Bericht der Aufsichtsstelle für Datenschutz

Autor(en): **Siegenthaler**

Objektyp: **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): - **(2001)**

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

PDF erstellt am: **11.05.2024**

Persistenter Link: <https://doi.org/10.5169/seals-418420>

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.

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Nur noch selten wird die Datenschutzaufsichtsstelle zu Informatikprojekten beigezogen. Die Kosten für das Berücksichtigen von Datenschutzanliegen steigen mit dem Projektfortschritt aber exponentiell. Es ist daher dringend notwendig, eine frühe Einflussnahme zu institutionalisieren. Zum Zeitpunkt der Kreditbewilligung durchgeführte Nachfragen haben dies bestätigt.

Autobahntunnel, Züge, Parkhäuser, Schulen aber auch generell öffentliche Plätze sollen mit Videotechnik überwacht werden. Erst durch das Schaffen gesetzlicher Grundlagen wird eine politische Diskussion über die Wünschbarkeit des Einsatzes dieser Technik sichergestellt. Dabei ist auch die rasche Entwicklung der Videotechnik (z. B. Ereignisdetektion) zu berücksichtigen.

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

Die Vereinigung der Schweizerischen Datenschutzbeauftragten (DSB+CPD.CH) erarbeitete mit Unterstützung des Eidgenössischen Datenschutzbeauftragten ein Merkblatt über die Information der Krankenversicherer nach Operationen und Spitalaustritten sowie eine Broschüre für Verwaltungsmitarbeitende über Informatik-sicherheitsvorgaben. Zu sechs Bundesgesetzen erarbeitete die Vereinigung eine Stellungnahme und stellte ihren Mitgliedern einen Entwurf für die kantonsinterne Stellungnahme zur Verfügung (siehe 3.6). Bei weiteren Erlassen stellte die Vereinigung nach einer Prüfung eine genügende Berücksichtigung der Datenschutzanliegen fest und entlastete damit die Mitgliederkantone vor weiteren Abklärungen. Bei der Ausarbeitung des teilrevidierten eidgenössischen Datenschutzgesetzes war eine Mitwirkung in der vom Eidgenössischen Justiz- und Polizeidepartement eingesetzten Arbeitsgruppe möglich. Zum Öffentlichkeitsgesetz fand eine Anhörung statt. Internet und Schule sowie – anlässlich der VIII. Nationalen Konferenz der Datenschutzbeauftragten – der Umgang mit Informatikprojekten (siehe 3.4.2) bildeten Gegenstand von Weiterbildungsveranstaltungen der Vereinigung.

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. Das in früheren Jahresberichten erwähnte Problem der überlangen Wartezeiten für Rechtsauskünfte blieb ungelöst (siehe 3.2.2).

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

In ihrem Bericht über den Verwaltungsbericht 2000 vom 14. August 2001 hat die Geschäftsprüfungskommission des Grossen Rates in Ziffer 10.2 festgehalten, der gesetzliche Auftrag des Datenschutzes werde chronisch untererfüllt. Sie empfahl dem Regierungsrat, er solle die erforderlichen Ressourcen bereitstellen, damit die gesetzlichen Aufgaben im Bereich des Datenschutzes erfüllt werden können (Empfehlung Nr. 6). Im November 2001 überwies der Grosse Rat eine Motion, die den Regierungsrat zu massiven Sparmassnahmen verpflichtet. Vor dieser Ausgangslage kam eine Stellenschaffung für den Regierungsrat nicht in Betracht. Eine Verbesserung soll vorab durch Umlagerungen herbeigeführt werden: Die im Fachbereich zuständigen Beratungsstellen sollen auch in Datenschutzfragen beraten, Prüfungen von Informatikprojekten und Kontrolltätigkeiten sollen auf Kosten der datenbearbeitenden Stellen an Externe übertragen werden (siehe 3.2.5 und 3.4.2). Die hierzu nötigen Umsetzungsarbeiten sind zurzeit im Gang.

3.2.3 Eigenverantwortung der Daten bearbeitenden Stellen

Neben den von den Daten bearbeitenden Stellen organisierten Weiterbildungsveranstaltungen (z. B. für die Informatikkonferenz der Finanzdirektion oder durch den Datenschutzbeauftragten des Inselspitals in Zusammenarbeit mit der Vereinigung datenschutzforum.ch) zeigten die zahlreichen Anfragen von Verwaltungsstellen deren Engagement in Datenschutzfragen. Entwürfe zu einer Datenschutzweisung für die drei staatlichen Psychiatriekliniken, zu einer Datenschutzweisung für die Opferhilfeberatungsstellen sowie zu einer Weisung über die Nutzung von Informatikmitteln der Bau-, Verkehrs- und Energiedirektion tragen zu einer Umsetzung der Datenschutzanliegen im Alltag bei. Erfreulich ist auch die vom Inspektorat der Steuerverwaltung durchgeführte Kontrolle der Zugriffe auf das System NESKO (Abrufverfahren). Diese Zugriffe auf Steuerdaten erfolgen zur Prüfung von Anträgen zur Prämienverbiligung bei der obligatorischen Krankenpflegeversicherung durch das Amt für Sozialversicherung und Stiftungsaufsicht.

3.2.4 Verhältnis Informatikmittel, Mittel für Datenschutz und Datensicherheit

Im Jahr 2001 waren 20 Mio. Franken in Informatikmittel zu investieren. 129,6 Mio. Franken sollte der Betrieb der Informatikmittel kosten (Budgetzahlen). 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

In der Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei (siehe 3.8.1) wie auch im Entwurf zum BEDAG-Gesetz sieht der Regierungsrat eine Verpflichtung zum periodischen

Beizug externer Kontrollstellen vor. Das im Vorjahresbericht vorgestellte neue Kontrollkonzept wird damit weiterverbreitet (Verpflichtung der datenbearbeitenden Stellen zum Beizug externer Kontrollstellen auf ihre Kosten).

Ebenfalls unter Beizug Externer führte die Finanzkontrolle bei allen Direktionen und bei der Staatskanzlei eine Risikobeurteilung im Informatikbereich durch. Diese Prüfung umfasste neben dem Umgang mit Personendaten auch den Umgang mit Sachdaten. Insgesamt geht die Prüfung weiter als die im Datenschutzgesetz vorgesehenen Prüfungen (z.B. Management der IT-Investitionen). Sie umfasst die Datenschutzprüfziele jedoch, stellen doch gerade auch Datenschutzverletzungen ein Risiko dar. Aus Ressourcengründen verzichtete die Finanzkontrolle allerdings auf eine Prüfung des Datenmanagements. Das unterstreicht den erheblichen Ressourcenbedarf für eine solche Prüfung, stehen der Finanzkontrolle im Vergleich zur Datenschutzaufsichtsstelle doch erhebliche Ressourcen zur Verfügung (2 Vollstellen und Externe). Die mit der Finanzkontrolle aufgenommenen Gespräche sollen es der Datenschutzaufsichtsstelle erlauben, die Prüfungsergebnisse der Finanzkontrolle auch für die Prüfungsaufgaben der Datenschutzaufsichtsstelle einzusetzen.

Zur Kontrolle des Inspektorates der Steuerverwaltung beim System NESKO siehe 3.2.3.

Die Ressourcen der Datenschutzaufsichtsstelle erlaubten keine anlasslosen Kontrollhandlungen gegenüber Informatiksystemen.

3.3 **Datensicherheit**

Die Universität Bern war, wenn auch in weit geringerem Umfang als die ETH Zürich, von einem Angriff (E-Mail-Lawine bzw. Lawine von Unzustellbarkeitsmeldungen) mitbetroffen. Nicht zuletzt solche Vorfälle zeigen die Bedeutung der Datensicherheit.

3.3.1 **Sollvorgaben**

Die im Vorjahresbericht bemängelten, teilweise überalterten, uneinheitlichen und unvollständigen Sollvorgaben für die Informatiksicherheit in der Kantonsverwaltung sind nach wie vor in Kraft. Beispielsweise in der Bewilligung der Datenbearbeitungssysteme der Kantonspolizei hält der Regierungsrat fest, diese Systeme müssten den für die Verwaltung des Kantons Bern geltenden Anforderungen an die Datensicherheit entsprechen (siehe 3.8.1). Diese – zu Recht gemachte – Verweisung setzt griffige Sollvorgaben voraus. Solche sind auch beim Auslagern von Informatikdienstleistungen nötig. Sie fehlen nach wie vor.

3.3.2 **Sicherheit von E-Mail**

Im Frühjahr bestätigte das Organisationsamt, der aktuelle Versuchsbetrieb zur sicheren Mailübertragung funktioniere mit Swisskey-Zertifikaten zur Zufriedenheit aller Beteiligten. Im Frühsommer kündigte Swisskey die Betriebseinstellung an. Im November beschloss die kantonale Informatikkonferenz den Abbruch der Pilotphase sicheres E-Mail, da kein langfristig befriedigender Betrieb einer Zertifizierungsstelle mehr sichergestellt werden konnte. Exponierten Stellen, wie psychiatrischen Kliniken und Personaldiensten, wurde empfohlen, für ihren Teilbereich auf verfügbare Lösungen abzustellen (z. B. PGP).

Dieser Entscheid der kantonalen Informatikkonferenz ist verständlich. Die Betriebseinstellung von Swisskey bedeutet einen schweren Rückschlag. Dies gerade vor dem Umstand, dass das Organisationsamt festgehalten hatte, sicheres E-Mail könne in der Praxis benutzerfreundlich und mit weniger als zehn Minuten Initialisie-

rungsaufwand pro Arbeitsplatz betrieben werden. Nachdem der vom Organisationsamt und dem mitbeteiligten Personalamt mit hohem Engagement gesuchte technische Lösungsweg gefunden werden konnte, ist nun die Verbreitung des sicheren Mails an der fehlenden Zertifizierungsstelle gescheitert. Gerade diese Erfahrung ist ermühtend (siehe zur elektronisch eingereichten Steuererklärung 3.5 und zum Bundesgesetz über die elektronische Signatur 3.6).

3.4 **Informatikprojekte**

3.4.1 **Projekte in Realisierung**

In den Projekten GRUDIS (Grundstückinformationssystem) und MIDI (Informatiksystem des Migrationsdienstes, allerdings beschränkt auf den Teilbereich Online-Zugriff des Ausländer- und Bürgerrechtsdienstes der Kantonspolizei als Vollzugsstelle) zogen die Projektverantwortlichen die Datenschutzaufsichtsstelle bei. Für das Projekt GRUDIS werden zurzeit die erforderlichen Rechtsgrundlagen ausgearbeitet und die Zugriffsberechtigungen definiert. Beim Online-Anschluss an das System MIDI liegt kein Abrufverfahren vor, sodass keine zusätzliche rechtliche Verankerung nötig ist. Sicherzustellen ist allerdings, dass die Kantonspolizei als Vollzugsstelle in Fremdenpolizeibelangen den Online-Anschluss nur für diesen Zweck verwendet.

Bei folgenden Projekten konnte die Datenschutzaufsichtsstelle erst nach der Kreditbewilligung Aufschluss über die Berücksichtigung der Datenschutzbelange verlangen: BESES-2+ (Kliniksysteme der drei psychiatrischen Kliniken), ABC+Q (Qualitätssicherungssystem in der ambulanten Suchthilfe des Kantons Bern), Videokameraeinbau in den Anstalten Hindelbank, Dokumentenmanagementsystem der Bau-, Verkehrs- und Energiedirektion, System zur Einführung elektronischer Ausweise für Studierende und Angehörige der Universität Bern, FABER/FAK (Anpassung der Informatikinfrastruktur beim Strassenverkehrs- und Schifffahrtsamt zur Einführung des neuen Fahrberechtigungsregisters und der maschinenlesbaren Führerausweise in Kreditkartenformat), Labor-EDV-System des Berner Reha-Zentrums Heiligenschwendi.

Das Nachbearbeiten der Stellungnahmen der angeschriebenen Stellen konnte ausser beim Kameraeinbau in den Anstalten Hindelbank bis heute nicht abgeschlossen werden. Während in einem Fall eine detaillierte Vorgabe von guter Qualität vorgelegt wurde, waren die übrigen Vorgaben nachbesserungsbedürftig oder löste erst die Nachfrage der Datenschutzaufsichtsstelle ein Verabschieden von Weisungen aus. Der Ressourcenbedarf für die Betreuung ist erheblich (siehe 3.4.2).

Durch eine betroffene Gemeinde wurde die Datenschutzaufsichtsstelle auf das in der Phase der Voranalyse stehende, umfangreiche Projekt GERES der Steuerverwaltung hingewiesen. Es handelt sich um eine den Gemeinden vom Kanton zur Verfügung gestellte Plattform für eine zentrale Einwohnerkontrolle. Das Projekt wurde unter anderem auch im Hinblick auf E-Government und die Volkszählung 2010 an die Hand genommen.

3.4.2 **Konzept zum Umgang mit Projekten**

Bereits die Vorbereitung der vom Kanton Bern organisierten VIII. Nationalen Konferenz der Datenschutzbeauftragten bot Anlass, den Umgang mit Projekten zu überdenken (siehe 3.1.2). Die gemachten Rückfragen (siehe 3.4.1) haben die von den Referenten anlässlich der Konferenz aufgezeigten Probleme bestätigt: Die Vorgaben für die Projektabwicklung sehen eine Berücksichtigung der Datenschutzanliegen nur ungenügend vor oder werden nicht beachtet. Dem muss entgegengewirkt werden.

Die Kosten der Berücksichtigung der Datenschutzanliegen steigen mit dem Projektfortschritt exponentiell an. Die Datenschutzauf-

sichtsstelle hat aber weder genügend informatiktechnisches Wissen noch genügend Ressourcen, um eine Projektbetreuung sicherzustellen. Diese müssten daher durch die Projektleitungen vorab bei Externen bezogen werden und die Datenschutzaufsichtsstelle sollte sich auf eine Kontrolle dieses Bezugs beschränken können.

Nachkontrollen gegenüber den im Betrieb stehenden Systemen sowie Kreditverweigerungen durch die zuständigen Organe, wenn eine Datenschutzprüfung unterblieben ist, müssten ein Berücksichtigen der Datenschutzanliegen in der Projektierungsphase lohnend machen.

Der Umstand, dass solche Forderungen an der VIII. Nationalen Konferenz der Datenschutzauftragten gerade auch von Informatiksicherheitsverantwortlichen und Projektleitern vertreten worden sind, zeigt den erheblichen Handlungsbedarf. Die Vereinigung der Schweizerischen Datenschutzauftragten hat sich inzwischen für eine diesbezügliche Überarbeitung der Projektabwicklungsvorgabe HERMES eingesetzt.

3.5 Internet und E-Government

Der Leitfaden zur Internet- und E-Mail-Überwachung am Arbeitsplatz des Eidgenössischen Datenschutzauftragten beantwortet die auch im Kanton Bern oft gestellte Frage, wie lange Protokolldateien über Internetzugriffe (Loggfiles) vom Arbeitgeber aufbewahrt werden sollen: Die Aufbewahrungsfrist beträgt vier Wochen. Sechs Monate beträgt dagegen die Frist für das Aufbewahren der Verbindungsranddaten bei konzessionierten Anbietern von Fernmeldediensten (Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs). Die Vorgabe für die Arbeitgeber wird in der Praxis erst noch umzusetzen sein.

Mit der Veranlagungsverordnung konkretisiert die Steuerverwaltung die bestehende Rechtsgrundlage für das Einreichen der Steuererklärung via Internet. Eine mit gewöhnlicher Post einzureichende handschriftliche Freigabeerklärung wird aber immer noch vorausgesetzt. Das steht in einem gewissen Spannungsverhältnis zum Umstand, dass die Interessierten ihre Steuererklärung direkt auf dem Server der Steuerverwaltung bearbeiten können. Diese Möglichkeit setzt nämlich bereits ein sicheres Verfahren zur Authentifizierung der Interessierten voraus. Den Interessierten wird aber zumindest eine nicht abhörbare Verbindung zum authentifizierten Server der Steuerverwaltung zur Verfügung gestellt. Dieses Vorgehen hebt sich in positiver Weise von andern staatlichen Internetseiten ab, die Interessierte zur unverschlüsselten Übertragung besonders schützenswerter Daten via Internet animieren. Ein einheitlicher Umgang kantonaler Stellen mit diesem Problem ist nötig.

Nötig sind ebenfalls einheitliche Vorgaben für den sicheren Internetauftritt im E-Government. Das deutsche Bundesamt für Sicherheit in der Informationstechnik stellt hierzu auf Internet ein detailliertes Papier zur Verfügung.

In der Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei wurde zu den auf Internet erfolgenden polizeilichen Datenbekanntgaben noch nicht Stellung genommen (z. B. Fahndungsaufrufe, siehe 3.8.1).

Die Gemeinde Zollikofen unterbreitete ihren Internetauftritt der Datenschutzaufsichtsstelle zur Prüfung. Das erfreuliche Bemühen um ein korrektes Vorgehen liess sich nur mit einem beträchtlichen Aufwand unterstützen. Als aufwändig erwies sich insbesondere die Verbindung von informatiktechnischen Sicherheitsfragen mit fachspezifischen Detailrechtsfragen (z. B. Zulässigkeit von Datenerhebungen für die Einwohnerkontrolle).

Im Einverständnis mit den Betroffenen hat das Oberstufenzentrum Täuffelen während zweier Wochen Videobilder im 15-Sekunden-Rhythmus aus einem Klassenzimmer auf das Internet übertragen. Dies zeigt, dass auch mit dem Einsatz geringer Mittel erhebliche Beeinträchtigungen der Persönlichkeitsrechte entstehen könnten.

3.6 Gesetzgebung

Gestützt auf die Vorschläge der Vereinigung der Schweizerischen Datenschutzauftragten nahm die Datenschutzaufsichtsstelle kantonsintern in den Vernehmlassungsverfahren zu sechs Bundesgesetzen Stellung: Zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur war auf die Wichtigkeit staatlich zertifizierter sicherer Komponenten (Tastaturen, Kartenleser) hinzuweisen. Ohne solche Komponenten werden die Betroffenen die ihnen zugewiesenen Risiken nicht tragen. Gerade aus der Sicht eines Kantons mit Öffentlichkeitsprinzip war zum teilrevidierten Bundesgesetz über den Datenschutz ein Aufheben der Verpflichtung der Kantone zur Führung des Registers der Datensammlungen zu verlangen: Wenn ein Kanton mit Öffentlichkeitsprinzip ohnehin allen Interessierten Auskünfte über die Datenbearbeitungen zu erteilen hat, steht der hohe Aufwand für die Registerführung in keinem Verhältnis zum Ertrag. Die neu vorgesehene Befugnis der Aufsichtsstellen, beim Bundesrechtsvollzug Rechtsmittel zu ergreifen, ist zu begrüßen. Ihre Einbindung in das kantonale Verfahrensrecht darf aber nicht unterschätzt werden. Im Entwurf zu einem Gesetz über die Schweizerische Strafprozessordnung wird auf die Regelung der DNA-Analysen im Entwurf zum DNA-Profilgesetz zurück verwiesen. Zum DNA-Profilgesetz wurde aber ein ordentliches Vernehmlassungsverfahren nie durchgeführt. Noch einmal ist daher auf die Mängel dieses Gesetzes hinzuweisen, nämlich auf den fehlenden Deliktscatalog und die teilweise fehlende Löschung von Amtes wegen. Zu den kantonalen Erlassen siehe 3.2.5 (BEDAG-Gesetz) und 3.5 (Veranlagungsverordnung: elektronisch eingereichte Steuererklärung).

3.7 Gemeinderechtliche Körperschaften

Die von mehreren Seiten angeregten Arbeitsblätter für kommunale Datenschutzaufsichtsstellen konnten in einer ersten summarischen Grobfassung verfasst werden. Sie sollen auf der künftigen Internetseite der Justiz-, Gemeinde- und Kirchendirektion veröffentlicht werden. Die Arbeitsblätter richten sich an Gemeinden mit mehr als 5000 Einwohner, da nur hier von einer zumindest teilweisen professionellen Betreuung ausgegangen werden kann. Ein umfassend miliztaugliches Vermitteln der Vorgaben erwies sich vorerst als unmöglich. Für die Informatiksicherheit wird auf das deutsche IT-Grundschutzhandbuch zurückverwiesen. Dieses ist in Deutsch und Englisch auf Internet verfügbar. Die für den Kanton Bern erforderliche französischsprachige Fassung fehlt.

Mit den Datenschutzaufsichtsstellen zweier grosser Gemeinden konnte eine Ausbildungsveranstaltung durchgeführt werden.

Eine betroffene Person führte zur Durchsetzung ihres Einsichtsrechts in Kommissions- und Gemeinderatsprotokolle ein Verwaltungsbeschwerdeverfahren vor dem Regierungsrat.

Die Bekanntgabe von Daten über Asylsuchende an einer Gemeindeversammlung löste ein Strafverfahren wegen Amtsgeheimnisverletzung gegen ein Behördemitglied aus. Das Verfahren ist inzwischen eingestellt worden.

Erst auf Beschluss des Gemeinderates hin gab eine Gemeinde die Praxis des Sozialdienstes auf, die Berechtigung von Sozialhilfebezügen vereinzelt durch einen Privatdetektiv überprüfen zu lassen. Zur Webcam des Oberstufenzentrums Täuffelen und zum Internetauftritt der Gemeinde Zollikofen siehe 3.5.

Dass die Verantwortlichen die Rahmenbedingungen für das Bearbeiten von Daten kennen müssen, steht vor diesen Beispielen ausser Frage. Die angebotenen Aus- und Weiterbildungsveranstaltungen wurden entsprechend gut besucht. Eine Nachfrage nach rechtlichen Unterstützungen besteht gerade auch bei überkommunalen Aufgabenträgern wie Väter- und Mütterberatungsstellen oder Beratungsstellen für Drogen- und Alkoholprobleme.

3.8 Berichtspunkte des Vorjahres

3.8.1 Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei

Im Januar hat der Regierungsrat die Betriebsbewilligung für die Datenbearbeitungssysteme der Kantonspolizei erteilt. Auf Antrag der Polizei- und Militärdirektion müssen Zugriffe auf das Subsystem OBORA protokolliert werden. Im Abstand von zwei Jahren hat zudem eine unabhängige und fachkundige Stelle den Datenschutz und die Gewährleistung der Datensicherheit zu prüfen. Es gelten die Informatiksicherheitsvorgaben des Kantons (siehe 3.3.1). Die Betriebsbewilligung umfasst die Hauptdatenbearbeitungssysteme. Ob weitere Datenbearbeitungssysteme der Kantonspolizei einer Betriebsbewilligung bedürfen, wird zurzeit geklärt (Webseite, Videosysteme, Ordnungsbussenzentrale, Datenbearbeitungssysteme, die in Zusammenarbeit mit dem Bund betrieben werden).

3.8.2 Sollvorgaben Informatiksicherheit

Siehe 3.3.1

3.8.3 Sicherheit von E-Mail

Siehe 3.3.2

3.8.4 DNA

Gestützt auf die bis Ende 2004 befristete Bundesverordnung über das DNA-Profil-Informationssystem liefern auch kantonale Stellen zu Strafverfolgungszwecken erhobene DNA-Profile in die vom Bund betriebene Datenbank ein. Der Entwurf zu einer schweizerischen Strafprozessordnung verweist auf den im Vorjahresbericht erwähnten Entwurf zu einem DNA-Profilgesetz zurück (siehe 3.6). Die Datenschutzaufsichtsstelle teilt die in der Antwort auf die Motion Rytz vertretene Auffassung, dem Kanton bleibe in Anbetracht der neuen Kompetenz des Bundes zur Regelung des Strafverfahrens (Justizreform) und der eingeleiteten Gesetzgebungsarbeiten des Bundes kaum mehr ein Spielraum für eine kantonale Regelung.

3.8.5 Kontrollen von Informatikdatenbearbeitungen

Siehe 3.2.5

3.9 Besonderes

3.9.1 Video

In der Stadt Biel sind Videokameras ohne Bildaufzeichnung zur Verkehrsüberwachung und zur Überwachung von Parkplätzen in Betrieb genommen worden. In der Stadt Bern wird bei den zuständigen Behörden über das Ob und das Wie eines Videokameraeinsatzes diskutiert. Eine Transportunternehmung unterbreitete der

Datenschutzaufsichtsstelle ein Projekt zum Videoeinsatz in Zügen. Vorgesehen war ein gleiches Vorgehen wie beim Pilotprojekt der SBB im Raum Genf. Das Bundesamt für Strassen verpflichtet auch den Kanton Bern, längere Autobahntunnel mit Videoanlagen mit Ereignisdetektion zu überwachen. Die Bilder werden in die Werkhöfe des Tiefbauamtes und die Einsatzzentralen der Kantonspolizei übertragen und zumindest bei besonderen Ereignissen auch aufgezeichnet. Eine Gemeinde rüstete ihr neues Parkhaus mit einer Videoanlage aus und erkundigte sich nach der erforderlichen rechtlichen Abstützung. Während eine Schule eine Videoüberwachung mit Aufzeichnung für die Velounterstände nur prüfte, richtete ein Oberstufenzentrum befristet eine Webcam in einem Klassenzimmer ein (siehe 3.5). Eine kommunale Gewerbepolizeistelle erkundigte sich nach den rechtlichen Voraussetzungen, damit ein Taxihalter rechtmässig von jedem Fahrgast ein elektronisches Bild aufnehmen darf. Konnte hier im Wesentlichen auf das vom Eidgenössischen Datenschutzbeauftragten herausgegebene Merkblatt über die Videoüberwachung durch private Personen verwiesen werden, war gegenüber den andern Vorgehensweisen die Notwendigkeit einer Rechtsgrundlage – jedenfalls dann, wenn Bilder aufgezeichnet werden – zu unterstreichen. Auf kantonaler Ebene besteht eine solche Rechtsgrundlage für Bild- und Tonaufzeichnungen bei Massenveranstaltungen im Polizeigesetz und in der darauf abgestützten Videoverordnung. Weitere Rechtsgrundlagen fehlen sowohl auf kantonaler wie regelmässig auch auf kommunaler Ebene. Der Erlass von Rechtsgrundlagen soll nicht nur die Frage, ob eine Videoüberwachung Einsatz finden soll, klären, sondern auch deren Rahmenbedingungen: Zweck, Aufbewahrungsdauer, Sicherheitsmassnahmen, Bekanntmachung und – vor einer sich rasch entwickelnden Technologie besonders aktuell – das Ausschöpfen weiterer technischer Möglichkeiten wie Ereignisdetektion.

3.9.2 Personalbefragung und andere Befragungen

Insbesondere im Zuge der neuen Verwaltungsführung werden vermehrt Befragungen Betroffener vorgenommen. Regelmässig ist darauf hinzuweisen, dass Fragebogen die gesetzliche Grundlage, den Zweck der Befragung sowie die Freiwilligkeit der Antwort erwähnen müssen.

Bei der vorgängig eingeholten Stellungnahme zur Befragung über die Personalfriedenheit konnten mit den Verantwortlichen datenschutzkonforme Lösungen gefunden werden: Zu diskutieren waren insbesondere die Anonymisierung, der Zeitpunkt der Datenvernichtung, die Erhebung von Daten über Vorgesetzte bei Mitarbeitenden und das Bemerkungsfeld. Das Datenschutzgesetz gibt Betroffenen einen Einsichts- und Auskunftsanspruch. Es ist daher unzulässig, Befragten Vertraulichkeit zuzusichern, wenn bei ihnen Daten über erkennbare Dritte (hier Vorgesetzte) erhoben werden sollen. Zudem steht dieser Datenbeschaffung auch der Umstand entgegen, dass Daten grundsätzlich bei den Betroffenen einzuholen sind. Diese Grenzen sind auch dann zu beachten, wenn ein Fragebogen ein Bemerkungsfeld enthalten soll.

18. Januar 2002

Der Datenschutzbeauftragte: *Siegenthaler*