Bericht der Aufsichtsstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

1998 liessen zwei Verwaltungsstellen ihre Informatiksicherheit durch eine externe Spezialfirma überprüfen. Gerade weil diese mit ihren Zugriffsversuchen (Hackingsimulationen) erfolgreich war, verbesserten die beiden Stellen mit ihrem Vorgehen die Sicherheit ihrer Anwendungen im Ergebnis entscheidend.
Das neue Polizeigesetz verlangt für die Datenbearbeitungssysteme der Polizei eine Betriebsbewilligung des Regierungsrates. Der Gesetzgeber wollte damit eine verstärkte Überprüfung herbeiführen. Als Folge davon musste die Polizei wegen ungenügender gesetzlicher Grundlagen mit dem Einrichten einer DNA-Datenbank (Erbgutsdatenbank) vorerst zuwarten.

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

In einer Resolution forderte die Konferenz, dass DNA-Datenbanken nur gestützt auf klare und bestimmte gesetzliche Grundlagen aufzubauen sind, dass die Aufnahme in eine DNA-Datenbank richterlich überprüfbar sein muss, dass DNA-Fingerprints von freigesprochenen Personen grundsätzlich sofort zu vernichten sind, dass die DNA-Identifizierungsmuster einzig zum Zwecke der Strafverfolgung Verwendung finden dürfen, dass die Aufbewahrungsdauer durch angemessene Prüf- und Löschfristen zu begrenzen ist und dass verantwortliche Labors höchsten Qualitätsansprüchen zu genügen haben. Diese Forderungen stellte die Konferenz nicht nur für den Umgang mit dem DNA-Zahlencode, sondern auch für den Umgang mit dem menschlichen Zellmaterial. Erlaubt eine klare gesetzliche Grundlage dessen Aufbewahrung, so verlangt die Resolution, dass diese Aufbewahrung bei einem unabhängigen Dritten zu erfolgen hat (vgl. auch Ziff. 3.8.2).
Ohne eine ausdrückliche Erlaubnis im Bundesrecht oder im kantonalen Recht dürfen keine Personendaten im Abrufverfahren bekannt gegeben werden. Der eidgenössische Datenschutzbeauftragte hielt dies in seiner (publizierten) Antwort zur Frage nach der Zulässigkeit eines Onlinezugriffs der Steuerverwaltung auf die Datenbank des Landwirtschaftsamtes fest.

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. Diese kundenfreundliche Vorgehensweise lässt die langen – oft überjährigen – Wartezeiten für die übrigen Geschäfte umso störender erscheinen. Unverändert genügen die Ressourcen zu einer Umsetzung der gesetzlichen Aufträge nicht. Insbesondere finden keine Inspektionen statt. An der Wichtigkeit solcher Inspektionen – gerade auch aus Sicht der Daten bearbeitenden Stellen – ist nicht zu zweifeln. Die zur Verfügung stehenden Ressourcen erlauben sie nicht.

3.2.2 Eigenverantwortung der Daten bearbeitenden Stellen

Nach wie vor besteht die Haupttätigkeit der Datenschutzaufsichtsstelle in Stellungnahmen zu Anfragen von amtlichen Stellen. Aus- und Weiterbildung erfolgten im üblichen Umfang. Unterschiedlich ist nach wie vor die Haltung der Führung gegenüber Datenschutzfragen. Hohe Eigenverantwortung bewiesen das Organisationsamt und die Justiz-, Gemeinde- und Kirchendirektion mit den in eigener Regie veranlassten Sicherheitsaudits (vgl. Ziff. 3.1.1 und 3.3.2). Insbesondere wurden die Audits aus direktionseigenen Mitteln finanziert. Dass gerade die Justiz-, Gemeinde- und Kirchendirektion einen Audit durchführen liess, ist hervorzuheben: Der von dieser Direktion eingesetzte Sicherheitskontrollausschuss betreut die Informatiksicherheit der Direktion im Sinne eines ständigen Prozesses. Es dürfte die Eigenverantwortung fördern, wenn entsprechende Prozesse in allen Direktionen verankert würden. In die gleiche Richtung geht das Einsetzen der «Arbeitsgruppe Security» durch die kantonale Informatikkonferenz: Ihre Aufgabe ist es, direktionsübergreifende Sicherheitsfragen zu lösen.

3.2.3 Verhältnis Informatikmittel/Mittel für Datenschutz und Datensicherheit

1998 waren 25,9 Mio. Franken in Informatikmittel zu investieren. 120,4 Mio. Franken sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Mit rund 0,25 Mio. Franken sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert geblieben. Unmittelbar der Datensicherheit dienten die beiden von den Direktionen finanzierten Audits: Das Einsetzen von einigen zehntausend Franken für Kontrollmassnahmen ist erfreulich. Die Prüfungsergebnisse (vgl. Ziff. 3.3.2) zeigen aber vor allem, wie notwendig es ist, das Verhältnis zwischen Gesamtinformatikkosten und Datenschutzkosten zu verändern.

3.2.4 Neue Aufgaben

Als Kontrollorgan für die Einhaltung des Datenschutzes anlässlich der Volkszählung 2000 setzte der Regierungsrat die Datenschutzaufsichtsstelle ein. Der Entwurf zur Verordnung über die eidgenössische Volkszählung 2000 gibt diesem Kontrollorgan ein grosses Pflichtenheft. Ohne zusätzliche Mittel wird diesem Pflichtenheft nicht zu genügen sein. Die gleiche Problematik führte bereits anlässlich der letzten Volkszählung zu einer aufsichtsrechtlichen Eingabe an die Geschäftsprüfungskommission.

3.2.5 Register

1998 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 (zur Frage nach dem Sinn der Registerführung: vgl. auch Ziff. 3.8.1).

3.3 Datensicherheit

3.3.1 Vorgaben des Regierungsrates

Ob die von den Direktionen gestützt auf den Regierungsratsbeschluss 4637/92 eingereichten Klassifikationen richtig sind, ist aus Zeitmangel nach wie vor ungeprüft (vgl. jedoch Ziff. 3.8.1). Ungeprüft ist auch, ob die vorgesehenen Massnahmen umgesetzt worden sind.
In der Verordnung über Niederlassung und Aufenthalt der Schweizer Bürger hielt der Regierungsrat für Onlinezugriffe der Kantonspolizei auf die Einwohnerkontrolle fest, sinngemäss gelte die Weisung S02 des Bundesamts für Informatik. Dieser Vorgabe für Datensicherheitsmassnahmen dürfte für alle Informatikanwendungen Signalwirkung zukommen.
In den überarbeiteten Weisungen für den Umgang mit Passwörtern legte der Regierungsrat neu die Mindestlänge eines Passworts auf sechs Zeichen fest (bisher fünf). Zudem wurden nicht nur detaillierte Weisungen für die Benützerinnen und Benützer, sondern auch solche für die System- und Anwendungsverantwortlichen erlassen. Die durchgeführten Audits haben gezeigt, dass auch die überarbeiteten Weisungen den Sicherheitsanforderungen nicht voll genügen (vgl. auch Ziff. 3.3.2). Wohl wäre eine erneute Anpassung der Weisungen machbar gewesen, deren kurzfristige Umsetzung schien aber kaum möglich. Dies nicht zuletzt deshalb, weil die neuen Weisungen mit dem im Berichtsjahr abgeschlossenen Ausbildungsprogramm Save übereinstimmen. Das Problem ist aber erkannt und wird vom Organisationsamt angegangen.

3.3.2 Audits: Sicherheitschecks

Das Datenschutzgesetz erlaubt grundsätzlich eine Datenbearbeitung durch beauftragte Dritte. Diese Rechtsgrundlage erlaubt es auch, Dritte mit Sicherheitschecks (Hackingsimulationen) zu beauftragen. Voraussetzung bildet, dass bei der Auswahl, Instruktion und Überwachung der Dritten die nötige Sorgfalt angewendet wird. Die Dritten sind rechtlich so einzubinden, dass Missbrauchsgefahren minimiert werden. Staatsintern sind mitbeteiligte Stellen einzubeziehen. So war bei den Sicherheitschecks der Justiz-, Gemeinde- und Kirchendirektion das Obergericht zu informieren.
Aus Sicherheitsgründen kann es nicht angehen, im öffentlichen Bericht das gewählte Vorgehen detailliert zu beschreiben. Detailliertere Informationen werden aber der Geschäftsprüfungskommission des Grossen Rates zu geben sein. Vereinfacht gesagt ging es darum, tatsächlich gegebene Zugriffsmöglichkeiten zu überprüfen. Solche Zugriffsmöglichkeiten wurden tatsächlich auch gefunden. Gesamthaft ergab sich folgendes Bild: Gute Noten erhielt die Anbindung an das Internet, die technische Ausrüstung und Qualität der Installationen sowie die Aufmerksamkeit der Netzbetreiber. Der Firewallbetrieb liess ein Eindringen nicht zu und der Angriff wurde von den Verantwortlichen nicht nur rasch bemerkt, sondern es wurde auch rasch darauf reagiert. Als verbesserungsfähig wurde die physische und organisatorische Zugangsbeschränkung, die Qualität der Passwörter und teilweise weiterer Konfigurationen eingestuft. Viele der festgestellten Mängel konnten durch Umorganisation und Neukonfiguration entschärft werden. Interne Kontrollen der Passwörter scheinen nötig und sind inzwischen eingeleitet.
Die auftraggebenden Stellen haben die Ergebnisse der Audits sehr ernst genommen und die vorgeschlagenen Massnahmen rasch umgesetzt. Dies jedenfalls dort – und das war die Mehrzahl der Empfehlungen –, wo nicht erhebliche finanzielle Mittel (Nachrüstungen, Ersatz) nötig sind. Intern wurden die festgestellten Mängel klar und schonungslos kommuniziert. Die hohe Sensibilisierung der Verantwortlichen war offensichtlich. Aus Sicht der Datenschutzaufsichtsstelle wirkte diese Betroffenheit beinahe unbillig: Einmal spricht vieles dafür, dass in den ungeprüften staatlichen Stellen die Verhältnisse durchaus nicht besser sind, zum andern ist bekannt, dass entsprechende Sicherheitschecks in der Privatwirtschaft ähnliche Ergebnisse zeigten. Daraus ist zu schliessen, dass Informatiksicherheit nicht mit der einmaligen Konfiguration eines Informatiksystems, sondern nur als ständiger Prozess mit ständigen Kontrollen der aufgezeigten Art herbeigeführt werden kann (vgl. Ziff. 3.2.2).

3.3.3 Viren

Viren sind nach wie vor eine schwere Sicherheitsbedrohung. Erstmals begegnete die Datenschutzaufsichtsstelle im Berichtsjahr Virenfalschmeldungen (sogenannte Hoaxes). Diese stellen durch den entstehenden (unbegründeten) Arbeitsaufwand ein Problem dar.

3.4 Gesetzgebung

In mehreren Verordnungsbestimmungen wurden Rechtsgrundlagen für Abrufverfahren geschaffen; so etwa in der Verordnung über Niederlassung und Aufenthalt der Schweizer für die Abrufverfahren der Kantonspolizei in die Einwohnerkontrolle. Auch das Steuergesetz 2001 schafft Rechtsgrundlagen für Abrufverfahren. Dieses Gesetz befasst sich zudem mit der Möglichkeit der elektronischen Steuererklärung. Die Öffentlichkeit des Steuerregisters bleibt unangetastet. Mit der Verordnung über die Ausnahmen von der Pflicht zur Vernichtung polizeilicher Daten wird der vom Gesetz über das Strafverfahren erteilte Regelungsauftrag erfüllt. Vorab Daten von Opfern, vermisster Personen und gemeingefährlicher Personen sowie Daten zur Verfolgung unverjährbarer Verbrechen können über die gesetzlichen Aufbewahrungsfristen hinaus aufbewahrt werden. Die Forschungsverordnung verpflichtet die Ethikkommission bei Bewilligungsverfahren auf weitere Bewilligungserfordernisse hinzuweisen. Im Vordergrund stehen Bewilligungen der eidgenössischen Expertenkommission für das Berufsgeheimnis in der medizinischen Forschung.

3.5 Internet, sicheres E-Mail, Telefonie

3.5.1 Internet

Mehrere Direktionen verfügen heute über Weisungen zur Benützung des Internet durch ihr Personal. Gestützt auf die Weisungen der Staatskanzlei hat die Datenschutzaufsichtsstelle Musterweisungen erstellt. In Missbrauchsfällen – die es erwartungsgemäss gibt – erlauben die Weisungen unter Respektierung des Privatbereichs der Mitarbeitenden eine Kontrolle.
Innert eines Jahres ist Internet in der bernischen Staatsverwaltung alltäglich geworden. Die Mitarbeitenden beschaffen sich Informationen via Internet, Mitarbeitende und Bürger werden vom Staat via Internet informiert. Auch staatliche Internetseiten setzen jedoch

Cookies (Einträge auf der Festplatte des Benutzers, in der Regel harmlos, aber unter Umständen zur Auswertung der Internetgewohnheiten auswertbar) oder animieren zur Kontaktaufnahme mit Verwaltungsstellen via E-Mail, ohne dass auf die damit verbundenen Risiken hingewiesen wird. Dass Cookies nicht zur Überwachung von Besuchern staatlicher Internetseiten eingesetzt werden dürfen, wurde im Vorjahresbericht dargelegt. Wird auf Cookies trotzdem nicht verzichtet, ist den Besuchern zumindest deren konkrete Bedeutung zu erklären. Wird eine Mailverbindung angeboten, so ist darauf hinzuweisen, dass ein Mail etwa die Sicherheit einer Postkarte bietet.

3.5.2 Sicherheit von E-mails

Nach wie vor macht ein Teil der verwaltungsintern versandten E-Mails seinen Weg über ein Rechenzentrum in Warwick (GB). Die mit dem Projekt BE-Mail vorgesehene staatsinterne Mailverschlüsselung befindet sich noch in der Pilotphase mit wenigen sicheren Mailarbeitsplätzen. Die vom Bundesamt für Kommunikation angekündigte Ausarbeitung einer Regelung zur digitalen Signatur bis zum Jahr 2000 erhöht die Chancen auf sichere elektronische Verbindungen in naher Zukunft.

3.5.3 Forschung mit und um Internet

Das soziologische Institut der Universität Bern führte a) in Zusammenarbeit mit einem Grossprovider auf elektronischem Weg eine Befragung von Internetbenützern über ihre Internetgewohnheiten durch und untersuchte b) die Verhaltensweisen von Teilnehmern in Chatgruppen (Schwatzzirkeln). In beiden Fällen wurden die für Forschungsvorhaben zu beachtenden Datenschutzvorgaben nicht eingehalten: Beim ersten Projekt war weder die Sicherheit der elektronischen Antwortübertragung überprüft, noch rechtlich sichergestellt, dass der Grossprovider die ihm zukommenden Antworten nur an das soziologische Institut weiterleitete. Bei einem allfälligen Missbrauch hätte der Kanton beispielsweise die Kosten von einigen hundert Franken pro antwortende Person für den Wechsel der Internetadresse übernehmen müssen. Auch wenn dies ein Bagatellschaden wäre, ist das Schadenspotenzial in Anbetracht von 17 000 antwortenden Personen doch durchaus erheblich. Die Fragebogen enthielten zudem besonders schützenswerte Daten. Gegenüber dem zweiten Projekt war deutlich zu machen, dass es unzulässig ist, die Nutzungsfrequenzen von nicht anonymen Teilnehmern in Chatgruppen ohne deren Zustimmung aufzuzeichnen.

3.5.4 Telefonkosten

In einer Stellungnahme zuhanden der Geschäftsprüfungskommission des Grossen Rates hielt die Datenschutzaufsichtsstelle im Wesentlichen fest, die bestehenden Rechtsgrundlagen erlaubten es weder der vorgesetzten Stelle noch der Finanzkontrolle, zu Kontrollzwecken die anfallenden Telefoniedaten umfassend auszuwerten (Nr. des Anrufenden, Nr. des Angerufenen, Zeitpunkt des Gesprächs, Dauer, Kosten).

3.6 Gemeinderechtliche Körperschaften

Nach einem «Beobachter»-Artikel über missbräuchliche Datenbearbeitungen durch Gemeinden stiegen die Rückfragen von Gemeindebehörden bei der Datenschutzaufsichtsstelle – auch wenn bernische Gemeinden nicht genannt waren – an. Häufig war ein gutes Problembewusststein der Verantwortlichen in den Gemeinden festzustellen: So erfolgte etwa eine Rückfrage über die Zulässigkeit der Bekanntgabe von Asylbewerberdaten oder einer Identitätskartenfoto zu Fahndungszwecken. Im ersten Fall war der Umfang der Datenbekanntgabe einzuschränken, im zweiten auf die Notwendigkeit einer untersuchungsrichterlichen Anordnung gemäss Strafverfahren hinzuweisen. Zwei kommunale Datenschutzaufsichtsstellen – gleichzeitig Rechnungsprüfungskommission – wiesen die Datenschutzaufsichtsstelle darauf hin, dass im Rahmen der Rechnungsrevision ungenügende Informatiksicherheitsmassnahmen für alle Informatikmittel der Gemeinde festgestellt worden seien. Es wurde angeregt, kantonale Stellen sollten mit Ausbildungsmöglichkeiten und miliztauglichen Checklisten Unterstützung leisten.
Die gleichen Fragen wie beim Kanton stellen sich den Gemeinden auch betreffend Telefonie.
Die von den Gemeinden gebildete Interessengemeinschaft zeigt unter anderem, dass das Jahr-2000-Problem grundsätzlich erkannt worden ist.

3.7 Berichtspunkte des Vorjahrs

3.7.1 Datenbekanntgabe durch Spitäler an Krankenversicherer

Die eidgenössischen Stellen klären zurzeit noch, welche Daten die Spitäler den Krankenkassen für Abrechnungen liefern sollen. Die von der Datenschutzaufsichtsstelle am 5. Dezember 1997 abgegebene Empfehlung, die gewünschten Diagnosedaten gemäss dem Forschungscode ICD-10 seien bis auf weiteres nicht zu liefern, gilt daher nach wie vor.

3.8 Besonderes

3.8.1 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Das Polizeigesetz verpflichtet die Kantonspolizei, für ihre Datenbearbeitungssysteme beim Regierungsrat eine Betriebsbewilligung einzuholen. Der Bewilligungsinhalt ist im Gesetz detailliert geregelt. Erwartungsgemäss vertraten Kantonspolizei und Datenschutzaufsichtsstelle über die Umsetzung dieser Vorgaben unterschiedliche Auffassungen. Die Datenschutzaufsichtsstelle nahm in einem 18-seitigen Papier Stellung. Über den weiteren Verlauf des Bewilligungsverfahrens wird nach Vorliegen des Regierungsratsbeschlusses zu berichten sein.
Bereits heute zeigen sich jedoch Probleme in der Datenschutzaufsicht gegenüber der Polizei: So zeigte sich, dass die Klassifikation der Informatikanwendungen des Polizeikommandos gemäss Regierungsratsbeschluss 4637/92 (Klassifikation betreffend Vertraulichkeit und Verfügbarkeit) vervollständigt und berichtigt werden muss. Die Vollständigkeit der Bewilligung müsste zudem anhand des Registers der Datensammlungen überprüft werden können. Eine solche Prüfung war jedoch nicht möglich, da die Kantonspolizei der ihr seit 10 Jahren obliegenden Meldepflicht bis heute nicht nachgekommen ist. Die der Datenschutzaufsichtsstelle vorliegenden polizeiinternen Arbeitsunterlagen für eine Anmeldung erlauben die erforderliche Überprüfung nicht.
Zu Recht werden heute Zweifel am Nutzen zumindest eines zentralen Registers der Datensammlungen angemeldet. Problematisch erscheint jedoch, dass ein Grossteil der übrigen Verwaltungsstellen mit erheblichem Aufwand ihrer Anmeldepflicht nachgekommen ist, die Kantonspolizei den gerade auch im Hinblick auf ihre Datensammlungen ergangenen entsprechenden Regierungsratsbeschluss bis heute noch nicht umgesetzt hat.

3.8.2 **DNA-Datenbank**

Mit Stellungnahme vom 14. Dezember 1998 empfahl das Rechtsamt der Justiz-, Gemeinde- und Kirchendirektion der Polizei- und Militärdirektion den Einsatz einer DNA-Datenbank in einem formellen Gesetz ausdrücklich zu regeln. Die Vorarbeiten für eine Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei (vgl. Ziff. 3.8.1 und 3.1.1) sowie zur Resolution der Nationalen Konferenz der Datenschutzbeauftragten (vgl. Ziff. 3.1.2) ermöglichten es, dass ein entsprechender interner Vorentwurf bereits Ende August bestand. Die veröffentlichten Anträge zu dem inzwischen in Deutschland in Kraft getretenen DNA-Identitätsfeststellungsgesetz waren für diese Vorarbeiten eine wichtige Unterlage.

15. Januar 1999

Der Datenschutzbeauftragte: *Siegenthaler*