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 ...

Herausgeber: Staatskanzlei des Kantons Bern

Band: - (1996)

Heft: [1]: Verwaltungsbericht : Berichtsteil

Artikel: Bericht der Aufsichtsstelle für Datenschutz

Autor: Siegenthaler

DOI: https://doi.org/10.5169/seals-418281

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 15.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

3. Bericht der Aufsichtsstelle für Datenschutz

3.1 Einleitung

3.1.1 Auf einen Blick

Der Einsatz neuer Informatikmittel (Vernetzung, Telefonie, Internet) führte im Berichtsjahr mehreren staatlichen Stellen die damit verbundenen Probleme (neue Kontrollmöglichkeiten, Machtverlagerungen) konkret vor Augen. Die in Teilbereichen erzielten Fortschritte betreffend Datensicherheit lassen die in den übrigen Bereichen bestehenden erheblichen Sicherheitsrisiken augenfälliger werden. Gegen das Jahresende waren mehrere Fälle von widerrechtlichen Datenbearbeitungen zu verzeichnen.

3.1.2 Zusammenarbeit mit dem eidgenössischen Datenschutzbeauftragten, 3. Nationale Konferenz der Datenschutzbeauftragten

Als erster schweizerischer Kanton übernahm der Kanton Zürich die Organisation der 3. Nationalen Konferenz der Datenschutzbeauftragten vom 2. Oktober 1996 in Zürich. In einer Resolution forderten die Konferenzteilnehmer, medizinische Daten seien nur im erforderlichen Mindestmass bekanntzugeben, nur durch dem Arztgeheimnis unterstehende Personen zu bearbeiten und stets befristet aufzubewahren. Die Behandlung ausserkantonaler Patienten (Kostengutsprachen des Wohnsitzkantons) und die im Aufbau begriffenen medizinischen Statistiken des Bundes boten Anlass zur Resolution. Beide Problemkreise sind auch für den Kanton Bern aktuell. Die Herausgabe eines schweizerischen Registers der Fahrzeughalter auf CD-ROM zeigt die Schnittstelle zwischen dem kantonalen öffentlich-rechtlichen und dem privatrechtlichen Datenschutz: Soweit zur Zeit der Drucklegung dieses Berichtes bekannt, beschaffte sich der private Herausgeber des Verzeichnisses die Fahrzeughalterdaten in den mit kantonaler Zustimmung in Buchform herausgegebenen Fahrzeughalterverzeichnissen. Das Bundesrecht erlaubt die Bekanntgabe von Fahrzeughaltern einzig gestützt auf die Kontrollschildnummer. Die CD-ROM mit angeblich drei Millionen Fahrzeughaltern ermöglicht es aber auch, durch Eingabe des Namens die Kontrollschildnummer zu erhalten. Auf Meldung der kantonalen Datenschutzaufsichtsstelle hin hat der eidgenössische Datenschutzbeauftragte beim privaten Herausgeber des Verzeichnisses interveniert. Der Kanton Bern muss zur Kenntnis nehmen, dass die gestützt auf sein Datenschutzgesetz allenfalls erlaubten Publikationen auf Papier mit wenig Aufwand in elektronische Nachschlagewerke übernommen (eingescannt) werden können. Für Betroffene stellt die elektronische Nachschlagemöglichkeit einen wesentlich schwereren Eingriff in die Persönlichkeitsrechte dar. In seiner Stellungnahme zuhanden der eidgenössischen Instanzen machte der Kanton Bern für künftige Volkszählungen darauf aufmerksam, in Anbetracht der hohen Anzahl kleiner Gemeinden im Kanton Bern sei eine strikte Bindung an den statistischen Zweck der Datenerhebung unrealistisch. Eine Überprüfung vorab der Einwohnerkontrolldaten anhand der Volkszählungsdaten könne zumindest im «Kopf des Gemeindeschreibers» nicht unterbunden werden. Dem Bürger gegenüber sei es daher ehrlicher, in der Volkszählungsgesetzgebung die Verwendung der Daten zu anderen Zwecken zuzulassen und offenzulegen, gleichzeitig aber das Ausbleiben nachteiliger Folgen wie Bussen und Nachsteuern zu verankern.

3.1.3 Internet

Obergericht (Kreisschreiben und Entscheidsammlung) und, noch in der Projektierungsphase, Erziehungsdirektion und Staatskanzlei wollen Informationen über das Internet abgeben. Dass das Zugänglichmachen von Personendaten via Internet nur mit der ausdrücklichen Zustimmung der über die Risiken aufgeklärten Betroffenen zulässig ist, hielt die Datenschutzaufsichtsstelle gegenüber den Gemeinden des Amtsbezirkes Oberhasli fest. Ein Anbieter hatte diesen Gemeinden vorgeschlagen, Gemeindeinformationen (auch Behördeverzeichnisse mit Privatadressen) auf eine Homepage aufzunehmen. Vgl. zum Problemkreis Internet auch Ziffer 3.7.4.

3.2 Aufgabenumschreibung, Prioritäten, Mittel

3.2.1 Prioritäten

Private und Verwaltungsstellen, deren Anfragen nicht ausser der Reihe behandelt werden, warten zurzeit auf Antworten, die einen gewissen Abklärungsaufwand mit sich bringen, mehr als 14 Monate. Das ist entschieden zu lang. In Anbetracht steigender Geschäftseingänge bei gleichbleibenden Mitteln ist eine Besserung nicht in Sicht. Ausser der Reihe zu behandeln sind Geschäfte, auf die die Datenschutzaufsichtsstelle ohne kurzfristiges Handeln nicht mehr Einfluss nehmen kann, allen voran Informatikprojekte in der Planungs- und Bewilligungsphase. Dies führt zu folgenden Prioritäten: 1. Informatikprojekte (auch Teilprojekte), 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. Ausgehend vom gesetzlichen Auftrag kommt die Inspektion zu kurz. Der Aufwand zu einer wirksamen Kontrolle insbesondere gegenüber EDV-Grosssystemen ist jedoch derart gross (vgl. Ziffer 3.2.3), dass eine Änderung der Prioritäten nicht zur Diskussion steht.

3.2.2 Eigenverantwortung der Dienststellen

Die Zahl der Dienststellen, die die Zulässigkeit einer Datenbearbeitung vorabklären liessen, hat 1996 zugenommen. Erfreulich sind die von den Dienststellen eingeleiteten Informations- und Weiterbildungsbemühungen. Rolf Schatzmann, Chef Sicherheitsdienst der Bundesverwaltung, informierte anlässlich des April-Kaderlunch auf Einladung des Organisationsamtes (vgl. zu dessen weiteren Bemühungen im Bereich Datensicherheit Ziff. 3.2.3) zum Thema Datensicherheit. Die Erziehungsdirektion führte erfolgreich eine Testphase durch, in der medizinische Abrechnungsdaten verschlüsselt über das Uninetz übertragen wurden. Die von der Staatskanzlei herausgegebene Broschüre «365 Tage Öffentlichkeitsprinzip – eine Bilanz» unterstützt die Anwender der Informationsgesetzgebung gerade auch bei Datenschutzfragen.
Nach wie vor fehlt es jedoch einem Teil der Führung am Interesse für Datensicherheits- und Datenschutzanliegen: So ist kaum zu übersehen, dass dem Referat Schatzmann wohl in erster Linie für Datensicherheitsfragen bereits sensibilisierte Kaderangehörige folgten. Fragen nach der Rolle der Führung werfen auch die unter der Ziffer 3.9 geschilderten Vorfälle auf.

3.2.3 Verhältnis Informatikmittel/ Mittel für Datenschutz und Datensicherheit

Gemäss einer Rückfrage beim Organisationsamt sind 1996 23 Mio. Franken in Informatikmittel investiert worden. 108 Mio. Franken kostete der Betrieb der Informatikmittel. Erfreulich ist, dass in diesen Kosten neu auch Beträge festgestellt werden können, die vorab der Datensicherheit dienen (Projekte: AIS: Erstellung einer CD-ROM zur Ausbildung des gesamten Personals im Bereich Informatiksicherheit; BEMAIL: Mailverschlüsselung; BEWAN: Netzwerkzugangssicherung). Mit rund 0,25 Mio. Franken sind die Gesamtkosten der Datenschutzaufsichtsstelle unverändert geblieben. Insbesondere die Mitarbeit in einer vom Datenschutzbeauftragten des Kantons Zürich eingesetzten Arbeitsgruppe zur Ausarbeitung von Methoden und Unterlagen zur Durchführung einer Datenschutzinspektion hat gezeigt, dass die für Datenschutz- und Datensicherheitskontrollen zur Verfügung stehenden Mittel nie genügen, um die im Datenschutzgesetz gegebenen Aufträge – insbesondere gegenüber EDV-Grosssystemen – umsetzen zu können.

3.2.4 Register

1996 blieb das Register auf dem gleichen Stand wie 1995. Weder wurde der gesetzliche Grundauftrag (Erfassen aller Datensammlungen) erfüllt, noch die Einträge der bereits erfassten Datensammlungen (810) rechtlich überprüft oder aktualisiert.

3.3 Datensicherheit

Unverändert präsentiert sich die Situation auch betreffend Datensicherheit. Die mit dem Regierungsratsbeschluss 4637 vom 9. Dezember 1992 (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. Die Richtigkeit der von den übrigen Direktionen und der Staatskanzlei eingereichten Klassifikationen ist nach wie vor ungeprüft. Ungeprüft ist auch, ob die vorgesehenen Massnahmen umgesetzt worden sind. Der in der Anwort auf die Interpellation Galli vom Regierungsrat in Betracht gezogene Sicherheitsausschuss (oder eine ähnliche Einrichtung) existiert nach wie vor nicht.

3.4 Informatikprojekte

Im Rahmen des Projektes Besis II war im Hinblick auf die Benützung von BEWAN-Teilstücken zur Datenübertragung (Psychiatrieabrechnungen) festzuhalten, eine Datenverschlüsselung sei unabdingbar. Auch bei der blossen Teilerneuerung von Netzwerkabschnitten ist der Stand der Sicherheitstechnik (Verschlüsselung) einzuhalten. Zu prüfen ist bei Teilprojekten immer, ob nicht mit einem verhältnismässigen Aufwand die Sicherheit des gesamten Systems dem aktuellen Stand der Technik (End-zu-End-Verschlüsselung) angepasst werden kann. Unzulässig ist es, mit der Begründung, in andern Netzwerkteilen seien dem Stand der Technik genügende Sicherheitsmassnahmen auch nicht realisiert, auf solche für ein neues Teilstück zu verzichten (vgl. zur Mail-Verschlüsselung Ziff. 3.2.3). Beim EDV- Projekt «Stipendien 97» der Erziehungsdirektion war auf die fehlende Rechtsgrundlage für das vorbestehende Abrufverfahren, auf die Anforderungen betreffend Kommunikationssicherheit sowie auf die gegenüber eingesetzten Drittfirmen vorzunehmende Verpflichtung betreffend Amtsgeheimniswahrung aufmerksam zu machen. Das Polizeikommando testete im Rahmen des Informatikprojektes «KOBI» den Einsatz eines (auch mobilen) Computers. Dieser erlaubt es Polizeimitarbeitern gleichzeitig, also ohne erneute Anmeldeformalitäten, über eine Person Anfragen in mehreren Datenbanken (ABI der Kantonspolizei, SUSA des Strassenverkehrsamtes, RIPOL und ZAR der Eidgenossenschaft) vorzunehmen. Die Datenschutzaufsichtsstelle wies darauf hin, dass mit dem System KOBI für einzelne Datenbanken (z.B. RIPOL) bestehende Regeln zur getrennten Datenbearbeitung unterlaufen werden können. Sodann führt die automatische Kombination von für sich allein rechtlich je genügend abgestützten Abfragemöglichkeiten für den Betroffenen zu einem qualitativ schwereren Eingriff in sein Grundrecht auf Datenschutz. Dieser bedarf seinerseits einer Rechtsgrundlage. Das System führt sodann zu Sicherheitsproblemen (Universalpasswort) und unterläuft spezifische Sicherheitsvorgaben. Zum Betrieb von KOBI ist demnach vorab eine gesetzliche Grundlage zu schaffen. In dieser sind die Rahmenbedingungen für den Einsatz von KOBI festzuhalten. Schliesslich dürfte das Verhältnismässigkeitsprinzip dazu führen, dass das System «KOBI» nur unter besonderen Umständen (z.B. Kontrollen gegenüber besonders gefährlichen Personen, Sofortkontrollen nach schweren Vorfällen) zugelassen werden kann.

3.5 Akteneinsicht

Erstmals verlangte eine Person Akteneinsicht in alle über sie beim Staat bearbeiteten Daten. Es zeigte sich erwartungsgemäss, dass für die betroffene Person ein erheblicher Aufwand entsteht. Bei länger zurückliegenden Kontakten mit staatlichen Stellen ist es insbesondere nach Reorganisationen kaum mehr möglich, die aktuell zuständige Dienststelle festzustellen. Eine erfreulich hohe Zahl von Dienststellen reagierte rasch und bürgerfreundlich. Andere waren offensichtlich zum ersten Mal mit Akteneinsichtsbegehren konfrontiert. Auch in Daten, die längstens hätten vernichtet sein müssen, wurde noch Einsicht gewährt. Schliesslich zeigte sich, dass Dienststellen – trotz präziser Umschreibung der bestehenden Anknüpfungspunkte – sich durchaus schwer daran tun, alle bei ihnen bearbeiteten Daten aufzufinden.

3.6 Gesetzgebung

3.6.1 Kantonale Erlasse

Im Umfeld Fürsorge und Volksschule gelang es, Gesetzesentwürfe vorzubereiten, die staatliche Stellen von der ihnen neu obliegenden Meldepflicht für Verbrechen befreien. Befreit werden sollen auch die Berufsberater. Gleichzeitig ermächtigt der entsprechende Gesetzesentwurf die Berufsschulen, Lehrbetriebe über die schulischen Leistungen der Auszubildenden zu informieren.

3.7 Informationelle Gewaltenteilung und Personalüberwachung

3.7.1 Gewaltentrennung Regierung/Gerichtsbarkeit: Neuunterstellung von Mitarbeitern des Informatikdienstes der Justiz-, Gemeinde- und Kirchendirektion

Auch unter dem neuen Gesetz über das Strafverfahren findet das Datenschutzgesetz auf hängige Verfahren der Strafjustiz keine Anwendung. Auf abgeschlossene Verfahren und auf noch nicht hän-

gige Verfahren ist das Datenschutzgesetz dagegen anwendbar. Hier anknüpfend wandte sich ein Richteramt an die Datenschutzaufsichtsstelle und wies darauf hin, die neue umfassende Vernetzung aller Bezirksverwaltungen und Gerichte führe zu umfassenden Einflussmöglichkeiten der einzig der Exekutive unterstellten Informatiker. Diesen sei es insbesondere jederzeit möglich, sich Daten eines Richteramtes zu beschaffen, abzuändern oder zu vernichten. Die Justiz-, Gemeinde- und Kirchendirektion schloss sich dieser Argumentation nach Konsultation der Kommission für die Aufsicht über die Richterämter an. Im Sinne einer von beiden Gewalten getragenen Massnahme ist nun vorgesehen, die nötige Rechtsgrundlage zu schaffen, damit Mitarbeiter des Informatikdienstes der Justiz-, Gemeinde- und Kirchendirektion unmittelbar dem Obergericht unterstellt sind. Dieses soll zudem in die Lage versetzt werden, die manipulationssicher vorzunehmenden Protokollierungen der Zugriffe durch Mitarbeiter des Informatikdienstes der Justiz-, Gemeinde- und Kirchendirektion auszuwerten. Die Wahrung des Grundsatzes der Gewaltentrennung ist vorab Sache der beteiligten Staatsgewalten und nicht der Datenschutzaufsichtsstelle. Was aber eindrücklich erscheint, ist der Umstand, dass Machtverlagerungen (die nun korrigiert werden) einzig durch das Einsetzen neuer Informatikmittel entstanden sind.

3.7.2 Aufzeichnung der Gesprächsdaten in Telefonzentralen

Die Einrichtung einer neuen Telefonzentrale in einer Bezirksverwaltung (für die Zentralverwaltung stellen sich die gleichen Fragen) führte zur Frage, ob nun das Richteramt oder das Regierungsstatthalteramt den Zugriff auf das Programm zur Aufzeichnung aller Gesprächsdaten erhalten solle. Neben der Gewaltentrennungsfrage war das Amtsgeheimnis tangiert: Weder darf das Richteramt wissen, mit wem vom Regierungsstatthalteramt aus telefoniert wird, noch dürfen die Gesprächsdaten des Richteramtes dem Regierungsstatthalteramt zugänglich sein. Auch hier genügte das Einrichten einer neuen technischen Anlage, um bisher anerkannte Grenzen in Frage zu stellen. Die involvierten Ämter werden nun gemeinsam Weisungen über den Umgang mit den in der Telefonzentrale automatisch aufgezeichneten Gesprächsdaten erlassen. Diese Weisungen werden voraussichtlich für den Zugriff auf das Programm das Vier-Augen-Prinzip vorsehen. Sodann wird sicherzustellen sein, dass jedes Amt nur auf seine Gesprächsdaten zugreift. Gerade dieser Zugriff ist aber nicht unproblematisch.

3.7.3 Personalüberwachung mittels technischen Massnahmen

Massnahmen zur Feststellung von Verhalten und Leistung der Mitarbeiter dürfen gemäss der Personalverordnung – wenn überhaupt – nur nach vorgängiger Information der Betroffenen eingesetzt werden. Die Kantonsverfassung garantiert nicht nur die persönliche Freiheit, sondern ausdrücklich auch die Achtung des Fernmeldeverkehrs jeder Person. Solange es den Mitarbeitern des Staates demnach erlaubt ist, private Telefongespräche (gegen Bezahlung) über ihre amtlichen Telefonapparate abzuwickeln, ist (jedenfalls ausserhalb eines Verfahrens) eine Auswertung der Telefongesprächsdaten ohne formelle gesetzliche Grundlage nicht zulässig. Neue Telefonzentralen erlauben es auch, die auf einem bestimmten Telefonapparat anfallenden Kosten festzustellen. Mit der blossen Erhebung der Telefonkosten wird die Privatsphäre des Mitarbeiters nun zwar respektiert, über ihn entstehen aber Aussagen, die dem Gebot der Richtigkeit und Vollständigkeit der Daten nicht genügen und durchaus einen falschen Eindruck vermitteln können.

3.7.4 Auswertung der Daten von Internetzugangsservern

Die Erziehungsdirektion unterbreitete der Datenschutzaufsichtsstelle von der Universität entworfene Weisungen über den Umgang mit Informatikmitteln. Diese Weisungen boten Anlass, klarzustellen, dass die im Rahmen der Telefonie festgestellten Grenzen der Überwachung von Mitarbeitern (hier auch von Studierenden) auch bei der Auswertung der in einem Internetzugangsserver verbleibenden Datenspuren (die aussagekräftiger sein können als die Gesprächsdaten einer Telefonzentrale) zu beachten sind. Weder die in einem Internetzugangsserver noch die in einer Telefonzentrale über einen Mitarbeiter aufgezeichneten Datenspuren dürfen demnach heute ausserhalb eines Verfahrens ausgewertet werden.

3.8. Gemeinderechtliche Körperschaften

1996 konnten sieben neue Datenschutzreglemente genehmigt werden. Auf Ende Jahr verfügten damit 205 Gemeinden über ein eigenes Datenschutzreglement. Auch die von Behörden gemeinderechtlicher Körperschaften im Berichtsjahr ausgelösten Abklärungen haben zugenommen. Vorab grosse Gemeinden zogen die Datenschutzaufsichtsstelle für die Personalausbildung bei. Betreffend die Bekanntgabe von Gemeindebehörden via Internet ist auf Ziffer 3.1.3 zu verweisen.

3.9 Besonderes

3.9.1 Zugriff der Steuerverwaltung auf die Datenbank des Amtes für Landwirtschaft

Im Bericht für das Jahr 1995 führte die Datenschutzaufsichtsstelle unter der Ziffer 3.5 aus, die Steuerverwaltung habe auf die Einrichtung eines Online-Anschlusses auf die GELAN-Datenbank des Amtes für Landwirtschaft verzichtet. Zweck des auf die Beitragszahlungen beschränkten Zugriffes wäre die stichprobenweise Überprüfung der Steuererklärungen von Landwirten gewesen. Nach Erscheinen des Jahresberichtes wies die Finanzdirektion darauf hin, das entsprechende Abrufverfahren sei inzwischen doch eingerichtet worden. Damit ein Abrufverfahren (elektronisches Selbstbedienungsprinzip) zulässig ist, ist eine Rechtsgrundlage (hier Verordnung) nötig, und der Zugriff ist soweit als möglich einzuschränken (Verhältnismässigkeit). Entsprechende Einschränkungen hat die Steuerverwaltung denn auch vorgenommen. Dagegen fehlt es nach wie vor an der Verankerung in einer Verordnung. Offenbar bestand seitens der Steuerverwaltung diesbezüglich nach einer gemeinsamen Besprechung eine irrtümliche Auffassung. Der gleichen Auffassung wie die Datenschutzaufsichtsstelle war jedoch die Volkswirtschaftsdirektion. Vor dieser Ausgangslage erstaunt, weshalb nun ausgerechnet diese die Einrichtung des Abrufverfahrens zuliess. Die Abklärungen der Datenschutzaufsichtsstelle haben gezeigt, dass der zuständige Informatikdienst sich schlussendlich mit der Zusicherung des Informatikdienstes der Steuerverwaltung, die rechtlichen Bedenken seien nun ausgeräumt, zufrieden gab. Eine Zustimmung der

Amtsleitung lag weder mündlich noch schriftlich vor. Der Rechtsdienst wurde über die Einrichtung des Abrufverfahrens zudem nie informiert. Der Vorfall zeigt, welche Freiheiten Informatikdienste geniessen. Er zeigt auch, wie wenig übergeordnete Stellen (Amtsleitung und Rechtsdienst) über Änderungen der Informatikanwendungen von erheblicher rechtlicher Tragweite informiert sind.

3.9.2 Ordnungsbussenzentrale

Ziffer 3.2.1 des Jahresberichts 1995 hielt fest, das bei der Ordnungsbussenzentrale im Einsatz stehende Informatiksystem führe aus buchhalterischen Gründen zu einer unzulässigen Registrierung von Ordnungsbussenschuldnern. Das Polizeikommando habe die Abänderung des entsprechenden EDV-Programmes zugesichert. Eine eingeholte Offerte ergab für die Programmänderung Kosten von 25000 Franken. Der zuständige Gesamtprojektausschuss verweigerte die entsprechende Kreditfreigabe. Mittelfristig scheint jedoch eine Gesamtablösung des Systems wenigstens geplant zu sein. Konkrete Anhaltspunkte, dass eine solche aber auch wirklich erfolgen wird (sie wäre frühestens im Verlaufe des Jahres 1998 möglich), fehlen. Bis zum Zeitpunkt der Drucklegung dieses Berichtes gelang es der Datenschutzaufsichtsstelle auch durch eine Intervention bei der dem Polizeikommando vorgesetzten Polizei- und Militärdirektion nicht, einen rechtmässigen Zustand herbeizuführen. Dass ausgerechnet bei der Ordnungsbussenzentrale eine Datenbearbeitungsanlage weiterbetrieben wird, die zu einer widerrechtlichen Datenbearbeitung führt, kann – es geht um mehr als 100000 Betroffene und um besonders schützenswerte Daten – nicht hingenommen werden.

3.9.3 Einzelfälle

Die bernische Pensionskasse händigte einer versicherten Person ein Schreiben aus, auf dessen Rückseite sich eine Liste des versicherten Verdienstes von 55 Versicherten befand. Ursache dieses Vorfalles war die (inzwischen aufgegebene) Praxis der Pensionskasse, die bei einer eingesetzten Informatikfirma anfallenden Computerausdrucke als Notizpapier zu übernehmen.
Das Amt für Militärverwaltung und Betriebe händigte entgegen militärischer Vorschriften einem privaten Verein mit Zeitschriftenverlag die Liste der Offiziere eines Infanterieregimentes aus. Nach einer Empfehlung der Datenschutzaufsichtsstelle hat das Amt für Militärverwaltung und Betriebe für die Vernichtung der entsprechenden Liste gesorgt. Aus eigener Initiative instruierte es zudem sein Personal erneut über die Datenschutzvorgaben.
Schliesslich führte der Tarifverbund «Bäre Abi» eine Umfrage durch. Auf dem Fragebogen wurde zugesichert, die Bestimmungen über den Datenschutz würden selbstverständlich strikte eingehalten. Bereits an der vom Datenschutzgesetz für Fragebogen zwingend vorgeschriebenen Nennung der gesetzlichen Grundlagen fehlte es aber.

23. Januar 1997

Der Datenschutzbeauftragte: *Siegenthaler*