Bericht der Aufsichtstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

1997 erarbeiteten die kantonalen Stellen Grundlagen, um das Internet als tragendes Informationsmittel einsetzen zu können. Die sich damit stellenden neuen Datenschutzfragen wurden angegangen. Mit der Einführung eines E-Mail-Systems mit Verschlüsselung zeigte sich deutlich der Bedarf nach übernationalen und nationalen Regelungen. Die Informatiksicherheitsausbildung für das Staatspersonal konnte gestartet werden. Erst in letzter Minute liess sich vorläufig verhindern, dass öffentliche Spitäler künftighin den Krankenversicherern mit der Abrechnung hochdetaillierte Diagnosedaten zustellen.

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

Der Kanton Tessin organisierte die IV. Nationale Konferenz der Datenschutzbeauftragten. Die Konferenz forderte in einer Resolution Krankenversicherer und Spitäler auf, darauf zu verzichten, mit den Abrechnungen hochdetaillierte Diagnosedaten bekanntzugeben. Genau dies zu tun, verpflichteten sich im gleichen Zeitraum Krankenversicherer und Spitäler. Für die Krankenversicherer ist der eidgenössische Datenschutzbeauftragte (EDSB) zuständig, die Spitäler fallen in den Zuständigkeitsbereich der kantonalen Datenschutzaufsichtsstellen. Nur der Zusammenarbeit zwischen den beiden Aufsichtsebenen ist es zu verdanken, dass diese Entwicklung vorerst gestoppt werden konnte (vgl. Ziff. 3.9.1).
Noch offen ist die Frage, welche bundesrechtlichen Voraussetzungen für einen Onlinezugriff der Steuerverwaltung auf die Datenbank des Landwirtschaftsamtes sowie für einen Zugriff der Finanzkontrolle auf die Verlustscheinsdatenbank der Steuerverwaltung gelten.
Schliesslich wies der EDSB die kantonale Datenschutzaufsichtsstelle darauf hin, für mehrere polizeiliche Informatiksysteme des Bundes seien angeschlossene bernische Stellen teilweise nicht in der Lage, die auf den 1. Juli 1998 hin neu geltenden Sicherheitsanforderungen zu erfüllen. Auf diesen Zeitpunkt hin läuft die Übergangsfrist des eidgenössischen Datenschutzgesetzes ab. Neu sind besonders schützenswerte Daten bei der Übertragung zu verschlüsseln.

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Neu versucht die Datenschutzaufsichtsstelle möglichst viele Geschäfte als Tagesgeschäfte zu behandeln. Tagesgeschäfte sind unmittelbar nach dem Posteingang zu erledigen. Das ist kundenfreundlich und verringert in geringem Umfang den Aufwand. Unvermeidbar steigen dadurch die Wartezeiten für die übrigen Geschäfte. Auf eine umfassende Abklärung über Neuzuzügermeldungen wartete eine Gemeinde 21 Monate. Prioritäten: 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. Die immer noch zunehmenden Eingänge erlauben es nicht, Inspektionen vorzunehmen.

3.2.2 Eigenverantwortung der datenbearbeitenden Stellen

Auch 1997 liess eine hohe Zahl von datenbearbeitenden Stellen die Zulässigkeit von Datenbearbeitungen abklären. Neben den üblichen Weiterbildungsanlässen starteten die Direktionen eine Grundausbildung in Informatiksicherheit (Ziff. 3.3). Beigezogen wurde die Datenschutzaufsichtsstelle vermehrt auch zu Fragen des Datenschutzes in Verwaltungsverfahren oder des privatrechtlichen Datenschutzes (vgl. Ziff. 3.4 am Ende). Vermehrt informierten Stellen über in eigener Regie getroffene Datenschutzmassnahmen (z.B. über die Datenschutzmassnahmen für die Dreharbeiten zu einem Kriminalfilm in der Volkswirtschaftsdirektion). Im Vorjahresbericht stellte die Datenschutzaufsichtsstelle fest, einem Teil der Führung fehle es am Interesse für Datensicherheits- und Datenschutzanliegen. Eine Wandlung dieser Haltung innerhalb eines Jahres war nicht zu erwarten und ist auch nicht eingetreten. Ein wichtiges Signal gab aber die Justiz-, Gemeinde- und Kirchendirektion mit ihrem gemeinsam mit dem Obergericht verabschiedeten Pflichtenheft für den EDV-Sicherheitskontrollausschuss: Vorsitzender dieses Ausschusses ist der Generalsekretär. Ebenfalls ein erfreuliches Signal ist der von der Erziehungsdirektion unterbreitete Entwurf zu einer PC-Richtlinie. In dieser Richtlinie wird auch der direktionsintern eingesetzte Datenschutzbeauftragte umschrieben.

3.2.3 Verhältnis Informatikmittel/Mittel für Datenschutz und Datensicherheit

Gemäss einer Rückfrage beim Organisationsamt waren 1997 21,5 Mio. Franken in Informatikmittel zu investieren. 120,6 Mio. Franken sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Mit rund 0,25 Mio. Franken sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert geblieben.
Vereinzelt hat der EDV-Sicherheitsverantwortliche der Justiz-, Gemeinde- und Kirchendirektion bei Bezirksverwaltungen einfache Informatikkontrollen durchgeführt. Er prüfte beispielsweise die verwendeten Passwörter. Bereits diese einfache Prüfung war mit einem erheblichen Arbeitsaufwand verbunden. Prüfungen, wie sie die Informatik erlaubt und nötig macht, wie beispielsweise die Auswertung von Protokolldateien, konnten nicht in Betracht gezogen werden. Die Einsicht hat sich bestätigt, dass die für Datenschutzmassnahmen und -kontrollen zur Verfügung stehenden Mittel in Relation zu den für die Informatik insgesamt zur Verfügung stehenden Mittel zu gering sind.

3.2.4 Neue Aufgaben

Der Regierungsrat regelte einerseits den Betrieb des kantonalen Weitbereichskommunikationsnetzes BEWAN, andererseits den Einsatz und die Nutzung von Internet. Aus beiden Beschlüssen

ergeben sich für die Datenschutzaufsichtsstelle zusätzliche Aufgaben (Betreuung des BEWAN, Betreuung der Internetaktivitäten und Mitwirkung im WWW-Komitee). In den Stellungnahmen zu beiden Regierungsratsbeschlüssen machte die Datenschutzaufsichtsstelle deutlich, dass die neuen Aufgaben nur mit neuen Ressourcen erfüllt werden können. Solche wurden nicht bereitgestellt. Die Beschlüsse sind exemplarisch für die ablaufende Entwicklung: Die durch die Datenschutzaufsichtsstelle von Gesetzes wegen zu betreuenden Aufgaben werden vergrössert, neue Mittel werden nicht bereitgestellt. Insgesamt erfüllt die Datenschutzaufsichtsstelle deswegen ihren gesetzlichen Auftrag laufend schlechter.

3.2.5 Register

1997 blieb das Register wegen fehlender Kapazität praktisch 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. Zu den Registern der gemeinderechtlichen Körperschaften vgl. Ziffer 3.7.

3.3 Datensicherheit

Die mit dem Regierungsratsbeschluss 4637/92 (ursprünglich auf Ende 1994) verlangte Klassifikation der Informatikanwendungen haben die Bau-, Verkehrs- und Energiedirektion (nur Einschätzung) nicht, die Justiz-, Gemeinde- und Kirchendirektion nicht wie vorgegeben (wobei ein weitergehender Sicherheitsbericht vorliegt) ausgearbeitet. Ob die von den übrigen Direktionen eingereichten Klassifikationen richtig sind, ist aus Zeitmangel nach wie vor ungeprüft (vgl. jedoch Ziff. 3.4). Ungeprüft ist auch, ob die vorgesehenen Massnahmen umgesetzt worden sind.
Zwei Direktionen haben – auch im Sinne der Interpellation Galli – interne Sicherheitskontrollorgane geschaffen (vgl. Ziff. 3.2.2).
Informatiksicherheit setzt präzise Vorgaben voraus: Mit der Weisung S02 des Bundesamtes für Informatik und den zugehörigen Unterlagen (Handbuch) lässt sich die im Datenschutzgesetz enthaltene Verpflichtung zu Datensicherheitsmassnahmen auch auf kantonaler Ebene praktikabel konkretisieren.
In der Antwort auf die Interpellation Koch umschrieb der Regierungsrat die für den Jahrtausendwechsel eingeleiteten Massnahmen. Kosten von über 5 Mio. Franken sind absehbar.
Wer im Kanton Bern an einem Computer arbeitet, soll Sicherheitsrisiken kennen und mit ihnen umgehen können. Die entsprechende, flächendeckende Ausbildung begann 1997. Basis bildet die CD-Rom «SAVE». Sie enthält ein interaktives Lernprogramm. Ausgearbeitet hat es unter der Verantwortung des Organisationsamtes ein Projektteam mit Sicherheitsfachleuten und Spezialisten der kantonalen Verwaltung unter Mitwirkung der Gleichstellungsbeauftragten und des Datenschutzbeauftragten. Das mit der Erstellung beauftragte und mitfinanzierende private Konsortium verwendet die gleiche CD, ohne spezifisch bernische Informationen, als Basis für eine CD zur allgemeinen Ausbildung in Informatiksicherheit weiter.

3.4 Informatikprojekte

Mit dem Projekt GEFnet der Gesundheits- und Fürsorgedirektion soll ein direktionsinternes Netzwerk geschaffen und der bestehende zentrale Rechner abgelöst werden. Beispielsweise beim Kantonsarztamt, im Asylbereich und im Umfeld Opferberatung werden besonders schützenswerte Daten bearbeitet. Es ging darum, im Pflichtenheft die diesen Daten angemessenen Datenschutz- und Datensicherheitsanforderungen zu formulieren. Zwischen dem Direktionsnetz und dem kantonalen Weitbereichsnetz BEWAN besteht ein Sicherheitsgefälle. Die Anbieter werden auch für dieses Problem Lösungen vorschlagen müssen.
Das Projekt ZBD des Zivilstands- und Bürgerrechtsdienstes der Polizei- und Militärdirektion soll die bisherige Textverarbeitung und Geschäftskontrolle durch ein in der Abteilung vernetztes System ablösen. Nachdem die (kleine) Abteilung räumlich gut abgeschottet ist, kann trotz der teilweise heiklen Daten auf eine generelle Datenverschlüsselung im Abteilungsnetzwerk verzichtet werden. Für heikle Dokumente ist allenfalls künftig auf die mit dem System BEMail zur Verfügung stehende Mailverschlüsselung zurückzugreifen. Die Informatikstrategie der Polizei- und Militärdirektion klassifiziert die Vertraulichkeit der Daten unrichtig. Sie ist zu korrigieren.
Gegenüber dem KOMKonzept II der Universitätsverwaltung (verschlüsselte Übertragung medizinischer Abrechnungsdaten über das Netz der Universität) war festzuhalten, dass eine kurze Schlüssellänge dann vorerst eingesetzt werden darf, wenn eine Nachrüstung mit längeren Schlüsseln möglich ist.
In einer Stellungnahme zu einem Teilprojekt des Projektes Stipendien 97 der Erziehungsdirektion ging es darum, abzuklären, unter welchen Voraussetzungen Stipendiengesuche auf dem Weg des Internets eingereicht werden könnten. Das Projekt führte über den Geltungsbereich des bernischen Datenschutzgesetzes hinaus (Verfahrensfragen, Datenübertragung durch Private).

3.5 Gesetzgebung

Der Grosse Rat verabschiedete verschiedene Gesetzesänderungen, die Schule, Fürsorge und Vormundschaft von der im Gesetz über das Strafverfahren vorgesehenen Meldepflicht für Verbrechen entlasten.
In einer Volksabstimmung ist das Polizeigesetz angenommen worden. In der parlamentarischen Beratung wurde dem Institut für Rechtsmedizin erlaubt, im Abrufverfahren im erforderlichen Umfang auf Daten der Kantonspolizei zu greifen. Vereinzelte Stimmen sehen in dieser Regelung eine Rechtsgrundlage für die Schaffung einer der Strafverfolgung dienenden Erbgutdatenbank (DNA). Die Datenschutzaufsichtsstelle teilt solche Auffassungen nicht. Gerade auch die aus Sicht der Strafverfolgung hohe Bedeutung einer DNA-Datenbank schliesst es aus, erforderliche gesetzliche Grundlagen gleichsam durch die Hintertür zu schaffen.
Mit einer Änderung der Verordnung über die Organisation der Justiz-, Gemeinde- und Kirchendirektion sind die Informatikverantwortlichen, soweit sie die Informatik der Gerichte betreuen, dem Obergericht unterstellt worden.

3.6 Internet, sicheres E-mail

3.6.1 Internet

Am 2. Juli verabschiedete der Regierungsrat die Weisungen für den Einsatz und die Nutzung von Internet und Angeboten der kantonalen Verwaltung im World Wide Web. Der Regierungsrat ordnet damit, wie der Kanton via Internet und Intranet aktiv informieren soll. Wer verwaltungsintern einen Internetzugriff haben soll, haben die Direktionen festzulegen. Die Datenschutzaufsichtsstelle wirkte bei diesen Weisungen von Anfang an mit. Zu verweisen war auf den im Mai 1996 vom Bundesamt für Justiz herausgegebenen Bericht einer interdepartementalen Arbeitsgruppe zu strafrechtlichen, datenschutzrechtlichen und urheberrechtlichen Fragen rund um Internet. Dieser Bericht enthält einen Teilbericht des Eidgenössischen Datenschutzbeauftragten. Der Einsatz von Internet kann den Persönlichkeitsschutz folgender Personengruppen be-

einträchtigen: a) von Personen, deren Daten der Kanton via Internet bekanntgibt (vgl. Ziff. 3.1.3 des Berichtes 1996), b) von Besuchern kantonaler Informationsangebote, c) des Personals, das Informationen aus dem Internet abruft (vgl. Ziff. 3.7.4 des Berichtes 1996). Dem Kanton fehlen Rechtsgrundlagen, um Daten über Besucher seiner Internetseiten zu bearbeiten. Sicherheitsfragen: Es geht darum, Gefahren aus dem Internet für das kantonale Netz und die angeschlossenen Anwendungen klein zu halten. Die Betreuung der Schnittstelle zum Internet (Firewallrechner) ist eine äusserst aufwendige Aufgabe. Auf neue bekannte Bedrohungen ist umgehend zu reagieren. Einen umfassend sicheren Internetzugang gibt es jedoch nicht. Auch die Internetseiten des Kantons können Angriffsziel sein (Verändern des Inhalts, setzen von Links). Zu verhindern ist schliesslich eine irrtümliche Ablage vertraulicher Information in einem via Internet zugänglichen Bereich. Die Datenschutzaufsichtsstelle hielt fest, dass sie – ohne die damit verbundenen Risiken zu verkennen – die aktive Vorgehensweise des Regierungsrats unterstützt. Wird für den Umgang mit Internet nicht zentral eine für die gesamte Verwaltung einheitliche Lösung angeboten, so entstehen risikoreichere Einzellösungen. Ein dem Datenschutz genügender Einsatz von Internet verlangt ein ständiges Weiterentwickeln der Datensicherheitsmassnahmen und ein Eingehen auf neu entstehende Persönlichkeitsbeeinträchtigungen. Von entscheidender Bedeutung für den gesetzeskonformen Einsatz von Internet wird sein, dass auf allen Ebenen Mittel für die Betreuung der Datenschutzanliegen bereitgestellt werden.

3.6.2 Sicheres E-mail

Mit dem Projekt BEMAIL wird der Kanton auch eine verschlüsselte Übertragung elektronischer Post einführen. Nur wenn eine Mailverschlüsselung zur Verfügung steht, kann das Verbot, heikle Daten mittels Mail zu übertragen, aufgehoben werden (RRB 3457/95). Technisch sind taugliche Verschlüsselungen vorhanden (Public Key Systeme). Technisch realisierbar ist auch die Schlüsselzertifikation. Diesem hohen Stand der Technik hinkt der Stand der Regelungen deutlich nach: Unbeantwortet blieben etwa die Fragen, auf welchem Weg die Zertifizierungsstelle die Schlüssel zu den Berechtigten zu bringen hat, wie sie die Identität der Berechtigten überprüfen muss, welche Haftung sie trifft, welche technischen Voraussetzungen für die Schlüsselaufbewahrung beim Berechtigten einzuhalten sind und wie lange ein Zertifikat gültig sein soll. Eine wichtige Orientierungshilfe liefert die deutsche Signaturgesetzgebung. Das vorerst für den Kanton Bern realisierbare Sicherheitsniveau genügt den deutschen Vorgaben nicht voll (Einsatz von Chipkarten). Tauglich erscheint es zur vertraulichen Übertragung heikler Daten (Vertraulichkeit). Der Schritt zur elektronischen Signatur (Verbindlichkeit) ist noch nicht machbar. Augenfällig hat sich aber gezeigt, dass nur national und international abgestimmte Standards einen elektronischen Dokumentenaustausch mit Vertraulichkeit und Verbindlichkeit ermöglichen können. Die Abhängigkeit von solchen Standards auch für den verwaltungsinternen Mailverkehr zeigt die Dringlichkeit des Problems.

3.7 Gemeinderechtliche Körperschaften

In der bernischen systematischen Information der Gemeinden (BSIG) publizierte die Datenschutzaufsichtsstelle Ansichtsäusserungen über die Datenbekanntgabe durch die Einwohnerkontrolle an Kirchgemeinden und über die Überprüfung von Steuerabzügen.
Die Gemeinde Wohlen stellte ihr vollständiges Register der Datensammlungen fertig.
Zwei Spitalverbände verzichteten auf Intervention der Datenschutzaufsichtsstelle darauf, ihren Patienten unverlangt Telefonabrechnungen zuzustellen, die alle angewählten Nummern vollständig auflisten.
Die Datenschutzaufsichtsstelle wies den Gemeindeschreiberverband schliesslich darauf hin, dass die zum Jahrtausendwechsel zu erwartenden Informatikprobleme auch für gemeinderechtliche Körperschaften ernst sind.

3.8 Berichtspunkte des Vorjahres

3.8.1 Ordnungsbussenzentrale

Das Informatiksystem der Ordnungsbussenzentrale führt aus buchhalterischen Gründen zu einer unzulässigen Registrierung von Ordnungsbussenschuldnern. Das Polizeikommando sicherte bereits 1995 zu, Abhilfe zu schaffen. Dass diese Abhilfe noch nicht erfolgt sei, bemängelte die Datenschutzaufsichtsstelle im Bericht 1996. Mit Direktionsweisung vom 30. Dezember 1997 teilt die Polizei- und Militärdirektion nun mit, aus Kostengründen verzichte sie auf das erforderliche Umprogrammieren des Informatiksystems (technische Massnahme). Ein Ablösen sei für das Jahr 2000 oder 2001 zu planen. Das Informatiksystem dürfe jedoch nur zu den von der Ordnungsbussengesetzgebung vorgesehenen Zwecken verwendet werden. Jeder Versuch einer Auswertung zu andern Zwecken sei unverzüglich dem Polizeikommandanten zu melden. Schliesslich sei das Generalsekretariat halbjährlich über den Vollzug der Weisung zu informieren (organisatorische Massnahme). Mit ihrer Weisung übernimmt die Polizei- und Militärdirektion die Verantwortung für das fehlende Umprogrammieren. Das ist ein anerkennenswerter Schritt zu klaren Verantwortlichkeiten. Die getroffenen organisatorischen Massnahmen werden sich im Vollzug noch zu bewähren haben. Mit der Direktionsanweisung gewichtet die Polizei- und Militärdirektion finanzielle Interessen höher als Datenschutzinteressen. Die Datenschutzaufsichtsstelle hält diese Interessenabwägung hier für unrichtig. Anders als privaten Betroffenen stehen ihr jedoch keine weiteren Interventionsmöglichkeiten mehr offen.

3.8.2 Informatikprojekt KOBI der Kantonspolizei

Unter der Ziffer 3.4 des Berichts 1996 hielt die Datenschutzaufsichtsstelle fest, das Polizeikommando teste im Rahmen des Informatikprojektes KOBI den auch mobilen Einsatz eines Computers. Dieser erlaube es Polizeimitarbeitern gleichzeitig – also ohne erneute Anmeldeformalitäten – über eine Person Anfragen in mehreren polizeilichen Datenbanken vorzunehmen. Die Datenschutzaufsichtsstelle wies darauf hin, dass mit dem System KOBI für einzelne Datenbanken bestehende Regeln zur getrennten Datenbearbeitung unterlaufen werden könnten. Sodann führe die automatische Kombination von für sich allein rechtlich je genügend abgestützten Abfragemöglichkeiten für die Betroffenen zu einem schwereren Eingriff in ihr Grundrecht auf Datenschutz. Ein solcher Eingriff bedürfe einer Rechtsgrundlage. Zudem könne das System mit seinem Universalpasswort zu Sicherheitsproblemen führen. Auch mit gesetzlicher Grundlage sei der Verhältnismässigkeitsgrundsatz zu beachten. Mit Schreiben vom 24. Dezember hielt die Polizei- und Militärdirektion fest, nach Rücksprache mit dem Generalprokurator habe sie den Einsatz des Systems KOBI erlaubt. Die Freigabe sei auch aus übermittlungstechnischen Gründen erforderlich gewesen. Sie diene aber vorab einer effizienten Arbeit im gerichts- wie auch im sicherheitspolizeilichen Bereich. Die polizeilichen Interessen würden die datenschutzrechtlichen Interessen überwiegen. Die Datenschutzaufsichtsstelle teilt auch diese Interessenabwägung der Polizei- und Militärdirektion nicht. Positiv beurteilt sie, dass die Polizei- und Militärdirektion über ihr Vorgehen klar informiert und die Verantwortung für den

Einsatz von KOBI übernimmt. Die sich stellenden Rechtsfragen können allenfalls durch ein Rechtsmittel eines Betroffenen geklärt werden. Ob sich der Regierungsrat mit der Frage befasst, wenn er die Informatiksysteme der Polizei bewilligt (neues Polizeigesetz), ist offen.

3.9 Besonderes

3.9.1 Datenbekanntgabe durch Spitäler an Krankenversicherer

Am 10. September schlossen der Verband bernischer Krankenkassen und der Verband bernischer Krankenhäuser auf den 1. Januar 1998 hin einen Tarifvertrag ab. Die Spitäler verpflichteten sich, den Krankenversicherern mit der Abrechnung die Diagnosedaten gemäss dem Forschungscode ICD-10 und ICD-9 CM mitzuteilen. Diese Angaben sind für die Überprüfung der Wirtschaftlichkeit der Behandlung durch die Krankenversicherer einerseits viel zu detailliert, andererseits teilweise ungeeignet, indem sie über behandlungsrelevante Lebensumstände keine Aussage machen. Für die Spitäler wurde der Vertrag mit deren Zustimmung verbindlich. Praktisch alle Spitalverbände stimmten dem Vertrag zu. Einige brachten Vorbehalte betreffend Datenschutz an. Mit Schreiben vom 5. Dezember empfahl die Datenschutzaufsichtsstelle allen Spitälern, die gewünschten Diagnosedaten bis auf weiteres nicht zu liefern. Sie wies auch auf die Haftungsfolgen und auf die mögliche Strafbarkeit hin. Die beiden Verbände einigten sich in der Folge darauf, den Vertrag diesbezüglich auszusetzen. Es ist davon auszugehen, dass auf eidgenössischer Ebene zwischen dem eidgenössischen Datenschutzbeauftragten und den Krankenversicherern eine Lösung gefunden wird (vgl. Ziff. 3.1.2).

21. Januar 1998

Der Datenschutzbeauftragte: *Siegenthaler*