Bericht der Aufsichtsstelle für Datenschutz

Autor(en): **Siegenthaler**

Objekttyp: **Article**

Zeitschrift: **Verwaltungsbericht des Regierungsrates, der kantonalen Verwaltung und der Gerichtsbehörden für das Jahr ... = Rapport de gestion du Conseil-exécutif, de l'administration cantonale et des autorités judiciaires pendant l'année ...**

Band (Jahr): **- (2002)**

Heft [1]: **Verwaltungsbericht : Berichtsteil**

PDF erstellt am: **29.03.2024**

Persistenter Link: https://doi.org/10.5169/seals-418464

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Unter anderem mit dem verstärkten Einsatz von Datenbearbeitungssystemen soll dem aktuellen Spardruck begegnet werden. Etwa die Informatikprojekte BEKIS (zentrales Klinikinformationssystem), SEP (Systematische Erfassung der Pflegeleistungen), GERES (zentrale Plattform für Einwohnerkontrollen) und GRUDIS (Grundstücksinformationssystem) zeigen dies. Während bei diesen Projekten Datenschutzverantwortliche von Anfang an beigezogen wurden, und – wenn auch mit bei weitem ungenügenden Ressourcen – Einfluss nehmen konnten, unterblieb ein solcher Beizug beim Projekt BAKAb (Einführung von Heimbewohnerbeurteilungssystemen). Wenn mit der flächendeckenden Einführung solcher Beurteilungssysteme nun die Persönlichkeitsrechte von 13000 Heimbewohnern gefährdet werden, illustriert dies die Gefahr, die entsteht, wenn unter Druck Datenbearbeitungssysteme ohne Datenschutzprüfung im Schnellverfahren eingeführt werden.

3.1.2 Zusammenarbeit mit dem eidgenössischen Datenschutzbeauftragten und der Vereinigung der Schweizerischen Datenschutzbeauftragten, IX. Nationale Konferenz der Datenschutzbeauftragten

Ohne den von der «Arbeitsgruppe Gesundheit» der Vereinigung der Schweizerischen Datenschutzbeauftragten ausgearbeiteten Bericht und der dazugehörigen Liste der notwendigen Systemanpassungen wäre es der Datenschutzaufsichtsstelle nicht möglich gewesen, zum Heimbewohnerbeurteilungssystem RAI Stellung zu nehmen (s. 3.10.1). Weder hätte der erforderliche Prüfungsaufwand erbracht werden können, noch wäre das vom eidgenössischen Datenschutzbeauftragten eingebrachte Informatikwissen vorhanden gewesen.
Die den Mitgliedern der Vereinigung zur Verfügung gestellte Broschüre «Der sichere Umgang mit Informations- und Kommunikationsgeräten» konnte an die Gemeinden verteilt werden (s. 3.8).
Neben der Unterstützung bei der Ausarbeitung kantonaler Vernehmlassungen zu Bundeserlassen sind die von der Vereinigung organisierten Weiterbildungsmöglichkeiten wichtig: an der Frühjahrsversammlung referierte Prof. Martin Killias zum Thema Strafverfolgung und Datenschutz, an der Herbstversammlung war die Einführung einer persönlichen Identifikationsnummer auf Bundesebene (s. 3.6.2) neben Gesichtserkennungssystemen und dem Verhältnis von Datenschutz und innerer Sicherheit nach dem 11. September Thema.

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Für das Bearbeiten der Geschäfte gilt unverändert folgende Prioritätenfolge: 1. 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. Geschäfte, die weder Rücksprachen bei andern Stellen noch langwierige eigene Abklärungen erfordern, werden als Tagesgeschäfte nach Eingang sofort erledigt. Als Tagesgeschäfte werden insbesondere die häufiger werdenden Mailanfragen behandelt. Das in früheren Jahresberichten erwähnte Problem der überlangen Wartezeiten für Rechtsauskünfte blieb ungelöst (s. 3.2.2). Kontrollhandlungen, insbesondere Inspektionen, fanden aus Ressourcengründen ohne Hinweise (Aufsichtsanzeigen) nicht statt.

3.2.2 Empfehlung der Geschäftsprüfungskommission des Grossen Rates zur chronischen Untererfüllung des gesetzlichen Auftrages des Datenschutzes

Wie im Vorjahresbericht dargelegt, will der Regierungsrat der chronischen Untererfüllung des gesetzlichen Auftrages des Datenschutzes durch eine Aufgabenumlagerung ohne Stellenschaffung begegnen. Die Ausarbeitung der hierzu nötigen Regierungsratsbeschlüsse konnte bis Ende Jahr nicht abgeschlossen werden. Insbesondere ein konsensfähiges Umschreiben der künftigen Prüfungen von Informatikprojekten und der Kontrolltätigkeiten gegenüber Informatikanwendungen erwies sich als schwierig. Die Arbeiten waren zum Zeitpunkt der Berichterstattung weiter im Gang.

3.2.3 Eigenverantwortung der Daten bearbeitenden Stellen

Nach wie vor besteht die Haupttätigkeit der Datenschutzaufsichtsstelle in Stellungnahmen zu Anfragen von amtlichen Stellen. Zahlreiche Informatikprojekte (s. 3.4.1) sind ihr unterbreitet worden. Bestehende Weisungen zum Datenschutz sind aktualisiert oder erweitert worden (Psychiatrische Klinken, Bau-, Verkehrs- und Energiedirektion). Das Organisationsamt liess einen Sicherheitsaudit (s. 3.2.5) durchführen.

3.2.4 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2002 waren 31 Mio. Franken in Informatikmittel zu investieren und 138 Mio. Franken (davon 50 Mio. Fr. für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Wichtige Projekte wie etwa BEKIS (s. 3.4.1, Kostenrahmen über 19 Mio. Fr.) laufen zudem nicht über das kantonale Budget. Mit rund 0,25 Mio. Franken sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert geblieben. Der Aufwand für Informatik und derjenige für Datenschutz steht nach wie vor nicht in einem adäquaten Verhältnis.

3.2.5 Kontrollen von Informatikdatenbearbeitungen

Als Erfolg versprechendes neues Kontrollkonzept stellte die Datenschutzaufsichtsstelle im Jahresbericht 2000 die in der Krankenversicherungsverordnung neu getroffene Lösung vor: Das über Ressourcen verfügende Amt für Sozialversicherung und Stiftungsaufsicht (ASVS) wurde verpflichtet, periodisch eine externe Kontrollstelle beizuziehen, die das interne Kontrollsystem überprüft.

Weder ist innert der im Vortrag genannten Frist von zwei Jahren ein internes Kontrollsystem aufgebaut worden, noch erfolgte der Beizug einer externen Kontrollstelle. Ein rasches Nachholen dieser Versäumnisse würde den Verdacht entkräften, die Bestimmung habe vorab als wohlfeiles Argument zur Begründung von weitgehenden Zugriffen auf Steuerdaten gedient.
Die Kantonspolizei hat die ihr in der Betriebsbewilligung des Regierungsrats für die Informationssysteme gemachte Vorgabe zur Auditierung durch eine unabhängige Stelle – soweit zum Zeitpunkt der Berichterstattung überprüfbar – ebenfalls nicht eingehalten. Allerdings baut das Polizeikommando die interne Kontrolle durch die «Kommission Datenschutz» erst auf und diese Kontrolle ist Voraussetzung für eine sinnvolle Auditierung durch Externe.
Dass eine solche gerade auch aus der Sicht der Systembetreiber wichtige Einsichten und Verbesserungsmöglichkeiten liefert, haben die vom Organisationsamt im Umfeld BEWEB, BEMAIL und BE-WAN und die vom Amt für Landwirtschaft für die Informatikanwendung GELAN (Bearbeitung von Landwirtschaftsdaten insbesondere für Direktzahlungen der Kantone Bern, Freiburg und Solothurn) veranlassten Sicherheitsaudits durch externe Stellen gezeigt.
Zu der bereits letztes Jahr erwähnten, unter Beizug einer externen Stelle durch die Finanzkontrolle durchgeführten Risikobeurteilung im Informatikbereich liegt nun auch der Querschnittsbericht vor. Wenn in diesem empfohlen wird, die im IT-Zonenplan aufgeführten Standards zur IT-Sicherheit zu erweitern und kantonale Richtlinien für die physische Sicherheit von Informatikinfrastrukturen zu erlassen, so kann dies nur unterstützt werden (s. 3.3.1).

3.3 Datensicherheit

Immer noch führt auch der Umgang mit Daten auf Papier zu Sicherheitsproblemen: So wurden von den Zahnmedizinischen Kliniken Krankengeschichten und weitere medizinische Unterlagen in Abfallcontainern zur Entsorgung bereit gestellt. Erst auf Intervention einer Drittperson hin erfolgte für die Nacht eine Umlagerung von der Containersammelstelle an einen sicheren Ort. Erlaubt die allgemeine Lebenserfahrung die Unzulässigkeit dieses Vorgehens leicht zu erkennen, sind die Informatiksicherheitsrisiken regelmässig schwerer erkennbar: Durch das Anklicken einer falschen Zeile im Mailadressverzeichnis verschickte ein Mitarbeiter eines Regionalgefängnisses eine Belegungsliste mit Namen und Deliktsart irrtümlich an einen externen Informatikdienstleister. Trotz anders lautenden Weisungen des Amtes für Freiheitsentzug und Betreuung erfolgte der tägliche Versand seit längerer Zeit – unverschlüsselt – per Mail. Mit dem Amt für Freiheitsentzug und Betreuung bestand Einigkeit, dass eine Belegungsliste besonders schützenswerte Daten enthält und nicht unverschlüsselt per Mail übermittelt werden darf. Neu steht den Regionalgefängnissen nun ein zentraler Server zur Ablage der Belegungslisten zur Verfügung, auf den die zuständige Stelle des Amtes Zugriff hat. Zurzeit wird sichergestellt, dass auch diese Zugriffe verschlüsselt erfolgen. Nicht zulässig war die geprüfte Lösung einer Faxübertragung: Die unverschlüsselte Faxübertragung ist ebenso unsicher wie die unverschlüsselte Mailübertragung. Dort wo kleinen Aussenstellen ein Anschluss zum zentralen Server fehlt, ist entweder eine Faxverschlüsselung einzusetzen oder die Listen sind als verschlüsselte Mailanhänge (s. 3.3.2) zu übertragen. Bei den zuständigen Stellen der Finanzdirektion war zudem darauf hinzuweisen, dass externe Informatikdienstleister künftighin nicht mehr auf der kantonalen Mailadressliste aufgeführt werden sollten. Schliesslich war zur Kenntnis zu nehmen, dass auch nach der Einführung eines Mailverschlüsselungssystems die Möglichkeit bestehen würde, den Adressaten falsch auszuwählen.

3.3.1 Sollvorgaben

Die Hauptsollvorgabe zur Informatiksicherheit bildet für die kantonale Verwaltung nach wie vor der Regierungsratsbeschluss 4637/92 (19 Massnahmen). Der Regierungsratsbeschluss 1347/98 regelt den Umgang mit Passwörtern. Das Organisationsamt hat im Rahmen des IT-Zonenplans Stichworte für Sicherheitsstandards zu Gebäudeverkabelung, Benutzeridentifikation, Zutrittsregelung für EDV-Räume, Raumschutz, Virenschutz, Authentifizierungs- und Verschlüsselungsverfahren, Datensicherung und Stromversorgung gegeben (3-seitige Tabelle). In mehreren Verordnungen wird zudem bereichspezifisch ergänzend auf die Weisung S 02 des Bundes «Grundschutz von Informatiksystemen und -anwendungen» verwiesen. An einer umfassenden Sollvorgabe – etwa entsprechend der Weisung S 02 für die Bundesverwaltung (ca. 260 Massnahmen) oder dem für Verwaltung und Industrie verfassten deutschen IT-Grundschutzhandbuch – fehlt es nach wie vor. Das ist (in Übereinstimmung mit der Auffassung der Finanzkontrolle s. 3.2.5) zu kritisieren. Insbesondere ist daran zu erinnern, dass sowohl mit dem neuen Bedag-Gesetz für das Outsourcing an die BEDAG als auch in der neuen Patientenverordnung für die Einführung einer elektronischen Behandlungsdokumentation verlangt wird, dass die Datenbearbeiter Informatiksicherheitssollvorgaben gemacht haben.

3.3.2 Sicherheit von E-Mail

Wie etwa Behördeprotokolle von Gemeinden unter Verwendung von E-Mail sicher übertragen werden können, ist die am häufigsten gestellte Frage zur Informatiksicherheit. In einem mit zwei Regierungsstatthalterämtern ausgearbeiteten Arbeitspapier werden die hierzu aktuell gegebenen Möglichkeiten und die Umsetzungsschwierigkeiten erläutert. Das Bedürfnis nach einem E-Mail-System, das praxistauglich Vertraulichkeit und Verbindlichkeit sicherstellt, ist nach wie vor gross (s. 3.3).

3.4 Informatikprojekte

3.4.1 Betreute Projekte

Um Prüfung der datenschutzrechtlichen Aspekte ersuchten die Projektleitungen für die Projekte BEKIS (Einführung eines einheitlichen Klinikinformationssystems für die somatische und psychiatrische, öffentlich subventionierte Versorgung des Kantons Bern als Massnahme zur Verbesserungen der Arbeitssituation im Pflegebereich [VAP] mit einem Kostenrahmen von über 19 Mio. Fr.), SEP (System zur Erfassung der Pflegeleistungen in den bernischen Spitälern, ebenfalls VAP Projekt, Kostenrahmen von 3,95 Mio. Fr.), elektronisches Vollzugsregister des Amtes für Freiheitsentzug und Betreuung (Kontrolle des Straf- und Massnahmevollzugs an Erwachsenen), ADS/RENO (Systemmanagementsystem als Lösung zur Standardisierung der Bewirtschaftung der IT-Betriebsmittel in den Direktionen und der Staatskanzlei, Kostenrahmen 4,815 Mio. Fr.), FIS 2000 (Finanzinformationssystem: nachträgliche Erstellung eines Datenschutzkonzepts), HP 71: Systemdesign Spezialrechnung PERSISKA (Schnittstelle Personalverwaltungssystem PERSISKA zu FIS 2000), ELAR (elektronisches Archiv des Amtes für Migration und Personenstand: nachträgliches Datenschutzkonzept), Migration Windows/Office (Erneuerung der Informatikgrundinfrastruktur der Gesundheits- und Fürsorgedirektion) und «gemeinsamer Benutzerpool IDS» (Informationsverbund Deutschschweiz, in dem die Nutzerdaten von über 250 Bibliotheken der Deutschschweiz bearbeitet werden). Auf Hinweis einer betroffenen Person hin wurde bei der Erziehungsdirektion zudem angeregt, das von mehreren Mittelschulen eingesetzte Schulverwaltungssystem Eco open einer Datenschutzüberprüfung zu unterziehen. (Zu GERES s. 3.6).

3.4.2 Arbeitspapier «Datenschutzkonzept»

Die Datenschutzaufsichtsstelle orientiert sich beim Umgang mit Informatikprojekten an einem halbseitigen Arbeitspapier. Dieses bringt die Umsetzung der Persönlichkeitsrechte (Einsichtsrecht, Berichtigungsanspruch, Datenvernichtung und Sperrecht) sowie die verhältnismässige Ausgestaltung der Zugriffsrechte und die Massnahmen der Informatiksicherheit zur Überprüfung. Trotz seiner Einfachheit hat sich das Papier bewährt. Folgende, zum Teil elementare Probleme sind bei den Prüfungen aufgetaucht: Falsche Klassifizierungen der Daten im Rahmen der Informatikstrategie, fehlende Möglichkeit zur Datenvernichtung, fehlende Sicherheitssollvorgaben (was insbesondere verhindert, dass Drittdienstleister auf diese Vorgaben verpflichtet werden), ungenügende Definition der Zugriffsrechte und teilweise bereits fehlender Informatikgrundschutz.

3.5 Internet und E-Government

Das Amt für Information der Staatskanzlei hielt in seinen Content- und Designrichtlinien für die Webauftritte des Kantons Bern fest, dass Angaben über Personen nur dann auf Webseiten publiziert werden dürfen, wenn die Betroffenen ihre Zustimmung erteilt haben oder eine Rechtsgrundlage besteht. Das Personalamt bereitet eine solche Rechtsgrundlage in einer Verordnungsbestimmung vor. Diese regelt, dass Publikationen dann erfolgen dürfen, wenn dies zur Aufgabenerfüllung erforderlich ist und welche Einwirkungsmöglichkeiten Betroffene haben sollen. Wenn etwa ein Kindergarten – mit der Zustimmung aller betroffenen Eltern – Bilder der Kinder auf seine Webseite aufnimmt, zeigt dies, wie verbreitet Webpublikationen geworden sind.
Mit einer Änderung des Universitätsstatuts schafft die Universität die Rechtsgrundlage um den Studierenden Mitteilungen elektronisch zustellen zu dürfen. Die Übermittlung besonders schützenswerter Daten und von Verfügungen im Rahmen der Verwaltungsrechtspflege ist nicht erlaubt. Alle Studierenden erhalten bei der Immatrikulation ein E-Mail-Konto.
Im Zusammenhang mit der elektronischen Steuererklärung befasste sich die kantonale Informatikkonferenz mit der Frage, welche Zertifikate zur Server-Authentifizierung einzusetzen sind.
(Zur Mailsicherheit s. 3.3.2, zum Gesetzgebungs- und Informatikprojekt GERES s. 3.6.2)

3.6 Gesetzgebung

3.6.1 Bundeserlasse

In Vernehmlassungsverfahren zu Bundesgesetzen gibt die Datenschutzaufsichtsstelle nur noch gestützt auf entsprechende Vorschläge der Vereinigung der Schweizerischen Datenschutzbeauftragten Stellungnahmen (an die koordinierende kantonale Stelle) ab.

3.6.2 Kantonale Erlasse

Im Vernehmlassungsverfahren zur GRUDIS-Verordnung wurde erstmals anhand eines Fragenkatalogs die Verhältnismässigkeit von neuen Abrufmöglichkeiten detailliert geprüft. Bei der Behandlung des Arbeitsmarktgesetzes war neben anderem zu prüfen, ob bei den Rechtsgrundlagen für Abrufverfahren nicht Doppelspurigkeiten zum parallel dazu entstehenden Bundesrecht vorliegen. In der Geodatenverordnung werden unter anderem ebenfalls Rechtsgrundlagen für Abrufverfahren zu verankern sein. Der frühe Beizug der Datenschutzaufsichtstelle zu diesem Gesetzgebungsprojekt ist erfreulich. Die Abschätzung der durch geographische Daten entstehenden Beeinträchtigungen der Persönlichkeitsrechte und deren Regelung erweist sich allerdings als anspruchsvoll. Anspruchsvoll gestaltet sich auch die Arbeit der Arbeitsgruppe GERES: Das Informatiksystem GERES (Gemeinderegister) soll den Gemeinden eine kantonsweite Plattform für die Führung der Einwohnerkontrollen zur Verfügung stellen. Die auf diese Weise bearbeiteten Daten sollen Basis für diverse kantonale Datenbearbeitungssysteme werden. Die einheitliche Datenbasis soll auch E-Governmentprozesse erleichtern. Zum Betrieb eines solchen Informatiksystems ist der Erlass eines formellen Gesetzes nötig (Gesetz über die Harmonisierung amtlicher Register). Da die auf Bundesebene stattfindenden Aktivitäten zur Schaffung einer eidgenössischen Personenidentifikationsnummer auf den Gesetzesentwurf Rückwirkungen haben können, ist auch diese Schnittstelle im Auge zu behalten. Auch hier ist der frühe Beizug der Datenschutzaufsichtsstelle positiv zu vermerken. Diese Feststellung trifft auch gegenüber der Patientenverordnung zu. Sie hält unter anderem fest, dass, wer die Behandlungsdokumentation elektronisch führen will, für deren Revisionsfähigkeit sorgen muss und schriftlich festzulegen hat, welche Grundschutzmassnahmen und welche zusätzlichen Schutzmassnahmen für die Informatiksicherheit zu treffen sind (s. 3.3.1). Zudem ist innerhalb von Gesundheitsinstitutionen der Zugriff auf die Behandlungsdokumentation so zu regeln, dass die Einsichtnahme nur auf den Teil der Behandlungsdokumentation möglich ist, den die jeweilige Aufgabenerfüllung erfordert. Geregelt wird schliesslich das Outsourcing medizinischer Datenbearbeitungen.
Bezirks- und Regionalspitäler werden mit dem Spitalversorgungsgesetz nicht mehr als Gemeindeverbände organisiert sein. Nur Gemeindeverbände sind aber verpflichtet, eine eigene Datenschutzaufsichtsstelle zu führen. Wer deren Aufgabe künftig übernehmen soll, wird neu zu regeln sein. Sinnvoll erscheint es insbesondere, auch bisher nicht als Gemeindeverbände organisierte Spitäler – wie etwa das Inselspital – zur Führung einer eigenen Datenschutzaufsichtsstelle zu verpflichten. Rechtsgrundlage für die Einführung der Bewohnerbeurteilungssysteme (s. 3.10.1) bildet die teilrevidierte Verordnung über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung. Sie wurde der Datenschutzaufsichtsstelle nicht unterbreitet.
(Zum geänderten Universitätsstatut s. 3. 5)

3.7 Justizentscheide

3.7.1 Zur Informationsgesetzgebung

Mit der Abweisung einer Beschwerde gegen eine Verfügung des Staatsarchivs bestätigte die Staatskanzlei, dass auch in ein über 50-jähriges Strafurteil einer Drittperson nur mit Zustimmung der Betroffenen (Opfer, Zeugen) Einsicht gewährt werden darf. Insbesondere durfte nicht davon ausgegangen werden, die Betroffenen seien bereits verstorben. Zu Recht ging das Staatsarchiv auch davon aus, ein Einholen der Zustimmungen führe zu einem unverhältnismässigen Aufwand. Einen unverhältnismässigen Aufwand hätte auch ein komplettes Anonymisieren der Akten verursacht. Einsicht gewährt wurde einzig in das anonymisierte Urteilsdispositiv (Urteilsspruch).

3.7.2 Zur Datenschutzgesetzgebung

Den Betroffenen ist auch dann Einsicht zu gewähren, wenn die gleiche Einsichtnahme bei andern Stellen erfolgen könnte. Dies bestätigte das Verwaltungsgericht gegenüber einer Gemeinde in seinen Erwägungen zur Kostenliquidation in einem gegenstandslos gewordenen Verfahren. Es ging um die Einsicht in einen Polizeibericht, den die herbeigerufene Kantonspolizei der Ortspolizeibehörde nach einer nachbarlichen Streitigkeit erstattet hatte.

3.8. Gemeinderechtliche Körperschaften

Die Gemeinde Langenthal startete ein Projekt um einen umfassenden Grundschutz der Informatik- und Kommunikationsdienste in der Stadtverwaltung herbeizuführen. Die Gemeinde Ostermundigen legte eine Verordnung über die Benutzung der Informatikmittel vor. Auch wenn auf der Internetseite der Datenschutzaufsichtsstelle zum kommunalen Datenschutz Hinweise gemacht werden, ist generell davon auszugehen, dass die Unterstützung der gemeinderechtlichen Körperschaften in Informatiksicherheitsfragen verbessert werden muss. Mit der Abgabe der Broschüre «Der sichere Umgang mit Informations- und Kommunikationsgeräten» (s. 3.2.1) konnte ein erster kleiner Schritt gemacht werden. Zur Sicherheit von E-Mail-Übertragungen s. 3.3.2. Nach wie vor ist der Anteil von Rechtsauskünften an gemeinderechtliche Körperschaften hoch.

3.9 Berichtspunkte des Vorjahres

(siehe 3.2.5, 3.3.1, 3.3.2, 3.3.5)

3.9.1 DNA

Zu Recht wurde in dem von der vorberatenden Kommission verabschiedeten Antrag zu einem Gesetz über den Straf- und Massnahmevollzug auf eine Regelung einer kantonseigenen DNA-Datenbank zu Strafverfolgungszwecken verzichtet.

3.10 Besonderes

3.10.1 Einführung von Heimbewohnerbeurteilungssystemen (Projekt BAKAb)

Bereits 1996 nahm die Datenschutzaufsichtsstelle zuhanden des Kantonsarztsamtes zu einem Bewohnerbeurteilungssystem Stellung. Das System sollte damals allein für die Pflege eingesetzt werden. Schon damals war an der Verhältnismässigkeit der Datenerhebung zu zweifeln. Auf Intervention von Interessenverbänden älterer Personen hin überprüfte die «Arbeitsgruppe Gesundheit» der Vereinigung der Schweizerischen Datenschutzbeauftragten im Sommer 2002 das in mehreren Altersheimen der Schweiz zum Einsatz kommende Bewohnerbeurteilungssystem RAI (Resident Assessment Instrument). Sie kam zum Schluss, das System erhebe insgesamt unverhältnismässig viele Daten, sei intransparent, verletze das Zweckbindungsgebot (es dient neben der Feststellung des Pflegebedarfs der Pflegeplanung, der Qualitätssicherung und der Kostenabrechnung), anonymisiere die Daten zu Statistikzwecken ungenügend und genüge den Datensicherheitssollvorgaben nicht. Im Projekt BAKAb, das das bisherige Abrechnungssystem BAK durch ein moderneres System ersetzen soll, kam die zuständige Stelle der Gesundheits- und Fürsorgedirektion unterstützt durch eine Arbeitsgruppe aber zum Schluss, für die 13000 Heimbewohner in den 300 Heimen des Kantons Bern sei auf Anfang 2003 hin flächendeckend entweder das System RAI oder das System BESA einzuführen. Mit Empfehlung von Ende August empfahl die Datenschutzaufsichtsstelle die Einführung des Systems RAI zu stoppen oder dessen Mängel kurzfristig zu beheben. Die Projektleitung entschied sich für die kurzfristige Mängelbehebung. Ob dieser Schritt die 68 das System RAI einführenden Heime allerdings noch beeinflusst hat, ist zu bezweifeln: Informationen, die ein Betroffener der Datenschutzaufsichtsstelle übergab, weisen daraufhin, dass die Korrekturen die Heime in der Vorbereitungsphase nicht mehr rechtzeitig erreichten. Gegenüber dem System BESA sind datenschutzrechtliche Abklärungen bisher unterblieben. Etwa die im Beobachtungsbogen vorgesehene Abklärung, ob ein Heimbewohner sexuelles Interesse zeige, lassen jedoch Zweifel aufkommen, ob hier nicht ähnliche Bedenken bestehen müssen.
Treibender Faktor zur Einführung der neuen Bewohnerbeurteilungssysteme war die neue Ausgestaltung der Kostenabrechnung. Vor diesem Hintergrund scheint ausgerechnet bei der Erhebung von heiklen Pflegedaten das Augenmass abhanden gekommen zu sein. Die Achtung der Persönlichkeitsrechte älterer Menschen hätte auch in Zeiten mit Spardruck verlangt, dass die Systeme vor ihrer Einführung einer gründlichen datenschutzrechtlichen Prüfung unterzogen und die dafür erforderlichen Mittel bereitgestellt worden wären.

15. Januar 2003

Der Datenschutzbeauftragte: *Siegenthaler*