SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 15/2287**
15. Wahlperiode 02-11-26

Antwort

der Landesregierung

auf die

Große Anfrage

der Fraktion der SPD

Datenschutzpolitik für Schleswig-Holstein

Drucksache 15/1995

Federführend ist der Innenminister

Vorbemerkung der Fragesteller:

Die Zunahme der Nutzung von Medien wie E-Mail, Internet und E-Commerce rückt den Datenschutz immer mehr in den Blickpunkt. Darüber hinaus haben sich die technischen Möglichkeiten zur Überwachung verbessert. Die Sorge vor der Entwicklung der Kriminalität ruft immer wieder Diskussionen über die Abwägung zwischen Datenschutz und Strafverfolgung hervor. Hinzu kommt die öffentliche Debatte um die sogenannten “Sicherheitspakete” der Bundesregierung nach den Terroranschlägen des 11. September 2001.

Frage 1

Wie beurteilt die Landesregierung vor dem Hintergrund des sogenannten “Volkszählungsurteils” die Verwirklichung des Rechts auf informationelle Selbstbestimmung in Schleswig-Holstein?

Antwort:

Das Recht auf informationelle Selbstbestimmung, das den Schutz des Einzelnen gegen unbegrenzte Datenerhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten umfasst, wird in Schleswig- Holstein in hohem Maße verwirklicht.
Mit dem neuen Landesdatenschutzgesetz (LDSG) vom 1. Juli 2000 wurde nicht nur die Europäische Datenschutzrichtlinie umgesetzt, sondern darüber hinaus wurden auch zeitgemäße Datenschutzbestimmungen eingeführt, die den Grundrechtsschutz gewährleisten. Hierzu gehören u.a. die gesetzliche Verpflichtung der Behörden zur Datenvermeidung und Datensparsamkeit, die Privilegierung der Verarbeitung anonymisierter oder pseudonymisierter Daten, die Förderung datenschutzfreundlicher Produkte sowie die Verschlüsselung von Daten bei einer Bearbeitung außerhalb der Dienststelle. Darüber hinaus hat die Service- und Beratungstätigkeit des Unabhängigen Landeszentrums für Datenschutz (ULD) gegenüber den Bürgerinnen und Bürgern als auch gegenüber den Behörden und nicht-öffentlichen Stellen besonderes Gewicht erhalten. Die Aufsicht für den öffentlichen und den nicht-öffentlichen Bereich wurde zusammengelegt und mit der Bündelung eine effektive Aufgabenerledigung durch das ULD ermöglicht.
Neben den Regelungen des LDSG wird das Recht auf informationelle Selbstbestimmung in zahlreichen bereichsspezifischen Gesetzen und Landesverordnungen umge-

setzt. Die Datenverarbeitung orientiert sich in diesen Fällen an speziellen Zweckbestimmungen, gleichermaßen werden Datenschutz und Datensicherheit an die speziellen fachlichen Erfordernisse angepasst. Die Datenverarbeitung wird durch die bereichsspezifischen Regelungen für die Bürgerinnen und Bürger transparenter; mögliche Beschränkungen der informationellen Selbstbestimmung sind erkennbar und nachvollziehbar. In der Gesetzgebung ist es stets erforderlich zwischen der sachlichen Notwendigkeit der Verarbeitung personenbezogener Daten und dem Recht auf informationelle Selbstbestimmung abzuwägen.
Darüber hinaus trägt auch die Funktion der behördlichen Datenschutzbeauftragten zu mehr Datenschutz und Datensicherheit bei, indem ein effektiver Datenschutz „vor Ort" gewährleistet wird. Die Landesregierung hat insbesondere im Polizeibereich frühzeitig gut ausgebildete behördliche Datenschutzbeauftragte bestellt. Wenngleich das LDSG keine Verpflichtung zur Bestellung enthält, wird nach Auffassung der Landesregierung mit fortschreitender automatisierter Datenverarbeitung auch die Bestellung von Datenschutzbeauftragten zunehmen.

Frage 2

Welche personenbezogenen Dateien nach § 11 (3) Landesdatenschutzgesetz werden bei der Landesregierung geführt?
Wie sind die Zugriffsmöglichkeiten zu diesen Dateien?
Inwieweit haben erfasste Personen ein Recht auf Einsicht in diese Dateien?

Antwort:

Die bei der Landesregierung geführten personenbezogenen Dateien nach § 11 Abs. 3 Landesdatenschutzgesetz (LDSG), die Zugriffsmöglichkeiten und die Einsichtsrechte sind nachstehend aufgeführt.
Nicht erfasst sind die Dateien, die aufgrund einer Datenverarbeitung nach § 11 Abs. 5 LDSG erstellt werden.

Ressort	**Welche personenbezogenen Dateien nach § 11 (3) LDSG werden bei der Landesregierung geführt?**	**Wie sind die Zugriffsmöglichkeiten zu diesen Dateien?**	**Inwieweit haben erfasste Personen ein Recht auf Einsicht in diese Dateien?**
alle Ressorts	Datei PERMIS-V (Personalmanagement und Informationssystem- Verwaltung)	passwortgeschützter Zugang durch zuständige Sachbearbeiter/innen	Einsichtnahme durch Beschäftigte in die sie betreffenden Daten
StK	Datei über personenbezogene Daten von Petentinnen/ Petenten	passwortgeschützter Zugang nur durch zuständige Sachbearbeiter/innen/	Einsichtnahme durch Petentinnen/ Petenten in ihre/ seine Daten
MJF	Dateien nach dem Buchungs- und Abrechnungssystem im Strafvollzug (BASIS)	zuständiges Vollzugspersonal der jeweiligen Justizvollzugsanstalt	Jede/ jeder Gefangene erhält einen Ausdruck ihres/ seines Vollstreckungsblattes
MBWFK	Datei PERLE (Personalverwaltung Lehrkräfte)	passwortgeschützter Zugang durch zuständige Sachbearbeiter/innen	Einsichtnahme durch Beschäftigte in die sie betreffenden Daten
IM	1. Datei über die Erfassung schwerbehinderter Bewerber/innen	1. passwortgeschützter Zugang durch zuständige Sachbearbeiter/innen	1. Einsichtnahme durch Bewerber/innen in ihre/ seine Daten
	2. Datei über Auszubildende zur/zum Verwaltungsfachangestellten und Funktionsebene des gehobenen Dienstes	2. zuständige Sachbearbeiter/innen[1]	2. Einsichtnahme durch Auszubildende in die sie betreffenden Daten

[1] Es handelt sich um eine manuell geführte Datei, die unter Verschluss ist.

Ressort	**Welche personenbezogenen Dateien nach § 11 (3) LDSG werden bei der Landesregierung geführt?**	**Wie sind die Zugriffsmöglichkeiten zu diesen Dateien?**	**Inwieweit haben erfasste Personen ein Recht auf Einsicht in diese Dateien?**
	3. Disziplinarregister[2]	3. passwortgeschützter Zugang durch zuständige Sachbearbeiter/innen und Referatsleitung	3. Einsichtnahme durch Betroffene in die sie betreffenden Daten
	4. Datei Wohnungssuchende (im Rahmen der Wohnungsfürsorge)	4. passwortgeschützter Zugang durch zuständige Sachbearbeiter/innen	4. Einsichtnahme durch Betroffene in die sie betreffenden Daten
	5. Datei über heilfürsorgeberechtigte Polizeibeamtinnen und Polizeibeamte	5. passwortgeschützter Zugang durch zuständige Sachbearbeiter/innen	5. Einsichtnahme durch Betroffene in die sie betreffenden Daten
MFE	Datei über Personal in Kernkraftwerken	zuständige Sachbearbeiter/innen	Einsichtnahme durch Betroffene in die sie betreffenden Daten

[2] Bis Ende 2001 wurde das Register manuell geführt; diese Datei ist unter Verschluss.

Frage 3

Welche Position hat die Landesregierung bei der letzten Novelle zum Bundesdatenschutzgesetz eingenommen?
Inwieweit fand diese Position Berücksichtigung?
Welche weiteren Reformnotwendigkeiten sieht die Landesregierung in Bezug auf das Datenschutzrecht und wie wirkt sich das neue Recht auf das Land aus?

Antwort:

Eine Kernforderung der Schleswig-Holsteinischen Landesregierung bei der Novellierung des Bundesdatenschutzgesetzes (BDSG) war und ist, ein übersichtliches, lesbares und anwenderfreundliches Gesetz zu schaffen, das aufwendige Verfahren nur vorsieht, wenn sie zur Gewährleistung schutzwürdiger Interessen der Betroffenen unbedingt erforderlich sind. Dieser Forderung wurde in der ersten Stufe der Novellierung nur teilweise entsprochen, weil an der Trennung der Rechtsvorschriften für den öffentlichen und nicht-öffentlichen Bereich festgehalten wurde. Trotz der bestehenden Unzulänglichkeiten bei der ersten Novellierungsstufe hat die Landesregierung diese letztlich mitgetragen, weil zunächst die lange überfällige Anpassung an die EG-Datenschutzrichtlinie vordringlich war. Die Landesregierung sieht den weiteren Änderungsbedarf und wird sich daher in der zweiten Stufe der Novellierung nachdrücklich für ein schlankes, verständliches und anwenderfreundliches Gesetz einsetzen.

Die Einführung eines Datenschutzaudits wurde entgegen der nachhaltigen Bedenken der meisten anderen Länder von der Landesregierung unterstützt, weil hierin ein wirksames Instrument zur Verbesserung des Datenschutzes und der Datensicherheit gesehen wird. Umso mehr wird die Aufnahme des Datenschutzaudits in § 9 a BDSG begrüßt.

Die Erweiterung der Anordnungs- und Untersagungsbefugnisse der Aufsichtsbehörden für den nicht-öffentlichen Bereich (§ 38 BDSG) war ebenfalls eine zentrale Position der Landesregierung im Novellierungsverfahren. Die bisherige Beschränkung dieser Befugnisse auf technische oder organisatorische Datenschutzverstöße sollte um materielle Verstöße, z.B. bei unzulässiger kommerzieller Datenverarbeitung, erweitert werden.

Diese Forderung wurde nur soweit umgesetzt, als eine Neuregelung der Straf- und Bußgeldvorschriften vorgenommen wurde. Bußgeldvorschriften wurden um bisherige Straftatbestände ergänzt, so dass sich der Handlungsspielraum der Aufsichtsbehörden bei der Verfolgung von Ordnungswidrigkeiten erhöht hat.

Die Regelungen für die Übermittlung personenbezogener Daten ins Ausland und die damit verbundene Differenzierung in Mitgliedstaaten der Europäischen Union und andere ausländische Staaten sowie die Ausnahmeregelungen wurden von der Landesregierung für unübersichtlich und in der Anwendung für zu aufwendig und unpraktikabel gehalten. Diese Auffassung wurde vom Bundesgesetzgeber nicht geteilt. Zwischenzeitlich haben sich jedoch bei der Anwendung dieser gesetzlichen Bestimmungen deutliche Probleme zur Auslegung eines angemessenen Datenschutzniveaus, zum Erfordernis der Genehmigung der Datenübermittlung ins Ausland sowie zu Vertragsklauseln oder verbindlichen Unternehmensregelungen gezeigt. Die Länder vertreten hierzu geteilte Auffassungen; die Diskussion ist noch nicht beendet.

Die Europäische Kommission hat bisher nur für einzelne Staaten eine Entscheidung über ein angemessenes Datenschutzniveau getroffen (Ungarn, Schweiz, und im begrenzten Umfang für Kanada), insofern bestehen viele Auslegungsschwierigkeiten fort. Die Landesregierung sieht daher die Notwendigkeit, diese Regelungen in der zweiten Novellierungsstufe des BDSG zu überarbeiten und für die datenübermittelnde und die datenempfangende Stelle sowie für die Aufsichtbehörden in ihrer Funktion als Genehmigungsbehörde praktikable Regelungen zu schaffen.
Für die Umsetzung des aufgezeigten Reformbedarfs des BDSG wird sich die Landesregierung in der zweiten Novellierungsstufe einsetzen. Das vom BMI in Auftrag gegebene Gutachten zur Modernisierung des Datenschutzrechts lässt ehrgeizige Modernisierungsansätze erkennen, die unterstützt werden, zumal einige zum Teil schon mit dem schleswig-holsteinischen Landesdatenschutzgesetz umgesetzt wurden. Das Ziel, durch die Neuregelung des BDSG die bereichsspezifischen Normen auf das notwendige Maß zu beschränken, wird befürwortet, wenngleich eine Abkehr vom bisherigen Vorrang bereichsspezifischer Regelungen schwierig sein dürfte. Auch die beabsichtigte Stärkung

der Position der behördlichen und betrieblichen Datenschutzbeauftragten wird unterstützt.
Die mit dem neuen BDSG vorgenommenen Änderungen (z.B. Erweiterung der Schutz- und Informationsrechte der Betroffenen, Meldepflicht nur für automatisierte Verfahren, Regelungen über Videoüberwachung und Chipkarten) haben einen erhöhten Informationsbedarf der Bürgerinnen und Bürger sowie der Wirtschaftsunternehmen in Schleswig-Holstein ausgelöst.
Das ULD hat u.a. in Zusammenarbeit mit der Industrie- und Handelskammer und Verbänden Informationsveranstaltungen durchgeführt und Veröffentlichungen vorgenommen.
Inwieweit sich die Anwendung der neuen gesetzlichen Regelungen in Schleswig-Holstein auswirken wird, bleibt abzuwarten. Bereits jetzt kann jedoch gesagt werden, dass die mit dem neuen BDSG eingeführte anlassunabhängige Kontrolltätigkeit der Aufsichtbehörden im nicht-öffentlichen Bereich zu einer Aufgabenvermehrung beim ULD geführt hat. Bei den Wirtschaftsunternehmen dürfte dies mit einem „Umdenken“ verbunden sein, weil nun mit unvorhergesehenen Prüfungen durch das ULD zu rechnen ist.

Frage 4

Welche Position hat die Landesregierung bei der Beschlussfassung über das Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses (G-10-Gesetz) eingenommen?
Inwieweit fand diese Position Berücksichtigung?

Antwort:

Die Landesregierung hat in der Sitzung des Bundesrates am 1. Juni 2001 dem Gesetzentwurf der Bundesregierung in der vom Bundestag am 11. Mai 2001 beschlossenen Fassung zugestimmt.
Der Feststellung des Bundesrates, dass das Gesetz gemäß Artikel 84 Abs. 1 des Grundgesetzes der Zustimmung bedarf, wurde beigetreten.
Eine Abstimmung über eine Reihe von Anträgen, die über den Gesetzentwurf der Bundesregierung hinausgingen, erübrigte sich, da der Antrag auf Einberufung des Vermittlungsausschusses im Bundesrat keine Mehrheit fand. Die Novellierung des Artikel 10-

Gesetzes macht eine Anpassung des schleswig-holsteinischen Ausführungsgesetzes erforderlich; sie ist in Vorbereitung.

Frage 5

Welche internationalen Vereinbarungen zum Datenschutz bestehen und welche Entwicklungen zeichnen sich ab?
Wie steht die Landesregierung zum freien Datenverkehr mit Nicht-EU-Ländern vor dem Hintergrund eines Unterschiedlichen Niveaus beim Datenschutz.
Gibt es Bestrebungen, das Thema “Datenschutz” auch im Rahmen der Ostseekooperation zu bearbeiten?
Sieht sich die Landesregierung ausreichend beteiligt bei der Erörterung internationaler Vereinbarungen im Bereich des Datenschutzes?
Sieht die Landesregierung die Gefahr, dass datenschutzrechtliche Standards auf internationaler Ebene im Interesse der Kriminalitätsbekämpfung gesenkt werden?

Antwort:

Von einer Aufzählung aller internationaler Vereinbarungen zum Datenschutz wird abgesehen. Die Antwort beschränkt sich auf folgende wichtige internationale datenschutzrechtliche Vereinbarungen:

- Leitlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980,

- Richtlinie betreffend personenbezogene Daten in automatisierten Dateien (von der Generalversammlung der Vereinten Nationen am 14. Dezember 1990 beschlossen),

- Europäische Datenschutzrichtlinie (Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr),

- Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 18. November 1999,

- Richtlinie über den elektronischen Geschäftsverkehr (Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt)

- Verordnung (EG) Nr.45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr,

- Verordnung über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission vom 30. Mai 2001,

- Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten sowie den Änderungen vom 15. Juni 1999 und dem Zusatzprotokoll vom 8. November 2001 zu diesem Übereinkommen,

- Europäische Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation).

Die genannten Vereinbarungen wurden bzw. werden - soweit erforderlich - von der Bundesregierung und ggf. den Ländern in nationales Recht umgesetzt. Darüber hinaus gibt es zahlreiche Abkommen und Verträge über datenschutzrechtliche Regelungen. Die Europäische Kommission hat auf der Grundlage der EU- Datenschutzrichtlinie Entscheidungen über die Anerkennung eines angemessenen Datenschutzniveaus für einzelne Länder, wie Ungarn, Schweiz, Kanada und die USA (sog. „Safe-Habor“-

Regelung) getroffen. Weiterhin existieren Standardvertragsklauseln der Europäischen Kommission für Datenübermittlungen in Drittländer. Die Vereinbarungen haben u.a. den Zweck, auf internationaler Ebene ein möglichst einheitliches Datenschutzniveau zu erreichen. Nach Einschätzung der Landesregierung werden auch künftig weitere datenschutzrechtliche Vereinbarungen erforderlich werden, um in einer globalen Informations- und Kommunikationsgesellschaft ein Mindestmaß an Datenschutz und Datensicherheit beim internationalen Datentransfer zu gewährleisten. Dies bedingt aber auch eine Umsetzung der internationalen Vereinbarungen in nationales Recht, um damit deren Verbindlichkeit sicherzustellen.

Bei einer **Datenübermittlung in Nicht-EU-Länder** muss grundsätzlich ein angemessenes Datenschutzniveau gewährleistet sein. Die Landesregierung hält die gesetzliche Regelung in § 4 b Abs. 2 und 3 BDSG für notwendig, um ein Mindestmaß an datenschutzrechtlichem Standard sicherzustellen. Die Beurteilung der Angemessenheit des Datenschutzniveaus ist unproblematisch, sofern die Europäische Kommission ein angemessenes Datenschutzniveau für einzelne Staaten anerkannt hat (z.B. Ungarn, Schweiz, Kanada) oder die Datenübermittlung auf der Grundlage der von der Europäischen Kommission herausgegebenen Standardvertragsklauseln durchgeführt wird. Auslegungsschwierigkeiten können sich jedoch für die übermittelnde Stelle ergeben, wenn die genannten Voraussetzungen nicht vorliegen.

Die im BDSG für diesen Fall vorgesehenen Ausnahmeregelungen hält die Landesregierung für angemessen und in der Praxis für anwendbar, soweit es sich um die Ausnahmetatbestände nach § 4 c Abs. 1 BDSG handelt. Also beispielsweise in den Fällen, in denen der Betroffene der Datenübermittlung eingewilligt hat, die Übermittlung zur Vertragserfüllung mit dem Betroffenen erforderlich ist oder wichtige öffentliche Interessen überwiegen.

Die Ausnahmeregelung in § 4 c Abs. 2 BDSG, die durch eine Genehmigung der zuständigen Aufsichtsbehörde erfolgen kann, wenn die datenübermittelnde Stelle ausreichende Garantien in Form von Vertragsklauseln oder verbindlichen Unternehmensregelungen vorweist, hält die Landesregierung in der Anwendbarkeit für schwierig. Einerseits sind bei internationalen Unternehmen mit Tochterunternehmen in Nicht EU-Ländern mit unterschiedlichem Datenschutzniveau Probleme bei der Durchsetzung verbindlicher Unternehmensregelungen für alle Teilunternehmen denkbar. Andererseits

können unterschiedliche Auslegungen bei der Genehmigung von Datenübermittlungen aufgrund von verbindlichen Unternehmensregelungen auftreten.
Nach den Erfahrungen des ULD wird von schleswig-holsteinischen Unternehmen mit Datentransfer in Nicht EU-Länder häufig nicht die Einwilligung des Betroffenen eingeholt, obwohl die anderen Ausnahmetatbestände nicht erfüllt sind. Das ULD geht beim internationalen Datentransfer von Vollzugsdefiziten aus und sieht diese insbesondere bei der Übermittlung von Arbeitnehmerdaten.
Die Landesregierung teilt diese Einschätzung hinsichtlich der Vollzugsdefizite, sieht aber auch einen Grund dafür in der kurzen Anwendungszeit dieser gesetzlichen Regelungen.
Die Landesregierung beabsichtigt zurzeit nicht, das Thema „Datenschutz“ im Rahmen der **Ostseekooperation** zu behandeln.

Bei der **Erörterung internationaler Vereinbarungen im Bereich des Datenschutzes** wirkt die Landesregierung über die Ständige Vertragskommission der Länder, über die Ländervertreter in Angelegenheiten der Europäischen Union sowie über den Bundesrat mit. Sie sieht sich hierdurch ausreichend beteiligt.

Die Bemühungen um **Standardisierung auf internationaler Ebene im Interesse der Kriminalitätsbekämpfung** sind richtig und wichtig. Die Landesregierung sieht durchaus die Gefahr, dass aufgrund der Bedrohungslage durch den internationalen Terrorismus und die grenzüberschreitende organisierte Kriminalität datenschutzrechtliche Standards auf internationaler Ebene gesenkt werden könnten. Deshalb muss insbesondere im Bereich der internationalen Kriminalitätsbekämpfung, die ohne Mitwirkung und Beteiligung der Bürgerinnen und Bürger in ihrer Wirksamkeit beeinträchtigt würde, großer Wert auf Akzeptanz der Instrumente der Kriminalitätsbekämpfung gelegt werden. Diese Akzeptanz setzt einen Datenschutzstandard voraus, welche der Bevölkerung einen ausreichenden und sichtbaren Schutz der Privatsphäre sichert. Deshalb wäre eine Nivellierung der internationalen Standards auf einem niedrigeren Datenschutzniveau für die Zwecke der Strafverfolgung nicht sinnvoll. Bei Verhandlungen über den Abschluss internationaler Vereinbarungen zur Kriminalitätsbekämpfung ist deshalb ein ausgewogener

Kompromiss zwischen nationalen und internationalen datenschutzrechtlichen Standards herzustellen.

Frage 6

Welche Richtlinien und Vorhaben zur internationalen Kriminalitätsbekämpfung bestehen und wie wirken sie sich auf das bestehende deutsche Datenschutzrecht aus, bzw. wie werden sie sich auswirken (z.B. EU-Cyber-Crime-Convention)?

Antwort:

Der in der Fragestellung verwandte Begriff der **"Richtlinie"** ist in zweifacher Hinsicht belegt. National wird er als Synonym für Verwaltungsvorschriften gebraucht. Im Bereich der Europäischen Gemeinschaft kennzeichnet er für die Mitgliedstaaten verbindliche Rechtsakte, ähnlich den Rahmengesetzen nach deutschem Verfassungsrecht. Richtlinien in diesem Sinne gibt es allerdings im Bereich der sog. Dritten Säule des EU-Vertrages, welche die hier einschlägigen "Bestimmungen über die polizeiliche und justizielle Zusammenarbeit in Strafsachen" beinhaltet, nicht. Insoweit ist es bei der sog. intergouvernementalen Zusammenarbeit verblieben. Unter Berücksichtigung dessen wird davon ausgegangen, dass die Fragestellung nicht auf "Richtlinien" in diesem Sinne, sondern allgemein auf "Regelungen" zur internationalen Kriminalitätsbekämpfung abzielt.

"**Regelungen** zur internationalen Kriminalitätsbekämpfung" gibt es in einer kaum noch überschaubaren Zahl und Vielfalt. Zu nennen sind vornehmlich Verträge auf der Ebene der Vereinten Nationen, des Europarats, der Europäischen Union und der Schengen-Staaten, bilaterale Übereinkommen vor allem mit den mittel-ost-europäischen Staaten (MOE-Staaten) sowie Rahmenbeschlüsse des Rates der Europäischen Union u.a.m. Die Landesregierung verfügt über keine abschließende Zusammenfassung aller dieser Regelungen. Sie bedient sich deshalb im Bedarfsfall der allgemein zugänglichen Quellen. Dies sind in erster Linie die Veröffentlichungen der völkerrechtlichen Vereinbarungen im Bundesgesetzblatt Teil II. Ein Auszug aus dem "Fundstellennachweis B" (abgeschlossen am 31. Dezember 2001) mit dem Sachgebiet IV "Rechtswesen" Ziff. 10 (Rechtsverkehr in Abgabensachen), Ziff. 11 (Zusammenarbeit in Strafsachen), Ziff. 12

(Auslieferung in Strafsachen) und Ziff. 13 (Bekämpfung von Straftaten) ist als **Anlage** beigefügt. Zu verweisen ist ferner auf die Veröffentlichungen im Amtsblatt der Europäischen Gemeinschaften. Als weitere Quelle dienen insbesondere die "Berichte der Bundesregierung über die Integration der Bundesrepublik Deutschland in die Europäische Union" (zuletzt BT-Drs. 14/8565 vom 13. März 2002 für den Berichtszeitraum 2001; vgl. insbesondere Abschnitte VI "Justiz und Inneres" und VII "Maßnahmen zur Terrorismusbekämpfung").

Über **"Vorhaben"** auf europäischer Ebene unterrichten ebenfalls die genannten Berichte wie auch Veröffentlichungen der EU-Kommission und des Europäischen Parlamentes über von diesen Organen initiierte legislative Vorhaben. Hinzuweisen ist in diesem Zusammenhang insbesondere auf den von der Kommission halbjährlich herausgegebenen ”Anzeiger der Fortschritte bei der Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts in der Europäischen Union", der einschlägige Vorhaben und ihre Realisierung im Einzelnen beschreibt.

Eine Auflistung sämtlicher Regelungen und Vorhaben zur internationalen Kriminalitätsbekämpfung ist wenig zielführend, weil der erbetene Abgleich der Regelungen und Vorhaben mit deutschem Datenschutzrecht bzw. eine Prognosestellung über die Auswirkungen auf das Datenschutzrecht nicht vorliegt. In diesem Zusammenhang muss daran erinnert werden, dass "Regelungen und Vorhaben zur internationalen Kriminalitätsbekämpfung" in die ausschließliche Gesetzgebungskompetenz des Bundes fallen (Artikel 73 Nrn. 1, 10 GG), der Gegenstand der Anfrage also ausschließlich vom Bund zu verantwortende Bereiche betrifft. Die Landesregierung wirkt allerdings an dem Zustandekommen von Regelungen und bei der Beratung von Vorhaben zur internationalen Kriminalitätsbekämpfung - einschließlich der datenschutzrechtlichen Aspekte - über die zuständigen Ressorts, die Ständige Vertragskommission der Länder, die Ländervertreter in den EU-Ratsarbeitsgruppen sowie über den Bundesrat mit. Insgesamt sieht sich die Landesregierung bei den Beratungen zu diesen Projekten als angemessen beteiligt.

Die Landesregierung unterstützt über die genannten Personen und Institutionen die Bundesregierung dabei, international zu vergleichbaren Datenschutzstandards auf hohem deutschen Niveau zu kommen.

So ist im Einzelnen festzustellen, dass die Bundesregierung mit Erfolg versucht, im Rahmen des Abschlusses bilateraler Verträge datenschutzrechtliche Standards mit den Partnerstaaten zu vereinbaren. Aus letzter Zeit ist etwa zu verweisen auf das "Abkommen über die Zusammenarbeit bei der Bekämpfung der Organisierten Kriminalität zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Litauen" vom 23. Februar 2001 sowie das "Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Slowenien über die Zusammenarbeit bei der Bekämpfung von Straftaten mit erheblicher Bedeutung" vom 2. März 2001. Beide Abkommen stellen für die Verwendung personenbezogener Daten, die im Rahmen der vertraglichen Zusammenarbeit dem jeweils anderen Vertragsstaat übermittelt werden, ein eigenständiges Datenschutzregime auf.
So ist etwa bestimmt, dass eine ”Verwendung von Daten” im Sinne der Abkommen in Übereinstimmung mit der Begrifflichkeit des Bundesdatenschutzgesetzes bei jeder Form des Umgangs mit personenbezogenen Daten vorliegt, die nicht Erheben ist. Die Datenschutzvorschriften sehen u.a. ein Unterrichtungsrecht der übermittelnden Stelle über die Verwendung der übermittelten Daten und die dadurch erzielten Ergebnisse durch die empfangende Stelle der anderen Vertragspartei vor. Auch ist eine Zweckbindung und eine Bindung an die Bedingungen, welche die übermittelnde Stelle im Einzelfall stellt, festgelegt. Ferner sind u.a. Auskunftsrechte des Betroffenen und Protokollierungspflichten vorgesehen. Gleichlautende oder ähnliche Klauseln sind in früher abgeschlossenen Abkommen mit Estland, Lettland, der Russischen Förderation sowie Polen enthalten.

Als Beispiele für die Umsetzung datenschutzrechtlicher Regelungen in völkerrechtliche Vereinbarungen sind ferner die zwischen der Bundesrepublik Deutschland und der Tschechischen Republik abgeschlossenen Verträge über die Rechtshilfe in Strafsachen und die Auslieferung vom 2. Februar 2000 zu nennen. Die Verträge enthalten - dem Bundesdatenschutz entsprechende - Definitionen der personenbezogenen Daten, Re-

gelungen über die Zweckbindung und zusätzliche Bestimmungen, die ein einheitliches Minimalschutzniveau für personenbezogene Daten in beiden Vertragsstaaten garantieren sollen. Zugleich wird deutlich gemacht, dass nationale Datenschutzvorschriften durch den Vertrag nicht aufgehoben, sondern ergänzt werden sollen.
Ziel dieser Vertragsregelungen mit den verschiedensten Ländern ist es, "Inseln des Datenschutzes" zu schaffen, aus denen sich Grundregeln für kommende Regelungen etwa auf der Ebene der EU ergeben können. Verwirklicht hat sich dies schon in dem "Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union", das am 29. Mai 2000 gezeichnet worden ist. Es ist das erste Rechtshilfe-Übereinkommen, das datenschutzrechtliche Bestimmungen über den Datenaustausch zwischen zwei und mehreren Mitgliedstaaten enthält, u. a. eine "Zweckbindungsregelung". Das Übereinkommen enthält ferner bereichsspezifische Regelungen über die grenzüberschreitende Telekommunikationsüberwachung. Die nach deutschem Recht insoweit geltenden Schutzvorkehrungen konnten weitgehend in das Vertragswerk übernommen werden.
Die Landesregierung sieht hierin erfolgversprechende Ansätze. Sie wird die Bundesregierung im Rahmen ihrer Möglichkeiten bei ihren Bemühungen um den Ausbau datenschutzrechtlicher Standards in Übereinkommen zur internationalen Verbrechensbekämpfung weiterhin unterstützen.

Frage 7

Hält die Landesregierung es für geboten, die bestehenden Gesetze und Verordnungen zur Überwachung der Telekommunikation zu überprüfen und ggf. zu verändern? Falls ja, in welcher Hinsicht?

Antwort:

Die Landesregierung hält die Überwachung der Telekommunikation gemäß §§ 100 a ff. StPO in Übereinstimmung mit den Strafverfolgungsbehörden wegen des damit verbundenen tiefen Eingriffs in die Privatsphäre für ein zwar äußerstes, letztlich aber unentbehrliches Instrument der Sachverhaltsaufklärung im Rahmen eines strafrechtlichen Ermittlungsverfahrens. Dies gilt vor allem in solchen Verfahren, die Erscheinungsformen der Organisierten Kriminalität zum Gegenstand haben. Denn diese sind von sorgfältiger

Planung in arbeitsteiligem Zusammenwirken - unter Ausnutzung der Möglichkeiten der modernen Telekommunikation - und gleichzeitiger Abschottung nach außen geprägt. So werden etwa mehr als 50 % aller angeordneten Überwachungsmaßnahmen aus Anlass von Ermittlungen im Bereich der organisierten Betäubungsmittelkriminalität getroffen.

Diese grundsätzlich positive Bewertung des strafprozessualen Instruments der Überwachung der Telekommunikation bedeutet nicht uneingeschränkte Zustimmung zu allen geltenden gesetzlichen Regelungen im Einzelnen. Denn der schwerwiegende Eingriff in das Grundrecht des Fernmeldegeheimnisses und das Recht der informationellen Selbstbestimmung bedarf ständiger Überprüfung und Kontrolle, insbesondere im Hinblick auf dessen Erforderlichkeit und Verhältnismäßigkeit. So hat die Landesregierung sich gegen das ursprüngliche Regelungskonzept zum - unter datenschutzrechtlichen Aspekten ohnehin bedenklichen - Einsatz des sog. ”IMSI-Catchers” ausgesprochen, mit dessen Technik die für die Verkehrsabwicklung in den Mobilfunknetzen gebräuchlichen Gerätekennungen IMSI und IMEI erfasst werden können. Das Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl. I S. 3018), das mit § 100 i StPO die Rechtsgrundlage zur Vorbereitung einer Telekommunikationsüberwachungsmaßnahme sowie zur vorläufigen Festnahme oder Ergreifung eines Täters einer erheblichen Straftat geschaffen hat, trägt diesen Bedenken jedenfalls teilweise Rechnung, indem es einen grundsätzlichen Richtervorbehalt (mit staatsanwaltlicher Eilkompetenz) vorsieht.

Der Landesregierung sind die von Staatsanwaltschaften und Polizei kritisierten Schwächen und auch die gegenläufige Position der Datenschutzbeauftragten aus Bund und Ländern an den Regelungen im Telekommunikationsgesetz (§§ 89, 90 TKG) bekannt. Vor allem bei der Verwendung anonym oder pseudonym erworbener sog. Prepaid-Karten für Mobilfunktelefone laufen notwendige strafverfolgende Maßnahmen ins Leere, weil Verwaltungsgerichte zu dem Ergebnis gekommen sind, dass §§ 89, 90 TKG nicht ausreichen, um die vom Telekommunikationsbetreiber erfassten Kundengrunddaten zu speichern. Ein entsprechender Ressortentwurf des Bundesministeriums für Wirtschaft und Technologie will diese Lücke schließen und die sog. unvollständige Suchanfrage sowie den Ähnlichenservice gesetzlich regeln, um Strafverfolgungsbehörden künftig Ermittlungsansätze an die Hand zu geben.

Die Landesregierung nimmt auch angesichts der in den vergangenen Jahren bundesweit kontinuierlich ansteigenden Zahl der Verfahren, in denen Maßnahmen der Telekommunikationsüberwachung angeordnet wurden, Besorgnisse ernst, die Strafverfolgungsbehörden und Gerichte setzten dieses Instrumentarium zu großzügig ein. Für Schleswig-Holstein ist allerdings kein auffälliger Anstieg der Anzahl der Fernmeldeüberwachungen zu verzeichnen: Die Spanne streut in den vergangenen sechs Jahren zwischen 74 Fällen (1996) bis 91 Fällen (1999) und lässt keinen "inflationären Gebrauch" von diesem einschneidenden Instrument erkennen.

Weiter ist zu fragen, ob die Anknüpfung an einen Straftatenkatalog auch künftig eine tragfähige Grundlage der Überwachung der Telekommunikation sein kann. Die Auswahl der Katalogtaten durch den Gesetzgeber ist Ausdruck seiner Entscheidung der Frage, in welchen Fällen der Eingriff in das Grundrecht des Fernmeldegeheimnisses bei generell-abstrakter Betrachtungsweise mit dem Verhältnismäßigkeitsgrundsatz vereinbar sein kann.

Angesichts des erheblichen Eingriffs in bedeutsame Grundrechte sollte der Katalog deshalb lediglich sozialschädliche Straftaten von besonderem Gewicht enthalten. In Deutschland besteht eine starke Tendenz zur Erweiterung dieses Kataloges, der die Landesregierung allerdings in der Vergangenheit grundsätzlich entgegengetreten ist. Zu prüfen wäre, ob angesichts dieser drohenden "Inflation" des Straftatenkataloges andere Kriterien sachgerechtere Voraussetzungen für eine Überwachungsmaßnahme bieten könnten. Zu denken wäre etwa an die Schwere einer Straftat und die Straferwartung. Wichtig sind verfahrenssichernde Regelungen, um dem Grundrechtsschutz auch bei Vorliegen sozialschädlicher Straftaten von besonderem Gewicht Rechnung zu tragen. So könnte es nahe liegen, dass im Hinblick auf die Schwere des Grundrechtseingriffs die Maßnahme der Telekommunikationsüberwachung ausschließlich durch den Richter angeordnet werden, die Kompetenz des Staatsanwaltes (bei ”Gefahr im Verzuge”) also entfallen sollte.

Schließlich wird das Verhältnis von Zeugnisverweigerungsrechten - insbesondere der Berufsgeheimnisträger - zur Überwachung der Telekommunikation kritisch zu überprüfen sein.

Um diesen und gegebenenfalls weiteren Fragen der Novellierung der Vorschriften über die Telekommunikationsüberwachung nachgehen zu können, bedarf es aber hinreichend gesicherter rechtstatsächlicher Erkenntnisse. Die Landesregierung begrüßt und unterstützt deshalb den im November 1999 dem Max-Planck-Institut für ausländisches und internationales Strafrecht erteilten Auftrag, eine rechtstatsächliche Untersuchung zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO durchzuführen.

In Bezug auf das (Bundes-)Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz), das die Verfassungsschutzbehörden und Nachrichtendienste zur Überwachung der Telekommunikation berechtigt, sieht die Landesregierung dagegen keinen Prüf- und Änderungsbedarf. Auf Landesebene ist eine Anpassung des schleswig-holsteinischen Ausführungsgesetzes an die durch die Novellierung des Artikel 10-Gesetzes im Jahre 2001 entstandene Rechtslage in Vorbereitung.

Frage 8

Wie beurteilt die Landesregierung das Vorhaben, auf Bundesebene ein Informationsfreiheitsgesetz zu erarbeiten und welche Position nimmt sie zu Einzelfragen ein?
Wie sind die Erfahrungen mit dem neuen Informationsfreiheitsgesetz für Schleswig-Holstein beim Land und in den Kommunen?

Antwort:

Die Landesregierung begrüßt das Vorhaben, den Zugang auch zu den Informationen zu eröffnen, die bei den Bundesbehörden vorhanden sind. Für Schleswig-Holstein wird ein solches Gesetz keine Auswirkungen haben. Das Informationsfreiheitsgesetz des Landes (IFG-SH) ist bereits seit Februar 2000 in Kraft und wird in seinem Geltungsbereich durch ein Bundesgesetz nicht berührt. Eine Positionierung zu Einzelfragen des Bundesgesetzes ist derzeit nicht möglich, weil noch kein unter den Bundesressorts abge-

stimmter Entwurf vorliegt. Die Beratungen sollen in der kommenden Legislaturperiode wieder aufgenommen werden.
Bei der Anwendung des IFG-SH hat sich gezeigt, dass in der Verwaltungspraxis Probleme dadurch entstanden sind, dass das Gesetz insbesondere in zwei Punkten unterschiedlich ausgelegt werden kann:

- Zum einen geht es um die Frage, ob Behörden einem Informationsbegehren nach dem IFG-SH nur insoweit unterliegen, als sie öffentlich-rechtliche Verwaltungstätigkeit ausüben.
- Zum anderen bestehen Meinungsverschiedenheiten darüber, ob § 17 IFG-SH nur auf bestehende landesrechtliche Informationsansprüche Anwendung findet.

Im Übrigen sind die Erfahrungen mit dem neuen Informationsfreiheitsgesetz für Schleswig-Holstein (IFG-SH) beim Land und in den Kommunen überwiegend positiv.

Eine vom ULD im Mai 2002 durchgeführte Umfrage, an der sich 357 Behörden des Landes und der Kommunen beteiligt haben, hat Folgendes ergeben:

- In den ersten beiden Jahren nach In-Kraft-Treten des IFG-SH haben Bürgerinnen und Bürger in mehr als 2000 Fällen Informationsgesuche gestellt (vermutlich liegt die Zahl noch höher, da die Gesuche nicht bei allen Behörden dokumentiert wurden).
- Die Anträge waren in den allermeisten Fällen (über 90 %) auch erfolgreich, d.h. die begehrten Informationen wurden zugänglich gemacht. Soweit dies nicht geschah, lag der Grund meist darin, dass die entsprechenden Informationen bei der Behörde gar nicht vorhanden waren.
- Die Anfragen betrafen nahezu alle Verwaltungsgebiete. Das größte Informationsinteresse im kommunalen Bereich bestand hinsichtlich des Bau- und Planungsrechts.
- Die Informationsersuchen wurden sehr zügig bearbeitet: In 90 % der Fälle wurden die Anträge binnen einer Woche beschieden.

Die überwiegende Zahl der Anfragen nach dem IFG-SH wurde an die kommunalen Behörden gerichtet. Landesbehörden waren von den Informationsersuchen vergleichsweise weniger betroffen. Gebühren wurden nur in wenigen Fällen erhoben.

Frage 9

Wie beurteilt die Landesregierung das Vorhaben, auf Bundesebene ein Verbraucherinformationsgesetz zu erarbeiten und welche Position nimmt sie zu Einzelfragen ein?

Antwort:

Die Landesregierung bedauert, dass der Bundesrat den Gesetzentwurf hat scheitern lassen. Die Landesregierung hat den Gesetzentwurf der Bundesregierung in den Beratungen des Bundesrates unterstützt.
Verbraucherinnen und Verbrauchern sollte im Bereich der Lebensmittel und Bedarfsgegenstände ein für die Wahrnehmung von Verbraucherrechten notwendiger Anspruch auf Produktinformationen gewährt werden, die sich auf den Verbraucherschutz beziehen.
Der freie Zugang zu Informationen ist das zentrale Instrument der mündigen Verbraucherinnen und Verbraucher. Mit dieser Regelung wäre ein selbstbestimmtes Verhalten der Verbraucherinnen und Verbraucher wesentlich erleichtert worden. Die Erfahrungen mit BSE und Nitrofen haben gezeigt, dass auch ein großes Interesse und ein großer Bedarf an verbesserten Verbraucherinformationen besteht.

Das im Gesetzentwurf ebenfalls enthaltene Recht der Behörden, aktiv die Öffentlichkeit über gesundheitsschädliche Produkte zu informieren, hätte auch diesem sinnvollen Ziel gedient, den Verbraucherinnen und Verbrauchern mehr Information, Transparenz und Klarheit zu verschaffen. Dies hätte auch den Interessen der Unternehmen entsprochen, die sich vorschriftsmäßig verhalten.
Der Gesetzentwurf bildete eine gute Grundlage, eine ausgewogene Balance zum Schutz besonderer öffentlicher und privater Interessen herzustellen. Ausdrücklich unterstützt hat Schleswig-Holstein die Forderung des Bundesrates, den Entwurf des Verbraucherinformationsgesetzes um eine klare Regelung zur Datennutzung zu ergänzen.
Die Landesregierung hat bei den Einzelfragen entsprechend den vorbildhaften Standards des Informationsfreiheitsgesetzes des Landes Schleswig-Holstein (IFG SH vom 9. Februar 2000) votiert.

Für den Verbraucherschutz der Bereiche Telekommunikation und Post bestehen sek-

torspezifische Regelungen im Telekommunikationsgesetz (TKG) und Postgesetz (PostG) und den aufgrund von Ermächtigungen in diesen Gesetzen mit Zustimmung des Bundesrates von der Bundesregierung erlassenen Kundenschutzverordnungen. Die Telekommunikationskundenschutzverordnung (TKV) und die Postkundenschutzverordnung (PKV) regeln im Einzelnen die Verbraucherrechte gegenüber den Anbietern von Telekommunikationsdienstleistungen und Postdienstleistungen. Insoweit wird kein zusätzlicher Regelungsbedarf im Rahmen eines neuen Verbraucherinformationsgesetzes gesehen.

Frage 10

Wie beurteilt die Landesregierung die weitere Entwicklung von elektronischen Übertragungsmedien in Bezug auf den Datenschutz vor dem Hintergrund der Vermeidung von Kriminalität (insbesondere Kinderpornografie, Drogenhandel, Betrugsdelikte, Extremismus)?
Welche Möglichkeiten sieht die Landesregierung eine effiziente Strafverfolgung bei Straftaten im Internet zu gewährleisten, ohne dass eine Überwachung Unverdächtiger erfolgt?
Welche Position nimmt die Landesregierung in Bezug auf die anonyme Nutzung des Internets ein?
Welche Möglichkeiten der Kriminalprävention sieht die Landesregierung in diesem Zusammenhang und welche Maßnahmen werden bereits durchgeführt?
Welche Position nimmt sie zu diesem Themenkomplex bei Beratungen auf Bundesebene ein?

Antwort:

Das Internet ist eine der größten Errungenschaften unserer Zeit. Leider offenbaren sich neben den großen Chancen dieses weltweiten Kommunikationssystems auch Risiken, denn in fast allen Bereichen der Kriminalität nimmt die multimediale Technik an Bedeutung zu.
Im Bereich der Staatsschutzkriminalität ist seit Jahren festzustellen, dass im deutschen linksextremistischen/-terroristischen Spektrum die elektronischen Medien genutzt werden (eMail, Chat-Rooms, Verschlüsselungssoftware).

Auch der Rechtsextremismus hat mittlerweile dieses Medium vorwiegend für Propagandazwecke entdeckt.
Die Auswertung der Erkenntnisse über die Ereignisse vom 11. September 2002 zeigt, dass auch ausländische Terroristen einen Großteil der Kommunikation elektronisch abwickeln.
Im Bereich der Wirtschaftskriminalität häufen sich unseriöse Angebote bei Kapitalanlage- und Kreditvermittlungsgeschäften, während sich im Bereich der Rauschgiftkriminalität in den letzten Jahren die Erkenntnisse über das Anbieten von Betäubungsmitteln über das Internet mehren. Darüber hinaus sind in der Vergangenheit im Internet bereits Anleitungen für die illegale Herstellung von synthetischen Drogen verbreitet worden.
Seit Jahren steigt die aufgedeckte elektronische Verbreitung von Kinderpornografie an.
Die Bekämpfung der o.g. Kriminalitätsphänomene wird wesentlich dadurch erschwert, dass die Strafverfolgungsbehörden sich stets neu an technische Entwicklungen anpassen müssen und dabei auch dem Datenschutz Rechnung zu tragen haben. Das Spannungsfeld zwischen informationeller Selbstbestimmung des Einzelnen und einer technisch effektiven Strafverfolgung muss zu einem Ausgleich gebracht werden. Die Möglichkeiten des Internet, sogenannte geschlossene Chat-Rooms einzurichten, verschleierte eMail-Konten zu unterhalten und Kryptierungssoftware (z.B. PGP[3]) einzusetzen, erschwert es den Strafverfolgungsbehörden, Verantwortliche zu ermitteln. Die Strafverfolgungsbehörden müssen in rechtlicher, technischer und personeller Hinsicht fortlaufend in die Lage versetzt werden, dem staatlichen Strafverfolgungsauftrag nachkommen zu können.

Die Landesregierung begrüßt jede sachdienliche normative Veränderung, die der Aufklärung besonders schädlicher Kriminalität wie z.B. sexuellen Missbrauchs von Kindern oder Kinderpornografie dient. Nach den bisherigen Gesetzentwürfen (BR-Drs. 275/01, BT-Drs. 14/9801) wird dieses Ziel freilich nicht erreicht. Erhebliche datenschutzrechtliche Bedenken begegnen einer „Vorratsdatenspeicherung“ von sensiblen personenbezogenen Daten im großen Umfang zum Zwecke möglicher polizeilicher oder geheimdienstlicher Ermittlungen.

[3] „Pretty Good Privacy“

Eine Überwachung Unverdächtiger muss vermieden werden. Ob es vor diesem Hintergrund möglich ist, Providern rechtlich aufzugeben, ihre Verbindungsdaten, die dort z.B. zum Zwecke der Abrechnung vorhanden sind, inhaltlich und zeitlich beschränkt auch einem Zugriff der Strafverfolgungsbehörden zu öffnen, wenn ein Anfangsverdacht entstanden ist, bedarf sorgfältiger Abwägungen. Jeder Zugriff muss rechtsstaatlichen und datenschutzrechtlichen Grenzen unterworfen und verhältnismäßig sein.

Die Landesregierung begrüßt grundsätzlich die Möglichkeit für den Einzelnen, sich z.B. im Wege der Kryptierung anonym und pseudonym die neuen technischen Kommunikationsmöglichkeiten nutzbar zu machen, als eine Form der privaten Vorsorge zur Sicherung des Datenschutzes. Allerdings kann der Datenschutz hier keine absolute Geltung beanspruchen. In Abwägung mit kollidierenden Individual- und Gemeinschaftsrechtsgütern muss auch der Einzelne sich bei der Abwehr von Gefahren für wichtige bis höchste Rechtsgüter anderer oder der Gemeinschaft einer Güterabwägung stellen, die dem Gesetzgeber vorbehalten ist.

Der Verschlüsselungsbericht der Bundesregierung nach Ziffer 4 der Eckpunkte der deutschen Kryptopolitik vom Juni 1999 kommt zu dem Ergebnis, „dass die Arbeit der Strafverfolgungs- und Sicherheitsbehörden durch die Entwicklung des Fortschritts in der Verschlüsselungstechnik nicht nachteilig beeinträchtigt wird. Gleichwohl ist das Bundesministerium des Innern der Auffassung, dass die Entwicklung auf diesem Gebiet weiterhin aufmerksam beobachtet werden muss.“
Dieser Auffassung schließt sich die Landesregierung an (Beschluss der Ständigen Konferenz der Innenminister und -senatoren (Innenministerkonferenz - IMK) vom Juni 2002).

Für die Landesregierung ist die Möglichkeit zur anonymen Nutzung des Internets ein wichtiges Anliegen, das sie auch mit ihrem eigenen Internetauftritt konsequent verfolgt. Techniken, die personifizierte Einblicke in Nutzerverhalten erlauben (z. B. Cookies[4]), werden nicht eingesetzt. Daten, die Rückschlüsse auf Nutzer zulassen (insbes. Logfi-

[4] Englisch für "Keks". Es handelt sich um Datenpäckchen, die von einer Internet-Seite erzeugt und auf dem Rechner des Benutzers abgelegt und auch unbemerkt weitergegeben werden können.

les[5]), werden von der Landesregierung und ihrem Partnerunternehmen „schleswig-holstein.de“ innerhalb der datenschutzrechtlich vorgesehenen Fristen gelöscht.

Das Programm „Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK)“ enthält Präventionstipps für den Umgang mit elektronischen Übertragungsmedien im Internet. Diese Informationen können auch auf der Homepage der Landespolizei Schleswig-Holstein abgefragt werden. Auf dieser Seite befinden sich u.a. Hinweise und Informationen zu folgenden Themenfeldern:

- 0190-Dialer-Problematik
  (rechtliche Ausgangssituation, Erkennungsproblematik, Vorsorge-Tipps, „Erste Hilfe“, Link-Tipps)
- E-Commerce
- Viren und Trojanische Pferde
- So schützen Sie Ihr Kind

Außerdem führt die „Zentralstelle zur anlassunabhängigen Recherche in Datennetzen – ZaRD“ im Bundeskriminalamt Recherchen deliktsübergreifend in allen Internetdiensten, wie IRC, www, Usenet (Newsgroups), FTP sowie den Online-Diensten mit dem Ziel durch, länderübergreifend und damit der Eigenart des Mediums entsprechend strafbare Inhalte im Internet zu erkennen. Diese Recherchen wirken präventiv und werden zusätzlich durch deliktsbezogene Präventionsmaßnahmen (z.B. Faltblätter zum Kapitalanlagebetrug, Warnung vor unseriösen Angeboten mit 0190er-Rufnummern) unterstützt.
Die Landesregierung teilt die Auffassung des Arbeitskreises II der IMK, dass sich die zentrale Aufgabenwahrnehmung der „anlassunabhängigen Recherche im Internet und den Online-Diensten“ durch das BKA bewährt hat und fortgeführt werden sollte. Sie sieht darin neben den Länderrecherchen ein wichtiges und effektives, dabei zugleich ressourcensparendes Instrument insbesondere auch zur Bekämpfung der Kinderpornografie.

[5] Bezeichnung für eine Datei, die Angaben zu einem Netzwerkzugang speichert. Dadurch sind Rückschlüsse auf einzelne Anwender und deren persönliche Daten möglich.

Gestützt wird ferner die Initiative der IMK gegenüber dem Bundesminister des Innern, sich bei der Bundesregierung dafür einzusetzen, den Providern und Betreibern von Servern eine Protokollierungspflicht hinsichtlich der Identifikationsnummer eines Computers im Internet (IP-Adresse) und des Nutzungszeitraums sowie eine angemessene Aufbewahrungszeit der Daten vorzuschreiben.

Die „Intensivierung der Bekämpfung des Rechtsextremismus“ bildet einen Schwerpunkt bei der gesamtgesellschaftlichen Prävention, der im Rahmen der IMK stetig behandelt wird.

Frage 11

Wie beurteilt die Landesregierung die Regelungen zum sogenannten “großen und kleinen Lauschangriff”?
Wie sind die Erfahrungen mit den gesetzlichen Regelungen und den ergriffenen Maßnahmen (Erfolg?)? Welchen Handlungs- bzw. Reformbedarf sieht die Landesregierung in Bezug auf die Regelungen?

Antwort:

Die Landesregierung hegte seit Beginn der Debatte um die Einführung des **"Großen Lauschangriffs"** (Artikel 13 Abs. 3 GG, § 100c Abs. 1 Nr. 3 StPO), ein Schlagwort zur Bezeichnung des verdeckten Abhörens und Aufzeichnens des nicht öffentlich gesprochenen Wortes in einer Wohnung, rechtsstaatliche und verfassungsrechtliche Vorbehalte gegen eine Wohnraumüberwachung und brachte diese Auffassung im Gesetzgebungsverfahren ein.
Die Landesregierung hatte sowohl das Gesetz zur Änderung des Grundgesetzes als auch die einfachgesetzlichen Änderungsgesetze abgelehnt. Nachdem der Bundesrat mehrheitlich der Grundgesetzänderung zugestimmt hatte, unterstützte die Landesregierung - erfolgreich - die Anrufung des Vermittlungsausschusses, um jede Möglichkeit zur Nachbesserung der zur Abstimmung stehenden Änderungen der Strafprozessordnung zu nutzen. Vor diesem Hintergrund hat Schleswig-Holstein letztlich der im Vermittlungsverfahren gefundenen Lösung zustimmen können, mit der das Anrufungsbegehren im Wesentlichen berücksichtigt wurde.

Die Landesregierung betrachtet die Wirksamkeit der akustischen Wohnraumüberwachung weiterhin skeptisch und misst ihr allenfalls als "ultima ratio" zur Wahrung und Rettung hoher Rechtsgüter bei strikter Beachtung der strengen verfahrenssichernden Rahmenbedingungen eine die Ermittlungen stützende Rolle zu.

In **Schleswig-Holstein** wurden seit In-Kraft-Treten des Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität am 9. Mai 1998 bis Ende 2001 in zwei Verfahren (wegen Verdachts des Mordes bzw. des Betäubungsmittelhandels) akustische Wohnraumüberwachungsmaßnahmen angeordnet und vollzogen. Hiervon waren insgesamt vier Personen betroffen, davon drei Beschuldigte. In einem der beiden Verfahren waren die Erkenntnisse aus der Überwachungsmaßnahme für das Verfahren von Bedeutung.
In einem weiteren Verfahren ist zwar eine richterliche Anordnung auf Wohnraumüberwachung erwirkt und die Umsetzung erarbeitet worden, die maßgeblichen Gespräche wurden dann aber nicht in der Wohnung geführt. Schließlich sind zwei weitere Verfahren anhängig gewesen, in denen gerichtliche Beschlüsse auf Wohnraumüberwachung zwar erwirkt worden sind, aber aus taktischen Gründen nicht vollstreckt werden mussten.

Bundesweit sind in dem gleichen Zeitraum in insgesamt 87 Verfahren akustische Wohnraumüberwachungsmaßnahmen angeordnet und vollzogen worden.

Angesichts dieser geringen Anzahl einschlägiger Verfahren und eines damit einhergehenden noch recht schmalen Erfahrungswissens kann sich die Landesregierung der im "Erfahrungsbericht der Bundesregierung zu den Wirkungen der Wohnungsüberwachung durch Einsatz technischer Mittel" vom 30. Januar 2002 (BT-Drs. 14/8155) enthaltenen Beurteilung anschließen, wonach "repräsentative Aussagen und verlässliche Schlussfolgerungen sowie eine abschließende Bewertung der akustischen Wohnraumüberwachung als Instrument zur Bekämpfung schwerer Kriminalität derzeit noch nicht möglich sind".
In Übereinstimmung mit der Bundesregierung ist deshalb zunächst die weitere Anwendung des Instruments der akustischen Wohnraumüberwachung über einen längeren Zeitraum abzuwarten, um genügend aussagekräftige Rechtstatsachen für repräsentative

Aussagen zu erlangen. Weitere Erkenntnisse können u. a. auch von dem Gutachten des Max-Planck-Instituts zur "Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen" erwartet werden, das sich im Auftrage des Bundesministeriums für Justiz auch mit der akustischen Wohnraumüberwachung befasst, soweit diese im Zusammenhang mit Telekommunikationsüberwachungsmaßnahmen durchgeführt wird (vgl. dazu auch Antwort auf Frage 7).

Mit dem Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität vom 15. Juli 1992 (BGBl. I S. 1302) wurde der „**Kleine Lauschangriff**“ (§ 100 c Abs. 1 Nr. 2 StPO) zum verdeckten Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb einer Wohnung bei Verdacht erheblicher Straftaten den Strafverfolgungsbehörden an die Hand gegeben. Für Maßnahmen nach § 100 c Abs. 1 Nr. 2 StPO werden in Schleswig-Holstein keine Statistiken geführt. Staatsanwaltschaften und Polizeidienststellen des Landes sehen in dem „Kleinen Lauschangriff“ ein reibungslos funktionierendes Ermittlungsinstrument, mit dem auch die persönliche Sicherheit der Ermittlungskräfte wirksam geschützt wird. Diese Bewertung wird von der Landesregierung geteilt.

Aus der Praxis gibt es Wünsche zur besseren logistischen Vorbereitung von „Lauschangriffen“ in Bezug auf Mitwirkungspflichten Dritter.
Auf Bitte der IMK prüft das Bundesministerium der Justiz hierzu den Gesetzgebungsbedarf. Die Landesregierung wartet diese Überprüfungen ab.

Frage 12

Welche Erfahrungen liegen der Landesregierung bezüglich des Einsatzes besonderer Mittel der Datenerhebung durch die Polizei (z.B. Observation, verdeckter Einsatz technischer Maßnahmen zur Anfertigung von Bildaufnahmen, Einsatz technischer Mittel zum Abhören oder Aufzeichnen von Gesprächen außerhalb von Wohnungen, Zusammenarbeit mit sogenannten “V-Leuten”) vor?

Antwort:

Das Gefahrenabwehrrecht des Landes im Landesverwaltungsgesetz (LVwG) stellt der Polizei seit 1992 die verdeckten Datenerhebungsmittel

- der Observation (§ 185 Abs. 1 Nr. 1 LVwG),
- des Einsatzes technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen (§ 185 Abs. 1 Nr. 2 Buchst. a LVwG),
- des Einsatzes technischer Mittel zum Abhören oder Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen (§ 185 Abs. 1 Nr. 2 Buchst. b LVwG, sog. „Kleiner gefahrenabwehrender Lauschangriff“),
- des Einsatzes technischer Mittel zum Abhören oder Aufzeichnen des nichtöffentlich gesprochenen Wortes innerhalb von Wohnungen (§ 185 Abs. 1 Nr. 2 Buchst. b LVwG i.V.m. § 185 Abs. 3 LVwG, sog. „Großer gefahrenabwehrender Lauschangriff“) und
- des Einsatzes von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (§ 185 Abs. 1 Nr. 3 LVwG, Einsatz sog. V-Leute)

zur Verfügung. Darüber hinaus können unter erschwerten Eingriffsvoraussetzungen des § 185 Abs. 3 LVwG zur unerlässlichen Abwehr gegenwärtiger Gefahr für Leib oder Leben einer Person neben dem sog. „Großen gefahrenabwehrenden Lauschangriff“ auch andere besondere Mittel der Datenerhebung wie z.B. der Einsatz von technischen Mitteln zur Anfertigung von Bildaufnahmen oder -aufzeichnungen (abschließend in § 185 Abs. 1 Nr. 1 bis 3 LVwG aufgezählt und durch Verwaltungsvorschrift IV 460 – 14.46/15.09 vom 1. Juni 1992 für den Einsatz zugelassen) innerhalb von Wohnungen eingesetzt werden.

Für das Gebrauchmachen von den beispielhaft genannten Gefahrenabwehrinstrumenten der Polizei gibt es nur wenige Anwendungsfälle.

Dennoch hat die Anwendung der besonderen Mittel der Datenerhebung nach dem LVwG mit Zielrichtung des Schutzes der eingesetzten Kräfte (Verdeckte Ermittler, Scheinaufkäufer, nicht offen ermittelnde Polizeibeamte) sich positiv bewährt. Das gilt auch für die damit verbundene umfangreiche Einsatzdokumentation sowie das rechtlich

zulässige Einbringen der gefahrenabwehrenden Erkenntnisse als Beweismittel in Strafverfahren.
Der polizeiliche Staatsschutz hat u.a. nach dem 11. September 2001 verdeckte Einsätze technischer Mittel zur Anfertigung von Bildaufnahmen (§ 185 Abs. 1 Nr. 2 Buchst. a LVwG) und gerichtlich angeordnete Observationsmaßnahmen (§ 185 Abs. 1 Nr. 1 LVwG) durchgeführt. Die Durchführung der Maßnahmen ist personal- und zeitaufwendig und rechtlich und taktisch „ultima ratio“. Sie erfolgen erst, nachdem andere Möglichkeiten der Erkenntnisgewinnung ausgeschöpft worden sind.

Aus dem geringen Mengengerüst kann nicht auf die Entbehrlichkeit dieser Instrumente geschlossen werden. Vielmehr zeigt es den verantwortungsvollen Umgang der Landespolizei mit sensiblen Eingriffsrechten. Der Grad der Eindringtiefe dieser Instrumente in die Grundrechte der Betroffenen schließt es aus, sie sozusagen als Maßnahme der ersten Wahl einzusetzen. Unter Verhältnismäßigkeitsgesichtspunkten ist es vielmehr geboten, die erforderlichen Feststellungen zur Begründung gefahrenabwehrender Maßnahmen zunächst mittels weniger einschneidender Maßnahmen zu treffen. Wenn dieses erfolgreich ist, ist damit aber noch nichts darüber ausgesagt, dass in anderen Fällen nicht doch auf das besonders „scharfe Schwert“ solcher Maßnahmen zurückgegriffen werden muss. Auch muss der unter Präventionsgesichtspunkten wichtige Abschreckungseffekt gesehen werden, der sich mit der Möglichkeit des Einsatzes dieser Instrumente verbindet.

Frage 13

Wie beurteilt die Landesregierung die Regelungen zur Videoüberwachung im privaten und öffentlichen Bereich?
Sieht sie Handlungsbedarf, diese Regelungen zu verändern?

Antwort:

Mit § 6 b Bundesdatenschutzgesetz (BDSG) wurde erstmals eine bundesgesetzliche Regelung zur Videoüberwachung - auch für den **privaten Bereich** - geschaffen.

Danach ist die Beobachtung öffentlich zugänglicher Räume zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke zulässig, sofern keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Die Landesregierung hat sich im Novellierungsverfahren des BDSG dafür eingesetzt, dass die Regelungen zur Videoüberwachung im öffentlichen Raum die Vorschläge des Beschlusses der Beauftragten für den Datenschutz des Bundes und der Länder vom 14./15.März 2000 berücksichtigen. Diese sehen eine strenge Zweckbindung, differenzierte Abstufungen sowie eine deutliche Erkennbarkeit der Videoüberwachung, die Unterrichtung der identifizierten Personen und kurze Löschungsfristen der nicht mehr erforderlichen Daten vor.
Nach Auffassung der Landesregierung fanden diese Vorschläge in weiten Teilen in § 6 b BDSG Berücksichtigung. Die im ursprünglichen Gesetzentwurf vorgesehene Zulässigkeitsvoraussetzung „ ...zur Erfüllung eigener Geschäftszwecke“ wurde durch die neu formulierte „... zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ ersetzt, was zu einer Einschränkung der Videoüberwachung führt und aus datenschutzrechtlicher Sicht zu begrüßen ist. Darüber hinaus sieht die Bestimmung für die Verarbeitung oder Nutzung von Videomaterial eine gesonderte Bewertung der Zulässigkeit vor, wodurch eine restriktive Nutzung des Videomaterials gewährleistet werden soll. Ferner sind die Daten unverzüglich zu löschen, wenn sie für die Zweckerreichung nicht mehr erforderlich sind.

Aufgrund der gesetzlichen Bestimmungen in § 6 b BDSG, die auch den landesrechtlichen Regelungen in § 20 LDSG zur Videoüberwachung und -aufzeichnung in vielen Bereichen entsprechen, sieht die Landesregierung derzeit keinen zwingenden Handlungsbedarf, diese Regelungen zu verändern. Es sollten zunächst Erfahrungen gesammelt werden, um die Effizienz der neuen Norm beurteilen zu können. Ferner liegen der Landesregierung auch keine Hinweise oder Erkenntnisse vor, dass die Regelungen zur Videoüberwachung für private Sicherheitsdienstleister nicht ausreichend sind.

Für den **öffentlichen Bereich** der Videoüberwachung sind § 20 LDSG und § 184 LVwG maßgebend.

§ 20 LDSG erlaubt öffentlichen Stellen, die Videoüberwachung zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung ihres Hausrechts in öffentlich zugänglichen Räumen einzusetzen, wenn schutzwürdige Belange Betroffener nicht überwiegen. Die Polizei kann nach Maßgabe des § 184 LVwG die offene Video-Überwachung ohne und bei gesteigertem Gefahrengrad mit Aufzeichnung zur Gefahrenabwehr einsetzen.

Die IMK (Beschluss vom 5. Mai 2000) sieht in dem offenen Einsatz von Videoüberwachungsmaßnahmen an Kriminalitätsbrennpunkten im öffentlichen Raum ein geeignetes Mittel, um die Wahrnehmung der polizeilichen Aufgaben im Rahmen der Gefahrenabwehr und der Strafverfolgung wirksam zu unterstützen. Durch den offenen Einsatz von Videotechnik an Kriminalitätsbrennpunkten im Rahmen eines den jeweils spezifischen Gegebenheiten Rechnung tragenden Konzeptes können die Prävention verstärkt, die Kriminalitätshäufigkeit reduziert, die Aufklärung von Straftaten gesteigert und das Sicherheitsgefühl verbessert werden. Die Landesregierung unterstützt diesen Beschluss und weist ergänzend auf folgendes hin:

- Die Videoüberwachung von Kriminalitäts- bzw. Gefahrenbrennpunkten auf öffentlichen Straßen und Plätzen kann potenzielle Straftäter von der Begehung von Straftaten abschrecken, Straftaten verhüten und bei der Aufklärung helfen, wenn die Polizei dabei ein unmittelbares Einschreiten durch eine Vernetzung personeller, kriminalstrategischer und technischer Ressourcen gewährleistet.

- Die Videoüberwachung ist als isoliertes polizeiliches Instrument nicht geeignet, der Technikeinsatz ist kein Allheilmittel zur Kriminalitätseindämmung, sondern allenfalls eine flankierende Maßnahme polizeilicher Präsenz.

- Die bloße Verdrängung von Kriminalität ist keine Lösung.

- Ein flächendeckender Einsatz der Videoüberwachungstechnik ist nicht beabsichtigt. Dies bewirkt nur einen unverhältnismäßigen latenten Anpassungsdruck bei unbeteiligten Dritten und berücksichtigt nicht das Grundrecht auf informationelle Selbstbestimmung in ausreichendem Maße.

Die Landespolizei Schleswig-Holstein geht mit der seit 1992 in § 184 LVwG gesetzlich geregelten Videoüberwachung zur Gefahrenabwehr behutsam um.
Zurzeit wird als Gefahren- bzw. Deliktsschwerpunkt nur der Bereich des Flensburger ZOBs ohne Aufzeichnungen offen videoüberwacht. Aufzeichnungen werden im Rahmen der gesetzlichen Maßgaben erst dann vorgenommen, wenn im Einzelfall Tatsachen für die Begehung von Verbrechen bzw. gewerbs- oder gewohnheitsmäßigen Vergehen sprechen.
Der Schleswig-Holsteinische Landtag hatte am 8. Juni 2000 beschlossen, dass die landesgesetzlichen Grundlagen der Videoüberwachung ausreichend sind und für Regelungen, die eine weitergehende Überwachung erlauben, kein Anlass besteht. Die Beschlussfassung hat für die Landesregierung weiterhin Gültigkeit.

Frage 14 (1. Teil)
Welche Position hat die Landesregierung bei der Diskussion zu den sicherheitspolitischen Maßnahmen bezogen, die nach den terroristischen Anschlägen des 11. September 2001 in den USA und am 11. April 2002 in Djerba / Tunesien eingeleitet wurden? Inwieweit konnte sie diese Position durchsetzen?

Antwort:
Dieses Thema hat die IMK im November 2001 erörtert. Mit Zustimmung Schleswig-Holsteins wurde folgender umfassender **Beschluss** gefasst, der wegen seiner Bedeutung nachfolgend im Wortlaut wiedergegeben wird:

> **„**1. Die Innenministerkonferenz und ... haben nach den Terroranschlägen am 11. September 2001 in den USA umgehend wirksame Maßnahmen zur Gewährleistung der inneren Sicherheit in der Bundesrepublik Deutschland eingeleitet.
>
> Die Innenminister und -senatoren bekräftigen ihren Willen, diese Maßnahmen aufbauend auf der bisherigen konstruktiven Zusammenarbeit mit dem Bundesminister des Innern weiter umzusetzen und konsequent fortzuentwickeln.
>
> Für die einzelnen Handlungsbereiche der Innenministerkonferenz in diesem Zusammen-

hang, namentlich Polizei und Ausländerrecht, Verfassungsschutz und Nachrichtendienste, Zivil- und Katastrophenschutz sowie die internationale Zusammenarbeit der Sicherheitsbehörden, halten sie unter Bezugnahme auf weitere Beschlüsse ... vom ... November 2001 im wesentlichen Folgendes fest:

1.1 Polizeilicher und ausländerrechtlicher Bereich

Die Innenministerkonferenz bekräftigt ihren Beschluss vom 18. September 2001, mit dem sie die ... für unverzichtbar gehaltenen Sofortmaßnahmen im Zusammenhang mit den Terroranschlägen in den USA zur Kenntnis genommen und insbesondere

- die bundesweite Abstimmung von Schutzmaßnahmen,
- Restriktionen bei der Visa-Erteilung an Besucher bestimmter Staaten,
- die Datenübermittlung an Sicherheitsbehörden im Rahmen von Visa- und Asylantragstellungen,
- Rasterfahndungen zur Erkennung verdeckt im Inland lebender internationaler Terroristen,
- die Überprüfung und Anpassung von Luftsicherheitsmaßnahmen sowie die Intensivierung der Sicherheitsüberprüfungen für das Personal in Risikobereichen,
- die sofortige Abstimmung aller Sicherheitsmaßnahmen von grenzüberschreitender Bedeutung auf europäischer Ebene sowie
- den verstärkten Einsatz der Bundeswehr zur Sicherung militärischer Einrichtung einschließlich der Einrichtungen der NATO-Verbündeten

veranlasst hat.

Diese Beschlusslage ist zwischenzeitlich ausgeweitet und mit den Beschlüssen der heutigen Sitzung um weitere Maßnahmen ergänzt worden, mit denen

- potenziellen terroristischen Gewalttätern die Einreise erschwert,
- Schleusungskriminalität bekämpft,
- Vereinsverbote durch eine wirksame Einziehung von Vereinsvermögen effektiviert werden sollen.

1.2 Verfassungsschutz und Nachrichtendienste

Die Innenministerkonferenz hält es für vordringlich, die in der Bundesrepublik Deutschland bestehenden islamisch-extremistischen Organisationen einer umfassenden Aufklärung und Beobachtung zu unterziehen, um gesicherte Erkenntnisse über deren Strukturen für weitergehende Entscheidungen zur Gewährleistung der inneren Sicherheit zu erhalten.

Die Innenministerkonferenz betont in diesem Zusammenhang das Erfordernis einer verstärkten und effektiven Zusammenarbeit der Nachrichtendienste untereinander sowie mit allen anderen Sicherheitsbehörden des Bundes und der Länder mit dem Ziel des frühzeitigen Erkennens von Gefahrenlagen und deren nachhaltiger Bekämpfung.

1.3 Zivil- und Katastrophenschutz

Die Anschläge in den USA haben eine neue Dimension terroristischer Schadensszenarien erkennbar werden lassen. Die Innenministerkonferenz ist deshalb der Auffassung, dass im Hinblick auf die geänderte Sicherheitslage eine wirksame Vor- und Fürsorge im Katastrophen- und Zivilschutz gewährleistet sein muss.
Sie nimmt den Beschluss des Arbeitskreises V vom 24. September 2001 zu den Auswirkungen der Terroranschläge im Bereich Feuerwehr, Rettungswesen, Katastrophenschutz und zivile Verteidigung zustimmend zur Kenntnis. Sie unterstreicht in diesem Zusammenhang, dass die Leistungsfähigkeit des Hilfeleistungssystems in der Bundesrepublik einer kritischen Überprüfung zu unterziehen ist. Die Ausstattung des Katastrophen- und Zivilschutzes sowie die Aus- und Fortbildung in diesem Bereich sind bedarfsgerecht auszugestalten. Vorhandene Ressourcen sind durch ein verbessertes Zusammenwirken der verschiedenen Träger des Zivil- und Katastrophenschutzes in Bund, Ländern und Kommunen sowie der Bundeswehr zu optimieren.

1.4 Internationale Zusammenarbeit der Sicherheitsbehörden

Die Innenministerkonferenz ist weiterhin der Auffassung, dass die internationale Zusammenarbeit in der Bekämpfung der Organisierten Kriminalität und des Terrorismus intensiviert und ausgebaut werden und sich über den unionsweiten Rahmen hinaus auf die Beitrittsländer zur Europäischen Union und Drittstaaten, vor allem die Vereinigten Staaten von Amerika, erstrecken muss. Europol kommt dabei eine besondere Bedeutung zu, die unter Berücksichtigung der Beschlüsse auf nationaler und internationaler Ebene den weiteren schrittweisen Ausbau der Behörde erfordert. Dazu nimmt die Innenministerkonferenz die Grundsatzbeschlüsse des Rates der Justiz- und Innenminister der Europäischen Union vom 27./28. September 2001 zur Erweiterung des Mandats von Europol auf die im Anhang zum Europol-Übereinkommen aufgeführten schwerwiegenden Formen internationaler Kriminalität sowie zur Einrichtung von Eurojust zustimmend zur Kenntnis.

2. Die Innenministerkonferenz spricht sich für eine konsequente Umsetzung ihrer Beschlüsse, deren Fortschreibung und wirksamen Ergänzung aus. Sie beauftragt die Ar-

beitskreise II, IV und V, die mit der weiteren Umsetzung dieses Beschlusses verbundenen Aufgaben aufzunehmen und ihr zeitnah zu berichten.

3. Der Bundesminister des Innern wird gebeten, an der Umsetzung der sich aus diesem Beschluss ergebenden Maßnahmen mitzuwirken und - soweit die Zuständigkeit anderer Ressorts gegeben ist - auf die Umsetzung hinzuwirken.

4. Die Innenministerkonferenz ist der Überzeugung, dass den für die Umsetzung der Beschlüsse erforderlichen sächlichen und personellen Mitteln in den Haushaltsentscheidungen von Bund und Ländern eine der aktuellen Gefahrenlage entsprechende Priorität zukommen muss. Ungeachtet des insgesamt guten Ausstattungsstandes der betroffenen Behörden und der in den vergangenen Wochen bereits getroffenen Maßnahmen sieht sie die Notwendigkeit die personellen und sächlichen Ressourcen zu überprüfen.

5. Die Innenministerkonferenz hebt die enge und vertrauensvolle Zusammenarbeit zwischen Bund und Ländern hervor und bittet den Bundesminister des Innern, auch künftig die Länder im Rahmen seiner Möglichkeiten personell und sächlich zu unterstützen.

6. Die Innenministerkonferenz begrüßt das vorgelegte Sicherheitspaket des Bundesministers des Innern und bittet ihn, Maßnahmen zur Terrorismusbekämpfung, insbesondere die aktuellen gesetzgeberischen Vorhaben der Bundesregierung, weiterhin mit den Ländern abzustimmen.

7. Die Innenministerkonferenz appelliert in Anbetracht der deutlich gewordenen Besorgnis in der Bevölkerung an alle Verantwortlichen, mit Umsicht und Besonnenheit zu einer sachlichen öffentlichen Diskussion der Gefahrenlage beizutragen. Sie legt in diesem Zusammenhang Wert auf die Feststellung, dass ihr keine Hinweise auf terroristische Aktionen mit atomaren, biologischen oder chemischen Stoffen in der Bundesrepublik Deutschland vorliegen. Vor diesem Hintergrund wird die notwendige Vorsorge getroffen, Überreaktionen sollte jedoch entgegengewirkt werden.
Die Innenministerkonferenz begrüßt in diesem Sinn, dass das Bundesministerium für Gesundheit eine Stelle beim Robert-Koch-Institut zur Information zu den Gefahren bakteriologischer Stoffe eingerichtet hat.**“**

Im Rahmen der Beratungen über die Sicherheitspakete der Bundesregierung und über das Terrorismusbekämpfungsgesetz im aufenthaltsrechtlichen Bereich setzte sich die Landesregierung im wesentlichen dafür ein,

- die Sicherheitsbehörden mit den nötigen gesetzlichen Kompetenzen hinsichtlich des Zugriffes auf die Daten des Ausländerzentralregisters (AZR) auszustatten,
- den Datenaustausch zwischen den Ausländer- und Sicherheitsbehörden zu verbessern,

- bereits die Einreise terroristischer Straftäter nach Deutschland zu verhindern,
- identitätssichernde Maßnahmen von Personen aus Problemstaaten im Visumverfahren einzuführen sowie
- die Aufenthaltsbeendigung von im Inland befindlichen Extremisten zu verbessern.

Sowohl im Terrorismusbekämpfungsgesetz als auch im Zuwanderungsgesetz sind diese Forderungen aufgegriffen und umgesetzt worden. Hierbei handelt es sich um Bundesrecht, landesrechtliche Regelungen sind davon nicht betroffen.
Das Zuwanderungsgesetz wird in seinen wesentlichen Teilen am 1. Januar 2003 in Kraft treten. Die im Terrorismusbekämpfungsgesetz vorgesehenen Maßnahmen sind zum Teil noch nicht umgesetzt. So werden z.B. derzeit geeignete Verfahren für den Einsatz biometrischer Daten im Aufenthaltstitel, im Ausweisersatz, in Passersatzpapieren und sonstigen ausländerrechtlichen Bescheinigungen auf Bundesebene analysiert. Das Bundesministerium des Innern hat Ende Juni 2002 in einer allgemeinen Verwaltungsvorschrift festgelegt, in welchen Fällen Sicherheitsbehörden zur Feststellung von Versagungsgründen beteiligt werden können.

Auf Initiative der Bundesregierung wurde das Vereinsgesetz in zwei Schritten geändert:

- Zum einen wurde das sog. Religionsprivileg gestrichen, so dass nunmehr auch gegen extremistische Religionsgemeinschaften ein Vereinsverbot ausgesprochen werden kann.
- Zum anderen wurden die Verbotsmöglichkeiten gegen extremistische Ausländervereine bzw. ausländische Vereine erweitert. Es gibt jetzt die Möglichkeit, gegen

Ausländervereine vorzugehen, die z.B. Spenden für seine ausländische „Mutterorganisation“ sammeln oder Kämpfer rekrutieren.

Die Landesregierung, die beiden Änderungen des Vereinsgesetzes zugestimmt hat, sieht darin wirksame Instrumente, um gegen extremistische Vereinigungen und Ausländervereine vorzugehen. Durch die Konkretisierung der Verbotstatbestände wird zudem ein Eingreifen der Verbotsbehörden und der Sicherheitsbehörden erleichtert.

Die Landesregierung hat im Oktober 2001 ein umfangreiches Sicherheitspaket mit einem Haushaltvolumen von fast 13 Millionen Euro bereitgestellt und damit die notwendigen Voraussetzungen geschaffen, damit die Sicherheitsbehörden den neuen Herausforderungen gewachsen sind.

Für die Landespolizei sind 100 zusätzliche Stellen für Anwärterinnen und Anwärter geschaffen worden, davon sind 75 bereits besetzt und in der – dreijährigen – Ausbildung, während die verbleibenden 25 Anfang 2003 mit der Ausbildung beginnen werden. Für bestimmte Aufgabenfelder im Landeskriminalamt sind zusätzlich 15 Angestelltenstellen geschaffen worden, das Budget für die finanzielle Abgeltung von Überstunden wurde deutlich erhöht. Polizeibeamte, die das Pensionsalter erreicht haben, können auf eigenen Wunsch ein Jahr länger im Dienst bleiben und so eine sofort wirksam werdende Personalverstärkung bewirken, weil diese Beamten nicht erst ausgebildet werden müssen.

Der Verfassungsschutz hat islamwissenschaftlich und fremdsprachlich vorgebildetes Personal sowie eine Verstärkung der Observationsgruppe und des EDV- Bereiches erhalten.

Der Katastrophenschutz wurde durch die Erhöhung der Zuschüsse an die Kreise und kreisfreien Städte auf 51.000 Euro für die zusätzliche Beschaffung von ABC-Abwehrgerät gestärkt. Fünf vorgesehene Stellenstreichungen im Bereich des Amtes für Katastrophenschutz wurden rückgängig gemacht.

Die Staatsanwaltschaften, Strafgerichte und der Strafvollzug sind personell verstärkt worden.

Frage 14 (2. Teil)
Welche landesrechtlichen Regelungen sind von der Verabschiedung der Sicherheitsmaßnahmen in welcher Weise betroffen?

Antwort:
Die Sicherheitsmaßnahmen der Bundesregierung haben unmittelbar zu einer Änderung des Landesverwaltungsgesetzes geführt. Da die im Strafverfahrensrecht vorhandene Befugnis zur Rasterfahndung mangels konkreten Anfangsverdachts nicht genutzt werden konnte, musste eine entsprechende Rechtsgrundlage auf Basis des Gefahrenabwehrrechts des Landes (Landesverwaltungsgesetz) geschaffen werden.
Deshalb hat der Landtag nach den Ereignissen des 11. Septembers 2001 mit dem Gesetz über die Einführung des automatisierten Datenabgleichs (GVOBl. Schl.-H. S. 166) § 195 a LVwG als Rechtsgrundlage für den automatisierten Datenabgleich aus gefahrenabwehrenden Gründen eingeführt.

Die Erweiterung des Sicherheitsüberprüfungsgesetzes des Bundes um Regelungen zum vorbeugenden personellen Sabotageschutz führte dazu, dass sich die Einbringung des Entwurfs des Landessicherheitsüberprüfungsgesetzes, der dem Landtagspräsidenten mit Schreiben des Innenministers vom 1. Juni 2001 bereits zur Kenntnisnahme zugeleitet worden war, verzögerte. Auch auf Landesebene ist unter Berücksichtigung der Änderung des Bundesrechts die Erforderlichkeit der Aufnahme derartiger Regelungen in den Gesetzentwurf geprüft worden. Der überarbeitete Gesetzentwurf ist dem Landtag zugeleitet worden.

Frage 14 (3. Teil)
Wie beurteilt die Landesregierung den bisherigen Erfolg dieser Maßnahmen?

Antwort:

Hinsichtlich des Erfolges des automatisierten Datenabgleichs gemäß § 195 a LVwG ist noch keine Aussage möglich, da die automatisierten Abgleichsmaßnahmen beim BKA zur inhaltlichen Informationsverdichtung der „Treffer“ aus dem automatisierten Datenabgleich in Schleswig-Holstein noch nicht abgeschlossen sind.
Das trifft gleichermaßen auch für die Ermittlungstätigkeiten zu, die im Anschluss an die Rasterfahndung auf der Grundlage anderer Eingriffsermächtigungen des Landesverwaltungsgesetzes durchgeführt wurden bzw. noch durchzuführen sind.

Frage 14 (4. Teil)

Inwieweit wurden diese Maßnahmen befristet und wie beurteilt die Landesregierung die erfolgte Befristung?
Wann und in welcher Form wird eine Evaluation dieser Maßnahmen erfolgen?

Antwort:

Die Landesregierung hat den automatisierten Datenabgleich gemäß § 195 a LVwG bis zum 31. Dezember 2005 befristet.
Die zurzeit laufenden polizeilichen Maßnahmen müssen aus Sicht der Landesregierung zunächst abgeschlossen sein, um auf der Grundlage der erzielten Ergebnisse beurteilen zu können, ob das Instrument des automatisierten Datenabgleichs zur Gefahrenabwehr die rechtspolitischen Erwartungen erfüllt. Die diesbezügliche Evaluation erfolgt rechtzeitig vor Ablauf der zeitlichen Befristung des § 195 a LVwG.

Frage 14 (5. Teil)

Welche dieser Maßnahmen sind noch nicht umgesetzt, bzw. wie ist der Stand der Umsetzung (z.B. Aufnahme biometrischer Daten in Ausweispapiere)

Antwort:

Nach Artikel 7 (Änderung des Passgesetzes) und Artikel 8 (Änderung des Gesetzes über Personalausweise) des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 (BGBl. I S. 361) dürfen Pass und Personalausweis biometrische Merkmale von Fingern oder Händen oder Gesicht des Dokumenteninhabers enthalten. Die Arten der biometri-

schen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt werden. Ein entsprechender Gesetzentwurf liegt noch nicht vor. Das Bundesministerium des Innern hat zusammen mit dem Bundeskriminalamt und der Bundesdruckerei die notwendigen Vorarbeiten für die weitere Gesetzgebung aufgenommen.
Auch auf europäischer Ebene wird gegenwärtig überlegt, biometrische Verfahren für Personaldokumente einzuführen. Die Bundesregierung plant - gemeinsam mit den Niederlanden - eine Initiative der Europäischen Union, um zu einer gemeinsamen Lösung zu gelangen.

Frage 14 (6. Teil)
Wie beurteilt die Landesregierung diese Maßnahmen aus Sicht der Gewährleistung des Rechts auf informationelle Selbstbestimmung?

Antwort:
Die Landesregierung hält das Recht auf informationelle Selbstbestimmung sowohl bezüglich des automatisierten Datenabgleichs gem. § 195 a LVwG als auch der Folgemaßnahmen auf der Grundlage des Landesverwaltungsgesetzes für gewahrt.

Die Landesregierung verweist auf die gesetzlich normierte Benachrichtigungspflicht und auf die Pflicht zur Löschung und Vernichtung der aus Anlass dieser Maßnahme erhobenen Daten, soweit die Daten nicht für mit dem Sachverhalt zusammenhängende Verfahren erforderlich sind.

Frage 14 (7. Teil)
Hält die Landesregierung eine Veränderung, Ergänzung oder Rücknahme von Regelungen durch die Sicherheitspakete zum gegenwärtigen Zeitpunkt für erforderlich?

Antwort:
Wie die landesrechtlichen sind auch die bundesrechtlichen normativen Maßnahmen im Zusammenhang mit den Sicherheitspaketen zu evaluieren. Bis zum Vorliegen dieser

Evaluierungsergebnisse sieht die Landesregierung vor dem Hintergrund der nach wie vor angespannten Sicherheitslage keine Veranlassung, auf Veränderungen bzw. Ergänzungen oder auf Rücknahme einzelner bundesgesetzlicher Regelungen hinzuwirken.

Frage 15

Wie beurteilt die Landesregierung Regelungen, Verfahren und Verwendung zu den Themen

a) “Genetischer Fingerabdruck”

b) Biometrie

c) Digitale Signaturen

d) Chipkartensysteme

Welche datenschutzrechtlichen Bestimmungen sind bei diesen Verfahren zu beachten?

Welche datenschutzrechtlichen Risiken bestehen dabei?

Sieht die Landesregierung hier Handlungsbedarf?

Inwieweit nutzt die Landesregierung diese Verfahren?

Antwort:

a) „Genetischer Fingerabdruck“

Die bereichsspezifischen Regelungen (§§ 81 e, 81 f, 81 g StPO, §§ 1,2 und 3 DNA-Identitätsfeststellungsgesetz) für die molekulargenetische Untersuchung menschlichen Spurenmaterials (DNA-Analyse) haben ihre Grundlage in:

- dem Strafverfahrensänderungsgesetz (DNA-Analyse ”Genetischer Fingerabdruck” vom 17. März 1997, BGBl. I S. 534): Regelung der DNA-Analyse in aktuellen Strafverfahren bei Beschuldigten und Dritten,
- dem DNA-Identitätsfeststellungsgesetz vom 7. September 1998 (BGBl. I S. 2646), geändert durch Gesetz vom 2. Juni 1999 (BGBl. I S. 1242): Regelung der DNA-Analyse zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren bei Beschuldigten und Verurteilten und
- dem Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl. I S. 3018): gesetzliche Klarstellung des Erfordernisses richterlicher Anordnung zur

molekulargenetischen Untersuchung bei Spurenmaterial unbekannter Spurenleger.

Die Landesregierung hat sich im Gesetzgebungsverfahren sowohl für Vollzugspraktikabilität der Regelungen als auch für die gebotene Begrenzung des mit der DNA-Analyse verbundenen Eingriffs in das informationelle Selbstbestimmungsrecht der Betroffenen eingesetzt. Die gesetzlichen Bestimmungen erfüllen nach Auffassung der Landesregierung ausgewogen Belange der Strafverfolgung und des Datenschutzes.

Unterschiedliche Rechtsauffassungen bestehen allerdings hinsichtlich der Frage, ob für die Entnahme und Untersuchung von molekulargenetischem Material stets eine richterliche Anordnung ergehen muss. Das Innen- und Justizministerium halten eine richterliche Anordnung bei erklärter Einwilligung der oder des Betroffenen nach entsprechender Belehrung für entbehrlich.
Nach intensiver Erörterung der Problematik haben der Generalstaatsanwalt und das Landeskriminalamt im Einvernehmen mit den beteiligten Ministerien mit den "Gemeinsamen Richtlinien zur Umsetzung des DNA-Identitätsfeststellungsgesetzes (DNA-IFG) für Altfälle" eine "modifizierte Freiwilligkeitslösung" eingeführt. Führt die von der Polizei gestellte Prognose zu einem negativen Ergebnis (besteht also Grund zur Annahme, dass gegen die oder den Betroffenen künftig erneut Strafverfahren wegen einer Straftat von erheblicher Bedeutung zu führen sind), holt die Polizei eine Einwilligungserklärung der oder des Betroffenen zur Entnahme von Körperzellen und zu deren molekulargenetischer Untersuchung ein und nimmt die Probe. Bestätigt die Staatsanwaltschaft die polizeiliche Negativprognose, erfolgen die Untersuchung und die Eingabe der durch die Analyse gewonnenen DNA-Identifizierungsmerkmale in die beim Bundeskriminalamt geführte DNA-Analyse-Datei ohne richterlichen Beschluss. Im Weigerungsfalle wird eine richterliche Entscheidung herbeigeführt. Diese "modifizierte Freiwilligkeitslösung" ist nicht bei Jugendlichen sowie bei Inhaftierten und Untergebrachten anzuwenden. In diesen Fällen ist stets eine richterliche Anordnung zu erwirken.

Generalstaatsanwalt und Landeskriminalamt prüfen zurzeit, ob diese Regelung auch für "Neufälle" (§ 81 g StPO) einzuführen ist.

Die molekulargenetische Untersuchungen durch die Kriminaltechnischen Institute der Landeskriminalämter und des Bundeskriminalamtes haben einen anerkannten herausragenden Stellenwert und tragen vermehrt zur gerichtsfesten Aufklärung von Straftaten, insbesondere bei Kapital-, Sexual- und Eigentumsdelikten, bei. In der Kriminaltechnik des Landeskriminalamtes werden jährlich ca. 1.700 Fälle mit ca. 8.000 bis 10.000 Spuren bzw. Proben untersucht.

Deren molekular-genetischen Untersuchungen ergeben neben der Auswertung von Finger- und Handflächenspuren die einzigen forensisch verwertbaren Ergebnisse, die direkt zu Personen führen und so einen bedeutenden Beitrag zur Ent- oder Belastung von Tatverdächtigen leisten. Die Landespolizei nutzt die DNA-Analyse intensiv. Seit Einführung des bundesweiten Zugriffs auf die beim BKA geführte DNA-Analyse-Datei im Jahre 1998 konnten eine Reihe von Straftaten, darunter auch einige Tötungsdelikte, aufgeklärt werden. In der DNA-Analysedatei werden die DNA-Identifizierungsmuster tatverdächtiger und verurteilter Personen sowie unbekannter Spurenleger gespeichert. Auf sie haben nur ausgewählte Mitarbeiterinnen und Mitarbeiter des Landeskriminalamtes Zugriff.

Die gesetzlichen Regelungen über die DNA-Analyse sind für die kriminaltechnische Aufgabenerfüllung sowohl im Verwaltungs- als auch im Analysebereich vollzugspraktikabel. Die auf dieser Normengrundlage im Landeskriminalamt Schleswig-Holstein entwickelte und von einigen Ländern übernommene Anonymisierungsregelung und die dazu getroffenen Verwaltungsregelungen haben sich auch in Großverfahren (Screening-Fälle) bewährt. Es wird einerseits die gesetzlich geforderte Anonymität (§ 81 f StPO), andererseits die aus Qualitätssicherungsgründen erforderliche Unverwechselbarkeit der zu untersuchenden Spuren und Proben gewährleistet. Ein datenschutzrechtliches Risiko gibt es demnach für den Bereich der Kriminaltechnik des Landeskriminalamts und für den Bereich der Ermittlungsdienststellen der Landespolizei Schleswig-Holstein nicht. Zu diesem Ergebnis hat im Übrigen auch die im Jahr 2001 durchgeführte datenschutzrechtliche Überprüfung der Kriminaltechnik des Landeskriminalamtes durch das ULD geführt. Die Landesregierung sieht keinen aktuellen Handlungsbedarf, die Verfahrens-

regelungen zu ändern.

b) Biometrie

Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) wurde der Einsatz von biometrischen Merkmalen in verschiedenen Bereichen ermöglicht.

Nach Artikel 7 (Änderung des Gesetzes über Personalausweise) und Artikel 8 (Änderung des Gesetzes über Personalausweise) des Terrorismusbekämpfungsgesetzes dürfen in Pass und Personalausweis enthaltene verschlüsselte biometrische Merkmale und Angaben nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Inhabers ausgelesen und verwendet werden. Auf Verlangen haben Pass- und Personalausweisbehörde der Dokumenteninhaberin oder dem Dokumenteninhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen. Durch die getroffenen Regelungen wird die Verwendung der verschlüsselten Merkmale und Angaben auf die notwendigen Zwecke beschränkt. Artikel 7 und 8 des Terrorismusbekämpfungsgesetzes enthalten darüber hinaus klarstellend die ausdrückliche Feststellung, dass eine bundesweite Datei nicht eingerichtet wird.

Daneben regeln sowohl das Terrorismusbekämpfungsgesetz durch die Änderung des geltenden Ausländergesetzes als auch das voraussichtlich am 1. Januar 2003 in Kraft tretende Zuwanderungsgesetz, dass Aufenthaltstitel, Ausweisersatz und sonstige ausländerrechtliche Bescheinigungen neben dem Lichtbild und der eigenhändigen Unterschrift weitere biometrische Merkmale von Fingern, Händen oder Gesicht der Inhaberin oder des Inhabers enthalten können. Die Einhaltung datenschutzrechtlicher Bestimmungen ist durch die §§ 75 ff. des geltenden Ausländergesetzes bzw. durch Artikel 1, Kap. 7, Abschnitt 4 und die §§ 86 ff. des Zuwanderungsgesetzes, gewährleistet.

Die Landesregierung sieht in der Verwendung biometrischer Verfahren eine geeignete Möglichkeit zur Überprüfung der Authentizität von Dokumenten oder zur Identitätsfeststellung von Personen. Zur Umsetzung der gesetzlichen Regelungen müssen allerdings noch die Verfahrensregelungen (z. B. über die Arten biometrischer Merkmale, die Verschlüsselung, die Speicherung, die Verarbeitung) erlassen und die erforderlichen tech-

nischen Voraussetzungen geschaffen werden. Dabei ist zu beachten, dass die biometrischen Verfahren eine objektive, sichere und schnelle Überprüfung der Dokumente oder der Identität von Personen gewährleisten, damit sie effektiv eingesetzt werden können. Ferner ist die Aufklärung über den Einsatz biometrischer Verfahren wichtig, damit diese Verfahren für jedermann transparent sind.
Die Landesregierung sieht auch die datenschutzrechtlichen Risiken, die durch eine Verwendung biometrischer Verfahren, z. B. durch Manipulationen der Merkmale oder missbräuchliche Verwendung, entstehen können. Diese Risiken auszuschließen sollte daher vorrangige Aufgabe der derzeitigen Forschungsvorhaben zur technischen Umsetzung biometrischer Merkmale sein.
Derzeit sieht die Landesregierung keinen Handlungsbedarf, eine Änderung der gesetzlichen Regelungen anzuregen. Biometrische Verfahren werden durch die Landesregierung zurzeit nicht genutzt.

c) Digitale Signaturen

Nach Auffassung der Landesregierung ist es durch die Zunahme der elektronischen Kommunikation im Rechts- und Geschäftsverkehr erforderlich geworden, die Urheber und die Integrität der Daten zuverlässig festzustellen. Die Umsetzung der gesetzlichen Regelungen des Signaturgesetzes vom 16. Mai 2001 sind daher notwendige Voraussetzung, damit die elektronische Signatur gleiche Rechtswirkungen wie die handschriftliche Unterschrift entfalten kann. Dies gilt für den privaten und öffentlichen Bereich.
Im **umsatzsteuerrechtlichen Bereich** können Unternehmen seit dem 1. Januar 2002 auch elektronische Rechnungen erteilen, wenn sie mit einer qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung nach § 15 Abs. 1 des Signaturgesetzes versehen sind (§ 14 Abs. 4 Satz 2 Umsatzsteuergesetz i.d.F. des Steueränderungsgesetzes 2001).
Darüber hinaus ist den Unternehmen im Vorgriff auf das ab dem 1. Januar 2004 geltende Gemeinschaftsrecht durch Artikel 1 h des Fünften Gesetzes zur Änderung des Steuerbeamten-Ausbildungsgesetzes und zur Änderung von Steuergesetzen bereits jetzt die Möglichkeit eröffnet, auf die Anbieter-Akkreditierung zu verzichten.
Die Finanzbehörden sind bei elektronischen Abrechnungen im vorstehenden Sinne sowie bei sonstigen in digitalisierter Form erstellten und aufbewahrungspflichtigen Unter-

lagen der Buchführung berechtigt, die formellen und materiellen Voraussetzungen der elektronischen Signatur des Dokuments zu überprüfen. Die zur Signaturprüfung erforderlichen Unterlagen sind nach den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen auf einem maschinell verwertbaren Datenträger beim Steuerpflichtigen anzufordern.
Die Landesregierung betrachtet die Prüfbarkeit der Signatur bei elektronischen Abrechnungen sowie anderer in digitalisierter Form erstellter Buchführungsunterlagen auf der Basis der allgemeinen Grundsätze des Besteuerungsverfahrens als notwendiges Mittel, um die Originalität des Dokuments mit einem besonders hohen Zuverlässigkeitsgrad nachzuweisen.

Die Entscheidung des Bundesgesetzgebers, die elektronische Rechnung im Bereich der Umsatzsteuer mit der Papierform gleich zu behandeln und in diesem Zusammenhang die DV-gestützten Prüfungstechniken zuzulassen, wird als sachgerecht bewertet, um die langjährigen Forderungen der Wirtschaft nach steuerlicher Wirksamkeit der papierlosen Rechnungslegung zu erfüllen und gleichzeitig der Finanzverwaltung die notwendige Kontrolle zu ermöglichen.
Der aufgrund der Gefahren der automatisierten Datenverarbeitung notwendige Schutz gegen Zweckentfremdung ist durch das Weitergabe- und Verwertungsverbot auf der Grundlage des Steuergeheimnisses in § 30 AO sichergestellt.
Es kann regelmäßig davon ausgegangen werden, dass die von den Unternehmen eingesetzten Betriebssysteme über Möglichkeiten verfügen, die Überprüfung durch die Finanzämter auf den Bereich zu beschränken, der für die Besteuerung von Bedeutung ist. Die beschriebene Signaturprüfung soll bei Rechnungen und sonstigen Buchführungsunterlagen Anwendung finden, die nach dem 31. Dezember 2001 erstellt worden sind.

Für den **Bereich der Entsorgung von Sonderabfällen** gibt es Bestrebungen des Bundes und der Länder zur abfallrechtlichen Überwachung für die abfallrechtliche Nachweisführung (Entsorgungsnachweisverfahren, Begleitscheinverfahren) die Papierform durch die elektronische Form abzulösen. Die Bestrebungen sind naheliegend, weil heute bereits alle mit dem Entsorgungsnachweisverfahren zusammenhängenden Daten

in einem eigens hierfür entwickelten EDV-System erfasst werden.

Aus diesem Grunde ist durch Verordnung vom 25. April 2002 (BGBl. I S. 1488) in § 32 Abs. 4 Nachweis-Verordnung eine Experimentierklausel für die Anwendung der EDV aufgenommen worden. Da die Nachweisführung auf einem Zusammenwirken von Abfallerzeuger, Einsammler, Beförderer und Abfallentsorger aufbaut, bereitet die Anwendung der elektronischen Datenverarbeitung bei der Nachweisführung besondere Probleme, die einer ausführlichen praxisbezogenen Erprobung bedarf. Entsprechend dem Erprobungszweck ist vorgesehen, dass die zuständige Behörde die Anforderungen an die Erprobung so bestimmt, dass das Nachweisverfahren in elektronischer Form nach Art, Inhalt und Umfang dem „Papierverfahren“ entsprechend abgebildet wird.
Die Digitalisierung bereits im Entstehungsprozess des jeweiligen Entsorgungsvorgangs (in Schleswig-Holstein gibt es jährlich nahezu 60.000 nachweispflichtige Entsorgungsvorgänge) würde für alle Beteiligten - Abfallerzeuger, Abfallbeförderer, Abfallentsorger, Erzeugerüberwachungsbehörde, Entsorgerüberwachungsbehörde - eine enorme Arbeitserleichterung bedeuten und wird daher von der Landesregierung grundsätzlich begrüßt. Voraussetzung ist allerdings die erfolgreiche Entwicklung einer unter Datenschutzaspekten sicheren digitalen Signatur im Sinne des Signaturgesetzes. Die Gesellschaft für die Organisation der Entsorgung von Sonderabfällen
(GOES mbH) führt derzeit ein entsprechendes Projekt durch, auf dessen Ergebnisse bundesweit gewartet wird. Dieses Projekt wird im Rahmen des Landesprogramms „e-Region Schleswig-Holstein“ gefördert.

Mit dem Dritten Gesetz zur Änderung **verwaltungsverfahrensrechtlicher Vorschriften** des Bundes, das am 1. Februar 2003 in Kraft treten wird, wird die Möglichkeit eröffnet, gesetzliche Schriftformerfordernisse durch die elektronische Form zu erfüllen. Die elektronische Form ist der durch Rechtsvorschrift vorgeschriebenen Schriftform nur dann gleichwertig, wenn sie mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist (§ 3 a Abs. 2 Satz 2 Verwaltungsverfahrensgesetz des Bundes). Das Verwaltungsverfahrensrecht der Länder soll entsprechend angepasst werden, um auch für den Länderbereich die rechtsverbindliche elektronische Kommunikation zwischen Bürger und Verwaltung zu ermöglichen. Die entsprechende Änderung

des schleswig-holsteinischen Landesverwaltungsgesetzes wird derzeit vorbereitet. Eine Verpflichtung, von der elektronischen Form Gebrauch zu machen, wird damit jedoch nicht begründet.

Durch die Verwendung digitaler Signaturen kann der Urheber der Daten zuverlässig identifiziert sowie Datenveränderungen festgestellt werden. Dies setzt aber auch eine entsprechende Sicherheitsinfrastruktur voraus. Unter der Federführung des Innenministeriums wird zurzeit in einer von der IT-Kommission eingesetzten Arbeitsgruppe eine zentrale Public Key Infrastruktur (PKI) für die Landesverwaltung erarbeitet. Das Konzept wird so ausgelegt, dass sowohl Schnittstellen für fortgeschrittene als auch für qualifizierte Signaturen vorgehalten werden können. Es ist vorgesehen, erste Pilotprojekte 2003 durchzuführen.
Die Landesregierung sieht bei der Anwendung der digitalen Signatur im elektronischen Rechts- und Geschäftsverkehr, insbesondere bei der Anwendung der qualifizierten Signatur im Sinne des Signaturgesetzes, ein hohes Maß an Datensicherheit gewährleistet. Da bei der Anwendung des elektronischen Rechts- und Geschäftsverkehrs in der Regel die Verwendung der qualifizierten elektronischen Signatur gesetzlich vorgesehen ist, sieht die Landesregierung keinen Handlungsbedarf, derartige Regelungen zu ändern. Aufgrund der großen Anforderungen an die Sicherheitsinfrastruktur wird der Einsatz digitaler Signaturen bei der elektronischen Kommunikation zwischen Bürgerinnen und Bürger und der Verwaltung nach Einschätzung der Landesregierung zunächst noch eingeschränkt sein. Mit fortschreitendem e-Commerce und e-Government wird sich diese Situation aller Wahrscheinlichkeit nach positiv verändern.
Nach Auffassung der Landesregierung ist dabei von Bedeutung, dass die elektronische Kommunikation und die Signatur von den Bürgerinnen und Bürgern eine frei zu wählende zusätzliche Kommunikationsmöglichkeit bleibt.
Weil die technischen Voraussetzungen für den Einsatz der digitalen Signatur bei der Landesregierung noch nicht vorliegen, wird sie zurzeit noch nicht genutzt.

d) Chipkartensysteme

Für den Einsatz von mobilen personenbezogenen Datenverarbeitungssystemen, z.B. Chipkarten, sind die Regelungen in § 18 LDSG maßgebend. Diese sehen vor dem Ein-

satz derartiger Systeme eine umfassende Information der Betroffenen über die Datenverarbeitungsvorgänge sowie die Einwilligung des Betroffenen zum Einsatz der Systeme vor. Ferner ist der Betroffene über seine weiteren Informationsrechte nach den §§ 26 ff. LDSG aufzuklären. Die Landesregierung sieht hierin ausreichende Regelungen, um den Einsatz derartiger Systeme zu ermöglichen und gleichzeitig die Rechte der Betroffenen angemessen zu wahren. Mit § 6 c BDSG wurde eine vergleichbare Regelung eingeführt. Ferner sind die jeweiligen bereichspezifischen Regelungen maßgebend.

Die Chipkartentechnik wird im **Gesundheitsbereich** vor allem in zweierlei Hinsicht Verwendung finden. Zum einen geht es um die unmittelbare Verfügbarkeit und Aktualisierbarkeit von z.B. persönlichen Gesundheits-Daten und Notfalldaten unmittelbar auf der Karte selbst. Zum anderen kommt einem Chipkartensystem eine Schlüsselfunktion für den ortsungebundenen Zugriff auf eine „elektronische Patientenakte“ bzw. auf einzelne diagnose- und therapierelevante Daten zu.
Ein Chipkartensystem stellt eine positive Entwicklung im Interesse einer besseren Versorgung aus folgenden Gründen dar:

- Sie hilft – mitunter gesundheitlich belastende – Doppeluntersuchungen zu vermeiden,
- sie ermöglicht den freieren und schnelleren Zugriff auf wichtige Daten im Interesse der Patientinnen und Patienten und
- sie ermöglicht aber auch eine bewusstere Mitwirkung der Patientinnen und Patienten hinsichtlich der Nutzung ihrer Daten.

Aus Sicht der Landesregierung müssen im Hinblick auf die erkennbare Dynamik zum Einsatz von Patienten-Chipkarten mit erweiterter Funktion frühzeitig datenschutzrechtliche Fragestellungen einbezogen und nach Möglichkeit bereits in der Entwicklung neuer Verfahren beantwortet werden.
Die im Rahmen der Projektgruppe 3.2 der Gesundheitsinitiative des Landes in Entwicklung befindliche „Gesundheitskarte Schleswig-Holstein“ ist eine Krankenversicherungskarte mit erweiterter Funktionalität (Notfalldaten und weitere unveränderliche Daten, die in einer nächsten Phase um aktuelle Medikation / elektronisches Rezept erwei-

terbar sind). Zur Zeit ist sie eine der vielversprechendsten Ansätze zur Realisierung einer umfassend funktionalen Patientenkarte.
Zurecht haben die datenschutzrechtlichen Fragestellungen im Rahmen der auf Bundesebene geführten Diskussion um die Nutzung multifunktionaler Chip-Karten-Systeme eine besondere Aufmerksamkeit gefunden. Die Entwicklung und Umsetzung der „Gesundheitskarte Schleswig-Holstein“ geschieht unter enger Einbindung des ULD.

Bei der **Landespolizei** wurde im Rahmen der Heilfürsorge für Polizeibeamtinnen und Polizeibeamte im Jahr 2001 die Krankenversichertenkarte auf Basis der Chipkartentechnologie (analog der Einführung bei gesetzlichen und privaten Krankenkassen) gem. SGB V § 291 eingeführt, die das bisherige Verfahren der Krankenscheinhefte ablöste. Für das Verfahren gelten die datenschutzrechtlichen Bestimmungen des SGB, vornehmlich SGB V §§ 284 ff. sowie SGB X §§ 67 ff. Die Chipkarten befinden sich im Besitz der oder des Heilfürsorgeberechtigten. Nach Beendigung des Anspruchs auf Heilfürsorge sind die Heilfürsorgeberechtigten verpflichtet, die Chipkarten den zuständigen Stellen der Landespolizei zurückzugeben.
Eine Verschlüsselung der Daten auf dem Chip besteht nicht, da nicht alle Leistungserbringer (Ärzte pp.) über entsprechende Einlesegeräte verfügen. Bei den auf der Versichertenkarte gespeicherten personenbezogenen Daten handelt es sich jedoch nicht um "sensible" Gesundheitsdaten", sondern um Adressdaten sowie Zuordnungsnummern (Versichertenkenn-Nummer/Leistungsträger) und Gültigkeitsdaten. Abgesehen von der Missbrauchmöglichkeit nach Verlust oder Diebstahl der Chipkarte ist ein unmittelbarer Zugriff auf weitere Daten nicht gegeben.
Vor dem Hintergrund der geltenden Rahmenbedingungen sieht die Landesregierung keinen Bedarf, dieses Chipkartenverfahren zu verändern.

Seit 1995 wird im Ministerium für Wirtschaft, Technologie und Verkehr ein **elektronisches Zeiterfassungs- und Zugangssystem** eingesetzt. Jede Mitarbeiterin und Mitarbeiter besitzen eine entsprechende Chipkarte, wobei einzelne Zugangsrechte vergeben werden. Die Erfahrungen mit diesem System sind insgesamt positiv.
Auch im Dienstgebäude Düsternbrooker Weg 64 wird gemeinsam für das Ministerium für Finanzen und Energie und die Staatskanzlei ein Chipkartensystem, allerdings aus-

schließlich als **Einlasskontrolle** (Schließsystem) für die Nebeneingänge im Innenhof des Gebäudes eingesetzt.

Darüber hinaus werden Chipkarten in Form von **Geldkarten** für die Kantinen im Bereich der Landesregierung verwandt.

Nach Einschätzung der Landesregierung wird das datenschutzrechtliche Risiko bei der Verwendung von Chipkarten überwiegend im Verlust der Chipkarte gesehen. Beim Einsatz multifunktionaler Chipkarten dürfte sich ein Verlust gravierender auswirken. Derartige Risiken lassen sich jedoch nicht vermeiden. Sie können allenfalls durch entsprechende Belehrungen reduziert werden.

Frage 16

Wie beurteilt die Landesregierung folgende Angebote des unabhängigen Landeszentrums für Datenschutz:

a) Gütesiegel Datenschutz

b) Datenschutzaudit

c) Verschlüsselungssoftware

d) Virtuelles Datenschutzbüro

Antwort:

a) Gütesiegel Datenschutz

Die Landesregierung ist davon überzeugt, dass mit der Einführung des „Datenschutz-Gütesiegels“ ein wirksames Instrument für mehr Datenschutz und Datensicherheit geschaffen wurde. Dieses neue Verfahren eröffnet den Hersteller- und Vertriebsfirmen die Möglichkeit, ihre IT- Produkte auf deren Eigenschaften zum Datenschutz und zur Datensicherheit überprüfen zu lassen. Nach § 4 Abs. 2 LDSG sollen die öffentlichen Stellen geprüfte Produkte vorrangig einsetzen.

Das Innenministerium, zuständig für das ressortübergreifende IT-Management, ist bestrebt, geprüfte IT-Produkte für das Landesnetz einzusetzen. Seitens der Datenzentrale Schleswig-Holstein bestehen Überlegungen, für einen Teil der betriebenen Firewalltechnik des Landesnetzes ein Gütesiegelverfahren durchführen zu lassen.

Nach Mitteilung des ULD wurden bisher insgesamt acht Sachverständige und Prüfstellen für die Produktprüfung anerkannt; weitere Anträge befänden sich in der Bearbeitung. Einige Sachverständige hätten erklärt, dass bereits diverse Begutachtungsverfahren durchgeführt werden. Die ersten beiden Anträge auf Verleihung eines Gütesiegels lägen dem ULD bereits vor; eine Entscheidung werde voraussichtlich bis Ende diesen Jahres getroffen.
Die Landesregierung begrüßt das Engagement des ULD auf diesem Gebiet und beteiligt sich auch finanziell an dieser Maßnahme. Das Projekt „Gütesiegel für IT-Produkte" ist Bestandteil des Landesprogramms „e-Region Schleswig-Holstein". Hierbei handelt es sich um ein gemeinsames Programm des Ministeriums für Wirtschaft, Technologie und Verkehr und der Technologiestiftung Schleswig-Holstein, das zu 50% von der EU-Kommission aus den Innovativen Maßnahmen des Europäischen Fonds für die Regionale Entwicklung (EFRE) kofinanziert wird. Im Rahmen dieses Projektes kann das ULD die Fördermittel insbesondere an kleine und mittlere Unternehmen vergeben und damit die Durchführung eines Gütesiegelverfahrens unterstützen.

b) Datenschutzaudit

Das Datenschutzauditverfahren nach § 43 Abs. 2 LDSG (sog. Behördenauditverfahren), mit dem öffentliche Stellen ihr Datenschutzkonzept durch das ULD prüfen und beurteilen lassen können, hält die Landesregierung für ein sehr erfolgreiches Verfahren, das bereits bei vielen öffentlichen Stellen auf großes Interesse gestoßen ist. Dies belegen die Zahlen des ULD.
Das ULD hat Ende August dieses Jahres mitgeteilt, dass bereits mit fünf Behördenauditverfahren begonnen werden konnte, von denen zwei erfolgreich abgeschlossen wurden. Die drei weiteren Verfahren werden voraussichtlich noch bis Ende dieses Jahres durchgeführt; für vier zusätzliche Verfahren wurden die Verträge teilweise schon unterzeichnet. Nach Auskunft des ULD betreffen die Behördenauditverfahren sämtliche Bereiche der Verwaltung, wie Landesbehörden, die Landtagsverwaltung und die Kommunalverwaltung. Inhaltlich beziehen sie sich auf die konventionelle Datenverarbeitung sowie auf die Datenverarbeitung unter Einsatz neuer Medien, wie z.B. des Internets.

Auch für das Landesnetz wurde das ULD mit der Durchführung des Behördenauditverfahrens beauftragt.
Die Landesregierung teilt die Auffassung des ULD, dass mit dem Behördenaudit eine Verbesserung des Datenschutzniveaus erreicht werden kann, indem Datenschutzverfahren geprüft und optimiert werden und ein Datenschutzmanagementsystem aufgebaut wird, das eine fortlaufende Anpassung des Datenschutzes an die sich verändernden Rahmenbedingungen sicherstellt. Damit wird auch das Ziel verfolgt, das Vertrauen der Bürgerinnen und Bürger in die von den Behörden angewandte Informations- und Kommunikationstechnik zu fördern.
Das Behördenaudit ist auch Bestandteil des Landesprogramms „e-Region Schleswig-Holstein“.

c) Verschlüsselungssoftware

Die Landesregierung begrüßt das bereits seit längerem vorhandene Angebot des ULD, mit den Bürgerinnen und Bürgern verschlüsselte e-Mails auszutauschen und teilt die Auffassung, dass Verschlüsselungssoftware ein zentrales Instrument des Selbstdatenschutzes ist. Es ist ein wirksames Mittel um sich gegen Datenmanipulationen bei der elektronischen Kommunikation und Datenspeicherung zu schützen.
Nach Mitteilung des ULD findet das Verschlüsselungsangebot zunehmend Resonanz bei den Bürgerinnen und Bürgern und es wurde bereits mehrfach der Wunsch geäußert, empfehlenswerte Software als Sammlung zur Verfügung zu stellen.
Diese erhöhte Sensibilisierung für den Umgang mit Daten ist sicher auch wesentlich das Resultat der umfangreichen Aufklärungsarbeit des ULD im Bereich der Verschlüsselungssoftware.
Die Landesregierung hat sich am 29. Januar 2002 im Rahmen des Beschlusses über den Handlungsrahmen Internet-Strategie dafür ausgesprochen, die neuen Medien noch stärker zu nutzen, um Verwaltungsvorgänge vollautomatisch und dadurch effektiver durchführen zu können. Im Wege der dafür benötigten Public-Key-Infrastruktur (PKI) wird auch die Verschlüsselung von Daten eine wesentliche Rolle spielen.
Das Innenministerium hat auch im Rahmen des Landessystemkonzeptes bei der Einführung des Standard-Arbeitsplatzes (IKOTECH III) den Themenbereich „Technologien zur Verschlüsselung“ aufgenommen.

Wenngleich die Landesregierung die Verschlüsselung von Daten für ein wirksames Instrument des Selbstdatenschutzes hält und im Rahmen der künftigen Sicherheitsinfrastruktur (PKI) diese voraussichtlich auch selbst anwenden wird, dürfen dennoch die Belange der Sicherheits- und Strafverfolgungsbehörden durch die Verschlüsselungstechnik nicht nachteilig beeinträchtigt werden.

d) Virtuelles Datenschutzbüro

Die Landesregierung hält das virtuelle Datenschutzbüro für eine wichtige und hilfreiche Informationsplattform für die vielfältigen Fragen im Bereich des Datenschutzes und der Datensicherheit. Gerade die breite Projektpartnerschaft mit dem Datenschutzbeauftragten des Bundes und den Datenschutzbeauftragten der Länder, Kirchen und anderer Institutionen bietet ein umfassendes Informationsangebot.

Nach Mitteilung des ULD werde das virtuelle Datenschutzbüro auch als Diskussionsforum zu Datenschutzfragen zwischen Nutzern sowie Experten in Anspruch genommen. Seit der Inbetriebnahme im Jahr 2000 werde es von den Bürgerinnen und Bürgern in erfreulich hohem Maße genutzt. Ebenfalls zeigen die themenbezogenen Mailinglisten, die häufig innerhalb von Fachgruppen auf hohem Niveau stattfinden, eine rege Beteiligung. Darüber hinaus erhalte das virtuelle Datenschutzbüro auch e-Mails von Bürgerinnen und Bürgern, mit denen das ULD über aktuelle Informationen und Veröffentlichungen zum Thema Datenschutz aufmerksam gemacht werde.
Diese Beispiele zeigen, dass das virtuelle Datenschutzbüro sich zu einer etablierten Serviceeinrichtung entwickelt hat. Es bietet den Bürgerinnen und Bürgern, der Wirtschaft sowie der Verwaltung ein umfassendes Informationsangebot und vielfältige Diskussionsforen.

Frage 17

Welche Erfahrungen liegen der Landesregierung in Bezug auf die neue Rechtsform als Anstalt des öffentlichen Rechts des Unabhängigen Landeszentrums für Datenschutz vor?

Antwort:

Durch die Zusammenführung der Datenschutzaufsicht für den öffentlichen Bereich und die Privatwirtschaft wurde das fachliche „know-how“ im ULD gebündelt und kann so noch effektiver eingesetzt werden. Nach den Erfahrungen der Landesregierung wird das ULD als kompetente Stelle beurteilt, die neben ihrer Aufsichtsfunktion auch besonderes Gewicht auf die Serviceaufgaben legt. Die Beratung und Information der öffentlichen Stellen zu rechtlichen, organisatorischen oder technischen Fragen des Datenschutzes und der Datensicherheit ist umfassend und sehr hilfreich. Das Informationsangebot online ist vielseitig, funktionell und anwenderfreundlich.

Auch im nicht-öffentlichen Bereich ist das ULD Datenschutzverstößen schnell und kompetent nachgegangen. Es ist zu erwarten, dass die mit dem neuen BDSG eingeführte anlassunabhängige Kontrollmöglichkeit der Aufsichtsbehörden zu vermehrten Prüfungen durch das ULD führen wird.

Im Hinblick auf die Vielfalt der Kommunikationsmöglichkeiten und die fortschreitende automatisierte Datenverarbeitung erhält der Datenschutz eine immer größere Bedeutung. Die Synergieeffekte durch die Zusammenlegung der Datenschutzaufsicht beim ULD sind daher von wesentlichem Vorteil.

Frage 18

Welche Vorhaben bestehen bei der Landesregierung, um die Medienkompetenz der Bürgerinnen und Bürger zu erhöhen? Inwieweit spielen bei entsprechenden Vorhaben nicht nur die technischen Fertigkeiten, sondern auch qualitative Gesichtspunkte zur sicheren und selbstbewussten Nutzung dieser Medien eine Rolle?

Antwort:

Die Landesregierung fördert in unterschiedlichsten Bereichen durch eine Vielzahl von Projekten die Medienkompetenz der Bürgerinnen und Bürger.

Beim hohen Nutzungsgrad neuer Medien nimmt Schleswig-Holstein nach einer aktuellen Emnid-Studie im Ländervergleich bei der Zahl der Internetnutzerinnen und -nutzer Platz 1 ein. Im Schulbereich wird dieser Prozess insbesondere durch das Projekt „Schulen ans Netz“ unterstützt.

Spezielle Aspekte von Informations- und Kommunikations-Technologien (IuK-Technologien) sind **Inhalt von Lehrplänen,** und die fachübergreifende Nutzung dieser neuen Medien hat die Landesregierung zur Pflicht gemacht. Dies führt über technische Fertigkeiten hinaus zur kompetenteren Nutzung und zum besseren Verständnis. Weitere Komponenten zur Erhöhung der Medienkompetenz wurden entwickelt und aufeinander abgestimmt. Hierzu zählen vor allem der „Landesbildungsserver“
- das „Lernnetz“ - als zentrale Bildungsplattform und Wissensportal im Schulbereich. Der Landesbildungsserver ist zugleich die Kommunikationsplattform für E-Learning-Prozesse. Auch in der Lehrerfortbildung wird eine notwendige Mediengrundkompetenz vermittelt. In dem Projekt „Fortbildung online“ werden schulart- und fächerübergreifende Probemodule für Internetnutzung, Schulvernetzung und Standardsoftware erarbeitet und für Lehrzwecke zur Verfügung gestellt. Der seit 2001 erfolgte flächendeckende Aufbau eines Schulungsnetzes für Lehrkräfte soll möglichst alle Lehrkräfte befähigen, die IuK-Techniken unterrichtsstützend und -verbessernd einzusetzen. Hierzu dient auch der Weiterbildungslehrgang „Neue Informations- und Kommunikationsmedien im Unterricht“ mit Lehrinhalten des CAU-Studienangebotes.

Im **Hochschul- und Fachhochschulbereich** gibt es eine Reihe von Projekten, die über fachspezifische Themen hinaus grundsätzlich alle zur Verbesserung im Umgang mit neuen Medien beitragen. Zu nennen sind hier insbesondere die „Virtuelle Fachhochschule Lübeck“ und der „Multimedia-Campus“. Im Rahmen des bundesweiten Leitprojektes ist das Ziel der virtuellen Fachhochschule die Realisierung eines offenen, modularen Studiums unter Nutzung des Internets mit ausgewählten Studien- und Weiterbildungsangeboten. Dazu werden die technischen, organisatorischen, pädagogischen, psychologischen, gesellschaftlichen und rechtlichen Bedingungen entwickelt, unter denen die nachhaltige Qualität und Relevanz des Fachhochschulstudiums gesichert werden kann. Der Multimedia-Campus soll durch die Ausbildung von Fach- und Führungskräften einen entscheidenden Impuls für die Informationsgesellschaft in Schleswig-Holstein geben und eine Multimedia-Industrie fördern und hiermit einen Beitrag zur Förderung der Medienkompetenz liefern.

Im **Bereich der Volkshochschulen** unterstützt die Landesregierung das Projekt VHS Info Netz Online (VINO). Ziel ist die Vernetzung der Volkshochschulen im Kreis Plön und die Möglichkeit zur interaktiven Nutzung von VHS-Angeboten. Fachunabhängig wird hierdurch der Umgang mit neuen Medien verbessert.

Auf dem Gebiet der **Frauenförderung** werden durch das Projekt „Frauen ins Internet" Internet-Schulungen, Informationsveranstaltungen und Beratungen für Frauen angeboten. Das Projekt wird wissenschaftlich begleitet, evaluiert und dokumentiert. Mit dem Projekt „Info-Net Frauen Schleswig-Holstein" wird zusätzlich eine Dialogplattform aufgebaut. Schulung und Qualifizierung im Umgang mit den neuen Medien ist hierbei ein vorrangiges Ziel. Im Rahmen der Offensive "Online - Frauen sind dran" fördert die Landesregierung ein mobiles Internetcafé. Dieser Internetbus bietet Frauen aus Gemeinden im ländlichen Raum die Möglichkeit, an kostenlosen Kursen zum Einstieg in die Nutzung des Internets wohnortnah teilzunehmen. Im Rahmen der gesamten Laufzeit wird der Internetbus an 170 Einsatztagen bis zu 7.500 Frauen einen dezentralen Einstieg in das Internet ermöglichen. Nach der jüngsten Emnid-Studie belegt Schleswig-Holstein auch bei dem Frauenanteil im Internet im Ländervergleich den Platz 1. Ziel dieser Offensive ist es, diesen erfolgreichen Trend fortzusetzen und Frauen zu motivieren, das Internet beruflich und privat verstärkt zu nutzen. Darüber hinaus sollen Zugangshemmnisse und Berührungsängste von Frauen gegenüber dem Internet abgebaut werden, Frauen sollen über die vielfältigen Informations- und Kommunikationsmöglichkeiten des Internets informiert werden und es soll die Befähigung der Nutzung vermittelt werden.

In vielen weiteren Bereichen leitet oder fördert die Landesregierung unterschiedlichste Projekte wie z.B. „Marktplatz seelische Gesundheit", „Jugend ans Netz", „Softwarehaus Schleswig-Holstein", „Kulturnetz Schleswig-Holstein" oder die Informationsplattform schleswig-holstein.de und stärkt damit auch die Medienkompetenz der Bürgerinnen und Bürger. Der Auftritt der Landesregierung im Internet soll hierbei barrierefrei gestaltet werden und auch an Anforderungen von blinden und sehbehinderten Menschen angepasst werden.

Als Basis für den sicheren Umgang mit den neuen Medien wird eine Vielzahl von Aktivitäten zum Datenschutz durch das ULD durchgeführt. Mit dem Projekt „Virtuelles Datenschutzbüro“ wird ein bürgernaher Datenschutzservice angeboten. Bürgerinnen und Bürger sollen online die Möglichkeit erhalten, allgemeine Fragen des Datenschutzes online einzuholen. In einem weiteren Projekt „Anonymer, unbeobachteter Netzzugang“ wird die Möglichkeit entwickelt, Server so auszustatten, dass sie anonym und unbeobachtbar genutzt werden können. Darüber hinaus fördert die Landesregierung das Projekt „Datenschutz mit P3P[6] für Internet-Surfer“. Ziel des Projektes ist es, durch intelligenten Technikeinsatz die Internet-Surfer in ihrem Datenschutz und ihrer kommunikativen Selbstbestimmung zu stärken.

Neben Medien aus dem IuK-Bereich ist die Unabhängige Landesrundfunkanstalt (ULR) seit 1999 nach dem Landesrundfunkgesetz auch ausdrücklich für die Vermittlung **rundfunkorientierter Medienkompetenz** zuständig. Dies geschieht schwerpunktmäßig in den von der ULR eingerichteten und finanzierten Offenen Kanälen (OK), durch Medienforschung, finanzielle Förderung medienpädagogisch ausgerichteter Organisationen und Projekte, öffentliche Veranstaltungen und Publikationen sowie durch sonstige geeignete Maßnahmen. Von den zahlreichen Aktivitäten der ULR ist das umfassende Angebot zum Gestalten, Produzieren und Senden von Hörfunk- und Fernsehbeiträgen in den vier Offenen Kanälen der ULR hervorzuheben. Diese bieten darüber hinaus eine Vielzahl von medienpraktischen Seminaren an. Als PC-orientierte Aktivitäten mit datenschutzrelevantem Lernpotenzial sind insbesondere zu nennen:

- In allen vier Offenen Kanälen der ULR existieren öffentlich zugängliche MultiMedia-Labs[7] mit Internetzugang, bestehend aus jeweils fünf bis sechs PCs, die insbesondere für redaktionelle Recherche und Video- und Audiobearbeitung geeignet sind. Diese MultiMediaLabs werden intensiv genutzt und finden für interne wie externe Fortbildungen Verwendung.

- Ein mobiles MultiMediaLab wird intensiv sowohl für die Produktion von Multimedia als auch für die Nutzung des Internets eingesetzt.

[6] Platform for privacy preferences
[7] bei dem Begriff MultiMediaLabs steht „Lab“ für Labor. Die Offenen Kanäle sind durch die MultiMediaLabs auch zu Internetcafe’s geworden.

- Im Rahmen der Offenen Kanal-Projekte „Fischauge“, ein rollendes Videocamp, oder „Floh im Ohr“, ein rollendes Audiocamp, kommt das mobile MultiMediaLab im ländlichen Raum, beispielsweise direkt auf dem Dorfplatz, zum Einsatz.

- Das Planspiel „MachtMedienMacht“, u. a. für Schulklassen und Jugendgruppen konzipiert, bei dem es um Mediengestaltung und Medienkonzentration geht und das PC-basiert arbeitet, steht vor dem ersten Testlauf.

Während bei Einführungen in die Nutzung von Multimedia und Internet Datenschutz und Datensicherheit naturgemäß eine große Rolle spielen, ist dies bei der aktiven Produktion von Multimedia kein Schwerpunkt der Arbeit.
Als Brückenschlag zwischen Filmwirtschaft und Bildung werden durch das Projekt „Lernort Kino - Schulfilmwoche in Schleswig-Holstein“ in allen Schularten Filme in einem ortsnahen Kino präsentiert. Im Rahmen dieser landesweiten Aktionswoche werden Schülerinnen und Schüler verschiedener Altersgruppen im Unterricht durch ergänzende Begleitmaterialien an einen kritischen Umgang mit dem Medium Film herangeführt. Hierdurch soll die Medienkompetenz der Schülerinnen und Schüler nachhaltig gestärkt werden.

Frage 19

Inwieweit findet das Thema “Datenschutz” Berücksichtigung im Schulunterricht – auch im Rahmen der Initiative “Schulen ans Netz”?

Antwort:

Fragestellungen des Datenschutzes werden in den Lehrplänen für alle Schularten– insbesondere im Lehrplan Informatik in der Sekundarstufe II (Gymnasium, Gesamtschule, Fachgymnasium) – thematisiert. Im Rahmen des Sachgebiets „Auswirkung auf den Einzelnen, die Gesellschaft und die Umwelt“ sind Datenschutzbestimmungen, Datensicherung, Datensicherheit, Schützen von Dateien und Zugriffsrechte verbindliche Inhalte.

Adressaten für Fragen des Datenschutzes sind neben den Schülerinnen, Schülern und Lehrkräften auch die Schulleitungen und das Schulverwaltungspersonal. Das Institut für Praxis und Theorie der Schule (IPTS) hat in den letzten Jahren sehr erfolgreich die Veranstaltung „Datenschutz an der Schule“ gemeinsam mit dem ULD angeboten. Auf der Bildungsmesse ProNetS wurde diesem Thema 2001 ein gebührender Raum zur Information der Schulen und Schulträger eingeräumt.

Im Mai 2002 ist allen Schulen die Verschlüsselungssoftware „GnuPP“ zugesendet worden (mit einem einführenden Begleitschreiben, ausführlichem Begleitheft und Sonderseiten auf dem Landesbildungsserver), um eine weitere Sensibilisierung für Datensicherheit zu gewährleisten.

Frage 20

Strebt die Landesregierung eine Vorreiterrolle bei der Einführung eines Datenschutzaudits in der öffentlichen Verwaltung an?
Ist die Förderung aus öffentlichen Mitteln von Projekten mit Bezug auf Informations- und Kommunikationstechnologie an die Bedingungen des Gütesiegels für den Datenschutz gebunden?
Falls nein, ist dieses beabsichtigt?

Antwort:

Schleswig-Holstein war das erste Land, das mit dem neuen Landesdatenschutzgesetz vom 9. Februar 2000 erstmals auch ein Datenschutzaudit nach § 43 Abs. 2 LDSG (sog. Behördenauditverfahren) eingeführt hat. Dies ermöglicht den öffentlichen Stellen, ihr Datenschutzkonzept durch das ULD prüfen und beurteilen zu lassen. Zwischenzeitlich wurde das ULD von verschiedenen Landes- und Kommunalbehörden beauftragt, ein Behördenauditverfahren durchzuführen.
Durch die Einführung dieses neuen Verfahrens und die Förderung dieses Projektes im Rahmen des Landesprogramms „e-Region Schleswig-Holstein“ durch die Europäische Union mit dem Ministerium für Wirtschaft Technik und Verkehr und der Technologiestiftung Schleswig-Holstein hat die Landesregierung bereits eine gewisse Vorreiterrolle übernommen.

Die Förderung von Projekten mit Bezug auf Informations- und Kommunikationstechnologie ist bisher nicht daran gebunden, dass das IT-Produkt ein Gütesiegel aufgrund des Datenschutzaudit-Verfahrens nach § 4 Abs. 2 LDSG erhalten hat. Die Landesregierung hält es nicht für richtig, zusätzliche Hürden für eine Projektförderung zu errichten.

Frage 21

Ist der Patienten-Datenschutz ein Qualitätsmerkmal beim Konzept für den Gesundheitsstandort Schleswig-Holstein?
Falls ja, in welcher Weise; falls nein, warum nicht?

Antwort:

Ja. Aus Sicht der Landesregierung kommt dem Datenschutz im gesundheitlichen Bereich eine hohe Bedeutung zu.

Im Rahmen der Gesundheits-Initiative der Landesregierung z.B. bei der Gesundheitskarte Schleswig-Holstein ist Patienten-Datenschutz fester Bestandteil in der konzeptionellen Entwicklung und in den Umsetzungsschritten. Dies wird nicht zuletzt durch die unmittelbare Teilnahme des ULD in der Projektgruppe gewährleistet.

Der Patienten-Datenschutz wird im Wesentlichen durch strafrechtliche, berufsrechtliche sowie öffentlich-rechtliche (BDSG, LDSG) Rechtsnormen geregelt. Hierdurch wird das Persönlichkeitsrecht der Patientin/des Patienten umfassend geschützt. Die Ärztekammer Schleswig-Holstein hat gemeinsam mit dem ULD sowie der Zahnärztekammer Schleswig-Holstein - unter der Schirmherrschaft der Gesundheitsministerin - eine Aktion "Datenschutz in meiner Arztpraxis" ins Leben gerufen, in welcher sehr detailliert Probleme des Persönlichkeitsschutzes in verschiedenen Situationen in der Praxis angesprochen und einer Lösung zugeführt werden. Eine vergleichbare Aktion im stationären Bereich ist in der Planung.

Die Einhaltung des Patienten-Datenschutzes im Krankenhausbereich obliegt jedem Krankenhausträger selbst. Für die öffentlichen Träger gilt das LDSG. Werden z.B. Pati-

entendaten zu Abrechnungszwecken an Dritte weitergegeben, sind die Vorschriften des Abschnitts II des LDSG zu beachten.
So beinhaltet das LDSG allumfassend die Bestimmungen, die ansonsten bzw. andernfalls in bereichsspezifische Datenschutzregelungen einzubeziehen wären.
Gegenüber nicht-öffentlichen Trägern führt das ULD die Aufsicht über die Einhaltung der entsprechenden Bestimmungen des Bundesdatenschutzgesetzes (§ 39 Abs. 2 LDSG).
Somit sind die gesetzlichen Voraussetzungen für die Einhaltung des Patientendatenschutzes als wichtiges Qualitätsmerkmal für das Konzept des Gesundheitsstandortes Schleswig-Holstein vorhanden.
Aktuelle spezialgesetzliche Regelungen enthalten § 6 (3) und § 16 des Gesundheitsdienstgesetzes (GDG), sowie die §§ 27 ff. des Gesetzes zur Hilfe und Unterbringung psychisch kranker Menschen (PsychKG) und die §§ 22 ff. des Maßregelvollzugsgesetzes (MVollzG).
Ausgestaltung und Verfahren des Krebsregisters des Landes Schleswig-Holstein entsprechen höchsten Datenschutzanforderungen. Auch hier wurde bereits während der Konzeption auf die aktive Einbindung des Datenschutzes geachtet.

Anlage zur Antwort auf Frage 6

Sachgebiet IV
10. Rechtsverkehr in Abgabensachen

zweiseitige Verträge

Ägypten	17.11.1959
Belgien	11.04.1967
Dänemark	30.01.1962
Finnland	25.09.1935
Unterstützung in Zollangelegenheiten	16.05.1975
Frankreich	21.07.1959
Griechenland	18.04.1966
Irland	17.10.1962
Island	
Unterstützung in Zollangelegenheiten	11.10.1977
Italien	09.06.1938
Jugoslawien, ehemaliges	02.04.1974
Kanada	
Unterstützung der Zollverwaltungen	10.09.1984
Luxemburg	23.08.1958
Norwegen	18.11.1958
Unterstützung in Zollangelegenheiten	11.07.1974
Österreich (3 Verträge)	04.10.1954
Finanz- und Ausgleichsvertrag	27.11.1961
Zoll-, Verbrauchssteuer- und Monopolangelegenheiten	11.09.1970
Pakistan	07.08.1958
Polen	
Unterstützung der Zollverwaltungen	29.07.1992
Russische Föderation	
Unterstützung der Zollverwaltungen	16.12.1992
Schweden	
Unterstützung der Zollverwaltungen	18.12.1972
Spanien	05.12.1966
Unterstützung der Zollverwaltungen	27.11.1969
Tschechische Republik	
Unterstützung der Zollverwaltungen	19.05.1995

Sachgebiet IV
10. Rechtsverkehr in Abgabensachen

Ungarn	
Unterstützung der Zollverwaltungen	18.12.1991
Vereinigtes Königreich	26.11.1964
Vereinigte Staaten	22.07.1954
Unterstützung der Zollverwaltungen	23.08.1973
mehrseitige Verträge	
Verwaltungshilfe im Zollwesen	05.12.1953
Empfehlung des Brüssler Zollrates zur zentralen Erfassung von Auskünften über Zollhinterziehungen	08.06.1967
Gegenseitige Unterstützung der Zollverwaltungen	07.09.1967
Empfehlung des Brüsseler Zollrates zur zentralen Erfassung von Auskünften über Zollhinterziehungen	22.05.1975

Sachgebiet IV
11. Zusammenarbeit in Strafsachen

zweiseitige Verträge

Belgien	
Forst-, Feld-, Fischerei- und Jagdfrevel	29.04.1885
Rechtshilfe	17.01.1958
Ergänzung des Europäischen Rechtshilfeübereinkommens	18.07.1975
Brasilien	16.06.1926
Strafregister	15.05.1957
Dänemark	
Ergänzung des Europäischen Rechtshilfeübereinkommens	22.07.1971
Finnland	14.05.1937
Frankreich	
Deutsche Gerichtsbarkeit für die Verfolgung bestimmter Verbrechen	02.02.1971
Ergänzung des Europäischen Rechtshilfeübereinkommens	24.10.1974
Griechenland	
Ergänzung des Europäischen Rechtshilfeübereinkommens	29.05.1976
Irak	
Austausch von Festnahme- und Verhaftungsmitteilungen	29.11.1958
Israel	
Zollstrafsachen	19.09.1966
Ergänzung des Europäischen Rechtshilfeübereinkommens	20.07.1977
Italien	
Ergänzung des Europäischen Rechtshilfeübereinkommens	24.10.1979
Jugoslawien, ehemaliges	
Rechtshilfe in Strafsachen	01.10.1971
Kenia	20.06.1970
Libanon	12.06.1956
Liechtenstein	29.05.1958
Luxemburg	
Forst-, Jagd- und Fischereifrevel	09.02.1849
Rechtshilfe in ausländerpolizeilichen Angelegenheiten	31.05.1961
Marokko	17.07.1958
Mexiko	18.12.1956
Monaco	21.05.1962

Sachgebiet IV
11. Zusammenarbeit in Strafsachen

Niederlande	
Ergänzung des Europäischen Rechtshilfeübereinkommens	30.08.1979
Norwegen	
Ergänzung des Europäischen Rechtshilfeübereinkommens	22.10.1973
Österreich	
Steuerstrafsachen	04.10.1954
Ergänzung des Europäischen Rechtshilfeübereinkommens	31.01.1972
Portugal	
Rechtshilfe	15.06.1964
Schweden	
Notenwechsel zum Europäischen Rechtshilfeübereinkommen	27.08.1976
Schweiz	
Ergänzung des Europäischen Rechtshilfeübereinkommens	13.11.1969
Senegal	17.04.1969
Tschechische Republik	
Ergänzung des Europäischen Rechtshilfeübereinkommens	02.02.2000
Tunesien	19.07.1966
Türkei	
Geschäftsweg	07.11.1974
Vereinigtes Königreich	02.05.1961
Vereinigte Staaten	03.11.1961
mehrseitige Verträge	
Europäisches Rechtshilfeübereinkommen	20.04.1959
Übereinkommen zwischen den Mitgliedstaaten der Europäischen Gemeinschaften über das Verbot der doppelten Strafverfolgung	25.05.1987
Übereinkommen über Geldwäsche sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten	08.11.1990

Sachgebiet IV
12. Auslieferung in Strafsachen

zweiseitige Verträge

Australien	14.04.1987
Bahamas	14.05.1872
Belgien	17.01.1958
Dänemark	
Ergänzung des Europäischen Auslieferungsübereinkommens	22.07.1971
Vereinbarung zu Artikel 5 des Europäischen Auslieferungsabkommens	09.09.1985
Dominica	14.05.1872
Fidschi	14.05.1872
Ghana	10.06.1966
Grenada	14.05.1872
Italien	
Ergänzung des Europäischen Auslieferungsübereinkommens	24.10.1979
Notenwechsel zum Europäischen Auslieferungsübereinkommen	19.05.1976
Jamaika	14.05.1872
Jugoslawien, ehemaliges	26.11.1970
Kanada	11.07.1977
Kenia	14.05.1872
Lesotho	14.05.1872
Luxemburg	09.03.1876
Malawi	14.05.1872
Malta	14.05.1872
Mauritius	14.05.1872
Monaco	21.05.1962
Niederlande	
Ergänzung des Europäischen Auslieferungsübereinkommens	30.08.1979
Norwegen	
Ergänzung des Europäischen Auslieferungsübereinkommens	22.10.1973
Vereinbarung zu Artikel 5 des Europäischen Auslieferungsübereinkommens	19.08.1985
Österreich	
Ergänzung des Europäischen Auslieferungsübereinkommens	31.01.1972
Portugal	15.06.1964

Sachgebiet IV
12. Auslieferung in Strafsachen

Schweden	
Notenwechsel zum Europäischen Auslieferungsübereinkommen	27.08.1976
Vereinbarung zu Artikel 5 des Europäischen Auslieferungsübereinkommens	16.03.1978
Schweiz	
Ergänzung des Europäischen Auslieferungsübereinkommens	13.11.1969
Seychellen	14.05.1872
Spanien	
Vereinbarung zu Artikel 5 des Europäischen Auslieferungsübereinkommens	14.03.1986
St. Christoph und Nevis	14.05.1872
St. Lucia	14.05.1872
St. Vincent und die Grenadinen	14.05.1972
Swasiland	14.05.1872
Thailand	26.05.1993
Tonga	14.05.1972
Trinidad und Tobago	14.05.1872
Tschechische Republik	
Ergänzung des Europäischen Auslieferungsübereinkommens	02.02.2000
Tunesien	19.07.1966
Türkei	03.09.1930
Uganda	14.05.1872
Vereinigtes Königreich	14.05.1872
Vereinigte Staaten	20.06.1978
mehrseitige Verträge	
Europäisches Auslieferungsübereinkommen	13.12.1957
Bekämpfung des Terrorismus	27.01.1977
Überstellung verurteilter Personen	21.03.1983
Vereinfachung und Modernisierung der Verfahren zur Übermittlung von Auslieferungsersuchen	26.06.1989
Vereinfachte Auslieferungsverfahren zwischen den Mitgliedstaaten der Europäischen Union	10.03.1995
Auslieferung zwischen den Mitgliedstaaten der Europäischen Union	27.09.1996

Sachgebiet IV
13. Bekämpfung von Straftaten

zweiseitige Verträge

Bulgarien	
Bekämpfung der organisierten Kriminalität und der Rauschgiftkriminalität	14.09.1992
Frankreich	
Zusammenarbeit der Polizeibehörden im deutsch-französischen Grenzbereich	03.02.1977
Zusammenarbeit bei der Bekämpfung von nicht angemeldeter Erwerbstätigkeit und des grenzüberschreitenden Missbrauchs bei mit einer Erwerbstätigkeit verbundenen Sozialleistungen sowie auf dem Gebiet der grenzüberschreitenden Leiharbeit	31.05.2001
Litauen	
Zusammenarbeit bei der Bekämpfung der organisierten Kriminalität, des Terrorismus und anderer Straftaten mit erheblicher Bedeutung	23.02.2001
Polen	
Bekämpfung der organisierten Kriminalität	06.11.1991
Rumänien	
Zusammenarbeit bei der Bekämpfung der organisierten Kriminalität sowie des Terrorismus und anderer Straftaten von erheblicher Bedeutung	15.10.1996
Slowenien	
Zusammenarbeit bei der Bekämpfung von Straftaten mit erheblicher Bedeutung	02.03.2001
Sowjetunion, ehemalige	
Suchtstoffe, psychotrope Stoffe	13.06.1989
Tschechoslowakei, ehemalige	
Bekämpfung der organisierten Kriminalität	13.09.1991
Ungarn	
Bekämpfung der organisierten Kriminalität	22.03.1991
Usbekistan	
Zusammenarbeit bei der Bekämpfung der organisierten Kriminalität, des Terrorismus und anderer Straftaten von erheblicher Bedeutung	16.11.1995
Vereinigte Staaten	
Betäubungsmittel	07.03.1956

Sachgebiet IV
13. Bekämpfung von Straftaten

Vietnam	
Verbrechensvorbeugung und -bekämpfung	28.02.1996
mehrseitige Verträge	
Alkoholschmuggel	19.08.1925
Bekämpfung der Bestechung	17.12.1997
Bekämpfung von Piratensendern	22.10.1965
Bekämpfung der widerrechtlichen Inbesitznahme von Luftfahrzeugen	16.12.1970
Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Zivilluftfahrt	23.09.1971
Bekämpfung des Terrorismus	27.01.1977
Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Seeschifffahrt	10.03.1988
Betäubungsmittel	
Opiumabkommen	23.01.1912
	19.02.1925
Betäubungsmittel	13.07.1931
Überwachung von sonstigen Rauschgiften	19.11.1948
Anbau von Mohnpflanzen und Erzeugung von Opium	23.06.1953
Suchtstoffe	30.03.1961
Psychotrope Stoffe	21.02.1971
Suchtstoffe, psychotrope Stoffe	20.12.1988
Suchtstoffe, psychotrope Stoffe, unerlaubter Verkehr auf See	31.01.1995
Branntweinhandel unter Nordseefischern	16.11.1887
Diplomatenschutzkonvention	14.12.1973
Falschmünzerei	20.04.1929
Fischerei	
Überfischung	05.04.1946
Fischerei im Nordostatlantik	24.01.1959
Lachsbestand in der Ostsee	20.12.1962
Frauen- und Kinderhandel	
Schutz gegen Mädchenhandel	18.05.1904
Bekämpfung des Mädchenhandels	04.05.1910
Unterdrückung des Frauen und -kinderhandels	30.09.1921
Geiselnahme, Internationales Übereinkommen	18.12.1979
Geldwäsche sowie Ermittlung, Beschlagnahme und Einziehung aus Straftaten	08.11.1990
Kontrolle des Erwerbs und Besitzes von Schusswaffen durch Einzelpersonen	28.06.1978

Sachgebiet IV
13. Bekämpfung von Straftaten

Menschenrechte und Grundfreiheiten	04.11.1950
Revidierte Rheinschifffahrtsakte	17.10.1868
Rotkreuz-Abkommen	12.08.1949
Schutz der finanziellen Interessen der Europäischen Gemeinschaften	26.07.1995
Schutz der unterseeischen Telegrafenkabel	14.03.1884
Sicherheit von Personal der Vereinten Nationen und beigeordnetem Personal	15.12.1994
Sklaverei	25.09.1926
	07.09.1956
Strafbare Handlungen an Bord von Luftfahrzeugen	14.09.1963
Strafgerichtshof, Internationaler, Römisches Statut	17.07.1998
Unzüchtige Veröffentlichungen	04.05.1910
Verschmutzung der See durch Öl	12.05.1954
Völkermord	09.12.1948
Zollverwaltungen, gegenseitige Amtshilfe und Zusammenarbeit	18.12.1997