**Fünfzehnter Jahresbericht des Landesbeauftragten für den Datenschutz**


Dr. Stefan Walz, Landesbeauftragter für den Datenschutz

<table>
<thead>
<tr>
<th>Inhaltsübersicht</th>
<th>Seite</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Vorwort</td>
<td>5</td>
</tr>
<tr>
<td>1.1 Zur Situation des Datenschutzes</td>
<td>5</td>
</tr>
<tr>
<td>1.2 Schwerpunkte, Gliederung und Redaktion des Berichts</td>
<td>6</td>
</tr>
<tr>
<td>1.3 Ausblick auf 1993</td>
<td>7</td>
</tr>
<tr>
<td>2. Schwerpunkte</td>
<td>8</td>
</tr>
<tr>
<td>2.1 Eingaben und Bürgerkontakte</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Entwicklung der Informations- und Kommunikationstechnik</td>
<td>9</td>
</tr>
<tr>
<td>2.2.1 Situation im Land Bremen</td>
<td>9</td>
</tr>
<tr>
<td>2.2.1.1 PC-Netze</td>
<td>9</td>
</tr>
<tr>
<td>2.2.1.2 Laptops und Notebooks</td>
<td>10</td>
</tr>
<tr>
<td>2.2.1.3 Protokollierung bei „Safeguard“</td>
<td>11</td>
</tr>
<tr>
<td>2.2.2 Fernwartung von DV-Systemen</td>
<td>11</td>
</tr>
<tr>
<td>2.2.3 Abhörtenden im Mobilfunk</td>
<td>13</td>
</tr>
<tr>
<td>2.2.3.1 Aufhebung der Funkfrequenzbeschränkungen</td>
<td>13</td>
</tr>
<tr>
<td>2.2.3.2 Regelungsinitiative der Innenministerkonferenz</td>
<td>13</td>
</tr>
<tr>
<td>2.2.3.3 Technische Gegenmittel</td>
<td>13</td>
</tr>
<tr>
<td>2.2.3.4 Maßnahmen in Bremen</td>
<td>14</td>
</tr>
<tr>
<td>2.3 Europäische Entwicklungen</td>
<td>14</td>
</tr>
<tr>
<td>2.3.1 Europarat: Bedeutungszuwachs für die Datenschutzkonvention von 1981</td>
<td>14</td>
</tr>
<tr>
<td>2.3.2 Europäische Gemeinschaft: Harmonisierung durch Richtlinie</td>
<td>15</td>
</tr>
<tr>
<td>2.3.2.1 Regelungsziele: Gemeinschaftsweiter Schutz des Persönlichkeitsrechts und Freiheit des grenzüberschreitenden Datenverkehrs</td>
<td>15</td>
</tr>
<tr>
<td>2.3.2.2 Vom 1. Entwurf zum geänderten Entwurf</td>
<td>15</td>
</tr>
<tr>
<td>2.3.2.3 Systemdivergenz als Hauptproblem</td>
<td>16</td>
</tr>
<tr>
<td>2.3.2.4 Abweichungen vom deutschen Datenschutzmodell</td>
<td>16</td>
</tr>
<tr>
<td>2.3.2.5 Akzeptanz der Rechtsangleichung</td>
<td>17</td>
</tr>
<tr>
<td>2.3.3 Aktuelle Themen der deutschen Diskussion</td>
<td>18</td>
</tr>
<tr>
<td>2.3.3.1 Höchststandard oder Mindestniveau?</td>
<td>18</td>
</tr>
<tr>
<td>2.3.3.2 Kontrollinstitutionen</td>
<td>18</td>
</tr>
<tr>
<td>2.3.3.3 Abschaffung des betrieblichen Datenschutzbeauftragten?</td>
<td>19</td>
</tr>
<tr>
<td>2.3.4 Gesamtbeurteilung und weiteres Verfahren</td>
<td>19</td>
</tr>
</tbody>
</table>
7. Bildung und Wissenschaft
7.1 Zweckbindung für Daten der Studenten und des Lehrpersonals — neue Rechtsverordnung 38
7.2 Vermischung von Landes- und kommunalen Aufgaben beim PC-Einsatz 39
7.3 Fall: Ungefragt im Philologen-Jahrbuch 40
8. Arbeit und Frauen
8.1 Krankenhausteilnahmsberichte an das Versorgungsamt 40
9. Jugend und Soziales
9.1 Beratungsgeheimnis und wirtschaftliche Hilfen (s. a. 14. Jahresbericht, Ziffer 2.5.2) 41
9.2 Auskunftspflicht aufgrund Unterhaltspflicht 42
9.3 Seniorenzentraldatei in Bremen 43
10. Gesundheit
10.1 Kontrollergebnisse in kommunalen Krankenhäusern 44
10.1.1 Konsequenzen des Krankenhausdatenschutzgesetzes 44
10.1.2 Prüfprogramm 45
10.1.3 EDV im Zentralkrankenhaus Reinkenheide 45
10.1.4 Nachlässigkeit bei externer Wartung (ZKH St.-Jürgen-Straße) 46
10.2 Eckpunkte für ein Gesetz über den öffentlichen Gesundheitsdienst (s. a. 14. Jahresbericht, Ziffer 2.6.6) 46
10.3 Patientendaten in der gesetzlichen Krankenversicherung 47
10.3.1 Umzug der unbelegenen Gesundheitsreformgesetzes 1989 47
10.3.2 Auswirkungen des Gesundheitsstrukturgesetzes (GSG) '93 49
10.3.3 Abrechnung mit Chipkarten 50
11. Umweltschutz und Stadtentwicklung
11.1 Einsichtsrecht in Umweltakten: Entwurf eines Umweltinformationsgesetzes 51
11.2 Die „codierte Mülltonne“ 53
11.3 Datenschutz im Naturschutzgesetz 54
11.4 Einwecklisten in bebauungssicheren (s. a. 13. Jahresbericht, Ziffer 2.8.4, Ergebnis) 55
12. Wirtschaft, Mittelstand und Technologie
12.1 Wählerverzeichnis als Mitgliederverzeichnis der Arbeitnehmerkammern (s. a. 10. Jahresbericht, Ziffer 5.12.21) 55
13. Finanzen
13.1 Die Landeshauptkasse als Sammelstelle für Belege 56
13.2 Datensicherung beim neuen Mittelbewirtschaftungssystem 56
13.3 Fall: „Informantengeheimnis“ bei der Steuererklärung von Journalisten 57
13.4 Datenflüsse nach dem Zinsabschlussgesetz 58
14. Nichtöffentlicher Bereich
14.1 Zugriffsprobleme bei Dialogsystemen 58
14.2 Fall: Unberechtigte Schul-Absprache 59
14.3 Aufbau eines Mietkaufsystems 61
14.4 Arbeitnehmerdatenschutz

14.4.1 Fall: Führungszeugnis im laufenden Arbeitsverhältnis 62
14.4.2 Fall: Unzulässige Rubriken in Bewerbungsfragebögen 62
14.4.3noch immer kein Arbeitnehmerdatenschutzgesetz 63

15. Register der nach dem Bundesdatenschutzgesetz meldepflichtigen Stellen 64

16. Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 64

16.1 Entschließung zum Arbeitnehmerdatenschutz vom 23./24.03.1992 64
16.2 Entschließung zur Neuregelung des Asylverfahrens vom 28.04.1992 66
16.3 Entschließung zum Grundrecht auf Datenschutz vom 28.04.1992 67
16.4 Entschließung zum „Lauschangriff” vom 01./02.10.1992 67
16.5 Entschließung zum Gesundheitsstrukturgesetz 1993 vom 01./02.10.1992 68
16.6 Entschließung zum Datenschutz bei internen Telekommunikationsanlagen vom 01./02.10.1992 68
1. Vorwort

1.1 Zur Situation des Datenschutzes


Kernpunkte der Kritik an dem im vergangenen Jahr verabschiedeten Gesetz zur Bekämpfung der organisierten Criminalität (OK) bleiben die Unbestimmtheit der Eingriffsvoraussetzungen sowie das Fehlen klarer Tatbestandskataloge. Es fehlt die Gewähr dafür, daß das neue Recht auf die Strafverfolgung bei schweren OK-Delikten beschränkt bleibt. Die aus diesen Gründen erfolgte Ablehnung des Gesetzes im Bundesrat durch den Bremer Senat habe ich begrüßt und hoffe, daß er die gleiche Haltung zu den anstehenden Vorschriften zur elektronischen Überwachung von Privatwohnungen einnehmen wird.

beitung von Patientendaten vorangetrieben wird. Die Krankenversicherungs-
karte als maschinenlesbare Chipkarte eröffnet eine neue Dimension des Zugriffs
auf sensible medizinische Angaben.

Keine Trendumkehr gibt es im Verhältnis zwischen der Technikentwicklung und
einem Datenschutzrecht, das seine Steuerungsfunktion zunehmend einbüßt.
Angesichts einer dezentralen Informatik-Landschaft, der zunehmenden Nutzung und
Vernetzung von Arbeitsplatzcomputern sowie der raschen Ausbreitung des
Mobilfunknetzes droht bereits die klassische Forderung nach der „Ordnungsmäßi-
gkeit“, also nach präzise programmierter, aussagefähig dokumentierter und überprifbar
protokolliert Datenverarbeitung zur Illusion zu werden. Um so mehr
kommt es auch in diesem Bundesland darauf an, die Gesamtplanung des Einsatzes
von Informations- und Kommunikationstechnologie anhand klarer Ziele, mit
präzisen Konzepten und entscheidungsbegleitenden Lenkungsgrößen durchzufüh-
ren, wobei Datenschutz und Datensicherung jeweils integrale Bestandteil sein
müssen (s. Ziffer 2.2). Die beträchtliche Nachfragemacht der öffentlichen Hand
muß genutzt werden, gegenüber den Herstellern, ggf. auch gegen deren Verkaufs-
interessen, Datenschutzstandards durchzusetzen, wie dies in Bremen ansatzweise
etwa bei der Beschaffung von ISDN-fähigen Telefonanlagen geschieht.

Die Datenschutzentwicklung auf europäischer Ebene ist gekennzeichnet durch
die Diskussion über die Richtlinien-Entwurf der EG-Kommission. Wer nicht nur
ein Europa der Händler, sondern auch ein Europa der Bürger und der Bürgerrechte
will, muß sich für einen EG-weiten Schutz des informationseltern Selbstbestim-
mungsrechts auf hohem Niveau einsetzen. Nur so kann ein Gegengewicht
gehalten werden gegen die Risiken der rapide zunehmenden Internationalisie-
 rung der Datenverarbeitung und der Datenflüsse, die mit der Vollandung des
Binnenmarktes noch zunehmen werden. Polizeidienststellen, Zollbehörden, aber
auch Banken und Versicherungen mit Auslandsfilialen sind auf wachsenden
grenzüberschreitenden Datenaustausch angewiesen. Die europäische Harmoni-
 sierung der Schutzbestimmungen hat auch zu der Konsequenz, daß sich die Regel-
ungen des EG-Bundes und Landes zunehmend verfassen. Anders ausgedrückt:
Datenschutzregelungen können zunehmend weniger isoliert im Bundes- bzw.
nationalen Kontext diskutiert und erarbeitet werden. Ein gutes Beispiel dafür ist
die EG-Richtlinie zum Einsichtsrecht in Unterlagen, die von Bund und Ländern
— jeweils im Bereich ihrer Gesetzgebungskompetenz — umgesetzt werden muß.

1.2 Schwerpunkte, Gliederung und Redaktion des Berichts

Dieser 15. Jahresbericht ist der erste, den ich nach meiner Amtsübernahme am
01. Juni 1992 auch inhaltlich voll verantwortet. An der Abfassung waren alle
Referate der Dienststelle beteiligt. Der Aufbau enthält gegenüber dem Vorgänger
einige neue Elemente. Vorangestellt sind drei Abschnitte, die Schwerpunkte
der Tätigkeit meiner Dienststelle wiedergeben. Im Kapitel 2.1 möchte ich — u. a.
an Hand einiger statistischer Zahlen — deutlich machen, daß die Beratung der
Bürgerinnen und Bürger, die Bearbeitung ihrer Anfragen, Eingaben und Beschwerden,
kurz: die „Ombudsmann-Funktion“ des Datenschutzbeauftragten im Vordergrund steht. Wer Bürgerrechte in der „Informationsgesellschaft“ sichern
will, kann dies nur mit der aktiven Mitwirkung der Betroffenen leisten; deren kri-
tische Wachsamkeit gegenüber dem „Datenhunger“ von Verwaltung und Wirt-
schaft ist unverzichtbare Hilfe für den Landesbeauftragten. Nur die Bearbeitung
eines breiten Spektrums von Einzelfällen vermag sicherzustellen, daß die Tätig-
keit meiner Dienststelle nicht zur renommierten Regierungsberatung für die senatorischen
behörden degeneriert. Die wenigen wichtigen Einzelfälle, die aus Rücksichten
im Bericht dokumentiert werden können, sind jeweils der besseren Aussichts-
lichkeit halber in der Übersicht ausdrücklich markiert (Fall).

Das zweite Schwerpunktkapitel (s. Ziffer 2.2) zur Entwicklung der Informa-
tions- und Kommunikationstechnik greift als das zur Zeit wohl aktuellste Thema
die Datenschutzzwecke im Mobilfunk, einem rasant wachsenden Segment der
Kommunikationstechnik, auf. Der andere Unterteilung glitzt der Situation im
Land Bremen: aus ihm wird deutlich, daß die Entscheidungen über die künftige
Rolle des ADV-Anschusses, über Rolle und Rechtsstellung des Rechenzentrums
der bremischen Verwaltung sowie des Fernmeldetechnischen Amtes sowie über
ein Gesamtprogramm der PC-Vernetzung möglichst bald fallen müssen, wenn
einerseits eine optimale, funktionsgerechte DV-Unterstützung der bremischen
Verwaltung erreicht und andererseits eine Verschwendung knapper Ressourcen
verhindert werden sollen. Der Beitrag zeigt auch, wie notwendig es war, die
„Technikkompetenz“ meiner Dienststelle zu erweitern, was mit der Besetzung der


Nach den Schwerpunktkapiteln folgt die Gliederung dem bisherigen Schema, d. h. insbesondere der Zuordnung der Berichtsabschnitte zu senatorischen Behörden. Insoweit dadurch thematisch eigentlich zusammengehörige Komplexe getrennt werden, wird dies in Kauf genommen, um die betroffenen Ansprechpartner leichter erkennen zu können und damit auch die Beratungen im Datenschutzausschuß zu erleichtern.

1.3 Ausblick auf 1993


Standpunkt zu Regelungsvorhaben und Automationsprojekten in den Fachdeputa-
tionen darlegen zu können. In diesem Anliegen werde ich vom Datenschutzaus-
schuß unterstützt.

2. Schwerpunkte

2.1 Eingaben und Bürgerkontakte


Von den 69 die öffentliche Verwaltung betreffenden Eingaben und Beschwerden bezogen sich 42 auf Dienststellen des Senats, 16 auf Ämter des Magistrats Bremerhaven sowie 11 auf sonstige Stellen. Was den Senat angeht, waren insbesondere die Ressorts Inneres und Sport, Justiz und Verfassung sowie der Bereich Jugend und Soziales angesprochen. Auch im öffentlichen Bereich stand die Kritik an wirklich und vermeintlich unerlaubten Datenübermittlungen im Vordergrund.


In den vorliegenden Fällen haben im übrigen die betroffenen Verwaltungsbehörden in keinem Fall einen Verwaltungsakt erlassen, d. h. ein rechtliches Verbot oder Gebot ausgesprochen. Deshalb war es erst recht nicht erforderlich und rechtlich geboten, die personenbezogenen Daten der Bürger, die die Mitteilung gemacht hatten, offenzulegen. Die von mir angesprochenen Dienststellen haben zugesagt, ihre Praxis in Zukunft entsprechend zu ändern.


2.2 Entwicklung der Informations- und Kommunikationstechnik

2.2.1 Situation im Land Bremen

Die technischen Veränderungen im EDV-Bereich machen auch vor der bremischen Verwaltung nicht halt. Teilweise bedingen diese technischen Entwicklungen neue Probleme im Bereich des Datenschutzes.

So ziehen in die bremische Verwaltung inzwischen vermehrt auch PC-Netze und tragbare Computer (Laptops, Notebooks) ein. Beide Entwicklungen haben eines gemeinsam: Die Daten werden mobil. Dies erfordert die Entwicklung von Sicherheitsstandards für „mobile Daten“ (s. u. Ziffern 2.2.1.1 und 2.2.1.2).

Manche Weiterentwicklungen im technischen Bereich bieten allerdings Möglichkeiten, die dem Datenschutz zugute kommen: Dies gilt z.B. für die Weiterentwicklung der in der bremischen Verwaltung eingesetzten Datenschutz- und Sicherheitssoftware (s. u. Ziffer 2.2.1.3).

— Organisatorische Veränderungen

Neben technischen Entwicklungen, die es zu beobachten gilt, sind auch organisatorische Veränderungen in der bremischen Verwaltung geplant, die Auswirkungen auf den Datenschutz haben können.

— ADV-Ausschuß


2.2.1.1 PC-Netze

Durch die Vernetzung von PC’s werden die Daten eines PC’s grundsätzlich für alle an diesem Netz angeschlossenen PC’s ohne Zeitverzögerung verfügbar. Ohne besondere Schutzvorschriften kann von jedem an das Netz angeschlossenen PC auf alle Daten aller an Netz hängenden PC’s zugreifen werden.

Erfahrung einiger Netzinstallationen in der bremischen Verwaltung zurückgegriffen werden kann. Zu diesen Forderungen zählen u. a.:

- Netze sollen nur dort eingesetzt werden, wo die Arbeitsorganisation und -strukturen es erfordern, d. h. wo von mehreren Personen auf die gleichen Datenbestände zugreifen werden muß.
- Der als Netz- bzw. Fileserver eingesetzte PC darf nicht als Arbeitsplatzrechner, sondern nur für diese Serverzwecke eingesetzt werden.
- Sobald auf einem der am Netz angeschlossenen PC's wegen der auf ihm zu verarbeitenden personenbezogenen Daten Schutzmaßnahmen einzurichten sind, sind diese auf allen anderen an das Netz angeschlossenen PC's ebenfalls zu installieren.
- Es muß sichergestellt sein, daß nur auf die Daten, die zur gemeinsamen Nutzung vorgesehen sind, von anderen Benutzerinnen und Benutzern zugreifbar werden kann und alle anderen Daten abgesichert sind, d. h., daß die lokalen Festplatten nur von dem jeweiligen PC aus gelesen werden können und die Netzzugriffe auf Serverfestplatten beschränkt werden.

Weitere Anforderungen ergeben sich aus den jeweiligen Anwendungen für die das Netz eingerichtet werden soll.

2.2.1.2 Laptops und Notebooks


Bei der Anschaffung der Geräte sollte von vornherein auf eine Sicherheitsausstattung Wert gelegt werden. Dazu gehören unter anderem das Vorhandensein

- eines Sicherheitsschlosses,
- eines festen Behälters mit Zündschloßkombination für den Transport, aber auch
- von Schutzvorrichtungen für die vorhandenen Schnittstellen.

Neben diesen Maßnahmen zum Schutz der Geräte sind u. a. folgende Mindestanforderungen an den Einsatz von tragbaren PC's zu stellen:

- Verarbeitung personenbezogener Daten auf tragbaren PC's darf nur erfolgen, wo dies aufgrund der Aufgaben unvermeidbar ist.
- Falls personenbezogene Daten auf dem PC verarbeitet werden, ist die Installation einer Schutzsoftware erforderlich, die die verschlüsselte Abspeicherung der Daten auch auf der Festplatte sicherstellt, sowie den Zugriff auf den PC nur nach Eingabe von Kennung und Passwortabfrage zuläßt. Passwörter müssen verschlüsselt abgelegt sein.
- Die Schnittstellen des tragbaren PC's sind zu sperren, um eine unbefugte Weitergabe von Programmen und Daten zu verhindern. Die Berechtigung zur Entsperrung der Schnittstellen zur internen Weiterleitung von Daten sollte bei der Systemverwaltung bzw. beim Systemverwalter liegen.
- Für die tragbaren PC's müssen in den Dienstdiensten, in denen sie eingesetzt werden, verschleißfeste Schränke vorhanden sein, in die sie nach Dienstschluß eingeschlossen werden.
- Besonders sensible Daten dürfen grundsätzlich nicht auf tragbaren PC's verarbeitet, erfaßt oder gespeichert werden. Nach § 28 Abs. 2 Nr. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) gehören hierzu insbesondere solche Daten, die sich
auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen oder auf arbeitsrechtliche Verhältnisse beziehen.

Auch hier ergeben sich je nach den auf dem tragbaren PC gehaltenen Daten noch weitere Anforderungen an die Datenschutzmaßnahmen. Daher werde ich die Entwicklung aufmerksam verfolgen.

2.2.1.3 Protokollierung bei „Safeguard“


2.2.2 Fernwartung von DV-Systemen

DV-Systeme müssen wie alle technischen Systeme gewartet werden, um funktionsfähig zu bleiben oder wieder zu werden. Die Wartung bezieht sich dabei auf die Hardware (sogenannte Hardware- oder Gerätewartung) und auf die Software, vor allem auf die Betriebs- und Netzsoftware und wichtige andere Fremdsoftware (sogenannte Software-Wartung).


In meinen 5. Jahresbericht (vor zehn Jahren!) habe ich bereits Anforderungen zur Ausgestaltung der Fernwartung formuliert, die sich nach dem Stand der Technik damals auf die großen Rechnersysteme bezogen. Inzwischen wird die Fernwartung auch bei kleineren Rechnersystemen und bei PC-Installationen praktiziert, was bedeutet, daß die seinerzeitigen Anforderungen auf ihre heutige Anwendbarkeit hin überprüft und ggf. angepaßt werden müssen. Hierbei hat sich gezeigt, daß die damaligen Anforderungen im wesentlichen auch heute noch gültig sind. In Übereinstimmung mit meinen Kollegen halte ich bei der Fernwartung folgende technische Anforderungen für angemessen:

— 11 —
1. Der Systembetreiber bzw. das Rechenzentrum und nicht die Wartungsfirma definiert Art und Umfang der Fernwartung (Eindringtiefe) und dokumentiert die Einzelheiten in prüffähiger Form.

2. Die Software-Fernwartung wird entweder ganz ausgeschlossen oder auf bestimmte Ausnahmefälle beschränkt.


5. Das Wartungszentrum darf nur Zugriff auf Dateien erhalten, die unter der Zugriffskennung der Wartung vom Systembetreiber/Rechenzentrum eingerichtet wurden.


7. Werden Test- und Serviceprogramme der Wartungsfirma auf der Anlage gespeichert, sind diese unter einer besonderen Kennung abzuspeichern.


2.2.3 Abhörрисiken im Mobilfunk

2.2.3.1 Aufhebung der Funkfrequenzbeschränkungen


Das BMPT hat in einer Presseerklärung die Auffassung vertreten, „der Empfang (solcher) Aussendungen, die nicht für die Allgemeinheit vorgesehen sind, bleibt aber zum Schutz des Fernmeldegeheimnisses untersagt“*. Diese Auffassung ist nicht unbestritten. Bei den juristischen Diskussionen darüber, ob bereits das Empfangen solcher Sendungen auf den Sonderfrequenzen unerlaubt ist oder erst die Verwertung des Gehörten bzw. ob ein eventuelles Verbot strafbewehrte ist oder nicht, ist immer zu berücksichtigen, daß sich eine Übertretung eines etwaigen Verbotes selten nachweisen läßt.


Die Deutsche Bundespost TELEKOM wäre verpflichtet, ihre Kundinnen und Kunden darauf hinzuweisen, daß sowohl schnurlose Telefone als auch Mobiltelefone relativ einfach abgehört werden können (vgl. § 3 Abs. 5 TELEKOM-Datenschutzverordnung — TDG).

Für Rettungsdienste, Feuerwehr, Polizei u. ä. ergibt sich die Problematik, daß über den Funkverkehr häufig z. T. sehr sensible personenbezogene Daten übermittelt werden, die leicht von Unbefugten abgehört werden können. Auch wäre das Szenario denkbar, daß Rettungsfahrzeuge eine Katastrophenstelle nicht erreichen können, weil Massen von Schaulustigen, die aus Sensationsgier die Sonderfrequenzen abgehört haben, zum Ort des Geschehens fahren und die Zufahrtswege verstopfen!

2.2.3.2 Regelungsinitiative der Innenministerkonferenz

Aus Sorge um die öffentliche Sicherheit hat die Ständige Konferenz der Innenminister und -senatoren der Länder am 20. 11. 1992 gefordert, „die bisher geltenden Funkfrequenzbeschränkungen wieder einzurichten und darüber hinaus in das Gesetz über Fernmeldeanlagen (FAG) durchsetzbare Verbote für den Vertrieb, Besitz und die Inbetriebnahme von Breitbandempfängern sowie das Abhören von geschützten Frequenzbereichen durch Unberechtigte aufzunehmen“.


2.2.3.3 Technische Gegenmittel

Schon vor der Freigabe der Sonderfrequenzen war der Schutz, den das Verbot der abhörmöglichen Geräte für die Bedürfnisse besonders der Sicherheitsbehörden (Militär, bestimmte Polizeidienststellen u. a.) darstellte, nicht ausreichend. In diesen Bereichen lief und läuft der Telefon- und Funkverkehr teilweise verschlüsselt bzw. verschleiert ab. So wird z. B. bei der Polizei Bremens ein — wenn auch
veraltetes – IDA-System zur Verschleierung von sensiblen Daten im Funkverkehr angewendet.

Eine Verschlüsselung der Funkstrecken, ob nun zwischen schnurlosen Telefonen und Basispunkt oder z. B. zwischen Rettungswagen und Leitstelle, würde das Abhören dieser Gespräche sehr erschweren bzw. nahezu unmöglich machen. Ein zufälliges Mithören wäre ausgeschlossen; nur mit hohem technischem Aufwand und viel krimineller Energie wäre das Abhören noch möglich.

Die Verschlüsselungstechnik wird aus Kostengründen weder im Bereich von Feuerwehr und Rettungsdienst noch in allen Bereichen der Polizei noch beim Fernsprechen (einschließlich der schnurlosen Telefone und der Mobiltelefone) eingesetzt. In wenigen Fällen werden Mobiltelefone in digitaler Technik (111, 12-Netz) verwendet, bei denen das Abhören schwieriger ist. Bei entsprechender Nachfrage nach Ver- bzw. Entschlüsselungstechnik wäre allerdings mit einer drastischen Preissenkung zu rechnen, so daß die Kosten nicht mehr als Grund gegen einen Einsatz dieser Technik angeführt werden könnten.

Durch die Verwendung eines schnurlosen Telefons, bei dem die Übertragung zwischen Basisstation und Handapparat digitalisiert geschieht, wird das Abhören zumindest erschwert. Einer der oben genannten Scanner reicht dazu nicht mehr aus, da die digitalisierten Funksignale auch wieder analogenisiert werden müssen, wozu eine entsprechende Synchronisation erforderlich ist. Dies erfordert einen höheren technischen Aufwand.

2.2.3.4 Maßnahmen in Bremen


2.3 Europäische Entwicklungen

2.3.1 Europarat: Bedeutungszuwachs für die Datenschutz-Konvention von 1981


### 2.3.2 Europäische Gemeinschaft: Harmonisierung durch Richtlinie

#### 2.3.2.1 Regelungsziele: Gemeinschaftsweiter Schutz des Persönlichkeitsrechts und Freiheit des grenzüberschreitenden Datenverkehrs


#### 2.3.2.2 Vom 1. Entwurf zum Geänderten Vorschlag

2.3.2.3 Systemdivergenz als Hauptproblem

Hauptproblem für eine schnelle Verständigung auf EG-Ebene sind die prinzipiellen Divergenzen der in den Mitgliedstaaten vorhandenen Datenschutzkonzeptionen. Diese Unterschiede machen die Schwierigkeit der Aufgabe deutlich, die die Kommission zu bewältigen hatte und hat, um eine inhaltliche Angleichung zu erzielen. Nur wenn man diese Systemdifferenzen kennt und akzeptiert, daß ein Rechtsinstrument der EG Bestandteile verschiedener Rechtsordnungen integriert muß, um in den Mitgliedstaaten akzeptiert zu werden, ist eine faire und gleichzeitig realistische Beurteilung des neuen Textvorschlags möglich.

Da gibt es den Unterschied zwischen Lizensierungsmodellen, also Rechtsordnungen, die die Einrichtung und Nutzung von Datenverarbeitung von der Genehmigung durch eine Kontrollinstanz abhängig machen (z. B. Frankreich, Großbritannien) und dem deutschen Konzept der genehmigungsfreien Verarbeitungs erlaubnis, wenn die Zulässigkeitsvoraussetzungen des Datenschutzes einbehalten sind. Stärker legalistisch orientierten Systemen, die nur staatlichem Recht effiziente Schutzqualität zuliehen, stehen Staaten gegenüber, die die Regelung des Umgangs mit personenbezogenen Daten mehr der Selbstregulierung durch die betroffenen Verbände und Interessengruppen überlassen wollen (z. B. die Niederlande). Die Datenschutzinstitutionen sind in mehreren Mitgliedstaaten stark auf Funktionen hoheitlicher Genehmigungen und Kontrolle beschränkt, während im deutschen Modell das Element der Hilfestellung und Beratung der datenverarbeitenden Stellen im Vordergrund steht. Während mancherorts, z. B. in Frankreich, sensible Datenkategorien benannt werden, die einem Sonderschutz unterstehen, folgt die Datenschutzdoktrin in Deutschland spätestens seit dem Volkszählungsgerichtsverfahren und der Entscheidung des Bundesverfassungsgerichts der These, daß die Schutzwürdigkeit personenbezogener Angaben ausschließlich vom Verwendungskontext abhängt. Während des Datenschutzes hierzu ist das höchste Eingriffsrisko eher dem öffentlichen Bereich zuliebe, also im Verhältnis zwischen Staat und Bürger sieht, sind es anderswo in erster Linie die privaten Datenverarbeiter, denen die Verarbeitungsrestriktionen gelten.

2.3.2.4 Abweichungen vom deutschen Datenschutzmodell


Für sensitive Daten — Art. 8 zählt dazu Angaben über die rassische und ethnische Herkunft, die politische Meinung, die religiöse, philosophische oder moralische
Überzeugung, die Gewerkschaftsangehörigkeit oder die Gesundheit — stellt die Richtlinie ein grundsätzliches Verhaltensverbot auf, das nur unter engen Voraussetzungen aufgehoben werden kann. Eine dieser Möglichkeiten besteht darin, daß die Mitgliedstaaten aus Gründen wichtiger öffentlicher Interessen gesetzliche Ausnahmen vorsehen. Im deutschen Regelungskontext wäre als Konsequenz dieser neuen Regel-Ausnahme-Systematik eine Reihe spezieller gesetzlicher Erlaubnisse zu schaffen, z. B. für die Nutzung des Merkmals Gewerkschaftsangehörigkeit durch den Arbeitgeber beim tarifvertraglich vereinbarten Direkteinzug der Beiträge.


In den Beratungen der EG-Gremien und in den Interventionen verschiedener Lobbygruppen — nicht zuletzt aus den USA — wurde die Regelung der Zulassungsvoraussetzungen für die Weitergabe personenbezogener Daten in Drittstaaten (Art. 26, 27) besonders intensiv diskutiert und kritisiert. Für Zelinder, die nicht Mitglied der EG sind und die kein angemessenes Schutzniveau, also insbesondere keine Datenschutzgesetzgebung, aufweisen, geht die Richtlinie von einem grundsätzlichen Verbot des Datenexports aus. Diesem Prinzip steht ein abschließender Katalog von Ausnahmen gegenüber, wozu insbesondere der Fall gehört, daß die Übermittlung von Daten in einen Drittstaat ohne Datenschutzrecht zur Erfüllung eines Vertrages (z. B. eines Reisevertrages) notwendig ist (Art. 26 Abs. 1 Satz 2). Als Ausnahme läßt die Richtlinie auch die viel diskutierte „Vertragslösung“ zu (Art. 27 Abs. 1), also die Absicherung der Einhaltung des Datenschutzrechts des Exportstaates durch einen Vertrag zwischen der übermittelnden Stelle und dem ausländischen Empfänger. § 17 BDSG, der die Datenübermittlung durch Bundesbehörden an Stellen außerhalb des Geltungsbereiches des BDSG normiert, müßte bei Inkrafttreten der Richtlinie entsprechend neu gefaßt bzw. präzisiert werden; für die grenzüberschreitende Weitergabe durch nichtöffentliche Stellen müßte eine entsprechende Bestimmung neu geschaffen werden.

2.3.2.5 Akzeptanz der Rechtsangleichung

Der an ausgewählten Divergenzbeispielen gezogene Vergleich von Konzeption und Regelungsinhalten des Richtlinien-Vorschlags einerseits und des deutschen Datenschutzrechts andererseits darf nicht mißverstanden werden. Es wäre ein verleitender Ansatz, aus der einzelstaatlichen Perspektive die Vorstellungen der Gemeinschaft anglistisch darzulegen, abzurütteln, insoweit sie ihrem eigenen Recht abweichen, und dann alle Bemühungen daran zu setzen, im weiteren Beratungsverfahren noch so viel wie möglich von dem in Deutschland bestehenden Regelungsmodell „zu retten“. Eine integrationsfreundliche Sichtweise muß die von unseren EG-Partnerländern entwickelten Lösungsmodelle zur Kenntnis nehmen, sich um deren Verständnis bemühen und sich auf den Versuch einlassen, gemeinsame Grundstrukturen herauszustellen und bewährte Elemente von unseren Nachbarstaaten zu übernehmen. Dies gilt auch dann, wenn das soeben reformierte BDSG oder die jüngeren Landesdatenschutzgesetze erneut novelliert werden mußten. Diese Konsequenz ergibt sich keineswegs nur im Bereich des Datenschutzes; die parallele Problematik stellt sich bei vielen anderen auf Harmonisierung angelegten Initiativen der Kommission, zuletzt vor allem im Bereich des Umweltschutzes.
2.3.3 Aktuelle Themen der deutschen Diskussion

2.3.3.1 Höchststandard oder Mindestniveau

In den Mittelpunkt der deutschen Diskussion hat sich jüngst vor allem die Frage geschoben, ob die Richtlinie einen Höchststandard an Datenschutz festlegt, der vom einzelstaatlichen Recht nicht überschritten werden kann, oder ob die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz auf nationaler Ebene intensiver auszugestalten und fortzuentwickeln. Das Rechtsinstrument der Richtlinie mit ihrem doppelstufigen Verfahren war zwar ursprünglich eindeutig für die Festlegung eines EG-weiten Mindestniveaus vorgesehen, wird inzwischen aber in der Rechtssetzungspraxis der EG-Institutionen vielfach ähnlich detailliert wie die in den Mitgliedstaaten unmittelbar verbindliche Verordnung ausgestaltet. Ähnlich wie in Deutschland hat der Bund Kompetenz zur Rahmengesetzgebung; immer wieder zum Erfolg von Vollregelungen benutzt hat (z.B. im Melderecht), machen auch oft und Kommission mit Richtlinien gelegentlich ins einzelne gehende Vorgaben, die den eigentlich vorgesehenen Spielraum für die Umsetzung in das einzelstaatliche Recht weitgehend einschränken.

Die Frage, ob die Datenschutz-Richtlinie „nach oben offen“ ist oder nicht, läßt sich nicht pauschal beantworten, verlangt vielmehr eine präzise Analyse der in den einzelnen Bestimmungen enthaltenen Spielräume. Die Richtlinie enthält einerseits ausdrückliche "Obligatorien", die mit der Formulierung "Die Mitgliedstaaten können vorsehen ... explizit den einzelstaatlichen Gesetzgebungsrahmen, die Erweiterungsmöglichkeiten einräumen. Beispiel dafür ist Art. 20, der die Errichtung der Meldepflicht zum Register auf nicht-autonomen Dateien zulässt.

In der Richtlinie gibt es andererseits eine allgemeine Interpretationsklause, wonach die Mitgliedstaaten "die Voraussetzungen näher bestimmen (können), unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist" (Art. 5 Abs. 2). Diese Formulierung erlaubt die Ausfüllung der zahlreichen Generalklauseln, etwa - wie die Begründung ausführt - die Feststellung der Fälle, in denen das Interesse der betroffenen Person dem Verarbeitungsinteresse der speichernden Stelle oder eines Dritten vorgeht (vgl. Art. 7 f). Die Konkretisierung einer solchen Interessenausgewogenheit erlaubt mithin eine erhebliche Bandbreite bereichsspezifischer Regelungen. Gleiches gilt z.B. für die zahlreichen weitergeteilten Ausnahmen bei der Verarbeitung sensibler Daten (Art. 8 Abs. 2 und 3).


Kollisionslagen können sich allerdings nur dort ergeben, wo es um einzelstaatliche bereichsspezifische Vorschriften im Geltungsbereich der Richtlinie geht, ein Großteil der sektoralen Regelungen dagegen - etwa im Recht der Sicherheitsbehörden - befindet sich außerhalb der Gemeinschaftskompetenz.

2.3.3.2 Kontrollinstitutionen

Jeder Mitgliedstaat muß eine oder mehrere staatliche Behörden benennen, die für die Überwachung der Einhaltung des Datenschutzes zuständig sind. Diese Behörden müssen „unabhängig“ sein, was im deutschen dualen Kontrollmodell insoweit Probleme schaffen könnte, als die Aufsichtsbehörden für den nicht-offiziellen Bereich anders als die Datenschutzbeauftragten des Bundes und der Länder in die Hierarchie der Verwaltungsbehörden eingegliedert sind. Das Erfordernis der Unabhängigkeit bezieht sich nach der Intention der EG-Kommission wohl in erster Linie auf das Verhältnis zur Regierung bzw. Exekutive und weniger auf die Abgrenzung von den zu kontrollierenden Stellen (Behörden, Unternehmen).
Bevor allerdings Abstriche an dieser Anforderung gemacht werden, sollten insbesondere die Organisationsmodelle der Nachbarstaaten auf übertragbare Elemente hin geprüft werden. Wird die Unabhängigkeit als institutionelle Bedingung der Kontrollinstitution in der Richtlinie wegen der deutschen Besonderheiten teilweise „geoptert“, besteht zum einen die Gefahr, daß der freie Status der in den EG-Mitgliedstaaten bestehenden Datenschutzinstanzen wieder in Zweifel gezogen wird. In den EG-Ländern, die aufgrund der Richtlinie erstmals ein nationales Datenschutzgesetz verabschieden müssen, könnte die Regierungsabhängigkeit der Überwachungsbehörden die Kontroll effizienz nachhaltig schwächen und die Implementation des neuen Rechts behindern.

2.3.3 Abschaffung des betrieblichen Datenschutzbeauftragten


2.3.4 Gesamtbewertung und weiteres Verfahren


Trotz aller Kritikpunkte im einzelnen verdient der geänderte Vorschlag im ganzen ein positives Urteil. Gegenüber dem ersten Text vom September 1990 lassen sich ein leichter verständlicher Aufbau, eine klarere Systematik und eine größere Praktikabilität feststellen. Im weiteren Gesetzgebungsverfahren besteht noch die Möglichkeit, die eine oder andere Verbesserung aus der Sicht deutscher Erfahrungen zu erzielen, etwa die ausdrückliche Verankerung einer einzelstaatlichen Option für die Bestellung betrieblicher Beauftragter für den Datenschutz (s. o. Ziffer 2.3.1.3). Änderungswünsche sollten sich aber auf unverzichtbar erscheinende Kernforderungen beschränken. Sonst besteht die Gefahr, daß dieses sehr schwierige Harmonisierungsprojekt, bei dem bereits viel erreicht worden ist, zerredet.

3. Senatskanzlei

3.1 Schutz von Teilnehmerdaten beim Privatfernsehen


Diese Form des „Bezahlfernsehens“ gibt es in Deutschland zwar derzeit nicht, sie könnte aber jederzeit eingeführt werden. § 28 des am 01.01.1992 in Kraft getretenen Rundfunksstaatsvertrages enthält daher vorsorglich die Vorschrift, daß die Abrechnungsdaten in einer Form zu speichern sind, die „Teilnehmerprofile“ verhindert, wenn nicht der Betroffene selbst ausdrücklich eine detaillierte Regelung verlangt.


Senatskanzlei und Bürgerschaftsausschuß sind meinen Vorschlägen gefolgt und haben sie in den Gesetzentwurf aufgenommen.

4. Personalwesen

4.1 Automatisierte Arbeitszeitverwaltung in der bremischen Verwaltung


Aufgrund dieses Berichts hat die Senatskommission für das Personalwesen (SKP) einen Entwurf zur Änderung der bremischen Arbeitszeitverwaltung sowie einen Entwurf zur Änderung der „Grundsätze für die gleitende Arbeitszeit“ vorgelegt.
Des weiteren beabsichtigt der Senator für Finanzen (SfF), in seinem Ressort die automatisierte Arbeitszeitfassung einzuführen und hat dazu den Entwurf einer „Musterdienstvereinbarung für die Arbeitszeitregelung und -erfassung“ vorgelegt.

— Verordnung zur Änderung der Bremischen Arbeitszeitverordnung (SKP)

Der Entwurf sieht in § 4 vor, daß entgegen der bisherigen Regelung alle Beamten — ausgenommen sind bestimmte Personalgruppen — an der gleitenden Arbeitszeit teilzunehmen haben und daß die tägliche Arbeitszeit automatisiert zu erfassen ist.

Ich habe die SKP darauf hingewiesen, daß die als Rechtsgrundlage für die Arbeitszeitverordnung vorgesehene Vorschrift des § 71 Abs. 1 Bremisches Beamtenverwaltungsrecht (BremBG) möglicherweise die in § 4 Abs. 5 des Verordnungsentwurfs vorgesehene ausnahmslose automatisierte Erfassung nicht abdeckt. Die Ermächtigungsnorm im Gesetz besagt lediglich, daß der Senator die regelmäßige Arbeitszeit durch Rechtsverordnung regeln soll. Die SKP hat zugesagt zu prüfen, ob die Ermächtigungsnorm im BremBG im Hinblick auf die Erfordernisse des Art. 80 Abs. 1 Satz 2 Grundgesetz (GG) präzisiert werden muß, wonach Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz bestimmt werden müssen.

— Grundsätze für die gleitende Arbeitszeit (SKP)


— Musterentwurf einer Dienstvereinbarung (SfF)


Auch hier ist vorgesehen, die tägliche Arbeitszeit durch automatisierte Zeiterfassungsgeräte an den Eingängen der Dienstgebäude zu erfassen. Die Dienstzeiten sollen für jeden Bediensteten auf einem Arbeitszeitkonto festgehalten werden, das in den Personalstellen der Beschäftigungsstellen geführt wird. Auch hier habe ich mich gegen die Einbeziehung der Beschäftigten ohne Gleitzeitoption gewandt und unterstrichen, daß als Zweck der automatisierten Erfassung eine
bloße „Pünktlichkeitskontrolle“ nicht in Betracht kommt (s. o.). Der Senator für Finanzen teilt meine Auffassung nicht und beabsichtigt nach wie vor, auch die Beschäftigten mit fester Arbeitszeit in die automatisierte Arbeitszeitermittlung einzubeziehen. In der SKP dagegen bestehen Überlegungen, in die „Grundsätze“ entsprechende Ausnahmevorschriften aufzunehmen.

Den vorgesehenen Katalog der zu erfassenden und auszuwertenden Daten habe ich als zu umfangreich bemängelt, weil Geburtsdatum, Personenzahl sowie die telefonische Telefonnummer für die Arbeitszeitermittlung nicht erforderlich sind. Der Senator für Finanzen wird den Datenkatalog entsprechend reduzieren.


Außerdem ist die im Haus des Reichs vorgesehene Hard- und Software für das Arbeitszeit-Erfassungssystem verändert. Da die Arbeitszeitkonten in den Personalstellen der einzelnen Dienststellen (senatorische Behörde, Finanzamt etc.) getrennt werden, ist eine zentrale behördenspezifische Speicherung zu vermeiden.


Der zentrale Drucker sollte nur dazu dienen, System-Fehlermeldungen auszudrucken. Durch geeignete Maßnahmen ist sicherzustellen, daß die Systemadministration keinen Zugriff auf die Arbeitszeitdaten erhält.

Eine zunächst vorgesehene gleichzeitige Nutzung des zentralen Servers für externe Bürokommunikationsdienste (z. B. elektronische Post, Telefax) ist abzulehnen, da durch den Anschluß an das offene Postnetz die Datensicherheit und der Datenschutz nicht mehr ausreichend gewährleistet werden können („Blacklisting“).


Der Senator für Finanzen hat erklärt, er werde meine Vorschläge zum Einsatz der Hard- und Software übernehmen, zumal eine Reduzierung der DV-Ausstattung auf das notwendige Maß kostengünstiger sei. Der überarbeitete Musterentwurf soll mir unverzüglich vorgelegt werden.

4.2 Personalplanungs- und -statistiksystem

Die Senatskommission für das Personalwesen (KSK) hat das Konzept „Personalcomputer-unterstützte Personal- und Stellendateninformationssystem (PSI)“ entwickelt, mit dem Ziel, diese PC-Anwendung bei allen Personalstellen der bremer Verwaltung einzuführen. Vorgesehen ist im wesentlichen, Personalinformationen
aus den automatisierten Abrechnungsverfahren bzw. Stellenplanverzeichnissen der SKP den Personalstellen mittels eines Abrufverfahrens zur Verfügung zu stellen. Diese Personaldatensysteme sollen durch die in den Personalstellen der Behörden vorhandenen Personaldaten ergänzt werden.

Ziel dieser dezentralen Personalführungsprogramme soll es sein, eine flexible und unabhängige Personal- und Stellenplanung zu ermöglichen. Hierzu ist insbesondere beabsichtigt, die bisher in unterschiedlicher Form vorhandenen Daten (Karteikarten, Geschäftsverteilungspläne, Personalakten und Stellenplan-Listen) zu integrieren. PePSI soll also eine Vielzahl von Personaldaten (z. B. Berufsbildung, Arbeitszeit, Dienstpostenübergabe, Datum der letzten Beförderung/ Höhergruppierung u. a.) enthalten, obwohl viele Daten für die Bearbeitung von Personalausweisungen nicht ständig benötigt werden.


Im Übrigen ist § 14 Bremisches Datenschutzgesetz (BrDSG) beachtlich, wonach die Einrichtung eines Abrufverfahrens den Erlaß einer Rechtsverordnung vorschreibt. Hierbei sind Datenempfänger, die Datenart und der Zweck des Abrufs festzulegen.

Soweit die Personalstellen an die SKP-Datenbanken angeschlossen werden und insoweit ein Datenaustausch stattfindet, ist grundsätzlich davon auszugehen, daß sowohl die SKP als auch die jeweiligen Personalstellen die gleichen personenbezogenen Geschäftstätigkeiten zur Verfügung stehen. Dies ist besonders dann problematisch, wenn unklar bleibt, welche konkreten Aufgaben im Rahmen der Personalausweisung und Personalverwaltung der SKP bzw. als Abgrenzung dazu den Personalstellen der einzelnen Dienststellen obliegen. Erst wenn geklärt ist, welche Stellen welche Aufgaben wahrnehmen, können die Geschäftstätigkeiten erkannt werden, welche Stellen zu welchem Zweck welche personenbezogenen Daten benötigen.


Die SKP hat Mitte Februar 1993 mitgeteilt, sie werde in Kürze einen Sachstandsbericht vorlegen und darin auch auf meine Rechtsauflösung detailliert eingehen.

4.3 Neues Personalkonzeption


Eine weitere Verbesserung des Datenschutzes ergibt sich aus der strikten Trennung der Beihilfeunterlagen, die stets als Teilakte zu führen und von der übrigen Personalakte getrennt aufzubewahren sind. Beihilfeunterlagen sollen in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Einheit haben.

Darüber hinaus enthält das novelliertere BRRG präzise Regelungen zum Aktenrechts- und Benachrichtigungspflicht bei erstmaliger Speicherung der Daten. Insbesondere ist dem Beamtentagungsausschuß sorgfältig der Zugang der Beamten und Beamtenkabinetten zu erlassen. Das Einsichtsrecht umfaßt auch andere Akten, die personenbezogene Daten über den Beamten enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden; dies gilt jedoch nicht für Sicherheitsakten.

Eine weitere Regelung beinhaltet, daß von den Unterlagen über medizinische oder psychologische Untersuchungen und Tests im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet oder genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz des Beamten dient.


Die Senatskommission für das Personalwesen hat erklärt, in der ersten Hälfte des Jahres 1993 einen Gesetzentwurf vorzulegen und mich frühzeitig zu beteiligen.

4.4 Bewerbungen in der Stadtverwaltung Bremerhaven
(s. a. 13. Jahresbericht, Ziffer 2.1.1. Ergebnis)


Nach Erörterungen im Datenschutzausschuß der Bremerischen Bürgerschaft hat der Magistrat beschlossen, daß grundsätzlich die Bewerbungen direkt an das Personalamt bzw. Schultamt zu richten sind, wobei es den Bediensteten freigestellt wird, ob sie den Weg über die Amtsleitung wählen wollen. Die Ausschreibungsrichtlinien sind entsprechend überarbeitet worden, so daß ein datenschutzgerechteres Bewerbsverfahren sichergestellt ist.

4.5 Eigenständiger Beihilfespruch für Familienangehörige
(s. a. 13. Jahresbericht, Ziffer 2.1.5. Ergebnis)


Nach Beratungen im Datenschutzausschuß der Bremerischen Bürgerschaft ist mit der Senatskommission für das Personalwesen (SKP) vereinbart worden, daß Familienangehörige eines Beihilfeberechtigten direkt bei der Beihilfestelle der SKP die Erstattung beihilfesfähig Erstattung beihilfesfähig der Aufwendungen beantragen können. Nach Gewährung der Beihilfe wird ein Duplikat des Bescheides in einem verschlossenen Umschlag, der nur unter bestimmten Bedingungen geöffnet werden kann, zur Personalakte

Die SKP beabsichtigt, anlässlich der anstehenden Anpassung der Beihilfewerkschriften an das Gesundheitsstrukturgesetz noch in diesem Jahr auf das neue Verfahren hinzuweisen.

5. Inneres

5.1 Polizei

5.1.1 PC-Netz für die Bearbeitung von Anzeigen (s. a. 14. Jahresbericht, Ziffer 2.2.2.1. Ergebnis)


5.1.2 Verringerung der bundesweiten Datenspeicherung bei Staatsschutzdelikten


Um eine Trennung zwischen den in APIS zu erfassenden Personen und den nur im Lande Bremen zu speicherdenden Personen aus dem Bereich des Staatsschutzes zu ermöglichen, hatte ich vorgeschlagen, alle in Bremen relevanten Fälle im Staats-
schutzbereich im bremischen Informationssystem der Polizei ISA (Informationssystem „Anzeigen“) zu speichern und nur die schweren oder überregional tätigen Täter in das beim Bundeskriminalamt geführte APIS einzuspeichern.

Mein Lösungsvorschlag, alle bremischen Staatschutzfälle vollständig in ISA zu führen, hat den Vorteil, daß der Staatschutz am Verfahren ISA/CANASTA (Zentrales Aktennummerversystem der Staatsanwaltschaft) teilnehmen kann und damit erheblich schneller über den Verfahrensausgang bei der Staatsanwaltschaft informiert ist. Zum anderen können die von Staatschutz in ISA gespeicherten Daten am Lückentestsverfahren teilnehmen und einer automatisierten geführten Lösungsprüfung zugeführt werden.

Bei einem Besuch im Dezember 1992 habe ich die Umsetzung meiner Anregungen überprüft. Ich konnte feststellen, daß ein beim Staatschutz installierter PC-Online mit dem ISA-Verfahren beim Rechenzentrum der bremischen Verwaltung (RhV) verbunden ist. Im einzelnen erfolgt die Umsetzung der ISA-Anbindung folgendermaßen:

Alle eingeleiteten Ermittlungsverfahren werden bei Eingang in die Staatsanwaltschaft abteilung in ISA erfaßt. Vor der Weitergabe an die Staatsanwaltschaft erfolgt vom Staatschutz eine Ausgangserfassung, d.h. soweit sich aufgrund der Ermittlungs-Sachverhalte geändert haben, werden die Daten in ISA entsprechend korrigiert oder ergänzt. Die Staatschutzfälle erhalten in ISA eine gesonderte Kennung und sind von anderen Polizeidienststellen nicht abrufbar.

Die Erfassung von Staatschutz-Fällen, die Eingabe von Änderungen sowie die Löschung von einzelnen Fällen erfolgt ausschließlich über den Staatschutz-PC. Aufgrund noch bestehender Probleme hinsichtlich der Druckersteuerung durch die RhV-Programme wird auch auf ein gesondert ausgewiesenes Terminal mit Druckausgabe in der ISA Zentrale zurückgegriffen. Ich gebe aber davon aus, daß dieses Problem demnächst beseitigt sein wird.


5.1.3 § 218 StGB: Speicherung betroffener Frauen


Auch das Polizeipräsidium Bremen hat sich mir gegenüber entsprechend erklärt. Im Februar 1993 sei über diesen Deliktbereich in ISA keinerlei Speicherungen mehr vorhanden.

Darüber hinaus hatte ich gehalten zu prüfen, ob auf eine automatisierte Speicherung in ISA nicht generell verzichtet werden kann. Es sollte vielmehr angestrebt werden, die Vorgänge nur noch unmittelbar in den zuständigen Kriminalkommissariaten zu verwalten.

Hierzu hat das Polizeipräsidium Bremen mitgeteilt, daß aus seiner Sicht keinerlei Bedenken gegen die von mir vorgeschlagene Verfahrensweise bestehen, aus
Gründen einer effizienten Vorgangsverwaltung jedoch die Speicherung der Personendaten in ISA zunächst (d. h. bis zum Abschluß des Strafverfahrens) erforderlich sei.

Ich beabsichtige, dem Senator für Inneres und Sport vorzuschlagen, entsprechend der technischen Lösung im Staatsschutzbereich einen abgeschlossenen Bereich in ISA für solche Fälle einzurichten. Spätestens mit der Einführung von ISA-D (s. a. o. Ziffer 5.1.1) muß ohne eine solche Lösung grundsätzlich auf eine Speicherung in ISA verzichtet werden.

5.1.4 Multifunktionale PC-Nutzung im Polizeiführungsstab


5.2 Ausländer

5.2.1 Asylbewerber

5.2.1.1 Erkennungsdienstliche Behandlung

(s. a. o. Jahresbericht, Ziffer 2.2.3.3)


Wie in diesem System die Prinzipien der Zweckbindung und der Erforderlichkeit bei der Datenverarbeitung eingehalten werden können, ist nicht erkennbar. Auch erneuere ich meine Kritik an der Führung einer Informationsdatenbank, die nach polizeilichen Gesichtspunkten angelegt wurde, nach der Rechtslage aber allein
asyl- und ausländerrechtlichen Zwecken dienen soll. Da die erkenntnisdienstliche Behandlung von Asylbewerbern nur verhindern soll, daß eine Person sich mit mehreren Namen registrieren läßt, rechtzeitig dies nur eine auf die Ausländerbehörden beschränkte Datei. Eine Speicherung der Identitätsunterlagen hätte daher bei den Ausländerämtern bzw. beim Ausländerzentralregister (AZR) — nach Schaffung einer entsprechenden gesetzlichen Grundlage — erfolgen müssen.


5.2.1.2 Fall: Bonitäts einschätzung an Mietwagenverleih


Ich habe zugesagt, an der Lösung der im Ausländeramt bestehenden Datenschutzprobleme mitzuarbeiten.

5.2.2 Automation im Ausländeramt


Ich habe meine Beteiligung an der notwendigen umfassenden Neuorientierung des DV-Verfahrens zugesagt.
5.3 Verfassungsschutz

5.3.1 PC-Netz im Landesamt
(s. a. 14. Jahresbericht, Ziffer 2.2.1.3, Ergebnis)

Wie in meinem letzten Tätigkeitsbericht dargestellt, hatte das Landesamt für Verfassungsschutz (LIV) geplant, die Terminalanbindung an das bundesweite NADIS-System des Verfassungsschutzes durch ein PC-Netz zu ersetzen. Dieses Netz ist mittlerweile installiert, und ich hatte Gelegenheit, die Installation zu besichtigen.

Im Einsatz sind vier PC, von denen einer die Server-Funktion übernimmt und somit die Verbindung zu dem NADIS-Rechner beim Bundesamt für Verfassungsschutz herstellt. Die anderen PC werden mittels eines Terminal-Emulationsprogramms als NADIS-Stationen eingesetzt und können darüber hinaus als Einzelplatzrechner zur Textverarbeitung und zur Tabellenkalkulation genutzt werden.

Ich hatte daraufhin gefordert, eine Sicherungssoftware derart einzusetzen, daß
— die Bereiche für die Terminal-Emulation und für die PC-spezifischen Anwendungen voneinander getrennt sind;
— die Anwender keinen Zugang zum Betriebssystem erhalten;
— die Diskettenlaufwerke gesperrt werden;
— die Zugangsberechtigung zum Server nur für Systemverwalter eingerichtet wird;
— die NADIS-Anmeldungen und -Abmeldungen landesweit protokolliert werden.

Mittlerweile hat mir das LIV bestätigt, daß die Sicherungssoftware entsprechend installiert sei. Unter diesen Voraussetzungen bestehen aus technischer und organisatorischer Sicht keine Bedenken gegen den Einsatz des PC-Netzes.

5.3.2 Sicherheitsüberprüfungen


Nachdem der Bund mit diesem Gesetz nur seinen Verantwortungsbereich regeln will, ist es Sache des Landes Bremen, für seine Bediensteten eigene gesetzliche Regelungen zu schaffen.

5.3.3 Kontrollbefugnis des LfV (s. a. 14. Jahresbericht, Ziffer 2.2.1.1. Ergebnis)


Gegenüber dem Senator für Inneres und Sport habe ich daraufhin auf die mir gesetzlich zustehende Zutritt-, Akteneinsichts- und sonstigen Prüfrechte hinge- wiesen. So habe ich z. B. gem. § 27 Abs. 3 Nr. 2 Bremisches Datenschutzgesetz (BrDSG) das Recht, das LfV unangemeldet aufzusuchen und die Diensträume zu betreten.

Der Senator für Inneres und Sport hatte daraufhin das LfV angewiesen, in jedem Fall das Zutrittsrecht des Landesbeauftragten für den Datenschutz zu allen Dienst- und Geschäftsräumen der Behörde (§ 27 Abs. 3 Satz 2 Nr. 2 BrDSG) und seine übrigen Rechte bei der Einsichtnahme in Unterlagen, Akten, gespeicherte Daten, Datenverarbeitungsprogramme und Programmunterlagen (§ 27 Abs. 3 Satz 2 Nr. 1 BrDSG) zu beachten. Dieser Punkt ist damit für mich erledigt.


Da diese Frage zuerst nur und dem Senator für Inneres und Sport kontrovers war, hat der Datenschutzausschuß die Problematisierung beraten.

Als Ergebnis kann festgehalten werden, daß anerkannt wurde, daß die materielle Prüfbefugnis für die von anderen Verfassungsschutzbehörden eingespeisten Daten dem jeweiligen Landesdatenschutzbeauftragten bzw. dem Bundesdaten- schutzbeauftragten obliegt, daß es aber notwendig ist, festzustellen zu können, welche anderen Verfassungsschutzbehörden die zu den jeweiligen Person eingespist haben. Für gemeinsame Daten im Sinne von § 6 Bundesverfassungs- schutzgesetz enthält die Gesetzesbegründung zur Vorschrift die Aussage, daß speichernde Stellen hinsichtlich des gesamten Datenbestandes alle (jeweils) beteiligten Verfassungsschutzbehörden sind. Der Abruf von Daten ist nach der Gesetzesbegründung als Nutzung und nicht als Abruf im automatisierten Verfahren zu qualifizieren. Eine Erweiterung der inhaltlichen Kontrollkompetenz der einzelnen für die beteiligten speichernden Stellen zuständigen Datenschutzbeauftragten kann und soll daraus nicht abgeleitet werden, wohl aber das Recht zur Kenntnisnahme.

5.4 Straßenverkehr

5.4.1 Meldung von Drogenkonsumenten an die Führerscheinstelle


Als Rechtsgrundlage kommt § 33 Abs. 1 Satz 1 Bremisches Polizeigesetz (BrempolG) in Frage. Danach darf die Polizei personenbezogene Daten an sonstige öffentliche Stellen übermitteln, wenn dies zur Erfüllung polizeilicher Aufgaben unerläßlich ist. Zu den originären polizeilichen Aufgaben gehört nach § 1 Abs. 1 BrempolG, Gefahren für die öffentliche Sicherheit abzuwenden.


Nach diesem Gutachten ergeben sich mithin erhebliche Zweifel an der Fahrtüchtigkeit des Haschischkonsumenten, so daß eine Gefahr für andere Verkehrsteilnehmer grundsätzlich zu unterstellen ist. Demzufolge stellt die Meldung von Personen, bei denen im Straßenverkehr Haschischkonzentrat bzw. -besitz festgestellt werden, eine Maßnahme zur Fahrerabwürfe dar, weil nur dadurch die Führerscheinstelle ermöglicht wird, die Fahrtüchtigkeit des Drogenkonsumenten festzustellen.


5.4.2 Fall: Nebentätigkeitskontrolle durch Aufsichtsbehörde

Der Senator für Inneres und Sport hat als Aufsichtsbehörde nach dem Fahrlehrergesetz (FahrLrG) eine Fahrerschule überprüft und dabei festgestellt, daß ein nebenberuflich tätiger Fahrlehrer hauptsächlich Beamter ist. Aus den Aufzeichnungen der Fahrerschule ergaben sich für die Aufsichtsbehörde Zweifel, ob die geleisteten Fahrstunden des nebenberuflichen Fahrlehrers mit seiner Nebentätigkeitsgenehmigung übereinstimmen. Aus diesem Grund hat sie den Dienstherrn über den eventuellen Verstoß gegen die Nebentätigkeitsverordnung informiert.
Der Senator für Inneres und Sport begründet die Datenweitergabe damit, bei Überschreiten einer Nebentätigkeitsgenehmigung sei er im Interesse der Verkehrssicherheit als seine Pflicht an, die Beschäftigungsdiensstelle zu informieren. Dies sei erforderlich, da die Aufsichtsbehörde nicht beurteilen könne, ob der Betroffene an seinem Arbeitsplatz so ausgelastet ist, daß die Überschreitung der Nebentätigkeitsgenehmigung dazu führt, daß er zu einer ordnungsgemäßen Fahr- ausbildung nicht mehr in der Lage ist. Die Beschäftigungsdiensstelle habe unter Berücksichtigung der Grundsätze der Verhältnismäßigkeit und nach eigenem Ermessen zu entscheiden, inwieweit sie gegen den Betroffenen vorgeht.

Im übrigen vertritt die Aufsichtsbehörde die Auffassung, eine Nebentätigkeitsgenehmigung beinhalte immer, daß der Betroffene neben seiner hauptberuflichen Tätigkeit nur in einem Zeitrahmen eine andere Tätigkeit zusätzlich ausüben kann, der ausschließlich, daß seine hauptberufliche Tätigkeit darunter leide. Außerdem sei das Erfordernis einer Nebentätigkeitsgenehmigung sinnlos, wenn sie nicht überprüft und das Überprüfungsergebnis nicht mitgeteilt werden dürfte.

Ich habe den Senator für Inneres und Sport darauf hingewiesen, daß die Datenweitergabe durch die Aufsichtsbehörde an den Dienstherrn des nebenberuflichen tätigen Fahrlehrers gegen das Zweckbindungsprinzip verstößt. Die Aufsichtsbehörde hat nach § 33 Abs. 2 Satz 2 FahrIG nur die Befugnis, in die vorgeschriebenen Aufzeichnungen Entschließung zu nehmen. § 18 Abs. 2 FahrIG regelt abschließend, welche Aufzeichnungen der Inhaber einer Fahrerschule über die Fahrlehrer vorzunehmen hat. Danach ist er verpflichtet, für jeden Fahrlehrer täglich die Anzahl der Fahrstunden und die Gesamtdauer des praktischen Fahrunterrichts in Minuten aufzuzeichnen. Diese Regelung schließt Hinweise auf Nebentätigkeiten der Fahrlehrer aus.

Gleichwohl hat die Aufsichtsbehörde Erkenntnisse darüber erhalten und diese an den Dienstherrn des betroffenen Fahrlehrers wegen eines eventuellen Verstoßes gegen die Nebentätigkeitsverordnung unzulässigerweise weitergegeben, obwohl personenbezogene Daten nach § 12 Abs. 1 Bremisches Datenschutzgesetz (BrDSG) nur für Zwecke verarbeitet werden dürfen, für die sie erstmals gespeichert worden sind. Eine Befugnis zur Durchbrechung dieses Zweckbindungsprinzips nach § 13 i. V. m. § 12 Abs. 2 und 3 BrDSG bestand nicht. Der Senator für Inneres und Sport hat sich noch nicht dazu geäußert, ob er die Praxis entsprechend meiner rechtlichen Würdigung geändert hat.

5.5 Statistik

5.5.1 Bevölkerungsstatistik

(s. a. 12. Jahresbericht, Ziffer 2.2.3.2)


Die datenschutzrechtlichen Mängel des Bevölkerungsstatistikgesetzes beziehen sich im wesentlichen auf folgende Punkte:


— 32 —
hervorrufen kann und ob das Ziel der Erhebung nicht auch durch eine anonymisierte Datenerhebung erreicht werden kann.


— Abstriche am Erhebungsprogramm und an den Erhebungsmöglichkeiten nicht vorgenommen wurden,

— weiterhin Daten über den Bedarf der Verwaltung hinaus mit Auskunftspflicht erhoben werden sollen und

— Datenschutzprobleme beim Vollzug dieses Gesetzes in Bremen bestehen,

habe ich auch gegenüber dem Senator für Inneres und Sport kritisch zu diesem Gesetzentwurf geäußert. Ich hoffe, daß der Regierungsentwurf die Mängel des Referententextes beseitigt und aus Datenschutzsicht befriedigende Ergebnisse erzielt werden.

5.5.2 Wohnungssstatistik


5.5.3 Bewährungshilfe, statistik/Strafverfolgungsstatistik


In Bremen wird die Bewährungshilfe, statistik lediglich aufgrund einer allgemeinen Verfügung des Senators für Justiz und Verfassung durchgeführt. Sie bedarf aber einer gesetzlichen Grundlage, die die Datenerhebung bei den Justizbehörden sowie die nachfolgenden Datenübermittlungs- und aufbereitungsverfahren umfaßt regelt. § 11 Landesstatistikgesetz, der die Befugnis zur Erstellung von Geschäftszustatistiken gibt, reicht für diese regelmäßige Statistik nicht aus, da die Daten nicht im Verwaltungsvollzug und aus dem Verwaltungsdatenbestand erhoben werden.


5.6 Standesämter

5.6.1 Überholte Dienstanweisung

Die bremer standesämter (Bremer Mitte, Bremen Nord, Bremerhaven) setzen schon seit längerem DV-Technik ein bei der Erledigung ihrer Aufgaben. Alle drei Standesämter haben sich daher für das vom Verlag für Standesamtswesen Frankfurt am Main unter Mitwirkung des Bundesverbandes der deutschen Standesämter entwickelte und betreute Programmsystem AUTISTA (Automation im Standesamt) entschieden, das auch in bremer Standesämtern in der Bundesrepublik angewendet wird.


5.6.2 Fall: Namensstreit um „Sascha“ und das Briefgeheimnis


5.7 Gewerbe

5.7.1 Fall: Komplette Strafakten beim Stadamt

Vor Erteilung einer Gewerbeerlaubnis hat die Behörde — soweit es sich nicht um eine nur anmeldpflichtige Gewerbeausübung handelt — die Zuverlässigkeit des Antragstellers zu beurteilen. Als Grundlage benötigt sie dazu neben den Unterlagen über die fachliche Eignung auch ein polizeiliches Führungszeugnis, das aus dem Bundeszentralregister erteilt wird. In das Führungszeugnis sind — je nach dem Grad der Zuverlässigkeitsvoraussetzungen, die für die Ausübung des Gewerbes erforderlich sind, und nach dem Zeitablauf einer Eintragung im Register — nur die Daten aufgenommen, die noch nicht getilgt sind oder für die kein Verwertungsverbot besteht. Diese Registerdaten stammen aus den Vorgängen und Urteilen der Gerichte, Staatsanwaltschaften und in bestimmten Fällen auch von Verwaltungsbehörden.

Diese Strafakte enthielten nicht nur das Urteil, sondern auch alle Ermittlungsvorgänge mit einer Vielzahl von Angaben, die dem Bundeszentralregister gar nicht mitzuteilen sind bzw. in das Führungszeugnis gerade nicht aufgenommen worden waren, weil das Verwertungsverbot nach § 52 Bundeszentralregistergesetz (BZRG) bei seiner Ausfertigung beachtet worden war. Durch die Mitteilung des Polizeipräsidiums an das Stadtmte und die Weitergabe der kompletten Akten durch die Staatsanwaltschaft wurde das gesetzliche Verwertungsverbot unterlaufen. Der Bürger, der seine berufliche und private Lebensplanung sowie persönliche Rehabilitation darauf abhält, daß die Daten über seine Verurteilung nach einer bestimmten Frist getilgt sind oder zumindest einem besonderen Verwaltungsverbot unterliegen, wird von seiner Vergangenheit eingeholt.


Anderes gilt nur für Daten über noch nicht gerichtlich abgeschlossene, also noch von der Polizei oder der Staatsanwaltschaft bearbeitete Vorgänge. Sie können in die Zuverlässigkeitsabwägung für eine Gewerbeerlaubnis einbezogen werden. Nach der Verurteilung gelten dagegen all die Regelungen des BZRG.


6. Justiz

6.1 Aufbewahrungsbestimmungen für Schriftgut der Gerichte, der Staatsanwaltschaften und der Justizvollzugsbehörden


Unabhängig von der Frage der Normqualität ist jedoch zu überprüfen, ob die genannten Aufbewahrungsbestimmungen tatsächlich angemessene Regelungen beinhalten, die als Grundlage der Speicherdauer entsprechender Informationen
auch in automatisierten Systemen dienen können und die dem informationellen Selbstbestimmungsrecht ausreichend Rechnung tragen. Der Gesichtspunkt der Erforderlichkeit ist auch für die Dauer der Speicherung und damit verbunden die potentielle Nutzbarkeit der Daten und Akten zu Lasten der Betroffenen zu beachten.

Ich habe daher beim Senator für Justiz und Verfassung angeregt, die Aufbewahrungsbestimmungen der Justiz für das verwaltete Schriftgut im Lichte des Rechts auf informationelle Selbstbestimmung kritisch zu überprüfen und zu überarbeiten, um in geeigneten Fällen eine Verkürzung der Aufbewahrungsduer herbeizuführen. Er hat mir daraufhin erklärt, die Landesjustizverwaltung Nordrhein-Westfalen habe die Federführung für die Überarbeitung der bundeseinheitlichen Aufbewahrungsbestimmungen übernommen; über die Ergebnisse wolle er mich unterrichten.


6.2 Automation bei der Strafverfolgung: Das SIJUS-Verfahren


SIJUS-Straf soll dazu dienen, alle für die Staatsanwaltschaft anfallenden Verfahrensdaten in einem Datenbank-System bereitzuhalten und zur weiteren Verarbei tung zur Verfügung zu stellen. Es sollen insbesondere folgende Anforderungen erfüllt werden:

- die Aktenverwaltung durch die Geschäftsstelle,
- die Textverarbeitung bei gleichzeitiger Nutzung der in der Datenbank vorhandenen Daten,
- die Übernahme und Verarbeitung der Daten aus dem bremischen Polizei Informationssystem ISA,
- der Datenaustausch mit anderen Dienststellen, z. B. Bundeszentralregister, Justizvollzugsanstalten, Einwohnermeldeämter,
- die Einbeziehung der Dezernenten und Rechtspfleger in die Technik-Lösung.


Bestandteil des mir vorgelegten ADV-Antrages war eine Dienstanweisung, die den Einsatz von SIJUS-Straf regelt. Diese Anweisung enthält den Ansatz eines Datenschutzkonzeptes, das aber noch wesentliche Punkte offen läßt. Ich habe daher gefordert, daß die konkreten Einsatzgebiete von SIJUS-Straf festlegen, die Rechtsgrundlagen für die einzelnen Verarbeitungsschritte darzulegen und Maßnahmen zur Sicherstellung einer effizienten Datensicherung zu treffen sind. Im einzelnen sind u. a. folgende Anforderungen einzuhalten:

In den dargestellten Anforderungskatalog des Senators für Justiz und Verfassung für die Anwendung von SIJUS-Strafw. wird u. a. von einem Datenaustausch mit anderen Dienststellen ausgegangen, ohne den Umfang und die Rechtsgrundlagen hierfür anzuführen. Ich habe daher gefordert, die angesprochenen Datenverbindungen zu konzentrifizieren und darzulegen, aufgrund welcher Rechtsgrundlagen diese erfolgen sollen. So ist z. B. festzulegen, in welcher Form welche Daten an das Bundeszentralregister sowie an das Verkehrs- zentralregister übermittelt werden sollen.

Weitere Defizite des mir vorgestellten Datenschutzkonzeptes betraten u. a. den Aufstellungsort und die Zugangsbeschaffung zum Zentralrechner, die Aufbewahrung der Sicherungskopien, den Einsatz der Drucker, die Protokollierung, die Verwaltung von aufgabenspezifischen Zugriffsrechten (z. B. differenziert nach einzelnen Geschäftsstellen), die Aufgaben des Systemverwalters, die automatische Umsetzung von Lösch- und Sperrfristen sowie die Wartung.


7. Bildung und Wissenschaft

7.1 Zweckbindung für Daten der Studenten und des Lehrpersonals — neue Rechtsverordnung


Der bremische Gesetzgeber hat im Jahre 1988 das Bremische Hochschulgesetz geändert und einen neuen § 44 a „Datenverarbeitung“ in das Gesetz eingefügt. Diese neue Bestimmung ermächtigt den Senator für Bildung und Wissenschaft, durch Rechtsverordnung die von Studienbewerbern, Studenten und Prüfungs-


### 7.2 Vermischung von Landes- und Kommunalaufgaben beim PC-Einsatz


Bei den Vollzugaufgaben, die das Referat über die Geschäftsverteilung hinaus für die anderen Referate wahrnimmt, wird die Trennung der Kommunalaufgaben (Stadtgemeinde Bremen) von den Aufgaben des Landes Bremen außer acht gelassen, obwohl das Schulverwaltungsgesetz eine solche Trennung vornimmt und das Datenschutzrecht vom Funktionstrennungsprinzip ausgeht.


bremischen Verwaltung zu überdenken. Der Senator für Bildung und Wissenschaft hat inzwischen erklärt, daß er seinen Antrag überarbeiten und neu stellen will.

7.3 Fall: Ungefragt im Philologen-Jahrbuch


Der in Bremerhaven für die Zusammenstellung und Übermittlung der Lehrerdaten verantwortliche Philologe teilte mir dazu mit, daß vor der Weitergabe der Lehrerdaten an die Landesverbandsstelle in den Bremerhaven Schulen ein Aushang erfolgt sei, mit dem auf die bevorstehende Herausgabe des Jahrbuchs und darauf, daß der Veröffentlichung der Daten von dem jeweils Betroffenen widersprochen werden kann, hingewiesen wurde. Der sich beklagende Lehrer hatte sich somit über die Weitergabe seiner Daten informieren und ihr, wenn er dies gewollt hätte, widersprechen können.


8. Arbeit und Frauen

8.1 Krankenhausentlassungsberichte an das Versorgungsamt


Unabhängig voneinander machten mich ein niedergelassener Arzt und der Medizinische Dienst der Krankenversicherung im Lande Bremen darauf aufmerksam, daß das Versorgungsamt vor ihnen Unterlagen über das erforderliche Maß hinaus angefordert habe. Von dem Arzt hatte das Amt Entlassungsberichte angefordert, die Krankenhäuser ihm zum Zwecke der Nachbehandlung seiner Patienten übermittelt hätten und die Daten enthielten, die das Amt für seine Entscheidung nicht benötigte. Im anderen Fall wurde berichtet, das Amt fordere regelmäßig alle Unterlagen des Medizinischen Dienstes über einen Versicherten an ohne jede inhaltliche Spezifizierung oder zeitliche Begrenzung. Man sei schon dazu herangegangen, nur die Unterlagen der letzten zwei Jahre zu übersenden; dies habe das Amt nicht moniert.

Auch mein Hinweis, das Amt sei lediglich befugt, die für seine Entscheidung erheblichen Unterlagen anzufordern, und dies auch nur, soviert der Antragsteller sich damit einverstanden erklärt habe, erwies die Versorgungsverwaltung, daran hatte man sich seit jeber. Diesen vor einigen Jahren mit meiner Dienst-
stelle abgestimmten Vordrucken zu entnehmen, die man noch heute verwendet. Im übrigen strebe der Antragsteller regelmäßig eine umfassende Beurteilung seiner Behinderung an, weil er das Ziel verfolge, daß seine Behinderung als möglichst schwer anerkannt werde. Immerhin hat die Versorgungsverwaltung auf meine Vorschläge hin den Vordruck für die Einverständniserklärung nachgebessert:

- Voraussetzung dafür, daß Auskünfte eingeholt und Unterlagen angefordert werden, ist nunmehr sowohl, daß die jeweilige Stelle (Krankenhaus, Arzt usw.) im Antrag benannt ist, als auch, daß die Auskünfte bzw. Unterlagen für die Entscheidung erheblich sind.

- Der Vordruck eröffnet nunmehr dem Antragsteller die Möglichkeit zu vermerken, ob und inwieweit er sein Einverständnis einschränken will.

Dagegen habe ich meinen ursprünglichen Vorschlag, das Amt solle in jedem Einzelfall konkrete Fragen formulieren und um deren Beantwortung bitten, nicht weiter verfolgt, nachdem ich auf eine Umfrage hin erfahren hatte, daß in anderen Bundesländern entsprechende Verfahrensregelungen daran gescheitert seien, daß viele der angesprochenen Ärzte mangels eines als angemessen angesehenen Entgelts ihre Mitarbeit verweigert hätten.


9. Jugend und Soziales

9.1. Beratungsgeheimnis und wirtschaftliche Hilfen (s. a. 14. Jahresbericht, Ziffer 2.5.2)

- Amt für Soziale Dienste


— Jugendamt Bremerhaven


— Eingliederungshilfe für Erwachsene


9.2 Auskunftspflicht aufgrund Unterhaltspflicht

Personen, die einen Sozialhilfeempfänger gegenüber zur Leistung von Unterhalt verpflichtet sind, müssen nach § 116 Bundessozialhilfegesetz (BSHG) dem Träger der Sozialhilfe Auskunft über ihre Einkommens- und Vermögensverhältnisse


9.3 Seniorenzentraldatei in Bremerhaven


Das Sozialamt verfolgte zunächst allerdings seine Pläne weiter, die Seniorenkartei künftig auf automatisierter Basis zu betreiben. In diesem Zusammenhang sollte man dem Senator für Inneres und Sport vorschlagen, die Meldedatenübermittlungsverordnung um eine entsprechende Übermittlungsbefugnis der Meldebehörde zu ergänzen. In der Datei sollten alle Bremerhavener Bürger, die älter als 60 Jahre sind, gespeichert werden, ausgenommen diejenigen, die dem ausdrücklich widersprochen hatten. Die Daten sollten genutzt werden, um die Betroffenen über Angebote der Seniorenhilfe zu informieren, die Teilnahme an Ausflugs- und Erholungsfahrten sowie an Gruppenprogrammen zu verwalten und zu überprüfen, ob der Betroffene einen Zuschuß für eine Erholungsreise erhalten kann, was alle drei Jahre der Fall ist. Schließlich sollten mit Hilfe der Datei Geschlechtsunterschiede dafür festgestellt werden können, ob sich der einzelne in einer Notlage befindet und ihn deshalb der Besuchsdienst der Seniorenbetreuung aufsuchen und beraten solle. Derartige Geschlechtsunterschiede sollten z. B. sein, daß ein Senior im Alter von 75 Jahren noch an keinem Angebot der Seniorenbetreuung teilgenommen habe, daß er zwar bislang regelmäßig Angebote wahrgenommen habe, nun aber nicht mehr, oder auch der Tod des Ehepartners.

Gegen das Vorhaben, die Daten der älteren Bürger Bremerhavens ohne ihre Einwilligung gesondert zu speichern und zu den vorgenannten Zwecken zu nutzen, bestanden grundsätzliche datenschutzrechtliche Bedenken. Es wäre ein Nebenregister zum Melderegister eingerichtet worden, das weder durch das Meldegesetz noch durch das Bundessozialhilfegesetz legitimiert gewesen wäre. Auch § 75 BSFG, der die Altenhilfe regelt, legt lediglich die Aufgaben des Sozialhilfeträgers fest, räumt ihm aber nicht die Befugnis zu einer derart umfassenden Datenspeicherung ein. Überdies ist der Schluß daraus, daß ein älterer Bürger die Angebote der Seniorenbetreuung nicht oder nicht mehr wahrnimmt, darauf, daß er sich in einer Notsituation befinden könne und deshalb geboten sei, daß ihm Mitarbeiter des Sozialamtes aufsuchen, in Frage zu stellen. Der rechtlich unproblematische Weg, uniformierte Senioren anzusprechen und denen unter ihnen zu helfen, die in Not geraten sind, geht nicht über ausnahmslose Registrierung aller älteren Mitbürger, sondern über zielgruppenspezifische Öffentlichkeitsarbeit und ein Netz von Nachbarschaftshilfen.
Jedoch bestehen keine Bedenken dagegen, daß die Meldebehörde aus Anlaß von Stadtteilfesten die Daten der im Einzugsbereich wohnenden älteren Mitbürger übermittelt, damit sie eingeladen werden können – wohlgerenkt nicht, damit ihre Daten auf Dauer gespeichert werden. Zulässig wäre nach dem Sozialgesetzbuch (SGB) auch eine Speicherung nur zum Zwecke der Entscheidung über einen Antrag und zur Abwicklung der daraufhin gewährten Sozialleistung, etwa einer Erholungsfahrt. Ebensowenig bestehen Bedenken dagegen, daß das Sozialamt die Daten älterer Bürger insoweit speichert, als sie sich ausdrücklich damit einverstanden erklärt haben.

Inzwischen hat der Magistrat meine Bedenken und Hinweise aufgenommen und umgesetzt. Nunmehr sollen nur noch die Daten derjenigen älteren Bürger auf Dauer gespeichert werden, die sich damit ausdrücklich einverstanden erklärt haben. Das Sozialamt hat in Abstimmung mit mir einen Vordruck für die Einverständniserklärung entwickelt. Der Betroffene kann sich darin auch darüber informieren, worin er einwilligt. d. h. es wird im einzelnen aufgeführt, zu welchen Zwecken das Sozialamt die Daten nutzen will. Damit ist ein Weg gefunden worden, der es einerseits dem Sozialamt gestattet, die älteren Bürger Bremerhavens zu erreichen und ihnen entsprechend seinem gesetzlichen Auftrag „die Möglichkeit zu erhalten, am Leben der Gemeinschaft teilzunehmen“. Andererseits aber wird respektiert, daß es auch ältere Menschen gibt, die an den Angeboten des Sozialamtes keinen Bedarf und kein Interesse haben.

10. Gesundheit

10.1 Kontrollergebnisse in kommunalen Krankenhäusern

10.1.1 Konsequenzen des Krankenhausdatenschutzgesetzes (KHDSG)

Der Krankenhauspatient befindet sich in einer für ihn oft existentiell bedrohlichen oder als bedrohlich empfundenen Situation. In ihr erwartet er Hilfe von einzelnen Ärzten und Pflegekräften, sieht sich aber zugleich einem für ihn unübersehbaren Apparat gegenüber. Er hat weder Einfluß noch Überblick, was im einzelnen mit seinen Daten. z. B. medizinischen Befunden, Röntgenaufnahmen, Blutproben, geschieht. Die allgemeinen Regelungen des Bremischen Datenschutzgesetzes (BrDSG) zum Datenschutz bzw. des Straf- und Berufsrechts zur ärztlichen Schweigepflicht werden den besonderen Anforderungen an den Schutz der Patientendaten im Krankenhaus nicht gerecht: Die einen sind auf die Datenverarbeitung in der Verwaltung, die anderen auf den niedergelassenen Arzt zugeschnitten.


Dementsprechend verpflichtet § 7 BrDSG, der nach § 1 Abs. 4 KHDSG auch für Krankenhäuser gilt, die Krankenhausleitungen dazu, ihr automatisierter Dateien bzw. für Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, in einer Dateibeschreibung bzw. in einem Geräteverzeichnis bestimmte datenschutzrechtlich wichtige Merkmale festzulegen. Diese Festlegungen dienen zugleich

– dazu, der Leitung zu ermöglichen, ihrer Verantwortung gerecht zu werden,
– als Unterlage für die Übersichten zur Datenverarbeitung, die die Leitung nach § 9 KHDSG i. V. m. § 37 Bundesdatenschutzgesetz (BDSG) dem von ihr zu befei-
lenden betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen hat, und damit als Grundlage für dessen Aufgabenerfüllung,

- als Unterlage für die Anmeldung der Dateien zum von mir geführten Dateienregister (§ 28 BrDSG),

- als Grundlage für meine Überwachung der Datenverarbeitung im Krankenhaus; Dateibelegungen, Geräteverzeichnisse und Übersichten sind mir auf Verlangen vorzulegen (§ 27 BrDSG),

- als Grundlage für die kommunale Rechtsaufsicht über die Krankenhäuser nach § 9 der Krankenhausbetriebsgesetze der Stadtgemeinden Bremen und Bremerhaven.

10.1.2 Prüfprogramm

Unabhängig von durch Patientenbeschwerden oder andere Hinweise veranlaßten punktuellen Überprüfungen in einzelnen Krankenhäusern habe ich begonnen, die fünf kommunalen Krankenhäuser im Lande Bremen systematisch auf die Einhaltung des KHDSG und des BrDSG hin zu überprüfen. Dabei nehme ich zum Ausgangspunkt die dargestellten Dokumentationspflichten und die Aufgabenerfüllung durch die betrieblichen Datenschutzbeauftragten. Damit möchte ich zunächst erreichen, daß die Krankenhäuser ihre gesetzlichen Dokumentationspflichten so erfüllen, daß die Verantwortlichen, vor allem die Leitung, die EDV-Leiter und die Datenschutzbeauftragten, ihrer jeweiligen Verantwortung gerecht werden können. Daneben möchte ich die Datenschutzbeauftragten in ihrer Stellung nach § 9 KHDSG i. V. m. § 36 BDSG und bei der Wahrnehmung ihrer Aufgaben nach § 9 KHDSG i. V. m. § 37 BDSG unterstützen. Nach meinen bisherigen Erfahrungen besteht Anlaß, darauf hinzuweisen, daß Datenschutzbeauftragte

- nicht personengleich mit dem EDV-Leiter sein dürfen.

- gegenüber dem EDV-Leiter eine selbständige und unabhängige Stellung haben müssen.

- über genügend Arbeitskapazität für ihre Aufgaben verfügen müssen.

Deshalb bewerte ich es positiv, daß das ZKH Bremen-Ost jetzt als erstes Krankenhaus einen hauptamtlichen Datenschutzbeauftragten — wenn auch nur mit halber Stundenzahl — bestellt hat. Ich bin gern bereit, die anderen Krankenhäuser dabei zu unterstützen, die Krankenkassen davon zu überzeugen, daß im Rahmen des Pflegesatzes auch die Kosten für einen effektiven Patientendatenschutz zu berücksichtigen sind.


10.1.3 EDV im Zentralkrankenhaus Reinkenheide


Datensicherheit in der zentralen EDV:

- Sicherung des EDV-Raumes, so daß nur Wartungs- und Bedienungspersonal der Zugang möglich ist;

- Kontrolle der Operatoraktivitäten durch Protokollierung der Systemaktivitäten und Einführung des „Vier-Augen-Prinzips“;

- Einführung der Funktionstrennung zwischen Durchführung und Kontrolle;
— Verbesserung der Passwortsteuerung durch
  ● Ausschluß einfacher Kombinationen
  ● Festlegung einer begrenzten Gültigkeitsdauer
  ● verschlüsselte Speicherung, d. h. Sicherstellung, daß nur der / die Passwort-
    inhaber / in Kenntnis haben kann.

Datensicherheit bei den Terminals:
— Verbesserung der Passwortsteuerung
— Protokollierung des Zugriffs auf Patientendaten
— Einschränkung des Zugriffs durch einzelne Mitarbeiter / innen auf die nur für
die jeweilige Aufgabenverfüllung erforderlichen Patientendaten.

Da einige der von mir geforderten Maßnahmen auf der vorhandenen EDV-Anlage
nicht zu realisieren sind, gehe ich davon aus, daß sie zumindest bei der geplanten
Modernisierung des EDV-Bereiches berücksichtigt werden. Datenschutzsoftware
auf den im Krankenhaus vorhandenen Einzelplatz-PCs wurde innerhalb des
Prüfungsterminos bereits installiert.

Datensicherheit bei Fernwartung:
Die beruflichen Schweigepflichten der Ärzte / Ärztinnen und ihrer Mitarbei-
ter / innen gelten auch im Krankenhaus. Schon im Hinblick darauf ist es unzuläs-
sig, wenn ein Krankenhaus einer Fernwartungsfirma den Zugriff auf personen-
bezogene Daten seiner Patienten Patienten eröffnet (zur Problematik der
Fernwartung allgemein s. o. Ziffer 2.2.2.1).

Eine Stellungnahme des ZKH Krankenheide zu meinen Anforderungen habe ich
noch nicht erhalten.

10.1.4 Nachlässigkeit bei externer Wartung (ZKH St.-Jürgen-Straße)

Allerdings gibt es außer der Fernwartung noch andere Wartungsmethoden, die
Gefahr für den Patientendatenschutz bedeuten. Dies erfuhr ich, als ich einen
entsprechenden Hinweis hinmach davon überzeugen wollte, ob bei der automati-
sierten Speicherung von medizinischen Patientendaten auf einem privaten
PC eines Chefärztes des ZKH St.-Jürgen-Str. die Datenschutzbestimmungen
beachtet wurden. Das Krankenhaus teilte mir mit, daß kurz vor Eingang meines
Ankündigungsblattes die Festplatte auf den Patientendaten, bei einer War-
tung neu partitioniert und formatiert und dabei versehentlich alle Daten auf der
Festplatte gelöscht worden seien. Zuvor habe der Chefarzt den PC persönlich —
wohlgeräumt mit Festplatte und darauf gespeicherten Patientendaten — zur War-
tungsfirma gebracht.

Ich habe darauf aufmerksam gemacht, daß vor der Wartung die Patientendaten
hätten auf Diskette übertragen, die personenbezogenen Merkmale auf der Fest-
platte hätten physikalisch gelöscht und die Diskette im ZKH hätte desinfiziert
aufbewahrt werden müssen. Ich habe um eine entsprechende Unterrichtung der Mit-
arbeiter / innen gebeten. Das ZKH hat sich hierzu und zu meinen sonstigen
Vorschlägen für eine künftige datenschutzgerechte Speicherung der Patienten-
daten noch nicht geäußert.

10.2 Eckpunkte für ein Gesetz über den öffentlichen Gesundheitsdienst
(s. a. 14. Jahresbericht, Ziffer 2.6.6)

Wiederholt habe ich in meinen Jahresberichten auf die Notwendigkeit hingewie-
nen, Aufgaben und Belastungen der Gesundheitsämter in einem zeitgemäßen
Gesetz zu regeln und damit die bisherigen Rechtsgrundlagen aus dem Jahre 1934 /b
zu ersetzen. Inhaltliche Anforderungen an die Regelung der Belastungen zur Daten-
verarbeitung hatte ich bereits im 12. Bericht (Ziffer 2.7.1.2) formuliert. Kurzlich
hat der Senat für Gesundheit, Jugend und Soziales Eckpunkte einer gesetzlichen
Regelung in der Deputation für Gesundheit und im Gesundheitsausschuß der Bre-
merhavenener Stadtverordnetenversammlung vorgelegt, die auch Aussagen zum
Datenschutz enthalten.

Ich entnehme diesen, daß Einigkeit darin besteht, daß die Garantie eines besonde-
ren Vertrauensschutzes für die Patienten, die die Beratungsangebote der Gesund-
heitsämter wahrnehmen, und eine enge Zweckbindung bei der Nutzung und
Übermittlung der von den Ärzten erhobenen Daten bzw. der von deren Ärzten und Psychologen erstellten Gutachten und Diagnosen eine wichtige Voraussetzung dafür ist, daß ein öffentlicher Gesundheitsdienst, der sich in erster Linie als Bürgerservice definiert, seine Aufgaben sinnvoll wahrnehmen kann.

In diesem Sinne verstehe ich auch die Verfahrensregelungen, die ich in konkreten Punkten mit dem Gesundheitsamt Bremerhaven und mit dem Hauptgesundheitsamt Bremen vereinbart habe (z. B. 13. Jahresbericht, Ziffer 2.6.2). Allerdings habe ich das Ressort kürzlich erneut darauf hinweisen müssen, daß die Kartelle und die Registraturen des Amtsärztlichen Dienstes im Hauptgesundheitsamt Bremen datenschutzrechtlichen Anforderungen nicht gerecht werden:

- Ältere Akten enthalten psychosoziale Diagnosen und andere Bestandteile, die nichts mit den Aufgaben des Amtsärztlichen Dienstes zu tun haben, vielmehr ausgesondert und in die Obhut des Sozialpsychiatrischen Dienstes oder anderer Beratungsstellen gegeben werden müssen.

- Es werden Uraltvorgänge aufbewahrt, die längst dem Staatsarchiv hätten angeboten oder vernichtet werden müssen. Jüngst wurde in diesem Zusammenhang die Aktenordnung des Senats von 1958 herangezogen, deren Anpassung an die Löschungsbestimmungen in § 20 Bremisches Datenschutz (BDSG) überfällig ist.

- Die vom Hauptgesundheitsamt selbst vorgenommene Regelung der Neugliederung und Nutzungsbeschränkung seiner eigenen Vorgänge ist noch nicht umgesetzt worden.

Das Hauptgesundheitsamt führt für die Verzögerungen fehlende Personal- und Sachmittel an und verweist auf die ins Auge gefaßte Automatisierung seiner Datenverarbeitung. Auf mein Betreiben hat es jetzt ein Konzept hierfür vorgelegt. Gegenüber der senatorischen Dienststelle drängte ich darauf, daß die Planung vorangetrieben wird. Unabhängig davon hat das Hauptgesundheitsamt zugesagt, schon jetzt technisch möglich und finanziell neutral datenschutzrechtlich unabdingbare Änderungen vorzunehmen:

- Wenn aus aktuellem Anlaß eine Kartei der ärztlichen Kartei gezogen wird, auf der noch unzulässigerweise die Inanspruchnahme eines Beratungsdienstes vermerkt ist, ist sie durch eine neue Kartei ohne Quervermerk zu ersetzen (so praktiziert im Gesundheitsamt Bremerhaven).

- Zugleich ist die dazugehörige Aktie dem entsprechenden Beratungsdienst zuzuleiten, damit dieser die Vorgänge entnimmt, die in seine Obhut gehören.

Außerdem gehe ich davon aus, daß im Laufe des Geschäftsganges angefallene lösungspflichtige Vorgänge ständig ausgesondert, dem Staatsarchiv angeboten bzw. gedrückt werden.

10.3 Patientendaten in der gesetzlichen Krankenversicherung

10.3.1 Umgebung des unbequemen Gesundheitsreformgesetzes 1989


Ein anderes der im 14. Jahresbericht dargestellten Probleme — Kontrolle des Verbrauchs medizinischer Hilfsmittel in Altenpflegeeinrichtungen mittels Erhebung der Verbrauchsdaten der Pflegebedürftigen — hat sich mit meiner Intervention dadurch erledigt, daß sich die beteiligten Stellen auf eine pauschalierte Abrechnung geeinigt haben. Dagegen ist leider noch nicht erkennbar, daß die Kranken-

— Erstes Beispiel: Der Abrechnungsschein für den ärztlichen Notfalldienst


— Zweites Beispiel: Meldung und Speicherung der Daten von Methadonsubstituierten Drogenabhängigen


Diese Datenübermittlungen finden im SGB V keine Grundlage. Meiner entsprechenden Kritik ist entgegengehalten worden, die Ärzte seien nach § 295 SGB V
ohnnehin verpflichtet, die Krankenscheine ihrer Patienten — also auch der Methadon-Substituierten — bei der Kassenärztlichen Vereinigung einzureichen. und diese leite die Unterlagen später an die jeweilige Krankenkasse weiter. Die NUB-Richtlinie verlangt also nur eine zeitliche Vorverlegung der Datenübermittlung. Dabei wird aber verkannt, daß, anders als es das Gesetz vorsieht,

— zusätzliche detaillierte Daten über psychosoziale Betreuung übermittelt werden sollen, in bestimmten als strittig gekennzeichneten Fällen auch der Therapieplan,

— die Kassenärztliche Vereinigung die ihr eingereichten Meldungen auf Dauer speichert (und auch auswertet), wohingegen sie die Krankenscheine mit ihren Abrechnungsunterlagen an die Kassen weiterleitet, also von den anderen Versicherten auf Dauer keine personenbezogenen Unterlagen zurückbehält,

— die Kassen ohne die Meldung der substituierenden Ärzte die Daten von Methadonsubstituierten Versicherten lediglich zusammen mit allen anderen eingereichten Krankenscheinen, also praktisch nicht getrennt auswertbar, erhielten.

Dies alles ist um so bedenklicher, als weder Kassenärztliche Vereinigung noch Kassen in Bremen bisher verbindlich erklärt haben, wozu sie die Daten der Methadon-Substituierten verwenden und wie sie die Einhaltung der von ihnen selbst definierten Zweckbestimmung gewährleisten wollen. Vielmehr berufen sie sich lediglich auf die NUB-Richtlinie. Diese aber — und hier sehe ich eine Parallele zum vorgenannten Beispiel — vermag über das gesetzliche Maß hinaus eine Verarbeitung von Versichertendaten durch Kassenärztliche Vereinigung und Kassen nicht zu rechtfertigen, zumal in § 135 SGB V, der als Rechtsgrundlage für die NUB-Richtlinie herangezogen wird, zwar von anderen Regelungsinhalten derartiger Richtlinien, nicht aber von der Einräumung von Befugnissen zur Datenverarbeitung die Rede ist.


10.3.2 Auswirkungen des Gesundheitsstrukturgesetzes (GSG ’93)

Das GSG 93 ist in seinen Neuregelungen zur Datenverarbeitung im Gesundheitswesen geprägt von dem Bestreben, die Automatisierung der Datenverarbeitung zu forciern. Dies spiegelt in der Androhung finanzieller Sanktionen, falls die Leistungserbringer nicht bis zum 01. 01. 1995 die Abrechnungsdaten automationsgerecht übermitteln, § 303 Abs. 3 SGB V. Der damit verbundenen und auch von mir während des Gesetzgebungsverfahrens beschworenen Gefahr, daß die Automatisierung der Verarbeitung von Versichertendaten es den Kassen ermöglicht werde, über das bisher mögliche und rechtlich legitimierte Maß hinaus Abrechnungsdaten versichertenspezifische zu verknüpfen und — etwa zum Zwecke der Beratung, Überwachung oder Risikominimierung — in Gestalt von Leistungs- und Gesundheitsprofilen der einzelnen Versicherten auszuwerten, hat das GSG 93 in seiner in Kraft getretenen Fassung Rechnung getragen. So ist im letztmöglichen Augenblick die Regelung des § 305 SGB V über den Anspruch der Versicherten an die Krankenkassen auf Auskunft über in Anspruch genommene Leistungen und deren Kosten mit dem erklärten Ziel verändert worden, eine auf die
einzelnen Versicherten bezogene Speicherung und Auswertung von medizinischen Daten auszuschließen. Dem selben Ziel dient die Klarstellung in § 295 Abs. 2 SGB V, wonach künftig die Kassenärztlichen Vereinigungen den Kassen die Abrechnungsdaten zwar fallbezogen, aber ausdrücklich nicht versichertengebogen übermitteln sollen.


10.3.3 Abrechnung mit Chipkarten


10.4 Verkauf von Arztpreisen: Einwilligung der Patienten

In der langjährigen Diskussion darüber, ob Ärzte ihre Patientenkarte zusammen mit ihrer Praxis verkaufen dürfen, ohne die einzelnen Patienten zuvor um der Ein-
verstanden gebeten zu haben, hat der Bundesgerichtshof (NJW 92, 737) jetzt entschieden, daß ein Arzt, der zuvor nicht die Einwilligung der Patienten eingeholt habe, damit das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche Schweigepflicht verletze.


— sichergestellt sein muß, daß der die Praxis übernehmende Arzt ohne Einwilligung des jeweiligen Patienten keinen Zugriff auf dessen Daten haben darf, d. h., daß ein vertragliches Verbot nicht ausreicht,

— die Einwilligung nur dann wirksam ist, wenn sie sich konkreter auf den Verkauf an einen namentlich genannten Käufer bezieht, d. h., daß ein vorsorglich für den Fall einer späteren Veräußerung an einen nicht genannten Arzt unterzeichnetes Formular nicht ausreicht.

Anders lautende Regelungen oder Vordrucke würden den Verdacht erregen, als wolle man mit ihnen der höchstrichterlichen Entscheidung zwar formell Genüge tun, sie in Wirklichkeit aber zu unterlaufen versuchen.

11. Umweltschutz und Stadtentwicklung

11.1 Einsichtsrecht in Umweltakten: Entwurf eines Umweltinformationsgesetzes


Der Gesetzentwurf regelt das Informationszugangsrecht nicht nur gegenüber den Behörden des Bundes, sondern auch gegenüber denen der Länder, Gemeinden und Gemeindeverbände. Dem Bund obliegt jedoch lediglich, materiellrechtliche Regelungen im Umweltrecht zu schaffen, soweit seine Kompetenz gegeben ist. Er verfügt beim Informationszugangsrecht in den Ländern und Kommunen weder
über eine ausschließliche noch über eine konkurrierende Regelungskompetenz, so daß es den Ländern obliegt, im Rahmen ihrer Gesetzgebungskompetenz nach Art. 70 Grundgesetz (GG) den Verpflichtungen der EG-Richtlinie nachzukommen. Der bremsische Gesetzgeber ist also gehalten, eigenständige Regelungen zu schaffen.


Die den Mitgliedstaaten nach der EG-Richtlinie überlassene Entscheidungsbefugnis, ob und inwieweit der Informationszugang unter bestimmten Voraussetzungen ausgeschlossen bzw. beschränkt werden kann, legt der Referentenentwurf äußerst extensiv aus.


Auch diese Regelung halte ich unter Berücksichtigung des durch die EG-Richtlinie den Mitgliedstaaten überlassenen Gestaltungsspielraums für zu restriktiv. Der Katalog der personenbezogenen Daten, die keine schutzwürdigen Belange der Verursacher tangieren, kann ohne weiteres ausgeweitet werden. Schutzwürdige Belange des Betroffenen stehen einer Offenbarung insbesondere dann nicht entgegen, wenn sich aus einer Umweltakte die Tatsache ergibt, daß der Betroffene als Gutachter, Sachverständiger oder in vergleichbarer Weise eine Stellungnahme abgegeben hat.

Die vorgesehene Ablehnung der Offenbarung von Unterlagen, die von einem Dritten übermittelt worden sind, der dazu nicht verpflichtet war, nutzt den Gestaltungsspielraum der EG-Richtlinie ebenfalls nicht aus. Um dem Zugangsrecht Rechnung zu tragen, wäre es z. B. möglich, Informationen, die ein Dritter an die Behörde weitergegeben hat, ohne dessen personenbezogene Daten zu offenbaren.

Nach dem Referentenentwurf können für alle Amtshandlungen nach diesen Gesetze Gebühren und Auslagen erhoben werden. Dagegen erlaubt die EG-Richtlinie nur, angemessene Gebühren ausschließlich für die Gewährung von Informationen zu erheben. Ich halte eine entsprechende Änderung des Entwurfs für erfor-
derlich und rege an, auch bei der Gewährung des Informationszugangs auf die Erhebung von Gebühren und Auslagen zu verzichten.


Des weiteren halte ich es zur Wahrnehmung des Informationszugangsgesetzes für geboten, die Öffentlichkeit regelmäßig auch darüber zu unterrichten, bei welchen Behörden Informationen über die Umwelt bereitliegen.

Insgesamt bleibt festzustellen, daß der Gesetzentwurf viel zu spät erarbeitet worden ist, zumal der Fristablauf spätestens Mitte 1990 bekannt war. Außerdem ist der Entwurf in wesentlichen Punkten viel zu restriktiv und wird den Intenten der EG-Richtlinie nicht gerecht.


Der Senator für Umweltschutz und Stadtentwicklung ist nicht bereit, den bereits herausgegebenen Erlaß zu ändern, weil damit zu rechnen sei, daß das neue Umweltinformationsgesetz ohnehin im Laufe des Jahres in Kraft treten wird. Im übrigen habe ich seinen Erlaß den anderen Ressorts zugesandt und anheimgestellt, entsprechende Regelungen zu treffen. Im Erlaß selbst sind auch die anderen senatorischen Behörden angesprochen.

Der Senator muß prüfen, welche gesetzlichen Vorschriften im Bereich der Landeskompetenz zu erlassen sind, wie dies in Einzelbereichen, z. B. für die Einsicht in das Wasserbuch nach dem Bremer Wassergesetz, bereits geschehen ist. Ich werde die Praxis genau verfolgen und darauf achten, daß dieses neue Instrument der Bürgerinformation und -partizipation nicht durch bürokratische Hemmnisse entwertet wird.

11.2 Die „codierte Mülltonne“


Zu diesem Zweck hat bereits im vergangenen Jahr ein Versuch in Bremen-Horn stattgefunden. Ich habe anlässlich dieser Probephase gegenüber dem Senator für Umweltschutz und Stadtentwicklung dargelegt, daß bei einer späteren haushalts-
bezogenen Speicherung dieser Daten der in § 19 Abs. 3 des Ortsgesetzes über die Abfallbeisetzigung in der Stadtgemeinde Bremen abschließende Datenkatalog entsprechend ergänzt werden muß. In den Datenkatalog muß aufgenommen werden, an welchem Tage und — soweit dies erforderlich ist — zu welcher Uhrzeit die Entleerung vorgenommen worden ist.


11.3 Datenschutz im Naturschutzgesetz

Der Senator für Umweltschutz und Stadtentwicklung hat mir den Entwurf einer Änderung des Bremischen Naturschutzgesetzes vorgelegt. Wesentlicher Teil dieser Änderungen ist die Schaffung bereichsspezifischer Datenverarbeitungsregelungen.


Aus dieser Datenübermittlungsregelung läßt sich jedoch nicht präzise erkennen, welchen öffentlichen Stellen im Rahmen der Verfahren die genannten personenbezogenen Daten übermittelt werden dürfen. Ich halte es daher für erforderlich, die für die jeweiligen Verfahren als Adressaten in Frage kommenden öffentlichen Stellen im einzelnen zu benennen.

11.4 Einwenderdaten in Bebauungsplänen
(s. a. 13. Jahresbericht, Ziffer 2.8.4, Ergebnis)


12. Wirtschaft, Mittelstand und Technologie

12.1 Wählerverzeichnis als Mitgliederverzeichnis der Arbeitnehmerkammern
(s. a. 10. Jahresbericht, Ziffer 5.12.2)

In meinem 10. Jahresbericht habe ich auf die fehlenden rechtlichen Voraussetzungen für die Übermittlung von Arbeitnehmerdaten durch die Arbeitgeber an die mit der Durchführung der Kammerwahlen beauftragten Wahlvorstände hingewiesen. Es war zwar in der Wahlordnung eine entsprechende Regelung enthalten, allerdings fehlte dafür die gesetzliche Grundlage.


Dabei ist präzise festzulegen, welche Daten aus den Wählerverzeichnissen an die Kammern für die Mitgliederlisten übermittelt werden dürfen.
13. Finanzen

13.1 Die Landeshauptkasse als Sammelstelle für Belege

Die Landeshaushaltsordnung (LHO) regelt die Haushaltsaufstellung, den Haushaltsvollzug, die Rechnungslegung sowie die Rechnungsprüfung in der Freien Hansestadt Bremen. Da diese Regelungen z.T. generalklauselartig formuliert sind, ist der Senator für Finanzen befugt (z.T. im Benehmen mit dem Rechnungshof), Verwaltungsvorschriften zu erlassen. Die Verwaltungsvorschriften zu einigen Paragraphen sind sehr umfangreich und detailliert ausformuliert.

Im Mai 1990 hat der damalige Landesbeauftragte für den Datenschutz die Verwaltungsvorschriften zu § 70 LHO auf ihre Vereinbarkeit mit dem Bremischen Datenschutzgesetz hin untersucht und daraufhin für den Haushaltsvollzug seiner Behörde verfügt, den Kassenanordnungen keine Einzelbelege mehr beizufügen. § 70 LHO bestimmt lediglich, daß die Zahlungen von Kassen und Zahlstellen nur auf Grund schriftlicher Anordnung des zuständigen Senators oder der von ihm ermächtigten Dienststelle angenommen oder geleistet werden dürfen und daß der Senator für Finanzen Ausnahmen zulassen kann.


Ich habe den Senator für Finanzen gebeten, die Verwaltungsvorschriften in diesem Punkt zu korrigieren. Er will jedoch zunächst mit den übrigen Länderfinanzverwaltungen dieses Problem erörtern. Im übrigen hat er auf das zukünftige automatisierte Mittelbewirtschaftungsverfahren (s. u. Ziffer 13.2) verwiesen, das ohnehin auf die Beihilfe der begründenden Unterlagen verzichtet.

Ich bin der Auffassung, daß Länderabsprachen und die beabsichtigte Einführung eines neuen EDV-gestützten Haushaltsverfahrens eine Verzögerung der Problemlösung nicht rechtfertigen und die derzeitige Praxis sofort eingestellt werden sollte. Die Rechnungsprüfung wird dadurch nicht behindert. Nach der gegebenen Rechtslage sind die Behörden und Dienststellen selbst und nicht dritte, wie etwa die Landeshauptkasse, verpflichtet, auf Anforderung des Rechnungshofs die Unterlagen für ihren Verantwortungsbereich prüfungsfähig zur Einsicht vorzulegen.

13.2 Datensicherung beim neuen Haushalts- und Mittelbewirtschaftungs- system

— Paßwortorganisation


— Auswertung von Dateien

Die Daten werden auf den Orginaldateien zwar grundsätzlich verschlüsselt; diese Verschlüsselung läßt sich aber durch den Sachbearbeiter aufheben. Daher sind mit Standardprogrammen die Daten für beliebige Zwecke auswertbar. Der Senator für Finanzen schlägt die Sperrung des entsprechenden Moduls vor. Bis zum Redaktionsschluß hatte ich keine Bestätigung, daß ein entsprechender Auftrag an die Softwarefirma ergangen ist.

— Individuelle Auswertungen

Buchungen können über ein Zusatzzfeld mit frei gestaltbaren individuellen Verschlüsselungen und Indizes versehen werden. Auch dies ermöglicht unkontrollierbare individuelle Auswertungen. Auch hier will der Senator für Finanzen statt mit technischen lediglich mit organisatorischen Maßnahmen die mögliche rechtswidrige Nutzung verhindern.

— Lösung

Nicht mehr benötigte personenbezogene Daten können nur durch Aufruf eines speziellen Moduls physikalisch gelöscht werden. Das hat zur Folge, daß sie bis dahin wieder lesbar gemacht und damit weiter genutzt werden können. Wird die Information nicht endgültig zum Verschwinden gebracht, sondern nur ihre Verwertbarkeit eingeschränkt, liegt zwar eine Sperrung, aber keine Lösung i. S. v. § 2 Abs. 2 Nr. 6 BrDSG vor. Anders ausgedrückt: Nach § 20 Abs. 3 BrDSG erford erliche Lösungen können in den meisten Fällen mit den in Standard-Software enthaltenen normalen „Löschfunktionen“ nicht getätigt werden. § 20 Abs. 3 BrDSG setzt voraus, daß die Lösung nicht mehr rücksichtlich gemacht werden kann. Auch diese Sicherungslücke will der Finanzsenator nur organisatorisch schließen.

— Leistungskontrolle

Bei jeder Buchung wird die Sachbearbeiternummer festgehalten, die auch für Leistungs- und Verhaltenskontrollen ausgewertet werden kann.


13.3 Fall: „Informantengeheimnis“ bei der Steuererklärung von Journalisten


13.4 Datenllüsse nach dem „Zinsabschlaggesetz“

Zahlreiche Bürger haben sich bei mir erkundigt, welche Daten zwischen den Kreditinstituten und den Steuerbehörden bei der Anwendung des sogenannten „Zinsabschlaggesetzes“ fließen.


14. Nicht-öffentlicher Bereich

14.1 Zugriffsprobleme bei Dialogsystemen


Im Hinblick darauf, daß dieartige Dialogsysteme weit verbreitet sind, möchte ich schon in diesem Bericht auf folgende Anforderungen hinweisen:

— Protokollierung der Systembenutzung

Zur ordnungsgemäßen Anwendung von DV-Programmen, mit denen personenbezogene Daten verarbeitet werden (§ 37 Abs. 1 Satz 3 Nr. 1 Bundesdatenschutzgesetz — BDSG), gehört auch angemessene technisch-organisatorische Schutzmaßnahmen (§ 9 BDSG nebst Anlage) vorzusehen und ihre Bearbeitung „sicherzustellen“. Zum „Stand der Technik“, insbesondere bei Dialoganwendungen, gehört eine möglichst umfassende, differenzierte und wirksame Protokollierung

— Protokollierung bei automatisierten Abrufverfahren

Für automatisierte Abrufverfahren, bei denen Daten von dritten Stellen online abgerufen oder von ihnen eingesehen werden können, sieht das BDSG in § 10 Abs. 4 Satz 3 vor, „zumindest durch geeignete Stichprobenverfahren“ eine Überwachungskontrolle zu gewährleisten. Ähnliches gilt nach § 10 Abs. 4 Satz 4 BDSG auch für die Übermittlung eines Gesamtdatenbestandes im Rahmen eines Stapellübertragungs, Stapellverarbeitungs- oder Datentransports. Die Protokollierungspflicht des § 10 Abs. 4 Satz 3 und 4 BDSG dient dazu, einzelne Datenabfragen bzw. automatisierte Datenübermittlungen auf ihre Zulässigkeit hin zu prüfen.


Bei Abruf oder Übermittlung eines Gesamtdatenbestandes (s. o.) bezieht sich die Protokollierungspflicht global auf diesen Bestand, nicht auf die einzelnen Daten. Hier könnten anstelle eines speziellen Stichprobenverfahrens die üblichen Job- und Syslog-Verfahren benutzt werden, die die einzelnen Vorgänge jeweils protokollmäßig festhalten.

Auch diese Protokolldaten sollten möglichst zeitnah überprüft werden; sie unterliegen ebenfalls einer strikten Zweckbindung. Die Aufbewahrungsduer sollte in diesem Fall wenigstens ein Jahr betragen.

— Beschränkung der Zugriffsberechtigung


14.2 Fall: Unberechtigte Schufa-Abrufe

Ein Patent beschwerte sich bei mir darüber, daß die Schutzgemeinschaft für allgemeine Kreditinformation (Schufa) Bremen eine falsche bzw. unsichere Angabe
gespeichert und einer Bank mit der er keinerlei Verbindung habe, eine Kreditauskunft erteilt habe. Meine Prüfung dieser Beschwerde bei der Schufa Bremen hat ergeben, daß die monierte Datenspeicherung unvollständig und somit unrichtig war; die gespeicherten Daten wurden berichtigt. Die Berechtigung der erteilten Kreditauskunft konnte seitens der Schufa Bremen nicht dargelegt werden; ein Angestellter der anfragenden Bank hatte ohne dienstliche Veranlassung, d. h. ohne berechtigtes Interesse, mißbräuchlich (für private Zwecke) die Kreditanfrage gestellt und Auskunft erhalten; die Datenübermittlung durch die Schufa Bremen war also unzulässig.


Dieser Vorgang gibt zu folgenden datenschutzrechtlichen Erwägungen Anlass:

— Glaubhafte Darlegung des berechtigten Interesses


Die obersten Datenschutzaufsichtsbehörden haben im Jahre 1979 kurz nach Inkrafttreten des BDSG eine stichprobenweise Überprüfung des dargelegten berechtigten Interesses durch die Auskunfteien als ausreichend akzeptiert. Maßgeblich dafür war damals der Hinweis der Auskunfteien auf die große Zahl ihrer Mitteilungen (Datenübermittlungen) und auf Praktikabilitätsprobleme bei den verschiedenen Anfrageformen (schriftlich, telefonisch, per Telex oder Telefax, automatisiert). Für die Schufa-Gesellschaften waren damals zehn Überprüfungen pro Geschäftsstelle und Monat verabschiedet. Dazu sollten dann noch die Überprüfungen kommen, die ggf. aufgrund von Anlaufkontrollen der Aufsichtsbehörden notwendig werden sollten.


— Aufbewahrungsduer der Aufzeichnungen zum Nachweis des berechtigten Interesses

Das BDSG sagt zur Aufbewahrungsduer dieser Aufzeichnungen, die von den Auskunfteien gem. § 29 Abs. 2 Satz 3 BDSG oder bei automatisierten Abfraverfahren

— Sorgfaltspflichten des Anfragers


14.3 Aufbau eines Mietkatasters


Ich habe die Organisation darauf hingewiesen, daß Vermieter mit der Weitergabe solcher Informationen aus ihren Dateien an die das Mietkataster führende Einrichtung personenbezogene Daten der Mieter übermitteln, obwohl hierfür die Voraussetzungen des § 28 Bundesdatenschutzgesetz (BDSG) nicht vorliegen.

Insbesondere besteht ein Grund zu der Annahme, daß die betroffenen Mieter ein schutzwürdiges Interesse an dem Ausschuß der Übermittlung an das Mietkataster haben. Für den Fall, daß ihre Wohnung als Vergleichsobjekt im Rahmen eines Mieterhöhungsverlangens benannt wird, sind sie nicht in der Lage, sich vor unverhältnismäßigen Belastungen, weil andere Mieter oder Vermieter ihre Wohnung besichtigen möchten, zu schützen.


Im Hinblick auf Mietwohnungen sind aber auch die Belange der Mieter zu berücksichtigen, für die die eigene Wohnung zum Kernbereich ihrer Privatsphäre gehört. Sie müssen fürchten, daß ihre Wohnungen aufgrund der durch die automatisierte Verarbeitung eröffneten schnellen und leichten Verfügbarkeit der Informationen deutlich häufiger als bisher zur Begründung von Mieterhöhungsverlangen herangezogen werden.

Damit besteht eine erhöhte Wahrscheinlichkeit, daß bei Mietern Nachforschungen über ihre Wohnungen angestellt werden. Außerdem enthält das Mietkataster Angaben, die Rückschlüsse auf Einkommenslage und sonstige Lebensumstände der Wohnungsinhaber ermöglichen.

Mehrere Aufsichtsbehörden kommen nach Abwägung der Interessen zum Ergebnis, daß die Übermittlung der Daten von Vergleichswohnungen durch die Ver-
mieter nur zulässig ist, wenn die Betroffenen nicht widersprochen haben. Nach meiner Auffassung genügt die Widerspruchsmöglichkeit nicht; vielmehr bedarf es einer Einwilligung des Mieters nach § 4 Abs. 2 BDSG, in der Regel also schriftlich. Ich habe daher folgendes Verfahren vorgeschlagen:


14.4 Arbeitnehmerdatenschutz

14.4.1 Fall: Führungszugnisse im laufenden Arbeitsverhältnis

Mehrere Beschäftigte eines Unternehmens wandten sich dagegen, daß ihr Arbeitgeber sie ohne konkreten Anlaß aufgefordert hat, polizeiliche Führungszugnisse vorzulegen.


14.4.2 Unzulässige Rubriken im Bewerbungsfragebogen

Ein großes Bremer Unternehmen hat von Bewerbern Personaldokumente ausgefordert, die eine Vielzahl von unzulässigen Angaben enthalten. Dieser Fall ist exemplarisch für die vielfach anzutreffende häufig aber auch auf Nachlässigkeit beruhende „Datensammelwut“ im Personalwesen der Privatwirtschaft.


Fragen nach dem Gesundheitszustand bzw. nach bestehenden Krankheiten sind nur zulässig, soweit sie auf eine mögliche Beeinträchtigung der konkreten Arbeit bezogen sind oder eine Gefährdung der zukünftigen Kollegen oder Kunden in Betracht kommt. Die entsprechende Rubrik im Fragebogen muß daher in diesem Sinne einschränkend formuliert werden.


Die Verwendung der Rentenversicherungsnummer unterliegt nach § 18 f Sozialgesetzbuch IV (SGB IV) der strikten Zweckbindung. Der Arbeitgeber darf sie nur erheben, speichern oder verwenden, soweit dies für die Erfüllung einer gesetzlichen Aufgabe der in dieser Rechtsvorschrift genannten Stellen erforderlich ist. Dies ist aber erst nach Eingehen des Arbeitsverhältnisses der Fall. Im Bewerbungsfragebogen ist dieses Datum daher zu streichen.

Die Frage nach erfolgten Plädenungen kann nur dann — bezogen auf den zu besetzenden Arbeitsplatz — von Bedeutung sein, wenn Bewerber besondere Vertrauensstellungen einnehmen sollen (z. B. Buchhaltung oder Kasse).

Auch die Frage nach Verwandten im Betrieb oder in der gleichen Branche läßt keinen Bezug zu einem konkreten Arbeitsplatz erkennen.

Ich habe das Unternehmen gekehrt, den Personalfragebogen entsprechend zu ändern. Es hat dies zugesagt und wird mir nach Abstimmung mit dem Betriebsrat den überarbeiteten Vordruck zuleiten.

14.4.3 Noch immer kein Arbeitnehmerdatenschutzgesetz


Bundesregierung erklärt, der Bundesminister für Arbeit und Sozialordnung habe die dazu erforderlichen umfangreichen Vorarbeiten (!) aufgenommen.

Eine weitere Verzögerung ist nicht mehr vertretbar.

15. Register der nach dem Bundesdatenschutzgesetz meldepflichtigen Stellen

In dem bei mir geführten Register der meldepflichtigen Stellen, sind derzeit gem. § 32 Bundesdatenschutzgesetz (BDSG) insgesamt 87 Unternehmen registriert, von denen 72 aus der Stadt Bremen und 15 aus Bremerhaven stammen. Unterteilt nach Art der meldepflichtigen Tätigkeit und regionaler Ansiedlung im Lande Bremen ergibt sich folgendes Bild:

<table>
<thead>
<tr>
<th>Art der Tätigkeit</th>
<th>insgesamt</th>
<th>Bremen</th>
<th>Bremerhaven</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speicherung personenbezogener Daten zum Zwecke der Übermittlung</td>
<td>8</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Verarbeitung oder Nutzung personenbezogener Daten im Auftrag als Dienstleistungsunternehmen</td>
<td>79</td>
<td>67</td>
<td>12</td>
</tr>
</tbody>
</table>

Zu den insgesamt acht Unternehmen, die Daten zum Zwecke der Übermittlung speichern, gehören fünf Kredit- und Handelsauskunftseien und drei Adressenhandelsunternehmen. Unter den 79 Unternehmen, die Daten im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, befinden sich drei Datensäle und -verwaltungsstätte. Die anderen Firmen betreiben in der Mehrzahl automatisierte Datenerarbeitung für Dritte (z. B. Service-Rechenzentren).


16. Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

16.1 Entschließung zum Arbeitnehmerdatenschutz vom 23./24. März 1992


Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnötigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

— 64 —

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.


3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.

4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.

5. Beurteilungen und Personalausschlußentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.


10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschn. 1 Abs. 4) eingewilligt hat.
16.2 Entschließung zur Neuregelung des Asylverfahrens vom 28. April 1992

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen:

1. über die erkrankungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und

2. über die Nutzung der dabei gewonnenen erkrankungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

Zu 1:

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern — bis auf wenige Ausnahmen — Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:

Der Staat hat selbstverständlich das Recht zu wissen, mit wellem er zu tun hat. Jeder — gleichgültig ob Deutscher oder Ausländer — muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkrankungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber — also nicht bloß diejenigen einzelner oder bestimmter Gruppen — zweifelhaft ist, wäre eine erkrankungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20% der Asylbewerber unverhältnismäßig einen deutschen Namen einen weiteren Asylantrag stellen, Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2:

Bei der zentralen Auswertung der Fingerabdrücke von Asylbewerbern durch das Bundeskriminalamt muß — ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird — unbedingt folgendes sichergestellt sein:

— Fingerabdrücke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzzeitverformung der Fingerabdrücke aus. Gerade aber dabei soll es nicht bleiben.

Mit der bevorstehenden Einführung von AFIS — einem neuen automatisierten Fingerabdrucksverfahren — sollen künftig auch die Fingerabdrücke von Asylbewerbern, die allein zur Feststellung deren Identität gedient wurden, genaues erfaßt und ausgewertet werden wie die Fingerabdrücke von Straftätern, die in § 22 Abs. 4 des Strafgesetzbuchs vorgesehene Trennung der erkrankungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte — über das Trennungsgebot des § 16 Abs. 4 hinaus — die Verformung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

— Die Datenschutzbeauftragten verkennt nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrücke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht — wie es der Gesetzentwurf vorsieht — praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem
abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

---

Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätsicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

16.3 Entschließung zum Grundrecht auf Datenschutz vom 28. April 1992


---

Für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,

---

der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freienheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,

---

der Grundrechtskatalog dem technologischen Wandel angepaßt und

---

die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundestages entwickelt worden sind.

Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:


2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte mit einzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:

---

Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungs techniken

Recht auf Zugang zu den Daten der Verwaltung (Akteure öffentlichkeits, Informationsfreiheit)

Instrumente zur Technikfolgenabschätzung.

16.4 Entschließung zum „Lauschangriff“ vom 1./2. Oktober 1992

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegens Stimme des I.D. Bayern):

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. „Lauschangriff“) zu ermöglichen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitsaufklärung um jedes Verbrechen nicht gibt. Deshalb folgt, daß der Lautengriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.


16.5 Entscheidung zum Gesundheitsstrukturgesetz 1993 vom 1./2. Oktober 1992

Die Bundesregierung will mit dem Gesundheitsstrukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begründenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u. a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die ärztlichen Verpflichtungen müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hat vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertenkarten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenstellung zwischen Krankenkassen und Medizinischen Dienst muß aufrechterhalten bleiben.

- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertenkarten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.


16.6 Entscheidung zum Datenschutz bei internen Telekommunikationsanlagen vom 1./2. Oktober 1992

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch
eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefonantwor- 

Der Schutz des Formmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonde- 

 Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind über- 

 Die automatische Speicherung der Rufnummern von externen Anrufen nach 

 Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß 

 Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unbe- 

 Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, 

 Druck: Anker-Druck Bremen