BREMISCHE BÜRGERSCHAFT **Drucksache 18/1521**
Landtag (zu Drs. 18/1320)
18. Wahlperiode 12.08.2014

Mitteilung des Senats vom 12. August 2014

Stellungnahme des Senats zum 36. Jahresbericht der Landesbeauftragten für Datenschutz

Mitteilung des Senats
an die Bremische Bürgerschaft (Landtag)
vom 12. August 2014

Stellungnahme des Senats zum 36. Jahresbericht der Landesbeauftragten für Datenschutz

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum „36. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit zum Datenschutz“ (Berichtszeitraum: 1. Januar bis 31. Dezember 2013) mit der Bitte um Kenntnisnahme.

Der Berichtszeitraum der Landesbeauftragten für Datenschutz und Informationsfreiheit war geprägt von dem politischen Großvorhaben auf europäischer Ebene, einheitliche rechtliche Regelungen für den Datenschutz zu schaffen. Das EU-Parlament hat sich auf einen Entwurf für eine europäische Datenschutzgrundverordnung verständigt. Der Senat der Freien Hansestadt Bremen begrüßt dies. Der immer häufiger werdende Datenklau durch Kriminelle, der sorglose Umgang von Konzernen mit den Daten ihrer Nutzerinnen und Nutzer und nicht zuletzt die illegalen oder zumindest zweifelhaften Aktivitäten der eigenen Geheimdienste erfordern ein starkes, aber eben auch länderübergreifend einheitliches Datenschutzrecht. Der Senat teilt die Einschätzung der Landesbeauftragten für Datenschutz und Informationsfreiheit, wonach die Stärkung des Datenschutzes auf nationaler, europäischer und internationaler Ebene unter anderem durch die Schaffung tragfähiger Regelungen erfolgen muss.

Der Senat hat daher im Rahmen einer Bundesratsinitiative im Mai 2014 die Bundesregierung aufgefordert, auf einen rechtzeitigen Eintritt des Rates der Europäischen Union in die Trilog-Verhandlungen mit dem Europäischen Parlament und der Europäischen Kommission hinzuwirken, damit die EU-Datenschutzgrundverordnung (KOM(2012) 11) in Verbindung mit der EU-Datenschutzrichtlinie (KOM(2012) 10) schnellstmöglich in Kraft treten kann. Dabei hat der Senat die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder formulierten Thesen für eine wirkungsvolle EU-Datenschutzreform aufgegriffen (BR-Drs. 123/3/14).

Die Sicherung der verfassungsrechtlich verbürgten informationellen Selbstbestimmung der Bürgerinnen und Bürger und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sind zentrale politische Anliegen des Senats. Der in den vergangenen Jahren erreichte hohe Datenschutzstandard im Land Bremen konnte auch im Berichtszeitraum gehalten werden, auch wenn es Einzelfälle gab, in denen die Landesbeauftragte berechtigte Kritik übte. Der Senat hat zur Lösung dieser Fälle in Abstimmung mit der Landesbeauftragten für Datenschutz und Informationsfreiheit

Maßnahmen zum Schutz personenbezogener Daten ergriffen und bekräftigt seine Absicht, dies auch künftig zu tun.

Zu den Einzelheiten des 36. Jahresberichts nimmt der Senat unter Bezugnahme auf die Nummerierung im Jahresbericht wie folgt Stellung:

3. Behördliche Beauftragte für den Datenschutz

3.2 Mangelnde Beteiligung des behördlichen Datenschutzbeauftragten

Im Bericht wird beanstandet, dass vor der Entscheidung über die Einführung des Verfahrens BAföG/Dialog 21, mit dem personenbezogene Daten verarbeitet werden, keine rechtzeitige Einbeziehung des behördlichen Datenschutzbeauftragten des Studentenwerks Bremen stattgefunden habe und die Aufnahme des Echtbetriebes des Verfahrens mit ihm nicht abgestimmt worden sei.

Diese Darstellung ist nach Auffassung des Studentenwerks nicht richtig.

Das Studentenwerk stand unter erheblichem Zeitdruck, die neu entwickelte Software BAföG/Dialog 21 einzuführen, weil die zuletzt verwandte Software mit dem - nach damaligen Sachstand - ab 1. Februar 2014 zu beachtenden SEPA-Verfahren nicht kompatibel gewesen wäre. Unabdingbar war sicherzustellen, dass die alljährlich etwa 11.000 gestellten BAFöG-Anträge rechtzeitig bearbeitet werden konnten. Der behördliche Datenschutzbeauftragte des Studentenwerks war bereits seit 2012 in die Vorbereitungen eingebunden und das erforderliche Datenschutzkonzept, mit dessen Erstellung eine Datenschutzfirma beauftragt wurde, wurde mehrfach in den damit zusammenhängenden Sitzungen mit ihm diskutiert.

Die Endversion des Datenschutzkonzeptes wurde schließlich am 10. Mai 2013 vorgelegt und ist mit dem behördlichen Datenschutzbeauftragten ausführlich und intensiv abgestimmt, wenngleich eine Abstimmung nicht bedeuten kann, dass eine "Genehmigung" vom behördlichen Datenschutzbeauftragten vorliegen oder sein Einverständnis eingeholt werden muss.

Damit wird konstatiert, dass der behördliche Datenschutzbeauftragte intensiv und rechtzeitig einbezogen wurde, wenngleich nicht in allen Fragen ein Konsens hergestellt werden konnte.

Durch die langwierigen Abstimmungsprozesse und die zahlreichen vorzunehmenden Veränderungen am Datenschutzkonzept erfolgte der Echtbetrieb vor der Fertigstellung des Datenschutzkonzeptes, um die Antragstellerinnen und Antragsteller zeitgerecht mit den ihnen zustehenden Leistungen nach dem BAföG versorgen zu können.

Die beanstandete Beeinträchtigung der Rechte des behördlichen Datenschutzbeauftragten kann insgesamt nicht nachvollzogen werden. Der Geschäftsführer des Studentenwerks wurde allerdings in einem persönlichen Gespräch durch den Abteilungsleiter 'Hochschulen und Forschung' der Senatorin für

Bildung und Wissenschaft auf die Pflicht hingewiesen, dass auf die Mängelrüge der Landesbeauftragten für Datenschutz und Informationsfreiheit eine Reaktion hätte erfolgen müssen.

4. Datenschutz durch Technikgestaltung und Technikbewertung

4.1 Flächendeckende Einführung des Dokumentenmanagementsystems VIS-Kompakt

Die Senatorin für Finanzen (SF) sieht durch die Vorlage des Rahmendatenschutzkonzeptes für VISkompakt, das der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) am 25.04.2014 übersandt wurde, die von der Landesbeauftragten für Datenschutz im Jahresbericht noch aufgeführten offenen Punkte als geklärt an.

Im Einzelnen:

Verschlüsselung

Die Senatorin für Finanzen hat Vorschläge für die Verschlüsselung der Inhaltsdaten und Metadaten vorgelegt. Die Transportverschlüsselung ist derzeit für den Mandanten der Senatorin für Soziales, Kinder, Jugend und Frauen im Produktivsystem umgesetzt. Für die übrigen Mandanten ist die Transportverschlüsselung in Vorbereitung.

Ein weiterer Workshop zur dokumentenbasierten Verschlüsselung hat unter Einbeziehung der Landesbeauftragten für Datenschutz im Mai 2014 stattgefunden. Die Verschlüsselung soll für die Landesbeauftragte für den Datenschutz auf der dort bereits eingesetzten Version VIS 5.1 umgesetzt werden. Diese Lösung soll dann Grundlage sein für weitere Dienststellen, die für ihren Bereich den Schutzbedarf „hoch“ festgestellt haben. Der Einsatz ist nach der Migration auf die Version 5.1, (aktuelle Version für die Freie Hansestadt Bremen ist die Version 4.8, geplanter Updatetermin auf die Version 5.1 ist Oktober/November 2014) vorgesehen.

Protokollierung

Mit dem Umzug in das neue Rechenzentrum RZ^2 wird die Administrationsplattform in Betrieb genommen (s. u., Ziffer 4.3). Die Transition in RZ^2 ist mit der Migration auf die Version 5.1 für Oktober/November 2014 geplant.

Durch Fach- oder Systemadministratoren vorgenommene Änderungen an Ablagerechten werden von VIS protokolliert und abgelegt. Die Senatorin für Finanzen hat Dataport angewiesen, die Protokollierung immer einzuschalten. Die Senatorin für Finanzen geht deshalb von der Vollständigkeit der Protokollierung auf Ebene der zentralen und dezentralen Fachadministration aus. Eines Beweises dafür bedarf es nach ihrer Ansicht nicht, da das System durch die Anstalt öffentlichen

Rechts Dataport betrieben wird und deshalb von einer auftragsgemäßen Verarbeitung auszugehen ist. Diese Logfiles wären theoretisch durch Systemadministratoren veränderbar/manipulierbar (jedoch nicht durch den Fachadministrator). Alle Tätigkeiten des Systemadministrators werden allerdings zukünftig durch die Administrationsplattform protokolliert. Die Protokollierung erfolgt nach verantwortlichen Stellen getrennt.

Mandantentrennung

Die Senatorin für Finanzen ist der Ansicht, dass durch die technischen Maßnahmen zur Einrichtung von Mandanten und Ablagen sowie durch die organisatorischen Maßnahmen zur Umsetzung des Rechte- und Rollenkonzeptes, wie im aktuellen Datenschutzkonzept von April 2014 beschrieben, die Anforderungen des § 7 Absatz 4 Nummer 8 Bremisches Datenschutzgesetz (BremDSG) erfüllt werden. Insofern besteht hier ein Dissens zur Auffassung der Landesbeauftragten für den Datenschutz.

Geschäftsgänge

Die von der Landesbeauftragten für den Datenschutz geäußerten Bedenken hinsichtlich der Erteilung von Geschäftsgängen mit einer damit verbundenen dauerhaften Rechteerweiterung teilt die Senatorin für Finanzen. VISkompakt wird daher (in der Version 5.1) die Rechteerweiterung nach Erledigung des Geschäftsganges rückgängig machen. Der Hersteller PDV hat zugesagt, die für die Version 5.2 eingeplante Funktionalität per Hotfix auch für die Version 5.1 für die Freie Hansestadt Bremen zur Verfügung zu stellen.

Zentrale Registraturen und Scan-Stellen

Sofern eine Einführung geplant ist, sind entsprechende Bedenken bzgl. der dafür notwendigen umfangreichen Berechtigungen zu berücksichtigen und entsprechende technische und organisatorische Regelungen zu treffen. Die Senatorin für Finanzen hält diese für mach- und zumutbar und damit angemessen. Zentrale Registraturen und Scan-Stellen können einen Beitrag zur Effizienzsteigerung des Verwaltungshandelns leisten.

Löschen von Daten

Da das Schriftgut in der Akte revisionssicher abgelegt werden soll, ist das Löschen von Schriftgutobjekten grundsätzlich nicht möglich, sondern erfolgt ausschließlich durch die Löschadministration, die bei der VIS-Administration verortet ist. Das Löschen von Dateien und Objekten erfolgt im Einzelfall über einen Geschäftsgang.

Für die Standardprozesse soll die Setzung von Lösch- und Aufbewahrungsfristen zukünftig zusätzlich durch ein Konzept Aussonderung, Vernichtung, Archivierung geregelt werden. Das Konzept mit den für Bremen geltenden Standardprozessen liegt im Entwurf vor.

Elektronische Handakte

Bei der E-Handakte wird eine Akte oder Teile einer Akte in ein pdf-Dokument exportiert. Eine Erweiterung der Rechte findet entsprechend dem Datenschutzkonzept vom April 2014 nicht statt.

4.2 Anforderungen an den Betrieb von SAP

Das Projekt zur Reorganisation zur Berechtigungen im SAP-Produktivsystem (ReBE) steht kurz vor dem Abschluss der Konzeptphase. Mit der Umsetzung von ersten Teilergebnissen des noch in Arbeit befindlichen Berechtigungskonzeptes wurde bereits in 2013 begonnen. Die restlichen Umsetzungsarbeiten werden mit Unterstützung durch Dataport bis Jahresende 2014 abgeschlossen werden können.

Die Fach- und Integrationstest erfolgen im Qualitätssicherungssystem mit einem kopierten Datenbestand aus dem Produktivsystem, um realistische und übertragbare Ergebnisse zu erhalten. Diese Vorgehensweise wurde im gültigen SAP-Betreiberkonzept für das Qualitätsmanagement festgelegt und im SAP-Einführungsprojekt CHIPSMOBIL mitbestimmt. Die Datensicherheit wird für die Testphase über besondere Einstellung in den Berechtigungen des SAP-Systems gewährleistet. Um aus heutiger Sicht der nachvollziehbaren Forderung der Landesbeauftragten für Datenschutz nach Anonymisierung bzw. Pseudonymisierung von zukünftigen Testdaten gerecht zu werden, wird ab Mitte 2014 die Einführung eines SAP-Tools für diese Zwecke geprüft.

Im Projekt zur Nutzung des Ticketmanagements im SAP-Solution Managers (TiMa-SAP) wurde die gesamte Projektdokumentation überarbeitet, aktualisiert und sowohl dem behördlichen Datenschutzbeauftragten als auch der Landesbeauftragten für Datenschutz zur Bewertung zur Verfügung gestellt.

4.3 Sichere Administrationsumgebung Dataport

Der Bitte der Landesbeauftragten für Datenschutz, prüffähige Unterlagen vorzulegen, wurde zwischenzeitlich nachgekommen. Die umfangreichen Unterlagen hat Dataport der Senatorin für Finanzen am 18. März 2014 vorgelegt und diese wurden von der Senatorin für Finanzen der Landesbeauftragten für Datenschutz am 30. April 2014 vorgestellt. Für die Fachverfahren im Rechenzentrum und die anderen dort betriebenen Basisdienste gibt es aus Sicht der Senatorin für Finanzen ein ausreichendes Konzept. Für die Administrationsplattform des neuen Rechenzentrums kann Dataport den Schutzbedarf „hoch“ abdecken und dies auch nachweisen.

Für den Endgerätebetrieb (also vor allem die PC) bei BASIS.bremen im Bremer Verwaltungsnetz (BVN) betreibt Dataport eine gesonderte Administrationsplattform, die aus der bestehenden Plattform weiterentwickelt worden ist. Diese Plattform ist

daher Grundlage für die Umsetzung der Anforderungen der Dienstvereinbarung zur Fernwartung bei BASIS.bremen durch Dataport.

Das bisherige Konzept ist bereits in einigen Punkten angepasst worden, lässt aus Sicht der Senatorin für Finanzen aber noch Antworten zur konkreten Realisierung in einigen wesentlichen Punkten vermissen, dazu gehört vor allem die Möglichkeit administrative Vorgänge bei Dataport „Videoprotokollieren“ zu lassen, d.h. den Ablauf am Bildschirm des Administrators festzuhalten. Die Senatorin für Finanzen hat mit der Landesbeauftragten für Datenschutz vereinbart, ihr eine Verfahrensbeschreibung vorzulegen, sobald von Dataport die notwendigen Informationen dafür vorgelegt worden sind. Die Senatorin für Finanzen hat Dataport die Bedeutung dieser Anforderungen deutlich gemacht.

4.5 Rahmendatenschutzkonzept BASIS.Bremen

Anders als die Landesbeauftragte für Datenschutz sieht die Senatorin für Finanzen in dem im September 2013 vorgelegten Rahmendatenschutzkonzept eine geeignete Grundlage für die Prüfung der durch BASIS.bremen erreichten Sicherheitsgewinne auch aus datenschutzrechtlicher Sicht. Wie von der Landesbeauftragten für Datenschutz beschrieben ist eine weitere Konkretisierung und Ergänzung dieser Grundlage sinnvoll.

Die Senatorin für Finanzen erarbeitet zurzeit die notwendigen Unterlagen, um die neun grundsätzlichen, im 36. Jahresbericht der Landesbeauftragten für Datenschutz genannten Anforderungen zu erfüllen. An diesem Prozess ist die Landesbeauftragte für Datenschutz beteiligt. Die Senatorin für Finanzen geht inzwischen davon aus, dass die Anforderungen erfüllt werden können, wenn entsprechende Vereinbarungen jeweils zwischen den verantwortlichen Stellen, Dataport und der Senatorin für Finanzen getroffen werden. Entsprechende Entwürfe für solche Vereinbarungen werden zurzeit von der Senatorin für Finanzen erstellt.

4.6 Länderübergreifendes Active Directory

Die Trägerländer von Dataport haben über ihren Kooperationstag ihren zuständigen Stellen den Auftrag erteilt, das Thema „Länderübergreifendes Active Directory“ auf der Basis eines Multidomänenmodells in Weiterentwicklung des Status Quo weiterzubearbeiten. In der vorhergehenden Phase waren die grundlegenden Modelle grundsätzlich bewertet worden.

Die Landesbeauftragte für Datenschutz erwartet die Beteiligung an dem Vorhaben und geht davon aus, dass das Vorhaben keine ausreichende Rechtsgrundlage hat.

Zielstellung der AG ist in der jetzigen Phase die Beschreibung der technischen Basis des Ziels „Multidomänenmodell“ und die Definition von Prozessen zur Steuerung und Entwicklung dieser Infrastruktur.

Zurzeit bestehen in den Ländern unterschiedliche Rahmenbedingungen für ein derartiges Vorhaben.

Die rechtliche und auch technische Situation in Bezug auf die Umsetzung dieses Vorhabens in der FHB wird die Senatorin für Finanzen mit der Landesbeauftragten für Datenschutz erörtern, sobald sich weitere Einzelheiten abzeichnen. Bis dahin wird sie sie anhand der Protokolle über den Stand der Arbeiten auf dem Laufenden halten.

5. Inneres

5.1 Telekommunikationsüberwachung durch die Polizeien

Durch aktuelle Nachfrage beim Landeskriminalamt (LKA) Niedersachsen lässt sich festhalten, dass die Unterlagen zum „Datenschutzkonzept für die Telekommunikationsüberwachung in verschiedenen Kooperationsstufen mit dem LKA Niedersachsen“ in der abschließenden Version von dort erst dann vorgelegt werden können, wenn durch das beauftragte Unternehmen das endgültige Update zur TKÜ-Software/-Anlage aufgespielt und vom LKA Niedersachsen abgenommen wurde. Durch das Dezernat 23 der Polizei Niedersachsen wurde mehrfach schlüssig dargestellt, dass eine Weiterführung von Entwurfsfassungen aus dortiger Sicht keinen Sinn macht und erhebliche Personalressourcen binden würde. Darüber hinaus ist eine Betrachtung von sich ständig in einer Aktualisierung befindlichen Dateiversion durch die Landesbeauftragte für Datenschutz und Informationsfreiheit keine zielführende Maßnahme zur Beurteilung der tatsächlichen Anlagenkonfiguration.

Das LKA Niedersachsen rechnet im Sommer 2014 mit der Installation der abschließenden Version durch das beauftragte Unternehmen. Voraussichtlich Ende 2014 können die entsprechenden aktualisierten Unterlagen für den Betrieb der Anlage sodann der bremischen Landesbeauftragten sowie dem niedersächsischen Landesbeauftragten für Datenschutz vorgelegt werden.

Bezüglich der Unterzeichnung des Verwaltungsabkommens hat es ebenfalls erhebliche Verzögerungen gegeben. Aus Sicht Bremens liegt eine unterschriftsfähige Version des Abkommens vor, die Abstimmung in Niedersachsen verzögert sich allerdings. Zurzeit befindet sich die aktuelle Version des Abkommens zur Prüfung beim niedersächsischen Landesbeauftragten für Datenschutz.

Einem von der Landesbeauftragten für Datenschutz im 36. Jahresdatenschutzbericht angesprochener inhaltlicher Dissens zu Teilen des Verwaltungsabkommens kann nicht abgeholfen werden, da ein Zuwarten auf die endgültige Konfiguration der TKÜ-Anlage beim LKA Niedersachsen einen weiteren erheblichen Zeitverzug bedeuten würde.

5.2 Einführung eines Terminmanagements

Die Einführung des Terminmanagement erfolgt als Pilot im Bereich der Zulassungsstelle des Stadtamtes. Im Piloten erfolgen die technischen Anpassungen

an die Rahmenbedingungen in Bremen. Hierzu zählen auch die Anforderungen des Datenschutzes. Daher wird die Einführung begleitet durch die Firma datenschutz nord GmbH, welche das Datenschutzkonzept des Stadtamts für das Online-Terminmanagementsystem sowie das Aufrufsystem erstellt.

5.3 Speicherung personenbezogener Daten bei der Polizei

Bezüglich der Speicherung polizeilicher Einträge werden die Vorgaben des Bremischen Polizeigesetzes in Verbindung mit den Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen eingehalten. Diese Bestimmungen sehen eine Aufbewahrung von Daten – auch über mehrere Jahre – vor. Dies ist zur Wahrnehmung polizeilicher Aufgaben insbesondere erforderlich, um den Fortgang krimineller Tätigkeit in die polizeilichen Betrachtungen einzubeziehen. Das Gesetz sieht die Möglichkeit einer einzelfallbezogenen, vorzeitigen Löschung polizeilicher Daten ausdrücklich vor. Im Rahmen einer Einzelfallprüfung werden bestehende Beurteilungsspielräume häufig zu Gunsten der Antragstellerin des Antragstellers genutzt.

Bei der Einführung neuer Verfahren werden datenschutzrechtliche Vorgaben bei der Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen eine große Bedeutung beigemessen. Eine rechtzeitige Umsetzung der Anforderungen ist auch im Interesse der Polizei Bremen.

5.4 Erweiterung der Anwendung INPOL und INPOL-Land

Im Jahr 2013 wurde im Rahmen eines Projektes bei der Polizei Bremen die Nutzung bzw. Erweiterung der in der INPOL-Land Software integrierten „Lokalen Fahndung“, die sog. „C-Gruppe“, erarbeitet. Ziel war es, diese Datei nicht nur für landesweite Fahndungen zu nutzen, sondern auch zur Abbildung von verfügten Auflagen und Weisungen zu Personen. Im Rahmen der Projektarbeit wurde festgestellt, dass für INPOL-Land Bremen bis zu diesem Zeitpunkt keine gültige Verfahrensbeschreibung vorlag. Aufgrund dessen wurde der Projektauftrag um diese Aufgabe erweitert. Die Umsetzung erfolgte im regelmäßigen Austausch mit der Landesbeauftragten für Datenschutz und Informationsfreiheit. Mit Abschluss der Projektarbeit wurde seitens der Landesbeauftragten keine Einwände zur Inbetriebnahme bzw. Erweiterung der „Lokalen Fahndung“ erhoben. Gleichwohl wurden die im 36. Jahresdatenschutzbericht dargelegten Forderungen an die Polizei hinsichtlich des Betriebes und der Datensicherheit formuliert. Innerhalb der Projektarbeit wurde stets darauf hingewiesen, dass durch personelle Engpässe bei der Polizei Bremen diese Forderungen nicht unmittelbar erfüllt werden können.

Offene Forderungen waren die Schutzbedarfsfeststellung, die Benutzerkonzeption sowie der Pflichtfeld – Abfragegrund.

Schutzbedarfsfeststellung

Durch Staatsvertrag ist geregelt, dass u. a. polizeiliche Anwendungen grundsätzlich beim Unternehmen Dataport betrieben werden müssen. Diesbezüglich wird derzeit über weitere Auslagerung von zurzeit betriebenen Systemen diskutiert (PIER/rsCase). Gleichzeitig beabsichtigt Dataport im Rahmen eines Umzuges/Neubaus ein gemeinsames zentrales Rechenzentrum für die vertraglich beteiligten Länder einzurichten. Es ist also davon auszugehen, dass in Kürze ein gemeinsamer Standard, insbesondere für den Sicherheitsaspekt, erreicht werden wird. Hierzu haben bereits erste Gespräche zwischen den Polizeien und Dataport stattgefunden. Gleichzeitig ist festzustellen, dass die Software INPOL-Land Bremen als identisches Produkt wie bei den Dataport-Vertragspartnern der Landespolizeien Hamburg und Schleswig-Holstein, genutzt wird. Eine andere Einschätzung des Schutzbedarfes wie bei den o. g. Landespolizeien ist deshalb grundsätzlich auszuschließen. Nach Abwägung der für die Polizei Bremen bestehenden Auswirkungen einer Zentralisierung wird die Schutzbedarfsfeststellung für INPOL-Land Bremen in zeitlicher Abhängigkeit umgesetzt werden. Eine planbare Einschätzung kann deshalb von hieraus nicht gegeben werden.

Benutzerkonzeption

Eine personelle Unterstützung im K 13 (Zentrale Berechtigungen) ist erfolgt. Die Umsetzung eines Benutzerkonzeptes wird derzeit vorgenommen. Eine in zeitlicher Hinsicht verbindliche Planung kann aufgrund des hohen manuellen Aufwandes derzeit nicht vorgenommen werden. Gleichzeitig befindet sich die zuständige Mitarbeiterin noch in der Einarbeitungszeit.

Pflichtfeld-Abfragegrund

Eine Stellungnahme zur Nichtumsetzung der verpflichtenden Angabe eines Abfragegrundes aus polizeilichen Informationssystemen ist noch nicht erfolgt. Ein Grund dafür ist, dass zuerst die Einführung von @rtus und das Kennenlernen der damit verbundenen Philosophien abgewartet werden musste. Es wird insoweit auf das Schreiben des Polizeivizepräsidenten an die Landesbeauftragte für Datenschutz und Informationsfreiheit vom 25. Oktober 2012 verwiesen.
Insbesondere konnte festgestellt werden, dass bei der Anlage von Personen aus @rtus grundsätzlich eine INPOL-Abfrage erfolgen muss. Dies ist erforderlich, um die Eindeutigkeit und Zuordnung einer Person herstellen zu können. Bei dieser Abfrage besteht ebenfalls keine Verpflichtung zur Angabe eines Abfragegrundes. Nach derzeitiger Einschätzung, würde dieser Automatismus den täglichen Arbeitsprozess auch erheblich einschränken.

Hinsichtlich der Forderung der Landesbeauftragten für Datenschutz und Informationsfreiheit ist deshalb ein Konsens beider Anwendungen/Zuständigkeiten zu finden, um der Umsetzung einer verpflichtenden Angabe eines Abfragegrundes weiterhin zu widersprechen.

5.5 Einführung des Vorgangsbearbeitungssystems @rtus

Die gesamten datenschutzrechtlichen Fragestellungen im Zusammenhang mit dem Vorgangsbearbeitungssystem-@rtus wurden bereits in der Projektphase im Rahmen eines Werkvertrages bearbeitet. Über diese Aufgabenzuweisung wurden der Landesbeauftragten für Datenschutz und Informationsfreiheit regelmäßig Unterlagen zur Verfügung gestellt. Aufgrund der noch offenen Aufgaben aus der Projektumsetzung bzw. der kritischen Anmerkungen der Landesbeauftragten wurde der Werkvertrag verlängert und um die Arbeiten im Zusammenhang mit der abschließenden Bearbeitung der offenen Punkte erweitert. Die offenen Fragestellungen werden zurzeit bearbeitet und die Landesbeauftragte für Datenschutz und Informationsfreiheit entsprechend beteiligt.

5.6 Aktuelle Situation im Stadtamt

Das Stadtamt befindet sich in einem umfangreichen Reorganisationsprozess. Hierbei ist auch die Bestellung einer oder eines Datenschutzbeauftragten bis Ende 2014 vorgesehen.

5.7 Neufassung des Bremischen Verfassungsschutzgesetzes

Die Landesbeauftragte für Datenschutz und Informationsfreiheit stellt fest, dass die Novellierung des Bremischen Verfassungsschutzgesetzes grundsätzlich datenschutzrechtliche Kernforderungen unterstützt. Gleichwohl bestehen seitens der Landesbeauftragten in folgenden Punkten noch Bedenken:

Trennungsgebot

Es wird kritisiert, dass die Eingliederung des Landesamtes für Verfassungsschutz als Abteilung beim Senator für Inneres und Sport dem Trennungsgebot nicht hinreichend Rechnung trage. Dies ist nach Auffassung des Senats unzutreffend. Die Eingliederung hat haushalts- und personalwirtschaftliche Bedeutung und verstärkt die demokratische Legitimation und Kontrolle durch die Aufgabe eines zwischengeschalteten Referats beim Senator für Inneres und Sport. Materiell-rechtlich bringt sie keine Veränderung. Nach wie vor werden Polizei und Verfassungsschutz in zwei getrennten Abteilungen der senatorischen Behörde geführt. Die Trennung des Verfassungsschutzes von der Polizeiorganisation stellt der Gesetzgeber weiterhin klar. Die neue Organisation entspricht vielmehr jener Struktur, die in der Mehrzahl der Länder bereits besteht. Vergleichend ist darauf hinzuweisen, dass beim Bundesministerium des Innern der Verfassungsschutz zwar als nachgeordnetes Amt, jedoch in der gleichen Abteilung mit dem Bundeskriminalamt organisatorisch eingeordnet ist.
Dem Vorschlag der Landesbeauftragten für Datenschutz und Informationsfreiheit, in das Gesetz einen Satz zur von der Polizei getrennten Dateiführung beim Verfassungsschutz einzufügen, konnte nicht entsprochen werden. Der von ihr in der Stellungnahme zum Gesetzentwurf vorgeschlagene Satz war nicht verständlich. Unklar blieb etwa, was mit den Worten „sonstigen Datenträgern“ gemeint war. Im

Übrigen sind auch gemeinsame Dateien von mehreren Verfassungsschutzbehörden nach wie vor „eigene“ bzw. „eigenständige“ Dateien der beteiligten Behörden. Die nunmehr im 36. Jahresdatenschutzbericht vorgeschlagene und leicht veränderte Formulierung vermag weithin nicht zu überzeugen. Neben den bundesgesetzlich geregelten gemeinsamen Dateien von Polizei und Verfassungsschutz, wie der Anti-Terror-Datei (ATD) und der Rechtsextremismusdatei (RED), gibt es in Bremen keine gemeinsamen Dateien von Polizei und Verfassungsschutz. Dies folgt daraus, dass das Einstellen von Informationen in eine gemeinsame Datei immer eine Übermittlung an die anderen beteiligten Behörden bedeutet; es finden mithin die allgemeinen gesetzlichen Übermittlungsregelungen und -begrenzungen auf jede in die Datei eingestellte Information Anwendung. Ein entsprechendes Verbot ist somit nicht erforderlich.

Erhebungsbefugnis

Die Landesbeauftragte für Datenschutz und Informationsfreiheit hält für den Schutz des Kernbereichs privater Lebensgestaltung eine gesetzliche Ausnahme für Daten zu „Gesundheit“ und „Sexualleben“ für erforderlich. Ihr Fehlen entspreche nicht der verfassungsgerichtlichen Rechtsprechung zur Online-Durchsuchung.

Diese Rechtsauffassung übersieht jedoch, dass der „Kernbereich privater Lebensgestaltung“ nicht abstrakt anhand feststehender Begrifflichkeiten und losgelöst vom Kontext abstrakt bestimmt werden kann. Selbst die vielfach verbreitete unzutreffende Meinung, wonach in rechtlicher Hinsicht Überwachungsmaßnahmen im Schlafzimmer nicht erfolgen dürfen, trifft nach der verfassungsgerichtlichen Rechtsprechung nicht ausnahmslos zu. So wären zum Beispiel etwaige Planungen von terroristischen Anschlägen im Schlafzimmer einer Überwachung zugänglich. Die Merkmale „Sexualleben“ und „Gesundheit“ werden in der Regel für das Erkennen und die Abwehr von extremistischen Vorgängen keine Bedeutung haben und sind folglich für die Arbeit der Sicherheitsbehörden nicht erforderlich. Die Erhebung der entsprechenden Daten ist durch den Verfassungsschutz auch nicht zulässig. Diese Feststellung ergibt sich aber bereits aus dem geltenden Recht. Gleichwohl können solche Aspekte jedoch im Fall von Attentatsplänen Bedeutung erlangen. Beispielsweise ist denkbar, dass Hinweise eingehen, wonach eine Gesundheitsstörung für eine verminderte Sicherheitskontrolle am Flughafen genutzt werden soll. In einem solchen Fall wäre die Suche nach einer Person, die ein solches Problem hat, für die Sicherheitsbehörden von überragender Bedeutung. Gleiches gilt, falls ein Attentäter gesucht werden soll, der Zugang zu bestimmten sexuell orientierten Kreisen hat, um dort einen Anschlag möglichst erfolgreich begehen zu können. Aus diesen Gründen kann und darf die Art der zu erhebenden Daten nicht apodiktisch festgeschrieben werden.

5.8 Rahmendatenschutzkonzept der Polizei Bremen

Vor dem Hintergrund zahlreicher aktueller Aufgabenstellungen, auch im Zusammenhang mit der Einführung des VBS-@rtus, konnte das Rahmendatenschutzkonzept für die Polizei Bremen noch nicht fertig gestellt werden. Die personellen Rahmenbedingungen konnten inzwischen jedoch verbessert werden. Auch im Interesse der Polizei Bremen wird ein Rahmendatenschutzkonzept schnellstmöglich zur Verfügung gestellt.

5.9 Rahmendatenschutzkonzept des Senators für Inneres und Sport

Die Arbeiten am Rahmendatenschutzkonzept des Senators für Inneres und Sport werden nach dem Umzug des File –Servers zu Dataport und der Umsetzung des künftigen File-Konzeptes im Rahmen des Basis.bremen-Projektes fortgeführt. Dies wird voraussichtlich im dritten Quartal 2014 geschehen.

6. Justiz

6.1 Projekt "Forderungsmanagement in der Justiz"

Das Projekt „Forderungsmanagement in der Justiz“ ist zum 31. Dezember 2013 abgeschlossen worden. Der Einzug von Justizforderungen erfolgt zukünftig ausschließlich durch die Landeshauptkasse unter Begleitung durch eine regelmäßig tagende Arbeitsgruppe. Sofern dafür Veränderungen im Umgang mit personenbezogenen Daten erforderlich sind, soll dies in enger Abstimmung mit der Landesbeauftragten für Datenschutz geregelt werden.

6.2 Videoüberwachung in der Justizvollzugsanstalt

Der Senat ist der Auffassung, dass die im Bericht angesprochene Videoüberwachung ihre Rechtsgrundlage im Bremischen Untersuchungshaftvollzugsgesetz (BremUVollzG) findet. Nach § 46 Absatz 1 BremUVollzG ist die Überwachung des Anstaltsgebäudes, einschließlich des Gebäudeinneren, des Anstaltsgeländes und der unmittelbaren Umgebung der Anstalt mit optisch-elektronischen Einrichtungen (Videoüberwachung) zulässig, wenn dies für die Sicherheit oder Ordnung der Anstalt erforderlich ist. Nach § 46 Absatz 2 Satz 2 BremUVollzG darf die Videoüberwachung auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind. Ziel der Videoüberwachung ist der sichere und wirksame Vollzug der Untersuchungshaft, der wiederum der Sicherung der Strafverfahren dient. Die Verfolgung dieses Ziels kann im Rahmen der gebotenen Prüfung der Verhältnismäßigkeit auch die Betroffenheit einer größeren Zahl von Dritten rechtfertigen. In Bremen wird die Untersuchungshaft in unmittelbarer Nähe der Strafhaft vollzogen und teilt sich mit dieser ein gemeinsames Anstaltsgelände einschließlich des gemeinsamen Mauerbereiches. Das Sicherungsinteresse der Untersuchungshaft lässt sich dementsprechend räumlich nicht ausschließlich auf deren engeren Bereich begrenzen.

Der aktuelle Entwurf eines Bremischen Strafvollzugsgesetzes enthält darüber hinaus eine zusätzliche Rechtsgrundlage für die Videoüberwachung unmittelbar für Strafgefangene.

Die Videoüberwachung des Außenbereiches der Anstalt bezieht grundsätzlich nur die angrenzenden öffentlichen Flächen ein. Die Kameras sind bzw. werden so justiert, dass wohl öffentliche Flächen, bis auf unvermeidbare Ausnahmen jedoch keine Privatgrundstücke einbezogen werden. Die Nachbarn der JVA Bremen sind dazu in einem Anhörungstermin gehört worden und haben gegen dieses Vorgehen keine Einwände erhoben. Sie haben sich im Gegenteil überwiegend ausdrücklich mit einer Einbeziehung jedenfalls von Teilen ihrer Grundstücke einverstanden erklärt. § 46 Absatz 1 Satz 1 BremUVollzG lässt ausdrücklich auch die Beobachtung der unmittelbaren Umgebung der Anstalt zu. Soweit Privatgrundstücke betroffen sind, rechtfertigt das Gesetz die mit der Beobachtung verbundene Beeinträchtigung der Rechte Dritter, wenn Gründe der Sicherheit oder Ordnung diese Maßnahme erfordern. Entsprechendes gilt für die Mitarbeiterinnen und Mitarbeiter der JVA Bremen. Auch hier ist die JVA bemüht, die Erfassung durch die Videoüberwachung soweit wie möglich zu begrenzen. Dabei geht die JVA jedoch davon aus, dass ihre Mitarbeiterinnen und Mitarbeiter Beschränkungen ihrer Rechte, die zur sicheren Durchführung der Haft erforderlich sind, grundsätzlich akzeptieren.

An dem der Landesbeauftragten für Datenschutz und Informationsfreiheit im Entwurf bereits im letzten Jahr vorgelegten Datenschutzkonzept wird unter ihrer Beteiligung zügig weiter gearbeitet.

7. Gesundheit und Soziales

7.1 Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten

Die in § 27 Absatz 6 des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten geregelte Überwachung des Paketverkehrs soll dahingehend geändert werden, dass eine Kontrolle von Paketen auch von nicht ärztlichem Personal, das von der Einrichtungsleitung mit dieser Aufgabe betraut wird, vorgenommen werden kann. Die praktischen Erfahrungen in der Unterbringungs- und Maßregelvollzugseinrichtung zeigen, dass der zu leistende Kontrollaufwand die Kapazitäten des ärztlichen Personals in unverhältnismäßigem Umfang mit nicht ärztlichen Aufgaben bindet. Daher sollen die Kontrollen künftig auch von damit beauftragten Klinikmitarbeiterinnen und -mitarbeitern durchgeführt werden können.

Zudem soll die bereits bestehende Praxis aus Gründen der Rechtssicherheit in das Gesetz aufgenommen werden, wonach die Öffnung und die Einsichtnahme in die Pakete nach Möglichkeit im Beisein der Adressatin oder des Adressaten

durchzuführen ist. Darüber hinausgehende Änderungen der Paketkontrolle sind nicht vorgesehen.

7.3 Mitgliederwerbung einer Krankenkasse

Im Zusammenhang mit der Aktion „Mit dem Rad zur Arbeit“ zeigt die Landesbeauftragte für Datenschutz und Informationsfreiheit an, dass eine Krankenkasse nicht erforderliche personenbezogene Daten erhebt und diese zur Werbung von Mitgliedern nutzt. Die Erhebung des Geburtsdatums, der e-mail-Adresse und der Mobilfunknummer werden ausdrücklich als nicht erforderlich genannt. Zudem kritisiert die Landesbeauftragte für Datenschutz und Informationsfreiheit, dass hinsichtlich einer Veröffentlichung der Gewinnerinnen und Gewinner der Aktion deren Einwilligung vorliegen muss. Die hierzu vorgelegte Einwilligungserklärung ist nach Auffassung der Landesbeauftragten fehlerhaft.

Die Bedenken der Landesbeauftragten für Datenschutz und Informationsfreiheit werden vom Senator für Gesundheit nicht geteilt, sodass kein Anlass für etwaige aufsichtsrechtliche Maßnahmen gesehen wurde. Zudem dauerte die datenschutzrechtliche Abstimmung zwischen der Landesbeauftragten für Datenschutz und Informationsfreiheit und der Krankenkasse zum Zeitpunkt der Veröffentlichung des Tätigkeitsberichts noch an.

Die Befugnis der Krankenkassen, zur Gewinnung von Mitgliedern Daten zu erheben, zu verarbeiten und zu nutzen, wenn sie allgemein zugänglich sind, ist in § 284 Abs. 4 des Fünften Buches Sozialgesetzbuch (SGB V) ausdrücklich geregelt. Eine Grenze findet die Befugnis dort, wo das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein Abgleich der erhobenen Daten mit den Angaben nach § 291 Abs. 2 Nr. 2 (Name und Vorname), 3 (Geburtsdatum), 4 (Geschlecht) und 5 (Anschrift) SGB V ist zulässig. Die Daten sind zu löschen, wenn sie für die Mitgliedergewinnung nicht mehr benötigt werden. Die Nutzung oder Übermittlung ist unzulässig, wenn die Betroffenen widersprechen.

Die Durchführung von Gewinnspielen zur Datengewinnung ist ein übliches Verfahren. Seitdem die Krankenkassen durch Entscheidungen des Gesetzgebers im Wettbewerb um Mitglieder (untereinander und mit den privaten Versicherungsunternehmen) stehen, sind ihnen auch Maßnahmen zur Gewinnung von Daten potentieller Mitglieder erlaubt. Zudem muss die Durchführung eines Wettbewerbs als „allgemein zugängliche“ Datengewinnung im Sinne von § 284 Abs. 4 SGB V zu werten sein. Die Erhebung des Geburtsdatums ist insoweit als zulässig anzusehen, als der Abgleich mit den Daten bereits vorhandener Versicherter ebenfalls zugelassen ist.

Ausweislich der online-Anmeldung und der Teilnahmebedingungen für die Kampagne 2014 der Aktion „Mit dem Rad zur Arbeit“ werden die e-mail-Adresse und die Mobilfunknummer benötigt, um die online-Anmeldung von den Anmeldenden bestätigen zu lassen. Dazu erhalten sie nach ihrer Anmeldung per SMS einen

Bestätigungscode, den sie per e-mail zur Bestätigung ihrer Anmeldung an die Kasse zurücksenden müssen. Auch hierbei handelt es sich um ein etabliertes Verfahren.

In den Teilnahmebedingungen wird darauf hingewiesen, dass ein jederzeitiger Rücktritt von der Teilnahme möglich ist. Die erhobenen Daten werden in diesem Fall sofort gelöscht. Für den Fall der Veröffentlichung des Gewinnernamens hat die Krankenkasse bereits zugesagt, dass die Veröffentlichung erst nach einer ausdrücklichen Einwilligung erfolgen wird.

7.6 Fachverfahren Kindergarten Online

Die Tagesbetreuung sowohl für unter 3-jährige Kinder als auch für Kindergartenkinder wird vom öffentlichen Jugendhilfeträger in Zusammenarbeit mit verschiedenen Trägern von Tageseinrichtungen in Bremen gewährleistet. Neben den stadteigenen Kindergärten, die durch KiTa Bremen als Eigenbetrieb in öffentlicher Trägerschaft betrieben werden, leistet eine Vielzahl freier Träger auf Grund eigener Initiative einen erheblichen Beitrag zur Gewährleistung der erforderlichen Tagesbetreuung. Zu diesen freien Trägern gehören u.a. kirchliche Träger, bundesweit organisierte gemeinnützige Vereine sowie kleinere Träger – etwa Elternvereine.

Sowohl der öffentliche als auch fast alle freien Träger, setzen das Fachverfahren zur Verwaltung ihrer Einrichtungen ein und sind somit datenschutzrechtlich verantwortliche Stelle. Daher haben die Träger jeweils einen eigenständigen Vertrag mit dem Softwaredienstleister geschlossen. Es wurden insbesondere kleinere freie Träger, aber auch der öffentliche Träger bei der Einführung des Fachverfahrens unterstützt, u. a. weil das Fachverfahren dazu führt, dass einheitliche und belastbare Daten, z. B. über Anmeldungen, Belegungen und Auslastungen bereit gestellt werden können. Diese von den Trägern bereitzustellenden Daten sind die Basis, um eine bedarfsgerechte Tagesbetreuung planen und anbieten zu können.

Die im Tätigkeitsbericht vertretene Rechtsauffassung der Landesbeauftragten in Bezug auf das Vorliegen der dargestellten Garantenpflicht wird nicht geteilt.

Die Zusammenarbeit zwischen öffentlichen und freien Trägern ist in § 4 des Achten Buches Sozialgesetzbuch (SGB VIII) ausdrücklich geregelt. Hieraus folgt, dass die anerkannten freien Träger auch im Bereich der gesetzlich vorgeschriebenen Aufgaben der Jugendhilfe mindestens gleichberechtigt neben dem öffentlichen Träger eigene Einrichtungen, Dienste und Veranstaltungen betreiben können. Der öffentliche Träger hat dabei die Selbständigkeit der freien Träger auch in Bezug auf die Durchführung ihrer Aufgaben sowie in der Gestaltung ihrer Organisationsstruktur zu achten. Die Zusammenarbeit ist partnerschaftlich auszugestalten.

Die im 36. Jahresdatenschutzbericht vertretene Auffassung, wonach dem öffentlichen Träger eine datenschutzrechtliche Garantenpflicht hinsichtlich der autonomen Tätigkeit der freien Träger zukomme, die insbesondere auch die Zulässigkeitsvoraussetzungen der Einschaltung von externen Dienstleistern über das

Bundesdatenschutzgesetz und sonstige spezialgesetzlichen Regelungen hinaus verschärfe, trägt den einführend genannten und verfassungsrechtlich gebotenen Grundprinzipien der Zusammenarbeit zwischen öffentlichen und freien Trägern nicht genügend Rechnung:

Zum einen sieht die Landesbeauftragte für Datenschutz und Informationsfreiheit bereits in der partnerschaftlichen Zusammenarbeit der Träger auf dem Gebiet der Jugendhilfe eine Inanspruchnahme der freien Träger, welche dazu führe, dass dem öffentlichen Träger nach § 61 Abs. 3 SGB VIII eine Garantenpflicht zukomme. Eine solche Inanspruchnahme ist jedoch im Bereich der Tagesbetreuung nicht gegeben, da die freien Träger aufgrund eigener Initiative gleichberechtigt neben dem öffentlichen Träger eigene Einrichtungen betreiben.

Zum anderen fordert die Landesbeauftragte für Datenschutz und Informationsfreiheit in Annahme einer Garantenpflicht, dass der öffentliche Träger in die Tätigkeit der freien Träger einzugreifen habe und diese durch Verwaltungshandeln verpflichten müsse, sich den für öffentliche Träger geltenden, sozialdatenschutzrechtlichen Spezialvorschriften zu unterwerfen. In diesem Rahmen seien die freien Träger auch dazu zu verpflichten, die Einschaltung externer Dienstleister anhand der für den staatlichen Bereich geltenden Vorschrift des § 80 Abs. 5 des Zehnten Buches Sozialgesetzbuch (SGB X) auszurichten. In der Folge dürften freie Träger externe private Dienstleister nur beauftragen, wenn andernfalls entweder Störungen im Betriebsablauf auftreten können oder die Arbeiten beim Dienstleister erheblich kostengünstiger besorgt werden können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst, sondern der überwiegende Teil der Speicherung des gesamten Datenbestandes beim Träger verbleibt. Ein solch weitgehender Eingriff in die Trägerautonomie ist jedoch weder gesetzlich geboten, noch durch Rechtsgrundlage gedeckt.

Der Landesbeauftragten für Datenschutz und Informationsfreiheit wurde mitgeteilt, dass der Klärung der Rechtsfragen grundsätzliche Bedeutung zukommt. Insgesamt hätte die Kombination der weiten Auslegung des § 61 Abs. 3 SGB VIII bei gleichzeitiger sehr enger Auslegung des § 80 Abs. 5 SGB X nach Einschätzung der Senatorin für Soziales, Kinder, Jugend und Frauen bundesweit gravierende Auswirkung auf die Zusammenarbeit zwischen freien und öffentlichen Trägern. Dabei wären nicht nur die über 1.000 Kindergärten freier Träger betroffen, die das im Tätigkeitsbericht angesprochene Fachverfahren in vergleichbarer Form schon in unterschiedlichen Bundesländern einsetzen. Vielmehr ist insgesamt die Frage zu klären, ob und wenn ja, ab welchem Zeitpunkt öffentliche Träger wie stark in die Autonomie der freien Träger eingreifen dürfen bzw. müssen. Nicht nur im Interesse der Klärung des vorliegenden Falles, sondern mit dem Ziel einer einheitlichen Interpretation der Aufsichtsbehörden wurde gegenüber der Landesbeauftragten angeregt, die Auslegung des Anwendungsbereichs des § 61 Abs. 3 SGB VIII sowie die damit einhergehende Auslegung der wortgleichen Anwendbarkeit des § 80 Abs. 5 SGB X im Düsseldorfer Kreis abzustimmen.

Die im 36. Jahresdatenschutzbericht erwähnte Erhebung personenbezogener Daten wurde mit Ausnahme der Staatsangehörigkeit der Eltern zu keiner Zeit verpflichtend abgefragt. Die Software enthielt lediglich entsprechende Felder, die aber nicht genutzt wurden (Detaildaten zu abholberechtigten Personen) bzw. auf freiwilliger Basis (Hausarzt des Kindes) angeboten worden sind. Bereits das entworfene Musterdatenschutzkonzept für die Träger traf entsprechende Feststellungen und sollte die Nutzerinnen und Nutzer des Verfahrens sensibilisieren, die entsprechenden Daten nicht bzw. nur dann zu erheben, wenn die Eltern auf die Freiwilligkeit hingewiesen wurden und deren Zustimmung vorlag. Es wird jedoch der Ansicht zugestimmt, dass eine technische Sperrung bzw. Löschung der nicht erforderlichen Datenfelder im Fachverfahren eine wirksamere Maßnahme darstellt, als auf die organisatorischen Maßnahmen zu vertrauen, die eine Befüllung der Datenfelder verhindern soll. Derzeit wird eine entsprechende Änderung der Datenfelder im Anwenderbeirat des Fachverfahrens, in welchem sowohl der öffentliche Träger als auch die freien Träger vertreten sind, abgestimmt. Dabei werden alle Datenfelder – nicht nur die Staatsangehörigkeiten der Eltern – auf deren rechtliche Grundlage und Notwendigkeit geprüft. Der Softwarehersteller wird dann entsprechend beauftragt, die nicht notwendigen, bzw. rechtlich nicht zulässigen Datenfelder aus dem Programm zu entfernen.

Hinsichtlich der technischen und organisatorischen Maßnahmen gilt Folgendes:

Das Fachverfahren wurde vor seinem Einsatz sowohl rechtlich als auch technisch bewertet und zudem ein Penetrationstest auf ein Testsystem durchgeführt, um etwaige Mängel am Schutz der Webanwendung vor Inbetriebnahme entdecken und ggf. abstellen zu können. Es wurde zusätzlich darauf bestanden, dass die beteiligten IT-Dienstleister über Zertifizierungen – etwa ISO 27001 – verfügen. Bezüglich der Einrichtungen von KiTa Bremen wurde zudem bereits im Jahr 2012 eine echte Zwei-Faktor-Authentisierung eingeführt. Eine Anmeldung ist nur aus zugriffsberechtigten IP-Adresskreisen unter Angabe von Benutzername und Kennwort sowie nach Prüfung eines Maschinenzertifikats möglich. Hinsichtlich der Einrichtungen der freien Träger ist neben Benutzername und Kennwort zudem die Freischaltung der verwendeten Clients für das Fachverfahren erforderlich. Das Fachverfahren bietet darüber hinaus die Möglichkeit, den Besitz einer Hardware-Komponente als zusätzliche Voraussetzung der Authentisierung abzufragen. Den freien Trägern, die diese Möglichkeit noch nicht nutzen, wurde diese erneut aufgezeigt. Im Hinblick auf die Sicherheit der Passwortverschlüsselung hat der Softwarehersteller das verwendete Hash-Verfahren mit einem im Mai 2014 durchgeführten Release durch eine zeitgemäße Hashfunktion zu ersetzt.

In Bezug auf die Absicherung der verwendeten Clients und deren Schnittstellen obliegt eine entsprechende Absicherung den jeweiligen Trägern. Aufgrund der Trägerautonomie wird weder eine Verpflichtung gesehen noch eine Möglichkeit, den freien Trägern Vorgaben zu machen, auf welche Weise diese eine angemessene Absicherung der Clients gewährleisten. Die freien Träger selbst sind z. B. dafür verantwortlich, ob und wann USB-Schnittstellen von Clients gesperrt werden, unter

welchen Voraussetzungen externe Datenträger am Client verwendet werden, wie die Administration der Clients organisiert wird. Dennoch wurden den freien Trägern vor dem Hintergrund partnerschaftlicher Zusammenarbeit Empfehlungen gegeben, wie ein datenschutzkonformer Umgang mit personenbezogenen Daten von Kindern, Eltern und sonstigen Personen erreicht werden kann. In diesem Rahmen wurden ihnen auch Organisationshinweise sowie ein Musterentwurf für ein Anwendermerkblatt als Orientierungshilfe übergeben. Im Hinblick auf die Absicherung der bei KiTa Bremen verwendeten Clients werden die in der bremischen Verwaltung üblichen Sicherheitsvorkehrungen getroffen, die angemessen sind und der Landesbeauftragten für Datenschutz und Informationsfreiheit separat dargelegt werden, sollte dies im Rahmen der Prüfung des Fachverfahrens für erforderlich erachtet werden.

Hinsichtlich der Zulässigkeit der Einschaltung nicht-öffentlicher Auftragsdatenverarbeiter durch öffentliche Träger (KiTa Bremen) gilt Folgendes:

Im Rahmen der Einführung des Fachverfahrens war zu prüfen, unter welchen Voraussetzungen öffentliche Träger nicht-öffentliche Stellen mit der Speicherung und Verarbeitung von Sozialdaten beauftragen dürfen. Gemäß § 80 Abs. 5 SGB X ist eine solche Beauftragung – neben weiteren Anforderungen an die Gestaltung des Vertrages, der Kontrolle und der Dienstleisterauswahl – zulässig, wenn die Arbeiten beim Dienstleister erheblich kostengünstiger erfolgen können und der Auftrag nicht die Speicherung des gesamten Datenbestandes des Auftraggebers umfasst, sondern der überwiegende Teil der Speicherung des gesamten Datenbestandes beim öffentlichen Träger oder einem öffentlichen Auftragsdatenverarbeiter verbleibt.

Vor der Beauftragung des nicht-öffentlichen Auftragsdatenverarbeiters wurde ein Kostenvergleich durchgeführt. Es ist davon auszugehen, dass der überwiegende Teil der Speicherung des gesamten Datenbestandes weiterhin beim öffentlichen Träger verbleibt. So speichert der öffentliche Träger nicht nur Daten in SAP, sondern führt auch Entwicklungsakten der Kinder und speichert große Teile des Schriftverkehrs selbst. Zudem erhält der öffentliche Träger eine monatsaktuelle Spiegelung aller im Rahmen des Fachverfahrens ausgelagerten Daten und speichert diese ebenfalls selbst. Dies stellt nicht nur eine künstliche Doppelung der Daten dar, sondern versetzt den öffentlichen Träger in die Lage, auch bei Störungen in der Sphäre des nicht-öffentlichen Auftragsdatenverarbeiters seinen Pflichten weiterhin nachzukommen.

7.7 Pharmakologische Forschungsdatenbanken

Die datenschutzrechtlichen Bedenken der Landesbeauftragten werden nicht geteilt.

Bremische Krankenkassen übermitteln Versichertendaten an die im 36. Jahresdatenschutzbericht beschriebene Datenbank im Rahmen eines übergeordneten Forschungsvorhabens. Das Forschungsvorhaben wurde u. a. mit Zustimmung der bremischen Aufsichtsbehörde, des Bundesgesundheitsministeriums und des Bundesbeauftragten für Datenschutz und Informationsfreiheit eingeleitet.

Datenschutzrechtliche Vorgaben im Hinblick auf Zugriffssicherheit, Verschlüsselung, Pseudonymisierung und Trennung des Datenbestandes von den auswertenden Stellen werden stets beachtet. Aus diesem sich regelmäßig erweiternden Datenbestand werden der Forschungseinrichtung für jedes einzelne Forschungsvorhaben die notwendigen Daten zur Verfügung gestellt. Die Datenübermittlung muss von den Krankenkassen unterstützt und nach § 75 SGB X von der für die Krankenkasse zuständigen Aufsichtsbehörde genehmigt werden. Eine direkte Anforderung durch die Forschungseinrichtung ohne Beteiligung der Krankenkasse als Herrin der Daten und der Aufsichtsbehörde unterbleibt. Ein Ersatz der aufgebauten Datenbank durch die nach §§ 303a ff SGB V an das Bundesversicherungsamt zu übermittelnden Daten ist nach Auffassung des Senators für Gesundheit nicht zielführend. Zum einen würden die in der Vergangenheit aufgebauten Datenbestände fehlen. Zum anderen blieben entsprechende Vorstöße in verschiedenen Gesetzgebungsverfahren, die ein solches Verfahren ermöglichen würden, bisher erfolglos.

8. Bildung, Wissenschaft und Kultur

8.1 Handreichung für den Einsatz sozialer Netzwerke in der Schule

Das gemeinsame Ziel der Verfasser der Handreichung (Zentrum für Medien des Landesinstituts für Schule, Universität Bremen, Landesbeauftragte für Datenschutz und Informationsfreiheit) bestand nicht darin, die Unzulässigkeit von Facebook in der Schule darzulegen. Wenn das die Intention gewesen wäre, hätte man dies mit einer Verfügung der Senatorin für Bildung und Wissenschaft eher erreichen können. Das Ziel war vielmehr, die vielfältigen Möglichkeiten und Risiken von sozialen Netzwerken auch aus unterschiedlichen Perspektiven darzustellen. Hierbei sollte die Medienkompetenz von Lehrkräften an Bremer Schulen erweitert werden. Eine vollständige und umfassende Einordnung der schulischen Nutzungsmöglichkeiten von sozialen Netzwerken in die Kategorien „Erlaubt“ und „Verboten“ kann schon deswegen nicht gelingen, weil diese Werkzeuge kontinuierlich weiter entwickelt werden. Die Verfasser der Handreichung haben stattdessen versucht, die vielfältigen Möglichkeiten und Risiken von sozialen Netzwerken aus unterschiedlichen Perspektiven darzustellen. Die grundsätzlichen Bedenken der Landesbeauftragten für Datenschutz und Informationsfreiheit zum Persönlichkeitsschutz werden hierbei im Kapitel „Problemlagen“ ausführlich dargestellt.

8.2 Einsatz einer webbasierten Lernplattform

Die in der Lernplattform enthaltenen personenbezogenen Daten können nicht von jeder daran interessierten Person „weltweit verarbeitet, verknüpft und in vielfältiger Weise ausgewertet werden“. Vielmehr ist der Zugriff (über Login-Name und Kennwort) beschränkt auf Lehrkräfte und Schüler/-innen der an der Einführung beteiligten Schulen.

Grundsätzlich wird das Datenschutzkonzept für die künftige webbasierte Lernplattform gegenwärtig von der Senatorin für Bildung und Wissenschaft und dem Zentrum für Medien entwickelt und in enger Rücksprache mit der Landesbeauftragten für Datenschutz und Informationsfreiheit abgestimmt.

9. Umwelt, Bau und Verkehr

9.1 Weitergabe der Telefonnummer von Mietern an mögliche Nachmieter

Bremen hat nur Kenntnis von dem Handeln der GEWOBA. Die GEWOBA verfügt über eine datenschutzkonforme Einwilligungserklärung für die Fälle des Mieterwechsels und die Weitergabe der Telefonnummer für die Vereinbarung von Wohnungsbesichtigungsterminen.

9.3 Luftbildaufnahmen zur Kontrolle von Kleingärten

Es wird befürchtet, dass auf den Luftbildaufnahmen, die zur Kontrolle der Einhaltung baurechtlicher Vorschriften gefertigt wurden, Personen erkannt werden könnten. Auf den Luftbildaufnahmen sind aber keine Personen oder Details zu Personen zu erkennen. Datenschutzrechtliche Bedenken hat die Landesbeauftragte daher nicht.

9.4 Solarkataster Bremen

Es wird auf die Gleichartigkeit der Solarkataster Bremerhaven und Bremen verwiesen, verbunden mit der Kritik, dass die im 33. Jahresdatenschutzbericht (2011) vorgetragenen Bedenken gegen das Solarkataster Bremerhaven bei der Umsetzung des Vorhabens in Bremen unbeachtet geblieben sind.

Durch die Veröffentlichung bzw. das Auffindbar-Machen von gebäudebezogenen Daten über die Suchkriterien Straße / Hausnummer und die mögliche Verknüpfung mithilfe weiterer elektronischer Datenquellen (wie z.B. Telefonbuch, Adressregister) seien quasi personenbezogene Daten herstellbar. Damit sind nach Auffassung der Landesbeauftragten für Datenschutz schutzwürdige Belange der Betroffenen berührt.

Mit dem Solarkataster Bremen ist die Fachverwaltung einer Aufforderung der Bremischen Bürgerschaft nachgekommen (Bürgerschaftsbeschluss vom 21.03.2012 auf der Grundlage eines Antrags der Fraktionen von SPD und Bündnis 90 / Die GRÜNEN (DrS. 18/216)).

Das Konzept des Bremer Solarkatasters wurde der Deputation für Umwelt, Bau, Verkehr, Stadtentwicklung und Energie am 07.02.2013 vorgestellt (Vorlage 18/218 (S)). Nach der Zustimmung des Gremiums wurde die Ausschreibung und Vergabe durchgeführt.

Im Vorfeld der Erstellung des Solarkatasters Bremen wurde sorgfältig abgewogen, ob eine ausschließlich straßengenaue Darstellung zielgenau sein könnte oder aus

fachlicher Sicht eine hausnummerngenaue Suchmöglichkeit erforderlich ist. Außerdem wurde die Frage erörtert, den Wirtschaftlichkeitsrechner, wie er im Bremerhavener Kataster enthalten ist, für Bremen nicht einzurichten.

Wesentlichstes Argument für die hausnummerngenaue Suchmöglichkeit war und ist, dass bei einer nur straßengenauen Recherchemöglichkeit das Auffinden eines bestimmten Gebäudes für Laien in vielen Fällen zu Schwierigkeiten führen kann und damit die vorgesehene Anwendbarkeit in Frage gestellt wird.
Der mit der Veröffentlichung beabsichtigte Effekt, nämlich die einfache und gleichzeitig individuelle Betrachtung eines bestimmten Gebäudestandortes auf seine Solareignung hin auch für fachliche Laien verständlich darzustellen, wäre bei einer Suchroutine auf der Ebene allein der Straße verfehlt worden. Die Beschäftigung der Bevölkerung mit der Thematik und die Schaffung der Sensibilisierung für das Solarthema wären somit geringer ausgefallen.

Es ist, anders als im 36. Jahresbericht dargestellt, nicht zutreffend, dass im Bremer Solarkataster die gleichen Daten wie im Bremerhavener Pendant veröffentlicht werden.

Bei der Umsetzung in Bremen wurde auf den Einsatz einer Wirtschaftlichkeitsberechnung und –darstellung verzichtet.

Inzwischen gibt es nämlich - auf Anforderung - eine für den Nutzer kostenlose und individuelle Solarberatung durch swb und BUND, in deren Rahmen auch diese Fragestellung beantwortet wird. Auf das entsprechende Beratungsangebot wird im Solarkataster hingewiesen.

Es wird jedoch, in Kenntnis dieses Unterschieds, die Frage aufgeworfen, ob nicht durch Eingabe der Randdaten eines Einzelgebäudes aus Bremen in das Bremerhavener Solarkataster die entsprechenden Wirtschaftlichkeitsdaten abrufbar wären.
Diese Frage kann verneint werden. Im Bremerhavener Kataster ist die Eingabe der technischen Gebäudedaten nicht per Hand möglich, sondern es wird der bei einem Gebäude hinterlegte Datensatz für die Wirtschaftlichkeitsberechnung verwendet. Eine manuelle Eingabe von Gebäudedaten (Fläche, Höhe, Ausrichtung, Dachneigung) ist nicht möglich. Vor allem aber ist das ansonsten von der Landesbeauftragten für Datenschutz häufig und zu Recht problematisierte Phänomen der massenhaften und vor allem automatisierten Datenverknüpfung über diesen Weg nicht gangbar.

Ergänzend räumen sowohl das Solarkataster Bremen wie auch das in Bremerhaven den betroffenen Grundstückseigentümern die Möglichkeit ein, ohne nähere Begründung der Darstellung ihres Gebäudes im Solarkataster zu widersprechen und die Darstellung löschen zu lassen. Auf diese Möglichkeit wird im Solarkataster hingewiesen. Bisher wurde in einer Handvoll Fällen davon Gebrauch gemacht.

9.5 Falsche Informationen im Rahmen einer Überprüfung nach dem Luftsicherheitsgesetz

In bestimmten sicherheitsempfindlichen Bereichen, wie dem Hafen oder dem Flughafen, muss das Personal eine Zuverlässigkeitsüberprüfung in Form einer Abfrage beim vom Bundesamt für Justiz geführten Bundeszentralregister bestehen. In dem geschilderten Fall war die Auskunft der Bundesverwaltung zunächst falsch und wurde nach Widerspruch des Betroffenen und der Landesbeauftragten für Datenschutz von der Bundesverwaltung berichtigt.

Die bedauerliche Fehlinformation fällt nicht in den Verantwortungsbereich bremischer Behörden und war somit von diesen auch nicht vermeidbar.

10. Wirtschaft und Häfen

10.1 Weitergabe des Ergebnisses einer Gesellenprüfung unter Kollegen

In diesem Fall hat es sich um eine Informationsweitergabe unter Kolleginnen gehandelt, die gleichzeitig Bekannte des betroffenen Auszubildenden, der seine praktische Prüfung nicht bestanden hatte, sind. Im Ergebnis kommt der Bericht daher zu dem Ergebnis, dass zwar ein Verstoß gegen das Bremische Datenschutzgesetz vorliegt, nach Würdigung der Gesamtumstände der Verstoß aber formlos beanstandet wird. Der örtliche Datenschutzbeauftragte wird in seiner Zusammenfassung beispielhafter Fälle aus dem Datenschutzbericht auf diesen Fall eingehen.

11. Finanzen und Verwaltungsmodernisierung

11.1 Umstellung von bargeldlosen Zahlungen auf SEPA

Die erforderlichen Dokumentationen zum Datenschutz liegen inzwischen der Landesbeauftragten für Datenschutz vor bzw. befinden sich in der abschließenden fachlichen Abstimmung mit der behördlichen Datenschutzbeauftragten. Die Berechtigungsthematik für den Zahlungsverkehr wird in der Dokumentation zur Reorganisation des SAP-Berechtigungswesens (s. Ziffer 4.2, ReBe) abgedeckt und entsprechend umgesetzt.

12. Medien/Telemedien

12.2 Nutzung von facebook durch öffentliche und nichtöffentliche Stellen

Der Senat der Freien Hansestadt Bremen hat sich am 22. April 2014 ausführlich mit der Thematik auseinandergesetzt und Folgendes beschlossen:

1. Der Senat der Freien Hansestadt Bremen bekräftigt das Ziel, soziale Netzwerke zur Informationsweitergabe und Kommunikation zu nutzen.

2. Er fordert die Dienststellen auf, den Betrieb ihrer Fanpages zu überprüfen und dabei das jeweilige Informationsinteresse bzw. bestehende Veröffentlichungspflichten mit dem Recht auf informationelle Selbstbestimmung abzuwägen. Im Falle der Einrichtung neuer Angebote sind die zuständigen Deputationen oder die Ausschüsse der Bremischen Bürgerschaft zu beteiligen.

Der Vorsitzende der Ständigen Konferenz der Innenminister und –senatoren der Länder hat mit Schreiben vom 18. März 2014 Facebook zu einem Gespräch über die Beantwortung datenschutzrechtlicher Fragestellungen eingeladen. Dem Einladungsschreiben wurde ein Fragenkatalog beigefügt. Facebook hat die Einladung mit Schreiben vom 29. April 2014 bestätigt. Ein genauer Gesprächstermin wurde indes nach derzeitigem Kenntnisstand noch nicht vereinbart. Eine Beantwortung des Fragenkatalogs ist ebenfalls bislang nicht erfolgt.

12.3 Veröffentlichung personenbezogener Daten im Internet

Die Senatorin für Finanzen teilt die Auffassung der Landesbeauftragten für Datenschutz und wird das Thema im IT-Ausschuss der Freien Hansestadt Bremen ansprechen.

13. Beschäftigtendatenschutz

13.1 Öffentlicher Bereich

13.1.2 Videoaufzeichnung und Tonbandaufzeichnung am Schreibtischarbeitsplatz

Ein Beschäftigter des Hansestadt Bremischen Hafenamtes hat an seinem Arbeitsplatz ein Gerät zur Video- und Tonaufzeichnung zum Testen installiert. Das Gerät sollte später in seinem privaten Keller eingesetzt werden. Der Amtsleiter hat diesen Test, nachdem er davon Kenntnis erhalten hatte, sofort unterbunden und die Löschung der Daten veranlasst. Der behördliche Datenschutzbeauftragte wird in seiner Zusammenfassung beispielhafter Fälle aus dem Datenschutzbericht auf diesen Fall eingehen.

Zusammenfassend ist festzustellen, dass es sich bei den Vorfällen um einmalige und keine systematischen, durch organisatorische Maßnahmen zu verhindernden Vorfälle handelt. Der behördliche Datenschutzbeauftragte wird durch seine Kommentierung versuchen, das Bewusstsein der Mitarbeiterinnen und Mitarbeiter für die Belange des Datenschutzes auch außerhalb der unmittelbaren Bürotätigkeit zu schärfen.

13.1.5 Umgang mit einem amtsärztlichen Gutachten

Künftig wird der Grundsatz der Vollständigkeit der Personalakten entsprechend den gesetzlichen Regelungen beachtet, insbesondere werden „überholte Gutachten“, die durch einen untersuchenden Arzt wegen falscher Diagnose durch ein neues Gutachten ersetzt werden, nicht zur Akte genommen, auch nicht in Kopie.

18. Internationaler Datenverkehr

18.3 Cloud Computing

Die Landesbeauftragte für Datenschutz hat den Sachstand dargestellt, allerdings nicht primär für die Nutzung durch die Öffentliche Verwaltung. Die Vertragsgestaltung mit den Cloud-Anbietern und die Nutzung datenschutzkonformer Musterverträge hat aus Sicht der Senatorin für Finanzen wesentliche Bedeutung auch für die Nutzung von Clouds in der Öffentlichen Verwaltung. Die Senatorin für Finanzen beobachtet die Entwicklung, auch in Zusammenarbeit mit den anderen Trägerländern von Dataport.

Davon unabhängig entsteht schon jetzt eine Nutzung von Cloud-Computing durch die wachsende Anzahl mobiler Endgeräte (vor allem Smartphones) in der Verwaltung. Daraus können zahlreiche Fragestellungen entstehen, deren Brisanz vom Schutzbedarf der betroffenen Daten abhängt. Dafür hat die Senatorin für Finanzen im Rahmen des Projekts „Mobile Connection“ gegenüber den Dienststellen einen Rahmen definiert, der die Nutzung von Cloud-Diensten bisher ausdrücklich nicht vorsieht.

In absehbarer Zukunft wird eine datenschutzkonforme Nutzung von Cloud-Diensten für mobile Endgeräte erforderlich werden.