Bericht der Aufsichtsstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

1999 befasste sich die Datenschutzaufsichtsstelle intensiv mit den Regeln für den Umgang mit DNA-Daten: War die Diskussion zu Beginn noch auf die kantonale DNA-Datenbank zu Strafverfolgungszwecken fokussiert, führten der Entwurf zu einem Bundesgesetz über genetische Untersuchungen beim Menschen und zahlreiche parlamentarische Vorstösse auf kantonaler Ebene zu einem weiteren Blickwinkel. Der Entwurf zu Weisungen über den Persönlichkeits- und Datenschutz am Institut für Rechtsmedizin zeigte die Notwendigkeit einer gesamthaften Betrachtungsweise der DNA-Problematik. Die differenzierten Stellungnahmen im Vernehmlassungsverfahren zur Änderung des Gesetzes über das Strafverfahren (Rechtsgrundlage für eine DNA-Datenbank zu strafrechtlichen Zwecken) belegten das hohe öffentliche Interesse.
Sowohl der Entwurf zu einem Bundesgesetz über die Ausweise für Schweizer Staatsangehörige als auch das Vorprojekt zur Änderung des Zivilgesetzbuches in Bezug auf die Zivilstandsakten (Schaffung eines schweizerischen Zentralzivilstandsregisters) sehen einen Zugriff zu polizeilichen Zwecken auf die neu zu schaffenden zentralen Datenbanken vor. Zentralisierung wie Online-Zugriff zu polizeilichen Zwecken sind datenschutzrechtlich kritische Punkte. Eine Abwägung der Interessen bedingt Transparenz im Gesetzgebungsverfahren.

3.1.2 Zusammenarbeit mit dem eidgenössischen Datenschutzbeauftragten und den Datenschutzaufsichtsstellen der Kantone, VI. Nationale Konferenz der Datenschutzbeauftragten

Viele kantonale Stellen vollziehen Bundesrecht. Feststellungen kantonaler Datenschutzaufsichtsstellen können Rückwirkungen auf Bundesvorgaben haben (Erlasse, Weisungen, Formulare). Eine gemeinsame Betreuung kantonaler Stellen durch den eidgenössischen Datenschutzbeauftragten und die kantonale Datenschutzaufsichtsstelle liegt daher nahe und ist im eidgenössischen Datenschutzgesetz als unterstützende Zusammenarbeit auch vorgesehen. Gemeinsam mit dem eidgenössischen Datenschutzbeauftragten fand ein Besuch bei einer regionalen Arbeitsvermittlungsstelle und bei der IV-Stelle Bern statt. Der Besuch bei der IV-Stelle Bern führte in einem begrenzten Bereich zu einer Prozessanalyse.
Die anlässlich der VI. Nationalen Konferenz der Datenschutzbeauftragten vertretenen Auffassungen bestätigten, dass der Kanton Bern mit seiner Informationsgesetzgebung in die richtige Richtung gegangen ist.

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Für die Bearbeitung 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. Unvereinbar mit den gesetzlichen Vorgaben sind die Wartezeiten für Geschäfte mit tiefer Prioritätsstufe: Einer Gemeinde war nach 17-monatiger Wartezeit mitzuteilen, sie sei in dieser Zeitspanne auf der Warteliste von Rang 80 auf Rang 40 vorgerückt. Kann die Ressourcensituation nicht verbessert werden, ist damit zu rechnen, dass derartige Geschäfte gar nicht mehr behandelt werden. Zu dieser Entwicklung trägt der Umstand bei, dass die anfragenden Stellen zunehmend komplexere Fragen unterbreiten. Es geht längst nicht mehr um die Vermittlung von Grundwissen.
Bei einem (oberflächlichen) Ressourcenvergleich unter den Kantonen dürfte der Kanton Bern immer noch zum ersten Drittel gehören. Unübersehbar ist jedoch die Entwicklung: Die andern Kantone bauen zunehmend eine Datenschutzaufsicht auf. Der Kanton Bern wird bei dieser Entwicklung überholt: Die Datenschutzaufsichtsstelle des Kantons Zürich verfügt über 415 Stellenprozente, diejenige der Stadt Zürich über 200 Stellenprozente.

3.2.2 Eigenverantwortung der Daten bearbeitenden Stellen

Nach wie vor besteht die Haupttätigkeit der Datenschutzaufsichtsstelle in Stellungnahmen zu Anfragen von amtlichen Stellen. Gegenüber dem Vorjahr verlangten die Daten bearbeitenden Stellen mehr Weiterbildungsveranstaltungen. Unterschiedlich ist nach wie vor die Haltung der Führung gegenüber Datenschutzfragen: Signalwirkung hatte es, dass sich auch die oberste Führungsebene mit den Fragen um den Umgang mit DNA-Daten intensiv befasste. Erfreulich ist die hohe Anzahl unterbreiteter Informatikprojekte, das Engagement der Universitären Psychiatrischen Dienste zum Erlass von Weisungen über die Datenbekanntgabe oder die Abklärungen der Erziehungsdirektion im Umfeld Internet und Schule. Ein Ernstnehmen der Datenschutzanliegen zeigt auch die Informationspolitik im Umfeld von Datenschutzpannen (vgl. Ziff. 3.11.2).

3.2.3 Verhältnis Informatikmittel/Mittel für Datenschutz und Datensicherheit

1999 waren 24,65 Mio. Franken in Informatikmittel zu investieren. 116,5 Mio. Franken sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Mit rund 0,25 Mio. Franken sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert geblieben. Auch wenn erneut dem Datenschutz dienende Audits (vgl. Ziff. 3.3.2) durchgeführt worden sind und auch wenn die Aktivitäten der «Fachgruppe Sicherheit» (vgl. Ziff. 3.3.1) positiv zu vermerken sind, steht der Aufwand für Informatik und derjenige für den Datenschutz nicht in einem adäquaten Verhältnis.

3.2.4 Aufgaben

Die mit dem Inkrafttreten des neuen Gemeindegesetzes entfallene Genehmigung von Gemeindedatenschutzreglementen entlastet von verzichtbaren Formalitäten. Der Aufwand für freiwillige Reglementsvorprüfungen ging nicht zurück.

Beim Ausarbeiten der Einführungsverordnung zum Bundesgesetz über die eidgenössische Volkszählung wurde klargestellt, dass die Datenschutzaufsichtsstellen der Gemeinden Aufsichtsorgan im Sinne der Bundesgesetzgebung sind. Der kantonalen Datenschutzaufsichtsstelle kommt (im Unterschied zur Volkszählung 90, bei der kommunale Datenschutzaufsichtsstellen weitgehend fehlten) einzig die Aufgabe der Oberaufsichtsstelle zu. Auch diese Aufgabe (vorab Instruktion) wird nur im Sinne einer Minimallösung und zu Lasten der ordentlichen Aufgaben erfüllt werden können. Die kommunalen Datenschutzaufsichtsstellen vermehrt einzubinden, erscheint grundsätzlich richtig (Gemeindeautonomie, Nähe zu den vollziehenden Stellen). Zu bedenken ist aber, dass damit Milizbehörden, die für ihre Datenschutzaufgaben generell ungenügend ausgebildet sind, erneut ohne genügende Instruktion für Spezialfragen in die Verantwortung genommen werden.

3.2.5 Register

1999 blieb das Register wegen fehlender Kapazität auf dem gleichen Stand wie in den Vorjahren. Weder wurde der gesetzliche Grundauftrag (Erfassen aller Datensammlungen) erfüllt, noch die Einträge der bereits erfassten Datensammlungen (812) rechtlich überprüft oder aktualisiert. Vereinzelt meldeten Verwaltungsstellen neue Datensammlungen an. Solche Anmeldungen wurden weder rechtlich überprüft noch in das elektronische Register übernommen.

3.3 Datensicherheit

3.3.1 Sollvorgaben

Die von ihr eingesetzte «Fachgruppe Sicherheit» beantragte der Kantonalen Informatikkonferenz, das Regelwerk des Kantons Zürich zur Klassifizierung von Informatikanwendungen zu übernehmen. Das Organisationsamt wurde gestützt auf diesen Antrag beauftragt, die Umsetzbarkeit und Verträglichkeit mit der Informatikorganisation des Kantons Bern zu prüfen. Das Zürcher Regelwerk stützt sich auf das IT-Grundschutzhandbuch des deutschen Bundesamtes für Sicherheit in der Informationstechnik. Die Datenschutzaufsichtsstelle begrüsst diesen Beschluss der Kantonalen Informatikkonferenz.

3.3.2 Audits: Sicherheitschecks

Das Organisationsamt liess durch eine externe Firma die Sicherheit der kantonalen Webserver-Infrastruktur prüfen. Während die erste Überprüfung keine Sicherheitsmängel aufdeckte, wurden bei einer zweiten Prüfung (mit einem «ethical hacking») Mängel gefunden; insbesondere hatte eine mit der Betreuung einer Webseite beauftragte Drittfirma ein Sicherheitsleck geschaffen. Die Mängel sind inzwischen behoben worden. Die Einsicht, dass Sicherheitsaudits erheblich zur Verbesserung der Sicherheit beitragen, hat sich gefestigt. Das hohe Engagement des Organisationsamtes in dieser Frage ist hervorzuheben.

3.3.3 Sicherheit von E-Mails

Am 10. November 1999 genehmigte der Regierungsrat den Abschluss des Projekts BEMAIL. Ein Ziel dieses Projektes war das Einführen verwaltungsinterner sicherer Mail-Verbindungen zwischen exponierten Stellen. Es wurde nicht erreicht. Wohl liessen sich technische Lösungen für kleine Benutzergruppen umsetzen. Insbesondere scheint die beauftragte Zertifikationsstelle ihre Aufgabe gut gelöst zu haben (Public-Key-Verfahren). Eine Ausbreitung im erwünschten Umfang blieb aber aus. Als Grund hierzu ist einmal auf das schnelllebige Umfeld zu verweisen: Stand am Anfang das verwaltungsinterne Übertragen von E-Mails mit garantierter Vertraulichkeit im Vordergrund, entstand – beeinflusst von der generellen Entwicklung – rasch ein Bedürfnis nach Verbindlichkeit und Authentizität und dies gerade auch für elektronische Nachrichten von und nach verwaltungsexternen Stellen. Das eingesetzte Produkt erlaubte verwaltungsintern grundsätzlich eine elektronische Unterschrift. Für den Umgang mit dem privaten Schlüssel fehlten aber Normen. Die etwa aus Deutschland bekannten Vorgaben waren ohne den Einsatz von Chipkarten praktisch nicht zu erfüllen. Die annäherungsweise eingesetzten Verfahren (privater Schlüssel auf Diskette) genügten weder den (deutschen) Sicherheitsanforderungen, noch wurden sie von den Anwendern akzeptiert. Das Engagement der Projektverantwortlichen für die Sicherheitsanliegen ist zu anerkennen.
Nicht zuletzt in Anbetracht des immer noch bestehenden Verbots, besonders schützenswerte Daten unverschlüsselt via E-Mail zu übertragen, ist die Forderung nach sicheren Mails uneingeschränkt aktuell. Im Nachfolgeprojekt BEMAIL II wird es darum gehen, digital-signierte Mails mit einem erweiterten Partnerkreis austauschen zu können.

3.4 Informatikprojekte

Mit dem Projekt Gelan 2002 der Volkswirtschaftsdirektion sollen die neuen bundesrechtlichen Vorgaben für die Auszahlung von Beiträgen an Landwirte umgesetzt werden. Neu werden auch Administrativ-Sanktionen bearbeitet. Das sind besonders schützenswerte Daten. Die Sicherheitsanforderungen und die Anforderungen an die Rechtsgrundlagen (Abrufverfahren) steigen dadurch. Das System soll neu gemeinsam mit den Kantonen Solothurn und Freiburg betrieben werden.
Gegenüber dem Projekt Electronic-Monitoring des Amtes für Freiheitsentzug und Betreuung (Vollzug kurzer Freiheitsstrafen in der Wohnung des Betroffenen mit elektronischer Ortung: Sender am Fussgelenk; Modellversuch 1999–2003) konnte einzig durch Übernehmen des Berichtes der Datenschutzaufsichtsstelle Baselland Stellung genommen werden. Zu verlangen war ein systematisches Erarbeiten eines Sicherheitskonzeptes.
Zum Projekt OBV 99 des Polizeikommandos (Ordnungsbussenzentrale) ist auf die Ziffer 3.10 zu verweisen, zu den Projekten GRIS (Grossratsinformationssystem auf Internet) und STEZE (Meldungen an die Stellvertretungszentrale der Erziehungsdirektion via Internet) auf die Ziffer 3.5.
Die Frage, ob die in der Wegleitung Projektabwicklung des Organisationsamtes vorgesehene Stellungnahme der Datenschutzaufsichtsstelle zu Informatikprojekten obligatorisch sei, war im Rahmen des Projektes BKM-2000 (EDV-Hilfsmittel zur finanziellen Führung und Überwachung von Projekten im Bereich des öffentlichen Hoch- und Tiefbaus) zu beantworten: Eine Stellungnahme schreibt weder ein Gesetz noch eine Verordnung vor. Die ausgabenkompetenten Stellen genehmigen EDV-Projekte regelmässig auch ohne eine Stellungnahme der Datenschutzaufsichtsstelle. Diese Praxis ist nicht rechtswidrig. Angesichts der hohen Priorität, welche die Datenschutzaufsichtsstelle den Informatikprojekten zumisst, ist diese Praxis allerdings zu bedauern. Es darf aber auch nicht darüber hinweggesehen werden, dass ein zeitgerechtes Überprüfen aller Informatikprojekte einen erheblichen Abbau in den übrigen Aufgabenbereichen mit sich bringen müsste.

3.5 Internet

Auf Anfrage der Erziehungsdirektion (Internetseiten von Schulen) und gegenüber den Informatikprojekten STEZE und GRIS war festzuhalten, dass das Zugänglichmachen von Personendaten via Internet ein weltweites Abrufverfahren bedeutet und einer Rechtsgrundlage bedarf. Bleibt die voraussetzungslose Sperrmöglichkeit des Betroffenen gewahrt, genügt für nicht besonders schützenswerte Daten eine Verordnung. In einer Übergangsphase darf auf die ausdrückliche Zustimmung der urteilsfähigen Betroffenen abgestellt werden. Schüler der Volksschulstufe sind in der Regel – ausser für einfache Sachverhalte – im Umfeld Internet nicht urteilsfähig. Wer öffentliche Funktionen ausübt, muss ein Bekanntgeben seiner Privatadresse durch staatliche Stellen auf Internet nicht dulden. Nicht geduldet werden muss auch das Bekanntgeben von Fotos. Erneut war darauf hinzuweisen, dass Internetseiten gegen Hackingangriffe zu sichern sind. Internetformulare dürfen nur dann eingesetzt werden, wenn die Identität der Formularbenutzer auf anderem Weg überprüft werden kann oder irrelevant ist. Die Verunglimpfung eines Lehrers in einem Gästebuch einer Schulwebseite rief die Verantwortung des Seitenbetreibers für den Seiteninhalt in Erinnerung. Verbietet die Trägergemeinde Listenauskünfte aus der Einwohnerkontrolle, darf eine Schule mit ihrer Internetseite dieses Verbot nicht untergraben. Kanton und Gemeinden haben die Internetmittel zügig eingeführt. Die Schaffung der erforderlichen Rechtsgrundlagen sollte nun nicht minder zügig erfolgen.

3.6 Gesetzgebung

Der Entwurf zu einem neuen Gesundheitsgesetz sieht vor, dass Patient und Arzt an Stelle der 20-jährigen Aufbewahrung der Krankengeschichte deren Herausgabe an den Patienten vereinbaren können. Damit wird einem seit langer Zeit bestehenden Datenschutzanliegen Rechnung getragen.
Die Volkswirtschaftsdirektion erarbeitete einen Entwurf zur Datenverkaufsverordnung. Gestützt auf die Informationsgesetzgebung (Öffentlichkeitsprinzip) hätte diese als Versuchsverordnung befristet den Datenverkauf ermöglichen sollen. In den mit Offenheit geführten Vorarbeiten, bei denen auch kritische Stimmen Gehör fanden, hat sich gezeigt, dass Datenverkaufsdienstleistungen des Kantons nur im Rahmen einer rechtlichen Gleichbehandlung eingeführt werden dürfen, dass sie einen schweren Eingriff in das Grundrecht auf Datenschutz darstellen, dass ein solcher Eingriff grundsätzlich eine formellgesetzliche Grundlage bedingt (auf die Besonderheiten der befristeten Versuchsverordnung ist hier nicht einzugehen), dass jedoch ein voraussetzungsloses Sperrrecht diesen Eingriff mildert, jedenfalls dann, wenn die tatsächliche Ausübungsmöglichkeit dieses Sperrrechtes auch sichergestellt ist. Die Datenschutzaufsichtsstelle wurde zu den Vorarbeiten von Anfang an beigezogen. Nach entsprechenden Hinweisen in der internen Vernehmlassung, entschied die Volkswirtschaftsdirektion, das Projekt nicht weiter zu verfolgen.
Die Einführungsverordnung zum Bundesgesetz über die eidgenössische Volkszählung erlaubt es den Gemeinden, im Einwohnerregister erfasste Personen mit den entsprechenden Haushalts- oder Wohnungsnummern gemäss dem eidgenössischen Gebäude- und Wohnungsregister zuzuordnen. Daten und Verknüpfung dürfen ausschliesslich zu statistischen Zwecken verwendet werden. Die Nützlichkeit dieser Rechtsgrundlage im Hinblick auf die Volkszählung 2010 ist gegeben. Ob allerdings ein Registrieren des Zusammenlebens zu andern Zwecken unterbleibt, hängt davon ab, mit welchen technischen und organisatorischen Massnahmen Missbräuchen entgegengewirkt wird (vgl. auch Ziff. 3.2.4).
Die Arbeitsgruppe der Datenschutzaufsichtsstellen der Kantone und des Bundes befasste sich mit dem Entwurf zu einem Bundesgesetz über die Ausweise für Schweizer Staatsangehörige. Der Datenschutzbeauftragte des Kantons Zürich arbeitete eine Stellungnahme aus, welche die Datenschutzaufsichtsstelle vollumfänglich übernahm. Auch zum Vorprojekt zur Änderung des Zivilgesetzbuches in Bezug auf die Zivilstandsakten wurde vollumfänglich die Zürcher Stellungnahme übernommen. Beide Gesetzgebungsprojekte sehen je für ihren Bereich ein zentrales schweizerisches Register vor. Auf beide Register soll zu polizeilichen Zwecken ein Online-Zugriff bestehen. Noch bei der in der Verordnung über die schweizerische Identitätskarte aus dem Jahre 1994 geregelten Datenbank der Identitätskartendaten war ausschliesslich ein Online-Zugriff zu administrativen Zwecken vorgesehen. In Erinnerung zu rufen ist der Bericht der Geschäftsprüfungskommission des Ständerates vom November 1998: Dieser verlangte, Online-Verbindungen im Bereich des Polizeiwesens auf ihre Notwendigkeit, Verhältnismässigkeit und Zweckbindung hin zu prüfen und diese Prüfung transparent zu machen. Gerade aus kantonaler Sicht ist diese Forderung zu unterstreichen.

3.7 Gemeinderechtliche Körperschaften

Nach wie vor geht ein hoher Anteil vor allem auch telefonischer Rechtsauskünfte an gemeinderechtliche Körperschaften. Auch diese klären die Rahmenbedingungen für Internetauftritte ab. Festzuhalten war beispielsweise, dass eine Abmeldung bei der Einwohnerkontrolle via Internetformular den Datensicherheitsvorgaben nicht zu genügen vermag.
Das Musterdatenschutzreglement wurde den geänderten rechtlichen Vorgaben angepasst (Entfallen der Genehmigung, kantonalrechtliche Grundlage für Online-Zugriffe der Kantonspolizei auf Einwohnerkontrolldaten). (Zur Volkszählung 2000 siehe Ziff. 3.2.4 und 3.6).

3.8 Archiv

Mit dem Inkrafttreten der Informationsgesetzgebung stellte sich die Frage, wann eine Drittperson in archivierte besonders schützenswerte Daten Einsicht nehmen darf. Konkreten Anlass zur Prüfung bot nun ein Einsichtsgesuch in zurückliegende Regierungsratsbeschlüsse mehrerer Jahre. In Übereinstimmung mit dem Rechtsdienst der Staatskanzlei war festzuhalten, dass – solange eine betroffene Person lebt – kein Einsichtsrecht in über sie aufbewahrte Akten mit besonders schützenswerten Daten besteht. Unter Vorbehalt des Andenkenschutzes ist nach dem Tod der Betroffenen sinngemäss die im Bundesarchivgesetz vorgesehene Lösung zu übernehmen. Ein Dossier wird damit frühestens 30 Jahre nach dem Datum des jüngsten Dokuments zugänglich, sofern die betroffene Person zu diesem Zeitpunkt mindestens seit drei Jahren verstorben ist. Ist das Todesdatum nicht bekannt, darf angenommen werden, eine Person werde nicht älter als 110-jährig. Das Füllen solcher Gesetzeslücken durch rechtsanwendende Behörden vermag wenig zu befriedigen. Der Erlass eines kantonalen Archivgesetzes scheint sinnvoll.

3.9 Informatikeinsatz in Spitälern

3.9.1 Zugriffsregelung in einem elektronischen Spitalinformationssystem

In einem Beschwerdeentscheid hielt die Gesundheits- und Fürsorgedirektion fest, ein Patient habe einen Anspruch darauf, dass Administrativdaten aus einem System entfernt werden, wenn dieses System allen Abteilungen des Spitals Zugriff auf die Administra-

tivdaten der andern Abteilungen gewährt. Die Systemausgestaltung sei unverhältnismässig und bereits die Kenntnis einer früheren Behandlung in einer anderen Abteilung könne den Patienten in seinem Grundrecht auf Datenschutz beeinträchtigen. Im Ergebnis hätte der Entscheid zu einer Ablösung des Informationssystems führen müssen. Diese stand aus anderen Gründen ohnehin bevor.

3.9.2 Outsourcing

Das Inselspital lagerte seine gesamte Informatik auf das mit der Firma Atag debis Informatik AG gegründete Zentrum für Informatik im Gesundheitswesen mit Sitz in Langenthal aus. 25 Mitarbeiterinnen und Mitarbeiter sowie zwei Lehrlinge wurden von der Firma übernommen. Noch in der Botschaft zum Bundesgesetz über den Datenschutz vom März 1988 ist festgehalten, dem Arztgeheimnis unterstehende Daten dürften nur nach Zustimmung des Patienten durch Dritte bearbeitet werden. Auf Anfrage der Arbeitsgruppe der kantonalen Datenschutzbeauftragten sieht das Bundesamt für Justiz die Rechtslage heute anders. Drittdatenbearbeiter – beispielsweise Informatikdienstleistungszentren – seien heute als Hilfsperson im Sinne der Regelung des ärztlichen Berufsgeheimnisses einzustufen und damit an das Arztgeheimnis gebunden. Auch ohne Zustimmung des Patienten sei Outsourcing unter Beachtung des Verhältnismässigkeitsgrundsatzes zulässig. Es sei Sache des Auftrag gebenden Spitals, dafür zu sorgen, dass das Informatikunternehmen die medizinischen Daten nicht für andere interne Zwecke – etwa die Personalrekrutierung – verwende. Schon heute würden sich Ärztinnen und Ärzte sowie ihre Hilfspersonen unterschiedlichen kantonalen Strafprozessordnungen und daraus resultierenden Aussageverpflichtungen gegenüber sehen. Die Auslagerung der Datenbearbeitung in andere Kantone vergrössere diese Probleme nicht. Erst eine einheitliche schweizerische Strafprozessordnung könne Abhilfe schaffen. Nach Auffassung des Bundesamtes für Justiz sei es dem medizinischen Informatikzentrum unter Umständen erlaubt, unabhängig vom Auftrag gebenden Spital eine Entbindung vom Arztgeheimnis zu beantragen. Kaum angängig dürfe eine solche Entbindung jedoch für eine ganze Patientengruppe – etwa im Rahmen von Rasterfahndungen – sein. Die vorgeschriebene Interessenabwägung müsse zu einer einzelfallweisen Prüfung führen. Ob ein Outsourcing ins Ausland durch kantonale Gesundheitsgesetze verboten werden solle, sei durch die kantonalen Gesetzgeber zu entscheiden.
Die Feststellung des Bundesamtes für Justiz, dass sich die arbeitsteilige Datenbearbeitung von medizinischen Daten in den letzten Jahren sehr stark entwickelt hat, ist nachvollziehbar. Auch wenn ein strafrechtliches Urteil zur Ausdehnung der Strafbarkeit noch fehlt, erscheint der Beizug eines externen Outsourcing-Partners für die Informatik durch ein Spital nach der Ansichtsäusserung des Bundesamtes für Justiz nicht mehr widerrechtlich. Die Outsourcing-Möglichkeit darf jedoch nur dann ausgeschöpft werden, wenn bei Auswahl, Instruktion und Überwachung des beauftragten Unternehmens besondere Sorgfalt an den Tag gelegt wird. Das bedingt insbesondere, dass der Auftraggeber die für den Outsourcing-Partner geltenden rechtlichen Rahmenbedingungen detailliert prüft und ihm vertraglich enge Vorgaben für die weiteren Datenbearbeitungen und für die Kontrollen macht. Es erscheint sinnvoll, wenn der Gesetzgeber hierzu Vorgaben macht. Erst wenn diese aufwändigen Umsetzungen nachfolgen, kann davon ausgegangen werden, es sei nicht vorab die Macht des Faktischen Auslöser für die neuen Auffassungen gewesen. Die eingeleitete Öffnung ist im Auge zu behalten.

3.10 Berichtspunkte des Vorjahres

3.10.1 Ordnungsbussenzentrale

Aus buchhalterischen Gründen führt das Informatiksystem der Ordnungsbussenzentrale zu einer unzulässigen Registrierung von Ordnungsbussenschuldnern. Noch 1997 lehnte die Polizei- und Militärdirektion eine Systemanpassung aus Kostengründen ab. Zur Lösung des Jahr-2000-Problems musste das System nun ersetzt werden. Das neue System (OBV 99) trägt nun auch dem ursprünglichen Anliegen Rechnung.

3.10.2 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Die Vorarbeiten für den entsprechenden Regierungsratsbeschluss sind immer noch im Gang.

3.11 Besonderes

3.11.1 DNA

Im Berichtsjahr behandelte der Grosse Rat drei Motionen, eine Interpellation und eine Frage zum Thema DNA. Das unterstreicht die hohe Bedeutung des Themas. Zum Entwurf für ein Bundesgesetz über genetische Untersuchungen beim Menschen nahm im Vernehmlassungsverfahren auch der Kanton Bern Stellung. Vom Bericht der Arbeitsgruppe des Bundes über die Errichtung einer gesamtschweizerischen DNA-Profildatenbank war Kenntnis zu nehmen. Mit dem Gesetz über den Straf- und Massnahmenvollzug wurde eine Änderung des Gesetzes über das Strafverfahren in die Vernehmlassung gegeben. Mit diesem Entwurf soll die Rechtsgrundlage für eine kantonale DNA-Datenbank und für den Umgang mit DNA-Material, Folgeprodukten der DNA-Analyse und DNA-Daten zu Strafverfolgungszwecken geschaffen werden. Die Erziehungsdirektion erarbeitete schliesslich einen Entwurf zu Weisungen über den Persönlichkeits- und Datenschutz am Institut für Rechtsmedizin. Auch im Alltag hat die DNA-Analyse Einzug gehalten: So war etwa die Frage zu beantworten, auf welchem Weg insbesondere anhand von Zivilstandsdaten der vermutete biologische Vater aufgefunden werden könne. Dies nachdem eine im Einverständnis mit dem sozialen Vater – einem betagten Mann – im Auftrag des über 40-jährigen «Kindes» durchgeführte DNA-Analyse bestätigt hatte, dass der soziale Vater nicht der biologische Vater sein konnte.
War die Diskussion um den Umgang mit DNA-Daten anfänglich von Teilaspekten geprägt (Ist eine Blutentnahme für eine strafrechtliche DNA-Analyse zulässig? Darf mit DNA-Daten eine polizeiliche Datenbank betrieben werden?), hat – vorab unter dem Eindruck des Entwurfs zu einem Bundesgesetz über genetische Untersuchungen beim Menschen – zunehmend eine Gesamtbetrachtungsweise Einzug gehalten. Dies zeigte sich sowohl bei der Behandlung der parlamentarischen Vorstösse als auch in den Vernehmlassungen zum geänderten Gesetz über das Strafverfahren. Die von Art. 24novies der Bundesverfassung (neu Art. 119 Abs. 2 Buchst. f der Bundesverfassung) aufgezeigte neue rechtliche Dimension des Umgangs mit dem Thema DNA dürfte ernst genommen werden: Erbgut des Menschen soll erst dann untersucht, registriert und offenbart werden, wenn die Rahmenbedingungen hierzu in einem demokratischen Rechtsetzungsvorgang diskutiert und festgeschrieben worden sind (vgl. auch den 6. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten, S. 97 und 98).

3.11.2 Verbilligung der Krankenkassenprämien, Verwechslung zweier Datenbänder

Zur Berechnung der verbilligten Krankenversicherungsprämien stellt der Kanton den Versicherungsgesellschaften Daten über die Prämienreduktionen ihrer Versicherten zu. Bei diesem Vorgehen wurden zwei Bänder verwechselt. Die Versicherungsgesellschaften machten auf die Verwechslung aufmerksam und gaben die Bänder zurück. Der Justiz-, Gemeinde- und Kirchendirektor ordnete eine Überprüfung der verwaltungsinternen Abläufe an. Der Vorfall bestätigt die Risiken der Informatikmittel. Die Reaktion der Verantwortlichen – nicht zuletzt die erfolgte Information der Öffentlichkeit – zeigt aber auch, dass diese Risiken ernst genommen werden.

11. Januar 2000

Der Datenschutzbeauftragte: *Siegenthaler*