BREMISCHE BÜRGERSCHAFT **Drucksache 16 / 1111**
Landtag 22. 08. 06
16. Wahlperiode

Mitteilung des Senats vom 22. August 2006

Stellungnahme des Senats zum 28. Jahresbericht des Landesbeauftragten für den Datenschutz

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum 28. Jahresbericht des Landesbeauftragten für den Datenschutz (Berichtszeitraum: 1. Januar bis 31. Dezember 2005) mit der Bitte um Kenntnisnahme.

Der Datenschutz hat im Land Bremen in den vergangenen Jahren einen hohen Standard erreicht. Dieser Standard ist, bei durchaus berechtigter Kritik im Einzelfall, auch im Berichtszeitraum gehalten worden. Die Sicherung der verfassungsrechtlich verbürgten informationellen Selbstbestimmung der Bürgerinnen und Bürger war und ist ein zentrales politisches Anliegen des Senats. Der Senat bekräftigt daher erneut seine Absicht, in Abstimmung mit dem Landesbeauftragten für den Datenschutz auch in Zukunft alle erforderlichen Maßnahmen zum Schutz personenbezogener Daten zu ergreifen und etwa noch bestehenden Mängeln abzuhelfen.

Zu den Einzelheiten des 28. Jahresberichts nimmt der Senat, soweit sein Kompetenzbereich betroffen und soweit dies in der Sache erforderlich ist, wie folgt Stellung.

1. Vorwort

1.4 Schuldatenschutzgesetz (S. 6 f.)

Siehe Stellungnahme zu Tz. 13.3.

1.5 Pilotprojekt „Elektronische Gesundheitskarte“ in Bremen (S. 7)

Siehe Stellungnahme zu Tz. 11.2.

1.8 ALG II (S. 8)

Siehe Stellungnahmen zu Tz. 5.1 und Tz. 12.1.

1.12 Datenschutzkontrolle zusammenhängend organisieren (S. 10)

Der Senat ist mit dem Landesbeauftragten für den Datenschutz der Auffassung, dass kein Anlass besteht, die in der Praxis bewährte Organisation der Datenschutzaufsicht im Land Bremen zu verändern.

3. Europa und Internationales

3.1 Vertragsverletzungsverfahren wegen mangelnder Unabhängigkeit (S. 15)

Die gegenwärtige Organisation der Datenschutzaufsicht im Land Bremen ist nach Auffassung des Senats mit europäischem Recht zu vereinbaren. Die Unabhängigkeit des Landesbeauftragten für den Datenschutz bei der Aufgabenwahrnehmung ist durch § 25 BremDSG – auch soweit er als Aufsichtsbehörde gemäß § 38 BDSG für den privaten Bereich tätig wird – hinreichend gewährleistet.

5. Medien

5.1 Verfahren der Rundfunkgebührenbefreiung (S. 18 f.)

Die kritisierte Regelung in § 6 Abs. 2 des Rundfunkgebührenstaatsvertrag (RfGebStV) wurde durch den 8. Rundfunkänderungsstaatsvertrag (8. RfÄndStV) eingefügt. Die fehlende Beteiligung des Landesbeauftrag-

ten für den Datenschutz war bereits Gegenstand seines 27. Jahresberichts, hierzu hat der Senat im letzten Jahr Stellung genommen. Von den materiellrechtlichen Vorschriften des 8. RfÄndStV hat der Landesbeauftragte für den Datenschutz im 27. Jahresbericht und in der vorangegangenen Korrespondenz mit der Senatskanzlei lediglich § 8 Abs. 4 RfGebStV moniert, nicht hingegen den nunmehr beanstandeten § 6 Abs. 2 RfGebStV.

Eine Ergänzung der Staatsvertragsnorm um die Möglichkeit, die Befreiungsvoraussetzungen alternativ auch durch behördliche Bescheinigung nachzuweisen, wird derzeit in der Rundfunkkommission der Länder geprüft. Die Gesetzgebungskompetenz der Länder ermöglicht allerdings keine Verpflichtung aller betroffenen Sozialbehörden (insbesondere nicht der Arbeitsgemeinschaften nach dem SGB II), eine Bescheinigung für die GEZ auszustellen.

Der erwähnte „Runde Tisch" wurde nicht erst aufgrund der Beratungen im Rechtsausschuss gebildet. Er ist bereits im März und April 2005 durch die Senatskanzlei einberufen worden. Das Amt für Soziale Dienste hat sich bereits in diesen Sitzungen bereit erklärt, auf dem GEZ-Formular die Leistungsgewährung durch einen Stempel zu bestätigen. Die Vertreterin des Landesbeauftragten für den Datenschutz hat erstmalig an der Sitzung im November 2005 teilgenommen.

Im Rahmen der 4. Sitzung des Runden Tischs am 16. Mai 2006 haben Vertreter der BAgIS sowie der Arbeitsgemeinschaft Job-Center Bremerhaven erläutert, dass eine Bestätigung auf dem GEZ-Formular nur nach vorheriger inhaltlicher Prüfung der Befreiungsvoraussetzungen (inklusive Nichtgewährung von Zuschlägen nach § 24 SGB II) erteilt werde. Nach weiterer Rücksprache mit der GEZ wurde in Abstimmung mit Radio Bremen, der BAgIS, der Arbeitsgemeinschaft Job-Center Bremerhaven und dem Landesbeauftragten für den Datenschutz nunmehr eine Einigung auf folgendes Verfahren erzielt: Die GEZ stellt zukünftig einen neuen Vordruck zur Verfügung, auf dem die BAgIS bzw. die Arbeitsgemeinschaft Job-Center Bremerhaven die Befreiungsvoraussetzungen bestätigen. Eine Übersendung weiterer Fotokopien ist dann nicht mehr erforderlich.

Langfristig soll die manuelle Bestätigung durch ein automatisiertes Verfahren ersetzt werden. In Kooperation mit der GEZ entwickelt die Bundesagentur für Arbeit eine Ergänzung des bundesweit verwendeten EDV-Programms. In einem ersten Schritt soll automatisch ein „Zweitbescheid" zur Vorlage bei der GEZ erstellt werden, der ausschließlich die für die Gebührenbefreiung erforderlichen Daten enthält. Diese Software-Lösung wird voraussichtlich Anfang 2007 umgesetzt werden können. In einem zweiten Schritt ist zusätzlich die automatische Übermittlung dieser Daten vorgesehen. Dadurch wird gleichermaßen datenschutzrechtlichen Aspekten Rechnung getragen sowie der Verwaltungsaufwand der Behörden reduziert.

7. Bremische Bürgerschaft – Die Arbeit des Rechtsausschusses

7.1 Ergebnisse der Beratung des 27. Jahresberichts (S. 21 ff.)

Ergebnisse des 26. Jahresberichts (27. Jahresbericht, Tz. 4.1) – Datenschutzrechtliche Situation im Stadtamt

Siehe Stellungnahme zu Tz. 9.15.

Prüfung der Telekommunikationsüberwachung (27. Jahresbericht, Tz. 6.6)

Der behördliche Datenschutzbeauftragte der Polizei Bremen hat dem Landesbeauftragten für den Datenschutz am 24. Juli 2006 eine überarbeitete Verfahrensbeschreibung vorgelegt. Diese genügt allerdings insbesondere hinsichtlich der Beschreibung der technischen und organisatorischen Maßnahmen zum Datenschutz noch nicht den vom Landesbeauftragten für Datenschutz formulierten Anforderungen, so dass eine Nachbesserung erforderlich ist. Unter anderem soll auch die eingesetzte Hardware der Firma ARTIS näher beschrieben werden. Ein überarbeiteter Entwurf wird Anfang September 2006 vorgelegt werden.

ISA-Web statt NIVADIS (27. Jahresbericht, Tz. 6.7)

Siehe Stellungnahme zu Tz. 9.7.

Stoffwechselscreening bei Neugeborenen (27. Jahresbericht, Tz. 8.1)

Die Vereinbarung mit dem Universitätsklinikum Hamburg-Eppendorf über die Einhaltung datenschutzrechtlicher Vorschriften im Rahmen des erweiterten Neugeborenen-Screenings wurde im März 2006 abgeschlossen. Der Landesbeauftragte für den Datenschutz wurde hierüber informiert.

Einführung der elektronischen Arbeitszeiterfassung (27. Jahresbericht, Tz. 1.2)

Siehe Stellungnahme zu Tz. 8.1.

Erlaubnis erweiterter Datenbeschaffung durch die GEZ (27. Jahresbericht, Tz. 2.2)

Siehe Stellungnahme zu Tz. 5.1.

8. Personalwesen

8.1 Technische Mängel bei der Arbeitszeiterfassung (AZE) (S. 26 f.)

Die bei der elektronischen Arbeitszeiterfassung festgestellten Sicherheitsmängel konnten bis zum Ende des Jahres 2005 vollständig und, mit Ausnahme der fehlenden Firewallinstallationen, auch zügig behoben werden.

Das mit dem Landesbeauftragten für den Datenschutz abgestimmte Datenschutzkonzept setzt die Einhaltung allgemeiner Datenschutzstandards voraus, ohne sie im Detail zu regeln. Der Senator für Finanzen ist davon ausgegangen, dass die mit der Installation beauftragte Firma diese allgemeinen Datenschutzstandards selbstverständlich einhält.

Zur Beseitigung der Probleme mit der Firewall wurden zunächst mehrere Lösungsalternativen erwogen. Es wurde schließlich für jedes Gerät eine separate Firewallinstallation gewählt, bei der lediglich einmalige Einrichtungskosten anfallen.

Die Maßnahmen zur Beseitigung der Sicherheitsmängel wurden laufend mit dem Landesbeauftragten für den Datenschutz abgestimmt. Nach Abschluss der Mangelbeseitigung bestätigte der Landesbeauftragte für den Datenschutz schließlich den dadurch erzielten ordnungsgemäßen Betrieb des Verfahrens.

9. Inneres

9.1 Neues Gesetz über den Verfassungsschutz im Lande Bremen (S. 27 ff.)

Das neue Verfassungsschutzgesetz wurde Anfang 2006 von der Bremischen Bürgerschaft auf Vorlage des Senats beschlossen. Der Senator für Inneres und Sport und der Senator für Justiz und Verfassung hatten den Gesetzentwurf zuvor eingehend geprüft und die Verfassungskonformität bejaht.

Zur Auffassung des Landesbeauftragten für den Datenschutz ist zunächst festzustellen, dass es in datenschutzrechtlicher Hinsicht ohne Belang ist, ob ein Gesetz in seiner Struktur dem Beispiel eines anderen Bundeslandes folgen sollte. Die inhaltlichen Bedenken des Landesbeauftragten für den Datenschutz können ebenfalls nicht geteilt werden:

a) Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung: Maßnahmen zur akustischen Wohnraumüberwachung durch den Verfassungsschutz sind nur unter besonders engen, gesetzlich normierten Voraussetzungen zulässig. Sie sind nur zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht vorhanden sind, dass jemand eine der in § 3 Abs. 1 Satz 1 des Artikel-10-Gesetzes normierten Straftaten plant, begeht oder begangen hat. Gleiches gilt nach § 3 Abs. 1 Satz 2 des Artikel-10-Gesetzes, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind. Damit wird sichergestellt, dass der erhebliche Eingriff in das Grundrecht aus Artikel 13 GG nur bei tatsächlichen Anhaltspunkten für besonders schwerwiegende Straftaten in Betracht kommt und einer restriktiven Handhabung unterliegt.

Ferner besteht die Voraussetzung, dass die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert sein muss. Der Einsatz der nachrichtendienstlichen Mittel darf sich dabei nur gegen die verdächtige Person richten.

Entsprechend dem Grundsatz der Verhältnismäßigkeit ist angesichts der Schwere des Grundrechtseingriffs ferner geregelt, dass die Maßnahme unverzüglich zu beenden ist, wenn die Voraussetzungen der Anordnung nicht mehr vorliegen oder der verdeckte Einsatz technischer Mittel zur Informationsgewinnung nicht mehr erforderlich ist.

Das Gesetz über den Verfassungsschutz im Land Bremen hat den Maßstab der durch die Rechtsprechung des Bundesverfassungsgerichts zum Strafprozessrecht (Urteil vom 3. März 2004) festgelegten verfassungsrechtlichen Vorgaben hinsichtlich der Wohnraumüberwachung im Kernbereich der privaten Lebensgestaltung übernommen und entspricht der mit Gesetz vom 24. Juni 2005 in § 100 c der Strafprozessordnung eingefügten Regelung. Eine Maßnahme zur akustischen Wohnraumüberwachung ist gemäß § 9 Abs. 2 Satz 1 BremVerfSchG „nur zulässig, soweit nicht aufgrund tatsächlicher Anhaltspunkte, insbesondere der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass dadurch Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden.“

Es kann daher keine Rede davon sein, dass die verfassungsrechtlich gebotene Vorabprognose unterbleiben oder ohne Rücksicht auf die konkreten Personen erfolgen würde. Das Bundesverfassungsgericht hat im Übrigen klargestellt, dass bei Gesprächen, die einen unmittelbaren Bezug zu Straftaten aufweisen, der Kernbereich privater Lebensgestaltung nicht betroffen ist. Im Kernbereich privater Lebensgestaltung findet daher eine akustische Wohnraumüberwachung nicht statt.

Es trifft auch nicht zu, dass vom Verfassungsschutz im Wege der akustischen Wohnraumüberwachung gewonnene personenbezogene Daten auch dann an die Strafverfolgungsbehörden übermittelt werden dürfen, wenn diese selbst die Daten nicht hätten erheben dürfen. Gemäß § 10 Abs. 2 Satz 4 BremVerfSchG dürfen die Daten nur zur Verfolgung der in § 100 c Abs. 2 StPO genannten Straftaten übermittelt werden und dies auch nur dann, sofern die Tat auch im Einzelfall besonders schwer wiegt. Im Übrigen lässt § 10 Abs. 2 Satz 4 BremVerfSchG eine Datenübermittlung nur zu Zwecken der Gefahrenabwehr zu.

b) Hilfestellung bei der Verwendung von Tarnmitteln: Mit der Verwendung von Tarnmitteln ist keine Erweiterung der Kompetenzen des Landesamtes für Verfassungsschutz verbunden. Die grundsätzliche Verpflichtung aller Behörden des Landes und der Stadtgemeinden zur technischen Hilfeleistung bei Tarnmaßnahmen stellt die Aufgabenwahrnehmung des Landesamtes für Verfassungsschutz in einem zentralen Bereich sicher. § 8 Abs. 7 BremVerfSchG ergänzt lediglich den allgemeinen Amtshilfegrundsatz nach Artikel 35 Abs. 1 des Grundgesetzes und nach § 4 des Bremischen Verwaltungsverfahrensgesetzes.

c) Datenschutzrechtliche Bestimmungen im Entwurf: Die im Bremischen Datenschutzgesetz enthaltenen allgemeinen Regelungen werden

der besonderen Aufgabenstellung des Landesamtes für Verfassungsschutz zum Teil nicht gerecht. In diesen Fällen wäre die durch den Landesbeauftragten für den Datenschutz angeregte Verweisung auf das Bremische Datenschutzgesetz nicht zweckmäßig. Dies stellt im Übrigen keine Besonderheit des Verfassungsschutzrechts dar; vielmehr finden sich spezielle datenschutzrechtliche Regelungen in zahlreichen Gesetzen, weil und soweit die allgemeinen Regelungen den besonderen Anforderungen der jeweils zu regelnden Fachmaterie nicht hinreichend gerecht werden.

d) Minderjährigenregelungen: Hinzuweisen ist zunächst darauf, dass sowohl im Bereich des Rechtsextremismus als auch bei anderen militanten Extremisten eine deutliche Verjüngung des Mitgliederkreises feststellbar ist. Insbesondere in rechtsextremistischen Skinhead-Gruppen und anderen gewalttätigen rechtsextremistischen Gruppierungen sind zunehmend jüngere Personen organisiert, die sich teilweise äußerst militant verhalten.

   Das Bremische Verfassungsschutzgesetz unterscheidet hinsichtlich der Speicherung, Veränderung und Nutzung der Daten über das Verhalten Minderjähriger danach, ob die Daten in Akten, die zur Person der oder des Minderjährigen geführt werden oder in Dateien verarbeitet werden sollen.

   Personenbezogene Daten dürfen vor Vollendung des 16. Lebensjahres in Akten nur im Zusammenhang mit Straftaten nach § 3 Abs. 1 des Artikel-10-Gesetzes gespeichert, verändert und genutzt werden, also im Bereich schwerster Kriminalität oder von Staatsschutzdelikten. In Dateien ist die Verarbeitung von Daten zum Schutz der Jugendlichen erst ab Vollendung des 16. Lebensjahres unter der Voraussetzung zulässig, dass tatsächliche Anhaltspunkte für den Verdacht einer Bestrebung oder Tätigkeit nach § 3 Abs. 1 Satz 1 BremVerfSchG vorliegen und diese Bestrebung oder Tätigkeit durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen verfolgt wird.

   Um ein Mitschleppen von „Jugendsünden“ zu verhindern, wurden spezielle nach dem Alter der Minderjährigen gestaffelte Überprüfungs- und Löschungsfristen eingeführt.

e) Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz: Eine Bekanntgabe personenbezogener Daten bei der Aufklärung der Öffentlichkeit ist nur zulässig, wenn die Veröffentlichung für die Aufklärung über Bestrebungen und Tätigkeiten nach § 3 Abs. 1 Satz 1 BremVerfSchG erforderlich ist und das Interesse der Allgemeinheit das schutzwürdige Interesse der betroffenen Person überwiegt. Entgegen der Behauptung des Landesbeauftragten für den Datenschutz sieht auch das Bundesverfassungsschutzgesetz seit jeher eine Veröffentlichung personenbezogener Informationen nach vorhergehender Güterabwägung vor. Ohnehin sind derartige Veröffentlichungen personenbezogener Informationen in der Praxis auf wenige Einzelfälle beschränkt. Sie betreffen in der Regel nur herausragende Führungspersönlichkeiten, über die gesicherte Erkenntnisse vorliegen, z. B. den Vorsitzenden einer extremistischen Partei oder Gruppierung.

f) Schutz von Amts- und Berufsgeheimnissen: Die besonderen Schutzvorschriften des § 8 Abs. 3 und des § 9 Abs. 4 BremVerfSchG sind dem § 100 c Abs. 6 der Strafprozessordnung nachgebildet. Der dadurch gewährte Schutz geht zum Teil über das verfassungsrechtlich gebotene Maß hinaus.

9.2 Prüfung beim Landesamt für Verfassungsschutz (S. 29)

a) Abruf von Meldedaten: Es trifft zu, dass Protokollierungsdaten, die beim Abruf von Meldedaten aus dem Melderegister durch das Landesamt für Verfassungsschutz aufgezeichnet wurden, versehentlich vorzeitig gelöscht wurden. Nach Bekanntwerden dieses Fehlers im Zuge einer Prüfung durch den Landesbeauftragten für den Daten-

schutz wurden umgehend geeignete Maßnahmen ergriffen, um künftig in allen Fällen eine den Anforderungen des § 30 Abs. 3 des bremischen Meldegesetzes entsprechende Protokollierung zu gewährleisten.

Allerdings hat der Landesbeauftragte für den Datenschutz den Fehler im Berichtszeitraum nicht formell beanstandet. Während die Prüfung beim Landesamt für Verfassungsschutz durch den Landesbeauftragten für den Datenschutz am 15. Juni 2005 erfolgte, wurde der Fehler erst über acht Monate später mit Schreiben des Landesbeauftragten für den Datenschutz vom 21. Februar 2006 beanstandet.

b) Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz und nach dem Hafensicherheitsgesetz: Die Darstellung des Landesbeauftragten für den Datenschutz trifft im Wesentlichen zu. Das Landesamt für Verfassungsschutz erhält allerdings vom Bundesamt für Verfassungsschutz lediglich eine Liste über „Positivfälle", bei „Negativfällen" erfolgt hingegen keine Meldung.

c) Datenschutzkonzept und Verfahrensbeschreibung: Das Landesamt für Verfassungsschutz hat nach dem gegenwärtigen Stand der Erkenntnisse keine Bedenken bezüglich der Sicherheit des eingesetzten DV-Systems und sieht daher derzeit keine Notwendigkeit, Veränderungen (z. B. an der Firewall) vorzunehmen. Der Landesbeauftragte für den Datenschutz hat bislang nicht mitgeteilt, welche Sicherheitsbedenken aus seiner Sicht im Einzelnen bestehen. Als Verschlusssachen eingestufte Informationen werden über das entsprechende Netz nicht ausgetauscht.

9.3 Änderung des Bremischen Polizeigesetzes (S. 29 f.)

a) Überarbeitete Regelung der akustischen Wohnraumüberwachung: Die vom Landesbeauftragten für den Datenschutz in Bezug auf den Schutz des Kernbereichs privater Lebensgestaltung geäußerten Bedenken werden vom Senat nicht geteilt. Zunächst ist darauf hinzuweisen, dass das Abhören des gesprochenen Worts mit technischen Mitteln aus Wohnungen überhaupt nur zulässig ist, soweit es sich um die Abwehr gegenwärtiger Gefahren für Leib, Leben oder Freiheit einer Person handelt und die Gefahr nicht auf andere Weise abgewehrt werden kann. Leib, Leben oder Freiheit sind Schutzgüter von hohem – auch verfassungsrechtlichem – Rang. Gleichwohl rechtfertigt nicht jede Gefährdung dieser Schutzgüter Maßnahmen der akustischen Wohnraumüberwachung: Zum einen muss die Gefahr „gegenwärtig" sein, d. h., die Einwirkung des schädigenden Ereignisses muss bereits begonnen haben oder unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorstehen. Zum anderen darf es kein anderes Mittel zur Abwehr der Gefahr geben (Wohnraumüberwachung als ultima ratio). Soweit es in einer solchen Situation durch das polizeiliche Abhören mit technischen Mitteln zu einer Beeinträchtigung des Kernbereichs privater Lebensgestaltung der Verursacher einer solch hochrangigen Gefahr kommen sollte, ist festgelegt, dass die Aufzeichnungen unverzüglich zu löschen sind. Derartige Äußerungen dürfen nicht verwertet werden. Nach Auffassung des Senats trägt diese Regelung dem verfassungsrechtlich gebotenen Schutz des Kernbereichs privater Lebensgestaltung ausreichend Rechnung. Eine Verpflichtung zum sofortigen Abschalten der Geräte im Falle vermuteter Beeinträchtigungen des Kernbereichs privater Lebensführung wäre hingegen in Situationen, in denen es um die Abwehr gegenwärtiger Gefahren geht, nicht umzusetzen, ohne polizeiliche Maßnahmen in erheblichem Maße zu erschweren oder zu verhindern; mögliche Folge wäre die Gefährdung des Lebens von Menschen oder deren Gesundheit oder Freiheit.

Verfassungsrechtlich ist die vom Landesbeauftragten für den Datenschutz vertretene Forderung eines sofortigen Abschaltens der Geräte im Falle vermuteter Beeinträchtigungen des Kernbereichs privater Lebensführung nicht geboten. Im Gegensatz zur Strafver-

folgung, mit der sich das Bundesverfassungsgericht in seiner Entscheidung vom 3. März 2004 zur akustischen Wohnraumüberwachung beschäftigt hat und bei der es in erster Linie um die Feststellung der Täter einer bereits geschehenen Straftat, mithin um die Durchsetzung des Strafanspruchs des Staates geht, ist bei der so genannten präventiven Wohnraumüberwachung eine akute Gefahr für dritte Personen durch die Handlungen des Verursachers gegeben. Verfassungsrechtlich ist der Staat nicht nur verpflichtet, den Schutz des Kernbereichs privater Lebensgestaltung der Verursacher zu gewährleisten, sondern muss auch das Leben, die Gesundheit und die Freiheit der von dem rechtswidrigen Eingriff Betroffenen schützen. In diesem verfassungsrechtlichen Spannungsverhältnis, das bei der Strafverfolgung nicht in gleicher Weise vorliegt, können, wie in der Gesetzesbegründung dargelegt, die Grundsätze der Entscheidung des Bundesverfassungsgerichts zur repressiven Wohnraumüberwachung nicht ohne weiteres unmittelbar angewendet werden. Das Bundesverfassungsgericht selbst hat in seiner Entscheidung zur präventiven Telekommunikationsüberwachung vom 27. Juli 2005 ausgeführt, dass das Risiko, dass präventive Abhörmaßnahmen Äußerungen aus dem Kernbereich privater Lebensgestaltung erfassen, hinzunehmen ist „bei einem besonders hohen Rang des gefährdeten Rechtsguts und einer durch konkrete Anhaltspunkte gekennzeichneten Lage, die auf einen unmittelbaren Bezug zur zukünftigen Begehung der Straftat schließen lässt. Hinzu müssen Vorkehrungen kommen, die sichern, dass die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden dürfen, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist." (Urteil vom 27. Juli 2005, 1 BvR 668/04, Rz. 164). Diesen Anforderungen trägt die Regelung des bremischen Polizeigesetzes zur präventiven akustischen Wohnraumüberwachung Rechnung.

Die vom Landesbeauftragten für den Datenschutz geäußerte Kritik an der Herausnahme von Gesprächen über die beabsichtigte Begehung oder Fortführung von Straftaten aus dem Kernbereichsschutz wird vom Senat ebenfalls nicht geteilt. Die entsprechende Bestimmung des bremischen Polizeigesetzes steht im Einklang mit der Rechtsprechung des Bundesverfassungsgerichts (vergleiche BVerfG, Urteil vom 27. Juli 2005, 1 BvR 668/04, Rz. 161: Nicht zum Kernbereich gehören Kommunikationsinhalte, „die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten.").

b) Ausweitung der Identitätsfeststellung: Es handelt sich bei der erfolgten Gesetzesänderung um eine rechtliche Klarstellung und nicht um eine Ausweitung von Befugnissen der Polizei, wie der Landesbeauftragte für den Datenschutz meint. Die Änderung geht zurück auf eine Entscheidung des Oberverwaltungsgerichts Hamburg, in der das Gericht eine Überprüfung von Personen an Gefahrenorten nur dann für zulässig gehalten hat, wenn diese an dem betreffenden Orten verweilen; damit wären nur Personen einer Kontrolle unterworfen, die zumindest deutliche Anzeichen eines verzögerten Ganges aufweisen oder an dem betreffenden Ort verharrten. Da dies so vom Gesetzgeber nicht beabsichtigt war, in der polizeilichen Praxis im jeweiligen Fall nur schwer eindeutig festzustellen wäre und erst recht kaum dokumentiert werden könnte, stellt die Änderung klar, dass die Überprüfung an Gefahrenorten alle Personen umfassen kann, die sich dort befinden, unabhängig davon ob sie sich zum Zwecke des Verweilens oder des Durchquerens dort aufhalten.

c) Ausweitung von Befragung und Auskunftspflichten: Die Darstellung des Landesbeauftragten für den Datenschutz, dass durch die erweiterten Befugnisse viele harmlose Personen in das Visier der Polizei gerieten und Eingriffe in ihr Persönlichkeitsrecht hinnehmen müssten, trifft so nicht zu. Die neue Regelung in § 13 Abs. 5 des Bremischen Polizeigesetzes sieht vor, dass die Befugnisse nur ausgeübt werden

dürfen, wenn aufgrund von konkreten Lageerkenntnissen mit Straftaten von erheblicher Bedeutung zu rechnen ist, die organisiert begangen werden sollen. Die Kontrollen werden durchgeführt, indem eine (dokumentierte) Festlegung des räumlichen Bereichs, des Zeitraums der Kontrollen und in der Regel eine Auswahl der Personen erfolgt, an die sich die Kontrolle richtet. Damit wird deutlich, dass nicht jede Person unabhängig davon kontrolliert wird, ob gegen sie Verdachtsmomente bestehen oder nicht.

d) Ausweitung von Kontrollstellen: Die Regelung ist an eine entsprechende Regelung des niedersächsischen Sicherheits- und Ordnungsgesetzes angelehnt. Sie sieht vor, dass die an einer Kontrollstelle erhobenen Daten unverzüglich gelöscht werden. Die vom Landesbeauftragten für den Datenschutz genannte Frist von einem Monat bezeichnet die maximale Aufbewahrungsdauer der Daten, nicht aber die Regelaufbewahrungsdauer. Sie ist als rechtsstaatliche Sicherung gegenüber einer sonst möglichen längeren Aufbewahrung durch die Polizei vorgesehen. Insofern überrascht die datenschutzrechtliche Kritik daran.

e) Elektronischer Kfz-Kennzeichenabgleich: Es bestand von vornherein die Absicht, den Abgleich der erfassten Kennzeichen mit dem Fahndungsbestand sofort, d. h., im Moment der Erfassung, durchzuführen. Mit dem Landesbeauftragten für den Datenschutz ist lediglich die Formulierung, die diese Absicht am besten zum Ausdruck bringt, entwickelt worden.

9.4 Fotos der Polizei in der „Galerie des Verbrechens“ (S. 31)

Die Veröffentlichung von polizeiinternen Daten und Lichtbildern in einer Boulevardzeitung stellt, insbesondere im Zusammenhang mit der Art der Publikation, einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen dar, durch den möglicherweise auch der Straftatbestand des § 201 a StGB erfüllt wird. Als wahrscheinliche Quelle der in den Veröffentlichungen verwendeten Daten konnte die von den Polizeien des Bundes und der Länder genutzte elektronische Informationsplattform „ExtraPol“ ermittelt werden. Die gemeinsamen Bemühungen, Verantwortliche zu benennen und zur Rechenschaft zu ziehen, erfolgten sowohl im Interesse des Landesdatenschutzbeauftragten als auch im Interesse der Polizei Bremen. Leider verliefen diese Anstrengungen nicht erfolgreich.

Zur Vermeidung von Wiederholungsfällen werden seitens der Polizei Bremen vorläufig keine weiteren Fahndungsblätter zur Nutzung in der gemeinsamen Informationsplattform ExtraPol bereitgestellt. Gleichzeitig werden die bundesweiten Bestrebungen zur datenschutzrechtlichen und datenschutztechnischen Optimierung der Plattform ausdrücklich unterstützt.

9.5 Errichtungsanordnungen und Verfahrensbeschreibungen (S. 31 f.)

Die dargelegten Kritikpunkte wurden in Gesprächen zwischen dem Landesbeauftragen für den Datenschutz, dem behördlichen Datenschutzbeauftragten und den zuständigen Mitarbeitern erörtert und weitestgehend ausgeräumt.

Eine aktualisierte Fassung der Richtlinien zur Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-R) wird zurzeit zwischen dem Landesbeauftragten für den Datenschutz, der Polizei Bremen und dem Senator für Inneres und Sport abgestimmt.

9.6 ApolWeb (S. 32)

Die im letzten Absatz der Tz. 9.6 des Jahresberichts erwähnte andere technische Lösung ist inzwischen umgesetzt worden. Der Zugriff erfolgt nunmehr im Einzelfall unmittelbar auf die Daten im Hoheitsbereich der Verwaltungspolizei. Eine Zusammenführung und Speicherung von Meldedaten und anderen Daten bei der Vollzugspolizei findet nicht mehr statt. Der Zugriff erfolgt nur auf solche Datenfelder, die nach der Meldedatenübermittlungsverordnung für den automatisierten Zugriff zugelas-

sen sind. Zugriffe werden protokolliert. Damit wird den Anforderungen des Landesbeauftragten für den Datenschutz entsprochen. Die abschließende Abstimmung wurde eingeleitet.

9.7 ISA-Web (S. 32 f.)

Die vom Landesbeauftragten für den Datenschutz angemahnten fehlenden Informationen sind mittlerweile bis auf wenige Ausnahmen von der Polizei Bremen übermittelt worden. Da sich weitere Fragen angeschlossen haben, die insbesondere das technische Fachkonzept betreffen, sind vertiefende Betrachtungen notwendig, die derzeit in einem abgestimmten Verfahren durchgeführt werden.

Aufgrund der aktuell stattfindenden Gespräche zwischen dem Landesbeauftragten für den Datenschutz und den bei der Polizei für ISA-Web Verantwortlichen geht der Senator für Inneres und Sport davon aus, dass die geforderten Unterlagen bald vollständig vorliegen.

Die angesprochene notwendige Aktualisierung der KpS-Richtlinien ist weitestgehend abgeschlossen und befindet sich in der internen Abstimmung. Sobald diese abgeschlossen ist, erfolgt eine Übermittlung an den Landesbeauftragten für den Datenschutz.

9.8 Datenschutzkonzepte bei der Ortspolizeibehörde Bremerhaven (S. 33)

Die Ortspolizeibehörde der Stadt Bremerhaven hat die Anregung des Landesbeauftragten für den Datenschutz, ein allgemeines Datenschutz- und Sicherheitskonzept zu erarbeiten, aufgegriffen. Die Erstellung wird allerdings noch einige Zeit beanspruchen. Der Landesbeauftragte für den Datenschutz wird im weiteren Verfahren beteiligt.

9.10 Mobile Videoüberwachung durch die Polizei (S. 35)

Die Darstellung im Jahresbericht trifft so nicht zu: Die Polizei Bremen prüft zurzeit im Auftrag des Senators für Inneres und Sport, ob neben dem Hauptbahnhof weitere Gefahrenorte in Bremen bestehen, an denen der Einsatz einer Videoüberwachung sinnvoll sein könnte und wie diese ausgestaltet sein müsste. Dabei wird auch die Variante einer mobilen Videoüberwachung geprüft. Ein Einsatz dieser Technik ohne entsprechende Begleitmaßnahmen (z. B. Hinweisschilder), wie dies der Landesbeauftragte für den Datenschutz zu befürchten scheint, kommt jedoch generell nicht in Betracht.

9.12 Datenverarbeitung bei der Feuerwehr in Bremen (S. 35)

Die vom Landesbeauftragten für den Datenschutz angeregten Ergänzungen und Aktualisierungen der Sicherheits- und Datenschutzkonzepte der Feuerwehr Bremen werden derzeit erarbeitet:

Es wird eine Benutzerordnung erstellt, die das von den Client-Anwendern einzuhaltende Verfahren regelt. Diese Benutzerordnung soll an alle Anwender persönlich ausgegeben werden. Ergänzt werden soll die Benutzerordnung um eine Erklärung, in der sich die Anwender zur Einhaltung der datenschutzrechtlichen Vorschriften verpflichten.

Eine Beschreibung der Verzeichnisstruktur sowie der Zugriffsrechte wird durch den Systemadministrator der Feuerwehr Bremen erstellt und nach Fertigstellung dem Landesbeauftragten für den Datenschutz vorgelegt.

Entwickelt wird ferner ein neues Rollenkonzept für die Administratoren. Künftig werden die Rollen „Netzgeräte-Administration“ und „Software-Administration“ getrennt.

Zur Erhöhung der Sicherheit bei der Fremdwartung wurde dem Landesbeauftragten für den Datenschutz ein Konzept vorgelegt, das eine Kombination verschiedener Techniken (IP-Sec, Einmalpasswörter, Fernwartungsgateway) vorsieht. Da aus Kostengründen eine kommerzielle Standardlösung nicht in Betracht kam, wurde auf Open-Source-Lösungen zurückgegriffen. Der Landesbeauftragte für den Datenschutz stimmte dem Konzept vorbehaltlos zu.

Für das Netzwerk der Feuerwehr Bremen wurde ein neues Konzept auf Basis eines Systems der Firma Cisco-Systems erarbeitet, das den Einsatz aller derzeit gängigen Sicherheitsmechanismen vorsieht. Dieses Konzept wurde dem Landesbeauftragten für den Datenschutz ebenfalls vorgelegt. Auch diesbezüglich erfolgte seine uneingeschränkte Zustimmung.

9.13 Einsatz von Unfalldatenspeichern bei der Feuerwehr Bremen (S. 36)

Die Verfahrensbeschreibung sowie die Dienstvereinbarung für die Unfalldatenschreiber wurden nach den Vorgaben des Landesbeauftragten für den Datenschutz ergänzt und ihm zur Stellungnahme vorgelegt.

Nach der am 20. April 2006 erfolgten Zustimmung durch den Landesbeauftragten für den Datenschutz wird die Dienstvereinbarung derzeit zwischen Amtsleitung und Personalrat abgestimmt. Im Abschluss daran soll ein sechsmonatiger Probebetrieb beginnen. Dem Probebetrieb hat der Landesbeauftragte für den Datenschutz unter Vorbehalt zugestimmt, da das Projekt Unfalldatenschreiber für alle Beteiligten neu ist und praktische Erfahrungen noch kaum vorhanden sind.

Nach Beendigung des Probebetriebs erfolgt eine Auswertung des dann vorhandenen Datenbestandes durch Mitarbeiter der Feuerwehr Bremen und des Landesbeauftragten für den Datenschutz, um unter anderem Klarheit über den Umfang der gespeicherten Daten und die tatsächliche Speicherdauer zu erhalten.

9.14 Internetnutzung bei der Feuerwehr Bremen (S. 36 f.)

Die Nutzung von E-Mail und Internet bei der Feuerwehr Bremen wird derzeit unter Berücksichtigung der Richtlinie für die Nutzung der Elektronischen Post vom 7. März 2002 (E-Mail-Richtlinie) und der Richtlinie für die Bereitstellung und Nutzung von Internet und Intranet-Zugängen vom 10. Februar 2004 (Internet-Richtlinie) neu geordnet. Dabei ist auf Folgendes hinzuweisen:

Für eine Aufstellung von zusätzlichen Personalcomputern für den ausschließlich privaten Internetzugang fehlen die finanziellen Mittel. Auch eine Bereitstellung von gesonderten DSL-Leitungen durch die Bremer Kommunikationstechnik GmbH (BreKom) kommt aus Kostengründen nicht in Betracht.

Ein Einsatz des in der Internet-Richtlinie geforderten Programms „PSD-Switch“ zur Unterscheidung von dienstlicher und privater Internetnutzung ist wegen fehlender Kompatibilität zur vorhandenen Thin-Client-Architektur nicht möglich. Hier wird eine Lösung mit zwei getrennten Browsern angestrebt. Eingesetzt werden sollen der Internetexplorer von Microsoft für die dienstliche Internetnutzung und der Firefox-Browser für die private Nutzung.

Eine dezentrale Protokollierung des privaten Internetzugangs kann ausgeschlossen werden. Die private Internetnutzung läuft über den Proxy-Server der Brekom, auf den die Feuerwehr Bremen keinen administrativen Zugriff hat.

Technische und organisatorische Sicherheitsfunktionen wie Firewall und Virenschutz sind vorhanden. Eine Deaktivierung von USB-Schnittstellen für den Bereich der externen Medien wurde durchgeführt.

Die E-Mail Nutzung wird durch die derzeit erstellte Benutzerordnung (siehe Tz. 9.12) geregelt.

9.15 Zentrales Datenschutzkonzept und Verfahrensbeschreibungen beim Stadtamt Bremen (S. 37)

Anfang 2006 konnte das Projekt zur Erstellung eines Gesamtdatenschutzkonzeptes für das Stadtamt begonnen werden. Maßgebliche Teilkonzepte (u. a. Waffenrecht, Gewerbe, Kfz-Zulassung) konnten in Zusammenarbeit mit der fidatas bremen als externer Projektunterstützung bereits fertig gestellt werden. Weitere Teilkonzepte, wie zum Beispiel zum Fachverfahren für das Meldewesen (MESO), stehen kurz vor der Fertigstellung. Die Verzögerungen bei der Erarbeitung des Rahmendatenschutz-

konzepts sind wesentlich auf den über Monate andauernden Streik zurückzuführen, der insbesondere die Einsatzfähigkeit des IT-Bereichs des Stadtamtes stark eingeschränkt hatte. Die Bestellung eines behördlichen Datenschutzbeauftragten nach § 7 a des Bremischen Datenschutzgesetzes ist am 22. Dezember 2005 erfolgt.

9.16 Einführung eines neuen DV-Verfahrens bei der Meldebehörde Bremen (S. 37 f.)

In der Stadtgemeinde Bremen ist als neues DV-Verfahren im Meldewesen das Programm „MESO“ eingeführt worden. Bremerhaven setzt dieses Programm bereits seit geraumer Zeit ein. Die Erstellung eines Datenschutzkonzeptes mit den erforderlichen Unterlagen unter Berücksichtigung der Besonderheiten des Meldewesens der Stadtgemeinde Bremen war aus Kapazitätsgründen vor Einführung des Verfahrens nicht möglich. Im Rahmen des Implementierungsprojekts des neuen Verfahrens war der Landesbeauftragte für den Datenschutz zu allen Sitzungen der Qualitätssicherungsgruppe eingeladen. Eine Teilnahme an diesen Sitzungen war dem Landesbeauftragten für den Datenschutz nicht möglich. Ebenfalls nicht in Anspruch genommen wurde ein vor Aufnahme des Echtbetriebs angebotenes Fachgespräch zu spezifischen verfahrensrechtlichen Aspekten des neuen Verfahrens. Anfang des Jahres wurde unverzüglich mit der Erstellung des Datenschutzkonzeptes begonnen. Dies steht kurz vor der Fertigstellung.

9.17 Fundinfo über das Internet (S. 38)

Die Verfahrensbeschreibung ist dem Landesbeauftragten für den Datenschutz im Februar 2006 übermittelt worden. Eine Rückäußerung liegt noch nicht vor.

9.18 Eingaben betreffend die Meldebehörde (S. 38 f.)

Nach § 21 des Bremischen Meldegesetzes (BremMeldG) ist die Meldebehörde bei Vorliegen von Anhaltspunkten für die Unrichtigkeit des Melderegisters verpflichtet, diesen nachzugehen. Verlässliche Informationen über den Verzug von Einwohnerinnen und Einwohnern werden dabei insbesondere auf Grundlage des § 20 BremMeldG über die wohnunggebende Person gewonnen. In dem dargestellten Fall ist diese Ermittlungsvariante nicht genutzt worden. Der Bürger wurde allein aufgrund einer Information von Nachbarn abgemeldet. Eine anschließende Überprüfung ergab jedoch, dass die Information über den Verzug des Betroffenen unzutreffend war. Dieser Fall wurde zum Anlass genommen, die zuständigen Mitarbeiterinnen und Mitarbeiter in der Meldebehörde darauf hinzuweisen, dass die Fortschreibung des Melderegisters nur zu erfolgen hat, wenn gesicherte und verlässliche Informationen über die Unrichtigkeit des Melderegisters vorliegen, unter anderem durch eine vorherige Ermittlung bei der wohnunggebenden Person.

Die Erteilung einer Melderegisterauskunft nach § 32 BremMeldG setzt voraus, dass die Person, zu der eine Auskunft verlangt wird, hinreichend eindeutig bestimmt werden kann. Es genügen auch unvollständige Identifizierungsangaben, wenn diese für sich genommen eine hinreichend eindeutige Bestimmung ermöglichen. Dies ist zum Beispiel der Fall, wenn die Auskunft verlangende Person lediglich über den Namen der gesuchten Person verfügt und diese nur einmal im Melderegister verzeichnet ist. Sofern neben dem Vor- und Familiennamen der Straßenname als weiteres Identifizierungsmerkmal angegeben wird und unter diesem Straßennamen keine weitere Person gleichen Namens gemeldet ist, steht auch die Angabe einer falschen Hausnummer einer Auskunftserteilung nicht entgegen. Generell sind alle vorliegenden Identifizierungsmerkmale vor Erteilung einer Melderegisterauskunft zu überprüfen. In dem im Jahresbericht geschilderten Fall ist dies nicht geschehen, was zu der beschriebenen Verwechslung und in der Folge zu einer mit § 32 BremMeldG nicht in Einklang stehenden Erteilung einer Melderegisterauskunft geführt hat. Die Meldebehörde hat diesen Fall noch einmal zum Anlass genommen, die zuständigen Mitarbeiterinnen und Mitarbeiter darauf hinzuweisen, dass zur Identifizierung von Personen, zu de-

nen eine Auskunft verlangt wird, alle vorliegenden Daten heranzuziehen sind, um Verwechslungen auszuschließen.

9.20 Veröffentlichung von Daten von Beiratsmitgliedern und „Fachberatern“ im Internet

Ausschüsse der Beiräte tagen gemäß § 22 Abs. 1 des Ortsgesetzes über Beiräte und Ortsämter grundsätzlich nicht öffentlich. Der Beirat hat aber die Möglichkeit, bestimmte Angelegenheiten Ausschüssen widerruflich zur endgültigen Beschlussfassung zu übertragen. Da in diesen Einzelfällen eine öffentliche Beratung erfolgt, trifft die im Jahresbericht getroffene Aussage, dass „die so genannten sachkundigen Bürger nur in nicht öffentlichen Sitzungen der Fachausschüsse in Erscheinung treten“ nicht zu.

Unter dem Gesichtspunkt der allgemeinen Aufgaben eines Beirats und seiner Ausschüsse wird es sich gegenüber der Bevölkerung kaum vermitteln lassen, dass ein Mandatsträger (und dazu zählen auch die Mitglieder eines Ausschusses), der sich z. B. mit den aus der Bevölkerung kommenden Wünschen, Anregungen und Beschwerden befassen sowie die im Beiratsbereich arbeitenden Institutionen, Vereine, Initiativen und sonstigen demokratischen Vereinigungen im Sinne eines Interessenausgleichs unterstützen soll, aus rein datenschutzrechtlichen Erwägungen heraus weitgehend anonym seiner Gremienarbeit nachgehen kann.

Der im Jahresbericht aufgeführte Einzelfall soll zum Anlass genommen werden, mit den in den Beiräten vertretenen Parteien zu erörtern, ob die Mitwirkung von so genannten sachkundigen Bürgerinnen und Bürgern in der Ausschussarbeit von einer Einwilligung der Bekanntgabe (Veröffentlichung) bestimmter Daten (Namen, Anschrift, Telefonnummer oder E-Mail-Adresse) abhängig gemacht werden soll, da nur so die Erreichbarkeit dieser Personen für die Bürgerinnen und Bürger in Beiratsangelegenheiten ermöglicht werden kann.

11. Gesundheit und Krankenversicherung

11.2 Neues zur elektronischen Gesundheitskarte (S. 44 f.)

Die Notwendigkeit der Einbindung des Landesbeauftragten für den Datenschutz bei der Erprobung und Einführung der elektronischen Gesundheitskarte ist mit Blick auf die Qualität und die Quantität der datenschutzrechtlichen und technischen Fragen unstrittig. Deswegen wurde er um Begleitung des Vorhabens gebeten. Im Hinblick auf seine nicht ausreichenden personellen Ressourcen hat er um Unterstützung aus Projektmitteln nachgesucht. Dem kann jedoch nicht entsprochen werden. Das Projekt finanziert sich aus Mitteln der Projektpartner aus der Selbstverwaltung vor Ort und aus Mitteln der gematik mbH, einer Gesellschaft der Selbstverwaltung, die auf Bundesebene das Projekt „Testregion“ umsetzen wird. Eine Refinanzierung der Personalkosten beim Landesbeauftragten für den Datenschutz aus dem Projektbudget ist, wie auch in den anderen Testregionen, nicht vorgesehen. Zwischen dem Landesbeauftragten für den Datenschutz und der Projektgeschäftsstelle der BIT (Bremer Initiative Telematik im Gesundheitswesen) hat es unbeschadet dessen Gespräche auf der Arbeitsebene gegeben.

11.3 Mammographie-Screening (S. 45 f.)

Bezüglich der Bildung einer Screening-ID sowie zum Abgleich mit dem Bremer Krebsregister laufen weiterhin Gespräche mit dem Landesbeauftragten für den Datenschutz, dem zuletzt am 31. Juli 2006 aktualisierte Unterlagen zum Datenschutzkonzept vorgelegt wurden. Die Zuordnung von Daten zu einer eindeutigen Screening-ID erfolgt nach erneutem Einlesen von Meldeamtsdaten. Zwischen den Einladungsintervallen werden die persönlichen Daten der Frauen gelöscht.

Die zentrale Einladungsstelle beim Gesundheitsamt Bremen wird die Problematik der Bildung der Screening-ID den bundesweiten Gremien zur Kenntnis geben.

11.4 Tumordokumentationszentrum (S. 46 f.)

Das Verfahren ruht zurzeit. Dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales sowie den beteiligten Partnern war und ist jedoch sehr daran gelegen, den Landesbeauftragten für den Datenschutz bereits in konzeptionelle Vorüberlegungen einzubinden.

11.6 Rechtswidrige Datenübermittlung durch zwei Krankenkassen (S. 48 f.)

Im November 2005 hatte die AOK Bremen/Bremerhaven um eine aufsichtliche Stellungnahme zu der Problematik der Datenübermittlung an das Bundesministerium für Wirtschaft und Arbeit (BMWA) gebeten. Zuvor war seitens des BMWA und der AOK Bremen/Bremerhaven die Auffassung vertreten worden, die einzelnen Krankenkassen seien datenschutzrechtlich berechtigt, dem BMWA die Daten derjenigen Fälle zur Verfügung zu stellen, in denen sie – anders als die zuständigen Stellen nach dem SGB II – davon ausgingen, dass keine Erwerbsfähigkeit im Sinne des SGB II und damit keine Pflichtversicherung in der GKV bestünden.

Mit Schreiben vom 5. Dezember 2005 wurde der Landesbeauftragte für den Datenschutz um Mitteilung seiner Rechtsauffassung gebeten. Seine Äußerung erfolgte mit Schreiben vom 15. Dezember 2005. Am 9. Januar 2006 wurde der AOK in Übereinstimmung mit der Auffassung des Landesbeauftragten für den Datenschutz mitgeteilt, dass sich die Datenübermittlung an dem Prinzip der Erforderlichkeit messen lassen müsse und dass angesichts der bilateral vor Ort geführten Klärung der Anspruchsberechtigung auf Arbeitslosengeld II die Übermittlung von Daten – insbesondere von Diagnosen – an das BMWA bzw. das Bundesministerium für Arbeit und Soziales (BMAS) nicht erforderlich und damit auch nicht zulässig sei.

12. Arbeit und Soziales

12.1 Datenerhebung bei Arbeitslosengeld-II-Empfängern durch Call-Center (S. 49 f.)

Die telefonische Befragung basierte auf einem Angebot der Bundesagentur für Arbeit (BA) zur Statusklärung von ALG-II-Empfängern. Ziel war die Entlastung der Vermittler bei zeitaufwendigen Sachbearbeitungstätigkeiten. In einer ersten Befragung wurden auch private Call-Center eingeschaltet, die aber keinen Zugriff auf personenbezogene Datensätze hatten. Diese lagen nur beim Service- und Support-Center (SSC) der BA. Mittlerweile wurde die Kritik der Datenschutzbeauftragten dahingehend aufgegriffen, dass keine privaten Call-Center mehr eingeschaltet werden. Weiterhin werden die betroffenen Personen bei einer Telefonbefragung vorab schriftlich informiert und dabei ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen.

12.2 Einsatz des A2LL-Verfahrens bei der BAgIS (S. 50 f.)

Die von den Datenschutzbeauftragten vorgetragene Kritik wird nach Kenntnis des Senats vom Bundesministerium für Arbeit und Soziales (BMAS) und von der Bundesagentur für Arbeit (BA) grundsätzlich anerkannt; es gibt aber offensichtlich noch Probleme in der praktischen Umsetzung. Da es sich bei dem A2LL-Verfahren um ein bundeseinheitlich vorgegebenes Verfahren handelt, das regional nicht modifizierbar ist, liegt die Zuständigkeit für die Beseitigung der Mängel beim BMAS und der BA.

12.3 JobCard – der Weg zum „gläsernen Arbeitnehmer“ (S. 51 f.)

Die JobCard soll – ähnlich wie die Chipkarte in der gesetzlichen Krankenversicherung –, zu einer Vereinfachung von Verwaltungsvorgängen für Arbeitssuchende und Mitarbeiter der Bundesagentur für Arbeit (BA), etwa bei der Arbeitslosmeldung, beitragen. Da eine solche JobCard bundeseinheitlich eingeführt werden soll, liegt die datenschutzrechtliche Zuständigkeit bei dem Bundesministerium für Arbeit und Soziales (BMAS), der BA und dem Bundesbeauftragten für den Datenschutz.

13. Bildung und Wissenschaft

13.1 Datenschutz im Hochschulbereich (S. 52)

Die Darstellung ist im Wesentlichen korrekt. Es ist allerdings darauf hinzuweisen, dass der unter Hinzuziehung des zuständigen Mitarbeiters des Landesbeauftragten für den Datenschutz erarbeitete Entwurf einer Änderungsverordnung zum Datenschutz im Hochschulbereich für § 11 des Bremischen Hochschulgesetzes (BremHG) in der geltenden Fassung durchaus für vereinbar gehalten wurde. Die in Folge zahlreicher neuer Anforderungen erweiterte Datenverarbeitung durch die Hochschulen hätte damit relativ kurzfristig auf eine tragfähige Rechtsgrundlage gestützt werden können. Aufgrund der in einem sehr späten Stadium der beabsichtigten Rechtsanpassung erhobenen Bedenken des zuständigen Mitarbeiters des Landesbeauftragten für den Datenschutz hat sich der Senator für Bildung und Wissenschaft dazu entschlossen, den Zustand der nicht hinreichend konkretisierten Rechtsgrundlagen für einen möglichst kurzen Übergangszeitraum weiterhin hinzunehmen und eine grundsätzliche Novellierung der datenschutzrechtlichen Bestimmungen mit der nächsten BremHG-Novelle vorzunehmen. Angestrebt wird dabei unter anderem, den Erlass der erforderlichen Rechtsvorschriften weitgehend auf die Hochschulen zu delegieren und auf eine Rechtsverordnung des Senators für Bildung und Wissenschaft künftig vollständig zu verzichten. In der Folgezeit ist in enger Abstimmung mit dem Landesbeauftragten für den Datenschutz und den Hochschulen eine entsprechende Datenschutzregelung innerhalb des Hochschulreformgesetzes entwickelt worden und befindet sich zurzeit im offiziellen Gesetzgebungsverfahren. Die neuen datenschutzrechtlichen Bestimmungen sollen noch im Laufe dieses Jahres in Kraft treten.

13.3. Novellierung des bremischen Schuldatenschutzgesetzes (S. 53)

Der Entwurf eines neuen Schuldatenschutzgesetzes befindet sich in der ressortübergreifenden Endabstimmung. Ziel dieser Abstimmung ist es, die Bestimmungen dieses Gesetzes mit den bereichsspezifischen Datenübermittlungsregelungen der anderen Fachgesetze kompatibel zu halten. Hier gibt es noch Dissense, die im weiteren Verlauf des Gesetzgebungsverfahrens geklärt werden müssen.

13.4 Prüfung des Schuldatenverwaltungsverfahrens MAGELLAN (S. 53 ff.)

Die im Bericht aufgeführten Mängel für einen datenschutzgerechten Betrieb des Systems werden durch mit dem Landesbeauftragten für den Datenschutz abgestimmte Maßnahmen bis Oktober 2006 abgestellt. Die Abstimmung hat bereits stattgefunden.

Die für die Eingabekontrolle, die Protokollierung der Benutzeraktivitäten sowie die Revision erforderlichen technischen und administrativen Maßnahmen sind in der in Bremen erstmalig umgesetzten flächendekkenden Lösung ein Novum. Sie mussten erst entwickelt werden und befinden sich jetzt in der technischen Umsetzung.

Der für die angestrebte pseudonymisierte Datenbank vom Landesbeauftragten für den Datenschutz zunächst vorgeschlagene Hash-Algorithmus lässt sich wegen technischer Schwierigkeiten nicht umsetzen. Hier ist eine mit dem Landesbeauftragten abgestimmte andere Lösung realisiert worden. Es wird täglich eine zufallsgesteuerte sowie unter Benutzung eines komplizierten Algorithmus erstellte ID erzeugt, die eine Re-Identifikation praktisch unmöglich macht.

Bis Oktober 2006 wird dem Landesbeauftragten für den Datenschutz eine Verfahrensbeschreibung mit ausreichenden Informationen für eine datenschutzrechtliche Bewertung vorgelegt.

15. Finanzen

15.1 Kontodatenabrufe nach § 24 c KWG und §§ 93, 93 b AO (S. 55 f.)

Die bremischen Finanzämter machen nach wie vor zurückhaltenden Gebrauch von der Kontenabfragemöglichkeit nach §§ 93, 93 b der Ab-

gabenordnung (AO). Die bestehenden einschränkenden Anweisungen werden gegebenenfalls erst nach der anstehenden Entscheidung des Bundesverfassungsgerichts modifiziert.

16. Häfen

16.1 Zuverlässigkeitsüberprüfungsverordnung

Es ist unstrittig, dass der Senat eine Verordnung über die Zuverlässigkeitsüberprüfung nach dem Hafensicherheitsgesetz erlassen wird.

Weder der Bund für die Luftsicherheit noch der Wettbewerbshafen Hamburg für die Hafensicherheit haben bisher derartige Verordnungen erlassen. Die bremische Verordnung wird sich inhaltlich und zeitlich an diesen Verordnungen orientieren. Von einer Verzögerung kann nicht die Rede sein.

17. Bremerhaven

Siehe Stellungnahmen zu Tz. 5.1, 9.6, 9.8 und 11.6.

Druck: Anker-Druck Bremen