstmals die Informationsgesetzgebung anzuwenden. Sie haben das mit Umsicht getan. Einführungsprobleme von unüblicher Tragweite sind ausgeblieben. Die fortschreitende Vernetzung in der elektronischen Datenbearbeitung bringt Sicherheitsrisiken mit sich. Unter anderem von den datenbearbeitenden Stellen eingeholte Berichte haben diese Entwicklung auch für den Kanton Bern bestätigt.

3.1.2 Zusammenarbeit mit dem eidgenössischen Datenschutzbeauftragten

Am 20. Oktober 1995 fand die 2. schweizerische Konferenz der Datenschutzbeauftragten statt. In einer gemeinsamen Resolution verlangten die Teilnehmer, der Bekanntgabe von Fahrzeughaltern über die Telefonnummer 111 und über Videotex sei ein voraussetzungsloses Sperrecht entgegenzusetzen. Sodann sei die Notwendigkeit der Publikation von Fahrzeughalterdaten erneut zu überprüfen. Das voraussetzungslose Sperrecht ist im Kanton Bern für den interessierenden Bereich gegeben.
Unterstrichen wurde anlässlich der Konferenz die Bedeutung der vom eidgenössischen Datenschutzbeauftragten gemachten (und noch zu machenden) Vorgaben betreffend Datensicherheit in der EDV. Der Bericht 1994 der bernischen Datenschutzaufsichtsstelle erwähnte die Problematik betreffend Analysenliste des eidgenössischen Departements des Innern (Aids-Diagnose auf Abrechnungen zuhanden der Krankenkassen). Wie dem 2. Tätigkeitsbericht des eidgenössischen Datenschutzbeauftragten zu entnehmen ist, entschärft die am 15. März 1995 in Kraft getretene neue Liste dieses Problem.

3.1.3 Internationales Recht

Am 13. Dezember hat der Regierungsrat mit seinem Beschluss 3457/95 Weisungen «betreffend Nutzung des kantonalen Bürokommunikationssystems BEMAIL, der Fernwartung und Internetanschlüsse» erlassen. Dieser Beschluss geht davon aus, der Betrieb eines Teilknotens des kantonalen Mail-Systems in Warwick, England erfolge vorläufig weiter (vgl. zu den vom Regierungsrat gemachten Einschränkungen Ziff. 3.4). Vom deutschen Bundesbeauftragten für den Datenschutz in seinem 15. Tätigkeitsbericht zum Betrieb von E-Mail-Systemen abgegebene Empfehlungen bildeten für den Regierungsratsbeschluss eine wesentliche Grundlage. Bei Forschungsprojekten der Universität fällt auf, dass häufig ein internationaler Datenaustausch stattfindet. Im besonders heiklen Bereich der medizinischen Forschung ist zu hoffen, dass die vom eidgenössischen Recht generell gemachten Vorgaben das Problem langfristig lösen helfen. Mit dem zunehmenden Einsatz medizinischer Spitzentechnologie geht ein Bedürfnis nach Fernwartung einher. Fernwartungen medizinischer Geräte im Kanton Bern (mit Zugriff auf Patientendaten) erfolgen auch vom Ausland aus.

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

In der Antwort auf die Interpellation Galli (Optimierung des Datenschutzes) bestätigte der Regierungsrat, die für die Datenschutzaufsicht zur Verfügung stehenden Mittel könnten nicht aufgestockt werden. Dies ziehe unausweichlich nach sich, «dass die sowohl nach kantonalem Datenschutzgesetz als beim Vollzug von Bundesrecht auch gestützt auf das eidgenössische Datenschutzgesetz vorgeschriebene Datenschutzaufsicht nur in einem reduzierten Rahmen stattfinden kann». Zu wiederholen ist daher der Hinweis, die knappen Mittel verpflichteten zu einer besonders sorgfältigen Prioritätensetzung. Die Prioritätenfolge stellt sich wie folgt dar: 1. allgemeine Gesetzgebung vor der Gesetzgebung in Spezialerlassen, 2. Betreuung von Informatikprojekten in der Planungsphase, 3. generelle Weisungen vor Einzelfällen, 4. Beratung und Instruktion vor Inspektion und 5. Einzelprobleme mit vielen Betroffenen vor Fällen mit wenigen Betroffenen und geringer Wiederholungschance. Unverändert ist in allen Bereichen die Bedeutung der Information als Arbeitsmittel zu unterstreichen. Neu erwähnt wird die Betreuung von Informatikprojekten. Im letztjährigen Bericht wurde festgestellt, dass eine Kontrolle gegenüber EDV-Grosssystemen nicht unterlassen werden dürfe. Diese Feststellung gilt uneingeschränkt weiter. Auch korrekt geplante Informatikanwendungen können zu problematischen Ergebnissen führen. Ein Beispiel hierzu liefert der Einsatz des Systems KOFINA (Finanzverwaltung) bei der Ordnungsbussenzentrale: um nicht mehrere Debitorennummern zuteilen zu müssen, registriert das System die unter einer bestimmten Fahrzeugkontrollschildnummer verhängten Ordnungsbussen der letzten drei Jahre. Das führt aus buchhalterischen Gründen zu einer Registrierung, die sich zu polizeilichen Zwecken auswerten lässt. Anhaltpunkte dafür, dass eine solche Auswertung vorgenommen worden wäre, fehlen. Die zuständigen Stellen der Kantonspolizei waren denn auch bereit, eine Umgestaltung des Systems einzuleiten. Bezeichnend ist aber, dass der Fehler nur gestützt auf einen Hinweis eines Betroffenen und nicht im Rahmen einer (eben fehlenden) ordentlichen Kontrolle festgestellt wurde. Die von Treuhandfirmen vorab betreffend Datensicherheit angebotenen Überprüfungen weisen darauf hin, dass umfassende Datenschutzkontrollen von EDV-Grosssystemen rasch zu einem Aufwand in der Grössenordnung von 100 000 Franken führen. Die Datenschutzaufsichtsstelle verfügt über keine Kredite. Nur ein Einsetzen der personellen Mittel kann daher in Frage kommen. Das scheitert nicht nur aus Kapazitätsgründen, sondern auch an fehlenden Informatikern. Soll die Situation nicht beschönigt werden, so müssen die der Datenschutzaufsichtsstelle gegenüber EDV-Grosssystemen möglichen Kontrollhandlungen (die regelmässig durch einen äusseren Anlass ausgelöst worden sind) als zu oberflächlich bezeichnet werden.

3.2.2 Eigenverantwortung der Dienststellen

In der Antwort zur Interpellation Galli hat der Regierungsrat auch festgehalten, die staatlichen Stellen seien für das Einhalten der Vorgaben der Datenschutzgesetzgebung letztlich selbst verantwortlich. Sie hätten im Rahmen der ihnen zur Verfügung stehenden Ressourcen auf allen Ebenen die zur Beachtung der Daten-

schutzvorgaben nötigen personellen und sachlichen Mittel bereitzustellen. Bestes Beispiel für eine Stelle, die diese Vorgabe ernst nahm, ist das Inselspital: es setzte auf den 1. Juli einen nebenamtlichen Datenschutzbeauftragten ein. Positiv zu erwähnen sind auch die von den kantonalen Erziehungsberatungsstellen gemeinsam mit dem Jugendpsychiatrischen Dienst oder die von den Anstalten Witzwil organisierten internen Weiterbildungsveranstaltungen. Das Obergericht hat im Berichtsjahr in seinem Bereich das Register der Datensammlungen erstellt. Die Gesundheits- und Fürsorgedirektion (Fürsorgeamt) hat im ausgearbeiteten Handbuch Sozialhilfe auch Datenschutzprobleme zuhanden der vollziehenden Stellen praxisnah erklärt. Die Inselschulen haben die Aktenaufbewahrung in einer detaillierten Weisung geregelt. Als Negativpunkt von zentraler Bedeutung hat sich (vgl. Ziff. 3.4) das fehlende Bewusstsein der Führung für Fragen der Datensicherheit bei der EDV erwiesen. Bezeichnend ist etwa, dass das interne Mitberichtsverfahren zum Regierungsratsbeschluss 3457/95 (BEMAIL) im wesentlichen den Informatikverantwortlichen überlassen wurde. Bedenklich stimmt, dass ein Informatikdienst einen Amtsleiter erst mit einer Stellungnahme der Datenschutzaufsichtsstelle davon überzeugen konnte, ein Server dürfe nicht in einer öffentlich zugänglichen Cafeteria untergebracht werden. Dem von der Justiz-, Gemeinde- und Kirchendirektion bei externen Stellen eingeholten Papier betreffend Datensicherheit ist folgender Satz zu entnehmen: «Das Bewusstsein für die Notwendigkeit von Sicherheits- und Kontrollmassnahmen im Informationsbereich ist insbesondere auch auf Managementebene ungenügend ausgeprägt». Das dürfte für andere Stellen verstärkt gelten.

3.2.3 Verhältnis Informatikmittel / Mittel für Datenschutz und Datensicherheit

Gemäss einer Rückfrage beim Organisationsamt sind 1995 20 Mio. Franken in Informatikmittel investiert worden. 118 Mio. Franken kostete der Betrieb der Informatikmittel. Demgegenüber sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert bei rund 0,25 Mio. Franken geblieben. Wie im letzten Bericht ist darauf hinzuweisen, die für die Datenschutzaufsichtsstelle einzusetzenden Mittel dürften sinnvollerweise nicht unabhängig von den Informatikmitteln festgelegt werden. Die bestehenden Probleme haben sich diesbezüglich 1995 nicht entschärft. Der von der Justiz-, Gemeinde- und Kirchendirektion eingeholte Bericht hat aufgezeigt, dass Sicherheit (losgelöst von den Aufgaben der Datenschutzaufsichtsstelle) nicht ohne entsprechenden Mitteleinsatz realisiert werden kann. Er ging von 1200 mit den marktüblichen Sicherheitsvorkehrungen ausgerüsteten Standardarbeitsplätzen aus. Die üblichen organisatorischen Sicherheitsmassnahmen waren sodann bereits vorhanden. Gestützt auf eine einlässliche Priorisierung wies der Bericht für ein angemessenes Sicherheitsniveau folgende zusätzliche Kosten aus: Einmalige Kosten 500 000 Franken, einmaliger personeller Aufwand 662 Personentage, jährlich wiederkehrende personelle Aufwendung 220 Personentage. Die Kosten des Berichtes selbst beliefen sich auf rund 80 000 Franken. Aus diesen Zahlen lässt sich nicht nur entnehmen, was Datensicherheit bei Informatikanwendungen kostet. Es lässt sich vielmehr auch abschätzen, wie leicht die der Datenschutzaufsichtsstelle im Datenschutzgesetz (Art. 34 Buchstaben b und e) gegebenen Kontrollaufträge toter Buchstabe bleiben können.

3.2.4 Neue Aufgaben

Das neue Gesetz über das Strafverfahren wird auf den 1. Januar 1997 hin in Kraft treten. Im Unterschied zum bisherigen Recht wird das polizeiliche Ermittlungsverfahren der Aufsicht der Datenschutzaufsichtsstelle unterstehen (vgl. Ziff. 3.6.2). Das Erfüllen dieser neuen Aufgabe erfordert Mittel. Werden diese nicht bereitgestellt, so wird einerseits die neue Aufgabe nicht oder nicht genügend erfüllt werden können, andererseits ein Abbau bei den bisherigen Aufgaben erfolgen müssen.

3.3 Register

Ende 1995 waren im Registerprogramm «Sisyphus» 809 Datensammlungen erfasst. Zur Datenerfassung wurde dieses Programm 1995 beim Obergericht und bei der psychiatrischen Klinik Münsingen vorübergehend installiert.

3.4 Datensicherheit

Fünf der sieben Direktionen haben bis Ende 1995 die mit dem Regierungsratsbeschluss 4637 vom 9. Dezember 1992 (ursprünglich auf Ende 1994) verlangte Klassifikation der Informatikanwendungen vorgelegt. Die Bau-, Verkehrs- und Energiedirektion legte anstelle der verlangten Klassifizierung eine vorläufige Einschätzung vor. Die Justiz-, Gemeinde- und Kirchendirektion legte einen von externen Stellen ausgearbeiteten Sicherheitsbericht vor. Mit diesem Bericht ist in materieller Hinsicht wesentlich mehr geleistet worden, als gemäss dem RRB 4637/92 zu leisten gewesen wäre. Die eigentliche Klassifikation der Informatikanwendungen soll in einer verfeinerten Abstufung vorgenommen werden und fehlte auf das Jahresende 1995 noch. Es ist nun zu prüfen, ob die vorgenommenen Klassifikationen richtig sind, und ob die im RRB 4637/92 vorgeschriebenen Massnahmen auch tatsächlich umgesetzt worden sind. In seiner Antwort auf die Interpellation Galli hat der Regierungsrat die Informatikkonferenz beauftragt, die Einsetzung eines Sicherheitsausschusses oder das Einsetzen je eines Informatikverantwortlichen als Sicherheitsverantwortlicher einer anderen Direktion zu prüfen. Der Regierungsrat hat damit unterstrichen, dass ihm an der Gewährleistung einer genügenden Informatiksicherheit liegt. Ob das vom Regierungsrat vorgeschlagene Vorgehen, das keine zusätzlichen Ausgaben verursacht, dem Problem gerecht wird, bleibt offen. Aufhorchen liess der sich im Sicherheitsbericht der Justiz-, Gemeinde- und Kirchendirektion findende Satz: «Das festgestellte Sicherheitsniveau in der JGK ist aus Sicht der Konzeptverfasser nicht haltbar und führt zu einem zwingenden Handlungsbedarf.» Entsprechende Sofortmassnahmen hat die Justiz-, Gemeinde- und Kirchendirektion durchgeführt. Der Bericht wurde zudem vor der Inbetriebsetzung des gesamten Projektes (alle Bezirksverwaltungen und Gerichte) eingeholt, so dass von einem zeitgerechten Handeln gesprochen werden kann. Gezeigt hat der Bericht jedoch, dass mit der rasanten Entwicklung der Informatik erhebliche Sicherheitsprobleme entstehen. Im Rahmen des Jahresberichtes ist es nicht möglich, auf den Bericht näher einzugehen. Stichworte wie Aktivierung der Bildschirmschonerpassworte, Deaktivierung der Diskettenlaufwerke bei den einzelnen Arbeitsstationen (u. a. gegen Virenbefall), Verbesserung der Sicherheitsdokumentation, Anschaffen von CO_2-Handfeuerlöschern für Serverräume, «Gewaltenteilung für Systemadministratoren» und sicherheitsmässige Überprüfung dieser Administratoren mögen genügen. Gerade das Beispiel der Systemadministratoren zeigt, wie rasch sich die Situation ändert: haben sie heute im wesentlichen auf die Daten der JGK am Standort Bern und auf diejenigen zweier Bezirksverwaltungen bzw. Gerichte Zugriff, werden sie künftig auf sämtliche Daten aller Bezirksverwaltungen und Gerichte greifen können. Aus dem von der Justiz-, Gemeinde- und Kirchendirektion eingeholten Bericht lassen sich für die gesamte Staatsverwaltung gültige Vorgaben entnehmen. Das Organisationsamt hat denn auch anlässlich der Klausurtagung der Informatikkonferenz den eingeholten Bericht vorgestellt

und die Informatiksicherheit thematisiert. Eine auf die allgemeinen Aussagen umgeschriebene Fassung des Berichtes wird den Informatikverantwortlichen zugänglich gemacht werden. Unübersehbar ist, dass die Sicherheitsprobleme insbesondere mit der Vernetzung stark ansteigen. Mit diesen Problemen befasst sich die zum Projekt BEWAN (bernisches Weitbereichsnetzwerk) eingeholte Vorstudie für ein Sicherheitskonzept. Wie eine umfassendere Zürcher Studie zur Netzwerksicherheit (Fakten I/96) gelangt die BEWAN-Vorstudie zum Schluss, die Gewährleistung der Datensicherheit in Netzen erfordere einen beträchtlichen Aufwand. Diesen Schluss bestätigt der RRB 3457/95 (vgl. Ziff. 3.1.3). Dem Regierungsrat kann nur zugestimmt werden, wenn er darin (unter anderem) die Übertragung von besonders schützenswerten Personendaten mittels E-Mail verbietet. Im Vortrag zum Beschluss zitiert der Regierungsrat einen am Projekt beteiligten EDV-Grosskonzern wie folgt: «Grundsätzlich ist festzuhalten, dass jede Kommunikation über Leitungsnetze irgendwelcher Art unsicher ist. Der einzig wirksame Schutz ist die Verschlüsselung.» Muss aber von einer grundsätzlichen Unsicherheit der unverschlüsselten elektronischen Datenübertragung in Netzen ausgegangen werden, stellen sich unausweichlich weitere Fragen. Zu fragen ist etwa, ob nicht in anderen Bereichen, wo ebenfalls Daten elektronisch über Netze übertragen werden, ein ebenso grosser Handlungsbedarf gegeben ist. Zu denken ist an zentral erfolgende Abrechnungen im medizinischen Bereich, für die (wohl ausnahmslos besonders schützenswerte) Daten unverschlüsselt elektronisch übertragen werden. Die rasante Entwicklung der EDV scheint mit solchen Ungereimtheiten verbunden zu sein. Bezeichnend ist schliesslich auch der Geltungsbereich des RRB 3457. Angesprochen werden alle Stellen (auch externe), die Träger öffentlicher Aufgaben des Kantons sind und über ihre lokalen Mail-Systeme am System BEMAIL angeschlossen sind. So richtig die umfassende Geltung des RRB sein mag, so deutlich zeigt sie, dass mit der Vernetzung ein Überspringen traditioneller Verantwortlichkeitsabgrenzungen einhergeht. Hinzuweisen ist etwa auf die das Mailsystem benützenden selbständigen Anstalten und Gerichte.

3.5 Informatikprojekte

Eine Voranfrage konnte mit den beteiligten Stellen dahin erledigt werden, dass die Einrichtung eines Online-Anschlusses der Steuerverwaltung auf die GELAN-Datenbank des Amtes für Landwirtschaft unverhältnismässig wäre. Zweck des auf die Beitragszahlungsverfügungen beschränkten Zugriffes wäre die stichprobenweise Überprüfung der Steuererklärungen von Landwirten gewesen. Selbst wenn die zumindest erforderliche Verordnungsgrundlage geschaffen worden wäre, hätte der Online-Zugriff zu einem Übermass im Datenfluss an die Steuerverwaltung geführt. Eine Kontrolle mit den konventionellen Mitteln (Einverlangen von Unterlagen) genügt. Im Zusammenhang mit dem Projekt ALIDAT des kantonalen Labors standen Fragen der Netzwerksicherung im Vordergrund. Eine umfassendere Stellungnahme forderten die Verantwortlichen zum Projekt EVOK (Elektronischer Vollzug der obligatorischen Krankenversicherung) ein. Gegenüber den hauptsächlich beteiligten Stellen (Amt für Sozialversicherung und Stiftungsaufsicht, Steuerverwaltung, Ausgleichskasse und indirekt Krankenkassen und Gemeinden) ging es neben den Datensicherheitsfragen darum, die im Hinblick auf die Aufgabenerfüllung nötigen bzw. nicht nötigen Datenmengen zu umschreiben. Auseinanderzuhalten waren insbesondere die für das Versicherungsobligatorium und die für die Ausrichtung von Beiträgen erforderlichen Datenmengen. Bejaht wurde zudem das Genügen einer (nach bernischem Verfassungsrecht gesetzesvertretenden) befristeten «Notverordnung» als «formell»-gesetzliche Grundlage für ein Abrufverfahren.

3.6 Gesetzgebung

3.6.1 Auswirkungen des eidgenössischen Datenschutzgesetzes

Das bernische Datenschutzgesetz verlangt im Unterschied zum eidgenössischen Datenschutzgesetz – von Ausnahmen abgesehen – zur Datensperre den Nachweis eines schützenswerten Interesses. Auf Bundesebene genügt das blosse Glaubhaftmachen eines solchen Interesses. Eine Angleichung an das eidgenössische Recht dürfte um so mehr am Platze sein, als die bernische Informationsgesetzgebung eine wesentlich weitergehende Bekanntgabe von nicht besonders schützenswerten Personendaten an Private erlaubt als das eidgenössische Recht.

3.6.2 Übrige kantonale Erlasse

Zu begrüssen ist die auf den 1. Januar 1997 in Kraft tretende Neuregelung des Datenschutzes im Gesetz über das Strafverfahren. Mit der grundsätzlichen Unterstellung des polizeilichen Ermittlungsverfahrens (Ausnahmen ergeben sich vorab für die Datenerhebung) unter das Datenschutzgesetz wird dem Bundesrecht Nachachtung verschafft. Der Rechtsprechung des Bundesgerichtes trägt die Regelung der Datenaufbewahrung im Bereich der gerichtlichen Polizei Rechnung. Wohl noch einer Differenzierung durch bereichsspezifische Regelungen auf Gesetzesstufe bedarf die neu vorgesehene generelle Meldepflicht der staatlichen und kommunalen Beamtenschaft für von Amtes wegen zu verfolgende Verbrechen. Im Bereich der betreuenden Verwaltung (z. B. Erziehungsberatung, Schule und Kindergarten sowie Fürsorge) sind unerwünschte Auswirkungen zu befürchten. So werden auf der Seite eines Opfers stehende Personen (z. B. bei einer Kindsmisshandlung) künftig zögern, bei Behörden Hilfe zu suchen. Jedenfalls ist auffällig, dass gerade über diesen Aspekt des Datenschutzes der Datenschutzaufsichtsstelle heikle Konstellationen unterbreitet wurden. Das im Vernehmlassungsverfahren stehende Polizeigesetz löst die Datenschutzfragen koordiniert zum Gesetz über das Strafverfahren. Geschaffen wird eine gesetzliche Grundlage für polizeiliche Abrufverfahren und eine Regelung der polizeilichen Berichte zur Person (Leumundsberichte).

3.7 Gemeinderechtliche Körperschaften

1995 konnten zwölf neue Datenschutzreglemente genehmigt werden. Auf Ende Jahr verfügten damit 198 Gemeinden über ein eigenes Datenschutzreglement. Als Folge der Informationsgesetzgebung war ein neues Musterdatenschutzreglement zu erlassen. Es konnte den Gemeinden über die vom Amt für Gemeinden und Raumordnung neu herausgegebene bernische systematische Information der Gemeinden zusammen mit weiteren Unterlagen (Erläuterungen, Musterartikel für eine Abänderung des Organisationsreglementes, Sperrgesuchsformular, Liste der anwendbaren Erlasse) zugestellt werden. Die kommunalen Datenschutzaufsichtsstellen wurden sodann Anfang Jahr mit einem Schreiben auf den durch die Gesetzgebung über die Information der Bevölkerung eintretenden Abbau des Datenschutzes hingewiesen. Sie wurden aufgefordert, die Bevölkerung über die neue Rechtslage und die Möglichkeit der Datensperre zu informieren.

3.8 Besonderes

3.8.1 Informationsgesetzgebung

Wie im Jahresbericht 1994 festgehalten worden ist, baut die Informationsgesetzgebung den Datenschutz vorab im Bereich der

nicht besonders schützenswerten Personendaten ab. Die Folgen der Informationsgesetzgebung werden erst nach einer längeren Zeitspanne zu beurteilen sein. Nach dem ersten Jahr überrascht, dass durchaus auch positive Reaktionen der Betroffenen zu vermerken sind: so ist auffällig, dass in denjenigen Gemeinden, die ihre Bevölkerung intensiv über den Abbau des Datenschutzes informiert haben (vgl. Ziff. 3.7) regelmässig weniger als 5 Prozent der Bevölkerung ihre Daten sperren liessen. Neben der Vermutung, dass ein Grossteil der Betroffenen sich um entsprechende Fragen überhaupt nicht kümmert, liegt doch auch der Schluss nahe, dass Betroffene mit der Bekanntgabe von nicht besonders schützenswerten Daten (wie etwa der Eigenschaft Hundehalter zu sein) durchaus leben können. Zudem dürfte sich in der tiefen Anzahl von Sperrgesuchen auch widerspiegeln, dass die Betroffenen davon ausgehen, die Gemeindeverwaltung werde in Zweifelsfällen die gebotene Interessenabwägung mit der nötigen Sorgfalt vornehmen. Die zahlreichen Anfragen von Verwaltungsstellen geben dieser Einschätzung Recht. Etwa in Zusammenhang mit einer Klassenzusammenkunft (unterbleibende Einladung) wurde neu auch nach den Nachteilen einer Datensperre gefragt. Wie erwartet hat sich sowohl auf kantonaler als auch auf kommunaler Ebene ein Interesse von Drittpersonen, die Löhne bestimmter Beamter zu kennen, gezeigt. Die (spärliche) Praxis hat in entsprechenden Fällen die Bekanntgabe der Lohnhöhe (ohne Sozialzulagen) grundsätzlich empfohlen und dazu geraten, den Betroffenen vorgängig die Möglichkeit zur Stellungnahme einzuräumen. Eine weitergehende erste Bilanz ist in einer von der Staatskanzlei geplanten Broschüre vorgesehen.

Bern, 23. Januar 1995

Der Datenschutzbeauftragte: *Siegenthaler*