Bericht der Aufsichtsstelle für Datenschutz

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Erst die externe Datenschutzkontrolle erlaube es ihm, seine Führungsverantwortung wahrzunehmen, hielt der scheidende Kantonsarzt an der Schlussbesprechung zur Datenschutzkontrolle beim Kantonsarztamt fest. Das zeigt die Notwendigkeit solcher Kontrollen. Der Regierungsrat hat im Jahr 2004 drei weitere Amtsstellen verpflichtet, eine externe Datenschutzkontrolle zu organisieren.
Die Sicherheits-Sollvorgaben für die Informatik genügen den aktuellen Bedürfnissen nicht mehr und müssen weiter entwickelt werden. Diese Feststellung des beauftragten Gutachters nahm der Regierungsrat zum Anlass, dem Organisationsamt einen Auftrag zur Überarbeitung der Sicherheits-Sollvorgaben bis Ende 2005 zu geben.

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

Informationen zu geklärten und ungeklärten Sexual- und Tötungsdelikten speichert die Kantonspolizei Bern für alle schweizerischen Polizeikorps in der Datenbank des Systems VICLAS. Mit dem System soll die «Handschrift» des Täters erkannt und seine Überführung ermöglicht werden. Die Kantonspolizei Bern betreibt VICLAS in Absprache mit der Konferenz der kantonalen Polizeikommandanten der Schweiz. An diese wandte sich die Vereinigung der Schweizerischen Datenschutzbeauftragten mit dem Hinweis, einer schweizweit wirkenden Datenbank sei zuzustimmen, sie bedürfe aber einer gesetzlichen Grundlage, beispielsweise in einem Konkordat (s. zur Zusammenarbeit mit der Arbeitsgruppe Gesundheit und dem Eidgenössischen Datenschutzbeauftragten zu Tarmed 3.7.2, zu APDRG 3.7.3, zu Vernehmlassungen zu Bundeserlassen 3.6.1, zur Liste über Lehrpersonen mit Entzug der Lehrbefugnis 3.9.4).

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Für das Bearbeiten der Geschäfte gilt folgende Prioritätenfolge: 1. Datenschutzkonzepte für Informatikprojekte, 2. Betreuung des Beizugs externer Kontrollstellen, 3. Allgemeine Gesetzgebung vor Spezialerlassen, 4. Generelle Weisungen vor Einzelfällen, 5. Beratung und Instruktion und 6. Einzelprobleme mit vielen Betroffenen vor solchen mit wenig Betroffenen und geringen Wiederholungschancen.
Im Informatikprojekt Schulverwaltungslösung für Mittelschulen EVENTO (s. 3.4.1) war bei der Behandlung des Datenschutzkonzeptes zu prüfen, ob den über 30 Rollen der Zugriff auf die über 200 Datenfelder je richtig zugeordnet war. Solche Prüfungen sind mit erheblichem Aufwand verbunden. Für die Betreuung von Datenschutzkonzepten ist dies symptomatisch. Die nötigen Ressourcen hierzu fehlen. Bereits im Regierungsratsbeschluss, der die Datenschutzkonzepte vorschreibt, wurde von einem Ressourcenengpass ausgegangen. Vorgesehen war, ein Projekt auch ohne Prüfbericht zu beschliessen, wenn die Ressourcen eine Prüfung bis zum Ausgabenbeschluss nicht erlauben. In der Praxis hilft diese Möglichkeit aber wenig: Datenschutzkonzepte werden regelmässig erst nach dem Ausgabenbeschluss in der definitiven Fassung unterbreitet. Die Projektverantwortlichen erwarten aber gerade auch zum bereinigten Datenschutzkonzept eine Rückmeldung der Datenschutzaufsichtsstelle.

3.2.2 Eigenverantwortung der Daten bearbeitenden Stellen

Zum Beispiel der Entwurf einer Weisung über den Umgang mit Personendaten der Lehrerinnen- und Lehrerbildung oder die Abklärungen der Steuerverwaltung zum Fragebogen zu behinderungsbedingten Kosten zeigen das Engagement der Daten bearbeitenden Stellen. (Zur Sicherheitszertifizierung der BEDAG-Informatik AG s. 3.2.4).

3.2.3 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2004 waren 40 Millionen Franken in Informatikmittel zu investieren. 149 Millionen Franken (davon 64 Mio. Franken für Drittdienstleister) sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). Für die Prüfung von Informatikanwendungen durch externe Prüfstellen stand der Betrag von 130000 Franken zur Verfügung (s. 3.2.4). Das Organisationsamt finanzierte das Gutachten zur Weiterentwicklung der aktuellen Informatiksicherheits-Sollvorgaben (s. 3.3.1). Im Rahmen des Projektes BEKISPlus (s. 3.7.1) stellte die Gesundheits- und Fürsorgedirektion erhebliche Mittel für die Ausarbeitung eines Rahmendatenschutzkonzeptes in den Spitälern zur Verfügung. In den Ausgaben für Informatikprojekte sind auch Aufwendungen für die Erstellung von Datenschutzkonzepten enthalten. Die Beratung von Gemeinden und Verwaltungsstellen in Datenschutzfragen durch die fachlich zuständigen Rechtsdienste bringt ebenfalls eine Bindung von Ressourcen für den Datenschutz mit sich. Das Verhältnis von Informatikmitteln und Datenschutzmitteln hat sich damit insgesamt etwas verbessert.

3.2.4 Kontrollen von Informatikdatenbearbeitungen

Wird eine Organisationseinheit vom Regierungsrat mit der Organisation einer Datenschutzkontrolle durch Externe beauftragt, hat sie das Kontrollmandat in einem schriftlichen Vertrag nach den allgemeinen Geschäftsbedingungen der Schweizerischen Informatikkonferenz festzuhalten. Der Vertrag muss vor Abschluss der Datenschutzaufsichtsstelle zur Genehmigung unterbreitet werden. Der Regierungsrat hält den Gegenstand der Kontrolle in seinem Prüfplan fest. Eine Vollprüfung hat den Datenschutz (Rechtsgrundlagen, Verhältnismässigkeit der Zugriffsrechte, Umsetzung der Rechte der betroffenen Personen) die Informatiksicherheit und die Datenschutzorganisation zu umfassen. Das Kontrollmandat darf nur an externe Stellen erteilt werden, die die fachlichen Anforderungen erfüllen (informatiktechnisches Fachwissen, rechtliches Wissen, Revisionswissen) und unabhängig sind. Die externen Fachstellen sind darauf

hinzuweisen, dass sie einen amtlichen Auftrag erfüllen und damit dem Amtsgeheimnis unterstehen. Sie haben ein Prüfungsprogramm zu erstellen. Als Kontrollmittel stehen ihnen Befragungen von Mitarbeitenden, Unterlagen, Vorführungen von Informatikanwendungen und Zugriffe auf Informatikmittel zu. Ein «ethical hacking» ist ihnen erlaubt. Als Prüfungsergebnis hat die externe Fachstelle einen Kontrollbericht abzufassen und Empfehlungen für Verbesserungsmassnahmen zu machen. Der Bericht ist mündlich zu erläutern und die Datenschutzaufsichtsstelle ist mit einer Kopie zu bedienen. Diese generellen Rahmenbedingungen hielt der Regierungsrat Mitte Jahr fest. In einem weiteren Beschluss verabschiedete er den Prüfplan für 2004 (s. 3.1.1).
Zeigte die Prüfung der Datenbanken und der Windows/Office-Umgebung beim Kantonsarztamt Verbesserungsmöglichkeiten in der Informatiksicherheit und bei den Zugriffsberechtigungen, waren bei der Informatikanwendung JABIS (Verwaltung der Jagdpatente, Kontrolle von Jagdstrafen und -massnahmen, Jagdstatistik) Verbesserungsmöglichkeiten bei der rechtlichen Verankerung festzustellen. Das Amt für Betriebswirtschaft und Aufsicht der Justizdirektion löste gegenüber dem System Tribuna (Geschäftskontrollsystem der Gerichte) eine Teilprüfung aus. Gegenstand war die Datenlöschung. Es zeigte sich, dass ein Löschkonzept fehlt und Einträge über Bagatellbussen entgegen der bundesrechtlichen Vorgabe nicht gelöscht und bei erneuten Strafverfahren unzulässigerweise beigezogen werden. Die vom Polizeikommando durchzuführende Überprüfung der Ordnungsbussenzentrale war zum Zeitpunkt der Berichterstattung noch nicht abgeschlossen.
Eine erste Bilanz zum neuen Vorgehen zeigt, dass genügend qualifizierte Fachstellen gefunden werden konnten. Die Mandatserteilung und -betreuung erfordert von den betroffenen Stellen ein hohes Engagement. Dieses Engagement haben die Verwaltungsstellen auch erbracht. Die Bereitschaft, gemachte Verbesserungsvorschläge aufzunehmen, war hoch. (s. auch 3.1.1).
Die Finanzkontrolle hat im Rahmen der Wirtschaftsprüfung die Risikobeurteilung im Informatikbereich der Dienststellen weitergeführt.
Den im BEDAG-Gesetz umschriebenen Auftrag zu einer jährlichen schwerpunktmässigen Prüfung der Informatiksicherheit durch eine externe Fachstelle setzte die BEDAG-Informatik AG durch einen Zertifizierungsaudit ihrer Informatiksicherheit nach dem British Standard BS 7799-2: 2002 um. Die BEDAG-Informatik AG wurde nach diesem Standart zertifiziert. Sie zeigt mit diesem Schritt, dass sie die Datensicherheit ernst nimmt.

3.3 Datensicherheit

3.3.1 Sollvorgaben

Der zur Frage der Weiterentwicklung der aktuellen Informatiksicherheits-Sollvorgaben beigezogene Gutachter schlägt folgende Schritte vor: Mit einer Informations- und Datenschutzanalyse soll künftig für alle Informatikprojekte festgestellt werden, ob sie zu heiklen Datenbearbeitungen führen. Ist dies der Fall, soll unabhängig von den Kosten des Projektes die Datenschutzaufsichtsstelle beigezogen werden und es ist ein Informationssicherheits- und Datenschutzkonzept zu erstellen. Zudem soll die Projektrolle eines Informationssicherheits- und Datenschutzverantwortlichen besetzt werden. Die Informationssicherheit und der Datenschutz sollen bei der Qualitätskontrolle thematisiert werden. Die Inbetriebnahme des Systems soll erst erfolgen, wenn zu Datenschutz und Informationssicherheit ein genügender Stand ausgewiesen ist. Der Projektabschlussbericht soll auch der Datenschutzaufsichtsstelle zugestellt werden. Die Mindestanforderungen an die Datensicherheit sowie der IT-Zonenplan sollen durch einen Regierungsratsbeschluss, eventuell durch eine Verordnung, in folgenden Punkten ergänzt werden: Verbesserte Klassifizierung der Systeme, verbindliches Festlegen von organisatorischen und technischen Massnahmen für den Grundschutz, Aufwerten der Risikoanalyse. Diese soll die Grundlage bilden für notwendige Massnahmen, die über den Grundschutz hinausgehen. Der Gutachter regt zudem an, die Ausbildung für Projektverantwortliche und Projektsachbearbeiter auf dem Gebiet der Informationssicherheit und des Datenschutzes zu verbessern und die Wegleitung für die Abwicklung von Informatikprojekten an HERMES 2003 anzupassen. Der Regierungsrat hat diese Vorschläge aufgenommen und dem Organisationsamt den Auftrag erteilt, bis Ende 2005 die gemachten Empfehlungen umzusetzen. (s. auch 3.1.1).
Die künftigen Informatiksicherheits-Sollvorgaben werden es erlauben, in den Verträgen mit der BEDAG-Informatik AG die zu erbringende Informatiksicherheit zu definieren. Das BEDAG-Gesetz verlangt dies. Nach dem Muster des Kantons Zürich wurden hierzu vom Organisationsamt allgemeine Geschäftsbedingungen über die Informationssicherheit und den Datenschutz beim Erbringen von Informatikdienstleistungen ausgearbeitet.

3.3.2 Sicherheit von E-Mail

Die kantonale Informatikkonferenz beschloss eine erste Testinstallation für SecureMail auszubauen (Einsatz von auf dem Markt erhältlichen Klasse-2-Zertifikaten und Soft-Tokens). Dieser Ausbau soll als Entscheidgrundlage für eine spätere Einführung dienen. Der Betrieb eines sicheren Mailsystems setzt den Aufbau einer Infrastruktur zur Erstellung und Verteilung des öffentlichen und privaten Schlüssels voraus (so genannte PKI-Infrastruktur). Da der Bund zur Zeit unter anderem für den sicheren Zugriff kantonaler Stellen auf Bundesanwendungen mit dem Aufbau von PKI-Infrastrukturen befasst ist, hielt die kantonale Informatikkonferenz fest, der Entscheid über die Einführung von SecureMail dürfe definitiv erst gefällt werden, wenn die Situation auf Bundesebene beurteilbar sei (Kompatibilität). (S. zum Virus Sober-I: 3.5).

3.4 Informatikprojekte

Die Vorgabe des Regierungsrats, Informatikprojekte ab 100000 Franken nur mit einem Datenschutzkonzept zum Ausgabenbeschluss zu unterbreiten, wird noch nicht konsequent beachtet. So wurden etwa Beiträge an die Informatikinfrastruktur im Spitalzentrum Biel oder an das Radiologieinformationssystem des Spitals Interlaken ohne Datenschutzkonzept beschlossen. Mit dem Spitalamt soll nun versucht werden, für künftige Projekte eine Umsetzung der Vorgabe sicherzustellen.

3.4.1 Betreute Projekte

Ein Datenschutzkonzept unterbreiteten die Projektleitungen für die Projekte EVENTO (früher VITSEK II, s. 3.2.1 und 3.5), eSVReg/GINA NT 2 (Elektronisches Strafvollzugsregister und Insassenverwaltungssystem), PERSISKA-Erneuerung (kantonsweites Personalverwaltungsinformationssystem) und BESIS II (Vollzug der kantonsweiten IT-Harmonisierung in den psychiatrischen Kliniken).
Zum Projekt ZEUS (Zivilstandsereignisse und Statistiken) wurde eine Informations- und Datenschutzanalyse unterbreitet. Diese bejaht die Notwendigkeit eines Datenschutzkonzeptes.
Schliesslich wurde das Sicherheitskonzept zum kantonalen IT-Harmonisierungsprojekt RENO fertiggestellt. Gerade das Sicherheitskonzept RENO und das Datenschutzkonzept BESIS II zeigen wie komplex die Informatikumgebung des Kantons Bern geworden ist: So war für BESIS II zu prüfen, ob die durch RENO von den einzelnen Organisationseinheiten verlangten Regelungen tatsächlich getroffen worden waren. Umgekehrt war für RENO zu prüfen, ob die Einbindung des Outsourcingpartners den hohen Sicherheitsansprüchen genügt, die die Datenbearbeitung durch psychiatrische Kliniken stellt.

Obwohl er weniger als 100000 Franken kostet, wurde vom Strassenverkehrs- und Schifffahrtsamt der eAutoindex der Datenschutzaufsichtsstelle unterbreitet. Dieses Projekt soll den Versicherungsgesellschaften den Zugriff auf die Halterdaten ihrer Versicherten via Internet ermöglichen. Der beigezogene Outsourcingpartner hat seinen Sitz im Fürstentum Lichtenstein, was zu einer Datenbearbeitung im Ausland führt. Auf die Möglichkeit, Privatpersonen einen Zugriff auf die Halterdaten einzuräumen, wurde verzichtet. Die neue Abrufmöglichkeit der Versicherer war in einer Verordnungsbestimmung zu verankern. (Zu den bei der Behandlung von Datenschutzkonzepten entstandenen Ressourcenproblemen s. 3.2.1).

3.5 Internet und E-Government

Beim Informatikprojekt EVENTO (s. 3.4.1) verzichtete die Projektleitung vorerst darauf, den Lehrkräften Noteneinträge über Internet zu ermöglichen. Eine genügende Datensicherheit konnte für diese Lösung vorerst nicht herbeigeführt werden. (Zum eAutoindex s. 3.4.1). Der Virus Sober-I war gegen Ende Jahr Anlass, die Mail-Empfänger der Kantonsverwaltung vorübergehend nicht mehr über den Eingang von mit diesem Virus verseuchten Mails zu informieren. Diese Massnahme wurde vorgängig angekündigt. Mehr als elf Prozent aller ankommenden Mails waren insgesamt mit diesem Virus verseucht. Für einzelne Benutzer betrug der Eingang an Virenmeldungen weit über die Hälfte ihrer Maileingänge. Die Datenschutzaufsichtsstelle hält die getroffene Massnahme für gerechtfertigt.

3.6 Gesetzgebung

3.6.1 Bundeserlasse

Zur Bahnreform 2 (unter anderem Videoüberwachung in Zügen), zum Bundesgesetz über die sektoriellen Personenidentifikatoren (SPING) und zur DNA-Profil-Verordnung (s. 3.9.1) verwies die Datenschutzaufsichtsstelle kantonsintern jeweils auf die Stellungnahme der Vereinigung der Schweizerischen Datenschutzbeauftragten.

3.6.2 Kantonale Erlasse

Die Arbeiten an der GEO-Datenverordnung wurden weitergeführt. Neben mehreren Stellungnahmen zu Einzelbestimmungen (s. zum eAutoindex 3.4.1) arbeitete die Datenschutzaufsichtsstelle an der Überarbeitung der GRUDIS-Verordnung mit.

3.7 Gesundheitswesen

3.7.1 Bernisches Klinikinformationssystem (BEKISPlus)

Der Grosse Rat lehnte das Projekt für ein Klinikinformationssystem für alle öffentlichen Spitäler des Kantons (BEKIS) ab und wies die Gesundheits- und Fürsorgedirektion an, dezentrale Klinikinformationssysteme zu projektieren (BEKISPlus). Für das Spitalamt verfasste eine externe Stelle ein Rahmendatenschutzkonzept für Spitäler (s. auch 3.2.3). Dieses Konzept ist gerade für die dezentrale Projektierung, aber auch für den Datenschutz in Spitälern generell, eine wichtige Grundlage.

3.7.2 Tarmed

In seinem Bericht zu Tarmed hielt der Eidgenössische Datenschutzbeauftragte fest, die vorgesehene systematische, personenbezogene Datenbearbeitung sei unverhältnismässig, für einzelne Aufgaben der Versicherer sei nicht immer der ganze personenbezogene Datensatz erforderlich und die Gesetzgebung verpflichte die Versicherer ein Bearbeitungsreglement zu erstellen. Insgesamt zeigte sich, dass die aus Tarmed folgende Datenbearbeitung bei den Versicherern die Datenschutzrechte der Patienten gefährden kann.
In Zusammenarbeit mit der Arbeitsgruppe Gesundheit der Vereinigung der Schweizerischen Datenschutzbeauftragten verfasste die Datenschutzaufsichtsstelle eine Empfehlung an alle öffentlichen Spitäler. Darin empfahl sie, die Patienten über die Situation bei den Abrechnungen zu informieren, den Normalfall sprengende Tarmedabrechnungen nur dem Vertrauensarzt zuzustellen, den Versicherern vorerst jegliche systematische Bekanntgabe von Diagnosedaten zu verweigern und diese einzig auf Nachfrage hin im Einzelfall – und nur soweit verhältnismässig – bekannt zu geben.

3.7.3 APDRG

Im Einverständnis mit dem Spitalamt rechnen das Inselspital und die Spitäler Thun und Aarberg für die Unfallversicherungen, die Militärversicherung und die Invalidenversicherung in einem Pilotversuch nach APDRG ab (Abrechnung nach 641 Fallpauschalen, All Patient Diagnoses Related Groups). Das Spitalamt erkundigte sich beim Eidgenössischen Datenschutzbeauftragten vor dem Versuch nach dessen Zulässigkeit. Der Eidgenössische Datenschutzbeauftragte hielt fest, für eine Abrechnung mit APDRG fehle die erforderliche gesetzliche Grundlage. Werde trotzdem – und ohne Zustimmung des Patienten – mit APDRG abgerechnet, stelle dies eine Verletzung des Amtsgeheimnisses und des ärztlichen Berufsgeheimnisses dar. Das Spitalamt hat den Pilotversuch ungeachtet dieser Rechtslage gestartet. Es wies darauf hin, in andern Kantonen werde auch nach APDRG abgerechnet. Gemeinsam mit der Medizinaltarifkommission werde mit dem Eidgenössischen Datenschutzbeauftragten das Gespräch gesucht.

3.8 Gemeinderechtliche Körperschaften

Vermehrt erkundigen sich gemeinderechtliche Körperschaften nach den rechtlichen Rahmenbedingungen für eine Videoüberwachung des öffentlichen Grundes. Sie können auf die im Internet publizierten Berichte der Kantone Basel-Landschaft und Zürich verwiesen werden. Soll eine Aufzeichnung stattfinden, bedingt dies eine Rechtsgrundlage in einem Gemeindereglement. Zunehmend überwachen auch Privatpersonen mit Videokameras den öffentlichen Grund. Die Bau-, Verkehrs- und Energiedirektion hielt auf Rückfrage hin fest, die Gesetzgebung über Bau und Unterhalt der Strassen erlaube es einer Gemeinde nicht, sich gegen ein solches Vorgehen mit einer Verfügung zur Wehr zu setzen.
Die Gemeinde Langenthal hat ein umfassendes Informatiksicherheitskonzept ausgearbeitet. Fragen kleinerer und mittlerer Gemeinden, welche Sicherheitsmassnahmen sie zu treffen haben, können sie neuerdings auf die von der Stiftung InfoSurance für kleine und mittlere Unternehmungen vorgeschlagenen Sicherheitsmassnahmen verwiesen werden. Diese sind auf Internet publiziert.
(Zur Überwachung des Fernmeldeverkehrs gegenüber Gemeinden s. 3.10.2).

3.9 Berichtspunkte des Vorjahres
(s. 3.7.2 und 3.7.3)

3.9.1 DNA

Auf Anfang 2005 hin tritt das Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von un-

bekannten und vermissten Personen und die zugehörige Verordnung in Kraft (s. 3.6.1). Die neuen Erlasse verlangen eine Datenvernichtung von Amtes wegen. Die hierzu erforderlichen Meldeflüsse sollen in einer kantonalen Verordnung umschrieben werden.

3.9.2 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Der Regierungsrat hat die Betriebsbewilligung für die Ordnungsbussenzentrale erteilt. Dagegen liegt für die Bewilligung der Datenbank des Dezernats Personenfahndung nach wie vor erst ein Bewilligungsentwurf vor. Die in der Betriebsbewilligung vom Januar 2001 verlangte Protokollierung der Lesezugriffe auf das Subsystem OBORA (Journaleinträge) soll auf Anfang 2005 – mit zweijähriger Verspätung – in Betrieb genommen werden.

Zuhanden des Grossen Rats bewilligte der Regierungsrat die Fernüberwachung von Lichtsignalen (mit Digitalkameras zur Geschwindigkeitsüberwachung und zur Erfassung von Rotlichtmissachtungen). Dieses Informatikprojekt benötigt kein Datenschutzkonzept. Die Datenschutzrahmenbedingungen sind vielmehr in der Betriebsbewilligung zu regeln. Gleiches gilt für das Informatikprojekt Metamorphose UVEK. Der Regierungsrat bewilligte mit diesem Projekt einen Online-Zugriff auf die Datenbank des Dienstes für besondere Aufträge des UVEK. Diesem obliegt die Überwachung des Post- und Fernmeldeverkehrs. Gleichzeitig wurden mehrere Abhörarbeitsplätze und DVD-Schreibgeräte bewilligt. Nach der neuen Regelung des Bundesgesetzes über die Überwachung des Post- und Fernmeldeverkehrs bleiben die Gesprächsaufnahmen während der langen Aufbewahrungszeiten für Daten zur Strafverfolgung bei der Polizei gespeichert. Dies betrifft auch Gesprächsaufzeichnungen völlig unbeteiligter Dritter. Wer auf diese Daten Zugriff haben soll, ist besonders sorgfältig zu regeln. (Zur Datenbank VICLAS s. 3.1.2).

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

Das Bundesamt für Sozialversicherung hat seinen im Vorjahresbericht erwähnten Entscheid zur Widerrechtlichkeit von Blankovollmachten in Wiedererwägung gezogen. Grund hierzu bildete ein vor dem Verwaltungsgericht hängiges ordentliches Rechtsmittelverfahren in der gleichen Frage. Der Entscheid des Verwaltungsgerichtes steht noch aus.

3.9.4 Liste der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren über Lehrpersonen mit Entzug der Lehrbefugnis/Unterrichtsberechtigung

Die Schweizerische Konferenz der kantonalen Erziehungsdirektoren (EDK) hat den Kantonen eine Konkordatsänderung unterbreitet, worin die vorgesehene Liste verankert werden soll. Den Einwendungen der Vereinigung der Schweizerischen Datenschutzbeauftragten wird damit Rechnung getragen. Im Kanton Bern soll zudem im Lehreranstellungsgesetz eine Rechtsgrundlage für Meldungen in diese Liste geschaffen werden.

3.9.5 Kontrollen der Informatikdatenbearbeitungen im Amt für Sozialversicherungen und Stiftungsaufsicht

Dem Auftrag aus der Krankenversicherungsverordnung zum Aufbau eines internen Kontrollsystems und zum regelmässigen Beizug einer externen Datenschutzkontrollstelle soll durch die eingeleitete Zertifizierung nach GoodPriv@cy nachgekommen werden.

3.10 Besonderes

3.10.1 Vorübergehend zu weit gehende Zugriffsrechte für Gemeinden in der Informatik-Anwendung IS-NESKO der Steuerverwaltung

Die Steuerverwaltung hat das System IS-NESKO in den Jahren 2002 und 2003 für alle rund 370 angeschlossenen Gemeinden ohne örtliche Eingrenzung des Zugriffs – also kantonsweit – geöffnet. Dies, weil es informatiktechnisch nicht möglich war, allein den zu diesem Zeitpunkt neu geschaffenen Erfassungszentren (27) und den neu für den Steuererlass zuständigen Erlassgemeinden (18) einen kantonsweiten Zugriff einzurichten. Dieses Vorgehen führte zu einem unverhältnismässigen Zugriff: Vorab kleinere und mittlere Gemeinden hatten wesentlich mehr Daten zur Verfügung, als sie zum Erfüllen ihrer Aufgaben benötigten. Zu den Veranlagungsdaten (wie steuerbares Einkommen und Vermögen) waren jedoch keine Details zugänglich. Das System IS-NESKO wird Anfang 2005 in das System TaxCellence übergeführt. Das neue System erlaubt es nun, die erforderlichen örtlichen Zugriffseinschränkungen umzusetzen. Die Registerdaten (wie Adresse, Zivilstand, Beruf, Familienstruktur, steuerrelevante Konfession) sollen allerdings auch unter TaxCellence kantonsweit offen bleiben. Dies etwa zur Erfassung auswärtiger Grundeigentümer. Ob und allenfalls unter welchen näheren Rahmenbedingungen (z. B. Protokollierung der Zugriffe und Sanktionen bei Missbräuchen) dieses Vorgehen zulässig ist, wird zurzeit geklärt.

3.10.2 Überwachung des Fernmeldeverkehrs in kantonalen Netzwerken für die Strafverfolgung

Das Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs legt fest, dass für Überwachungshandlungen in diesem Bereich abschliessend der Dienst für besondere Aufträge des UVEK zuständig ist. Der Kanton Bern stellt sein Weitbereichsnetz BEWAN auch den Gemeinden zur Verfügung. Er hat damit die Rolle eines Providers. Die Polizei- und Strafjustizorgane des Kantons Bern dürfen auch gegenüber dem kantonalen Netz nicht direkt Überwachungsmassnahmen anordnen. Auch für solche – gleichsam interne – Massnahmen ist stets der Dienst für besondere Aufträge zuständig.

3. Januar 2005

Der Datenschutzbeauftragte: *Siegenthaler*