36. Jahresbericht
der Landesbeauftragten für Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen Bericht über das Ergebnis der Tätigkeit im Jahr 2013. Redaktionsschluss für die Beiträge war der 31. Dezember 2013.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. 2013: Das Informationsimperium schlägt zu(rück)

Der bremische Vorsitz der Konferenz der Datenschutzbeauftragten des Bundes und der Länder fiel in spannende Zeiten für die informationelle Selbstbestimmung der Menschen. Allerdings ahnten wir alle zu Beginn des Jahres 2013 noch nicht, dass dieses Jahr weltweit eines der denkwürdigsten für die Datenschutzgrundrechte sein würde.

Im Januar war die datenschutzrechtliche Aufmerksamkeit noch ganz auf das Innere des deutschen Gesetzgebungsapparates gerichtet. Wir sahen uns mit einer Attacke auf den Beschäftigtendatenschutz konfrontiert, die dank einer großen Woge der Sympathie für die Rechte der Beschäftigten gegen Angriffe auf ihre informationelle Selbstbestimmung pariert werden konnte (siehe dazu die Entschließung "Beschäftigtendatenschutz nicht abbauen, sondern stärken!" der Datenschutzkonferenz vom 25. Januar 2013 unter Ziffer 22.1). Der als Überraschungscoup auf die Tagesordnung des Bundestages gelangte Antrag zur Änderung des Bundesdatenschutzgesetzes wurde nach wenigen Wochen heftiger öffentlicher Debatte abgesetzt.

Bei der Frühjahrstagung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder Mitte März in Bremerhaven hatte sich der datenschutzrechtliche Blick auf Europa erweitert. Die Kommission der Europäischen Union (EU) hatte im Jahr 2012 den Entwurf einer Datenschutz-Grundverordnung vorgelegt. Die Datenschutzkonferenz wandte sich gegen diejenigen Änderungsvorschläge von Abgeordneten des Europäischen Parlaments, deren Umsetzung das Grundrecht auf Datenschutz schwächen würde. Diese Anträge scheinen von Lobbyistinnen und Lobbyisten der großen Internetfirmen und anderen inspiriert, die die Erkenntnis noch nicht erreicht hat, dass das Vertrauen der Menschen in das Internet Voraussetzung der wirtschaftlichen Nutzung dieses Mediums ist. Die Webseite www.lobbyplag.eu weist nach, dass Texte aus Lobbypapieren zum Teil wortwörtlich in Anträgen auftauchen. Als Reaktion auf den Ansturm der Anti-Datenschutzlobby formulierte die Datenschutzkonferenz zehn unhintergehbare Thesen, die eine europäische Datenschutzreform beachten muss, um die Datenschutzgrundrechte der Europäerinnen und Europäer wirksam schützen zu können:

- Jedes personenbeziehbare Datum muss geschützt werden.
- Es darf keine grundrechtsfreien Räume geben.
- Einwilligungen müssen ausdrücklich erteilt werden.
- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern.
- Profilbildungen müssen beschränkt werden.
- Die Eigenverantwortung der Datenverarbeiter muss durch machtvolle betriebliche Datenschutzbeauftragte gestärkt werden.

- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können.
- Die völlige Unabhängigkeit der Aufsichtsbehörden muss auch gegenüber der Kommission bestehen.
- Grundrechtsschutz braucht effektive Kontrollen.
- Gewährleistung eines hohen Datenschutzstandards für ganz Europa.

Auf der Grundlage dieser Thesen bewerteten die Landesbeauftragten Bremens, Bayerns und Berlins die in die Tausende gehenden Änderungsanträge zum Kommissionsentwurf aus den Reihen des Europäischen Parlamentes. Als Konferenzvorsitzende hatte ich die Gelegenheit, diese Position den zuständigen Abgeordneten des Europäischen Parlamentes in Brüssel deutlich zu machen.

1.1 Die NSA-Affäre

Anfang Juni 2013 platzte dann die Bombe: Die "Washington Post" und der britische "Guardian" veröffentlichten und bewerteten erste geheime Dokumente der US-amerikanischen National Security Agency (NSA), die Edward Snowden, der ehemalige Angestellte einer für die NSA arbeitenden Internetfirma, diesen Zeitungen übergeben hatte. Die Dokumente wiesen auf massenhafte und anlasslose Überwachungspraktiken der NSA hin. Sofort wurde deutlich, dass es sich um weltweite Aktivitäten handelt. Von da an riss die Kette der Veröffentlichungen zu diesem Thema nicht ab.

1.1.1 Die Bundesregierung muss sich schützend vor die Grundrechte stellen

In ihrer Pressemitteilung von Ende Juni stellte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass das Grundrecht auf informationelle Selbstbestimmung weder von inländischen noch von ausländischen Stellen verletzt werden darf. Angesichts der Enthüllungen über die umfassenden und anlasslosen Überwachungsmaßnahmen der US-amerikanischen und der britischen Geheimdienste, auf deren Überwachungsmaßnahmen durch das Government Communications Headquarters (GCHQ) sich weitere Enthüllungen bezogen, formulierte die Datenschutzkonferenz ihre äußerste Besorgnis darüber, dass sich die Hinweise dafür verdichtet hatten, dass ein großer Teil des Kommunikationsverhaltens auch der Menschen in Deutschland ohne ihr Wissen von diesen Geheimdiensten überwacht wird.

Die Datenschutzkonferenz forderte die Bundesregierung erstmalig auf, alles zu unternehmen, um die Menschen in Deutschland vor informationellen Zugriffen Dritter zu schützen, die mit der Verfassungsordnung des Grundgesetzes nicht im Einklang stehen. Die Bundesregierung müsse für eine restlose Aufklärung des Sachverhaltes sorgen und dabei auch die Frage beantworten, ob deutsche Behörden diese Informationen übermittelt

bekamen und verwendeten. Daneben appellierte die Datenschutzkonferenz an die Bundesregierung, sich sofort in Brüssel für ein hohes Datenschutzniveau und für Regelungen einzusetzen, die umfassende und anlasslose Überwachungsmaßnahmen europäischer wie außereuropäischer Stellen ausschließen. Damit pochte die Datenschutzkonferenz auf das Recht der Menschen darauf, dass sich ihre Bundesregierung aktiv dafür einsetzt, dass das Grundrecht auf informationelle Selbstbestimmung weder von inländischen noch von ausländischen Stellen verletzt wird.

Nach einer Sitzung des Parlamentarischen Kontrollgremiums erklärte der für die Koordination der Nachrichtendienste zuständige Kanzleramtsminister Ronald Pofalla Mitte August: "Die Vorwürfe sind vom Tisch. (...) Die NSA und der britische Nachrichtendienst haben erklärt, dass sie sich in Deutschland an deutsches Recht halten. (...) Der Datenschutz wurde zu einhundert Prozent eingehalten." Dem widersprach die Datenschutzkonferenz, indem sie sich am 5. September 2013 unter dem Motto "Zeit für Konsequenzen" in der Bundespressekonferenz gegen die umfassende und anlasslose Überwachung der elektronischen Kommunikation durch Nachrichtendienste wandte. Schon die bisherigen Erkenntnisse ließen den Schluss zu, dass die Aktivitäten unter anderem des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinausliefen, zumal große Internetunternehmen und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden seien. Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den Vereinigten Staaten von Amerika (USA) stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiteten, beträfen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachten, auch ihre Daten. Unklar sei daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Es hatte den Anschein, dass sich angesichts des Ausmaßes der bekannt gewordenen Überwachung zu diesem Zeitpunkt auch bei denjenigen Resignation breit gemacht hatte, die Abwehrmaßnahmen treffen mussten. Daher betonte die Datenschutzkonferenz, dass es die staatliche Pflicht zum Schutz der Grundrechte erfordert, sich nicht mit der Situation abzufinden, sondern sich schützend vor die Grundrechte der Menschen in der Bundesrepublik Deutschland zu stellen und verfassungswidrige Situationen zu beenden. Die Datenschutzbeauftragten forderten die Regierungen und Parlamente des Bundes und der Länder auf, nationales, europäisches und internationales Recht zu ändern, verfassungswidrige nachrichtendienstliche Kooperationen abzustellen, die Kontrolle der Nachrichtendienste zu intensivieren, Initiativen zum Schutz der informationellen Selbstbestimmung und des Grundrechts auf Vertraulichkeit und Integrität

informationstechnischer Systeme zu starten, völkerrechtliche Abkommen wie das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehrs auf den Prüfstand zu stellen und auch innerhalb der Europäischen Union sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung der Europäischen Grundrechtecharta erfolgt.

1.1.2 Keine unsicheren Häfen anlaufen

Die massenhaften und anlasslosen Überwachungen durch Geheimdienste der USA gefährden den Datenverkehr zwischen Deutschland und den USA. Nach der gegenwärtig geltenden europäischen Datenschutzrichtlinie dürfen Daten von EU-Bügerinnen und EU-Bürgern in Staaten außerhalb der Europäischen Union (EU) nur dann übermittelt werden, wenn im Empfängerstaat ein dem EU-Recht vergleichbares Datenschutzniveau besteht. Das ist nach Auffassung der Kommission bei den USA nicht der Fall. Die Europäische Kommission hat im Jahr 2000 die Entscheidung getroffen, wonach solche Daten gleichwohl ausnahmsweise in die USA übermittelt werden dürfen, wenn sie dort in einem "sicheren Hafen" ("Safe Harbor") landen. Um sich als "sicherer Hafen" zu qualifizieren, können sich US-Unternehmen auf einer Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die in der entsprechenden Entscheidung der Kommission niedergelegten Grundsätze und die dort formulierten FAQ (frequently asked questions = häufig gestellte Fragen) zu beachten.

In ihrer Pressemitteilung von Ende Juli 2013 wies die Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf die Befugnisse hin, die den datenschutzrechtlichen Aufsichtsbehörden beim internationalen Datenverkehr zwischen Unternehmen in Deutschland und Drittstaaten nach dem Bundesdatenschutzgesetz und der europäischen Datenschutzrichtlinie zustehen. Nationale Aufsichtsbehörden können die Datenübermittlung in die USA aussetzen, wenn eine "hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt sind. Dieser Fall ist nach Auffassung der Datenschutzkonferenz angesichts der Berichte über die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste eingetreten. Die Grundsätze in den Kommissionsentscheidungen seien mit hoher Wahrscheinlichkeit verletzt, weil die NSA und andere ausländische Geheimdienste nach den vorliegenden Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugriffen, die von Unternehmen in Deutschland an Stellen in den USA übermittelt würden. Zwar enthalte die Safe-Harbor-Entscheidung eine Regelung, die die Geltung der Grundsätze des "sicheren Hafens" begrenze, sofern es die nationale Sicherheit erfordere oder Gesetze solche Ermächtigungen vorsähen. Im Hinblick auf das Ziel eines wirksamen Schutzes der Privatsphäre solle jedoch von diesen Eingriffsbefugnissen nur im Rahmen des tatsächlich

Erforderlichen und nicht exzessiv Gebrauch gemacht werden. Ein umfassender und anlassloser Zugriff auf personenbezogene Daten könne daher durch Erwägungen zur nationalen Sicherheit in einer demokratischen Gesellschaft nicht gerechtfertigt werden. Auch bei Datenübermittlungen in die USA aufgrund der Standardverträge müsse der Datenimporteur zusichern, dass seines Wissens in seinem Land keine Rechtsvorschriften bestehen, die die Garantien aus den Klauseln in gravierender Weise beeinträchtigen. Eine solche Generalermächtigung scheine aber in den USA zu bestehen; denn nur so lasse sich erklären, dass der US-amerikanische Geheimdienst auf personenbezogene Daten, die aufgrund der Standardverträge übermittelt werden, mit hoher Wahrscheinlichkeit routinemäßig zugreife.

In diesem Zusammenhang forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Bundesregierung auf, plausibel darzulegen, dass der unbeschränkte Zugriff ausländischer Nachrichtendienste auf die personenbezogenen Daten der Menschen in Deutschland effektiv im Sinne der genannten Grundsätze begrenzt werde. Bevor dies nicht sichergestellt sei, würden die Aufsichtsbehörden für den Datenschutz keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten (zum Beispiel auch zur Nutzung bestimmter Cloud-Dienste [Dienste, die im Internet bereitgestellt werden]) erteilen und prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen seien. Auch forderte die Datenschutzkonferenz die Europäische Kommission auf, ihre Entscheidungen zu Safe Harbor und zu den Standardverträgen vor dem Hintergrund der exzessiven Überwachungstätigkeit ausländischer Geheimdienste bis auf Weiteres zu suspendieren.

Auf diese Pressemitteilung erhielt die Datenschutzkonferenz viele Reaktionen in Deutschland, auf EU-Ebene, aber auch aus den USA. In einer Anhörung des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) in Straßburg hatte ich im Oktober die Gelegenheit, den Abgeordneten des Europäischen Parlamentes die Position der Datenschutzkonferenz zu erläutern. Die Untersuchungen des dort ebenfalls befragten Sachverständigen Christopher Conolly ergeben im Übrigen, dass die Selbstbezeichnung als Safe-Harbor-Unternehmen oftmals in die Irre führt. Die Liste derjenigen Unternehmen, die sich fälschlicherweise als "sichere Häfen" bezeichneten, sei im September des Berichtsjahres mit 427 Unternehmen der weniger als 3.000 Safe-Harbor-Unternehmen mehr als doppelt so lang wie im Jahr 2008 (208 Unternehmen) gewesen.

1.1.3 Drei Konsequenzen aus der NSA-Affäre

Aus Sicht der informationellen Selbstbestimmung der Menschen muss es drei Konsequenzen aus der NSA-Affäre geben: Wir brauchen Transparenz über die Datenflüsse von und zu Nachrichtendiensten, wir müssen den Gefahren der Privatisierung der

Gewährleistung von Sicherheit begegnen und wir müssen die Handlungsmacht gegenüber ausländischen Datensammlern zurückgewinnen.

Transparenz über die Datenflüsse von und zu Nachrichtendiensten herstellen

Die erste Konsequenz aus der NSA-Affäre muss die Herstellung von Informationsfreiheit auch für den Bereich der Nachrichtendienste sein. Informationsfreiheit garantiert den Menschen die Transparenz des öffentlichen Bereichs. Das auf diesem Wege gewonnene Wissen ist Voraussetzung für die demokratische Willensbildung. Die Enthüllungen Edward Snowdens zeigen, dass die riesigen Datenpools, die private Telekommunikationsdienste und Internetdienste vorhalten, nicht nur von diesen selbst, sondern auch von Nachrichtendiensten genutzt werden. Ihm ist es zu verdanken, dass wir mehr und mehr über die Datenflüssen von und zu Nachrichtendiensten erfahren. In demokratischen Rechtsstaaten kann es aber nicht darauf ankommen, dass ein Whistleblower mit Insiderkenntnissen mit diesen Informationen an die Öffentlichkeit geht.

In ihrer Entschließung vom 27. Juni 2013 forderte die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb die Verantwortlichen in Deutschland und Europa auf, für Transparenz von Sicherheitsbehörden auf nationaler und internationaler Ebene zu sorgen. Das Vertrauen der Bevölkerung könne nur zurückgewonnen werden, wenn die Aufgaben und Befugnisse der Sicherheitsbehörden völkerrechtlich festgelegt und deren tatsächliche Arbeitsweisen nachvollziehbar seien. Zweifellos verfügten die Nachrichtendienste über Informationen, die nicht offengelegt werden dürften. Gleichwohl halte die Konferenz der Informationsfreiheitsbeauftragten die pauschale Ausnahme der Nachrichtendienste des Bundes und der Länder vom Anwendungsbereich der Informationsfreiheitsgesetze und Transparenzgesetze für nicht hinnehmbar und erwarte von den Gesetzgebern entsprechende Verbesserungen. Darüber hinaus bedürften die weit gefassten Ausnahmeregelungen für Sicherheitsbelange in den Informationsfreiheitsgesetzen und Transparenzgesetzen einer Überprüfung und Einschränkung. Gleichzeitig unterstützten die Informationsfreiheitsbeauftragten die Verbesserung der Transparenz der nachrichtendienstlichen Aktivitäten gegenüber den Parlamenten und die Stärkung der parlamentarischen Kontrollgremien.

Der Privatisierung der Sicherheitspolitik entgegenwirken

Die zweite Konsequenz aus der NSA-Affäre muss die Auseinandersetzung mit der Privatisierung der Sicherheitspolitik sein. In seinem 2007 erschienenen Buch "Das Ende der Privatsphäre" warnte Peter Schaar davor, die Wirtschaft werde zum "Hilfssheriff der Strafverfolgungsbehörden". Angesichts der Enthüllungen von Edward Snowden sehen wir, dass es inzwischen eine unauflösbar scheinende Verquickung zwischen privater Datenansammlungswut und Datenanalysewut ungeahnten Ausmaßes und

sicherheitspolitischer Überwachungstätigkeit gibt. Was zuerst da war, ist wie bei der Frage nach der Henne und dem Ei, schwer zu entscheiden.

Auf der einen Seite weckt die Tatsache, dass private Stellen große Mengen von Daten produzieren und nutzen, Begehrlichkeiten auch bei öffentlichen Stellen. Nicht nur US-amerikanischen Internetdiensteanbieter und Telekommunikationsanbieter sind gesetzlich verpflichtet, Verbindungsdaten ihrer Kundinnen und Kunden an Polizeibehörden und Nachrichtendienste zu geben.

Aber auch dadurch, dass Private direkt mit der Erfüllung von Aufgaben der öffentlichen Sicherheit betraut werden, verwischen die Grenzen zwischen der durch öffentliche Stellen zu gewährleistenden öffentlichen Sicherheit und den privaten Gehilfinnen und Gehilfen, derer sich die öffentlichen Stellen bedienen. Süddeutsche Zeitung und Norddeutscher Rundfunk haben im Berichtsjahr über den "Geheimen Krieg" (www.geheimerkrieg.de), den US-amerikanische Regierungsorganisationen von deutschem Boden aus mit Hilfe von unbemannten Drohnen führen, recherchiert. Dabei wurde deutlich, dass im Bereich der Sicherheitspolitik private und staatliche Sicherheitsorganisationen Hand in Hand arbeiten und die Übergänge zwischen diesen Organisationen fließend sind. Edward Snowden war zunächst Techniker für IT-Sicherheit des US-amerikanischen Auslandsnachrichtendienstes Central Intelligence Agency (CIA). Bis zum Juni 2013 war er bei der privaten Sicherheitsfirma Booz Allen Hamilton beschäftigt. Dort führte Snowden als Infrastruktur-Analytiker und einer von 24.500 Mitarbeiterinnen und Mitarbeitern Aufträge aus, die die Firma von der NSA erhalten hatte. Alle Dokumente über die umfassende und anlasslose Überwachung durch US-amerikanische und andere Nachrichtendienste, die nun sukzessive veröffentlicht werden, konnte er als Mitarbeiter einer privaten Firma erhalten.

Der Privatisierung der öffentlichen Sicherheit und der damit verbundenen Erosion der Grundrechtsgeltung im Bereich der öffentlichen Sicherheit müssen wir entgegenwirken. Zuallererst ist sicherzustellen, dass die Funktion der Grundrechte als Abwehrrechte auch gewährleistet ist, wenn es Private sind, die die öffentliche Sicherheit mittelbar oder unmittelbar gewährleisten sollen. Aber dann muss eine ausführliche öffentliche Diskussion darüber geführt werden, wie weit Private in die Gewährleistung öffentlicher Sicherheit überhaupt eingebunden werden sollen und dürfen.

Die Handlungsmacht gegenüber ausländischen Datensammlern zurückgewinnen

Die dritte Konsequenz aus der NSA-Affäre besteht darin, alles zu tun, um die Handlungsmacht gegenüber ausländischen Datensammlern zurückzugewinnen. Der US-amerikanische Auslandsgeheimdienst NSA und die Mehrzahl der großen privaten US-amerikanischen Internetdienste haben eine Gemeinsamkeit: Auch wenn sie Informationen über Menschen in Deutschland sammeln und speichern und damit in unsere

Grundrechte eingreifen, halten sie die Grundrechte des Grundgesetzes und die Gesetze, die diese Grundrechte ausgestalten, nicht für sich für anwendbar. NSA und die US-Internetdienste bewegen sich hier in Europa in ihren Augen in einem anarchistischen Urzustand, in dem sie sich nach ihrer Auffassung nur an ihre eigenen Regeln halten müssen. Die Regeln lauten überspitzt gesagt: "Gib mir deinen echten Namen, gib mir die Informationen über dich und mir gehört, was du mir gibst" beziehungsweise "Ich nehme mir alles, was du äußerst, und du wirst nichts davon erfahren." Welche Informationen über sie in diesen Kanälen landen und was mit diesen Informationen geschieht, wer welche Schlussfolgerungen aus ihnen zieht, wissen die Menschen in Europa nicht. Das klingt nach Informationsimperialismus, den abwehren muss, wer nicht die Auflösung der demokratischen Grundfeste erleben will.

Es geht hier nicht darum, dass alle, die sich im Geltungsbereich des Grundgesetzes bewegen, irgendeine Verordnung zur Hundesteuer beachten, es geht um unsere Grundrechte, die wir historisch gesehen erst so kurz haben und die uns jetzt durch die Hände gleiten. Die Allgemeinheit des Gesetzes musste errungen werden gegen die Unterscheidung in feudale Rechte für einige und willkürliche, Existenz bedrohende und unentrinnbare Pflichten für die Nicht-Privilegierten. Die Allgemeinheit des Gesetzes ist deshalb notwendige Garantin der Freiheit, der Gleichheit und der Demokratie. Die Allgemeinheit des Gesetzes gilt für alle, die in unsere Grundrechte eingreifen, also auch für ausländische Geheimdienste und IT-Firmen. Wer es für unschädlich hält, dass ausländische Geheimdienste und IT-Firmen gegen unsere grundrechtsschützenden Gesetze verstoßen, unterwirft sich nicht der vermeintlich unhintergehbaren Macht der Tatsachen, sondern untergräbt die eigene Macht. Wir üben sie aus, indem wir diejenigen wählen, die die Gesetze beschließen, die von allen eingehalten werden müssen. Die Geltung dieser Gesetze für ausnahmslos alle in Frage zu stellen, ist ein Angriff auf uns alle. Wenn wir es zulassen, dass sich wichtige Akteure nicht an die Gesetze halten, ist das gefährlich für den Rechtsstaat und für unsere Grundrechte.

Das Bundesverfassungsgericht hat dazu die Maßstäbe formuliert: "Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss."

Was das Pochen auf dem Postulat der Allgemeinheit des Gesetzes gegenüber privaten US-Internetdiensten anbelangt, wäre der Rückzug öffentlicher Stellen aus der Anwendung von facebook beispielsweise ein Schritt in die richtige Richtung. Die jetzt deutlich werdende Verbindung zwischen den US-amerikanischen Geheimdiensten und facebook kann diesen Schritt noch einfacher machen. Weil die NSA in der bekannt gewordenen Weise Informationen auf facebook im großen Stil nach ihr verdächtig scheinenden Begriffen scannt, kann es kein Lehrer und keine Bürgermeisterin mehr verantworten, durch den Betrieb von

"Profilseiten" und "Fanseiten" NSA und facebook Informationen zu liefern. Einreiseverbote ihrer "Fans" und "Freunde" in die USA sind wahrscheinlich die harmlosesten Folgen, die ein solches Verhalten nach sich ziehen kann. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte sich nach ihrer Frühjahrstagung an die Konferenz der Ministerpräsidentinnen und Ministerpräsidenten gewandt und ihre Mitarbeit dabei angeboten, bei den Betreibern von facebook auf eine Rechtmäßigkeit der Anwendungen hinzuwirken. Dazu müsste facebook sein Geschäftsmodell auch für die Daten derjenigen Menschen offenlegen, die sich entschieden haben, nicht Mitglied dieses sozialen Netzwerkes zu sein. Die Konferenz der Ministerpräsidentinnen und Ministerpräsidenten hat diese Anregung aufgenommen.

Was die Grundrechtseingriffe durch inländische und ausländische Geheimdienste anbelangt, ist es Aufgabe und Pflicht der Bundesregierung als derjenigen Institution, die uns in europäischen und internationalen Zusammenhängen vertritt, unsere Grundrechte auch gegen Akteure aus den USA zu schützen. Die Bundesregierung muss darauf hinwirken, dass Grundrechtsverstöße unverzüglich abgestellt werden. Die Forderungen der Datenschutzkonferenz zeigen, dass es dafür jetzt schon wirksame Werkzeuge gibt. Diese müssen unverzüglich genutzt werden.

Angesichts von "Big Data", also der technischen Möglichkeiten, in unglaublich großen Datenmengen Muster zu erkennen und mit Hilfe von Algorithmen unser Verhalten "voraussagen" zu können, dürfen wir dabei nicht stehen bleiben. Wir müssen darüber diskutieren, wie wir die grundrechtsschützenden Regelungen noch verschärfen können. Wir müssen genau festlegen, bei wem welche Datenmengen entstehen dürfen, wer sie wofür nutzen darf und welche darauf basierenden Verhaltensprognosen wir zulassen wollen. Und dann müssen wir aufpassen, dass die Menschen nicht resignieren angesichts der Ungewissheit darüber, ob die Überwachung ihrer Kommunikation umfassend ist. Wir müssen verhindern, dass sie auf die Ausübung ihrer Grundrechte verzichten. Eine funktionierende Demokratie braucht Menschen, die ihr Grundrecht auf freie Meinungsäußerung wahrnehmen. Für die Wahrnehmung des Grundrechtes der freien Meinungsäußerung bilden das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme die Basis. Das wird an der Aussage des Bundesverfassungsgerichts im Urteil zum Verbot der Vorratsdatenspeicherung deutlich: Schon das "diffuse Gefühl des Beobachtet seins" greift in unsere Grundrechte ein. Eine permanente Videoüberwachung und die anlasslose Überwachung der digitalen Kommunikation können eine "Schere im Kopf" bewirken, können zu antizipiertem vermeintlichem Wohlverhalten führen. Demgegenüber stehen starke Datenschutzgrundrechte dafür, dass sich die Menschen darauf verlassen können, dass sie selbst steuern können, wer welche ihrer Äußerungen wann kennt.

Wir müssen mehr als in der Vergangenheit dafür tun, dass die Regeln, die die für den demokratischen Staat unverzichtbaren Grundrechte garantieren, durchgesetzt werden. Damit das Informationsimperium nicht mehr zu(rück)schlagen kann.

1.2 Neue Legislaturperiode

Da trifft es sich gut, dass in das Berichtsjahr die Wahl zum 18. Deutschen Bundestag fiel. Die Enthüllung des ungeahnten Ausmaßes der Überwachung durch private und staatliche Organisationen und die damit verbundene Erkenntnis, dass in Zeiten von Big Data auch die Gefährdungen für die Grundrechte auf informationelle Selbstbestimmung und auf Vertraulichkeit und Integrität informationstechnischer Systeme riesig geworden sind, machen deutlich, dass es in der nächsten Legislaturperiode für den Schutz der Kommunikationsgrundrechte viel zu tun gibt.

1.2.1 Forderungen der Datenschutzkonferenz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appellierte auf ihrer Herbsttagung in Bremen an alle Akteurinnen und Akteure der 18. Legislaturperiode, sich für die Stärkung des Datenschutzes auf nationaler, europäischer und internationaler Ebene einzusetzen. Angesichts der anlasslosen und umfassenden internationalen Überwachungsaktivitäten von Nachrichtendiensten forderten die Datenschutzbeauftragten von dem Bundesgesetzgeber und der neuen Bundesregierung wirksame Maßnahmen zum Schutz der Vertraulichkeit der Kommunikation und der Privatsphäre. Dazu gehören auch die oben genannten Konsequenzen aus der NSA-Debatte.

Die Datenschutzbeauftragten des Bundes und der Länder nahmen zu drei für die Datenschutzgrundrechte besonders bedeutsamen Bereichen Stellung. In ihrer Entschließung zur öffentlichen Sicherheit betonte die Datenschutzkonferenz dringenden Handlungsbedarf für diesen besonders eingriffsintensiven Bereich. Sie forderte insbesondere eine rechtsstaatlich transparente Kontrolle der Nachrichtendienste im nationalen wie im internationalen Rahmen. Darüber hinaus müssten diesen Behörden, deren Tätigkeit tief in die Grundrechte der Bürgerinnen und Bürger eingriffen, enge Grenzen gesetzt werden. Auch für Grundrechtseingriffe anderer Sicherheitsbehörden seien wirksame Beschränkungen erforderlich. Mit der Entschließung zur "Stärkung des Datenschutzes im Sozialwesen und Gesundheitswesen" forderte die Konferenz angesichts der mit dem zunehmenden Wettbewerb im Sozialwesen und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung die Stärkung der Schutzrechte für die Privatsphäre und Intimsphäre von Patientinnen, Patienten und Versicherten. In ihrer Entschließung "Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln" setzte sich die Datenschutzkonferenz für die Förderung der Vertraulichkeit und Integrität elektronischer Kommunikation ein. Sie forderte, dass der öffentliche Bereich

mit gutem Beispiel vorangeht und die Ende-zu-Ende-Verschlüsselung unter Verwendung des in Bremen entwickelten Standards OSCI-Transport (Online Services Computer Interface) flächendeckend einsetzt.

1.2.2 Auf anlasslose Vorratsdatenspeicherung verzichten

Eine weitere Forderung bleibt angesichts der Enthüllungen über die anlasslose Vorratsdatenspeicherung in den USA in der neuen Legislaturperiode auch hierzulande aktuell: Auf die anlasslose Vorratsdatenspeicherung muss verzichtet werden. Das Bundesverfassungsgericht hatte 2010 die deutsche Variante der Vorratsdatenspeicherung der Verbindungsdaten gekippt und dabei auch eine Aussage zur quantitativen Grenze für anlasslose Datensammlungen gemacht: "Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen (…) erheblich geringer". Das vom Bundesverfassungsgericht für verfassungswidrig erklärte Gesetz sollte die europäische Vorratsdatenspeicherungsrichtlinie umsetzen.

Einiges deutet darauf hin, dass der europäische Gerichtshof kurz davor steht, die europäische Richtlinie selbst für unvereinbar zu erklären mit dem Recht der Menschen in Europa auf Datenschutz. Die Informationen darüber, wer wann wie lange mit wem telefoniert und wer welche Internetseite wie lange geöffnet hat, dürften dann nicht mehr ohne Anlass monatelang gespeichert werden.

Die Skepsis gegenüber der anlasslosen Vorratsdatenspeicherung ist angebracht,

- weil ihre Eignung, ihre Erforderlichkeit und ihre Angemessenheit für die verfolgten Zwecke der Strafverfolgung und Strafprävention noch immer nicht erwiesen sind,
- weil die Anhäufung von unglaublichen Datenmassen verfassungswidrige missbräuchliche Nutzungen nicht nur durch ausländische Geheimdienste ermöglicht,
- weil auf Vorrat gesammelte Daten neue Nutzungsideen und Nutzungswünsche sogar hervorrufen können.

Im Koalitionsvertrag für die 18. Legislaturperiode heißt es zum Thema Vorratsdatenspeicherung: "Wir werden die EU-Richtlinie über den Abruf und die Nutzung von Telekommunikationsverbindungsdaten umsetzen. Dadurch vermeiden wir die Verhängung von Zwangsgeldern durch den Europäischen Gerichtshof (EuGH). Dabei soll ein Zugriff auf die gespeicherten Daten nur bei schweren Straftaten und nach Genehmigung durch einen Richter sowie zur Abwehr akuter Gefahren für Leib und Leben erfolgen. Die Speicherung der deutschen Telekommunikationsverbindungsdaten, die abgerufen und genutzt werden sollen, haben die Telekommunikationsunternehmen auf Servern in Deutschland vorzunehmen. Auf EU-Ebene werden wir auf eine Verkürzung der Speicherfrist auf drei Monate hinwirken."

Bedeutsam an dieser Formulierung ist, dass die Vermeidung von Zwangsgeldern, die der EuGH verhängen könnte, und nicht die Eignung der Speicherung der Telekommunikationsverbindungsdaten zur Verbrechensbekämpfung als Begründung für eine Vorratsdatenspeicherungsregelung herangezogen wird. Dies ermöglicht eine vorgängige ernsthafte Auseinandersetzung mit der Eignung und der Erforderlichkeit der Speicherung aller Kommunikationsverbindungsdaten zur Verbrechensbekämpfung, zu der sich auch der Europäische Gerichthof nach Presseberichten in der mündlichen Verhandlung zur Rechtmäßigkeit der EU-Vorratsdatenrichtlinie sehr kritisch geäußert hatte. Europäischer Rat, Kommission und Parlament hätten keine belastbaren Zahlen präsentieren können, inwieweit auch die verdachtsunabhängige Speicherung aller Telekommunikationsdaten bei der Aufklärung von Straftaten helfen. Auch das Votum des Generalanwaltes ist hier sehr skeptisch. Es zeichnet sich also ab, dass die Entscheidung des Europäischen Gerichtshofes die Eignung und Erforderlichkeit von anlasslosen Speicherungen der Telekommunikationsdaten zumindest ausführlich diskutieren, wenn nicht sogar ablehnen wird. Es ist höchste Zeit, die nach dem 11. September 2001 aus dem Ruder gelaufene Praxis der riesigen Datensammlungen auf das nach der europäischen Grundrechtecharta zulässige Maß zurückzufahren.

Dr. Imke Sommer

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 35. Jahresberichts

Der Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum 35. Jahresbericht der Landesbeauftragten für Datenschutz vom 8. März 2013 (Drucksache 18/805) und zur Stellungnahme des Senats vom 27. August 2013 (Drucksache 18/1037) lag zum Redaktionsschluss noch nicht vor.

3. Behördliche Beauftragte für den Datenschutz

3.1 Gesetzeskonforme Bestellung behördlicher Datenschutzbeauftragter

Im Berichtsjahr waren wir erneut mit Problemen befasst, die sich daraus ergaben, dass bremische Dienststellen ihrer Pflicht zur Bestellung einer oder eines behördlichen Datenschutzbeauftragten nicht nachgekommen waren oder die Bestellungen nicht den gesetzlichen Anforderungen entsprachen (siehe auch 35. Jahresbericht, Ziffer 3.2).

Wie unserem 35. Jahresbericht zu entnehmen ist, hatten wir die Nichtbestellung einer oder eines behördlichen Datenschutzbeauftragten bei einer großen bremischen Behörde mit zahlreichen Verfahren personenbezogener Datenverarbeitung gegenüber dem zuständigen Senator beanstandet. Der Senator hatte in seiner Stellungnahme die Nichtbestellung mit dem in der Behörde stattfindenden Reorganisationsprozess begründet. Unseren Wissens ist bei der betroffenen Behörde auch zum Redaktionsschluss noch keine behördliche Datenschutzbeauftragte beziehungsweise kein behördlicher Datenschutzbeauftragter bestellt worden.

In einem Ressort, in dem die Wahrung des Sozialgeheimnisses eine Rolle spielt, wurde erneut ein Vertrag mit einem externen Datenschutzdienstleister geschlossen, der neben datenschutzrechtlichen Dienstleistungen auch die Bestellung des Geschäftsführers zum behördlichen Datenschutzbeauftragten beinhaltet. Der Vertrag enthält deutliche datenschutzrechtliche Verbesserungen, die wir gern anerkannten. Weiterhin unberücksichtigt bleibt in dem Vertrag aber, dass Sozialdaten einem besonderen Berufsgeheimnis oder Amtsgeheimnis unterliegen und das Sozialgeheimnis zu wahren ist. Eine Befugnis zur Preisgabe von Sozialdaten gegenüber einer oder einem Dritten, die beziehungsweise der die Funktion der oder des behördlichen Datenschutzbeauftragten wahrnimmt, gibt es nicht. Wir verblieben somit bei unserer Empfehlung, eine dienststelleninterne Lösung für die Besetzung der Funktion der oder des behördlichen Datenschutzbeauftragten zu finden. Eine Reaktion der verantwortlichen Stelle hierauf steht noch aus. Die betreffende verantwortliche Stelle möchte an dem externen Datenschutzdienstleister als behördlichem Datenschutzbeauftragten festhalten.

3.2 Mangelnde Beteiligung des behördlichen Datenschutzbeauftragten

Im Berichtsjahr informierte uns der behördliche Datenschutzbeauftragte des Studentenwerks darüber, dass dort eine neue Software eingeführt werde. Weil er hierüber nicht unterrichtet worden sei, sei die nach dem Bremischen Datenschutzgesetz erforderliche Vorabkontrolle durch den behördlichen Datenschutzbeauftragten nicht erfolgt. Die Aufnahme des Echtbetriebs und die Verarbeitung von Echtdaten seien mit ihm nicht abgestimmt worden.

Nach dem Bremischen Datenschutzgesetz ist vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, von der für die Datenverarbeitung verantwortlichen Stelle zu untersuchen, ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Die zu treffenden technischen und organisatorischen Maßnahmen sind zu dokumentieren. Das Ergebnis der Untersuchung ist dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten (Vorabkontrolle). Darüber hinaus verlangt das Gesetz, den behördlichen Datenschutzbeauftragten über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten, damit dieser seine Aufgaben erfüllen kann. Auch dieser Bestimmung wurde im vorliegenden Fall nicht entsprochen.

Wir forderten das Studentenwerk zunächst zu einer Stellungnahme auf, zu deren unverzüglicher Erteilung die dem Bremischen Datenschutzgesetz unterliegenden Stellen verpflichtet sind. Die benötigte Stellungnahme erhielten wir vom Studentenwerk trotz wiederholter Fristsetzung nicht. Wegen der fehlenden Unterrichtung des behördlichen Datenschutzbeauftragten, der unterbliebenen Vorabkontrolle und der Nichtabgabe der erforderlichen Stellungnahme sprachen wir eine formelle Beanstandung aus.

3.3 Meldungen der behördlichen Datenschutzbeauftragten von Kammern

Die öffentlichen Stellen im Lande Bremen müssen nach dem Bremischen Datenschutzgesetz eine behördliche Datenschutzbeauftragte beziehungsweise einen behördlichen Datenschutzbeauftragten bestellen und sowohl die Bestellung als auch die Beendigung des Amtes unverzüglich der Landesbeauftragten für Datenschutz und Informationsfreiheit melden. Diese Pflichten gelten auch für die Kammern. Im Rahmen einer Rundschreibeaktion erinnerten wir die Kammern im Berichtsjahr daran und baten sie, ihre bisherigen Meldungen auf ihre Aktualität zu überprüfen und uns mitzuteilen, ob die von ihnen gemeldeten Personen noch zur beziehungsweise zum behördlichen Datenschutzbeauftragten bestellt sind. Für den Fall, dass dies nicht zutrifft, baten wir außerdem um Nachricht, wer gegenwärtig mit dem Amt der oder des behördlichen Datenschutzbeauftragten betraut ist.

Die Rundschreibeaktion ergab, dass bei einem Großteil der Kammern die zuletzt gemeldeten Angaben zur beziehungsweise zum behördlichen Datenschutzbeauftragten nicht mehr

aktuell waren. Die Kammern holten die Erfüllung ihrer Pflichten verspätet nach. In einigen Fällen stellte sich außerdem heraus, dass die Funktion der oder des behördlichen Datenschutzbeauftragten mittlerweile nicht mehr vergeben war. Eine Neubestellung erfolgte in diesen Fällen erst auf unser Rundschreiben hin. Um Unvereinbarkeiten mit anderen Funktionen zu vermeiden, wirkten wir bei einigen Kammern auch darauf hin, dass das Amt der oder des behördlichen Datenschutzbeauftragten nicht mit der Geschäftsführerin oder dem Geschäftsführer der jeweiligen Kammer besetzt wurde.

Wir werden unsere Rundschreibeaktionen zur Aktualisierung der Meldungen auch im kommenden Jahr fortsetzen, weisen aber darauf hin, dass die öffentlichen Stellen zur Bestellung von behördlichen Datenschutzbeauftragten bereits gesetzlich verpflichtet sind.

3.4 Workshops für behördliche Datenschutzbeauftragte

Die Workshops mit den behördlichen Datenschutzbeauftragten der bremischen Verwaltung wurden im Berichtsjahr weiter fortgesetzt. Aus aktuellem Anlass fand in Bremen eine nochmalige Veranstaltung des bereits im Herbst 2012 durchgeführten Workshops zum Thema "Kommissionsentwurf zur EU-Datenschutzverordnung" statt. Die durch diese Verordnung angestrebten Veränderungen regten auch in diesem Workshop zu umfangreichen Diskussionen an, weil auch die Datenschutzgesetzgebung im Land Bremen und somit die Funktion der behördlichen Datenschutzbeauftragten davon betroffen sind. Darüber hinaus hatten alle Teilnehmenden wieder die Möglichkeit, über ihr Tätigwerden zu berichten und bereits gesammelte Erfahrungen auszutauschen.

4. Datenschutz durch Technikgestaltung und Technikbewertung

4.1 Flächendeckende Einführung des Dokumentenmanagementsystems VISkompakt

Über die Einführung der elektronischen Akte mit dem Dokumentenmanagementsystem VISkompakt haben wir bereits mehrfach berichtet (vergleiche 32. Jahresbericht, Ziffer 4.3; 33. Jahresbericht, Ziffer 4.2; 34. Jahresbericht, Ziffer 4.4 und 35. Jahresbericht Ziffer 4.2).

Das System VISkompakt ist derzeit ausgerichtet auf Daten mit dem Schutzbedarf "normal". Sofern einzelne Dienststellen den Einsatz von VISkompakt für Daten mit hohem Schutzbedarf vorsehen sollten, fordern wir ergänzende Maßnahmen wie beispielsweise die umfangreiche Verschlüsselung. Zu diesem Thema fand im Frühjahr dieses Jahres ein Workshop statt. Im Ergebnis wurde festgestellt, dass der Test für eine Verschlüsselung von Daten auf dem Übertragungsweg möglich sei. Ob dieser Test zwischenzeitlich durchgeführt wurde und mit welchem Ergebnis, ist uns nicht bekannt. Nach unserem Kenntnisstand liegen bisher keine Lösungsvorschläge für die Verschlüsselung der Inhaltsdaten und Metadaten

vor. Insofern sehen wir die Voraussetzungen für die Verarbeitung von Daten mit hohem Schutzbedarf derzeit noch nicht gegeben.

Umfassenden Klärungsbedarf sehen wir weiterhin bei der Protokollierung administrativer Tätigkeiten. Derzeit können wir einem Verweis auf die Nutzung einer Administrationsplattform mit Aufzeichnung von Arbeitssitzungen (siehe Ziffer 4.3 dieses Berichts) nicht folgen. Auch die Vollständigkeit der Protokollierung auf Ebene der zentralen und dezentralen Fachadministration wurde nicht nachgewiesen. Weiterhin wurde nicht dargelegt, ob die Protokollierungen nach verantwortlichen Stellen getrennt werden.

Nach wie vor besteht das Problem der unzureichenden Mandantentrennung im Sinne einer Abschottung der verantwortlichen Stellen gegeneinander. Wir haben unsere Position dazu mit dem Referat 02 der Senatorin für Finanzen erörtert und auch im 35. Jahresbericht unter der Ziffer 4.2 ausgeführt. Eine Annäherung beider Auffassungen konnte bisher nicht erzielt werden. Wir haben nach wie vor Zweifel an der Realisierung und Einhaltbarkeit des Trennungsgebotes gemäß § 7 Absatz 4 Nummer 8 Bremisches Datenschutzgesetz (BremDSG), weil der Schutz vor ungeprüften, unzulässigen oder auch unbeabsichtigten Zugriffen allein durch Zugriffsberechtigungen auf Ablagen gewährleistet werden soll.

Probleme bestehen nach unserem Kenntnisstand ebenfalls bezüglich der Zugriffskontrolle bei der Erteilung und Abschluss von Geschäftsvorgängen, der damit im Zusammenhang stehenden Rechtevergabe sowie deren Protokollierung. Die verantwortliche Stelle nach § 2 Absatz 3 Nummer 1 BremDSG kann nach unserer derzeitigen Einschätzung keine vollständige Zugriffskontrolle gemäß § 7 Absatz 3 Nummer 3 BremDSG sicherstellen. Weiterhin ist die Gewährleistung der Nachvollziehbarkeit der Rechtevergabe fraglich. Insofern sehen wir erhebliche datenschutzrechtliche Probleme im Zusammenhang mit der Vergabe von Geschäftsvorgängen zwischen verschiedenen datenschutzrechtlich verantwortlichen Stellen.

Weitere Probleme sehen wir bei eventuell geplanten zentralen Registraturen und Scan-Stellen, da solche Stellen mit umfangreichen Schreibberechtigungen und Leseberechtigungen auf Daten verschiedener verantwortlicher Stellen ausgestattet sein müssen. Dies stellt eine unverhältnismäßige Anhäufung von umfangreichen Berechtigungen dar, wodurch den verantwortlichen Stellen ebenfalls keine effektive Zugriffskontrolle möglich ist.

Das Konzept zur Löschung von Vorgängen oder Dokumenten liegt uns nicht vor. Die Datenschutzkonzepte liegen nicht oder nur in veralteter Form vor.

Zum Ende des Berichtsjahres wurden wir über den Start von Teilprojekten wie etwa "Die Elektronische Handakte" informiert. Auch zu den Teilprojekten liegen uns keine prüfbaren Unterlagen vor.

Gerade im Hinblick auf die flächendeckende Einführung von VISkompakt bis 2016 an voraussichtlich 2.300 Arbeitsplätzen halten wir die Klärung der beschriebenen offenen Punkte für dringend erforderlich.

Wir werden das Projekt weiter begleiten.

4.2 Anforderungen an den Betrieb von SAP

Das System SAP wird seit 2003 in der bremischen Kernverwaltung flächendeckend eingesetzt und derzeit von etwa 1800 Benutzerinnen und Benutzer genutzt.

Bereits mehrfach (vergleiche 34. Jahresbericht, Ziffer 4.3, 33. Jahresbericht, Ziffer 4.1, 32. Jahresbericht, Ziffer 10.3) hatten wir berichtet, dass die diversen Konzepte für das System SAP einer grundsätzlichen Überarbeitung bedürfen. Ein Teil der anzupassenden Dokumentation sowie deren anschließenden Umsetzung betraf die Berechtigungen, also die Rechte und Rollen im System. Durch die Senatorin für Finanzen wurde ein entsprechendes Projekt aufgesetzt, welches Konzepte zur Reorganisation der Berechtigungen erarbeitete. Bisher sind erst einzelne Anforderungen aus diesen Konzepten realisiert worden und auch die konkrete Umsetzung der Rechte und Rollen steht noch aus. In diesem Berichtsjahr wurden wir von der Senatorin für Finanzen informiert, dass nun geplant sei, mit der Implementierung der Berechtigungen zu beginnen.

Nach unserem Kenntnisstand sollen die Erstellung der Berechtigungen sowie der Funktionstest in einer Systemumgebung ohne personenbezogene Echtdaten vorgenommen werden. Für den nachfolgenden Integrationstest der Berechtigungen auf dem Qualitätssicherungssystem müsste die Erstellung einer anonymisierten beziehungsweise pseudonymisierten Datenbasis als eigenes Arbeitspaket im Umsetzungsprojekt aufgenommen werden. Zumindest erwarten wir für diese Projektphase unter anderem die Erstellung eines speziellen Sicherheitskonzeptes, aus dem hervorgeht, wie der unberechtigte Zugriff auf personenbezogene Daten während der Integrationstests im Qualitätssicherungssystem verhindert wird.

Außerdem wurden wir über das Projekt zum Ticketmanagement der fachlichen Leitstelle für SAP informiert. Dabei geht es darum, ein bereits eingesetztes Produkt für die Bearbeitung von Fehlermeldungen sowie für das Berechtigungsmanagement zu nutzen. Die uns vorliegenden Unterlagen für dieses Projekt reichen für eine Bewertung noch nicht aus. Wir haben eine enge Einbindung der behördlichen Datenschutzbeauftragten in das Kernteam des Projektes gefordert.

Schließlich machten wir deutlich, dass wir den Beginn der angekündigten Folgeprojekte für eine kontinuierliche Anpassung der Dokumentenlage und deren Umsetzung erwarten. Gemäß § 7 Absatz 2 Bremisches Datenschutzgesetz sind die Datenschutzdokumentationen laufend auf dem neusten Stand zu halten.

4.3 Sichere Administrationsumgebung Dataport

Im Zusammenhang mit der Einführung der Betriebsinfrastruktur Basis.Bremen (siehe Ziffer 4.4 dieses Berichts) berichteten wir in der Vergangenheit mehrfach über die Einführung einer Administrationsplattform, mit der ein einheitlicher und revisionssicherer Weg zur Durchführung von Administrationstätigkeiten geschaffen werden soll. Die im letzten Berichtsjahr vorgelegten Unterlagen waren im Wesentlichen Beschreibungen der technischen Implementierung. Wir baten die Senatorin für Finanzen daher darum (vergleiche 35. Jahresbericht, Ziffer 4.1), uns ein aussagefähiges Datenschutzkonzept zur Administrationsplattform vorzulegen und machten deutlich, dass sich die Maßnahmen der Administrationsplattform sowie der dafür eingesetzten Management-Domäne am Schutzbedarf "hoch" der zu administrierenden Daten und Verfahren auszurichten haben.

In diesem Berichtsjahr wurde uns in der Stellungnahme des Senats das Konzept einer sicheren Administrationsumgebung und seiner genutzten Werkzeuge angekündigt, welche durch zahlreiche zusätzliche Maßnahmen die Anforderungen eines hohen Schutzbedarfs erfüllen soll. Die dafür zu erstellenden Dokumente liegen uns bislang nicht vor. Somit ist derzeit unter anderem keine Aussage über die Vollständigkeit und Prüfbarkeit der Protokollmaßnahmen und die Revisionsfähigkeit der Administrationsplattform möglich.

4.4 Rahmendatenschutzkonzept für BASIS.Bremen

Zur Bearbeitung der mit dem Projekt BASIS.Bremen verbundenen offenen Datenschutzfragen und Datensicherheitsfragen und zur Sicherstellung der vom Senat getroffenen Zusagen (vergleiche 35. Jahresbericht, Ziffer 4.4) startete zusammen mit dem allgemeinen Projektstart auch das Arbeitspaket Datenschutz und Datensicherheit. Bis jetzt lieferte diese Arbeitsgruppe keine Ergebnisse zu unseren Anforderungen. Die vom Senat in seiner Antwort zu unserem 33. Jahresbericht geäußerte Auffassung, dass mit dem Projekt BASIS.Bremen durch die Schaffung standardisierter Betriebsabläufe ein erheblicher Sicherheitsgewinn erzielt wird, ist weiterhin für uns nicht nachvollziehbar. Auch das uns im September vorgelegte Rahmendatenschutzkonzept deckt wesentliche Themenbereiche inhaltlich nicht ab. Wir glichen deshalb die im Konzept benannten Themen mit unseren bisherigen Anforderungen ab und nannten der Senatorin für Finanzen die Erfüllung von neun grundsätzlichen Anforderungen, die wir für absolut erforderlich zur Gewährleistung eines angemessenen Datenschutzniveaus halten:

1. Erstellung einer Strukturanalyse und Entwicklung eines Sicherheitskonzeptes zu den zentral gesteuerten Standardisierungsprozessen als Grundlage für die Dienststellen;

2. Risikoanalyse auf der Basis von IT-Grundschutz BSI-Standard 100-3 und Festlegungen organisatorischer und technischer Maßnahmen;

3. Bereitstellung einer verlässlichen Informationsbasis, um den Dienststellen zu ermöglichen, die Eignung des Auftragnehmers zu prüfen;

4. Gewährleistung der Wahrnehmung der Kontrollbefugnisse durch einzelne Dienststellen im Rahmen der Auftragskontrolle;

5. Bereitstellung eines sich aus den Strukturanalysen ergebenden Maßnahmenkatalogs für die Dienststellen, aus dem sie geeignete technische Maßnahmen entsprechend dem festgestellten Schutzniveau ihrer Daten auswählen und direkt beauftragen können;

6. Entwicklung von Fachdatenschutzkonzepten für unterschiedliche Schutzstufen und deren Bereitstellung zum Zeitpunkt des Beginns des Echtbetriebs auf Basis der Ergebnisse der Strukturanalyse;

7. Erstellung einer Sicherheitsdokumentation für die Administrationsplattform, ihrer Infrastruktur und der eingesetzten Werkzeuge sowie die Sicherstellung der Revisionssicherheit aller administrativen Tätigkeiten;

8. Verifikation der im Rahmendatenschutzkonzept enthaltenen Vorannahmen hinsichtlich der Gewährleistung des hohen Schutzbedarfs;

9. Einbeziehung der anderen mit dem BASIS-PC gekoppelten Infrastrukturdienste.

Diese Anforderungen verbanden wir mit der Forderung zur Erstellung eines entsprechenden Umsetzungsplans bis März 2014. Dieser soll insbesondere zeitliche Festlegungen und konkrete Umsetzungsschritte beinhalten. Die Senatorin für Finanzen stimmte unseren Anforderungen zu und organisierte eine Umsetzungsunterstützung für die erforderlichen Arbeitsprozesse durch das Ifib (Institut für Informationsmanagement Bremen). In einer ersten gemeinsamen Sitzung wurde die weitere Vorgehensweise festgelegt. Danach werden ein oder zwei Prototypen des BASIS-PC mit dem Schutzbedarf "hoch" hinsichtlich der Vertraulichkeit ausgewählt. Die Strukturanalyse wird zunächst die Bereiche erfassen, die von dem Funktionsumfang des BASIS-PC berührt werden. Es soll dabei der ganze Weg durch die Systemumgebung bis zum Rechenzentrum Dataport und die entsprechenden dortigen technischen Abläufe, insbesondere die administrativen Eingriffsmöglichkeiten, erfasst werden. Die Senatorin für Finanzen sagte zu, hierfür den von uns geforderten Umsetzungsplan bis März zu erstellen.

Ziel ist es, ein Soll-Modell nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu errichten mit der Betrachtung der hierfür notwendigen Elemente der Infrastruktur. Das Modell soll in die Breite gehen. Checklisten und generische Konzepte sowie standardisierte Maßnahmen (security as a service) sollen für alle Dienststellen bereitgestellt werden. Weiterhin sollen Vorgehensweisen entwickelt werden, die den einzelnen Dienststellen ermöglichen, innerhalb einer weitgehend zentral gesteuerten Sicherheitsinfrastruktur ihre datenschutzrechtliche Verantwortung angemessen

wahrzunehmen. Es wird die Etablierung eines Sicherheitsprozesses, eingebunden in das ISMS (Informationssicherheitsmanagement), angestrebt, durch die das Datenschutzniveau und Sicherheitsniveau eng verzahnt mit der technischen Entwicklung und den damit verbundenen Veränderungsprozessen aufrechterhalten und verbessert werden kann. Zunächst soll ein verbindlicher Weg zur Umsetzung unserer Anforderungen festgelegt werden. Erst nach Umsetzung der Anforderungen steht eine solide Basis bereit, auf der der notwendige und laufende Sicherheitsprozess aufsetzen kann.

4.5 Einführung eines neuen Personalmanagementverfahrens

Die IT-Verfahren zum Personalmanagement in Bremen sind veraltet und müssen zur Sicherstellung eines zeitgemäßen Systembetriebs, der die Anforderungen eines modernen Managementsystems in Verbindung mit effektiven Datenschutzmaßnahmen gewährleisten kann, abgelöst werden. Wir begleiteten im Berichtsjahr zunächst das Vorprojekt des integrierten Personalmanagementverfahrens. Ziel war es, vor dem Projektstart in den entsprechenden Teilprojekten die Möglichkeiten der Software zur Umsetzung datenschutzrechtlicher Anforderungen zu prüfen. Wir konnten feststellen, dass grundsätzlich eine datenschutzgerechte Implementierung des Systems möglich ist. Im Sommer des Berichtsjahres beschloss der Senat die Einführung des Verfahrens.

In einem ersten Schritt müssen die Daten aus den alten bremischen Verfahren in das neue Verfahren "KoPers" migriert werden. Zunächst teilte uns die Senatorin für Finanzen mit, dass im Rahmen einer Analysephase bereits sämtliche Personaldaten in das neue System überführt werden sollten. Zur Erfüllung der datenschutzrechtlichen Anforderungen, insbesondere hinsichtlich der Gewährleistung von Vertraulichkeit und Datensparsamkeit, lehnten wir die vollständige Migration der Klardaten in dieser Phase ab und forderten die Definition einzelner Prozessschritte und die begründete Benennung der zur Durchführung der einzelnen Schritte jeweils erforderlichen Daten.

Hierzu war zunächst zu prüfen, ob Funktionstests zur Klärung der Frage der grundsätzlichen Verwendbarkeit des Programms beziehungsweise funktionaler Änderungen ausreichend sind. Nur für die Fragestellungen, zu deren Klärung Funktionstests nicht ausreichen, kann der Test in einer quasi produktiven Umgebung erfolgen. Jedoch sind diese Tests dann nach Möglichkeit mit nicht personenbezogenen Daten durchzuführen. Hierfür ist die Methode der Pseudonymisierung identifizierender personenbezogener Daten zu prüfen. Da diese Nutzung jedoch nicht der Anforderung auf Verzicht der Verarbeitung personenbezogener Daten bei nicht vorhandener Erforderlichkeit entspricht, weil die Daten personenbeziehbar bleiben, muss ein auf die Testumgebung und die Testbedingungen abgestimmtes Sicherheitskonzept entwickelt werden. Die Pseudonymisierung stellt eine deutliche Abschwächung des Risikos dar, insbesondere, wenn die Pseudonyme aus den bremischen Verfahren heraus gebildet und entweder gelöscht oder in Bremen datenschutzgerecht verwaltet werden und ist deshalb

akzeptabel, sofern die entsprechenden Rahmenbedingungen bestehen. Dazu gehört, dass eine Auflösung der Pseudonyme nur dann zur Klärung von Abweichungen zulässig ist, wenn diese ohne Kenntnis von Echtdaten nicht möglich ist. Erst nach Klärung aller zu beachtenden Abweichungen kann der Pilotbetrieb mit Klardaten zur Bewertung der Praxistauglichkeit des Systems und der aufgrund des Sicherheitskonzeptes vorgenommenen technischen und organisatorischen Maßnahmen erfolgen.

Zusätzlich baten wir die Senatorin für Finanzen, uns eine Risikoanalyse, das Migrationskonzept mit der Definition der einzelnen Prozessphasen in Verbindung mit der Beschreibung der für die jeweilige Durchführung erforderlichen Daten und entsprechende Sicherheitskonzepte vor dem Projektstart zukommen zu lassen.

Die Senatorin für Finanzen teilte unsere datenschutzrechtlichen Anforderungen und vertrat diese gegenüber der die Migration durchführenden Firma. Sie erarbeitete eine Zeitplanung und Maßnahmenplanung, in der unsere Anforderungen vollständig berücksichtigt werden. Die Datenmigration erfolgt demnach in einem drei-gestuften Verfahren mit Test-, pseudonymisierten- und Klardaten. Der nächste Teilschritt wird die Konzeptentwicklung für die Pseudonymisierung sein. Wir gehen im Moment davon aus, dass der Projektstart datenschutzgerecht erfolgen kann .

4.6 Länderübergreifendes Active Directory

Im Sommer des Berichtsjahres erfuhren wir durch die Datenschutzbeauftragten der anderen Dataport-Vollträgerländer, dass seit dem Jahr 2012 eine länderübergreifende Arbeitsgruppe mit dem Titel "AD Kopplung" existiert. Diese Arbeitsgruppe, die aus Vertretern der Länder Bremen, Hamburg und Schleswig-Holstein sowie von Dataport besteht, soll sich nach unseren Informationen damit befassen, welche technischen und organisatorischen Maßnahmen zu treffen wären, um die Active Directories (AD) der Länder miteinander zu koppeln und so Synergieeffekte daraus für alle Beteiligten nutzbar zu machen.

Wie sich herausstellte, war die Arbeitsgruppe bis dahin zu den datenschutzrechtlichen und datenschutztechnischen Fragestellungen zur Koppelung von Active Directories im Wesentlichen von Vertreterinnen und Vertretern des Unabhängigen Datenschutzzentrums Schleswig-Holstein beraten worden.

Das Ergebnis der Beratungen sollte eine gemeinsame Stellungnahme der Datenschutzbeauftragten der Dataport-Vollträgerländer zum Aufbau und Betrieb eines gemeinsamen Active Directory sein. Diese gemeinsame Stellungnahme konnte nicht zustande kommen, weil wir, wie unsere Kolleginnen und Kollegen aus Hamburg, nicht ausreichend über den aktuellen Stand der Überlegungen informiert waren. Bis Redaktionsschluss lagen uns keine belastbaren Unterlagen zur geplanten Gesamtstruktur eines länderübergreifenden Active Directory vor.

Wir wiesen darauf hin, dass in Bremen eine Rechtsgrundlage fehlt, die den Betrieb länderübergreifender Verfahren wie eines Active Directory ermöglichen würde.

4.7 Arbeitskreis Technik

Zentrale Themen des Arbeitskreises Technik (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder waren im Berichtsjahr unter anderem die Datenschutzrisiken bei kontaktlosen Transaktionen mit Geldkarten und Kreditkarten und die Zusammenarbeit des Arbeitskreises Technik mit der Koordinierungsstelle für IT-Standards (KoSIT).

Die KoSIT hat die Aufgabe, die Entwicklung und den Betrieb von IT-Standards für den Datenaustausch in der öffentlichen Verwaltung zu koordinieren. Im Rahmen der Frühjahrssitzung des AK Technik, die bei der KoSIT in Bremen stattfand, beschäftigte sich der Arbeitskreis unter anderem damit, die Möglichkeiten der Zusammenarbeit mit der KoSIT auszuloten. Dem AK Technik ist die Zusammenarbeit mit KoSIT wichtig, weil sie datenschutzfreundliche Standards geschaffen hat und dies auch weiterhin tun wird. Dabei ist die Unterstützung der Datenschutzbeauftragten von großem Nutzen. Die Diskussion zeigte eine ganze Reihe von Punkten auf, bei denen die Zusammenarbeit zwischen KoSIT und dem AK Technik und auch eine Mitarbeit des AK Technik in den Gremien des IT-Planungsrates aufgebaut oder fortgeführt werden soll. Dies sind insbesondere die Mitarbeit im KoSIT-Beirat, in der Arbeitsgruppe Informationssicherheitsleitlinie des IT-Planungsrates, in der Arbeitsgruppe XTA (zur Entwicklung und Fortschreibung eines Konzeptes für einen standardisierten Transportadapter für die öffentliche Verwaltung) und in der Arbeitsgruppe XMeld (zur Entwicklung und Fortschreibung eines bundeseinheitlichen elektronischen Datenaustauschformates für die Übermittlung von Daten des Meldewesens). Weiterhin wird der AK Technik auch die Arbeit der bei der KoSIT noch zu gründenden Fachgruppe Netzwerksicherheit unterstützen. Trotz der geringen personellen Ressourcen bei den Datenschutzbeauftragten sollten diese Gremien besetzt werden.

Zum Thema der kontaktlosen Transaktionen mit Geldkarten und Kreditkarten gab es im Berichtsjahr eine umfangreiche Zusammenarbeit mit der Arbeitgruppe Kreditwirtschaft (AG Kreditwirtschaft) des Düsseldorfer Kreises. Beide Gremien tagten gemeinsam und luden dazu auch Vertreter der Deutschen Kreditwirtschaft und der beiden großen Kreditkartenunternehmen ein, um den datenschutzrechtlichen Rahmen des Verfahrens abzustimmen. Der AK Technik drängte besonders darauf, dass für diese Verfahren durch die Anbieter vollständige Datenschutzfolgeabschätzungen (englisch Privacy Impact Assessments, kurz PIA) erarbeitet werden. Dabei werden anhand eines durch die Europäische Kommission entwickelten Konzeptes ("Framework") die Datenschutzbedrohungen und Auswirkungen untersucht. Die Anlehnung an das Konzept der Europäischen Union ermöglicht eine Standardisierung bei der Erarbeitung von

Datenschutzfolgeabschätzungen. Die Möglichkeit zur Durchführung kontaktloser Transaktionen mit Geldkarten und Kreditkarten auf der Basis der Nahfeldkommunikationstechnologie (englisch Near Field Communication, kurz NFC) birgt einige datenschutzrechtliche Risiken, die im Rahmen der Datenschutzfolgeabschätzungen identifiziert und bewerten werden. Sowohl die Deutsche Kreditwirtschaft als auch die Kreditkartenunternehmen erstellten und verfeinerten in Zusammenarbeit mit dem AK Technik die PIAs. Die Zusammenarbeit wird fortgeführt.

5. Inneres

5.1 Telekommunikationsüberwachung durch die Polizeien

Für die Polizei Bremen wird wie berichtet (vergleiche 35. Jahresbericht, Ziffer 5.11) die Telekommunikationsüberwachung (TKÜ) in verschiedenen Kooperationsstufen mit dem Landeskriminalamt (LKA) Niedersachsen durchgeführt. Bereits im vergangenen Berichtsjahr wurde das Projekt "Datenschutzkonzept für die Telekommunikationsüberwachung in verschiedenen Kooperationsstufen mit dem LKA Niedersachsen" bei der Polizei Bremen gestartet.

Schon im letzten Berichtsjahr hatten wir umfassend Stellung zu den übermittelten Unterlagen genommen und einen entsprechenden Anforderungskatalog vorgelegt. Zwischenzeitlich erhielten wir erneut Unterlagen, deren Entwicklungsstand weiterhin noch nicht unseren Anforderungen genügen. Dies begründeten wir umfassend und formulierten erneut unsere Erwartungen.

Zum Verwaltungsabkommen nahmen wir mehrfach Stellung. Trotzdem fand ein Teil unserer Hinweise keinen Eingang in das Verwaltungsabkommen, den Auftrag zur Datenverarbeitung und seiner Anlagen. Nach den Vorschriften des Bremischen Datenschutzgesetzes hat sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen. Wir stellten fest, dass die dafür erforderlichen Unterlagen dem Auftraggeber derzeit noch nicht vollständig vorliegen.

5.2 Einführung eines Terminmanagements

Das beim Senator für Inneres und Sport angesiedelte Projekt zur Einführung eines Terminmanagements in der bremischen Verwaltung wurde im Berichtsjahr fortgesetzt. In der Zwischenzeit wurde ein Anbieter ausgewählt. Wir gehen davon aus, dass er in der Lage ist, die datenschutzrechtlichen Anforderungen umzusetzen. Ein Datenschutzkonzept für das Verfahren wurde uns allerdings noch nicht vorgelegt.

5.3 Speicherung personenbezogener Daten bei der Polizei

Im Berichtsjahr erreichten uns Beschwerden darüber, dass Daten, die im Rahmen polizeilicher Tätigkeiten erhoben wurden, teilweise Jahre nach der Erhebung noch immer in den Auskunftssystemen der Polizeien gespeichert waren. Überwiegend konnten wir darauf hinwirken, dass die Erforderlichkeit durch die Polizeien erneut geprüft wurde und einzelne Eintragungen gelöscht wurden.

Gegenüber dem Senator für Inneres und Sport sowie der Polizei Bremen und der Ortspolizeibehörde Bremerhaven machten wir unsere Bedenken hinsichtlich der aktuellen Datenverarbeitung deutlich und wiesen darauf hin, dass die Speicherung nur zulässig ist, soweit dies zur Erfüllung der Aufgaben erforderlich ist. Personenbezogene Daten dürfen nur für den bestimmten Zweck verarbeitet werden, für den sie im Einzelfall erhoben wurden. Die Zweckbestimmung ist bei jeder Speicherung festzulegen. Weiter dürfen personenbezogene Daten, die im Rahmen der Verfolgung von Straftaten über eine tatverdächtige Person und in Zusammenhang damit über Dritte rechtmäßig erhoben oder rechtmäßig erlangt wurden, gespeichert, verändert und genutzt werden, wenn wegen der Art, Ausführung oder Schwere der Tat sowie der Persönlichkeit der tatverdächtigen Person anzunehmen ist, dass sie weitere Straftaten begehen wird und die Speicherung erforderlich ist, um diese Straftaten zu verhüten. Dies ist im Einzelfall zu prüfen.

Darüber hinaus machten wir gegenüber dem Senator für Inneres und Sport deutlich, dass die Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) als Verwaltungsvorschrift nach dem Bremischen Polizeigesetzes ausschließlich die Speicherung zu präventiven Zwecken zur Gefahrenabwehr und zur Verhütung von Straftaten regeln können.

Wir erwarten, dass insbesondere bei der Gestaltung der neuen Verfahren, die bei der Polizei Bremen und bei der Ortspolizeibehörde Bremerhaven eingeführt werden sollen (siehe Ziffer 5.5 (@rtus) und 5.4 (INPOL-Land) dieses Berichts), die Umsetzung der rechtlichen Vorgaben durch technische und organisatorische Maßnahmen vor der Einführung der Verfahren sichergestellt ist.

5.4 Erweiterung der Anwendung INPOL und INPOL-Land

Die Polizei Bremen hat in diesem Jahr einen Entwurf für die Verfahrensbeschreibung für die Anwendung INPOL-Land erstellt; den Prozess haben wir beratend begleitet.

INPOL ist ein bundesländerübergreifendes Informationssystem der Polizeien. Das System ist als Verbunddatei konzipiert, das heißt, dass neben dem zentralen Bereich beim Bundeskriminalamt (BKA) die bei der jeweiligen Landespolizei betriebenen Systeme INPOL-Land bestehen. Das System INPOL-Land ist bereits bei der Polizei Bremen im Einsatz, soll künftig aber verstärkt genutzt werden, die bisherige Anwendung ersetzen und damit neben

dem Vorgangsbearbeitungssystem @rtus (siehe Ziffer 5.5 dieses Berichts) das Auskunftssystem der Polizeien werden. Nur bei einem Bundesbezug werden einzelne Datensätze in das Zentralsystem INPOL beim BKA übertragen.

Der erste Entwurf der Verfahrensbeschreibung war unvollständig. Aufgrund der vorgelegten Dokumentenlage ist nicht erkennbar, ob die dem hohen Schutzbedarf dieser Daten angemessenen technischen und organisatorischen Maßnahmen getroffen worden sind. Zusätzlich haben wir bemängelt, dass diese Dokumente nicht - wie rechtlich vorgeschrieben - vor der Entscheidung über die Einführung erstellt wurden, sondern auch gegenwärtig trotz laufenden Betriebes noch nicht vollständig vorliegen. Keine Einigung gibt es derzeit über unsere Anforderung, den Abfragegrund in INPOL als Pflichtfeld vorzusehen. Hierzu erwarten wir eine Stellungnahme der Polizei Bremen. Seit unserem letzten Termin im Sommer sind keine ergänzenden Unterlagen bei uns eingegangen.

Daher fordern wir, dass die Erstellung der erforderlichen Dokumentation vollständig und unverzüglich erfolgt, dass unsere Anforderungen an technische und organisatorische Maßnahmen und die Gestaltung des Verfahrens ebenso zeitnah umgesetzt werden und wir weiterhin in den Prozess eingebunden werden.

5.5 Einführung des Vorgangsbearbeitungssystems @rtus

Wie wir bereits im letzten Jahresbericht berichteten (siehe 35. Jahresbericht, Ziffer 5.10), ist zum Januar 2014 die Einführung des Vorgangsbearbeitungssystems @rtus VBS (VorgangsBearbeitungsSystem) bei der Polizei Bremen und der Ortspolizeibehörde Bremerhaven geplant. Auch im Berichtsjahr haben wir den Planungsprozess intensiv begleitet, um eine datenschutzkonforme Gestaltung des Systems sicherzustellen.

Im Frühjahr wurde uns die Anwendung @rtus VBS auf Basis der in Schleswig-Holstein zum Einsatz kommenden Variante der Anwendung vorgeführt und einzelne Module, deren Einsatz in Bremen geplant ist, wurden uns erläutert. Insbesondere die Recherchemöglichkeiten mit dem Zusatzmodul @rtus Recherche sind von Bedeutung. Die geplante Teststellung der für Bremen angepassten Version verzögerte sich stark, sodass wir bisher keine Möglichkeit hatten, diese näher zu prüfen.

Ein erster Entwurf der Verfahrensbeschreibung für @rtus VBS wurde uns übersandt, zu dem wir jedoch nur eingeschränkt Stellung nehmen konnten, da uns wesentliche Informationen und ergänzende Konzepte nicht vorlagen. Zum Modul @rtus Recherche liegen uns keinerlei Unterlagen vor. Damit konnte auch die Vorabkontrolle des Verfahrens durch die behördlichen Datenschutzbeauftragten vor der Einführung des Verfahrens nicht auf den erforderlichen Grundlagen durchgeführt sowie der datenschutzkonforme Betrieb nicht gewährleistet werden.

5.6 Aktuelle Situation im Stadtamt

Auch in diesem Berichtsjahr konnte bezüglich der aktuellen Situation im Stadtamt Bremen im Vergleich zu den Vorjahren (vergleiche 34. Jahresbericht, Ziffer 5.11 und 35. Jahresbericht, Ziffer 5.5) kein Fortschritt erzielt werden. Nach wie vor ist im Stadtamt keine behördliche Datenschutzbeauftragte beziehungsweise kein behördlicher Datenschutzbeauftragter bestellt sowie eine große Anzahl von Verfahren ohne ausreichende Datenschutzkonzepte und mit nicht bewertbaren technischen und organisatorischen Maßnahmen im Echtbetrieb. Auch die vormals quartalsweise stattfindenden Gespräche mit dem Stadtamt Bremen konnten nicht wieder aufgenommen werden.

Weiterhin ungeklärt ist die Frage, ob den zuständigen und verantwortlichen Fachbereichen im Stadtamt ausreichende Kapazitäten zur Verfügung gestellt werden, um die erforderlichen und längst ausstehenden Verfahrensbeschreibungen durch die jeweils verantwortlichen Stellen erstellen zu können.

5.7 Neufassung des Bremischen Verfassungsschutzgesetzes

Der Gesetzentwurf soll nach dessen Begründung aus datenschutzrechtlicher Sicht im Wesentlichen die Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2009 zur Online-Durchsuchung umsetzen. In dieser Entscheidung wurden Vorgaben zur gesetzlichen Regelung der Voraussetzungen einer Eingriffsmaßnahme in informationstechnische Systeme sowie zum Schutz des Kernbereichs privater Lebensgestaltung entwickelt. Die Entscheidung hatte sich erstmalig auf das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme bezogen. Des Weiteren soll mit dem Entwurf die Zusammenarbeit der Verfassungsschutzbehörden des Bundes und der Länder sowie des Landesamtes für Verfassungsschutz mit den Staatsanwaltschaften und den Polizeidienststellen verbessert werden. Die Reformbedürftigkeit hatte sich bei der Aufarbeitung der Mordserie der Terrororganisation "Nationalsozialistischer Untergrund (NSU)" gezeigt.

Der Entwurf unterstützt grundsätzlich datenschutzrechtliche Kernforderungen, wonach der Grundrechtsschutz, das Trennungsgebot und eine effiziente rechtsstaatliche parlamentarische Kontrolle zu gewährleisten sind. Die in die Persönlichkeitsrechte potenziell Betroffener eingreifenden Befugnisse des Verfassungsschutzes sollen nunmehr gesetzlich geregelt werden. Dazu gehören der Einsatz von Personen zur Informationsbeschaffung, sogenannter Informanten beziehungsweise Vertrauenspersonen, der Einsatz technischer Mittel zur Ermittlung des Standortes aktiv geschalteter Mobilfunkendgeräte sowie weitere Auskunftsverlangen gegenüber Telekommunikationsdiensten.

Allerdings äußerten wir Bedenken, dass das verfassungsrechtliche Trennungsgebot der Verfassungsschutzbehörden gegenüber der Polizei hinreichend berücksichtigt wird. Die

Eingliederung des bisherigen Landesamtes für Verfassungsschutz als Abteilung in die senatorische Behörde Inneres und Sport neben der Abteilung Öffentliche Sicherheit, die die Aufsicht über die Polizeidienststellen hat, erscheint diesem Gebot ohne entsprechende gesetzliche Klarstellungen nicht hinreichend zu entsprechen. Beide sind nämlich Bestandteile einer Behörde. Wir schlugen daher vor, im Gesetz festzulegen, dass die betreffenden Behörden personenbezogene Daten nur in eigenständigen Dateien auf separaten Datenträgern verarbeiten dürfen.

Des Weiteren äußerten wir Bedenken, weil die Erhebungsbefugnis sich auch pauschal auf alle besonderen Arten von Daten erstreckt. Dies genügt nicht dem Grundsatz der Beschränkungen bezüglich des Kernbereichs privater Lebensgestaltung. Angaben über die Gesundheit und das Sexualleben sind nach der Entscheidung des Bundesverfassungsgesetzes zur Online-Durchsuchung und seiner dort zitierten ständigen Rechtsprechung dazu diesem Kernbereich eindeutig zuzuordnen. Auf die Erhebung dieser Daten muss auch der Verfassungsschutz daher verzichten.

Angesichts der Enthüllungen über die anlasslosen und umfassenden Überwachungen durch ausländische Nachrichtendienste und der Frage, inwieweit inländische Geheimdienste hiervon Kenntnis hatten beziehungsweise an diesen Überwachungen beteiligt waren, muss die Diskussion über die Rolle und die Befugnisse inländischer Nachrichtendienste weiter geführt werden. Dies haben wir in der Diskussion des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zum im Berichtsjahr vorgelegten Gesetzesentwurf deutlich gemacht.

5.8 Rahmendatenschutzkonzept der Polizei Bremen

Die Datenschutzkonzepte der Fachverfahren der Polizei Bremen verweisen bezüglich zentraler Anforderungen an die Kontrollziele gemäß § 7 Bremisches Datenschutzgesetz auf das Rahmendatenschutzkonzept der Polizei Bremen. Bisher haben wir zu unserer Stellungnahme zu diesem Dokument und zu den noch offenen Fragen keine Antworten erhalten. In der Stellungnahme des Senats zu unserem 35. Jahresbericht heißt es dazu, dass uns das Rahmendatenschutzkonzept im dritten oder vierten Quartal in Gänze vorgelegt werden soll. Dies ist nicht geschehen. Auf Rückfrage bei der Polizei Bremen wurden wir bezüglich der Antworten auf unsere Fragen an dieses für die datenschutzrechtliche und datenschutztechnische Gesamtbewertung relevante Konzept wiederum auf das kommende Jahr verwiesen. Nach unserem Kenntnisstand ist keine Fortschreibung dieses zentralen Konzeptes erfolgt.

Sowohl in diesem Bereich, bei der Erstellung zentraler Dokumentationen für den Datenschutz wie auch bei der Einführung des Systems @rtus (siehe Ziffer 5.5 dieses Berichts) und bei der Erweiterung der Nutzung von Funktionen des Systems INPOL (siehe Ziffer 5.4 dieses Berichts) wird deutlich, dass der Polizei Bremen personelle Ressourcen zur

Erstellung der Datenschutzdokumentation und der Bearbeitung unserer diesbezüglichen Fragen fehlen.

5.9 Rahmendatenschutzkonzept des Senators für Inneres und Sport

Der Senator für Inneres und Sport kündigte in diesem Berichtsjahr an, die Arbeiten am Rahmendatenschutzkonzept voraussichtlich im Herbst dieses Jahres fortzusetzen. Wir erwarten nunmehr die Erstellung einer Prioritätenliste mit Terminnennungen; bisher sind uns keine Informationen zugegangen. Unsere mehrfachen Anfragen zur Verarbeitung sensibler Daten im Rahmen der Migration zu BASIS.Bremen wurden nicht beantwortet.

5.10 Arbeitskreis Sicherheit

Der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) beschäftigte sich im Berichtsjahr unter anderem mit den aktuellen technischen Möglichkeiten der "intelligenten" Videoüberwachung und der Zulässigkeit von Drohnen zur Videobeobachtung durch öffentliche Stellen. Des Weiteren waren die Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei, die Initiativ-Datenübermittlung der Polizei an Fußballvereine sowie die Gestaltung der polizeilichen Informationssysteme Thema. Zudem konnten für den Sicherheitsbereich Anliegen identifiziert werden, in denen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder dringenden Handlungsbedarf für die neue Bundesregierung sieht. Diese sind in die Entschließung Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit der DSK (siehe Ziffer 22.8 dieses Berichts) eingeflossen.

6. Justiz

6.1 Projekt "Forderungsmanagement in der Justiz"

Über das Projekt "Forderungsmanagement in der Justiz" berichteten wir bereits im letzten Jahresbericht. Wir begleiteten das Projekt weiter. Zu dem Datenschutzkonzept nahmen wir Stellung. Da sich im Rahmen der bisherigen Projekterfahrung gezeigt hatte, dass der telefonische Kontakt mit den Schuldnerinnen und Schuldnern in vielen Fällen gute Wirkung zeigt, deren Telefonnummern häufig aber nicht bekannt sind, wurde an uns die Frage gerichtet, ob es zulässig sei, mithilfe eines externen Anbieters die Rufnummern aus öffentlich zugänglichen Quellen zu beschaffen. Grundsätzlich bestehen von unserer Seite dagegen keine Bedenken. Nach Durchsicht der entsprechenden Unterlagen ergab sich allerdings die Vermutung, dass personenbezogene Daten der Betroffenen während der Bearbeitung von Abgleichsaufträgen und der Dauer der Regresshaftung zwischengespeichert würden, was wir für unzulässig halten. Zudem war in den Unterlagen auch von nicht öffentlich zugänglichen Telefondaten die Rede. Sofern an der Beauftragung des Anbieters

festgehalten werden soll, müsste das Verfahren entsprechend angepasst werden. Des Weiteren wurden wir um Stellungnahme zu der Frage gebeten, ob zur Einschätzung der Bonität der Schuldnerinnen und Schuldner Auskunfteien herangezogen werden dürften. Wir wiesen den Senator für Justiz und Verfassung darauf hin, dass zunächst geprüft werden müsste, inwieweit für diesen Zweck Daten aus öffentlichen Registern erhoben werden könnten. Zweifel äußerten wir zudem an der Eignung einer solchen Maßnahme, da Auskunfteien häufig Fehler aufweisen.

6.2 Videoüberwachung in der Justizvollzugsanstalt

Bereits im 35. Jahresbericht berichteten wir über unsere Bedenken im Rahmen der Errichtung einer Videoüberwachungsanlage in der Justizvollzugsanstalt Bremen. In der Zwischenzeit wurden die Kameras in Betrieb genommen. Nach unserer Rechtsauffassung existiert noch nicht für alle überwachten Bereiche eine Rechtsgrundlage. Für problematisch halten wir beispielsweise die Überwachung von Teilen der Nachbargrundstücke, auch wenn uns vonseiten der Justizvollzugsanstalt zugesichert wurde, dass beinahe alle Nachbarinnen und Nachbarn damit einverstanden seien. Vermeintliche Einwilligungen der Nachbarinnen und der Nachbarn sind nicht geeignet, die Videoüberwachung zu rechtfertigen. Einen Dissens gibt es zudem über die Frage, ob die Überwachung der Strafgefangenen auf eine Vorschrift des Bremischen Untersuchungshaftvollzugsgesetzes gestützt werden kann, die vorsieht, dass eine Beobachtung auch dann erfolgen darf, wenn Dritte unvermeidbar mit betroffen sind. Im Gegensatz zur Justizvollzugsanstalt vertreten wir die Auffassung, dass die Strafgefangenen in diesem Fall nicht lediglich mitbetroffene Dritte sind, sondern gezielt überwacht werden, sodass das Untersuchungshaftvollzugsgesetz nicht als Rechtsgrundlage herangezogen werden kann. Dafür spricht auch der hohe Anteil der betroffenen Strafhäftlinge im Verhältnis zu der Anzahl der Untersuchungshäftlinge. Wir halten es für unverhältnismäßig, eine derart große Anzahl von mitbetroffenen Dritten in Kauf zu nehmen, um einen relativ geringen Anteil von Untersuchungshäftlingen zu beobachten. Als weiterer wichtiger Aspekt sind die Mitarbeiterinnen und Mitarbeiter der Justizvollzugsanstalt zu nennen. Sie dürfen keinem dauerhaften Überwachungsdruck ausgesetzt sein. Wir werden die Videoüberwachungsanlage vor Ort besichtigen und darauf hinwirken, dass das noch ausstehende Datenschutzkonzept fertiggestellt wird.

6.3 Datenübermittlung durch Rechtsanwältin an Steuerberatungsgesellschaften

Eine Bürgerin wandte sich an uns, da die Rechtsanwältin ihres geschiedenen Ehemannes zwei Steuerberatungsgesellschaften angeschrieben hatte, um für die Abwicklung des Verfahrens benötigte Steuerunterlagen der Petentin zu erhalten. Bei einer der

Steuerberatungsgesellschaften war die Petentin schon seit längerer Zeit keine Mandantin mehr. Sie wollte wissen, ob sie in ihren Datenschutzrechten verletzt worden sei.

Wir baten die Rechtsanwältin um Stellungnahme. Uns stellte sich die Frage, woher sie Kenntnis hatte, dass die Petentin bei den Steuerberatungsgesellschaften Mandantin gewesen war beziehungsweise noch ist. Auf Nachfrage wurde uns mitgeteilt, dass die Kenntnis aus vorangegangenem Schriftverkehr mit der Petentin stamme. Wir wiesen die Rechtsanwältin darauf hin, dass nach den Vorschriften des Bundesdatenschutzgesetzes personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind. Ausnahmen von diesem Grundsatz sind nur dann zulässig, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder die zu erfüllende Aufgabe eine Erhebung bei anderen Personen oder Stellen erforderlich macht. Eine weitere Ausnahme liegt vor, wenn die Erhebung der Daten beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Es dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schützwürdige Interessen der Betroffenen beeinträchtigt werden. Das Vorliegen dieser Gründe war im konkreten Fall nicht ersichtlich, sodass die benötigten Steuerunterlagen direkt von der Petentin und nicht von den Steuerberatungsgesellschaften hätten angefordert werden müssen. Die Rechtsanwältin bestätigte uns, zukünftig die Vorgaben der entsprechenden datenschutzrechtlichen Vorschrift zu beachten.

7. Gesundheit und Soziales

7.1 Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten

Im Juni des Berichtsjahres wurde uns vom Senator für Gesundheit der Entwurf eines Gesetzes zur Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (BremPsychKG) sowie der Entwurf einer Begründung zu diesem Gesetz mit der Bitte um Kenntnisnahme beziehungsweise Stellungnahme übersandt.

Der uns zugesandte Entwurf beinhaltet unter anderem eine Änderung der Regelung über die Kontrolle von Paketsendungen. Bisher ist das Einsehen und Öffnen von Paketen zulässig, "wenn tatsächliche Anhaltspunkte dafür vorliegen, dass eine Weiterleitung der Patientin oder dem Patienten erhebliche Nachteile zufügen oder die Sicherheit der Einrichtung gefährden könnte, insbesondere wenn die Gefahr des Einschmuggelns von Suchtstoffen oder gefährlichen Gegenständen oder der Verabredung von Straftaten besteht" (§ 27, Absatz 2 BremPsychKG).

Nach dem Änderungsentwurf ist nunmehr geplant, die entsprechende Norm in der Weise zu ändern, "dass Pakete jederzeit durch von der ärztlichen Leitung hierfür beauftragte Mitarbeiterinnen oder Mitarbeiter eingesehen werden dürften" (Normtext des Entwurfes). In

der Begründung zum Gesetzentwurf wird hierzu angeführt, den Gefahren, die durch das Verbringen von gefährlichen und unerwünschten Gegenständen in die Unterbringungseinrichtungen und Maßregelvollzugseinrichtungen entstehen, könne nur durch eine lückenlose Überwachung des Paketverkehrs begegnet werden.

Wir teilten dem Senator für Gesundheit mit, dass wir aufgrund der Tatsache, dass die verdachtsunabhängige Kontrolle des gesamten Paketverkehrs einen erheblichen Eingriff in die Persönlichkeitsrechte der Betroffenen darstellt, die geplante Regelung für unverhältnismäßig halten. Durch das Zur-Kenntnis-Nehmen von Fotos, Bildern, Zeitschriften oder Büchern können weitgehende Rückschlüsse auf die Persönlichkeit oder das persönliche Umfeld der oder des Betroffenen gezogen werden. Denkbar sind etwa Rückschlüsse auf die politische oder sexuelle Orientierung oder das familiäre oder soziale Umfeld der Betroffenen. Nicht bezweifelt wird dabei unsererseits, dass Kontrollen im Einzelfall geboten sind, um die Sicherheit der Kliniken nicht zu gefährden. Pauschal, unabhängig von der jeweiligen Diagnose und/oder Therapie der Betroffenen von einer generellen Gefahr auszugehen, die ohne vorherige Einzelfallprüfung Eingriffe in die Persönlichkeitsrechte der Betroffenen rechtfertigt, ist nach den uns vorliegenden Informationen nicht gerechtfertigt. Auch ein Vergleich mit den Regelungen anderer Bundesländer über die Paketkontrolle im Rahmen der öffentlich-rechtlichen Unterbringung sowie der Unterbringung im Maßregelvollzug zeigt, dass die Kontrolle nach einer Einzellfallprüfung der Regelfall ist und zudem – soweit ersichtlich – nicht als problematisch angesehen wird.

Schließlich regten wir an, in den Gesetzesentwurf aufzunehmen, dass eine Kontrolle nur in Anwesenheit der oder des Betroffenen stattfinden darf.

7.2 Kopieren beziehungsweise Scannen von Kontoauszügen durch das Sozialamt Bremerhaven

Im August des Berichtsjahres informierte uns ein Bürger darüber, dass er vom Sozialamt Bremerhaven im Zusammenhang mit dem Beziehen einer Grundsicherung wegen Erwerbsminderung schriftlich aufgefordert worden sei, "vollständige Kontoauszüge" der letzten drei Monate vorzulegen. Bei der Vorlage der Kontoauszüge habe eine Mitarbeiterin des Sozialamtes Bremerhaven diese zudem einscannen und archivieren wollen.

Auf Nachfrage teilte das Sozialamt Bremerhaven uns mit, auf die Möglichkeit der Schwärzung einzelner Angaben innerhalb der Ausgabebuchungen würde vonseiten der Mitarbeiterinnen und Mitarbeiter regelmäßig bei der persönlichen Vorsprache der Antragsstellerinnen und Antragssteller hingewiesen. Es sei zudem gängige Praxis, Kontoauszüge einzuscannen und zu archivieren. Dies sei nach Ansicht des Sozialamtes auch zulässig.

Wir teilten dem Sozialamt Bremerhaven daraufhin mit, dass schon bei der Aufforderung zur Vorlage von Kontoauszügen auf die Möglichkeit der Schwärzung einzelner Passagen hingewiesen werden muss. Hinsichtlich der Praxis, Kontoauszüge einzuscannen und digital zu speichern, erklärten wir, dass wir diese für unzulässig halten.

Die Zulässigkeit der Speicherung von Kontoauszügen würde voraussetzen, dass die Speicherung zur Erfüllung einer Aufgabe des Sozialamtes Bremerhaven nach dem Sozialgesetzbuch erforderlich wäre. Für eine Bedarfsfeststellung bei Betroffenen ist die Speicherung der Kontoauszüge hingegen nicht erforderlich. Nach der Einsicht in die Auszüge dürfte regelmäßig ein Vermerk in der Akte ausreichen, nach dem die Auszüge vorgelegen und keine Auswirkung auf den Leistungsanspruch haben. Eine Speicherung einzelner Buchungen oder Auszüge kommt nur dann in Betracht, wenn sich aus den Unterlagen ein weiterer Ermittlungsbedarf oder eine Änderung in der Leistungshöhe ergibt.

Im November des Berichtsjahres übersandte uns das Sozialamt Bremerhaven dann ein an die Mitarbeiterinnen und Mitarbeiter gerichtetes Rundschreiben, in dem diese darauf hingewiesen wurden, dass das Einscannen von Kontoauszügen im Regelfall unzulässig und nur in Einzelfällen nach Schwärzung aller nicht erforderlichen Daten zulässig ist. Die Mitarbeiterinnen und Mitarbeiter wurden zudem darauf hingewiesen, dass die Betroffenen bereits mit Anforderung der Kontoauszüge auf die Möglichkeit der Schwärzung einzelner Passagen hinzuweisen sind.

7.3 Mitgliederwerbung einer Krankenkasse

Im Juni des Berichtsjahres erlangten wir Kenntnis darüber, dass eine Krankenkasse in diesem Jahr erneut im Rahmen der Aktion "Mit dem Rad zur Arbeit" personenbezogene Daten erhebt und diese zur Werbung von Mitgliedern nutzt. Bereits in den Jahren 2005 und 2006 waren wir mit der Sache befasst. Damals hatte die Krankenkasse zugesagt, zukünftig weniger umfangreich Daten zu erheben und zudem bestimmte Angaben innerhalb der Anmeldebroschüre als freiwillig zu kennzeichnen.

In diesem Jahr umfassten die Anmeldeformulare entgegen der damaligen Zusage nicht mehr nur die freiwillige Angabe des Geburtsjahres, es wurde vielmehr das Geburtsdatum als Pflichtangabe gefordert. Zudem war die Mobilfunknummer nunmehr im Rahmen der Online-Anmeldung genauso verpflichtend anzugeben wie die E-Mail-Adresse. Darüber hinaus enthielt zwar der Datenschutzhinweis die Information, dass eine Weitergabe der Daten an Dritte ausgeschlossen sei. Innerhalb der Teilnahmebedingungen versteckte sich hingegen die "Erklärung", dass die teilnehmende Person sich für den Fall eines Gewinnes damit einverstanden erkläre, dass ihr Name in Web-, Print- und/oder sonstigen Publikationen der Krankenkasse veröffentlicht werde.

Wir wiesen die Krankenkasse darauf hin, dass wir die Erhebung des Geburtsdatums im Rahmen der Aktion für unzulässig halten und in Bezug auf die Erhebung der Mobilfunknummer sowie der E-Mail-Adresse Zweifel hinsichtlich der Erforderlichkeit haben. Die seitens der Krankenkasse vorgebrachte Argumentation, das Geburtsdatum sei erforderlich, um feststellen zu können, ob die teilnehmende Person das zur Teilnahme erforderliche Alter erreicht habe, überzeugte uns nicht. Sofern die Erhebung des Geburtsdatums allein dem Zweck dient, das Alter festzustellen, so ist sie nicht erforderlich, da dieser Zweck auch schlicht durch die direkte Erfragung des Alters erreicht werden kann. Auch die Begründung für die Erforderlichkeit der Erhebung von E-Mail-Adresse und Mobilfunknummer überzeugte nicht. Nach Auffassung der Krankenkasse sind diese Daten erforderlich, um im Rahmen der Online-Anmeldung sicherzustellen, dass kein Dritter im Namen der eingeschriebenen Person teilnimmt. Wir teilten der Krankenkasse mit, dass die Erhebung einer Mobilfunknummer sowie einer E-Mail-Adresse kein geeignetes Mittel zur Identifikation einer Person ist. So ist es problemlos möglich, einen falschen Namen aber die eigene E-Mail-Adresse und Mobilfunknummer anzugeben. Hinsichtlich der widersprüchlichen Angaben in der Datenschutzerklärung und in den Teilnahmebedingungen teilten wir der Krankenkasse mit, dass die "Erklärung" innerhalb der Teilnahmebedingungen keine wirksame Einwilligung in die Veröffentlichung der Namen der Gewinnerinnen und Gewinner darstellt und diese daher ohne noch zu erklärende ausdrückliche Einwilligung der Gewinnerinnen und Gewinner unzulässig ist. Auf unsere Bitte, uns umgehend zuzusichern, dass eine Veröffentlichung der Gewinnernamen ohne vorherige Einwilligung der Gewinnerin oder des Gewinners nicht stattfinden werde, erhielten wir die schriftliche Zusage, dass eine Veröffentlichung nur nach vorheriger Einwilligung der jeweiligen Person erfolgen würde.

Im Folgenden mussten wir feststellen, dass sich auf der Homepage der Krankenkasse die Ankündigung befand, nach Ziehung der Gewinnernamen würden diese in der lokalen Presse sowie auf der Homepage der Krankenkasse veröffentlicht. Wir forderten die Krankenkasse daraufhin abermals zur Stellungnahme sowie zur Übersendung eines Exemplars der von den Gewinnerinnen und Gewinnern der Aktion zu unterschreibenden Einwilligungserklärung auf. Im Folgenden erklärte die Krankenkasse erneut, eine Veröffentlichung der Gewinnernamen würde erst nach Einwilligung der betroffenen Person erfolgen. An ihrer Auffassung, nach der die Erhebung des Geburtsdatums, der Mobilfunknummer sowie der E-Mail-Adresse erforderlich und somit zulässig ist, hielt die Krankenkasse fest. Sie sagte aber zu, bei der Aktion im nächsten Jahr zu prüfen, ob die Erhebung des Alters der teilnehmenden Person ausreichend ist. Die uns übersandte Einwilligungserklärung entspricht nicht den gesetzlichen Vorschriften. Die datenschutzrechtliche Abstimmung hinsichtlich der genauen Formulierung dauert an.

7.4 Datenübermittlung an Dritte durch das Klinikum Bremen-Mitte

Im Frühjahr wurde in der Presse darüber berichtet, dass Patientendaten vom Klinikum Bremen-Mitte an einen falschen Adressaten versandt worden seien. Es soll sich dabei um Patientenrechnungen des Krankenhauses gehandelt haben, in denen Daten über Eingriffe und Untersuchungen, also besonders sensible Gesundheitsdaten, aufgeschlüsselt waren. Ursache der falschen Versendung war offenbar eine Verwechslung aufgrund eines ähnlichen Namens. Wir baten das Klinikum um Stellungnahme und um Auskunft darüber, welche Maßnahmen ergriffen worden sind, um zukünftig einen korrekten Versand sicherzustellen.

Das Klinikum bestätigte den Vorfall, der darauf beruhte, dass dem Patienten im Computersystem ein falscher Debitor zugeordnet worden war. Ein solcher Fehler kann entweder durch eine manuelle falsche Auswahl zustande kommen oder durch nicht korrekt eingestellte Suchkriterien im Computerprogramm. Uns wurde mitgeteilt, dass die Suchkriterien in der Zwischenzeit so angepasst worden seien, dass Name, Vorname und komplette Adresse exakt mit den Daten der Patientinnen und Patienten übereinstimmen müssten. Zudem werde nur noch ein passender Eintrag angezeigt, sodass manuelle Fehleingaben in dem Prozess nicht mehr möglich seien. Wir gehen davon aus, dass durch die getroffenen Maßnahmen ein Falschversand zukünftig nicht mehr vorkommt.

7.5 Verkauf von Rezeptdaten durch ein Apothekenrechenzentrum an Unternehmen der Marktforschung

Bereits im letzten Jahresbericht (vergleiche 35. Jahresbericht, Ziffer 7.7) berichteten wir über den Verkauf von Rezeptdaten durch ein unserer datenschutzrechtlichen Aufsicht unterliegenden Apothekenrechenzentrum an Unternehmen der Marktforschung. Zum damaligen Zeitpunkt übermittelte das Apothekenrechenzentrum nicht anonymisierte, sondern lediglich pseudonymisierte Verordnungsdaten an die Marktforschungsunternehmen. Anfang des Jahres legte uns das Apothekenrechenzentrum dann eine Dokumentation vor, die in ihrer Umsetzung eine vollständige Anonymisierung der Datenlieferung garantiert.

Da uns das Rechenzentrum im April des Berichtsjahres eine neue Anfrage eines Unternehmens der Marktforschung mit der Bitte um datenschutzrechtliche Prüfung vorlegte, waren wir auch in diesem Berichtszeitraum detailliert mit den Inhalten der Datenlieferung von Abrechnungsdaten befasst.

Der Prüfung, ob eine vollständige Anonymisierung der Rezeptdaten stattgefunden hat, haben wir dabei die folgenden Grundsätze zugrunde gelegt. Um die Anonymität der Verordnungsdaten sicherzustellen, muss jede Veränderung des Verordnungsdatensatzes durch ein Apothekenrechenzentrum, die nicht sozialgesetzlichen Zwecken dient, zu einem Ergebnis führen, das sich nicht mit der versicherten Person, der verordnenden Ärztin

beziehungsweise dem verordnenden Arzt oder der Apothekerin beziehungsweise dem Apotheker verknüpfen lässt. Bei der Bewertung, ob für die Wiederherstellung des Personenbezugs der Daten ein unverhältnismäßiger Aufwand an Zeit, Kosten und Arbeitskraft nötig ist, sind das Interesse und die Möglichkeit des Marktforschungsinstituts sowie weiterer Stellen, die auf die Daten zugreifen könnten, zu berücksichtigen. Die erfolgversprechendste Methode zur Wiederherstellung des Personenbezugs der Daten ist dabei in dem Einsatz von Zusatzwissen sowie der Ausnutzung innerer Zusammenhänge zwischen verschiedenen Verordnungen zu sehen. Das Apothekenrechenzentrum trifft die Pflicht, nicht lediglich das bei den Marktforschungsunternehmen, sondern auch das bei Dritten bestehende oder mit verhältnismäßigem Aufwand erlangbare Zusatzwissen mit angemessener Sorgfalt einzuschätzen. Im Zweifel ist von der Verfügbarkeit des Zusatzwissens auszugehen. Aufgrund der Vielzahl von Sekundärdaten, der Schwierigkeit, vorhandenes Zusatzwissen einzuschätzen und schließlich des erheblichen Mehrwerts arztbezogener gegenüber nicht arztbezogener Daten, ist ein besonders strenger Maßstab bei der Beurteilung der Risiken, Personenbezüge herstellen zu können, anzulegen. Die Möglichkeit der Herstellung solcher Bezüge wurde im Berichtszeitraum auch durch die öffentliche Berichterstattung (vergleiche Der Spiegel, Heft 34/2013) untermauert.

Das unter unserer Aufsicht stehende Apothekenrechenzentrum übernahm die im Bereich uns bekannter Forschungsvorhaben ohnehin als Standard anerkannte Methode der Anonymisierung durch komplette Löschung der identifizierenden Daten. Nur so ist sicher eine Zuordnung zu einzelnen Patientinnen und Patienten oder Ärztinnen und Ärzten auszuschließen.

7.6 Fachverfahren Kindergarten online

Ende des Jahres 2012 wurden wir aus einem Elternverein, der Träger einer Kinderbetreuungseinrichtung ist, darüber informiert, dass geplant sei, in der betreffenden Kinderbetreuungseinrichtung das Fachverfahren Kindergarten online [Ki·ON] einzuführen. Bei [Ki·ON] handelt es sich um ein Fachverfahren, mit dem der Verwaltungsaufwand und Organisationsaufwand von Kindertageseinrichtungen reduziert werden soll und das (nach unserem Kenntnisstand) mittlerweile in fast allen Kindertageseinrichtungen im Land Bremen eingeführt wurde. Im Rahmen einer Informationsveranstaltung der Senatorin für Soziales, Kinder, Jugend und Frauen im Zusammenhang mit der Einführung des Verfahrens hatten Vertreterinnen und Vertreter des Elternvereins erfahren, dass in dem genannten Verfahren teilweise sehr sensible Daten erfragt werden und uns gegenüber Bedenken hinsichtlich der Zulässigkeit der Datenerhebung geäußert. Eine Prüfung der uns auf Anfrage von der Senatorin für Soziales, Kinder, Jugend und Frauen übersandten Unterlagen des Verfahrens ergab erhebliche datenschutzrechtliche Verstöße. So werden sensible personenbezogene Daten erhoben, die für die Aufgabenerfüllung der Betreuungseinrichtungen nicht erforderlich

sind und zudem teilweise keinem nachvollziehbaren Zweck dienen. Erfragt werden beispielsweise Krankenversicherung, Versicherungsnehmer und Hausarzt des Kindes; Geburtsort, Geburtsdatum und Staatsangehörigkeit der sorgeberechtigten Person sowie Berufstätigkeit, berufliche Belastung, Staatsangehörigkeit, Herkunftsland, Geburtsort und Geburtsdatum der abholberechtigten Person.

Wir teilten der Senatorin für Soziales, Kinder, Jugend und Frauen mit, dass die Erhebung solcher Daten, die für die Aufgabenerfüllung der Betreuungseinrichtungen nicht erforderlich sind, grundsätzlich unzulässig ist. Sofern allerdings ein nachvollziehbarer Zweck für die Datenerhebung besteht, kann sich deren Zulässigkeit aus der Einwilligung der betroffenen beziehungsweise sorgeberechtigten Person ergeben. Ausdrücklich betonten wir zudem, dass die Erhebung der Staatsangehörigkeit der sorgeberechtigten Person unter keinen denkbaren Gesichtspunkten erforderlich ist, insbesondere auch nicht nach der Migrationshintergrund-Erhebungsverordnung, da die Staatsangehörigkeit der sorgeberechtigten Person kein Kriterium zur Bestimmung des Migrationshintergrundes des Kindes ist. Die senatorische Behörde schloss sich unserer Auffassung in diesen Punkten an und kündigte eine Abstimmung der Problematik im Anwenderbeirat an.

Darüber hinaus halten wir nach der derzeitigen Ausgestaltung des Verfahrens, bei der der überwiegende Teil des Datenbestandes beim Auftragnehmer gespeichert wird, eine Auftragsdatenverarbeitung für unzulässig. Die Voraussetzung der entsprechenden Norm des Zehnten Sozialgesetzbuches liegt nicht vor. Entgegen der Meinung der senatorischen Behörde sind die Normen des Sozialdatenschutzes auf vorliegenden Fall unseres Erachtens auch unbeschränkt anwendbar. Auf die Träger der öffentlichen Jugendhilfe finden die Normen des Sozialdatenschutzes direkt Anwendung. Darüber hinaus erstreckt sich der Sozialdatenschutz auch auf die Träger der freien Jugendhilfe, soweit diese zur Erfüllung öffentlicher Aufgaben in Anspruch genommen werden. Da es sich bei der Jugendhilfe um eine öffentliche Aufgabe handelt, finden die Normen des Sozialdatenschutzes demnach auf die Träger der freien Jugendhilfe entsprechende Anwendung, soweit diese auf dem Gebiet der Jugendhilfe tätig werden. Dementsprechend richtet sich die Zulässigkeit der Auftragsdatenverarbeitung nach den sozialrechtlichen Vorschriften.

Hiernach ist die Einschaltung von privaten Auftragsdatenverarbeitern, wie sie hier erfolgt ist, nur dann zulässig, wenn entweder ohne die Beauftragung der Auftragnehmerin oder des Auftragnehmers bei der Auftraggeberin beziehungsweise beim Auftraggeber Störungen im Betriebsablauf auftreten können oder die Arbeiten durch die Beauftragung erheblich kostengünstiger besorgt werden können und der überwiegende Teil der gespeicherten Daten bei der Auftraggeberin beziehungsweise beim Auftraggeber verbleibt. Störungen im Betriebsablauf der Betreuungseinrichtungen ohne die Auftragsdatenverarbeitung sind unseres Wissens nicht zu befürchten. Wir gehen davon aus, dass die Auftragsdatenverarbeitung allein zum Zwecke der Kostenersparnis stattfindet. Dies setzt

nach dem Gesetz voraus, dass der überwiegende Teil des gesamten Datenbestandes beim Auftraggeber gespeichert wird. Da dies im Verfahren [Ki·ON] nicht der Fall ist, halten wir die Auftragsdatenverarbeitung in der derzeitigen Form für unzulässig. Etwas Anderes ergibt sich entgegen der Meinung der senatorischen Behörde auch nicht daraus, dass KiTa Bremen monatliche Backups (Sicherungskopien) der Daten erhält. "Doppelte Daten" in die Berechnung der Datenmenge mit einzubeziehen, wäre allenfalls nachvollziehbar, wenn die entsprechende Regelung den Verlust der Daten verhindern sollte. Die in Rede stehenden strengeren Anforderungen an die Auftragsdatenverarbeitung durch nicht öffentliche Stellen dürften hingegen dem Zweck dienen, die Daten vor unberechtigten Zugriffen zu schützen. Durch die doppelte Speicherung der Daten wird dieser Zweck hingegen gerade nicht erreicht.

Entgegen der Meinung der senatorischen Behörde gehen wir zudem davon aus, dass dem zuständigen Träger der öffentlichen Jugendhilfe – Amt für Soziale Dienste – eine Garantenpflicht hinsichtlich der Einhaltung eines Datenschutzes bei den Trägern der freien Jugendhilfe auf einem Niveau, das dem des Sozialgesetzbuches entspricht, zukommt. Schließlich entspricht auch das technische Sicherheitsniveau nicht dem hohen Schutzbedarf der Daten. Aus den uns von der senatorischen Behörde übergebenen Unterlagen geht hervor, dass im Rahmen des Authentifizierungsverfahrens ein Hash-Algorithmus verwendet wird, der seit 2006 nicht mehr als sicher gilt. Es gibt keinen Nachweis über ein gesichertes Authentifizierungsverfahren, ebenso nicht über den Schutz der Webanwendung, die Absicherung der Schnittstellen und der Verfahren beim Rechenzentrum des Auftragnehmers (Mandantentrennung, Administration, Support, Revision, Zugriff auf Inhaltsdaten durch ein Tool, Abschottung gegenüber Clouddiensten, Revision). Die uns momentan zur Verfügung stehenden Informationen lassen vermuten, dass das technische Datenschutzniveau des Auftragnehmers nicht ausreichend geprüft worden ist.

7.7 Pharmakologische Forschungsdatenbanken

Die Landesbeauftragte für Datenschutz und Informationsfreiheit kritisiert, dass derzeit ohne Rechtsgrundlage pharmakologische Forschungsdatenbanken mit Versichertendaten betrieben werden. Privatrechtlich organisierte Forschungsinstitute unterhalten zu Forschungszwecken Datenbanken mit hochsensiblen, lediglich pseudonymisierten Versichertendaten, die zu Forschungszwecken von Krankenkassen übermittelt werden.

Eine gesetzliche Grundlage für die Übermittlung dieser Daten durch die Krankenkassen besteht nicht. Zwar sieht § 75 Absatz 1 Sozialgesetzbuch (SGB) X die Möglichkeit der Datenübermittlung durch Krankenkassen zu Forschungszwecken vor. Diese Regelung umfasst hingegen nur die Datenübermittlung für ein bestimmtes Forschungsvorhaben nicht hingegen eine solche für die Verarbeitung und Nutzung der Daten in einer

pharmakologischen Forschungsdatenbank, in der die Daten zu immer neuen und zudem bei der Übermittlung der Daten noch nicht absehbaren Zwecken verarbeitet und genutzt werden.

Als Lösungsansatz für eine Legalisierung der Datenübermittlungen an Forschungsdatenbanken ist die Anpassung des § 75 SGB X denkbar. Gegen eine Erweiterung des § 75 SGB X spricht unseres Erachtens, dass es sich bei den übermittelten Daten um hochsensible Versichertendaten handelt. Um einen Ausgleich zwischen den Belangen des Datenschutzes einerseits und der Forschungsfreiheit andererseits zu ermöglichen, regt die Landesbeauftragte für Datenschutz und Informationsfreiheit an, dass die Forschungsinstitute stattdessen den – gegebenenfalls gesetzlich zu erweiternden – Datenpool nach §§ 303 a fortfolgende SGB V nutzen. Dieser Datenpool enthält Versorgungsdaten der gesetzlichen Krankenversicherungen, die jährlich durch das Bundesversicherungsamt übermittelt werden. Vor dem Hintergrund, dass zum Zwecke der Forschung die Möglichkeit der Nutzung der Daten aus dem erforderlichenfalls gesetzlich zu erweiternden Datenpool nach §§ 303 a fortfolgende SGB V besteht, hält die Landesbeauftragte für Datenschutz und Informationsfreiheit eine Änderung des § 75 SGB X nicht für sinnvoll.

7.8 Datenerhebung durch einen Medizinproduktehersteller im Auftrag einer Krankenkasse

Im September 2012 meldete sich ein Bürger bei uns und schilderte nachfolgenden Sachverhalt. Ihm werde durch seine Krankenkasse ein Beatmungsgerät eines Medizinprodukteherstellers zur Verfügung gestellt. Die Kosten der Zurverfügungstellung übernehme seine Krankenkasse. Zuständig für die Wartung des Gerätes hingegen sei der Medizinproduktehersteller. Zum wiederholten Male habe der Medizinproduktehersteller ihm, anscheinend im Auftrag der Krankenkasse, Fragebögen mit Fragen zur Benutzung des Gerätes zugesandt. Erfragt werde beispielsweise, wie oft das Gerät benutzt werde, ob es Gründe für eine unregelmäßige Benutzung gebe sowie die Zählerstände des Beatmungsgerätes.

Auf Nachfrage teilte die Krankenkasse uns mit, dass der Fragebogen in der Form, in der er versandt wurde, nicht zwischen dem Medizinproduktehersteller und der Krankenkasse abgestimmt worden sei. Abgestimmt worden seien lediglich Fragen, die die Notwendigkeit des Hilfsmittels betreffen, etwa Angaben zum Zählerstand und zum Umfang der täglichen Therapiestunden. Diese Fragen würden auch berechtigterweise gestellt, da eine Folgegenehmigung des Hilfsmittels nur dann möglich sei, wenn der Nachweis darüber geführt werde, dass das Hilfsmittel im Einzelfall erforderlich sei, um den Erfolg der Krankenbehandlung zu sichern, einer drohenden Behinderung vorzubeugen oder eine Behinderung auszugleichen (§ 33 Absatz 1 Satz 1 Sozialgesetzbuch V). Dies wiederum

setze voraus, dass das Gerät innerhalb eines Jahres mindestens 1.400 Betriebsstunden genutzt würde.

Wir teilten der Krankenkasse mit, dass die Übertragung der Aufgabe der Datenerhebung für die Prüfung der Erforderlichkeit des Hilfsmittels eine Einwilligung der betroffenen Person oder ein Auftragsdatenverarbeitungsverhältnis voraussetzt. Darüber hinaus teilten wir der Krankenkasse mit, dass wir in dem vorliegenden Fall erhebliche Zweifel an der Zulässigkeit der Auftragsdatenverarbeitung hätten.

Die Krankenkasse vertrat in einem weiteren Schreiben die Auffassung, die Datenerhebung des Medizinprodukteherstellers sei schon deshalb zulässig, da dieser zur Wartung, Reparatur und Instandhaltung der Geräte ohnehin die Zählerstände ablesen dürfe.

Wir erläuterten daraufhin erneut, dass die Prüfung der Frage, ob Versicherte Anspruch auf die Versorgung mit bestimmten Hilfsmitteln haben, eine Aufgabe der jeweiligen Krankenkasse ist. Die Prüfung der Leistungspflicht kann nicht im Wege eines Vertrages über die Versorgung mit Hilfsmitteln auf den Medizinprodukthersteller übertragen werden. Da zwischen dem Medizinprodukthersteller und der Krankenkasse offenbar zudem kein Auftragsdatenverarbeitungsvertrag geschlossen wurde, setzt die Zulässigkeit der Datenerhebung durch den Medizinprodukthersteller eine Einwilligung der Versicherten voraus.

Die Argumentation der Krankenkasse, nach der der Medizinprodukthersteller Angaben zu den Zählerständen erheben darf, soweit dies zur Wartung der Geräte erforderlich ist, ist zwar zutreffend. Eine Übermittlung dieser Daten an die Krankenkasse hingegen ist für die Wartung der Geräte nicht erforderlich und somit unzulässig.

Die Krankenkasse teilte daraufhin mit, zukünftig würde eine Einwilligung der Versicherten eingeholt. Würde eine solche nicht erteilt, werde man die Daten, die zur Prüfung der Frage, ob die versicherte Person Anspruch auf die Versorgung mit bestimmten Hilfsmitteln habe, erforderlich sind, direkt bei der versicherten Person erheben.

Im Oktober des Berichtsjahres teilte uns der Bürger erneut mit, dass der Medizinprodukthersteller abermals Daten für die Prüfung der Frage, ob die versicherte Person Anspruch auf die Versorgung mit bestimmten Hilfsmitteln habe, erhebe.

Auf eine weitere Nachfrage bei der Krankenkasse teilte diese mit, sie habe feststellen müssen, dass der Medizinprodukthersteller tatsächlich nicht wie abgesprochen das überarbeitete Formular verwende. Nunmehr sei aber vereinbart worden, ab sofort nur noch das überarbeitete Formular zu verwenden.

7.9 Erhebung des Geburtsortes anlässlich einer Röntgenaufnahme beim Zahnarzt

Im Oktober 2012 berichtete uns eine Patientin, dass sie anlässlich einer Röntgenaufnahme beim Zahnarzt nach ihrem Geburtsort gefragt worden war. Auf Nachfrage habe man ihr mitgeteilt, dieses Datum müsse neuerdings zu Abrechnungszwecken erhoben werden.

Auf unsere Bitte, uns die Rechtsgrundlage für die Datenerhebung mitzuteilen, berief sich die Zahnarztpraxis auf die Röntgenverordnung sowie die Richtlinie zu Aufzeichnungspflichten nach den §§ 18, 27, 28 und 36 der Röntgenverordnung und Bekanntmachung zum Röntgenpass des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit. Seit dem letzten Update der Zahnarztsoftware könne ohne die Eingabe des Geburtsortes keine Abrechung mehr erfolgen. Die Erhebung des Geburtsortes sei für die Abrechung erforderlich, da aufgrund der oben genannten Regelungen in der Kopfzeile des elektronischen Röntgenbildes neben dem Namen des Patienten auch dessen Geburtsort und Geschlecht notiert sein müsse.

Wir wiesen die Zahnarztpraxis daraufhin, dass der in Rede stehende Paragraf der Röntgenverordnung keine Rechtsgrundlage für die Erhebung des Geburtsortes darstellt, sondern lediglich eine Regelung für die Aufbewahrung von personenbezogenen Patientendaten enthält. Die offenbar vielfach fehlinterpretierte Norm bezweckt die eindeutige Zuordnung unter anderem der Röntgenbilder zu der untersuchten Person.

Auch der von der Zahnarztpraxis angeführte Abschnitt der oben genannten Richtlinie des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit stellt keine Rechtsgrundlage für die Erhebung des Geburtsortes anlässlich einer zahnärztlichen Röntgenaufnahme dar. Voraussetzung hierfür wäre nach dem Bundesdatenschutzgesetz, dass es sich bei der Richtlinie um ein Gesetz oder eine andere Rechtsvorschrift handelt. Dies ist bei der Richtlinie mangels Außenwirkung hingegen nicht der Fall.

Schließlich ist die Erhebung des Geburtsortes auch nach den Vorschriften des Bundesdatenschutzgesetzes nicht ohne Einwilligung der betroffenen Person möglich. Voraussetzung hierfür wäre, dass die Erhebung des Datums für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist (§ 28 Absatz 1 Bundesdatenschutzgesetz). Dies ist regelmäßig nicht der Fall. In einer Zahnarztpraxis wird zum Zwecke der eindeutigen Zuordnung von Röntgenbildern zur Person der Patientin beziehungsweise des Patienten – zumal regelmäßig die Adresse der Patientin oder des Patienten erhoben und gespeichert wird – grundsätzlich die Erhebung von Name, Vorname, Geburtsdatum und Geschlecht ausreichen. Eine darüber Hinausgehende Erhebung von Daten ist nicht erforderlich.

Die Erhebung des Geburtsortes anlässlich einer zahnärztlichen Untersuchung kann demnach, da es an einer Rechtsgrundlage fehlt, nur nach vorheriger Einwilligung der betroffenen Person auf freiwilliger Basis erfolgen.

Die Zahnarztpraxis teilte uns im Juni des Berichtsjahres mit, dass die Erhebung des Geburtsortes anlässlich einer Röntgenaufnahme zukünftig nicht mehr stattfindet.

7.10 Antragsformular einer Pflegekasse auf Wohngruppenzuschlag

Anfang des Berichtsjahres wurden wir durch Rundschreiben aus anderen Bundesländern darauf aufmerksam gemacht, dass mit den in den jeweiligen Bundesländern verwendeten Antragsformularen zur Prüfung des Anspruchs auf zusätzliche Leistungen für Pflegebedürftige in ambulanten Wohngruppen teilweise Daten erhoben werden, die für die Antragsbearbeitung nicht erforderlich sind.

Die Nachfrage bei einer unserer Zuständigkeit unterliegenden Pflegekasse ergab, dass auch von dieser in erheblichem Umfang für die Antragsbearbeitung nicht erforderliche Daten erhoben wurden. Beispielsweise wurde die genaue Anzahl der in der Wohngemeinschaft wohnenden pflegebedürftigen Personen erfragt. Für die Antragsbearbeitung hingegen ist einzig die Kenntnis der Tatsache, dass mindestens drei pflegebedürftige Personen in der Wohngruppe wohnen, erforderlich. Zudem wurden Postleitzahl, Wohnort, Straße, Hausnummer und Unterschrift der Pflegekraft erfragt. Auch diese Angaben sind für die Prüfung des Anspruches auf Wohngruppenzuschlag nicht erforderlich. Sofern die Pflegekasse für die Antragsbearbeitung die Unterschrift der Pflegekraft verlangt, zwingt dies die Antragsstellerinnen und Antragssteller überdies, die im Übrigen im Antrag erfassten Daten auch der Pflegekraft preiszugeben. Problematisch an der Erhebung der Unterschrift der Pflegekraft ist zudem, dass eine Mitwirkungspflicht Dritter gesetzlich nicht vorgesehen ist. Neben weiteren für die Antragsbearbeitung nicht erforderlichen Daten, wie etwa den Telefonnummern aller pflegenden Personen oder dem Datum der Übernahme der hauswirtschaftlichen Versorgung wurde zudem unter Hinweis auf die Freiwilligkeit der Angabe eine Kopie des aktuellen Mietvertrages verlangt. In den dem Antrag beiliegenden "Informationen zum Wohngruppenzuschlag in ambulant betreuten Wohngruppen" befand sich dann aber der Hinweis, der Mietvertrag sei dem Antrag auszugsweise beizufügen.

Wir wiesen die Pflegekasse darauf hin, dass die Vorlage des Mietvertrages für die Antragsbearbeitung nicht erforderlich und daher ebenso wie die Erhebung der übrigen für die Anspruchsprüfung nicht erforderlichen Daten unzulässig ist.

Am Ende des Berichtsjahres sendete uns die Pflegekasse eine komplette Überarbeitung des Antragsformulars zu. Auch in dieser werden Daten erhoben, die nicht für die Antragsbearbeitung erforderlich sind. Die datenschutzrechtliche Abstimmung dauert insoweit noch an.

8. Bildung, Wissenschaft und Kultur

8.1 Handreichung für den Einsatz sozialer Netzwerke in der Schule

Im schulischen Bereich werden soziale Netzwerke immer stärker eingesetzt. So haben sich Eltern bei uns beschwert, dass eine Lehrkraft ihre Schülerinnen und Schüler aufforderte, weitere Lernunterlagen auf ihrem Profil bei facebook abzurufen. Aufgrund eines Streits zwischen einer Schülerin und einem Schüler hatte ein Betreuer den Schüler aufgefordert, ihm gegenüber sein Profil bei facebook zu öffnen, um feststellen zu können, ob er tatsächlich die Schülerin über facebook beleidigt hatte. Wir konnten diesem Fall bei der verantwortlichen Schule nicht nachgehen, weil die Eltern aus Angst vor Nachteilen für ihre Kinder die Schule beziehungsweise den Namen der Lehrkraft und des Betreuers nicht nennen wollten. Diese Fälle zeigen, dass der Einsatz sozialer Netzwerke für alle Beteiligten ein großes Problem darstellen kann.

Auch am Runden Tisch Digitale Kultur und Schule in Bremen (siehe Ziffer 12.1 dieses Berichts) wurde diese Problematik kontrovers diskutiert. Wir halten den Einsatz sozialer Netzwerke in der Schule nur für zulässig, wenn das betreffende Netzwerk die Persönlichkeitsrechte, insbesondere der Schülerinnen und Schüler, vollständig wahrt. Dies ist bei facebook, das derzeit am häufigsten genutzt wird, nicht der Fall. Vielfach wird zudem diskutiert, ob sich Lehrkräfte und Schülerinnen und Schüler auf facebook gegenseitig als "Freunde" verlinken dürften.

Aus diesen Gründen haben Vertreterinnen und Vertreter der Universität Bremen – vorwiegend aus der Lehrerausbildung – sowie des Zentrums für Medien des Landesinstituts für Schule und die Landesbeauftragte für Datenschutz und Informationsfreiheit eine entsprechende Handreichung für Lehrkräfte erarbeitet. Unser gemeinsames Ziel war, die Unzulässigkeit der Nutzung von facebook in der Schule darzulegen und anhand von Beispielen den Lehrkräften zu verdeutlichen, dass diese für schulische Zwecke mit so hohen Risiken für die Persönlichkeitsrechte der Schülerinnen und Schüler verbunden ist, dass darauf verzichtet werden muss.

Leider ist uns dies offensichtlich nicht gelungen. Die Aussagen in der Handreichung sind widersprüchlich. Wir können nur den von uns erstellten Teil der Handreichung mittragen, der sich mit den Persönlichkeitsrechten der Schülerinnen und Schüler sowie der Lehrkräfte befasst.

8.2 Einsatz einer webbasierten Lernplattform

Die Kompetenz der Nutzung digitaler Medien ist inzwischen ein bedeutsamer Aspekt im Schulunterricht. Dazu gehört auch der Einsatz von webbasierten oder Online-Lernplattformen. Hierbei wird eine Vielzahl personenbezogener Daten von

Schülerinnen und Schülern und von Lehrerinnen und Lehrern verarbeitet. Weil diese Daten weltweit verarbeitet, verknüpft und in vielfältiger Weise ausgewertet werden können, bestehen erhebliche Risiken für die Persönlichkeitsrechte der Betroffenen. Insbesondere besteht die Gefahr, das Persönlichkeitsprofile erstellt werden. Das Zentrum für Medien des Landesinstituts für Schule hat in den letzten Jahren verschiedene Lernplattformen in einigen Schulen erprobt. In der anschließenden Evaluation hat das Zentrum für Medien festgestellt, dass digitale Medien wie facebook oder Dropbox – und andere in der Regel ausländische Dienstleister von Lernplattformen zur Unterstützung des Unterrichts – elementare Anforderungen des Datenschutzes nicht erfüllen. Nunmehr ist von Seiten des Zentrums für Medien geplant, eine entsprechende Ausschreibung für eine Lernplattform für die Schulen in der Stadtgemeinde Bremen durchzuführen.

Wir haben das Zentrum für Medien gebeten, wegen der besonderen Bedeutung für den Datenschutz der Schülerinnen und Schüler sowie der Lehrkräfte noch vor der Ausschreibung beteiligt zu werden. Insbesondere aufgrund des bekannt gewordenen anlasslosen und flächendeckenden Zugriffs des US-amerikanischen Geheimdienstes auf personenbezogene Daten von US-Unternehmen, die sich an europäische Nutzerinnen und Nutzer wenden und über deren Daten verfügen, halten wir es für unabdingbar, dass bei webbasierten Systemen wie einer Online-Lernplattform ein derartiger Zugriff ausgeschlossen ist, soweit er die Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung verletzt. Aus diesem Grunde haben wir gebeten, gemeinsam zu klären, wie eine datenschutzrechtlich wirksame Begleitung durch uns sichergestellt werden kann. Das Zentrum für Medien hat erklärt, dies werde mit der Firma Dataport, die die Ausschreibungen im Auftrage der Freien Hansestadt Bremen durchführen wird, in Kürze geklärt.

In diesem Zusammenhang haben wir das Zentrum für Medien auf einige wesentliche, jedoch nicht abschließende Anforderungen hingewiesen, die bei der Entscheidung über den Einsatz einer derartigen Lernplattform zu beachten sind.

Dabei geht es um die Einhaltung des Bremischen Schuldatenschutzgesetzes und des Bremischen Beamtengesetzes. Die datenschutzrechtliche Verantwortlichkeit liegt bei der Schule oder der Schulaufsicht. Aus unserer Sicht sollte ausschließlich die Schulaufsicht über den Einsatz einer Lernplattform in den Schulen entscheiden. Außerdem sind insbesondere folgende Aspekte zu prüfen beziehungsweise festzulegen:

- Richtlinien oder Grundsätze einschließlich Nutzungsbedingungen für eine Online-Lernplattform,
- Gestaltung und Auswahl einer Lernplattform nach den Grundsätzen der Datensparsamkeit und Datenvermeidung,
- keine Verarbeitung personenbezogener Daten außerhalb der Zuständigkeit der deutschen Gerichtsbarkeit,

- Klärung von Aufgabenübertragung und Auftragsdatenverarbeitung sowie Abschluss entsprechender Verträge,
- Unterrichtung der Betroffenen über Art und Ausmaß der Datenverarbeitung auf der Lernplattform,
- Löschung der Daten der Schülerinnen und Schüler im Regelfall zum Schuljahresende sowie Löschung der Benutzerkonten von Schülerinnen und Schülern sowie Lehrkräften nach deren Ausscheiden aus der Schule,
- Beachtung der Orientierungshilfe der Arbeitskreise Medien und Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder,
- technische und organisatorische Maßnahmen einschließlich der Zugriffsverwaltung.

Wir haben das Zentrum für Medien gebeten, uns zu bestätigen, dass unsere Hinweise beachtet werden und darauf hingewiesen, dass der behördliche Datenschutzbeauftragte der Schulen in der Stadtgemeinde Bremen und der Senatorin für Bildung und Wissenschaft vor der Entscheidung über den Einsatz einer Lernplattform einzubeziehen ist. Dies ist uns inzwischen zugesichert worden.

8.3 Beschaffung und Weitergabe von Adressdaten durch ein Museum

Ein Mitglied eines privaten Förderkreises eines Museums hatte unter seiner Privatanschrift Post eines auf Schiffsreisen spezialisierten Reiseveranstalters erhalten. Das Schreiben enthielt neben Informationen über Marketing zum Unternehmen Hinweise auf drei abendliche Veranstaltungstermine in den Räumlichkeiten des Museums, durchgeführt in Kooperation zwischen Unternehmen und Museum, und lud zur Teilnahme ein. Auf welchem Wege der private Reiseveranstalter seine Adressdaten als Fördermitglied des Museums erhalten hatte und ob dies datenschutzrechtlich zulässig war, diese Fragen wollte nun der Bürger durch uns geklärt wissen. Auf seine eigene schriftliche Nachfrage beim Museum zum dortigen Umgang mit Daten zu seiner Person hatte er auch nach Ablauf von über einem Monat noch keine Antwort erhalten.

Unsere Nachforschungen ergaben, dass sich das Museum im Zusammenhang mit einer Ausstellungseröffnung zur Durchführung der themenbezogenen Abendvorträge in Kooperation mit dem Reiseveranstalter entschlossen hatte. Es hatte Kontakt zur Leitung des Förderkreises aufgenommen und um Mitteilung der Adressdaten der Mitglieder des Förderkreises gebeten. Die erhaltenen Adressdaten reichte das Museum an den Reiseveranstalter beziehungsweise an dessen mit Erstellung und Versendung der entsprechenden Briefe beauftragten Dienstleister weiter.

Maßstab für die Bewertung der rechtlichen Zulässigkeit des Datenumgangs durch das Museum war das Bremische Datenschutzgesetz, da das Museum als rechtsfähige Stiftung

des Öffentlichen Rechts eine öffentliche Stelle ist. Rechtsfehlerhaft war zunächst die mehrwöchige Nichtbeantwortung der Nachfrage des Bürgers. Nach dem Bremischen Datenschutzgesetz haben öffentliche Stellen Betroffenen auf Antrag grundsätzlich unverzüglich Auskunft zu erteilen zu

- den zu ihrer Person gespeicherten Daten,
- dem Zweck und der Rechtsgrundlage der Speicherung und sonstigen Verarbeitung,
- dem logischen Aufbau einer automatisierten Verarbeitung der sie betreffenden Daten, soweit durch eine automatisierte Verarbeitung automatisierte Einzelentscheidungen getroffen werden sowie
- der Herkunft der Daten und dem Empfänger oder dem Kreis von Empfängern, an denen die Daten weitergegeben werden.

Als rechtsfehlerhaft erachteten wir auch die Erhebung der Adressdaten der Mitglieder des Förderkreises. Datenerhebungen durch öffentliche Stellen bei Stellen außerhalb der Verwaltung sind durch eine spezielle Vorschrift des Bremischen Datenschutzgesetzes geregelt. Danach können im Einzelfall ohne Kenntnis des Betroffenen bei Dritten außerhalb des öffentlichen Bereichs Daten nur erhoben werden, wenn eine (besondere) Rechtsvorschrift dies erlaubt oder zwingend voraussetzt oder wenn der Schutz von Leben und Gesundheit dies gebieten. Diese Voraussetzungen lagen nicht vor. Auch unter Zugrundelegung der allgemeinen Befugnisnorm wäre die Datenerhebung unrechtmäßig gewesen. Denn die Adressbeschaffung potenzieller Interessenten für offenkundig auch dem Ziel der Absatzförderung dienende Veranstaltungen eines Unternehmens war – unabhängig von möglichen mittelbaren Vorteilen auch für das Museum – ersichtlich bereits keine gesetzliche Aufgabe des Museums. Zudem war die Datenerhebung nicht erforderlich im Sinne des Fehlens einer objektiv zumutbaren Alternative, denn es hätte genügt, die entsprechenden Werbeschreiben und Einladungsschreiben mit der Bitte um Verteilung an die Leitung des Freundeskreises zu geben. War bereits die Erhebung der Adressdaten durch das Museum rechtswidrig, so konnten die unzulässig erhobenen Daten auch nicht rechtmäßig an den Reiseveranstalter beziehungsweise dessen Dienstleister übermittelt werden.

Da das Museum die rechtliche Problematik seiner Vorgehensweise einsah und eine Wiederholung eines solchen Vorgehens ausschloss, zudem die unzulässig übermittelten Daten bei dem Reiseveranstalter beziehungsweise seinem Dienstleister gelöscht waren und zu guter Letzt auch den betroffenen Mitgliedern des Freundeskreises kein weitergehender Schaden entstanden war, sahen wir von einer förmlichen Beanstandung ab.

8.4 Arbeitsgruppe Datenschutz und Schule

Die Arbeitsgruppe Datenschutz und Schule hat unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Berichtsjahr in Erfurt getagt. Hauptsächlich wurden folgende Themen erörtert:

- Datenschutz im Klassenzimmer,
- Weiterleitung sensibler Schülerdaten innerhalb der Schule und der Lehrerschaft sowie der Schulaufsicht per E-Mail,
- Nutzung privater E-Mail-Konten der Lehrkräfte zur Kommunikation mit den Eltern,
- Datenverarbeitung auf privaten Datenverarbeitungsgeräten der Lehrkräfte und Betreuungskräfte,
- soziale Medien im Schulbereich,
- Videoüberwachung an Schulen,
- Einführung von Chipkarten an Schulen für die Toilettenbenutzung,
- Datenverarbeitung durch Dritte im Auftrag von Schulen.

Darüber hinaus beabsichtigt die Arbeitsgruppe Datenschutz und Schule, eine Orientierungshilfe für Online-Lernplattformen im Schulunterricht (siehe Ziffer 8.2 dieses Berichts) zu erstellen, die es für Schulaufsichtsbehörden und Schulen ermöglicht, deren Einsatz datenschutzgerecht zu gestalten.

9. Umwelt, Bau und Verkehr

9.1 Weitergabe der Telefonnummer von Mietern an mögliche Nachmieter

Mehrmals erreichten uns Beschwerden von Mieterinnen und Mietern darüber, dass im Falle einer Kündigung der Mietwohnung ihre Telefonnummer von ihrer Wohnungsbaugesellschaft an interessierte Nachmieterinnen und Nachmieter zwecks Vereinbarung eines Besichtigungstermins weitergegeben wurde. Wir baten daraufhin die entsprechende Wohnungsbaugesellschaft um Auskunft, wie das Verfahren bei Kündigung einer Wohnung ablaufe. Stellten wir dabei datenschutzrechtliche Verstöße fest, wirkten wir auf deren Behebung hin. So ist eine Weitergabe der Telefonnummer der aktuellen Mieterinnen und Mieter an Interessenten zur Absprache eines Besichtigungstermins nur dann zulässig, wenn die betroffene Person der Datenübermittlung ausdrücklich zugestimmt hat. Auf die Vorschriften des Datenschutzgesetzes lässt sich die Weitergabe der Rufnummer hingegen nicht stützen, da die Datenübermittlung zur Vereinbarung eines Besichtigungstermins nicht erforderlich ist. Die Terminkoordination kann ebenso durch die Wohnungsbaugesellschaft erfolgen.

9.2 Datenübermittlung im Rahmen der energetischen Stadtsanierung

Eine Petentin machte uns auf das beim Senator für Umwelt, Bau und Verkehr angesiedelte Projekt "Energetische Stadtsanierung" aufmerksam. Es handelt sich dabei um ein gemeinsames Förderprogramm des Bundesministeriums für Verkehr, Bau und Stadtentwicklung und der Kreditanstalt für Wiederaufbau. Das Programm bezweckt eine Verbesserung der Energieeffizienz von ganzen Quartieren. Der Senator für Umwelt, Bau und Verkehr hatte sich für ein Bremer Quartier beworben und eine Förderzusage erhalten. Die Umsetzung soll gemeinsam mit einigen Bremer Wohnungsbaugesellschaften sowie dem Bildungsressort erfolgen. Mit der Erstellung des Quartierskonzepts wurde ein externes Büro beauftragt.

Uns stellte sich die Frage, ob für das Projekt personenbezogene Verbrauchsdaten der Mieterinnen und Mieter verarbeit werden. Dies sind sensible Informationen, die – insbesondere wenn noch weiteres Zusatzwissen hinzukommt – etliche Rückschlüsse auf die Lebensgewohnheiten der Betroffenen zulassen. Wir baten den Senator für Umwelt, Bau und Verkehr um Stellungnahme. Er teilte uns mit, dass für die Erstellung des integrierten Quartierskonzepts grundsätzlich keine personenbezogenen Verbrauchsdaten, sondern lediglich gebäudebezogene Daten, die die Wohnungsunternehmen beziehungsweise Versorgungsunternehmen zusammengefasst lieferten, erhoben und verarbeitet werden würden. Die Daten dienten dazu, für einzelne Gebäudetypen modellhafte Energiegutachten zu erstellen. Darüber hinaus sei den Eigentümerinnen und Eigentümern von selbst genutzten Einfamilienhäusern sowie den Mieterinnen und Mietern der Mietwohnungen die Möglichkeit gegeben worden, auf Basis einer Einwilligung Daten zur Verfügung zu stellen. Die Daten würden bei der Berechnung von Energieverbrauchsdaten einzelner Gebäude als Stichprobe zur Gegenkontrolle der errechneten Verbrauchsdaten verwendet und seien anonymisiert. Da es in dem Projekt um die Ertüchtigung des Gebäudetatbestands und nicht um die etwaige Änderung des Nutzerverhaltens gehe, bestehe kein Interesse daran, personenbezogene Daten zu verarbeiten.

Im Rahmen der weiteren datenschutzrechtlichen Prüfung nahmen wir Einsicht in die Daten. Einen Personenbezug der Verbrauchsdaten konnten wir anhand der uns vorliegenden Informationen nicht erkennen.

9.3 Luftbildaufnahmen zur Kontrolle von Kleingärten

Ein Kleingärtner beschwerte sich darüber, dass der Senator für Umwelt, Bau und Verkehr zur Kontrolle der Einhaltung baurechtlicher Vorschriften in Kleingärten Luftbildaufnahmen heranziehen würde. Der Petent hatte dagegen insbesondere deshalb Bedenken, weil nach seinem Eindruck die Aufnahmen an Sommertagen, also zu Zeiten, in denen die Kleingärten verstärkt besucht seien, gefertigt würden, was die Verletzung datenschutzrechtlicher

Belange der Betroffenen zur Folge haben könne. Er übersandte uns eine an ihn gerichtete Verfügung des Umweltsenators, mit der ihm verboten worden war, eine Überdachung an einem Gartenhaus erneut zu errichten. Als Beweismittel für die unzulässige Bebauung hätten Luftbildaufnahmen gedient. Nach Angaben des Petenten handelte es sich bei dem Objekt jedoch lediglich um eine Wetterschutzplane, die im Herbst wieder entfernt werden würde. Insofern stellte sich bereits die Frage nach der Geeignetheit der Luftbildaufnahmen zur Kontrolle der Kleingärten.

Wir forderten den Senator für Umwelt, Bau und Verkehr zur Stellungnahme auf und baten ihn um Übersendung einer solchen Luftbildaufnahme. Dieser teilte uns mit, dass die Fotografien nach Möglichkeit im Winter vor der Belaubung angefertigt werden würden. Personen seien auf den Aufnahmen nicht zu erkennen. Diese Auskunft bestätigte sich nach Sichtung der Luftbildaufnahme, deren Auflösung so gering war, dass weder Menschen, noch weitere Details, die Informationen zu bestimmten Personen preisgegeben hätten, zu erkennen waren. Insofern hatten wir keine datenschutzrechtlichen Bedenken gegen die Verwendung der Aufnahmen zur Kontrolle der Einhaltung baurechtlicher Vorschriften.

9.4 Solarkataster Bremen

Der Senator für Umwelt, Bau und Verkehr teilte uns mit, dass für die Stadt Bremen die Erstellung eines Solarkatasters, beziehungsweise einer Solarpotenzialanalyse ähnlich dem Solarkataster Bremerhaven geplant sei. Über die datenschutzrechtlichen Bedenken gegen das Bremerhavener Projekt berichteten wir unter Ziffer 9.3 in unserem 33. Jahresbericht. Dieser Bedenken ungeachtet wurde das Solarkataster Bremerhaven online gestellt. Um dem Datenschutz besser Rechnung zu tragen, wurde von den Initiatorinnen und Initiatoren des Solarkatasters Bremen zunächst vorgeschlagen, Recherchemöglichkeiten nur straßenbezogen, also ohne Hausnummern einzurichten, sodass eine immobilienbezogene Datenverarbeitung nicht möglich sei. Später wurde uns dann mitgeteilt, dass eine Suchmöglichkeit nach Hausnummern doch eingerichtet werden solle, da andernfalls vielen Nutzerinnen und Nutzern eine Identifikation des eigenen Hauses von oben schwerfalle oder nicht gelinge. Weitere Informationen, wie sie in Bremerhaven mit dem Wirtschaftlichkeitsrechner verbunden seien, solle es in Bremen hingegen nicht geben. Nach Durchsicht der uns übersandten Unterlagen stellten wir fest, dass im Solarkataster Bremen die gleichen Daten wie im Solarkataster Bremerhaven veröffentlicht werden. Hinsichtlich des Wirtschaftlichkeitsrechners stellte sich uns die Frage, ob die Werte aus dem Solarkataster Bremen nicht entsprechend in den Rechner auf der Internetseite aus Bremerhaven eingegeben werden könnten und dann das gleiche Ergebnis errechnet werden könnte, wie es bei einem separaten Rechner für Bremen der Fall wäre. Wir verwiesen insofern auf unsere Bedenken, die wir bereits gegen das Solarkataster Bremerhaven geäußert hatten. Auch das Solarkataster Bremen wurde online gestellt.

9.5 Falsche Informationen im Rahmen einer Überprüfung nach dem Luftsicherheitsgesetz

Ein Bürger teilte uns mit, dass er durch seinen Arbeitgeber im Hafengebiet eingesetzt werden solle. Dafür sei eine Zuverlässigkeitsüberprüfung durch die Luftsicherheitsbehörde erforderlich. Im Laufe des Verfahrens wurde ihm von dort mitgeteilt, dass er strafrechtlich erheblich in Erscheinung getreten sei, was Auswirkungen auf seine Zuverlässigkeit im Sinne des Verfahrens haben könne. Der Petent versicherte, bisher keine strafrechtlich relevanten Verfehlungen begangen zu haben. Eine zeitnahe Rehabilitierung sei für ihn sehr wichtig, da die Feststellung Auswirkungen auf seinen Arbeitsplatz haben könne. Auf die ihm eingeräumte Gelegenheit zur Stellungnahme hin habe er die Behörde bereits aufgefordert, seine Daten zu berichtigen. Zudem bat er um Auskunft über die Quelle der Informationen sowie über alle zu seiner Person gespeicherten Daten.

Auch wir baten die Luftsicherheitsbehörde um Stellungnahme zu der Herkunft der Daten, der Rechtsgrundlage, dem Zweck der Erhebung sowie möglichen Empfängern. Zudem forderten wir die Behörde auf, die Richtigkeit der Daten zu überprüfen.

Die Luftsicherheitsbehörde teilte uns mit, dass sie für die Zuverlässigkeitsüberprüfung auf Grundlage des Luftsicherheitsgesetzes und der Luftsicherheits-Zuverlässigkeitsüberprüfungsverordnung Auskünfte aus dem beim Bundesamt für Justiz geführten Bundeszentralregister einholen dürfe. Das Bundesamt für Justiz habe der Luftsicherheitsbehörde zum Petenten die strafrechtlichen Eintragungen benannt. Aufgrund der Schreiben der Landesbeauftragten für Datenschutz und des Petenten habe eine erneute Anfrage beim Bundesamt für Justiz stattgefunden. Es habe sich herausgestellt, dass dort offenbar ein Fehler unterlaufen sei, der eine unrichtige Auskunft aus dem Bundeszentralregister verursacht habe. Im Anschluss wurde eine korrekte Auskunft ohne Eintragungen an die zuständige Behörde übersandt.

10. Wirtschaft und Häfen

10.1 Weitergabe des Ergebnisses einer Gesellenprüfung unter Kolleginnen

Ein Auszubildender hatte die praktische Prüfung im gewählten Ausbildungsberuf nicht bestanden. Die für die Berufsausbildungsorganisation zuständige Mitarbeiterin der zur Prüfungsabnahme berufenen Körperschaft teilte dies einer mit anderweitigen Aufgaben betrauten weiteren Mitarbeiterin in einem Gespräch am Rande mit. Beide Mitarbeiterinnen waren Bekannte des Prüflings. Einige Zeit später ergab sich bei einem privaten Zusammentreffen ein Gespräch zwischen einer Angehörigen des Prüflings und jener

Mitarbeiterin. Als die Angehörige von dem missglückten Prüfungsversuch berichtete, erwiderte jene, sie habe hiervon schon von ihrer Kollegin gehört.

Nach dem Bremischen Datenschutzgesetz gelten auch für die Zulässigkeit der Weitergabe von personenbezogenen Daten innerhalb einer öffentlichen Stelle bestimmte Voraussetzungen, wenn es sich um einen Datenaustausch zwischen Einheiten mit unterschiedlichen Aufgabenbereichen handelt. Abgesehen von speziellen und vorliegend nicht einschlägigen Ausnahmen dürfen personenbezogene Daten allgemein zwischen Arbeitseinheiten mit unterschiedlichen Aufgabenbereichen nur ausgetauscht werden, wenn dies für die rechtmäßige Erfüllung der (gesetzlichen) Aufgaben der datenweitergebenden oder der datenempfangenden Arbeitseinheit erforderlich ist. Die persönliche Verpflichtung der Mitarbeiterinnen und Mitarbeiter der datenverantwortlichen öffentlichen Stellen zur Einhaltung dieser internen Datenumgangsgrenzen ergibt sich aus dem ebenfalls im Bremischen Datenschutzgesetz normierten sogenannten Datengeheimnis.

Die fragliche Mitteilung unter den Kolleginnen erfolgte lediglich im privaten Interesse, diente also weder bei der einen noch bei der anderen der Erfüllung der beruflichen Aufgaben. Mithin lag in der "Indiskretion" ein Verstoß gegen das Bremische Datenschutzgesetz vor. Da allerdings die Körperschaft und die Mitarbeiterinnen diesen Vorfall bedauerten und sich unmittelbar bei dem Betroffenen entschuldigt hatten, es sich zudem wohl um eine einmalige Indiskretion der Mitarbeiterin bei langjähriger gewissenhafter Beachtung des Datengeheimnisses handelte, zudem auch von einer generell gegebenen ausreichenden Sensibilität der Körperschaft für datenschutzgerechtes Verhalten ausgegangen werden konnte, und schließlich dem Betroffenen auch keine weitergehenden Nachteile aus der "Indiskretion" entstanden waren, beanstandeten wir diesen Verstoß formlos, sahen jedoch keine Notwendigkeit einer förmlichen Beanstandung.

11. Finanzen und Verwaltungsmodernisierung

11.1 Umstellungen von bargeldlosen Zahlungen auf SEPA

Im Berichtsjahr (vergleiche 35. Jahresbericht, Ziffer 10.2) wurde bei der Senatorin für Finanzen das Projekt SEPA (Single Euro Payments Area) fortgeführt. Von der Umstellung sind verschiedene zentrale Verfahren betroffen.

Zur Umstellung der Stammdaten sowie zu einzelnen Beschreibungen zu Schnittstellenprogrammen nahmen wir Stellung und wiesen mehrfach darauf hin, dass uns in diesem Zusammenhang die erforderliche Datenschutzdokumentation für die Verfahren SEPA, Giro und Fikus und die neu einzuführende Mandatsverwaltung nicht vorliegen. Ebenso erwarten wir nun unverzüglich die angepasste Verfahrensbeschreibung zum Verfahren TransX der Landeshauptkasse (vergleiche 35. Jahresbericht, Ziffer 4.3) und die Berechtigungskonzepte für die Verarbeitung von Zahlungsdaten im System SAP.

11.2 Einrichtung einer zentralen Zuwendungsdatenbank

Das Projekt ZEBRA zur Einrichtung einer zentralen Zuwendungsdatenbank wurde in diesem Berichtsjahr (vergleiche 34. Jahresbericht, Ziffer 11.2 und 33. Jahresbericht, Ziffer 10.2) fortgeführt.

Wir erhielten die ersten Entwürfe der angeforderten Verfahrensbeschreibung, das Rechtekonzept und das Rollenkonzept sowie die Dokumentation der Schnittstelle zum System SAP. Wir prüfen derzeit die Datenschutzdokumentation daraufhin, ob die getroffenen Maßnahmen den von uns aufgezeigten Anforderungen genügen.

11.3 Arbeitskreis Steuerverwaltung

Die Mitglieder des Arbeitskreises Steuerverwaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder befassten sich im Berichtsjahr unter anderem mit den Themen Kontendatenabrufverfahren, Steueridentifikationsnummer, ElsterOnline (elektronische Steuererklärung), Organisation des Postversandes in Finanzämtern (Infopost), ElsterLohn II/ELStAM, Kulturabgabe und Tourismusförderabgabe sowie mit der Kommunikation zwischen Steuerverwaltung und den Steuerpflichtigen sowie den Steuerberaterinnen und den Steuerberatern.

12. Medien/Telemedien

12.1 Runder Tisch Digitale Kultur und Schule

Der Runde Tisch Digitale Kultur und Schule hat im Berichtsjahr mehrfach getagt. Dabei hat er sich mit dem Projekt "Internet-ABC für Grundschülerinnen und Grundschüler" der Landesmedienanstalt und des Landesinstituts für Schule, dem Thema "facebook – Schule – Ein Dilemma?", mit der Evaluation eines Projektes zum Einsatz von Online-Lernplattformen des Landesinstituts für Schule, mit 3D-Druckern, also Maschinen, die dreidimensionale Werkstücke aufbauen, und Lasercuttern (Laserschneider) sowie mit dem Stand des Medienplans für die Grundschule befasst. Außerdem war die Präsenz und Aktivität von Menschen im Netz Thema. Dabei geht es insbesondere um die Berufsvorbereitung von Schülerinnen und Schülern sowie um digitale Bewerbungen.

12.2 Nutzung von facebook durch öffentliche und nicht öffentliche Stellen

Die Nutzung von facebook durch öffentliche und nicht öffentliche Stellen hat uns im Berichtsjahr weiter beschäftigt (vergleiche 34. Jahresbericht, Ziffer 12.5 sowie 35. Jahresbericht, Ziffer 11.2). Öffentliche Stellen, die planten, das soziale Netzwerk zu dienstlichen Zwecken zu nutzen, konnten wir überwiegend davon überzeugen, datenschutzkonforme Alternativlösungen zu wählen. Insbesondere die datenschutzkonforme

Verarbeitung von besonderen Arten personenbezogener Daten und der Wahrung des Sozialgeheimnisses oder der Verschwiegenheitspflicht ist bei der Nutzung von facebook nicht zu gewährleisten.

Als Vorsitzland der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben wir uns in diesem Jahr an die Vorsitzende der Konferenz der Regierungschefinnen und Regierungschefs der Länder gewandt. In unserem Schreiben haben wir im Namen der Datenschutzkonferenz das Bestreben des Arbeitskreises der Innenministerkonferenz begrüßt, die Offenlegung der technischen Abläufe bei Social Plugins, gemeint sind damit Erweiterungen für externe Seiten, und Fanseiten (insbesondere den Inhalt und den Nutzungszweck der verwendeten Cookies, im Besonderen des datr-Cookies) durch facebook zu fordern. Die Datenschutzkonferenz bot der Konferenz der Regierungschefinnen und Regierungschefs der Länder ihre Unterstützung bei einer solchen Initiative an. Gemeinsam mit der Innenministerkonferenz sollen nun Gespräche mit facebook aufgenommen werden.

12.3 Veröffentlichung von personenbezogenen Daten im Internet

Immer wieder erreichen uns Beschwerden über die Veröffentlichung von E-Mails, Briefen oder Fotos im Internet. Diese personenbezogenen Daten werden meist ohne Einwilligung, oft sogar ohne Kenntnis der Betroffenen auf Webseiten, in Foren oder auf Profilseiten in sozialen Netzwerken veröffentlicht. Liegt keine Einwilligung der Betroffenen in die Veröffentlichung ihrer personenbezogenen Daten im Internet vor, sind diese von der Webseite oder von der Profilseite in einem sozialen Netzwerk zu löschen. Sollten die Verantwortlichen dem Löschanspruch nicht nachkommen, unterstützen wir die Betroffenen bei der Durchsetzung ihrer Rechte.

Im Berichtsjahr erreichten uns Beschwerden zu Bürgeranträgen, die auf Webseiten der öffentlichen Stellen, bei denen die Einträge eingingen, veröffentlicht wurden. Diese Anträge enthalten in der Regel personenbezogene Daten wie Namen oder Adressen der Antragsstellerinnen und Antragssteller. Liegt keine Einwilligung der oder des Betroffenen zur Veröffentlichung der Daten vor, ist auch hier eine Veröffentlichung im Internet unzulässig. Zusätzlich ist die Veröffentlichung der personenbezogenen Daten nicht erforderlich. Der Inhalt des Antrags kann auch personenbezogene Daten der Antragstellerin oder des Antragstellers der Öffentlichkeit zugänglich gemacht werden.

Kritisch ist ebenfalls die Darstellung eines Unfallgeschehens oder eines Tathergangs in Pressemitteilungen oder Presseberichten, bei denen zwar keine Namen genannt werden, aber durch die Beschreibung von Tathergang beziehungsweise Unfallhergang, Ort und Zeit ein Rückschluss auf die tatsächlichen Personen möglich ist. Auch hier ist aus unserer Sicht in der Regel keine Beschreibung erforderlich, die die Identifizierung der beteiligten Personen zulässt, um die Öffentlichkeit über das Geschehene zu informieren und vor den mit der Unfallursache verbundenen Gefahren zu warnen.

12.4 Weitergabe von personenbezogenen Daten in Newslettern

Uns erreichten im Berichtsjahr einige Beschwerden und zahlreiche Nachfragen zu der Versendung von Newslettern und Rundschreiben per E-Mail. Der Anlass war regelmäßig, dass Newsletter per E-Mail an einen Verteiler mit verschiedenen E-Mail-Adressen versendet wurden, die offen über das Adressfeld für alle Empfängerinnen und Empfänger sichtbar waren.

E-Mail-Adressen sind grundsätzlich personenbezogene Daten, die nur dann an Dritte übermittelt werden dürfen, wenn die oder der Betroffene eingewilligt hat. Die Verwendung eines offenen E-Mail-Verteilers ohne Einwilligung der Betroffenen ist datenschutzrechtlich unzulässig; allein innerhalb eines Unternehmens oder einer Behörde kann dies aus beruflichen oder dienstlichen Gründen erforderlich sein und bedingt so keine explizite Einwilligung. Dies gilt allerdings nur, wenn die dienstlichen E-Mail-Adressen verwendet werden. Ist auch die private Nutzung des dienstlichen E-Mail-Dienstes zulässig und werden private E-Mail-Adressen für den Verteiler verwendet, ist auch hier die Einwilligung der Betroffenen erforderlich.

Liegt keine Einwilligung zur offenen Versendung der Empfängerinnen und Empfänger über das Adressfeld vor, sind die E-Mail-Adressen in das sogenannte BCC-Feld (Blind-Carbon-Copy, die sogenannte Blindkopie) einzutragen. Der Inhalt dieses Feldes ist für die Empfängerinnen und Empfänger nicht sichtbar.

12.5 Durchsetzung des Löschrechts bei Kundenkonten im Internet

Im Berichtsjahr erreichten uns zahlreiche Beschwerden zu verschiedenen Portalen im Internet, bei denen Nutzerinnen und Nutzer Probleme hatten, ihre Daten selber zu löschen oder durch den Anbieter löschen zu lassen. Meist hatten die Nutzerinnen und Nutzer ein Kundenkonto angelegt, um verschiedene Funktionalitäten der Webseite nutzen, an speziellen Kundenprogrammen teilnehmen oder in geschlossenen Bereichen mit anderen Nutzerinnen und Nutzern kommunizieren zu können. Die Beschwerden bezogen sich mehrheitlich darauf, dass die Nutzerinnen und Nutzer nach der Entscheidung, die Registrierung rückgängig zu machen, ihr Konto nicht oder nur nach sehr großem Aufwand löschen konnten.

Demgegenüber muss Nutzerinnen und Nutzern das Recht eingeräumt werden, ihr Kundenkonto ohne Angaben von Gründen jederzeit zu löschen, es sei denn, einer Löschung stehen gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegen. Dies kann beispielsweise bei Rechnungsdaten der Fall sein. Aber auch dann ist nur die Speicherung der dafür erforderlichen Daten zulässig. In den von uns im Berichtsjahr geprüften Fällen konnten wir fast immer darauf hinwirken, dass die Gestaltung der betroffenen Portale nutzungsfreundlicher gestaltet wurde und die Löschung für Nutzerinnen

und Nutzer leichter durchführbar wurde. Zusätzlich empfahlen wir den Unternehmen regelmäßig, weitere Informationen in einem gut gekennzeichneten Hilfebereich unterzubringen und eventuell kostenlose telefonische Unterstützung zu bieten.

12.6 Prüfung der Creditreform Mainz als Auftragnehmerin von Radio Bremen

Gemeinsam mit den Landesbeauftragten für Datenschutz der Länder Berlin und Hessen prüften wir im Berichtsjahr die Informationssicherheit des Unternehmens Creditreform Mainz, das im Auftrag der Landesrundfunkanstalten die Aufgaben der ehemaligen Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ), seit 2013 den sogenannten Beitragsservice, ausführt. Das Unternehmen ist dem Auftrag nach als Verwaltungshelfer zuständig, rückständige Rundfunkgebühren gegenüber den Rundfunkteilnehmerinnen und Rundfunkteilnehmern geltend zu machen.

Der Beginn der Prüfung der Informationssicherheit hatte sich stark verzögert, da die erforderlichen Unterlagen unvollständig und die ergriffenen technischen und organisatorischen Maßnahmen trotz zweier Gesprächstermine vor Ort und mehrfacher Aufforderungen nicht abschließend beschrieben worden waren. Die Prüfung vor Ort, die wir dennoch im Herbst gemeinsam mit den Landesbeauftragten für Datenschutz der Länder Berlin und Hessen durchführten, konnten wir daher nicht abschließen. Die Prüfung wird uns voraussichtlich auch im Jahr 2014 weiter beschäftigen.

12.7 Arbeitskreis Medien

Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschäftigte sich sowohl mit Themen des öffentlichen Bereichs als auch des nicht öffentlichen Bereichs. Relevant für beide Bereiche waren die datenschutzrechtliche Bewertung einzelner Angebote des Web 2.0, insbesondere die Kontrolle und Auswertung der Kommunikation und der Nutzungsverhalten durch die Anbieter sowie die Verarbeitung personenbezogener Daten durch Anbieter von Telemedien zu Werbezwecken. Zudem beschäftigte der Arbeitskreis Medien sich mit der Verarbeitung personenbezogener Daten bei Internet Protocol Television (über das Internet übertragenes Fernsehen, IPTV). Für die erste Jahreshälfte 2014 ist die Veröffentlichung einer Orientierungshilfe zur datenschutzkonformen Entwicklung und Gestaltung von Apps geplant, an der sich die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen neben Datenschutzbeauftragten der anderen Bundesländer aktiv beteiligt. Im öffentlichen Bereich lag der Schwerpunkt auf der Verarbeitung von Inhaltsdaten und Verkehrsdaten beziehungsweise Nutzungsdaten bei der Nutzung von elektronischen Kommunikationsdiensten durch inländische und ausländische Geheimdienste.

13. Beschäftigtendatenschutz

13.1 Öffentlicher Bereich

13.1.1 Verarbeitung von Gesundheitsdaten über Beschäftigte beziehungsweise Krankenversicherte zur Erstellung von Gesundheitsberichten

Im Gesundheitsbericht des bremischen öffentlichen Dienstes ist darüber berichtet worden, Performa Nord liefere einer Krankenkasse jährlich anonymisierte Auswertungen der Fehlzeiten und Krankheitsbilder der dort versicherten Beschäftigten. Wir haben bei der Behörde nachgefragt, ob hierzu personenbezogene Beschäftigtendaten an die Krankenkasse übermittelt werden, in welcher Weise die Krankenkasse die bei ihr vorhandenen Versichertendaten verknüpft beziehungsweise auswertet, um welche Krankheitsbilder oder Diagnosen es sich dabei handelt und auf welche Betriebsgröße sie bezogen sind.

Performa Nord erklärte, es würden keine personenbezogenen Daten an die Krankenkasse übermittelt. Die Krankenkasse werte die dort vorhandenen Versichertendaten anhand einer Betriebsnummer der Behörde aus. Bei den Krankheitsbildern in den Auswertungen handele es sich um 14 Diagnosegruppen, die sich auf die Gesamtheit der bei der Krankenkasse unter der Betriebsnummer von Performa Nord versicherten 71 Beschäftigten beziehe.

Daraufhin haben wir Performa Nord darauf hingewiesen, dass sich die Diagnosegruppen und Fehltage auf weniger als zehn Betroffene beziehen, sodass durch Zusatzwissen innerhalb der Behörde ein Personenbezug herstellbar ist. Insoweit haben wir nachgefragt, weshalb diese dezidierte Aufteilung in 14 Krankheitsbilder für Maßnahmen der Gesundheitsförderung erforderlich ist und ob es nicht ausreichen würde, Auswertungen zu erstellen, bei denen sich zusammengefasste Krankheitsbilder und Fehltage – auch hinsichtlich der jeweiligen Altersgruppen – auf mindestens zehn Beschäftigte beziehen.

Performa Nord erklärte, nur noch Differenzierungen vorzunehmen, die sich auf mindestens zehn Fälle beziehen. Alle aus den Erkenntnissen der Gesundheitsberichterstattung folgenden Angebote richteten sich jeweils offen an alle Beschäftigten und seien somit ohne Personenbezug zu den Auswertungsdaten.

13.1.2 Videoaufzeichnung und Tonbandaufzeichnung am Schreibtischarbeitsplatz

Wir erhielten eine Information, wonach ein Beschäftigter des Hansestadt Bremischen Hafenamtes an seinem Arbeitsplatz ein System installiert habe, mit dem

Videoaufzeichnungen und Tonaufzeichnungen der Personen erfolgten, die ebenfalls in dem Arbeitszimmer tätig seien beziehungsweise sich dort aufhielten. Begründet habe der Beschäftigte dies damit, er wolle das Gerät in seinem privaten Keller aufstellen und habe es am Arbeitsplatz lediglich getestet. Der Amtsleiter habe unmittelbar nach Feststellen des Sachverhalts dafür gesorgt, dass keine weiteren Aufzeichnungen erfolgten. Der Amtsleiter habe das Bildmaterial gesichtet und festgestellt, dass keinerlei Aufzeichnungen vorhanden seien, die den höchstpersönlichen Lebensbereichen der abgebildeten Personen zuzuordnen gewesen seien und die Löschung der Dateien veranlasst.

Erst danach wurden wir über den Vorfall unterrichtet und um eine Bewertung gebeten. Wir legten dar, dass es sich um eine unbefugte Datenerhebung durch einen Beschäftigten der Behörde an dessen Arbeitsplatz handelte, sodass das Bremische Datenschutzgesetz anwendbar war. Danach stellt die vorsätzliche oder fahrlässige unzulässige Datenverarbeitung eine Ordnungswidrigkeit dar, für die der Leitende Oberstaatsanwalt zuständig ist. Darüber hinaus kann es sich um eine Straftat handeln, soweit das nicht öffentlich gesprochene Wort unbefugt aufgenommen wird. Diese Tat wird grundsätzlich auf Antrag verfolgt. Die Betroffenen können deshalb innerhalb eines Zeitraums von drei Monaten, nachdem sie Kenntnis über diese Datenverarbeitung erhalten haben, einen Strafantrag bei der Staatsanwaltschaft stellen.

13.1.3 Namenskürzel von Lehrkräften in öffentlich zugänglichen Vertretungsplänen

Auf Vertretungsplänen einzelner Schulen in der Stadtgemeinde Bremen waren die Namenskürzel von Lehrkräften angegeben, die Vertretungen für andere Lehrkräfte übernehmen. Häufig werden diese Vertretungspläne auch im Internet veröffentlicht. Da es sehr kurze Namen gibt, ist ohne besonderen Aufwand an Zeit, Kosten und Arbeitskraft ein Bezug zu einzelnen Lehrkräften herstellbar. Wir haben die Senatorin für Bildung und Wissenschaft darüber unterrichtet und erklärt, dass die Angabe der Namenskürzel auf Vertretungsplänen generell für die Bekanntgabe von Stundenausfällen und Änderungen des Unterrichts nicht erforderlich und damit nicht zulässig ist. Die senatorische Behörde hat daraufhin eine Verfügung erlassen. Darin wird geregelt, dass Namen und Namenskürzel auf der Öffentlichkeit zugänglichen Vertretungsplänen nicht verwendet werden dürfen. Es handelt sich um Pläne, die im Internet, an einem digitalen Schwarzen Brett oder in Papierform innerhalb der Schule eingesehen werden können. Nach der Verfügung sind beispielsweise folgende Einträge möglich:

- Der Unterricht einer Klasse / eines Kurses fällt aus;
- Statt Mathematik findet Deutsch statt.

13.1.4 Weitergabe der Mobilfunknummer eines Lehrers an eine Schülerin

In einer Schule hatte der Leiter der Abteilung Fachoberschule das Sekretariat der Schule angewiesen, die private Mobilfunknummer eines Lehrers an eine Schülerin herauszugeben. Der Lehrer hatte in diese Datenübermittlung nicht eingewilligt. Da die Schülerin dem Lehrer ihr Anliegen bereits per E-Mail mitgeteilt hatte und ihm ein bestimmtes Dokument in dessen Postfach gelegt hatte, war die Übermittlung der Mobilfunknummer nicht erforderlich. Auf unsere Veranlassung hat der Leiter der Fachoberschule die Schülerin gebeten, unverzüglich die privaten Mobiltelefondaten des Lehrers zu löschen und sich dies bestätigen zu lassen. Dies ist inzwischen erfolgt.

13.1.5 Umgang mit einem amtsärztlichen Gutachten

Ein Beschäftigter hatte sich einer amtsärztlichen Untersuchung über seine Arbeitsfähigkeit zu unterziehen. Das zunächst an die Personalstelle der Senatorin für Soziales, Kinder, Jugend und Frauen übermittelte Gutachten enthielt falsche Diagnosedaten. Darüber hatte der untersuchende Arzt die senatorische Behörde unterrichtet und eine neue Version des Gutachtens übermittelt. Dem Wunsch des Petenten auf Vernichtung des "überholten Gutachtens" entsprach die senatorische Dienststelle nicht. Das "überholte Gutachten" wurde kopiert und die Kopie – zunächst offen – später in einem verschlossenen Umschlag zur Personalgrundakte genommen. Die Behörde erklärte, die vorübergehende Aufnahme der Kopie stehe nicht der Verwaltungsvorschrift über die Erhebung von Personalaktendaten und die Führung von Personalakten entgegen; sie sei unter Beachtung des Grundsatzes der Vollständigkeit der Personalakte geboten. Nach Eingang des Gutachtens in der geänderten Fassung wurde dieses ebenfalls in die Personalakte aufgenommen.

Wir haben die Behörde darauf hingewiesen, dass in diesem Fall die Richtigkeit bestimmter Angaben im Gutachten bestritten wurde und sich ohne Prüfung durch den untersuchenden Arzt weder die Richtigkeit noch die Unrichtigkeit feststellen lassen. In derartigen Fällen sieht das Bremische Datenschutzgesetz vor, die Daten zu sperren. Der Grundsatz der Vollständigkeit der Personalakte erlaubt keinesfalls eine Abkehr von dieser gesetzlichen Regelung. Es steht damit nicht im Einklang, eine Kopie eines vom Amtsarzt als unzutreffend bezeichneten Gutachtens anzufertigen und zur Personalakte zu nehmen. Es hätte hier stattdessen ausgereicht, in der Personalakte die Rückforderung des Gutachtens durch den untersuchenden Arzt zu vermerken. Auf unsere Anforderung hat die Behörde die Kopie des überholten Gutachtens aus der Personalakte entfernt und schließlich mitgeteilt, zukünftig in gleichgelagerten Fällen entsprechend unserer Anforderung zu verfahren.

13.1.6 Übermittlung von Beschäftigtendaten für eine Sonderprüfung an eine Wirtschaftsprüfungsgesellschaft

Die Handelskammer Bremen und die Industrie- und Handelskammer Bremerhaven hatten eine Sonderprüfung beider Kammern durch ein Wirtschaftsprüfungsunternehmen vereinbart. Dafür sollten personenbezogene Beschäftigtendaten an das Wirtschaftsprüfungsunternehmen übermittelt werden. Zweck der Sonderprüfung sollte sein, dass im Rahmen der beabsichtigten Fusionierung beider Kammern jede Kammer die finanziellen und vertraglichen Verpflichtungen, verbunden mit einer Perspektive über die Lastenrisiken bis 2020, der jeweils anderen Kammer erkennen können sollte.

Wir haben die Kammern darauf hingewiesen, dass sie als öffentliche Stellen dem Bremischen Datenschutzgesetz unterliegen und sich die Verarbeitung von Beschäftigtendaten nach dem Bremischen Beamtengesetz richtet. Danach dürfen Beschäftigtendaten verarbeitet werden, soweit dies für die dort genannten Zwecke erforderlich ist und schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Die Übermittlung von Beschäftigtendaten richtet sich nach der Vorschrift über Auskünfte an Dritte. Danach darf dies nur mit Einwilligung der oder des Betroffenen erfolgen, es sei denn, dass unter anderem der Schutz berechtigter höherwertiger Interessen des Dritten die Auskunftserteilung zwingend erfordert.

Die Übermittlung der Personaldaten hielten wir für die Sonderprüfung nicht für erforderlich, also nicht für das mildeste Mittel zur Zweckerreichung. Die jährlich zu erstellenden Berichte der Wirtschaftsprüfer beider Kammern enthalten bereits entsprechende Informationen. Zudem kann jede Kammer die laufenden Personalkosten sowie Pensionslasten als jeweilige Gesamtsumme ohne Angabe von Einzeldatensätzen wie Geburtsdaten und Eintrittsdaten sowie Aufgabenbeschreibungen der Beschäftigten und Geburtsdaten von Versorgungsempfängern vorlegen. Das Gleiche gilt für Honorare an Lehrbeauftragte oder Kosten für Lieferverträge oder sonstige Dienstleistungsverträge mit natürlichen Personen.

Letztlich wurde vereinbart, dass personenbezogene Angaben nur anonymisiert an das Wirtschaftsprüfungsunternehmen übermittelt werden. Beide Kammern baten das Unternehmen, die bereits übermittelten und dort gespeicherten personenbezogenen Beschäftigtendaten zu löschen.

13.2 Nicht öffentlicher Bereich

13.2.1 GPS-Überwachung von Taxifahrerinnen und Taxifahrern und Aufzeichnung von Telefongesprächen in einer Taxizentrale

Eine Taxizentrale verwendete ein GPS (Global Positioning System = Globales Positionsbestimmungssystem) zur Vermittlung von Fahrten für cirka 500 Taxen der angeschlossenen Unternehmen. Zusätzlich erhielten die Taxiunternehmen auf Wunsch den eigenen Zugriff auf das GPS. Ziel war es, den Unternehmen zu ermöglichen, ihre eigenen Fahrten mit eigenen Kundinnen und Kunden zu organisieren. Durch diese Zugriffe konnten die Unternehmen als Arbeitgeber ihre Beschäftigten lückenlos überwachen. So konnte der Arbeitgeber im 30-Sekunden-Abstand den genauen Standort feststellen, wann und wie lange sich eine Fahrerin oder ein Fahrer aus dem System abschaltete, wie lange einzelne Fahrten dauerten und vieles mehr. Die Taxifahrerinnen und Taxifahrer unterlagen insoweit einem ständigen Überwachungsdruck durch ihre Arbeitgeber. Sie mussten stets damit rechnen, dass ihr Arbeitgeber nicht nur die Erbringung ihrer jeweiligen Fahrleistungen sondern auch ihr Verhalten im Allgemeinen beobachtete, weil sie nicht wussten, ob und wann der jeweilige Arbeitgeber das Fahrzeug ortete und damit den Aufenthaltsort der Fahrerinnen und Fahrer feststellte, welche Strecke sie fuhren, wann, wie häufig und wo sie Pausen machten.

Für die datenschutzrechtliche Einordnung dieses Sachverhaltes kam es nicht darauf an, wie lange die Ortungsdaten den Arbeitgebern zur Verfügung standen und dass sie Leistungskontrollen und Verhaltenskontrollen nur unter Einhaltung des Bundesdatenschutzgesetzes und Beachtung der Grundsätze der Erforderlichkeit und Verhältnismäßigkeit vornehmen durften. Allein die Bereitstellung der Ortungsdaten der Fahrerinnen und Fahrer und die jederzeitige, von den Beschäftigten nicht nachprüfbare Einsichtnahme in die Daten durch die Arbeitgeber erzeugten einen unzumutbaren Überwachungsdruck auf die Betroffenen. Insoweit verwiesen wir auf die ständige Rechtsprechung des Bundesarbeitsgerichts zum Verbot der lückenlosen Überwachung von Beschäftigten durch Arbeitgeber.

Der Zugriff auf die GPS-Daten war nicht das mildestes Mittel zur Erteilung von Fahrtenaufträgen an die Fahrerinnen und Fahrer und daher nicht erforderlich. Ein milderes Mittel wäre der Zugriff der Taxiunternehmen auf das GPS der Taxizentrale nur im zeitlichen Zusammenhang mit der Entscheidung über den Fahrtauftrag gewesen. Ein weiteres milderes Mittel wäre beispielsweise die Nutzung von Rundrufen, die eine Meldungsmöglichkeit für diejenigen Fahrerinnen und Fahrer geboten hätten, die sich in der Nähe des Standortes befinden, an dem Fahrgäste abgeholt werden sollen.

Die Taxizentrale hat auf unsere Anforderung den Zugriff der angeschlossenen Mitgliedsunternehmen auf das GPS abgestellt.

Des Weiteren wurden alle bei der Taxizentrale eingehenden Telefongespräche (beispielsweise Taxibestellungen, Kundenbeschwerden und Notrufe von Fahrerinnen und Fahrern) aufgezeichnet. Anrufende Kundinnen und Kunden wurden auf die Gesprächsaufzeichnung hingewiesen. Wir erklärten dazu, dass die Gesprächsaufzeichnung das Recht am gesprochenen Wort verletzt, wenn nicht beide Gesprächsteilnehmer darin eingewilligt haben. Hierzu verwiesen wir auf die ständige Rechtsprechung des Bundesverfassungsgerichts. Eine wirksame Einwilligung der Betroffenen kam hier nicht in Frage. Gerade bei Taxibestellungen unter Zeitdruck dürfte für Fahrgäste keine angemessene Zeit vorhanden sein, über die Erteilung einer Einwilligung zu entscheiden. Auch Einwilligungen der Beschäftigten in der Taxizentrale und der Taxifahrerinnen und Taxifahrer wären ebenfalls nicht wirksam. Die Einwilligung im Arbeitsverhältnis ist regelmäßig nicht wirksam, weil die Freiwilligkeit in einem hierarchischen Verhältnis in der Regel nicht gegeben ist und insofern nur unter faktischem Zwang erfolgt. Das Gleiche gilt hinsichtlich der Einwilligungen von Fahrerinnen und Fahrern bei Notrufen. Hier kommt noch hinzu, dass in diesen Fällen ein Mithören durch die Taxizentrale zur Gefahrenabwehr ausreicht und insofern das mildeste Mittel ist.

Die Taxizentrale hat nunmehr die Aufzeichnung der Telefongespräche eingestellt.

13.2.2 Datenerhebung bei Dritten im Rahmen des Betrieblichen Eingliederungsmanagements

Im Rahmen des Betrieblichen Eingliederungsmanagements erkundigte sich der Personalbereich eines Autoherstellers bei einer Tagesklinik danach, ob sich ein bestimmter Beschäftigter dort eingefunden habe. Begründet wurde diese Datenerhebung mit der Fürsorge gegenüber dem Betroffenen. Auf die Frage, weshalb nicht beim Betroffenen selbst nachgefragt worden sei, erklärte das Unternehmen, es habe sich hier um einen Einzelfall gehandelt und versicherte, regelmäßig würden nur bei den Betroffenen entsprechende Daten erhoben. Dem Unternehmen seien keine weiteren Fälle bekannt, in denen in vergleichbarer Form vorgegangen worden sei.

13.2.3 Offenbarung sensibler Daten durch einen Beschäftigungsträger

Von einem Betroffenen erfuhren wir, dass Teilnehmerinnen und Teilnehmer an Maßnahmen eines Beschäftigungsträgers in Bremerhaven bei der Verrichtung von Arbeiten im öffentlichen Raum Arbeitskleidung (Jacken beziehungsweise Westen) tragen mussten, auf der der Name des Beschäftigungsträgers groß und deutlich aufgedruckt war. Außerdem enthielten die Müllbehälter, die die Betroffenen transportierten, einen entsprechend groß und deutlich erkennbaren Aufdruck der Firma. In Bremerhaven ist allgemein bekannt, dass der Beschäftigungsträger praktisch ausschließlich Personen in Qualifizierungsmaßnahmen oder in sogenannten Ein-Euro-Jobs beschäftigt. Damit wurde durch das Tragen der

Arbeitskleidung in der Öffentlichkeit erkennbar, dass es sich bei den Betroffenen um Empfängerinnen und Empfänger von Hartz IV handelte. Die Betroffenen fühlten sich insoweit stigmatisiert.

Der Beschäftigungsträger erklärte auf unsere Anfrage, die Arbeitskleidung der Teilnehmerinnen und Teilnehmer an derartigen Maßnahmen sei ausgetauscht worden und weise diesen Aufdruck nicht mehr auf. Auch seien die Beschriftungen mit dem Hinweis auf den Beschäftigungsträger von den eingesetzten Handkarren und Müllbehältern entfernt worden.

13.2.4 Aufbau einer webbasierten Praktikumsbörse

Ein Unternehmen bat uns um Beratung zum Aufbau einer internetbasierten Praktikumsbörse. Zweck der insbesondere von Medien und der Handelskammer Bremen sowie der Handwerkskammer Bremen entwickelten Praktikumsbörse sei die gezielte Information junger Menschen zur Berufswahl und Berufsorientierung in der Metropolregion Bremen/Oldenburg. Über die webbasierte Praktikumsbörse könnten sich Schülerinnen und Schüler sowie Studierende einem sogenannten Persönlichkeitstest unterziehen, sodass dieses Verfahren besondere Risiken für die Rechte und Freiheiten der Betroffenen aufwies.

Wir formulierten die folgenden Anforderungen: Insbesondere muss von den Möglichkeiten der Pseudonymisierung und Anonymisierung Gebrauch gemacht werden. Dafür ist es erforderlich, dass bei der Anmeldung in den Datenbanken auf die Angabe von Namen, Adressen, Telefonnummern und Profilbilder verzichtet wird. Bei der Angabe der E-Mail-Adressen muss den Betroffenen ermöglicht werden, eine E-Mail-Adresse ohne Namensbestandteile zu verwenden, damit sie anonym an dem Persönlichkeitstest teilnehmen können. Außerdem dürfen bei den Angaben zur Qualifikation wegen der Anforderungen nach dem Allgemeinen Gleichbehandlungsgesetz keine Angaben über Alter, Geschlecht und Herkunft (Geburtsort) erhoben und gespeichert werden. Soweit Unternehmen Interesse an einer oder einem Betroffenen formulieren, darf nur die E-Mail-Adresse der oder des Betroffenen weitergeleitet werden. Es reicht aus, wenn die oder der Betroffene ihre beziehungsweise seine Identität gegenüber dem Unternehmen oder der Behörde erst im Rahmen der Anbahnung eines Praktikumsverhältnisses beziehungsweise Beschäftigungsverhältnisses offenbart.

Hinsichtlich der Vorgaben nach dem Telemediengesetz müssen die Nutzerinnen und Nutzer zudem umfassend über Art, Umfang und Zweck der Erhebung und Verwendung ihrer personenbezogenen Daten in verständlicher Form unterrichtet werden (Datenschutzerklärung). Das Unternehmen sagte zu, unsere Vorgaben zu übernehmen und umzusetzen.

13.2.5 Vertrauliche Personaldokumente im offenen Postfach

Wir erhielten eine Mitteilung darüber, dass sich im Postfach einer Beschäftigten eine Vielzahl ausgedruckter Protokolle über vertrauliche Personalgespräche zwischen Vorgesetzten und Beschäftigten befunden hatte. Das Unternehmen, bei dem sie beschäftigt ist, bestätigte dies und erklärte, es habe zur Aufklärung die zuständige Staatsanwaltschaft eingeschaltet. Im Übrigen würden die Originale der Gesprächsprotokolle mit Einwilligung der Betroffenen in den Personalakten aufbewahrt, zusätzlich gescannt und in einem passwortgeschützten digitalen Ordner abgelegt.

Wir wiesen das Unternehmen auf unsere erheblichen Zweifel über die Freiwilligkeit dieser Einwilligungen hin und darauf, dass es ausreicht, dass Protokolle derartiger Personalgespräche lediglich den jeweiligen Vorgesetzten und jeweiligen Betroffenen ausgehändigt werden. Sobald zu einem späteren Zeitpunkt ein neues Personalgespräch stattfindet, muss das bisherige Protokoll vernichtet werden. Die elektronische Speicherung der Protokolle halten wir nicht für erforderlich und baten das Unternehmen, darauf zu verzichten. Darüber hinaus haben wir erklärt, dass die Einschaltung der Staatsanwaltschaft nicht ausreicht. Vielmehr muss das Unternehmen zusätzlich seine Datenverarbeitung analysieren, um datenschutztechnische Mängel feststellen zu können und gegebenenfalls zu beseitigen.

Inzwischen hat das Unternehmen erklärt, nunmehr sämtliche im elektronischen System gespeicherten Protokolle über die Personalgespräche gelöscht zu haben und zukünftig keine derartigen Protokolle mehr elektronisch zu speichern.

13.2.6 Angabe von E-Mail-Adressen zur Weiterleitung

Eine Beschäftigte fragte uns, ob Arbeitgeberinnen und Arbeitgeber berechtigt seien, die Beschäftigten zu verpflichten, ihre E-Mail-Adressen zum Zweck der Übersendung ihrer Gehaltsabrechnungen anzugeben. Gehaltsabrechnungen enthalten Angaben über die Höhe des Gehalts, Zusatzleistungen für Partner und Kinder sowie über die Religionszugehörigkeit. Während es sich schon bei Gehaltsdaten um sensible Daten handelt, unterliegen Angaben über die Religionszugehörigkeit darüber hinaus nach dem Bundesdatenschutzgesetz einem besonderen Schutz.

Insbesondere wegen dieses besonderen Datums ist der Arbeitgeber verpflichtet, besondere technische und organisatorische Maßnahmen zu treffen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung – also auch per E-Mail – nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Eine unverschlüsselte E-Mail ist wie eine offene Postkarte anzusehen, weshalb der unverschlüsselte Versand sensibler Daten gegen das Bundesdatenschutzgesetz verstoßen würde.

Unabhängig davon verstößt die Aufforderung an die Beschäftigten, ihre privaten E-Mail-Adressen mitzuteilen, gegen die speziellen Vorschriften zum Beschäftigtendatenschutz des Bundesdatenschutzgesetzes. Die Erhebung und Speicherung dieses Datums durch Arbeitgeberinnen und Arbeitgeber ist für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich. Es ist zumutbar, den Beschäftigten die Gehaltsabrechnungen in verschlossenen Umschlägen zu übergeben oder bei längerer Abwesenheit die Dokumente an die Betroffenen per Post zu versenden.

13.2.7 Aufbewahrung von Kopien über Meldungen zum eingestellten ELENA-Verfahren

Wir sind gefragt worden, ob Arbeitgeberinnen und Arbeitgeber die Kopien sämtlicher ELENA-Meldungen (Elektronische Einkommensnachweise, die monatlich von allen Arbeitgeberinnen und Arbeitgebern an die Zentrale Rentenstelle der Deutschen Rentenversicherung zu melden waren) aufbewahren müssen. Daraufhin haben wir erklärt, dass nach der Pressemitteilung des Bundesbeauftragten für den Datenschutz und für die Informationsfreiheit alle entsprechenden Meldungen bei den Stellen der Deutschen Rentenversicherung gelöscht worden sind, nachdem das ELENA-Aufhebungsgesetz im Jahr 2011 in Kraft getreten ist. Demzufolge ist eine weitere Speicherung der Kopien dieser Meldungen bei den Arbeitgebern nicht mehr erforderlich, sodass sie zu löschen sind.

13.2.8 Arbeitskreis Beschäftigtendatenschutz

Der Arbeitskreis Beschäftigtendatenschutz befasst sich mit Themen aus dem öffentlichen und dem nicht öffentlichen Bereich. Im Berichtszeitraum sind insbesondere folgende Themen behandelt worden:

- Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes,
- Fragerecht des Arbeitgebers oder Dienstherrn im Einstellungsverfahren,
- Vorlage erforderlicher Bewerberunterlagen,
- polizeiliches Bewerberauswahlverfahren,
- zentrales elektronisches Bewerbungsverfahren einer gesetzlichen Krankenkasse,
- Betriebliches Eingliederungsmanagement,
- Nutzung sozialer Netzwerke durch Personalstellen oder Personalabteilungen,
- E-Mail-Nutzung und andere Internetnutzung am Arbeitsplatz,
- elektronische Personalakte.

14. Videoüberwachung

14.1 Videokameras an privaten Gebäuden

In den letzten Jahren hat die Zahl der Eingaben von Bürgerinnen und Bürgern erheblich zugenommen, die sich durch Videokameras beobachtet fühlten, die durch Privatpersonen an, auf oder in deren Wohnhäusern sowie Wohnungen installiert wurden. Allein in diesem Berichtsjahr gingen über zwanzig Beschwerden bei uns ein, weil Bürgerinnen und Bürger die Befürchtung hatten, dass durch Kameras auch öffentlich zugängliche Bereiche (zum Beispiel Straßen, Fußwege, Parkflächen) miterfasst würden. In den meisten Fällen wurde uns nur der Straßenname sowie die Hausnummer des Kamerastandortes mitgeteilt, sodass wir die für die Kameras verantwortlichen Hauseigentümer oder Wohnungseigentümer erst ermitteln mussten. Unsere Anfragen an die verantwortlichen Personen wurden in den meisten Fällen zügig und bereitwillig beantwortet. Wir teilten den verantwortlichen Personen daraufhin mit, wie Kameras datenschutzkonform betrieben werden können. In vielen Fällen konnte dies durch eine Neuausrichtung der Kameras erreicht werden, weil die öffentlich zugänglichen Bereiche danach nicht mehr im Erfassungsbereich der Kameras lagen. Einen Abbau der Kameras verlangten wir in den Fällen, in denen die verantwortlichen Personen den vor dem Gebäude gelegenen öffentlich zugänglichen Parkplatz überwachten, um ihr dort abgestelltes Fahrzeug zu erfassen. Die Umsetzung der jeweils von uns geforderten Maßnahmen ließen wir uns schriftlich bestätigen.

14.2 Beratung zu geplanten Videoüberwachungen

Auch in diesem Berichtsjahr erhielten wir zahlreiche Anfragen, in denen es um geplante Videoüberwachungsmaßnahmen ging. Neben den telefonischen Beratungen nahmen wir zu den uns geschilderten Sachverhalten schriftlich Stellung. In einigen Fällen führten wir auch eine Beratung vor Ort durch.

So wandte sich im Februar eine Veranstaltungsgesellschaft an uns, die beabsichtigte, eine offene Videoüberwachung des öffentlichen Raumes vor dem Gebäude ihres Konzerthauses durchzuführen. Der Platz vor dem Gebäude sei zwar durch Schilder für den Fahrzeugverkehr gesperrt, dennoch würden dort mit zunehmender Tendenz unautorisiert Fahrzeuge geparkt. Hierdurch würden bei Veranstaltungen die Eingangsbereiche sowie die Notausgänge blockiert und im Brandfall oder Gefahrenfall sei die Sicherheit der Besucherinnen und Besucher sowie der Vorbeigehenden nicht zu gewährleisten. Durch die Videoüberwachung könnten die Störungen durch das Sicherheitspersonal erkannt und behoben werden.

Den anwesenden Vertretern der Gesellschaft wurde während des Vor-Ort-Termins erläutert, dass die genannten Beweggründe für eine Videoüberwachung des Vorplatzes durchaus nachvollziehbar seien. Wir wiesen aber gleichzeitig darauf hin, dass eine Videoüberwachung

nur zulässig ist, soweit sie für den genannten Zweck erforderlich ist, was voraussetzt, dass der Zweck der Videoüberwachung nicht durch mildere, ebenfalls geeignete Mittel erreicht werden kann. Wir vertraten daher im geschilderten Fall die Auffassung, dass eine Videoüberwachung nicht erforderlich ist, da die Beseitigung der angeführten Sicherheitsrisiken auch durch andere geeignete Maßnahmen erreicht werden kann. Im vorliegenden Fall schlugen wir in Anbetracht der örtlichen Begebenheiten vor, den Vorplatz durch Abgrenzungspoller für Falschparker unzugänglich zu machen. Auf unsere Anregung hin wollen sich die Vertreter der Gesellschaft nunmehr an die zuständigen Stellen der Stadt sowie die Feuerwehr wenden und dort die Bedenken hinsichtlich der Sicherheit im Ernstfall vorbringen, um dann mit diesen Stellen eine akzeptable Lösung für die Sicherheitsproblematik auf dem Vorplatz zu finden.

In einem weiteren Fall wurden uns Unterlagen über die Videoüberwachung in einer Kunstsammlung übersandt, die auf den neuesten technischen Stand gebracht werden sollte. Auf unsere Anregung hin nahmen an dem vor Ort geführten Beratungsgespräch neben der Geschäftsführung auch ein Techniker der beauftragten Installationsfirma sowie Personen der gewählten örtlichen Interessenvertretung der Mitarbeiterinnen und Mitarbeiter teil. Diese Runde besichtigte sämtliche betroffenen Räumlichkeiten der Kunstausstellung. Aufgrund der hierbei gewonnenen Erkenntnisse stellte sich für uns heraus, dass vor allem Lösungen dafür gefunden werden mussten, die lückenlose Überwachung der in den überwachten Bereichen tätigen Mitarbeiterinnen und Mitarbeiter sowie Besucherinnen und Besucher zu verhindern. Ebenso sollten die Zugänge zu den Sozialräumen und Sanitärräumen sowie die Durchgänge zwischen den Ausstellungsräumen von der Überwachung ausgenommen werden. Als weiteres Problem stellte sich die Überwachung eines Kunstwerkes dar, welches sich über mehrere Etagen erstreckt, von einer Wendeltreppe umgeben ist und durch Berührungen stark beschädigt werden könnte.

An dem sich anschließenden Beratungsgespräch nahmen alle Anwesenden teil und trugen ihre jeweiligen Positionen vor. Aus datenschutzrechtlicher Sicht wurden von uns zu den einzelnen Problembereichen entsprechende Lösungsmöglichkeiten vorgeschlagen. Es wurde letztlich Einigkeit darüber erzielt, dass diese auch im neu zu installierenden System umgesetzt werden sollen. Im Wesentlichen werden die von den Kameras gezeigten und auch vom System gespeicherten Videobilder so eingestellt, dass bestimmte Bereiche des Bildes elektronisch und unwiederbringlich geschwärzt werden. Die zu überwachenden Bereiche, die nur einen Teilbereich des von der jeweiligen Kamera abgedeckten Bereiches umfassen, werden innerhalb der Software elektronisch gekennzeichnet. Das bedeutet, dass die Aufzeichnung erst dann beginnt, wenn eine Person diesen Bereich betritt. Halten sich die Personen außerhalb dieses Bereiches auf, erfolgt keine Aufzeichnung.

Hinsichtlich der Überwachung des sich im Mittelschacht einer Wendeltreppe befindenden Kunstobjektes verständigten wir uns darauf, dass ein Teilbereich der Treppe mit im

Erfassungsbereich der Kameras liegt, aber eine Aufzeichnung beziehungsweise Bildansicht erst dann ausgelöst wird, wenn die Videoanlage Bewegungen innerhalb eines Radius von einem Meter um das Objekt herum ermittelt. Hierdurch wird sichergestellt, dass nicht die gesamte Treppenbreite erfasst wird und somit keine dauerhafte Überwachung des Personals sowie der Besucherinnen und Besucher stattfinden kann.

14.3 Videoüberwachungskameras im Foyer eines Theaters

Ein Petent unterrichtete uns darüber, dass im Foyer eines Bremer Theaters diverse Kameras angebracht seien. Es sei zu befürchten, dass die Gäste des Restaurants und das Publikum sowie das Personal überwacht würden. Außerdem seien keine Hinweisschilder auf eine Videoüberwachung vorhanden.

Das Theater bestätigt uns auf unsere Anfrage das Vorhandensein von sechzehn Kameras. Die Kameras seien im Zuge der Einrichtung einer Theatergalerie installiert worden. Die Videoüberwachungsanlage diene dem Schutz der Ausstellungsstücke und sei zumeist auch Anforderung der ausstellenden Künstler beziehungsweise verleihenden Galerien. Die Anlage sei jedoch seit neun Monaten deaktiviert, da die künstlerische Leitung des Theaters keine Ausstellungen mehr durchführe.

Wir legten daraufhin dar, dass auch die deaktivierten Kameras optisch den Eindruck erweckten, es handele sich um funktionstüchtige Kameras. Hierdurch werden bei den Betroffenen der Eindruck erweckt, es finde eine Videoüberwachung statt. Damit unterscheidet sich die Situation für die Betroffenen nicht wesentlich von derjenigen, die durch Anbringung einer funktionstüchtigen Kamera geschaffen werde. Hierdurch wird in das allgemeine Persönlichkeitsrecht der Betroffenen eingegriffen, da von solchen Kameras derselbe Überwachungsdruck ausgeht wie von einer tatsächlich einsatzbereiten Überwachungseinrichtung, zumal es jederzeit möglich wäre, die Kameras wieder zu aktivieren.

Wir forderten das Theater daher auf, die deaktivierten Kameras entweder abzumontieren oder abzuhängen. Zunächst wurde uns als Übergangslösung bestätigt, dass die Kameras zur Decke oder Wand gedreht worden seien. Hierdurch ist für die Betroffenen klar erkennbar, dass sie nicht von einer der Kameras erfasst werden und mit den Kameras keine Aufnahmen mehr durchgeführt werden können. Inzwischen wurde uns mitgeteilt, dass sämtliche Kameras komplett demontiert seien.

15. Auskunfteien

15.1 Falschauskunft einer Auskunftei

Die Anmietung einer Wohnung im Großraum Hamburg stand kurz bevor, als das in die Vermittlung eingeschaltete Maklerbüro noch bei einer Auskunftei in Bremen über den potenziellen Mieter eine Bonitätsauskunft einzuholen beschloss (auf die datenschutzrechtliche Zweifelhaftigkeit der Einholung von umfassenden Bonitätsauskünften über Mietinteressenten aus Sicht der bremischen Datenschutzaufsichtsbehörde sei in diesem Zusammenhang hingewiesen). Die eingeholte Bonitätsauskunft wies auf dem Papier für den Mietinteressenten eine äußerst kritische finanzielle Lage aus, zur Überraschung auch des Mietinteressenten, der den Mietzins seiner vorhergehenden Wohnung anstandslos über den Mietzeitraum beglichen hatte und dies auch nachweisen konnte. Auch der Umstand, dass er bei einem konkurrierenden großen Anbieter von Auskunfteiprodukten mit keinerlei negativem Eintrag geführt war, konnte die entstandenen Zweifel beim Vermieter nicht mehr beseitigen. Der Abschluss des Mietvertrages scheiterte.

Daraufhin wandte sich der Mietinteressent umgehend an die Auskunftei, um deren Negativdatenbestand zu seiner Person im Wege einer sogenannten Selbstauskunft im Einzelnen zu ergründen und auf Beseitigung etwaiger fehlerhafter Einträge hinzuwirken. Eine solche Selbstauskunft kann grundsätzlich jede von Verarbeitungen ihrer Daten betroffene Person bei der Daten verarbeitenden Stelle kostenfrei beanspruchen. In Beantwortung seiner Anfrage teilte ihm die Auskunftei mittels einer automatisiert generierten E-Mail jedoch wahrheitswidrig mit, dass sie innerhalb der letzten zwölf Monate vor Zugang des Eigenauskunftsersuchens keine Daten zu seiner Person übermittelt hätte und auch keine zu beauskunftenden Bonitätsdaten zu seiner Person vorhanden seien.

Wir haben wegen dieser unrichtigen Selbstauskunft, die den gesetzlichen Auskunftsanspruch des Datenverarbeitungsbetroffenen grob verletzt, rechtliche Schritte eingeleitet.

16. Dienstleistungen, Handel und Werbung und Adresshandel

16.1 Werbe-E-Mails trotz Widerspruchs

Obwohl ein Petent bereits vor längerer Zeit einem Unternehmen gegenüber der Nutzung seiner Daten zu Werbezwecken widersprochen und die Löschung seiner Daten verlangt hatte, bekam er weiterhin Werbe-E-Mails an seine E-Mail-Adresse. Das Unternehmen erklärte, die E-Mail-Adresse des Petenten sofort in die Sperrdatei aufgenommen zu haben. Aufgrund eines EDV-Fehlers habe der Petent jedoch weiterhin versehentlich Werbe-E-Mails erhalten. Inzwischen habe die Firma das Newsletter-System dahingehend umgestellt, dass zukünftig keine Sperrdatei mehr vorgehalten werde und bei Kündigung des

Newsletterabonnements die entsprechenden Daten sofort aus dem System gelöscht würden. Kundendaten im Warenwirtschaftssystem würden nach Abschluss der Geschäftsbeziehung gelöscht beziehungsweise gesperrt, soweit gesetzliche Bestimmungen, insbesondere steuerrechtliche Auskunftspflichten, eine sofortige Löschung nicht zuließen. Diese Lösung halten wir für datenschutzrechtlich unbedenklich.

16.2 Arbeitsgruppe Werbung und Adresshandel

Schwerpunktmäßiges Thema der Arbeitsgruppe Werbung und Adresshandel war im Berichtszeitraum die Überarbeitung der Anwendungshinweise der Aufsichtsbehörden.

Die Überarbeitung erfolgte vor dem Hintergrund neuer Rechtsprechung. Danach ist eine Einwilligung in die Nutzung von Daten für Werbezwecke nur wirksam, wenn sie in Kenntnis der Sachlage und für den konkreten Fall erklärt wird. Die Einwilligungserklärung muss daher verständlich formuliert sein.

Außerdem wird den verantwortlichen Stellen empfohlen, die Betroffenen über den Sinn und Zweck zu informieren, weshalb ihre Daten in eine Sperrdatei im Falle von Widersprüchen aufgenommen werden. Damit soll gewährleistet werden, dass die Daten der Betroffenen zukünftig nicht mehr zu Zwecken der Werbung genutzt werden.

Ein weiterer Punkt beinhaltet die Erläuterung, dass bereits laufende Werbeaktionen regelmäßig nicht mehr gestoppt werden können, wenn Betroffene erst nach Beginn dieser Aktionen widersprechen. Darüber hinaus wird darauf hingewiesen, dass der Adresshandel einer Aufzeichnungspflicht und Auskunftspflicht über die Herkunft und die Empfänger von Daten unterliegt, wenn er Daten ohne Einwilligung der Betroffenen erhebt.

Sobald die Anwendungshinweise mit den Aufsichtsbehörden des Bundes und der Länder abgestimmt worden sind, werden sie auf unserer Homepage unter www.datenschutz.bremen.de veröffentlicht.

17. Kreditwirtschaft

17.1 Änderung der Rechtslage zugunsten eines Kreditinstituts nach Erlass einer datenschutzrechtlichen Anordnung der Bremischen Landesbeauftragten

Ein Kreditinstitut erfragte bei Vermietern, die ein (treuhänderisches) Konto zur Anlage der von ihren Mietern erhaltenen Mietkautionsgelder eröffnen wollten, Vorname und Nachname, Geburtsdatum, Geburtsort und Anschrift zu den Mietern. Wir forderten das Kreditinstitut auf, auf eine generelle Abfrage der über den Namen hinausgehenden Daten zu Mieterinnen und Mietern zu verzichten, da diese mit der Rechtslage nach dem Geldwäschegesetz unvereinbar sei. Entgegen unserer Aufforderung setzte das Kreditinstitut jedoch seine

Datenerhebungen fort. Nach umfangreichem Schriftwechsel, der sich weit über ein Jahr hinzog, erließen wir schließlich im Mai 2012 eine Anordnung, um die aus unserer Sicht dem Geldwäschegesetz und dem Bundesdatenschutzgesetz widersprechende Praxis des Kreditinstituts abzustellen. Die entscheidende Vorschrift des Geldwäschegesetzes lautete in der zur Zeit der Anordnung geltenden Fassung wie folgt:

> "Bei einem wirtschaftlich Berechtigten hat der Verpflichtete zur Feststellung der Identität zumindest dessen Name, und, soweit dies in Ansehung des im Einzelfall bestehenden Risikos der Geldwäsche oder der Terrorismusfinanzierung angemessen ist, weitere Identifizierungsmerkmale zu erheben…"

Aufgrund dieser Gesetzesformulierung und unter Berücksichtigung weiterer rechtlicher Gründe gingen wir davon aus, dass das Kreditinstitut zur Identitätsfeststellung der Mieterinnen und Mieter als wirtschaftlicher "Eigentümer" der Mietkautionsgelder eben zunächst einmal nur deren Namen (= Vornamen und Nachnamen) erheben durfte. Um weitere Identifizierungsmerkmale der Mieterin oder des Mieters beim Vermieter zu erheben, also etwa das Geburtsdatum, den Geburtsort und die Mietanschrift, bedurfte es aus unserer Sicht einer Berücksichtigung des Risikograde einer Geldwäsche oder Terrorismusfinanzierung durch den Vermieter und/oder den beziehungsweise die Mieterinnen und Mieter im konkreten Einzelfall.

Das Kreditinstitut erhob im Juni 2012 gegen unsere Anordnung Klage. Eine Begründung der Klage erfolgte nicht. Erst nach mehrfacher gerichtlicher Erinnerungen an die Vorlage der Klagebegründung und wiederholten Fristverlängerungsbitten des Kreditinstituts erfolgte mit Schreiben vom 26. Februar 2013 eine Klagebegründung.

Währenddessen hatte die Bundesregierung Ende September 2012 den Entwurf eines Gesetzes zur Ergänzung des Geldwäschegesetzes in den Deutschen Bundestag eingebracht (Bundestagsdrucksache 17/10745). Vorschläge, die sich auf die vorstehend zitierte Vorschrift und damit unsere Anordnung ausgewirkt hätten, beinhaltete der vorgelegte Gesetzentwurf der Bundesregierung nicht.

Der – aus sechs Abgeordneten bestehende – Finanzausschuss des Deutschen Bundestages in der 17. Legislaturperiode, der sich federführend mit dem Gesetzentwurf der Bundesregierung befasste, führte in seiner 108. Sitzung im Oktober 2012 eine öffentliche Anhörung zu dem Gesetzentwurf unter Beteiligung von Verbänden wie der Betfair Group plc., der BITKOM, der Deutschen Kreditwirtschaft), Institutionen (etwa BaFin, Bundeskriminalamt) und Sachverständigen durch. Er beschloss, mehrere Ergänzungen in den Gesetzentwurf der Bundesregierung aufzunehmen. Unter anderem entschied er sich dazu, die oben zitierte Vorschrift des Geldwäschegesetzes um einen weiteren, neu aufzunehmenden Satz zu ergänzen, der wie folgt lautete:

"Geburtsdatum, Geburtsort und Anschrift des wirtschaftlich Berechtigten dürfen unabhängig vom festgestellten Risiko erhoben werden."

Zur Begründung dieser Neuregelung führte der Finanzausschuss aus, bei der Überprüfung wirtschaftlich Berechtigter müsse auch geklärt werden, ob es sich insoweit um eine politisch exponierte Person handele. Dabei träten häufig Namensgleichheiten auf. Folglich bedürfe es in einer Vielzahl von Fällen neben dem Namen weiterer Identifizierungsmerkmale, um die tatsächlich politisch exponierten Personen treffsicher bestimmen und von bloßen nicht verwandten "Namensvettern" unterscheiden zu können. Und weiter: Entsprechend erlaube es nun der neue § 4 Absatz 5 Satz 2 Geldwäschegesetz, dass neben dem Namen auch das Geburtsdatum, der Geburtsort und die Anschrift wirtschaftlich Berechtigter in jedem Fall erhoben werden könne (Bundestags-Drucksache 17/11416, Seite 9). Der Finanzausschuss empfahl sodann am 7. November 2012 mit den Stimmen der Abgeordneten der Koalitionsfraktionen unter Enthaltung der Mitglieder der Oppositionsfraktionen dem Deutschen Bundestag die Annahme des Gesetzentwurfs mit dieser und anderen Änderungen (Bundestags-Drucksache 17/11335, Seite 6).

Der Gesetzentwurf in der Fassung der Beschlussempfehlung des Finanzausschusses wurde vom Deutschen Bundestag am 8. November 2012 mit den Stimmen der Koalitionsfraktionen angenommen. Das Gesetz zur Ergänzung des Geldwäschegesetzes wurde sodann am 25. Februar 2013 im Bundesgesetzblatt verkündet (Bundesgesetzblatt I 2013 Nummer 9, Seiten 268 fortfolgende) und trat am Tag nach der Verkündung, also dem 26. Februar 2013, in Kraft. Die durch dieses Gesetz mit Wirkung ab dem 26. Februar 2013 geänderte Vorschrift des § 4 Absatz 5 Sätze 1 und 2 – neu – Geldwäschegesetz lautet(e) nunmehr wie folgt:

"Bei einem wirtschaftlich Berechtigten hat der Verpflichtete zur Feststellung der Identität zumindest dessen Name und, soweit dies in Ansehung des im Einzelfall bestehenden Risikos der Geldwäsche oder Terrorismusfinanzierung angemessen ist, weitere Identifizierungsmerkmale zu erheben. Geburtsdatum, Geburtsort und Anschrift des wirtschaftlich Berechtigten dürfen unabhängig vom festgestellten Risiko erhoben werden..."

Zeitgleich mit dem Inkrafttreten der Gesetzesänderung am 26. Februar 2013 legte nun das Kreditinstitut, bei Gericht seine Klagebegründung vor und verwies darin im Wesentlichen auf die geänderte Rechtslage. In Ansehung der Rechtsänderung blieb uns lediglich, die Anordnung mit Wirkung für die Zukunft aufzuheben.

18. Internationaler Datenverkehr

18.1 Überwachung durch den US-amerikanischen Geheimdienst

Im Frühsommer 2013 enthüllte Edward Snowden, ein ehemaliger Mitarbeiter des US-amerikanischen Geheimdienstes National Security Agency (NSA) umfassende und anlasslose Überwachungsmaßnahmen der NSA. Es steht im Raum, dass ein großer Teil des Kommunikationsverhaltens auch der Menschen in Deutschland ohne ihr Wissen von der NSA überwacht wird. Dies wird insbesondere dadurch untermauert, dass die Vereinigten Staaten von Amerika (USA) Edward Snowden wegen Geheimnisverrats strafrechtlich verfolgen. Auch hat die NSA den Berichten Snowdens nicht substantiiert widersprochen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, deren Vorsitz im Berichtsjahr in Bremen lag, hat in mehreren Entschließungen die Erwartung geäußert, dass die Bundesregierung alles unternimmt, um die Menschen in Deutschland vor informationellen Zugriffen zu schützen, die mit der Verfassungsordnung des Grundgesetzes nicht im Einklang stehen. Die Bundesregierung müsse für eine restlose Aufklärung sorgen und dabei auch die Frage beantworten, ob deutsche Behörden diese Informationen übermittelt bekamen und verwendeten. Die bekannt gewordenen Überwachungsmaßnahmen unterstrichen die Dringlichkeit, für Europa hohe Datenschutzstandards zu beschließen und sicherzustellen, dass diese auch für staatliche und private Stellen aus Staaten außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (Drittstaaten) gelten. Die Bundesregierung müsse sich im Europäischen Rat für ein hohes Datenschutzniveau und für Regelungen einsetzen, die umfassende und anlasslose Überwachungsmaßnahmen europäischer und außereuropäischer Stellen ausschließen. Dies gelte sowohl für die Datenschutz-Grundverordnung der Europäischen Union als auch für das zwischen Europa und den USA anstehende Freihandelsabkommen (siehe hierzu die Ziffern 22.5 und 22.6 dieses Berichts).

Dies trug die diesjährige Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auch der Bundeskanzlerin in einem Schreiben Ende Juli 2013 vor. Die Antwort des Kanzleramtsministers im August 2013 war sehr allgemein gehalten und daher enttäuschend.

Die Bundeskanzlerin hat im Juli 2013 ein Acht-Punkte-Programm für einen europäischen und internationalen Datenschutz vorgelegt. Ob aufgrund dieser Punkte, nämlich

1. Aufhebung von Verwaltungsvereinbarungen,
2. Gespräche mit den USA auf Expertenebene,
3. UN-Vereinbarung zum Datenschutz,
4. Datenschutz-Grundverordnung,

5. Standards für Nachrichtendienste in der EU,

6. Europäische IT-Strategie,

7. Runder Tisch "Sicherheitstechnik im IT-Bereich" und

8. "Deutschland sicher im Netz",

tatsächlich in kurzer Zeit die anlasslose und flächendeckende Überwachung durch die NSA abgestellt wird, darf bezweifelt werden.

Auf eine Kleine Anfrage der Bundestagsfraktion der Sozialdemokratischen Partei Deutschlands hat die Bundesregierung vor der Bundestagswahl im Wesentlichen erklärt, sie habe von den in den Medien berichteten Überwachungsprogrammen keine Kenntnis. Des Weiteren legte sie sehr allgemein dar, was ihr seitens der US-Regierung anlässlich diverser Gespräche mitgeteilt wurde (Bundestags-Drucksache 17/14560).

Im Frühherbst 2013 wurde des Weiteren enthüllt, dass die NSA seit Jahren Zugriff auf die Mobilfunktelefone der Bundeskanzlerin hatte. Dadurch erhielt die Diskussion über die Überwachungsmaßnahmen der NSA wieder Auftrieb. Aus Sicht des Grundrechtes auf informationelle Selbstbestimmung wiegt diese Verletzung nicht schwerer als die flächendeckende Überwachung der Menschen in Deutschland.

18.2 Prüfung der Datenübermittlung in die Vereinigten Staaten von Amerika bei Unternehmen im Land Bremen aufgrund der Datenzugriffe des US-amerikanischen Geheimdienstes

Den Aufsichtsbehörden stehen beim internationalen Datenverkehr zwischen Unternehmen in Deutschland und Drittstaaten Befugnisse nach dem Bundesdatenschutzgesetz und der EU-Datenschutz-Richtlinie zu. Die Europäische Kommission hat in mehreren Entscheidungen Grundsätze des sogenannten Safe Harbor (sicherer Hafen) zum Datentransfer in die Vereinigten Staaten von Amerika (USA) und Standardvertragsklauseln zum Datenverkehr auch in andere Drittstaaten festgelegt. Die Beachtung dieser Vorgaben soll gewährleisten, dass personenbezogene Daten, die in die USA oder andere Drittstaaten übermittelt werden, dort einem angemessenen Datenschutzniveau unterliegen. In ihrer Safe-Harbor-Entscheidung hat die Kommission betont, dass die Aufsichtsbehörden die Datenübermittlung in die USA aussetzen können, wenn eine "hohe Wahrscheinlichkeit" besteht, dass die Safe-Harbor-Grundsätze oder Standardvertragsklauseln verletzt werden.

Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, welche die diesjährige Konferenzvorsitzende Anfang Oktober auch dem zuständigen Ausschuss des Europäischen Parlamentes vorgetragen hat, ist dieser Fall jetzt eingetreten, weil die National Security Agency (NSA) nach den gegenwärtigen Erkenntnissen umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und

Zweckbindung auf personenbezogene Daten zugreift, die von Unternehmen an Stellen in den USA übermittelt werden. Zwar enthält die Safe-Harbor-Vereinbarung eine Regelung, die die Geltung der Grundsätze des "sicheren Hafens" begrenzt, sofern es die nationale Sicherheit erfordert oder Gesetze solche Ermächtigungen vorsehen. Im Hinblick auf das Ziel eines wirksamen Schutzes der Privatsphäre soll jedoch von diesen Eingriffsbefugnissen nur im Rahmen des tatsächlich Erforderlichen und nicht exzessiv Gebrauch gemacht werden. Ein umfassender und anlassloser Zugriff auf personenbezogene Daten kann daher durch Erwägungen zur nationalen Sicherheit in einer demokratischen Gesellschaft nicht gerechtfertigt werden. Auch bei Datenübermittlungen in die USA aufgrund von Standardverträgen muss der Datenimporteur zusichern, dass seines Wissens in seinem Land keine Rechtsvorschriften bestehen, die die Garantien aus den Klauseln in gravierender Weise beeinträchtigen. Eine solche Generalermächtigung scheint in den USA zu bestehen. Nur so lässt sich erklären, dass die NSA auf personenbezogene Daten, die aufgrund der Standardverträge übermittelt werden, mit hoher Wahrscheinlichkeit routinemäßig zugreift.

Bevor die Anforderungen nicht sichergestellt sind, beabsichtigen die deutschen Aufsichtsbehörden, keine neuen Genehmigungen für die Datenübermittlung in Drittstaaten beispielsweise auch zur Nutzung bestimmter Cloud-Dienste (webbasierte Dienste) zu erteilen und zu prüfen, ob solche Datenübermittlungen auf der Grundlage des Safe-Harbor-Abkommens und der Standardvertragsklauseln auszusetzen sind (siehe auch Ziffer 18.1 dieses Berichts).

Außerdem forderten die deutschen Aufsichtsbehörden die Europäische Kommission auf, ihre Entscheidungen zu Safe Harbor und zu den Standardvertragsklauseln vor dem Hintergrund der exzessiven Überwachungstätigkeit ausländischer Geheimdienste bis auf Weiteres zu suspendieren. Hierzu erklärte die Kommission, das Safe-Harbor-Abkommen bis Ende 2013 evaluieren zu wollen.

Zu diesem Thema tagte im September 2013 auch die für den internationalen Datenverkehr zuständige Untergruppe der Artikel-29-Datenschutzgruppe. Diese unabhängige Gruppe besteht aus je einer Vertreterin oder einem Vertreter der Kontrollstellen der Mitgliedsstaaten der Europäischen Union (EU) sowie der Kontrollstelle für die Einrichtungen der EU und trägt zu einer einheitlichen Anwendung der EU-Datenschutz-Richtlinie bei. Der Vorsitzende trug in einem Brief an die Vizepräsidentin der Europäischen Kommission im Wesentlichen die gleichen Anforderungen wie die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an die Bundesregierung vor.

Derzeit prüfen wir, ob Datenübermittlungen in die USA durch Unternehmen im Land Bremen auszusetzen sind.

Dazu haben wir zunächst entsprechende Auskünfte bei in Bremen ansässigen Unternehmen eingeholt. Insbesondere geht es darum, ob und welche personenbezogenen Daten an

Stellen in die USA übermittelt werden und nach welchen Ausnahmebestimmungen dieser Datentransfer erfolgt. Außerdem wollten wir wissen, welche technischen und organisatorischen Maßnahmen die Unternehmen in Bremen und die entsprechenden Stellen in den USA getroffen haben, um zu verhindern, dass Dritte unbefugt auf diese Daten zugreifen. Dies umfasste insbesondere auch die Auskunft darüber, ob und gegebenenfalls auf welche personenbezogenen Daten der US-amerikanische Geheimdienst zugreift beziehungsweise zugegriffen hat und, auf welchem technischen Wege und aus welchen Anlässen dies gegebenenfalls geschah oder geschieht. Ebenso baten wir um Auskunft, ob, inwieweit und welche Datenimporteure in den USA gegen nachrichtendienstliche Zugriffe gerichtlich oder in sonstiger Weise mit welchem Ergebnis vorgegangen sind.

Die erteilten Auskünfte haben uns veranlasst, weitere Auskünfte von den Unternehmen zu verlangen, bevor wir nach Gesprächen mit den Unternehmen abschließende Bewertungen und Entscheidungen treffen können.

18.3 Aktualisierung der Orientierungshilfe Cloud Computing aufgrund der Überwachung durch den US-amerikanischen Geheimdienst

Aufgrund der unter Ziffer 18.1 und 18.2 berichteten anlasslosen und flächendeckenden Überwachung durch den US-amerikanischen Geheimdienst beabsichtigen die Aufsichtsbehörden für den Datenschutz, ihre Orientierungshilfe zum Thema "Cloud Computing" zu überarbeiten. Insbesondere soll den Nutzerinnen und Nutzern geraten werden, keine webbasierten Datenverarbeitungsprogramme zu nutzen, deren Anbieter ihren Sitz in den Vereinigten Staaten von Amerika haben. Dies gilt auch für Anbieter, die sich darauf berufen, die Safe-Harbor-Grundsätze (siehe dazu Ziffer 18.2 dieses Berichts) zu beachten, oder die Auftragsdatenverarbeitung aufgrund eines Standardvertrages der Europäischen Kommission zur Datenverarbeitung in Drittstaaten durchführen. Drittstaaten sind nicht Mitgliedsstaaten der Europäischen Union oder nicht Vertragsstaaten über das Abkommen über den Europäischen Wirtschaftsraum. Ein weiterer wichtiger Baustein bei der Aktualisierung wird die Forderung nach einer Ende-zu-Ende-Verschlüsselung für die komplette Datenverarbeitung sein. Zum Redaktionsschluss berieten die zuständigen Arbeitskreise der Konferenz der Datenschutzbeauftragten des Bundes und der Länder noch. Die derzeitige Fassung der Orientierungshilfe mit Stand von September 2011 ist unter http://www.datenschutz.bremen.de/sixcms/media.php/13/oh_cloud.pdf abrufbar.

18.4 Arbeitsgruppe Internationaler Datenverkehr

Die Arbeitsgruppe Internationaler Datenverkehr beschäftigte sich hauptsächlich mit folgenden Themen:

- Befugnisse der Aufsichtsbehörden aufgrund der anlasslosen und flächendeckenden Überwachung durch den US-amerikanischen Geheimdienst,
- Kooperationsabsprachen des Bundesdatenschutzbeauftragten und der Landesdatenschutzbeauftragten mit ausländischen Stellen,
- verschiedene Anwendungsfälle zur Auftragsdatenverarbeitung durch Stellen außerhalb des Europäischen Wirtschaftsraums,
- Stand des europäischen Prüfverfahrens für ein amerikanisches Produkt im Cloud Computing,
- Fortschreibung der Orientierungshilfe "Cloud Computing" (siehe auch Ziffer 18.3 dieses Berichts).

19. Ordnungswidrigkeiten/Zwangsverfahren

19.1 Ordnungswidrigkeitsverfahren nach dem Bundesdatenschutzgesetz

In mehreren Fällen wurden von uns im Berichtsjahr erneut Ordnungswidrigkeitsverfahren eingeleitet und betrieben. Dabei wurden Geldbußen in Höhe von zusammen 12.500 Euro festgesetzt. Die Verfahren betrafen unterschiedliche Verstöße gegen das Bundesdatenschutzgesetz. Neben der Nichteinhaltung von Auskunftspflichten gegenüber den Betroffenen oder der Aufsichtsbehörde betrafen die Verstöße unter anderem die Nutzung von Daten für Zwecke der Werbung trotz Widerspruchs des Betroffenen durch ein Restaurant in Bremen. In einem anderen Fall, der die Nichtabgabe einer Mitteilung betraf, waren bei einer Filiale einer großen deutschen Supermarktkette in Bremerhaven Unterlagen abhanden gekommen, die neben Verkaufsdaten und der Unterschrift der Kundin oder des Kunden auch die Bankleitzahl, die Kontonummer sowie das Gültigkeitsdatum der ausgestellten Eurocheckkarte enthielten.

Ein Bußgeld in Höhe von 3.250 Euro wurde von uns wegen einer Vielzahl unzulässiger Abrufe bei einer Auskunftei, bei der das erforderliche und angegebene berechtigte Interesse nicht vorlag, festgesetzt. Gegen unseren Bußgeldbescheid wurde in diesem Fall Einspruch eingelegt, unseren Bescheid hielten wir jedoch aufrecht. Wir gaben den Fall daher an die Staatsanwaltschaft ab. Ein Termin vor dem zuständigen Amtsgericht ist in der Zwischenzeit anberaumt worden. Der Ausgang des Verfahrens bleibt abzuwarten.

19.2 Zwangsmittelverfahren

Auch im Berichtsjahr wurden in mehreren Fällen wieder Zwangsgelder angedroht und festgesetzt, um datenschutzrechtliche Verpflichtungen durchzusetzen. Die Höhe der Zwangsgelder betrug hierbei bis zu 3.000 Euro. Erneut ging es insbesondere um die Herbeiführung von Auskünften an die Aufsichtsbehörde, zu denen die datenschutzrechtlich Verantwortlichen gesetzlich verpflichtet sind. Aber auch die Herbeiführung von Löschungen und Meldungen und die Bestellung betrieblicher Datenschutzbeauftragter waren Gegenstand der Zwangsmittelverfahren.

Da die Androhung nicht zum beabsichtigten Erfolg führte, wurden in einem Fall mit mehreren Verfügungen Zwangsgelder in Höhe von zusammen 3.900 Euro festgesetzt, die allerdings noch nicht bezahlt sind. Um in diesem Fall den Beschuldigten zur Erfüllung seiner Pflichten zu veranlassen, haben wir ihn auch auf die Möglichkeit der Anordnung einer Erzwingungshaft hingewiesen. Eine Ersatzzwangshaft, die der Bestätigung durch das Verwaltungsgericht bedarf, kann von uns als zuständige Verwaltungsbehörde angeordnet werden, wenn die Beitreibung des Zwangsgeldes ohne Erfolg versucht worden ist oder feststeht, dass sie keinen Erfolg haben wird.

19.3 Unterlassene Information über abhandengekommene Einzugsermächtigungsbelege

Eines Morgens erreichte uns ein Anruf einer aufmerksamen Anwohnerin, die uns mitteilte, dass sie soeben im Hof ihres Hauses wie auf der vorbei führenden Straße eine Vielzahl von Einzugsermächtigungsbelegen eines Supermarktes mit Verkaufsdaten, eigenhändiger Unterschrift der Käuferinnen und Käufer sowie deren Bankleitzahl, Kontonummer und Gültigkeitsdatum der eingesetzten Eurocheckkarte entdeckt habe. Der Wind sei gerade dabei, diese Belege auf der Straße zu verteilen. Sie habe auch bereits dem betroffenen Supermarkt Bescheid gesagt. Wir konnten mithilfe der Polizei und eines weiteren sorgsamen Bürgers, der bereits etliche Belege eingesammelt und später bei einer Polizeidienststelle abgegeben hatte, einen Großteil der Belege sicherstellen und diese letztendlich dem erleichterten Verantwortlichen des betroffenen Marktes aushändigen. Dieser hatte nach Erhalt des Anrufs ebenfalls bereits umgehend Beschäftigte losgeschickt, um die verstreuten Belege einzusammeln. Eine mögliche Kenntnisnahme und gegebenenfalls missbräuchliche Verwendung der auf den Belegen aufgedruckten, unverschlüsselten Bankangaben nebst Unterschrift durch Dritte konnte zunächst jedoch nicht ausgeschlossen werden. Wie sich später herausstellte war es zu dieser Panne gekommen, weil versehentlich eine Tasche mit den Belegen im Warenlieferungsbereich des Marktes liegen geblieben und dort in der Folge durch Unbekannte entwendet worden war. Nachdem sich bei diesen wohl die Hoffnung auf

Geld oder sonstige Wertgegenstände zerstreut hatte, entsorgten sie die geöffnete Tasche im Hinterhof eines nahe gelegenen Hauses.

Obwohl eine im Jahre 2009 neu in das Bundesdatenschutzgesetz aufgenommene Vorschrift regelt, dass private Stellen, die mit personenbezogenen Daten verantwortlich arbeiten, es unter bestimmten näher festgelegten Voraussetzungen sowohl gegenüber der Aufsichtsbehörde als auch den Betroffenen melden und über ergriffene Sicherheitsmaßnahmen et cetera informieren müssen, wenn bei ihnen gespeicherte Daten abhanden gekommen sind, hatten wir seitens des Verantwortlichen des Marktes keine unverzügliche Information in der vorgeschriebenen Form erhalten. Auch die Kundinnen und Kunden des Marktes wurden in der Folge nicht, etwa durch einen Aushang im Markt, über diese Panne und die Notwendigkeit einer sorgsamen Kontrolle der Kontoauszüge im Hinblick auf etwaige unberechtigte Abbuchungen informiert.

Wir erließen daraufhin wegen Verstoßes gegen die gesetzliche Informationspflicht einen Bußgeldbescheid gegen den Verantwortlichen. Dieser akzeptierte die auferlegte Geldbuße.

19.4 Bußgeld für "Briefkastenfirma" wegen Nichtbeantwortung unseres Auskunftsersuchens

Bereits Ende des Jahres 2011 hatte eine Bürgerin eine postalische Mitteilung einer "RC Gloria Limited" über einen Preisgewinn aus einer angeblichen Preisrätselteilnahme erhalten. Das Unternehmen hatte im Briefkopf lediglich eine Postfachanschrift angegeben. Die Bürgerin, die an keinem Preisrätsel teilgenommen hatte, unter anderem jedoch gerne in Erfahrung bringen wollte, wie das Unternehmen an ihre Adresse gekommen war und an welche Stellen es diese weitergegeben hatte, schrieb an das Unternehmen und bat in Geltendmachung ihres Selbstauskunftsanspruchs um Erteilung einer entsprechenden Auskunft. Als das Unternehmen nicht antwortete, wandte sie sich an uns mit der Bitte um Hilfe bei der Durchsetzung ihres datenschutzrechtlichen Auskunftsanspruchs. Nachdem wir eine Geschäftsanschrift ermittelt hatten, ersuchten wir das Unternehmen beziehungsweise seine Leitung in Ausübung unseres gesetzlichen Auskunftsrechts mit zugestelltem Schriftstück um Beantwortung mehrerer Fragen. Wir erhielten keine Auskunft. Auch Erinnerungen blieben unbeantwortet.

Bei Überprüfung der Geschäftsanschrift unter Mitwirkung des Gewerbeaußendienstes stellten wir fest, dass an der vermeintlichen Geschäftsanschrift lediglich noch ein Briefkasten vorhanden war, Geschäftsräumlichkeiten oder gar handelnde Personen jedoch nicht. Die Deutsche Post AG "schloss" aufgrund unserer Informationen das Postfach. Unsere Überprüfung des nationalen Handelsregisters wie auch ausländischer Register für Handelsunternehmen hatte zwischenzeitlich ergeben, dass es sich bei der

"RC Gloria Limited" um eine Fantasiefirma handelte, kein Unternehmen hier als verantwortlich handelnd ausfindig zu machen war.

Wir leiteten in der Folge ein Bußgeldverfahren gegen Unbekannt wegen Verletzung unseres gesetzlichen Auskunftsrechts ein. Es gelang uns schließlich unter Einholung diverser Auskünfte und Zeugenvernehmung, eine Person zu ermitteln, bei der die gesamte Indizienlage dafür sprach, dass sie für die Gewinnschreiben unter dem Namen der Fantasiefirma verantwortlich war. Wir erließen daraufhin einen Bußgeldbescheid wegen Nichtbeantwortung unseres behördlichen Auskunftsersuchens, gegen den der Betroffene unter Hinweis darauf, dass er mit der Sache nichts zu tun habe, Einspruch einlegte. Da die vorgetragenen Einwände die vorliegenden Indizien unseres Erachtens nach nicht entkräfteten, halfen wir dem Einspruch nicht ab und legten die Bußgeldsache dem zuständigen Amtsgericht über die Staatsanwaltschaft zur Entscheidung vor. Kurz bevor der anberaumte Hauptverhandlungstermin stattfand, wurde der Einspruch zurückgenommen. Der Bußgeldbescheid ist damit rechtskräftig geworden.

19.5 Missachtung datenschutzrechtlicher Rechtspositionen durch Internetdienstleister

Bereits in unserem 33. Jahresbericht (siehe Ziffer 15.1) hatten wir über ein Internetunternehmen mit dubiosen Geschäftspraktiken berichtet, das als Premium Software GmbH firmierte. Dieses Unternehmen hatte in zahlreichen Fällen auch gegen das Recht Betroffener auf Auskunft zu gespeicherten personenbezogenen Daten verstoßen. Unsere Auskunftsersuchen gegenüber dem Unternehmen beziehungsweise seinen kurzfristig wechselnden Leitungspersonen, welche wohl als "Strohmänner" die Geschäfte für einen oder mehrere uns unbekannte „Hintermänner“ führten, blieben ebenfalls weitestgehend unbeantwortet. Da sich das Unternehmen und seine Leitungspersonen systematisch, beispielsweise durch Anschriftenwechsel, Führung bloßer Briefkastenanschriften und so weiter, allen Kontaktaufnahmeversuchen zu entziehen suchten, bereitete uns die Durchsetzung des Bundesdatenschutzgesetzes erhebliche Schwierigkeiten.

Uns war es schließlich jedoch gelungen, die Anschrift einer der formalen Leitungspersonen zu ermitteln und gegen diese ein Bußgeld wegen Verstoßes gegen unser gesetzliches Auskunftsrecht festzusetzen. Einen Nachfolger in der Unternehmensleitung hatten wir mit bestandskräftiger Anordnung verpflichtet, uns Auskunft darüber zu erteilen, woher Daten zu einer bestimmten Person bezogen worden seien. Da er die geforderte Auskunft in der Folge nicht erteilte, leiteten wir ein Zwangsvollstreckungsverfahren ein. Nachdem es uns schließlich auch insoweit wieder gelungen war, die neue Zustellanschrift zu ermitteln, setzten wir ein angedrohtes Zwangsgeld wegen Auskunftsverweigerung fest. Hiergegen wurde Klage

vor dem Verwaltungsgericht erhoben. Das Verwaltungsgericht wies in der Folge die Klage ab, sodass unsere Zwangsgeldfestsetzung bestandskräftig wurde.

Zwischenzeitlich war jedoch das Unternehmen aufgelöst und das Insolvenzverfahren über das Vermögen eröffnet worden. Im Zuge steuerrechtlicher wie strafrechtlicher Ermittlungen gegen Unternehmensverantwortliche waren Server beziehungsweise auch Festplatten mit Dateien des Unternehmens beschlagnahmt worden. Die ehemalige Leitungsperson hatte insoweit keine Kenntnisse mehr über den Verbleib der Kundendateien und konnte unser Auskunftsersuchen folglich tatsächlich nicht mehr beantworten. Eine Fortsetzung des Zwangsvollstreckungsverfahrens war insoweit sinnlos geworden. Wir sahen daher von der Einziehung des Zwangsgeldes ab.

Die unsererseits gegen das Unternehmen geführten Verfahren haben somit nach über zweieinhalb Jahren einen Abschluss gefunden. Wesentliche Fragen zum Umgang der Premium Software GmbH mit personenbezogenen Daten bleiben jedoch trotz unserer intensivsten Aufklärungsbemühungen leider unbeantwortet.

20. Verfahrensregister

20.1 Aktualisierung des Verfahrensregisters

Nach dem Bundesdatenschutzgesetz sind Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von nicht öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde zu melden. Handelt es sich um automatisierte Verfahren, in denen geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung gespeichert werden, sind diese ohne Ausnahme der zuständigen Aufsichtsbehörde zu melden. Zur Aktualisierung des Verfahrensregisters schrieben wir im Berichtsjahr zahlreiche Detekteien in Bremen und Bremerhaven an und baten diese, entweder eine Meldung der dort eingesetzten automatisierten Verfahren vorzunehmen oder uns unter Darlegung ihres Dienstleistungsangebots schriftlich mitzuteilen, warum sie glauben der Meldepflicht nicht zu unterliegen.

Die Antworten der Detekteien fielen sehr unterschiedlich aus. Während wir von einigen Stellen bereits auf unser erstes Anschreiben eine den gesetzlichen Anforderungen entsprechende Meldung erhielten, bedurfte es in anderen Fällen einem oder mehrerer Erinnerungsschreiben verbunden mit dem Hinweis, dass ordnungswidrig handelt, wer eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden. Wir stellten auch fest, dass einige Detekteien aufgrund der Besonderheit ihrer Tätigkeit keine personenbezogenen Daten speichern, sodass eine Meldung nicht erforderlich war. Bestanden Unklarheiten hinsichtlich der zu meldenden Angaben, so ließen sich diese in den betreffenden Fällen auf schriftliche oder mündliche Weise ausräumen.

Wir beabsichtigen, die Arbeiten zur Aktualisierung des Verfahrensregisters auch mit Schreiben an Unternehmen anderer Gewerbebereiche fortzusetzen.

21. Arbeitskreis Europa und Arbeitskreis Grundsatzfragen des Datenschutzes

Der Arbeitskreis Europa befasste sich mit dem Rechtsetzungsverfahren bei der Datenschutz-Grundverordnung und deren besonders aktuellen Schwerpunkten.

Der Arbeitskreis Grundsatzfragen des Datenschutzes erörterte die Anwendbarkeit deutschen Rechts auf ausländische Internetanbieter, Grundsatzfragen der Auftragsdatenverarbeitung, das Verhältnis der Datenschutzgesetze zum Kunsturhebergesetz sowie die Wirksamkeit der datenschutzrechtlichen Einwilligung bei der Verwendung elektronischer Unterschriftspads. Unterschriftspads sind Signaturtabletts beziehungsweise Geräte, mit denen eigenhändige Unterschriften elektronisch erfasst werden können.

22. Die Entschließungen der Datenschutzkonferenzen im Jahr 2013

22.1 Beschäftigtendatenschutz nicht abbauen, sondern stärken!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Januar 2013)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.
- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf

eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.

- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.
- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.
- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

22.2 Europa muss den Datenschutz stärken

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013)

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025[INI]) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden

sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.
- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufsgruppen und Unternehmensgruppen ist daher abzulehnen.
- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.
- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.
- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.
- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.
- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.
- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.
- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und

geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.

- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

Erläuterungen

zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13. und 14. März 2013 in Bremerhaven "Europa muss den Datenschutz stärken"

- Jedes personenbeziehbare Datum muss geschützt werden

Nach Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie zum Beispiel IP-Adressen, Kenn-Nummern, Standortdaten ein.

- Es darf keine grundrechtsfreien Räume geben

Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

- **Einwilligungen müssen ausdrücklich erteilt werden**

Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäischen Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es – auch mit Blick auf Artikel 8 Absatz 2 der Grundrechtecharta – nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

- **Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern**

Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch – in Anlehnung an Artikel 8 Absatz 2 der Grundrechtecharta – das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

- **Profilbildung muss beschränkt werden**

Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

- **Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte**

Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der

Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

- **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**

Ein kohärenter Datenschutz in der Europäischen Union (EU) setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

- **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**

Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Artikel 8 Absatz 3 der Grundrechtecharta und Artikel 16 Absatz 2 Satz 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

- **Grundrechtsschutz braucht effektive Kontrollen**

Die Sanktionen müssen – wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat – abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

- **Hoher Datenschutzstandard für ganz Europa**

Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die über den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG (Europäische Gemeinschaft) hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

22.3 Pseudonymisierung von Krebsregisterdaten verbessern

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013)

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden sogenannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor circa 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen beziehungsweise absehbar kommen sollen. Hierzu hat der Arbeitskreis "Technische und organisatorische Datenschutzfragen" der

Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungsgesetz und Krebsregistergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Absatz 3 BKRG festgelegt werden.

Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen

(Anlage zur Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder)

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

- Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.
- Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.
- Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.
- Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.

- Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.
- Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.

22.4 Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013)

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe "Soziale Netzwerke" erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plugins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

22.5 Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 13. und 14. März 2013)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

22.6 Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten unter anderem des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internetunternehmen und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den Vereinigten Staaten von Amerika (USA) stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es "zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss", "dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf". Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.
- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.
- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.
- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

- Dazu gehört,
    - zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der Europäischen Union (EU) erfolgen kann.
    - sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.
    - die Voraussetzungen für eine objektive Prüfung von Hardware und Software durch unabhängige Zertifizierungsstellen zu schaffen.
- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.
- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Artikel 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

22.7 Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013)

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt – wie repräsentative Studien belegen – mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiterzuentwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.[1]
- Angesichts der mit dem zunehmenden Wettbewerb im Sozialwesen und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privatsphäre und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.[2]
- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung zum Beispiel mit Hilfe von OSCI-Transport flächendeckend einsetzen.[3]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

22.8 Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht

[1] Siehe dazu die Entschließungen "Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" und "Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags".
[2] Siehe dazu die Entschließung "Stärkung des Datenschutzes im Sozial- und Gesundheitswesen".
[3] Siehe dazu die Entschließung "Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln".

praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlasslosen und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung "Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU-Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

22.9 Stärkung des Datenschutzes im Sozialwesen und Gesundheitswesen

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013)

Sozialdaten und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozialwesen und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozialwesen und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von "gläsernen Patientinnen und Patienten oder Versicherten" weiter verstärkt.

Der Wettbewerb im Sozialwesen und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privatsphäre und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.
- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

22.10 Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober 2013)

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung "Sicherheit bei E-Government durch Nutzung des Standards OSCI" Bund, Ländern und Kommunen empfohlen hat. Das sogenannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI-Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vorteile und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit

garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikationsendpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

23. Die Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich

23.1 Videoüberwachung in und an Taxis

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 26./27. Februar 2013)

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6 b Bundesdatenschutzgesetz (BDSG). Gemäß § 6 b Absatz 1 Nummer 3, Absatz 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines "stillen Alarms" oder eines GPS-gestützten Notrufsignals (GPS = Globales Positionsbestimmungssystem).

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (zum Beispiel über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6 b Absatz 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6 b Absatz 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potenzielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6 b Absatz 1, Absatz 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kraftfahrzeugkennzeichen, Aufschriften auf Fahrzeugen et cetera erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst

jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit "Unfallkameras", wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

23.2 Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

(Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 11./12. September 2013)

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (zum Beispiel §§ 28 und 32 Bundesdatenschutzgesetz [BDSG]) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Absatz 1 BDSG zulässig sein muss (vergleiche § 3 Absatz 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Absatz 1 Satz 1 Nummer 2 BDSG, bei sensitiven Daten ist § 28 Absatz 6 fortfolgende BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4 c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

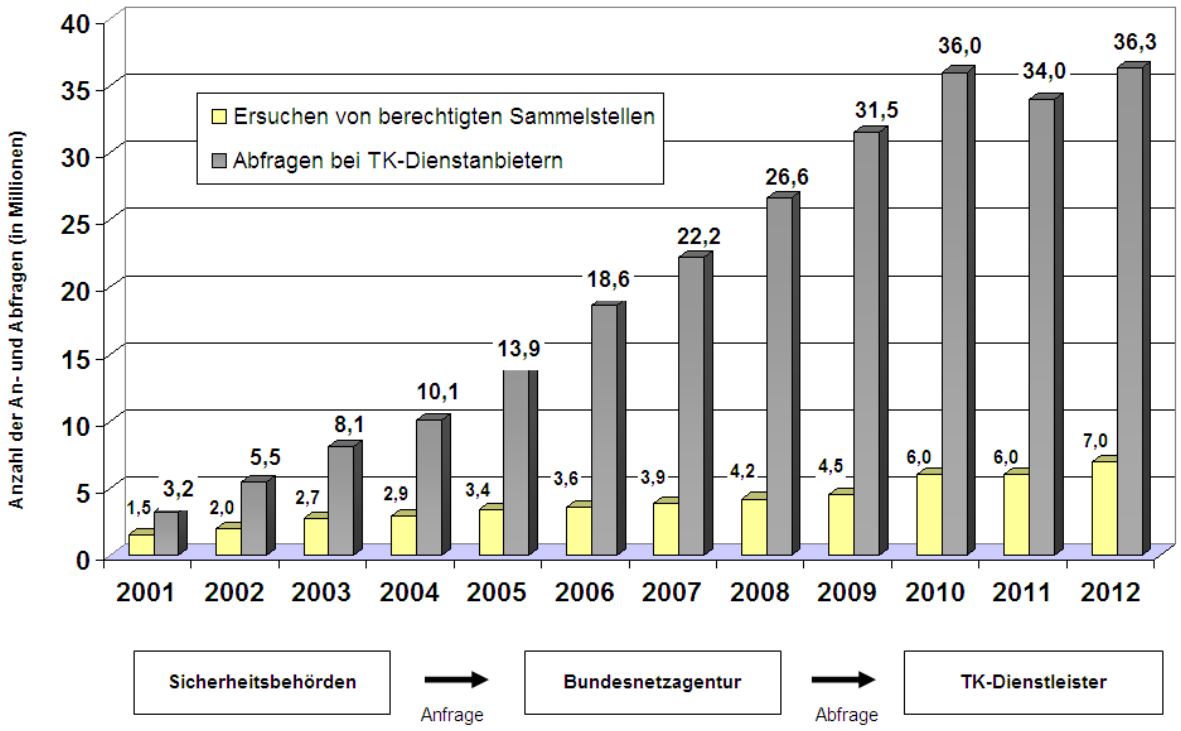
24. Die Europäische und die Internationale Datenschutzkonferenz

Die Entschließungen der Europäischen Datenschutzkonferenz im Jahr 2013 sowie Informationen zu den Entschließungen der Internationalen Datenschutzkonferenz stehen auf der Seite der Bundesbeauftragten für den Datenschutz und für die Informationsfreiheit unter http://www.bfdi.bund.de/DE/Entschliessungen/entschließungen_node.html zur Verfügung.

25. Anhang

25.1 Automatisiertes Auskunftsverfahren gemäß § 112 Telekommunikationsgesetz

Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Bundesnetzagentur von Telekommunikationsdiensteanbietern Auskünfte aus deren Kundendateien (Namen und Anschriften der Inhaber von Rufnummern). Derzeit erhalten etwa 200 berechtigte Stellen und mehrere tausend hieran angeschlossene Abfragestellen der Strafverfolgungsbehörden automatisiert entsprechende Bestandsdaten bei circa 140 Telekommunikationsdiensteanbietern. Die Anzahl der Abfragen ist im Vergleich zum Vorjahr leicht angestiegen.



Quelle: Jahresbericht 2012 der Bundesnetzagentur

25.2 Informationsmaterial

Informationen zu verschiedenen Bereichen können im Internet unter www.datenschutz.bremen.de abgerufen werden; hier können auch Formulare heruntergeladen werden.

25.3 Stichwortverzeichnis

A **Ziffer**

B

C

D

E