Bericht der Aufsichtsstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Mit ihren Datenschutzfragen müssen sich Verwaltungsstellen neu vorerst an ihren Rechtsdienst wenden. Neu kann der Regierungsrat Betreiber von Informatikanwendungen zu einer externen Datenschutzprüfung verpflichten. Ausgaben für Informatikprojekte dürfen zudem erst beschlossen werden, wenn ein Datenschutzkonzept vorliegt. Mit diesen Massnahmen will der Regierungsrat dafür sorgen, dass die Datenschutzaufgaben besser erfüllt werden.
Vernetzte Grosssysteme – wie etwa die kantonsweite Plattform für die Führung der Einwohnerkontrollen GERES – belegen, wie notwendig solche Verbesserungen sind. Selbst der Eidgenössische Datenschutzbeauftragte sieht sich ausser Stande auf Grossprojekte – wie etwa die Tarmed-Einführung – rechtzeitig einzugehen. Dies zeigt, dass sich die Datenschutzaufsichtsstellen auch in Zukunft darauf beschränken müssen, Impulse zu geben.

3.1.2 Zusammenarbeit mit dem eidgenössischen Datenschutzbeauftragten und der Vereinigung der Schweizerischen Datenschutzbeauftragten

Der in die Vernehmlassung geschickte Entwurf für ein neues Bundesgesetz zur Harmonisierung der Einwohnerkontrollen und anderer amtlicher Register sieht die Schaffung eines eidgenössischen Personenidentifikators vor. Die Vereinigung der Schweizerischen Datenschutzbeauftragten fordert, dass ein solcher Personenidentifikator ausschliesslich zu statistischen Zwecken eingesetzt werden darf und über die Notwendigkeit einer Personennummer eine breite politische Grundsatzdiskussion stattfindet. An der Frühjahrsversammlung verabschiedete sie hierzu die Resolution «Der Bürger im E-Government darf nicht zur Nummer werden». (s. zur Einführung einer kantonalen Verwaltungsnummer 3.6.2; s. zur Zusammenarbeit mit der Arbeitsgruppe Gesundheit und dem Eidgenössischen Datenschutzbeauftragten zu Gesundheitsfragen 3.7.)

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Für das Bearbeiten der Geschäfte gilt unverändert folgende Prioritätenfolge: 1. Datenschutzkonzepte für Informatikprojekte, 2. Allgemeine Gesetzgebung vor Spezialerlassen, 3. Generelle Weisungen vor Einzelfällen, 4. Beratung und Instruktion vor Inspektion und 5. Einzelprobleme mit vielen Betroffenen vor solchen mit wenig Betroffenen und geringen Wiederholungschancen. (Zum Problem der überlangen Wartezeiten für Rechtsauskünfte s. 3.2.2.)

3.2.2 Regierungsratsbeschlüsse über Massnahmen gegen die chronische Unterfüllung des gesetzlichen Auftrages des Datenschutzes (RRB 1102, 1103, 1104 vom 9. April 2003)

Die Rechtsdienste der Direktionen, allfällige Datenschutzberaterinnen und -berater und – für Informatikfragen – die Informatikdienste sind neu Anlaufstellen für Datenschutzfragen der Organisationseinheiten. Direkten Zugang zur Datenschutzaufsichtsstelle haben nur noch Bürger und die Anlaufstellen (s. für gemeinderechtliche Körperschaften 3.9). Mit diesem Beschluss entlastete der Regierungsrat im Frühjahr die Datenschutzaufsichtsstelle. Er nahm zur Kenntnis, dass die Datenschutzaufsichtsstelle Geschäfte, die im Frühjahr älter als ein Jahr waren, unerledigt zu den Akten legte (ca. 120).
Ungefähr ein Promille der jährlichen Betriebskosten der Informatik will der Regierungsrat künftig für Datenschutzkontrollen von Informatikanwendungen durch externe Stellen bereitstellen. In einem Prüfplan bezeichnet er die zu prüfenden Anwendungen und was zu prüfen ist. Der Beizug der unabhängigen externen Prüfungsstelle obliegt dann der Organisationseinheit, die die Informatikanwendung betreibt.
Bevor eine Organisationseinheit einen Ausgabenbeschluss für ein Informatikprojekt auslösen darf, hat sie nach dem dritten in diesem Umfeld gefassten Regierungsratsbeschluss ein Datenschutzkonzept vorzulegen. In diesem ist darzulegen, wie das Projekt die Informatik-Sicherheitssollvorgaben (s. 3.3.1) und die Datenschutzrechte der Betroffenen umsetzen will (Sperrrecht, Berichtigungsanspruch, Einsichtsrecht, Anspruch auf Datenvernichtung). Darzulegen sind zudem die vorgesehenen Zugriffsrechte und Protokollierungen.
Es ist noch zu früh, um zu beurteilen, welche Wirkungen diese Regierungsratsbeschlüsse zeigen. Festgestellt werden kann, dass die Rechtsdienste ihre Organisationseinheiten auch in Datenschutzfragen sehr gut beraten. Die Entlastung ist denn auch spürbar.
Der Prüfplan für die Prüfung der Informatikanwendungen steht erst in Ausarbeitung. (Zu den Datenschutzkonzepten s. 3.4.1.)

3.2.3 Eigenverantwortung der Daten bearbeitenden Stellen

Zum Beispiel der Entwurf einer Weisung über die Benutzung der Informatikmittel der Lehrerinnen- und Lehrerbildung, die Aufnahme des Fachs Datenschutz in die überbetrieblichen Kurse der Lehrlingsausbildung oder das Ausarbeiten eines Sicherheitskonzepts für die Informatikanwendung GELAN (Auszahlung von Landwirtschaftsbeiträgen) zeigen das Engagement der datenbearbeitenden Stellen. Zunehmend lässt sich auch feststellen, dass Dateninhaber, wie etwa die Steuerverwaltung, bei neu vorgesehenen Zugriffen anderer Systeme sehr genau abklären, welche Bearbeitungen ihrer Daten in den Fremdsystemen erfolgen sollen.

3.2.4 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2003 waren 39 Mio. Franken in Informatikmittel zu investieren und 140 Mio. Franken (davon 61 Mio. für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Der

Regierungsrat hat für die Prüfung von Informatikanwendungen durch externe Prüfstellen für 2004 und die kommenden Jahre ein Promille der Informatikbetriebskosten vorgesehen (s. 3.2.2). Dieser Betrag ist im Verhältnis zu den Gesamtkosten der Datenschutzaufsichtsstelle (rund 0,25 Mio. Franken) nicht unerheblich.

3.2.5 Kontrollen von Informatikdatenbearbeitungen

Im Rahmen der Wirtschaftsprüfung führt die Finanzkontrolle neu eine Risikobeurteilung im Informatikbereich der Dienststelle durch (Interview mit dem Informatikverantwortlichen). Den im BEDAG-Gesetz umschriebenen Auftrag zu einer jährlichen schwerpunktmässigen Prüfung der Informatiksicherheit durch eine externe Fachstelle setzte die BEDAG Informatik AG durch einen Voraudit im Hinblick auf die Zertifizierung ihrer Informatiksicherheit nach dem British Standard BS 7799-2:2002 um.
(Zum künftig vorgesehenen Beizug unabhängiger externer Fachstellen für die Prüfung von Informatikanwendungen s. 3.2.2, zur Änderung der dem Polizeikommando auferlegten Pflicht zum Beizug unabhängiger externer Prüfstellen s. 3.10.4, zur Umsetzung des Kontrollkonzeptes durch das Amt für Sozialversicherung und Stiftungsaufsicht s. 3.10.2).

3.3 Datensicherheit

Die Datenschutzkonzepte für Informatikprojekte (s. 3.2.2 und 3.4) geben regelmässig Hinweise auf Sicherheitslücken. So war zur Übertragungssicherheit in Erinnerung zu rufen, dass der Regierungsrat im Jahr 1997 das Weitbereichskommunikationsnetz BE-WAN einzig für die Übertragung von internen oder nicht klassifizierten Daten, nicht aber für die Übertragung vertraulicher oder geheimer Daten freigegeben hat.

3.3.1 Sollvorgaben

In seinen Beschlüssen zur Entlastung der Datenschutzaufsichtsstelle beauftragte der Regierungsrat das Organisationsamt, bis Mitte 2004 in Zusammenarbeit mit der kantonalen Informatikkonferenz und unter Beizug der Datenschutzaufsichtsstelle einer Informatikfachperson einen Auftrag für ein Gutachten zu erteilen, das sich darüber äussert, wie die Sollvorgaben zur Informatiksicherheit weiterzuentwickeln sind. Das Ungenügen der aktuellen Sollvorgaben zeigte sich auch bei der Behandlung der neu vorzulegenden Datenschutzkonzepte für Informatikprojekte. So wird etwa im Datenschutzkonzept für das Informatikprojekt FIS 2000 (Finanzinformationssystem) festgehalten, es müssten auf kantonaler Ebene detaillierte und aktuelle Vorgaben zur Informatiksicherheit geschaffen werden. Auch bei der Behandlung von E-Government-nahen Projekten (Schübe und VPZ-Dispo s. 3.4.1) erwiesen sich die Sollvorgaben als ungenügend.
Die von der kantonalen Informatikkonferenz erlassene Weisung zum Umgang mit User-IDs weist – beschränkt auf einen Teilbereich – in die richtige Richtung.

3.3.2 Sicherheit von E-Mail

Die kantonale Informatikkonferenz beschloss ein Vorprojekt Public-PKI und SecureMail. Durch den Einsatz von auf dem Markt erhältlichen Klasse-2-Zertifikaten und Soft-Tokens soll die Übertragung auch besonders schützenswerter Daten per Mail ermöglicht werden. Die Datenschutzaufsichtsstelle hatte in der Evaluationsphase darauf hinzuweisen, dass ihre Ressourcen eine Abklärung der schwierigen Rechtsfragen in diesem Umfeld nicht erlauben. Das Vorprojekt beansprucht deren Lösung auch nicht. Es geht vielmehr darum, auf pragmatische Weise das bei der Übertragung besonders schützenswerter Daten bestehende Sicherheitsproblem kurzfristig anzugehen.

3.4 Informatikprojekte

Der Regierungsrat verlangt neu (s. 3.2.2) dass alle Informatikprojekte ab Fr. 100000.– erst zum Ausgabenbeschluss unterbreitet werden, wenn ein Datenschutzkonzept vorliegt. Das Konzept ist der Datenschutzaufsichtsstelle zur Stellungnahme zu unterbreiten. Diese Vorgabe verbessert die Umsetzung der Datenschutzanliegen.

3.4.1 Betreute Projekte

Ein Datenschutzkonzept unterbreiteten die Projektleitungen für die Projekte «GEO-Datenbank» (s. zum zugehörigen Verordnungsentwurf 3.6.2), «Leistungserfassung mit IBIcare» (für ein neues Informatiksystem zur Erfassung der medizinischen Leistungen), «ELAR» (Elektronisches Archiv des Amtes für Migration und Personenstand, Überarbeitung des nachträglichen Datenschutzkonzepts) und «FIS 2000» (Finanzinformationssystem, nachträglich erstelltes Datenschutzkonzept).
Das Instrument des Datenschutzkonzeptes muss sich noch festigen. Unter Beizug externer Stellen hat die Projektleitung von «FIS 2000» aber ein Datenschutzkonzept erarbeitet, das künftigen Datenschutzkonzepten als Muster dienen kann.
Unabhängig von der Beschlussfassung über das Projekt BEKIS (einheitliches Klinikinformationssystem für die somatische und psychiatrische, öffentlich subventionierte Versorgung des Kantons Bern) hat die Gesundheits- und Fürsorgedirektion einer externen Stelle den Auftrag erteilt, ein generelles Datenschutzrahmenkonzept für Spitäler zu erarbeiten. Dieser Schritt ist zu begrüssen. Wenn aber das Spitalamt – wie beim Staatsbeitrag an das Regionalspital Emmental für IBIcare – unter Verweis auf das künftige Rahmendatenschutzkonzept auf die Umsetzung von projektbezogenen Datenschutzverbesserungen verzichtet, weist dies in die falsche Richtung.
Zu einer nachträglichen Ausarbeitung eines Datenschutzkonzeptes verpflichteten sich die Projektleitungen der Projekte «PERSISKA-Erneuerung» (Erneuerung des Personalinformationssystems, überarbeitete Zusammenfassung der bisherigen Datenschutzvorgaben), «IT-Harmonisierung BESIS» (Umsetzung der kantonsweiten IT-Harmonisierung im Bereich der drei staatlichen psychiatrischen Kliniken) und «VITSek II» (Verwaltungsinformatik für Schulen der Sekundarstufe II).
Für E-Government-nahe Projekte ist das Fehlen von kantonseigenen Sicherheitssollvorgaben erschwerend. Zu betreuen waren die Projekte «VPZ-Dispo, Internet-Anbindung» (Disposition von Fahrzeug- und Führerprüfungen durch Privatpersonen, Garagen und Fahrlehrer über das Internet) und «Schübe» (Erfassung der Schülerbeurteilungen durch die Lehrkräfte über Internet auf einem von der Erziehungsdirektion zur Verfügung gestellten zentralen Server und Archivierung dieser Unterlagen während 15 Jahren seit Schulaustritt). Schübe wurde der Datenschutzaufsichtsstelle erst auf Rückfrage hin und ohne Datenschutzkonzept unterbreitet. (Zu GERES s. 3.6.2).

3.5 Internet und E-Government

Wie Privatspitäler bieten auch öffentliche Spitäler Eltern die Möglichkeit, Bilder ihrer neugeborenen Kinder auf einer Internetseite zu zeigen. Diese Spitäler waren daran zu erinnern, dass die Zustimmung der Eltern die fehlende Rechtsgrundlage für diese Veröffentlichung nicht zu ersetzen vermag.

Neben einer Rechtsgrundlage ist für die Aufnahme von Bildern von Mitarbeitenden, auch wenn sie nicht auf Internetseiten, sondern im Intranet erfolgt, eine Notwendigkeit zur Aufgabenerfüllung erforderlich (Verhältnismässigkeit). Darauf waren mehrere Stellen aufmerksam zu machen.
Verschiedene Organisationseinheiten erliessen Weisungen für den Umgang mit Internet und E-Mail.
(Zu den fehlenden Informatiksicherheitssollvorgaben für E-Government-Lösungen s. 3.4.1; zu GERES s. 3.6.2).

3.6 Gesetzgebung

3.6.1 Bundeserlasse
(s. 3.1.2 und 3.10.1).

3.6.2 Kantonale Erlasse

Die Arbeiten an der GEO-Datenverordnung wurden weitergeführt (s. auch 3.4.1), ebenso diejenigen am Gesetz zum Betrieb des Informatiksystems GERES (Gemeinderegister). Dieses Gesetz soll auch den Einsatz einer kantonale Verwaltungsnummer regeln. Zur Frage nach den verfassungsrechtlichen Grenzen einer solchen Regelung konnte auf das von Prof. Giovanni Biaggini dem Eidgenössischen Datenschutzbeauftragten zur gleichen Frage auf Bundesebene erstattete Gutachten abgestellt werden.

3.7 Gesundheitswesen

Für die Erfassung und Abrechnung medizinischer Leistungen werden neue Instrumente eingesetzt oder in Pilotphasen erprobt. Nicht selten bedingt die Einführung einer neuen Methode auch die Einführung neuer Informatikmittel. So stützt sich das im Vorjahresbericht erwähnte Informatikprojekt «SEP» (System zur Erfassung der Pflegeleistungen in den bernischen Spitälern) auf die Methode «LEP» (Leistungserfassung für die Gesundheits- und Krankenpflege) ab. Die Methode «APDRG» (All Patient Diagnoses Related Groups) soll in mehreren Spitälern in einem Pilotversuch eingeführt werden. Auf den 1.1.2004 erfolgt die Tarmedeinführung (s. 3.1.1; Tarmed führt zu einer standardisierten und systematischen Übermittlung von detaillierten Personendaten mittels eines Rechnungsformulars).
Die datenschutzrechtliche Beurteilung solcher Methoden und Informatiksysteme ist anspruchsvoll und zeitaufwändig. Sie erfordert neben informatiktechnischen Kenntnissen auch Kenntnisse des Krankenversicherungsrechtes und medizinische Kenntnisse. In der Regel geht es um schweizweit einzuführende Methoden (Krankenversicherungsgesetzgebung). Die Datenschutzaufsichtsstelle versucht daher, die Datenschutzfragen in Zusammenarbeit mit der Arbeitsgruppe Gesundheit der Vereinigung der Schweizerischen Datenschutzbeauftragten und mit dem Eidgenössischen Datenschutzbeauftragten zu lösen. Die so gewonnenen Ressourcen genügen jedoch regelmässig nicht einmal zur rechtzeitigen Prüfung auch nur eines Instruments. Die übrigen Instrumente können – wie Tarmed (s. 3.1.1) – erst im nachhinein oder überhaupt nicht geprüft werden. Dass das Betreuen von Datenbearbeitungen des Gesundheitswesens aufwändig ist, zeigt sich etwa auch daran, dass die für die medizinische Forschung des Inselspitals erforderliche Klinikbewilligung der Eidgenössischen Expertenkommission für die Offenbarung des Berufsgeheimnisses im Bereich der medizinischen Forschung erst 2003 – also zehn Jahre später als von der Gesetzgebung vorgesehen – ausgestellt wurde.

3.8 Aufsichts- und Justizentscheide

3.8.1 Blankovollmacht zum Einholen von Auskünften durch die IV-Stelle Bern

Wer sich zum Bezug von IV-Leistungen anmeldet, hat nach der Praxis der IV-Stelle Bern eine Vollmacht zu unterzeichnen, worin alle in Betracht fallenden Personen und Stellen, namentlich Ärzte und Ärztinnen, medizinisches Hilfspersonal, Spitäler, Heilanstalten, Krankenkassen, Arbeitgeber, Anwälte und Anwältinnen, Treuhandfirmen, private und öffentliche Versicherungen, Amtsstellen der privaten Fürsorgeeinrichtungen und die zuständigen Stellen der Alters-, Hinterlassenen- und Invalidenversicherung ermächtigt werden, der IV-Stelle diejenigen Auskünfte zu erteilen, welche diese für die Abklärung des Anspruchs und die Prüfung des Leistungsanspruchs des Versicherten sowie die Durchführung des Rückgriffes auf Dritte benötigt. Das Bundesamt für Sozialversicherung hiess eine gegen diese Vollmacht geführte Aufsichtsbeschwerde gut und bestätigte damit die von der Datenschutzaufsichtsstelle gegenüber der IV-Stelle schon früher geäusserte Auffassung, die Vollmacht sei als Blankovollmacht widerrechtlich.

3.8.2 Einsichtsrecht naher Angehöriger in die Strafakten eines Verstorbenen

Nahe Angehörige (hier Mutter, Lebenspartnerin und gemeinsame Kinder) eines verstorbenen Angeschuldigten haben – sofern nicht Geheimhaltungsinteressen überwiegen – unter anderem auch aus persönlichkeitsrechtlichen Gründen ein Einsichtrecht in die Akten des gegen den Verstorbenen geführten Strafverfahrens. Einen anderslautenden Entscheid eines Untersuchungsrichters korrigierte die Anklagekammer auf Rekurs hin.

3.8.3 Zugriff auf die Kundenkarten-Datenbank eines Grossverteilers im Strafverfahren

Finden sich am Tatort Werkzeuge, die bei einem Grossverteiler eingekauft worden waren, ist es zulässig, dass die Untersuchungsbehörde aus der Kundenkarten-Datenbank des Grossverteilers erhebt, wer solche Werkzeuge unter Benützung der Kundenkarte gekauft hat (mit örtlichen Einschränkungen). Einen durch den Grossverteiler aus Gründen des Persönlichkeitsschutzes erhobenen Rekurs wies die Anklagekammer ab. Neben der Rechtsgrundlage im Strafverfahren zum Erheben von Daten aus einer elektronischen Datenbank prüfte sie insbesondere die Verhältnismässigkeit des Eingriffs und bejahte diese im konkreten Fall. Die Untersuchungsbehörde wurde verpflichtet, dem Grossverteiler die Löschung der Daten bei Untersuchungsbehörde und Polizei mitzuteilen.
Der Entscheid ruft zwei Dinge in Erinnerung: Einmal führt der Einsatz moderner Datenbearbeitungsmittel, wie eben von Kundenkarten, dazu, dass auch nach längerer Zeit präzise Aufzeichnungen über alltägliche Massenvorgänge (Werkzeugkauf) auswertbar sind. Zum andern entstehen auf diese Art auswertbare Dateien nicht nur bei privatrechtlichen sondern auch bei öffentlich-rechtlichen Datenbearbeitern.

3.8.4 Einbürgerungen an der Urne
(s. 3.9).

3.9. Gemeinderechtliche Körperschaften

Als Massnahme gegen die chronische Untererfüllung des gesetzlichen Auftrages des Datenschutzes (s. 3.2.2) steht neu das Amt für Gemeinden und Raumordnung oder die fachkompetente kantonale Stelle den gemeinderechtlichen Körperschaften als Anlaufstelle of-

fen. Nach wie vor können sich jedoch die kommunalen Datenschutzaufsichtsstellen an die kantonale Datenschutzaufsichtsstelle wenden. Soweit zurzeit überblickbar, bewährt sich die neue Regelung.
Etwa die Frage nach der Zuständigkeit zum Erlass einer Rechtsgrundlage für Videoaufnahmen in öffentlichen Verkehrsmitteln (z. B. Bussen), die mehrere Gemeinden bedienen oder die Frage, wie der Steuerwohnsitz von Wochenaufenthaltern festgestellt werden dürfe, zeigen, dass sich gemeinderechtliche Körperschaften in einem datenschutzrechtlich anspruchsvollen Umfeld bewegen.
Dass Datenschutzkonzepte, wie sie neu für kantonale Informatikprojekte verlangt werden (s. 3.4), auch für gemeinderechtliche Körperschaften Sinn machen würden, ergab sich etwa aus dem Hinweis eines Behördemitgliedes einer mittleren Gemeinde, wonach in dieser Gemeinde allen Mitarbeitenden – trotz unterschiedlichen Aufgaben – im Informatiksystem einschränkungslos zu allen Informationen Zugang gewährt werde.
Unter anderem zur Wahrung des Grundrechts auf Datenschutz der Einbürgerungswilligen entschied das Bundesgericht, es sei unzulässig, Einbürgerungsverfahren als Urnenabstimmung durchzuführen. Finden Einbürgerungsverfahren an der Gemeindeversammlung statt, bedeutet dies neu, dass die Datenschutzansprüche der Einbürgerungswilligen dem Informationsanspruch der Stimmberechtigten entgegenstehen. Anträge auf Nichteinbürgerung sind erste Beispiele dafür, dass die Abwägung der entgegenstehenden Interessen in der Praxis erhebliche Schwierigkeiten bereiten kann.
Zu der unter der Verantwortung der Gemeinden stehenden Informatikanwendung Schübe s. 3.4.1.

3.10 Berichtspunkte des Vorjahres
(s. 3.2.2, 3.3.1, 3.3.2)

3.10.1 DNA

Das Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten und vermissten Personen ist Mitte Jahr von den eidgenössischen Räten verabschiedet worden. Es wird nach seiner Inkraftsetzung auch im Kanton Bern zu vollziehen sein. Gehör fand die Forderung der Datenschutzbeauftragten nach einer Datenvernichtung vom Amtes wegen. Ungehört blieb die Forderung nach einem Katalog der Delikte, die zu einer Aufnahme in die Datenbank führen.

3.10.2 Kontrollen der Informatikdatenbearbeitungen im Amt für Sozialversicherungen und Stiftungsaufsicht

Mit der Erteilung eines Auftrags an eine externe unabhängige Fachstelle wurde die Umsetzung des in der Krankenversicherungsverordnung enthaltenen Auftrags zum Aufbau eines internen Kontrollsystems und zum regelmässigen Beizug einer externen Datenschutzkontrollstelle eingeleitet.

3.10.3 Einführung von Heimbewohnerbeurteilungssystemen (Projekt BAKAb)

Das zu einer unverhältnismässigen Datenbearbeitung führende Bewohnerbeurteilungssystem RAI/ RUG wird vom Hersteller überarbeitet. Für das System BESA liegt eine überarbeitete Version bereits vor. Der Datenschutzbeauftragte des Kantons Zürich hielt nach einer Überprüfung des für dieses System vorgelegten Datenschutzkonzeptes fest, Verbesserungen seien feststellbar. Auch für das System RAI/RUG soll eine Überprüfung des Datenschutzkonzeptes durch den Datenschutzbeauftragten des Kantons Zürich erfolgen. Sollten die Systeme die erforderlichen Verbesserungen aufweisen, wird für den Kanton Bern die Ablösung der bisherigen Systeme durchzuführen sein. Vor diesem Schritt kann trotz der eingeleiteten Verbesserungen noch nicht von einer konformen Situation ausgegangen werden.

3.10.4 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Mit dem Regierungsratsbeschluss zur Überprüfung von Informatikanwendungen (s. 3.2.2) legte der Regierungsrat neu fest, dass auch die Datenbearbeitungssysteme der Kantonspolizei nach dem vom Regierungsrat noch festzulegenden Prüfplan zu prüfen seien. Damit wurde einerseits die Frist zur erstmaligen Prüfung durch eine externe Kontrollstelle verlängert, andererseits wurde die Verpflichtung, im Abstand von zwei Jahren eine Prüfung durch eine unabhängige und fachkundige externe Stelle durchführen zu lassen, aufgehoben. Erst nach Vorliegen mehrerer Prüfpläne wird beurteilt werden können, ob dieser Schritt zu einer Verstärkung oder Reduzierung der Kontrollen führt.
Erst als Entwurf vorgelegt wurden der Datenschutzaufsichtsstelle die Betriebsbewilligung für die Ordnungsbussenzentrale und für die Datenbank des Dezernats Personenfahndung.
In der Betriebsbewilligung vom Januar 2001 verlangte der Regierungsrat vom Polizeikommando, dass die (Lese-)Zugriffe auf das Subsystem OBORA (Journaleinträge) protokolliert werden. Im Vortrag zu seinem Beschluss hielt der Regierungsrat fest, die Protokollierung müsse bis Ende 2002 realisiert werden. Zum Zeitpunkt der Berichterstattung fehlt die Protokollierung aber immer noch. Nach den Angaben des Polizeikommandos soll sie nun im Jahr 2004 realisiert werden.

3.11 Besonderes

3.11.1 Videoaufzeichnungen in Strafvollzugseinrichtungen

In seinem Bericht stellte der zur Überprüfung betrieblicher und personalrechtlicher Unregelmässigkeiten in den Regionalgefängnissen Bern und Thun eingesetzte Untersuchungsbeauftragte fest, es sei sicherzustellen, dass die Videoüberwachung in den Gefängnissen nicht für die Personalüberwachung missbraucht werde. Die daraufhin von der Leitung des Amtes für Freiheitsentzug und Betreuung durchgeführten Erhebungen zeigten, dass Videoaufnahmen nicht nur auf Monitore übertragen, sondern auch aufgezeichnet wurden. Solche Aufzeichnungen sind nur gestützt auf eine Grundlage in einem Gesetz erlaubt. Deren Fehlen veranlasste die Leitung des Amtes für Freiheitsentzug und Betreuung Aufzeichnungen dieser Art umgehend zu untersagen. Zurzeit klärt das Amt für Freiheitsentzug und Betreuung ab, ob und welche Bedürfnisse nach einer Videoaufzeichnung bestehen und wie diese rechtlich abzustützen wären.

3.11. 2 Datenbank der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren über Lehrpersonen mit Entzug der Lehrbefugnis/ Unterrichtsberechtigung

Der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) teilte die Erziehungsdirektion im Herbst mit, sie hege erhebliche Zweifel an der Rechtmässigkeit einer von der EDK geplanten Datenbank über Lehrpersonen mit Entzug der Lehrbefugnis/Unterrichtsberechtigung. Für die Datenschutzaufsichtsstelle steht fest, dass eine solche Datenbank nur gestützt auf eine Grundlage in einem Gesetz aufgebaut werden darf. Ohne ein solches Gesetz sind den Schulen des Kantons Bern Meldungen in die Datenbank untersagt. Die erforderliche gesetzliche Grundlage fehlt.

Es erstaunte daher, dass die EDK die Datenbank in das Register der Datensammlungen des Kantons Bern eintragen lassen wollte. Der EDK war mitzuteilen, dass die Datenschutzaufsichtsstelle des Kantons Bern ihr gegenüber keine Aufsichtsfunktionen hat und ein Registereintrag damit ausgeschlossen ist.

7. Januar 2004

Der Datenschutzbeauftragte: *Siegenthaler*