BREMISCHE BÜRGERSCHAFT **Drucksache 18/551**
Landtag (zu Drs. 18/302)
18. Wahlperiode 28.08.2012

Mitteilung des Senats vom 28. August 2012

Stellungnahme des Senats zum 34. Jahresbericht der Landesbeauftragten für Datenschutz

Mitteilung des Senats

an die Bremische Bürgerschaft (Landtag)

vom 28. August 2012

Stellungnahme des Senats zum „34. Jahresbericht der Landesbeauftragten für Datenschutz“

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum „34. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit zum Datenschutz“ (Berichtszeitraum: 1. Januar bis 31. Dezember 2011) mit der Bitte um Kenntnisnahme.

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 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 34. Jahresberichts nimmt der Senat unter Bezugnahme auf die Nummerierung im Jahresbericht wie folgt Stellung:

4. Datenschutz durch Technikgestaltung und Technikbewertung

4.1 Gestaltungsmöglichkeiten datenschutzrechtlicher Verantwortung beim Einsatz technischer Dienstleister

Im Rahmen der Weiterentwicklung der Konsolidierung der IT der bremischen Verwaltung hat die Senatorin für Finanzen mit der Landesbeauftragten für Datenschutz und Informationsfreiheit die Diskussion zum Thema „Bündelung von Verantwortung für Datenschutz“ begonnen. Dahinter steht die Idee, dass viele Verfahren gleicher Schutzstufe mit einer für diese Verfahren wirksamen Sicherheitsarchitektur angemessen geschützt werden können. In welcher Form bei Verfahren gleicher Schutzstufe die Daten dann zwischen einzelnen Zwecken („Mandanten“) zu trennen sind, wenn auch gemeinsame IT-Systeme benutzt werden, bedarf weiterer Erörterung. Der Senat begrüßt ausdrücklich, dass die Landesbeauftragte für Datenschutz und Informationsfreiheit in ihren übergreifenden Arbeitskreisen diese Thematik behandelt.
Das von der Landesbeauftragten für Datenschutz und Informationsfreiheit angesprochene Grundproblem, nämlich der Kapazitätsunterschied zwischen Auftraggeber und Auftragnehmer hinsichtlich der verfügbaren Ressourcen in Bezug auf die zentrale Si-

cherheitsarchitektur, wird auch von der Senatorin für Finanzen ähnlich wahrgenommen. Hauptursache für diesen Kapazitätsunterschied ist das unterschiedliche Know-how bzw. der Zugang zu technischen Informationen. Aus Sicht der Senatorin für Finanzen kann hier nur die zentrale Kompetenz beim Auftraggeber helfen. In diese Richtung müssen die knappen personellen Ressourcen umgesteuert werden. Ein erster Schritt wird die personelle Ausstattung der Funktion des IT-Sicherheitsbeauftragten bei der Senatorin für Finanzen sein. Die von der Landesbeauftragten für Datenschutz und Informationsfreiheit angesprochene Nutzung des bereits bestehenden Dataport-Sicherheitsmanagements durch die Freie Hansestadt Bremen findet bereits regelmäßig statt. Weitere Maßnahmen werden zur Zeit mit den anderen Dataport-Trägerländern vereinbart.

4.2 Sichere Betriebsinfrastruktur Basis.Bremen (vorher: Verwaltungs-PC)

In dem Projekt Basis.Bremen existiert ein Arbeitspaket „Sicherheit/Datenschutz“, das dienststellenübergreifende Fragestellungen beinhaltet. Sofern sich innerhalb einer Dienststelle besondere Sicherheits- oder Datenschutzfragen ergeben, muss der Bedarf von der Migrationsteuerungsgruppe der jeweiligen Dienststelle festgestellt, dieses “dezentrale“ Arbeitspaket initiiert und Personal dafür eingesetzt werden. Das Gesamtprojekt steht an dieser Stelle in beratender Funktion zur Verfügung.
Im zentralen Arbeitspaket Sicherheit/Datenschutz des Gesamtprojektes wird eine Auseinandersetzung mit den im Datenschutzbericht angemerkten Punkten stattfinden. Da die angemerkten Aufgabenstellungen zu „Active Directory“ und „Public-Key“-Infrastruktur sich auch auf den Regelbetrieb nach Ende des Projektes Basis.Bremen auswirken, ist zu ihrer Bearbeitung eine enge Zusammenarbeit zwischen dem Projekt Basis.Bremen und der Linienorganisation des Referates 02 der Senatorin für Finanzen sowie der Landesbeauftragten für Datenschutz und Informationsfreiheit notwendig. Nach dem ersten Treffen der Lenkungsgruppe Basis.Bremen wird das Arbeitspaket „Sicherheit/Datenschutz“ offiziell begonnen.

4.3 Anforderungen an den sicheren Betrieb von SAP

Die von der Landesbeauftragten für Datenschutz und Informationsfreiheit geforderten Änderungen im Berechtigungs- und Transportwesen wurden im Vorfeld der diesjährigen SAP-Systemaktualisierung (Patchen) im März 2012 bei Dataport beauftragt und dort bereits teilweise umgesetzt. Mit dem Abschluss des Patchens und der Wiederaufnahme des Standardbetriebes ab Juni 2012 wird die Berechtigungspflege ausschließlich im Entwicklungssystem durchgeführt und von dort über das Qualitätssicherungssystem bis in das Produktivsystem transportiert. Damit einher geht auch eine Vereinheitlichung der Berechtigung über die Systeme hinweg.
Die benannte Problematik der Sammelbenutzer wurde in der Anzahl bereits reduziert und wird nach der o. g. Aufnahme des Standardbetriebes weiter analysiert und reduziert werden. Außerdem ist beabsichtigt, finanziert durch beantragte Mittel zum Umbau der Verwaltung und Infrastruktur (UVI-Mittel) und mit Unterstützung durch Dataport, die von der Landesbeauftragten für Datenschutz und Informationsfreiheit genannten noch offenen Punkte des Berechtigungskonzeptes konzeptionell zu bearbeiten und umzusetzen.
Die Senatorin für Finanzen bedauert die noch unvollständige Umsetzung des Berechtigungskonzeptes. Mit der beabsichtigten personellen Stärkung des SAP-Bereichs bei der Senatorin für Finanzen ergeben sich aber zukünftig die Ressourcen, um dieses Konzept abzuschließen und in Folgeprojekten die von der Landesbeauftragten für Da-

tenschutz und Informationsfreiheit genannten weiteren Konzepte (wie z.B. das Informationstechnologie-Rahmenkonzept und das Betriebskonzept, das Datenschutz- und das Archivierungskonzept) zu überarbeiten. Außerdem ist damit auch die dauerhafte und fortlaufende Anpassung der für die SAP-Nutzung notwendigen Konzepte eher möglich.

4.4 VISkompakt – Zentrales System zur elektronischen Aktenführung

Die Gespräche mit der Landesbeauftragten für Datenschutz und Informationsfreiheit und der für das Verfahren VISkompakt zuständigen behördlichen Datenschutzbeauftragten wurden fortgesetzt. Es wurden weitere Unterlagen überarbeitet und aufgrund der Stellungnahmen der Landesbeauftragten für Datenschutz und Informationsfreiheit angepasst. Zu den von der Landesbeauftragten für Datenschutz und Informationsfreiheit aufgeführten offenen Punkten gibt es folgende Sachstände:

- Verarbeitung von sensiblen personenbezogenen Daten:

Bisher werden Dokumente mit dem Schutzbedarf „normal“ gespeichert. Die Landesbeauftragte für Datenschutz und Informationsfreiheit geht davon aus, dass zumindest in Einzelfällen sich auch Dokumente mit dem Schutzbedarf „hoch“ darunter befinden. Die Senatorin für Finanzen wird alle betroffenen Dienststellen darauf hinweisen und sie bitten, die Schutzbedarfsfeststellung zu überprüfen. Bei einem geplanten Vorhaben im Gesundheitsamt Bremen geht es ausdrücklich um Dokumente mit dem Schutzbedarf „hoch“. Für dieses Vorhaben wird gerade die Umsetzung der Verschlüsselung des Transportweges geprüft. Dafür gibt es unterschiedliche Wege. Aktuell wird die Verschlüsselung über „https“ favorisiert. Nach der Umsetzung im Gesundheitsamt und einer Evaluierungsphase soll geprüft werden, ob diese Verschlüsselung auch auf alle anderen Dienststellen ausgedehnt werden kann.

- Administrationskonzept und revisionssichere Protokollierung:

Die zentralen Administrationsaufgaben werden im Rechte- und Rollenkonzept und bezogen auf den technischen Verfahrensbetrieb im Infrastrukturkonzept beschrieben. Diese Konzepte wurden überarbeitet und werden nach noch zu erfolgenden Abstimmungsprozessen der behördlichen Datenschutzbeauftragten und der Landesbeauftragten für Datenschutz und Informationsfreiheit vorgelegt.
Die Einführung der revisionssicheren Protokollierung bei Dataport erfolgt in einem ersten Schritt für die Verfahren, die in das „BSI“-konforme Rechenzentrum verlagert wurden. Für VISkompakt ist ebenfalls eine Verlagerung geplant. Diese kann aber erst ab dem Jahr 2013 erfolgen. Bis dahin gelten die im Organisationskonzept beschriebenen organisatorischen Maßnahmen für genehmigungspflichtige Administrationsaufgaben. Alternativ soll für die Übergangszeit geprüft werden, ob noch festzulegende Administrationsaufgaben über den Fernwartungszugang erfolgen können. Dabei werden alle Tätigkeiten aufgezeichnet und für einen noch festzulegenden Zeitraum gespeichert.

- Erstellung von Berechtigungskonzepten:

Die dezentralen Rechte- und Rollenkonzepte liegen weitgehend vor. Die Senatorin für

Finanzen hat ein Projekt zur flächendeckenden Einführung von VISkompakt aufgelegt, in dessen Rahmen die teilnehmenden Dienststellen die dezentral erforderlichen Konzepte (insbesondere das Rechte- und Rollenkonzept, das Datenschutzkonzept und das Einführungskonzept) mit externer Unterstützung erstellen sollen.

- Gewährleistung des Trennungsgebots:

Das Trennungsgebot wird in erster Linie über die Zuweisung unterschiedlicher Ablagen und die Zuweisung spezifischer Rechte und Rollen umgesetzt. Damit ist gewährleistet, dass die Mitarbeiterinnen und Mitarbeiter nur auf bestimmte Dokumente zugreifen können. Das Trennungsgebot wird zusätzlich über die Einrichtung von Mandanten umgesetzt. Gesonderte Mandanten wurden für alle Ressorts eingerichtet. Zusätzlich gibt es eigene Mandanten für Dienststellen mit besonders schutzwürdigen Daten oder für Mandanten mit hohen Anforderungen an Performance und/oder den Speicherbedarf.

4.5 Orientierungshilfe Cloud-Computing des Arbeitskreises Technik

Im IT-Planungsrat werden im Rahmen der Nationalen E-Government-Strategie (NEGS) verschiedene Maßnahmen erörtert, an denen die Freie Hansestadt Bremen, vor allem als Trägerland von Dataport, sich beteiligen wird und die das Thema Cloud Computing bearbeiten werden. Dabei wird die Senatorin für Finanzen die Landesbeauftragte für Datenschutz und Informationsfreiheit über die IT-Steuerungsgruppe (ITSG) einbeziehen. Die Überlegungen sind noch im Anfangsstadium und konzentrieren sich auf die Nutzung einer privaten Cloud der öffentlichen Verwaltung für „Exchange“-Dienste, also insbesondere E-Mail und Kalender.

4.6 E-Mail Migration in der bremischen Verwaltung

Die Landesbeauftragte für Datenschutz und Informationsfreiheit hat die Probleme der derzeitigen Verschlüsselungsverfahren für das E-Mail-System zutreffend beschrieben. Auch nach Einschätzung der Senatorin für Finanzen werden immer mehr E-Mails mit sensiblen Daten ohne Nutzung von Verschlüsselung - und damit abweichend von der geltenden E-Mail Richtlinie - verschickt.
Die Nutzung der Verschlüsselung ist sehr stark von der Konfiguration des Endgerätes, also des PCs abhängig. Dies wird sich durch Basis.Bremen (siehe Punkt 4.2) ändern, so dass für verwaltungsinterne E-Mails schrittweise eine deutliche Verbesserung eintreten wird.
Für E-Mails, die eine „Ende-zu-Ende“-Verschlüsselung erfordern, insbesondere zu Empfängern außerhalb des Bremer Verwaltungsnetzes (BVN), wird zur Zeit an einer Lösung gearbeitet. Die Steuerverwaltung pilotiert für die Freie Hansestadt Bremen ein serverbasiertes Verfahren auf der Basis von Governikus, das auch außerhalb der Steuerverwaltung bzw. des Bremer Verwaltungsnetzes eine „Ende-zu-Ende“-Verschlüsselung herstellt. Darüber hinaus ist es für die Dienststellen auch möglich, das bereits vorhandene Verfahren „Elektronisches Gerichts- und Verwaltungspostfach“ (EGVP) für solche Anwendungszwecke zu nutzen.

5. Inneres

5.1 Zensus 2011

Die Landesbeauftragte für Datenschutz und Informationsfreiheit berichtet von der Verärgerung zahlreicher Gebäude- und Wohnungseigentümer über einen Mehrfachversand von Erhebungsunterlagen. Dieses Phänomen des sogenannten „Mehrfachversands“ trat in Bremen ebenso wie in anderen Bundesländern auf. In der Tat konnten nicht alle Eigentümeranschriften im vollen Umfang ermittelt bzw. aufbereitet werden. Allerdings war der Mehrfachversand zu einem großen Teil auch methodisch bedingt und daher kein spezifisch bremisches Problem.

Die Einrichtung der Erhebungsstelle in Bremerhaven folgte vollständig den fachlichen Anforderungen des Zensus 2011. Insbesondere wurden die Erhebungsunterlagen gemäß fachlicher Weisung verschlossen und getrennt gelagert, hier zunächst in einem eigenen, nur dafür vorgesehenen Raum. Der von der Landesbeauftragten für Datenschutz und Informationsfreiheit geforderte zusätzliche weitere Verschluss der Unterlagen in einem Stahlschrank innerhalb dieses Raumes wurde unmittelbar nach Besichtigung als Beschaffungsmaßnahme in die Wege geleitet. Als Sofortmaßnahme erfolgten jedoch zusätzliche Transfers der Erhebungsunterlagen in das Statistische Landesamt Bremen, so dass eine Lagerung in der Erhebungsstelle Bremerhaven nur noch für wenige Unterlagen und wenige Tage erfolgte.

5.2 Einrichtung eines automatisierten Direktzugriffs auf Melderegisterdaten für Kommunalbehörden ohne gesetzliche Grundlage

Die zwischen der Landesbeauftragten für Datenschutz und Informationsfreiheit und dem Senator für Inneres und Sport bestehende unterschiedliche Rechtsauffassung zur Auslegung des § 18 Abs. 5 Melderechtsrahmengesetz bzw. § 30 Abs. 5 Bremisches Meldegesetz konnte bislang nicht ausgeräumt werden.

Die in Aussicht genommene Novellierung der Meldedatenübermittlungsverordnung, mit der u. a. dieses Thema geklärt werden sollte, wurde im Hinblick auf das vom Bund vorgesehene Bundesmeldegesetz, mit dem ein einheitliches Melderecht für die Bundesrepublik Deutschland geschaffen werden soll, zurückgestellt.

5.4 Erteilung einer Auskunft aus dem Melderegister trotz Übermittlungssperre

Nach § 32 Abs. 5 des Bremischen Meldegesetzes hat die Meldebehörde auf Antrag oder von Amts wegen eine Auskunftssperre im Melderegister einzutragen, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Auskunft aus dem Melderegister eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Die Erteilung einer Melderegisterauskunft ist in diesen Fällen unzulässig, es sei denn, nach Anhörung der betroffenen Person kann eine Gefahr ausgeschlossen werden.

Im vorliegenden Fall lag der erteilten Auskunft die Anfrage eines Inkassounternehmens zugrunde. Nach Anhörung der betroffenen Person waren nach Auffassung der Zentralen Meldebehörde im Stadtamt als auch des Senators für Inneres und Sport keine Gründe erkennbar, die unter Berücksichtigung der schutzwürdigen Belange der

betroffenen Person eine Gefährdung nach allgemeiner Lebenserfahrung erkennen ließen.

Gleichwohl hätte die Auskunft nicht erteilt werden dürfen, weil die betroffene Person innerhalb der genannten Frist dem Stadtamt schriftlich mitgeteilt hatte, dass die die Anfrage begründende Angelegenheit erledigt sei. Aufgrund eines Versehens ist dieses Schreiben der Zentralen Meldebehörde jedoch erst verspätet zugegangen.

Für eine Änderung grundsätzlich bewährter organisatorischer Regelungen bei der Eingangsbearbeitung besteht nach übereinstimmender Auffassung des Stadtamtes und des Senators für Inneres und Sport keine Veranlassung, weil es sich hier um ein individuelles Fehlverhalten gehandelt hat.

5.6 Kontrollbesuch bei der Polizei Bremen

Sofern durch die Landesbeauftragte für Datenschutz und Informationsfreiheit die Möglichkeit eines Zugriffes auf personenbezogene Daten durch Nichtberechtigte festgestellt worden ist, wurde seitens der Polizei Bremen eine entsprechende Korrektur vorgenommen. Der behördliche Datenschutzbeauftragte hat im Rahmen seiner Vorabkontrolle festgestellt, dass eine rechtskonforme Ausführung der Intrapol-Verfahren möglich ist. Eine Realisierung einer feineren Abstimmung wird trotz technischer Probleme angestrebt.

Die fehlenden Verfahrensbeschreibungen für die personenbezogenen Anwendungen im Intranet der Polizei Bremen werden zurzeit unter Einbindung des behördlichen Datenschützers erstellt.

5.7 Sichere Kommunikation zwischen der Polizei Bremen und der Staatsanwaltschaft Bremen

Die Polizei Bremen und die Staatsanwaltschaft Bremen haben großes Interesse an einem geordneten und sicheren Verfahren für den elektronischen Datenaustausch.

Nachdem von der Landesbeauftragten für Datenschutz und Informationsfreiheit ein Vorschlag der Polizei Bremen wegen der symmetrischen Verschlüsselung abgelehnt wurde, fand am 16. Mai 2012 ein Gespräch zwischen Vertretern des Senators für Justiz und Verfassung, der Polizei Bremen und der Landesbeauftragten für Datenschutz und Informationsfreiheit statt, in dem der Senator für Justiz und Verfassung einen Vorschlag unterbreitete, der die Forderungen nach Vertraulichkeit, Integrität, Authentizität der Daten und der Kommunikationspartner sowie, in Abhängigkeit von der Weiterverwendung, auch die Nicht-Abstreitbarkeit der Herkunft und des Erhalts gewährleistet und damit dem notwendigen Sicherheitsniveau entspricht.

Nach ausführlicher Diskussion der Beteiligten wurde die Landesbeauftragte für Datenschutz und Informationsfreiheit um Prüfung des Vorschlages gebeten. Unter der Voraussetzung, dass der Vorschlag von der Landesbeauftragten für Datenschutz und Informationsfreiheit akzeptiert wird, sollen die nächsten Schritte zur Umsetzung im Anschluss eingeleitet werden.

5.9 Datenschutzkonzepte der Ortspolizeibehörde Bremerhaven

Aus fachlicher Sicht muss eine Speicherungsfrist von zwei Jahren möglich sein. Nicht immer ist innerhalb der von der Landesbeauftragten für Datenschutz und Informationsfreiheit als zulässig angesehenen Frist erkennbar, dass die erhobenen Daten und aufgezeichneten Gespräche in einem strafrechtlichen Verfahren oder Ermittlungsverfahren benötigt werden. Es kann der Fall sein, dass die Daten erst nach Verstreichen der Fristen als relevant betrachtet werden und dann unwiederbringlich verloren sind. Es ist somit notwendig, solche Daten zum Schutz von Rechtsansprüchen Dritter gegenüber der Polizei, zur Verfahrenssicherung und aus Fürsorgepflicht für Polizeibeamte bis zu zwei Jahre zu speichern. Eine endgültige Festlegung der Speicherfristen ist noch nicht erfolgt.

Da ein Mithören unter bestimmten Voraussetzungen zulässig ist, ist eine Veränderung der Software nicht möglich. Die Mitarbeiter in der Einsatzleitstelle der Ortspolizeibehörde Bremerhaven sind angewiesen von der Möglichkeit des Mithörens nur in zulässigen Ausnahmefällen Gebrauch zu machen. Das Problem wurde dennoch an den Softwareentwickler gemeldet.

Die Volltextrecherche wurde von der Ortspolizeibehörde Bremerhaven verworfen.

5.10 Datenschutzkonzepte beim Senator für Inneres und Sport sowie bei der Zentralen Antikorruptionsstelle

Der Senator für Inneres und Sport hat sich durch Ortstermine und Besprechungen überzeugt, dass der Datenschutz und die Datensicherheit bei der Zentralen Antikorruptionsstelle genauso sorgsam gehandhabt werden wie in allen anderen verantwortlichen Stellen, in denen mit personenbezogenen Daten mit hoher Schutzbedürftigkeit gearbeitet wird. Die Zentrale Antikorruptionsstelle ist ihrer Verpflichtung nachgekommen, ein eigenes Datenschutzkonzept zu erstellen. Eine revisionsfeste Protokollierung des Erstellens, Nutzens, Veränderns, Übermittelns und Löschens der genannten Dateien wäre nur über ein spezielles Dateimanagementsystem möglich. Der Windows Explorer ist hierfür ungeeignet. Da sich datenschutzrechtliche Fragen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten mit hoher Schutzbedürftigkeit nicht nur in der Zentralen Antikorruptionsstelle stellen, sondern allgemein in allen entsprechenden verantwortlichen Stellen, die derartige Daten verarbeiten, erscheint eine zentrale Evaluation und Beschaffung eines geeigneten Dateimanagementsystems durch die Senatorin für Finanzen in Absprache mit der Landesbeauftragten für Datenschutz und Informationsfreiheit angezeigt. Eine lokale Speicherung personenbezogener Daten wird erfolgen, gegebenenfalls unter Beachtung weiterer technischer und organisatorischer Maßnahmen. Andernfalls wäre konsequenterweise auch die Führung physischer Akten in der verantwortlichen Stelle nicht mehr zulässig, was die Ermittlungstätigkeit unmöglich machen würde.

Ein erbetenes klärendes Gespräch mit der Landesbeauftragten für Datenschutz und Informationsfreiheit kam bedauerlicherweise nicht mehr zustande. Der Senator für Inneres und Sport hält es auch für deutlich verfrüht, bereits für das Berichtsjahr 2011 über konkrete Details zu den laufenden Gesprächen zu berichten. Eine Veröffentlichung von Einzelheiten des bestehenden Sicherheitssystems wäre aus Ressortsicht erst angezeigt, wenn zuvor gemeinsam mit der betroffenen Dienststelle der Sachver-

halt vollständig erfasst und die Praktikabilität ihrer technischen Vorschläge überprüft wurde. Zwischenzeitlich wurde im Juli 2012 in einem gemeinsamen Gespräch zwischen Vertretern der Zentralen Antikorruptionsstelle, dem Datenschutzbeauftragten des Senators für Inneres und Sport und der Landesbeauftragten für Datenschutz und Informationsfreiheit erörtert, dass es wirkungsvoller ist, die Diskussion über bestimmte Maßnahmen, die viele verantwortliche Stellen gleichermaßen betreffen, nicht nur am konkreten Beispiel der Zentralen Antikorruptionsstelle zu führen, sondern auf höherer Hierarchieebene weiterreichende Optimierungen des Datenschutzes über alle Ressorts hinweg zu erreichen.

5.13 Datenschutz in Sportvereinen

Der Senator für Inneres und Sport weist daraufhin, dass er vor dem Hintergrund der Autonomie des Sports keine direkte Möglichkeit besitzt, die rechtlich unabhängigen Sportvereine und –verbände zu einer Änderung ihres Verhaltens zu bewegen.

Er hat den aktuellen Bericht der Landesbeauftragen für den Datenschutz und Informationsfreiheit aber zum Anlass genommen, den Landessportbund auf den geschilderten Sachverhalt hinzuweisen und darum zu bitten, seine Mitglieder im Sinne der Empfehlungen der Landesbeauftragten für Datenschutz und Informationsfreiheit zu informieren. Hinsichtlich der im Bereich der Vorlage von erweiterten Führungszeugnissen gegebenen Hinweise, hat der Senator für Inneres und Sport dem Landessportbund empfohlen, diese in die entsprechenden Schulungen zum Thema der sexualisierten Gewalt in Sportvereinen aufzunehmen und in diesem Zusammenhang auch die relevanten Druckerzeugnisse zu überarbeiten.

6. Justiz

6.1 Adressangabe von Zeugen im Strafverfahren

Die Praxis bei der Polizei Bremen wird den Vorgaben der Landesbeauftragten für Datenschutz und Informationsfreiheit gerecht. Besteht für eine Zeugin oder einen Zeugen ein begründeter Anlass zu der Besorgnis, dass durch die Offenbarung der Identität oder des Wohn- oder Aufenthaltsortes Leben, Leib oder Freiheit gefährdet wird, so werden die detaillierten Daten über den Wohnort nicht in der Ermittlungsakte oder dem Informationssystem der Polizei Bremen vermerkt. Die entsprechenden Daten werden beim Sachbearbeiter der Polizei separat gespeichert und ggf. der Staatsanwaltschaft oder dem Gericht übermittelt. Hierdurch wird der erforderliche Schutz der Zeugen im Falle einer Akteneinsichtnahme durch den Verteidiger gewährleistet.

Derzeit erfolgt im Rahmen der regelmäßigen Überprüfung bestehender Regelwerke auch eine Überarbeitung der Dienstanweisung Stalking. Dabei findet der Hinweis der Landesbeauftragten für Datenschutz und Informationsfreiheit Berücksichtigung.

7. Gesundheit und Soziales

7.2 „Kostenlose“ Babyfotos im Krankenhaus

Bereits im vorliegenden Jahresbericht wird dargestellt, dass datenschutzrechtliche Mängel zwischenzeitlich abgestellt wurden.

7.3 Akteneinsicht durch Abgeordnete

Es besteht Einigkeit mit der Landesbeauftragten für den Datenschutz und Informationsfreiheit, dass es bei der Entscheidung über ein Akteneinsichtsgesuch eines Abgeordneten der Bremischen Bürgerschaft nach Art. 105 Abs. 4 Satz 4 Bremische Landesverfassung (BremLV) einer Abwägung bedarf, in welcher die besondere Schutzbedürftigkeit von Sozialdaten Betroffener einzubeziehen ist. Diese Vorgaben hat der Senator für Justiz und Verfassung in der Vergangenheit beachtet und wird dies auch künftig tun.

Zu dem angesprochenen Fall sei auf Folgendes hingewiesen: Im September 2010 berichtete der Weser-Kurier über die – noch nicht rechtskräftige – Verurteilung wegen Betrugs in 44 Fällen mit einem Gesamtschaden zu Lasten der öffentlichen Hand in Höhe von etwa 106.000 Euro. Nach den Feststellungen des Amtsgerichts Bremen waren dem Verurteilten seine Taten durch mangelnde Kontrolle „besonders leicht gemacht worden." (AG Bremen, Urteil vom 2. September 2010 – 90 Ls 211 Js 14260/10 – UA, S. 18). Nach einem Beschluss des Rechtsausschusses gemäß Art. 105 Abs. 4 Satz 3 BremLV gewährte der Senator für Justiz und Verfassung einem Abgeordneten der Bremischen Bürgerschaft am 22. Dezember 2010 Akteneinsicht in die zu diesem Komplex gehörenden Ermittlungsverfahren, nachdem der Abgeordnete sich schriftlich verpflichtet hatte, „über die Informationen zu den persönlichen Verhältnissen der Beschuldigten, insbesondere zu Namen und Anschriften, Gesundheitsdaten, Sozialdaten (Angaben zu persönlichen und sachlichen Verhältnissen im Rahmen des Bezugs von Sozialleistungen) und Vorstrafen … Verschwiegenheit zu bewahren."

Diese Gewährung von Akteneinsicht stand in Übereinstimmung mit Art. 105 Abs. 4 Satz 4 BremLV. Danach darf die Vorlage von Akten nur abgelehnt werden, wenn überwiegende schutzwürdige Belange des Betroffenen entgegenstehen oder öffentliche Belange eine Geheimhaltung zwingend erfordern. Dabei haben Bürgerschaft und Senat nach der Rechtsprechung des Staatsgerichtshofs zur Sicherung eines möglichst umfassenden parlamentarischen Kontrollrechts Vorkehrungen zu treffen, um einerseits auch besonders schutzwürdige Informationen den Parlamentsausschüssen zugänglich zu machen und andererseits Vertraulichkeit und Geheimhaltung solcher Informationen auch auf Seiten des Parlaments sicherzustellen (BremStGHE 7, 9 <36 f.>). Der Senator für Justiz und Verfassung hat die schutzwürdigen Belange in dem konkreten Fall abgewogen und die Akteneinsicht erst nach Abgabe einer Verpflichtungserklärung gewährt, welche auf die besondere Schutzbedürftigkeit von Sozialdaten hinwies. Mit dieser Verpflichtungserklärung hat der Senator zugleich die Pflicht des Abgeordneten zur Geheimhaltung aus Art. 83 Abs. 2 BremLV in Erinnerung gebracht. Eine Pflicht zur schriftlichen Dokumentation der Abwägung bestand nicht (vgl. Art. 105 Abs. 4 Satz 5 BremLV).

Wegen der Bedeutung des Akteneinsichtsrechts konnte auch nicht der Abschluss der Strafverfahren abgewartet werden. Nach den vorangegangenen Presseberichten war dem Abgeordneten daran gelegen, dem behaupteten Mangel an behördlicher Kontrolle nachzugehen. Er war auf eine zeitnahe Akteneinsicht angewiesen, um weitere parlamentarische Kontrollrechte auszuüben, bevor das öffentliche Interesse an der Angelegenheit nachließ. Es kann schon aus Gründen der Gewaltenteilung nicht Sache der senatorischen Behörden sein, dieses Interesse eines Abgeordneten politisch zu bewerten. Denn das Informationsrecht des Abgeordneten dient dazu, diesem die nötigen

Informationen „rasch und zuverlässig“ zu verschaffen (BVerfGE 13, 123 <125>).

Das Vorgehen des Senators für Justiz und Verfassung stand auch in Übereinstimmung mit den Vorschriften des Sozialdatenschutzes. Denn die §§ 67a ff. SGB X regeln nicht das Informationsrecht der Abgeordneten gegenüber der Landesregierung. Diese Frage entscheiden die Länder selbst im Rahmen ihrer in Art. 28 Abs. 1 Satz 1 des Grundgesetzes gewährten Verfassungsautonomie (vgl. BayVerfGH, NVwZ 2004, 204 <207>; BVerfGE 36, 342 <362>).

7.4 Vorgaben für die Verarbeitung von Sozialdaten durch Träger der freien Jugendhilfe

Im Amt für Soziale Dienste soll nach den Vorgaben für die Verarbeitung von Sozialdaten durch Träger der freien Jugendhilfe in Bezug auf die flächendeckende Einführung sicherer Übertragungswege für eine elektronische Kommunikation – wie im 34. Jahresdatenschutzbericht dargestellt - verfahren werden. Aufgrund technischer Einschränkungen konnten und können die genannten Kommunikationswege bisher nicht eingerichtet werden. Die Mitarbeiterinnen und Mitarbeiter des Amtes für Soziale Dienste wurden daher angewiesen, bis zum Einsatz von sicheren Kommunikationswegen den Versand von personenbezogenen bzw. Sozialdaten per E-Mail zu unterlassen.

7.5 Konzept zur Umsetzung eines präventiven Kinderschutzes

Der Magistrat der Stadt Bremerhaven nimmt wie folgt Stellung:

Die Ausführungen der Landesbeauftragten für den Datenschutz und Informationsfreiheit wurden vom Amt für Jugend, Familie und Frauen zur Kenntnis genommen; die inhaltliche Position wird jedoch nicht geteilt.

Das Amt für Jugend, Familie und Frauen hat ausführliche Gespräche mit der Landesbeauftragten für den Datenschutz und Informationsfreiheit zur Umsetzung des Programms „Willkommensbesuche“ im Rahmen der Umsetzung einer Präventionskette geführt. Dabei wurde deutlich gemacht, dass die Hausbesuche nicht mit einer heimlichen Datenerhebung verbunden sind. Zudem erfolgten die Besuche auf freiwilliger Basis der Eltern, wie auch der Landesbeauftragten für Datenschutz und Informationsfreiheit mitgeteilt wurde.

Aus Sicht des Amtes für Jugend, Familie und Frauen ist es nicht zutreffend, dass Kindeswohlgefährdungen nicht gemeldet werden dürfen. Diese Ausführungen der Landesbeauftragten für Datenschutz und Informationsfreiheit stehen im Widerspruch zu dem auch gesellschaftlich gegebenen Auftrag des Kinderschutzes. Die Darstellung zu den Zielsetzungen der Präventionskette entsprechen nicht der Konzeption. Die Hausbesuche sind in der vorliegenden Konzeption als präventive Angebote geplant, die dazu beitragen sollen, dass junge Familien über präventive und familienfreundliche Angebote wie Krippen etc. informiert werden und somit einen besseren Zugang zur Wahrnehmung präventiver Angebote finden.

In den geführten Gesprächen mit der Landesbeauftragten für Datenschutz und Informationsfreiheit wurde auch auf die Zielsetzungen des Gesetzes zur Kooperation und Information im Kinderschutz – KKG - vom 22.12.2011 (BGBl. I 2011, S. 2975) hinge-

wiesen, welche in § 2 KKG den zuständigen örtlichen Jugendämtern ausdrücklich das Recht gibt, entsprechende Daten abzurufen. Weiter ist hier geregelt, dass Eltern auf Wunsch in ihrem Haushalt zu besuchen sind und aktive Prävention erforderlich ist.

Im Sinne des Subsidiaritätsauftrages kann eine solche Aufgabe auch an einen freien Träger übertragen werden.

Die Auffassung, wonach die Durchführung der Information durch einen Träger der freien Jugendhilfe nicht zulässig sei, ist aufgrund der bestehenden Rechtsgrundlagen des Sozialgesetzbuchs – Achtes Buch - und des KKG nicht nachvollziehbar.

Das Amt für Jugend, Familie und Frauen bezieht sich in diesem Zusammenhang auch auf ein Gutachten von Götte/Meysen zu Rechtsfragen im Zusammenhang mit der Durchführung von Familienbesuchen vom 20.01.2012, erstellt im Auftrag der Universitätsklinik Ulm, das die Rechtsposition des Amtes für Jugend, Familie und Frauen bekräftigt.

Das Amt für Jugend, Familie und Frauen weist darauf hin, dass das seinerzeit durchgeführte Angebot von den Eltern überwiegend positiv aufgegriffen wurde, da ein umfassendes Informationsangebot insbesondere jungen Eltern durchgängig nicht zur Verfügung stand bzw. steht.

7.6 Anforderungen von medizinischen Unterlagen bei Pflegediensten

Es entspricht geltendem Recht, dass die Krankenkassen in geeigneten Fällen den Medizinischen Dienst der Krankenkassen (MDK) mit der Prüfung beauftragen, ob eine beantragte Leistung medizinisch notwendig ist. Liegen der Krankenkasse nicht alle Unterlagen vor, die der MDK für diese Prüfung benötigt, fordert sie diese bei dem Behandler oder Leistungserbringer an. Wie im Jahresdatenschutzbericht dargestellt, muss der Behandler oder Leistungserbringer die angeforderten Daten in einem für den MDK bestimmten, verschlossenen Umschlag der Krankenkasse zur Verfügung stellen. Diese leitet den Umschlag ungeöffnet weiter. Das Verfahren ist sowohl den Krankenkassen als auch den betroffenen Behandlern und Leistungserbringern bekannt.
Die Krankenkasse hat in dem dargestellten Fall versichert, die Umschläge jeweils ungeöffnet weitergeleitet zu haben. Sie sicherte zudem zu, künftig auf den Versand der medizinischen Unterlagen in einem verschlossenen Umschlag hinzuweisen. Anlass für aufsichtsrechtliche Maßnahmen wird daher seitens der Senatorin für Bildung, Wissenschaft und Gesundheit nicht gesehen.

8. Bildung, Wissenschaft und Kultur

8.1 Beratungsgeheimnis bei der Raumplanung für regionale Beratungszentren

Bei der Ausstattung der Räume für die Regionalen Beratungs- und Unterstützungszentren wird künftig darauf geachtet, dass diese den besonderen Anforderungen der vertraulichen Beratung entsprechen.

8.2 “Stopp der Jugendgewalt”- Einrichtung von Interventionsteams

Nach einem weiteren Gespräch der beteiligten Ressorts mit der Landesbeauftragten für Datenschutz und Informationsfreiheit liegt dieser jetzt eine überarbeitete Fassung der Kooperationsvereinbarung vor, die als Ergebnis des Gesprächs entstanden ist und seitens der Landesbeauftragten beanstandete Punkte nicht mehr enthält.

8.3 Konzept Bildung und Teilhabe und „Blaue Karte“

Der Hinweis der Landesbeauftragten für Datenschutz und Informationsfreiheit wird aufgenommen, wonach das Schuldatenschutzgesetz und die Verordnung nach § 2 des Gesetzes an die Erfordernisse des Bildungs- und Teilhabepakets anzupassen wäre. Die notwendigen Änderungen werden zur Zeit geprüft und mit anderen Änderungswünschen in die Verfahren eingebracht.

Das elektronische Schulverwaltungssystem wird für die Speicherung von Sozialdaten mit hohem Schutzbedarf von der Senatorin für Bildung, Wissenschaft und Gesundheit als geeignet angesehen. Die automatische Löschung der Daten unmittelbar nach Beendigung der Leistungen für Bildung und Teilhabe wird sich für bestimmte Leistungspakete nicht realisieren lassen, für die zur Berechnung von Höchstbeträgen und für die Revision durch die Bundesbehörde eine Speicherung von bis zu zwei Jahren erforderlich ist. Hier wird nach einer angemessenen Lösung zur automatischen Überwachung der Speicherdauer gesucht.

Für die Vorlage der „Blauen Karte" gilt ohne Einschränkung, dass sie nicht den Lehrkräften, sondern ausschließlich im Schulsekretariat vorzulegen ist. Die Farbe der Karte ist durch den Träger der Sozialleistungen vorgegeben, dem Betroffenen wird das Angebot gemacht, die Karte in einem neutralen Umschlag zu übergeben oder sein Anliegen im Rahmen einer Einzelberatung im geschützten Raum vorzutragen. Im Übrigen findet die weiße Farbe bereits beim Stadtticket Anwendung.

8.4 Weiterleitung sensibler Schülerdaten innerhalb und außerhalb der Schule per E-Mail

Zum Umgang mit sensiblen personenbezogenen Schülerdaten innerhalb der Schule und der Lehrerschaft und dem Verfahren per E-Mail an Schulen in öffentlicher Trägerschaft wurde der Landesbeauftragten für Datenschutz und Informationsfreiheit mitgeteilt, dass solche Daten sowohl von der Schulaufsicht als auch von den Schulen verschlüsselt weitergeleitet werden. Es kann aber nicht mit abschließender Sicherheit ausgeschlossen werden, dass es mitunter in wenigen Einzelfällen doch zu unverschlüsseltem Mailverkehr von Schulen mit externen Personen oder Einrichtungen gekommen ist. Die Senatorin für Bildung, Wissenschaft und Gesundheit nimmt aber diesen konkreten Vorfall zum Anlass und befasst sich aktuell erneut mit diesem Thema. Weil der Aufbau des Active-Directories als Grundlage für ein praktikables und benutzerfreundliches Verschlüsselungsverfahren von sensiblen E-Mail-Inhalten für die bremischen Behörden erst in den Jahren 2014/2015 abgeschlossen sein wird, sind die Ressorts für ihren Dienstverkehr und ihre Fachanwendungen somit auf die Sicherheit im abgeschlossenen Bremer Verwaltungsnetz angewiesen. Für den Fall, dass E-Mails diesen geschlossenen Raum verlassen, werden die Mitarbeiterinnen und Mitarbeiter der Behörde und Schulen auf die anzuwendenden Verschlüsselungsverfahren per Verfügung und Handreichung hingewiesen.

Der Landesbeauftragten für Datenschutz und Informationsfreiheit wurde auch mitgeteilt, dass in den Schulleiterdienstbesprechungen die Schulleitungen aufgefordert werden, dafür Sorge zu tragen, dass sensible personenbezogene Schülerdaten nur auf verschlüsselten mobilen Datenträgern transportiert werden dürfen, sofern keine Verschlüsselungsverfahren im E-Mail-Verkehr angewendet werden. Dies wird jeweils im Vermerk über diese Sitzung schriftlich dokumentiert.

Abschließend muss perspektivisch darauf verwiesen werden, dass es im Rahmen der Konsolidierung der Netzinfrastruktur für die bremische Verwaltung ein einheitliches Verschlüsselungsverfahren für E-Mails geben wird.

Die Anordnungen für Schulaufsicht und Schulen sehen vor, E-Mails mit personenbezogenen Daten zu verschlüsseln. Weil noch kein allgemeingültiges, leicht praktikables Verfahren für das Bremer Verwaltungsnetz vorhanden ist, bleibt der Behelf mit einem weniger nutzerfreundlichen Verfahren. Es kann nicht ausgeschlossen werden, dass aus diesem Grund in Einzelfällen die Verschlüsselung unterbleibt. Soweit dies bekannt wird erfolgt eine angemessene Abmahnung und Aufklärung. Die Datenübermittlung von privaten Schulträgern an die Behörde der Senatorin für Bildung, Wissenschaft und Gesundheit erfolgt über gesicherte Verbindungen.
Für die den Lehrkräften nach § 3 Abs. 2 Schuldatenschutzgesetz zugestandene Verarbeitung von Schülerdaten auf privaten Geräten steht ein einfach zu installierendes und zu bedienendes Programm zur Verfügung, welches die Daten auf dem (mobilen) Datenträger gegen fremde Zugriffe wirksam schützt. Gleiches gilt für private Geräte, die nicht ausschließlich von der Lehrkraft genutzt werden.
Hier besteht offenbar dringender Handlungsbedarf gegenüber den Schulen bzw. Gesprächsbedarf mit der Landesbeauftragten für Datenschutz und Informationsfreiheit hinsichtlich der Differenz zwischen gesetzmäßigem und praktischem Handeln.

11. Finanzen und Verwaltungsmodernisierung

11.1 Berechnung der Pensionsrückstellungen im Rahmen der Eröffnungsbilanz

Der Senat teilt grundsätzlich die Position der Landesbeauftragten für den Datenschutz und Informationsfreiheit hinsichtlich der Erhöhung des Schutzniveaus bei der Datenverarbeitung zur Berechnung der Pensionsrückstellungen. Das Programm zur Berechnung der Pensionsrückstellungen (Pzva) läuft zukünftig auf dem Server im Referat 32 der Senatorin für Finanzen. Das Referatsnetz ist aufgrund der besonderen Belange von Personaldatenverarbeitung gegen Zugriffe von Außen abgesichert. Für alle Referatsaufgaben, inklusive der User- Verzeichnisse wird ein eigener Server betrieben, der weder intern vom Netzwerk der Senatorin für Finanzen aus noch extern erreichbar ist. Die Administration dieses Servers wird durch Beschäftigte des Referates 32 sichergestellt.

Bis zur Entscheidung über eine mögliche Überführung in ein datenbankgestütztes Gesamtsystem (z.B. KoPers) bzw. eine vollständige Integration in die vorhandene SQL-Datenbank-Architektur wird weiterhin mit den historisch begründeten Access-Datenbanken gearbeitet werden müssen.

11.2 Einrichtung einer zentralen Zuwendungsdatenbank

Während des Kalenderjahres 2011 haben keine weitergehenden Arbeiten an der zum Ende 2010 in einem ersten Testbetrieb installierten Datenbank stattgefunden, da in einem Ausschreibungsverfahren (Zuschlag November 2011) erst der Dienstleister ausgewählt werden musste.

Seitdem haben mehrere Arbeitsgruppen in verschiedenen Sitzungen und Workshops die für einen Echtbetrieb notwendigen Anpassungen für die Datenbank erarbeitet. Neben den Ressorts und dem Gesamtpersonalrat (GPR) wurde die Landesbeauftragte für Datenschutz und Informationsfreiheit laufend beteiligt. Exemplarisch sind hier die Workshops zum Thema Workflow inklusive Historisierung und Protokollierung zu nennen. Hier ist ein abgestimmter Entwurf entwickelt worden, der dann zusammen mit dem Dienstleister konkretisiert und zur Zeit programmiert wird. Im darauf folgenden Testverfahren wird die Umsetzung überprüft.

Aus dem Workflow und anderen Arbeitsergebnissen haben sich neue Erkenntnisse hinsichtlich der Rollen und Rechte ergeben. Das entsprechende Konzept wird parallel zur Testphase überarbeitet. Danach erfolgt die Abstimmung in den Gremien, die Landesbeauftragte für Datenschutz und Informationsfreiheit wird beteiligt.

Der im Bericht explizit genannte „lesende Zugriff“ wird grundsätzlich nur dem Rechnungshof gewährt. In einigen Organisationseinheiten sind aufgrund unterschiedlicher Strukturen eventuell auch Vorgesetzte mit einer solchen Rolle zu betrauen. Das setzt aber auch zwingend ein örtliches Rollen- und Rechtekonzept voraus. Entsprechende Hinweise erfolgten und erfolgen jeweils in den jeweiligen Sitzungen und Workshops, das Rollen- und Rechtekonzept wird entsprechend der Anmerkungen und Hinweise der Landesbeauftragten für Datenschutz und Informationsfreiheit angepasst.

Hinsichtlich der Frage der Stellenpläne und fachtechnischen Unterlagen, die in der Datenbank hinterlegt werden, befinden sich die Arbeitsgruppen noch im Entscheidungsprozess. Es werden aber nur fallrelevante Daten erhoben, die auch nur vom jeweils berechtigten Personenkreis eingesehen werden können.
Die Einführung einer zentralen Datenbank wird in einigen Ressorts zu organisatorischen Änderungen führen. Der Gesamtpersonalrat ist bei den Sitzungen vertreten und wird parallel zur Projektleitung die örtlichen Personalräte informieren.

Die administrativen Arbeiten im Competence Center (CC-eGovernment) am Aus- und Fortbildungszentrum werden auch über VISkompakt protokolliert und sind nachvollziehbar. Der Versand von Daten, wie Adressdaten, Bankdaten etc. an das CC-eGovernment sollen mit dem sog. „PKI“-Verfahren abgebildet werden. Eine entsprechende Anforderung ist im März 2012 an das Referat 02 der Senatorin für Finanzen in Form einer Genehmigungsanfrage gestellt worden. Es ist zukünftig beabsichtigt, mittels des Governikus Add Ins per Outlook die PDF-Formulare der sachbearbeitenden Ressorts sicher und verschlüsselt an das CC-eGovernment zu übertragen. Um den Pilotbetrieb nicht zu behindern, sollen in der Übergangsphase die PDF-Formulare mit einem Zertifikat signiert und per Outlook versandt werden. Dieses „PKI“ –Verfahren wird bereits in Bremen eingesetzt. Eine Entscheidung hierzu steht noch aus.
Mit der Entwicklung der Online-Antragsstellung ist noch nicht begonnen worden.

11.3 Telefonisches BürgerServiceCentrum/D115

Administrative Zugriffe auf die Software und deren Protokollierung waren zu Beginn des Projektes zunächst nicht geplant und auch nicht gefordert. Die Protokollierung wird aber beauftragt und nachprogrammiert. Dieses Vorgehen ist mit der Landesbeauftragten für Datenschutz und Informationsfreiheit abgesprochen.

Zur Versendung von Tickets innerhalb des Bremer Verwaltungsnetzes ist eine organisatorische Lösung mit der Landesbeauftragten für Datenschutz und Informationsfreiheit verabredet worden. Alle Dienststellen, die am Ticketversand teilnehmen, werden im Rahmen einer Leistungsvereinbarung o. ä. darauf hingewiesen, die Verschlüsselung entweder händisch oder automatisch an den teilnehmenden Arbeitsplätzen einzustellen und auch zu gewährleisten. Es handelt sich hierbei allerdings nur um eine Übergangslösung bis ein geeignetes Verschlüsselungsverfahren für den sicheren Versand von E-Mails innerhalb des Bremer Verwaltungsnetzes eingeführt worden ist. Der Vertrag für die Auftragsdatenverarbeitung wird von der Brekom erst nach Abschluss des Projektes erstellt. Die Endabnahme des Projektes ist noch nicht erfolgt, da der Auftragnehmer die Barrierefreiheit bisher nicht in allen geforderten Punkten erfüllt hat.

12. Medien

12.5 Nutzung von Web 2.0 durch öffentliche Stellen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit hat die Probleme der Fan-Seiten bei Facebook – insbesondere den „gefällt mir“-Button und die Social Plugins zutreffend beschrieben. Die Senatorin für Finanzen teilt ihre Auffassung.

Die Senatorin für Finanzen hat die Ressorts im Rahmen der Sitzungen des IT-Ausschusses über die Probleme bezüglich der Nutzung sozialer Netzwerke wie z. B. Facebook durch das Betreiben von Fan-Seiten durch öffentliche Stellen informiert.

Daraufhin werden keine Social-Plugins eingesetzt, weder von Facebook noch von Google+. Es wird lediglich in gewohnter Weise auf diese Seiten verlinkt, wobei für Facebook noch die ausführlichen Warnhinweise als Zwischenseite eingeblendet werden. Darüber hinaus werden bis auf weiteres keine neuen Fan-Seiten eingerichtet.

Die Senatorin für Finanzen hat Facebook angeschrieben und die Einhaltung des Datenschutzrechtes eingefordert. Facebook hat der Senatorin für Finanzen auch bereits geantwortet. Die Antwort wird noch ausgewertet. Parallel werden die zurzeit laufenden Gerichtsverfahren gegen Facebook hinsichtlich der Einhaltung datenschutzrechtlicher Bestimmungen beobachtet. Sollten sich daraus weitere Handlungsanforderungen ergeben, wird die Senatorin für Finanzen in Abstimmung mit den Ressorts das weitere Vorgehen festlegen.

13. Beschäftigtendatenschutz im öffentlichen Bereich

13.1.1 Versendung von Höhergruppierungsanträgen und fristloser Kündigung per E-Mail

Der in der Hochschule Bremen festgestellte Verstoß ist, wie bereits im Bericht dargestellt, als einmaliger Vorfall mit den Beschäftigten besprochen worden, die datenschutzrechtlichen Bestimmungen werden seitdem eingehalten.

13.1.2 Urlaubsgenehmigungen in offenen Postfächern der Raumpflegerinnen

Die gerügte Praxis der Hochschule Bremen, Urlaubsgenehmigungen in offene Postfächer der Raumpflegerinnen zu legen, ist von der Hochschule abgestellt worden.

13.1.6 Namen und Namenskürzel über Lehrkräfte auf ausgehängten Stundenplänen und im Internet

Vertretungspläne dienen der Organisation des Schulbetriebes. Die ursprünglich von einigen Schulen erfolgte unbeschränkte Veröffentlichung der Vertretungspläne im Internet ist jeweils unverzüglich nach Bekanntwerden abgestellt worden. Auch hat eine Vielzahl Schulen ihre Praxis des Aushängens der Pläne an den dafür in den Gebäuden vorgesehenen Plätzen umgestellt. Allerdings gehört die (frühzeitige) Bekanntgabe von Vertretungsplänen gegenüber Lehrkräften und Schülerinnen und Schülern sowie deren Eltern nach Auffassung der Senatorin für Bildung, Wissenschaft und Gesundheit gleichwohl zu den notwendigen Informationen, die der schulischen Öffentlichkeit leicht zugänglich sein müssen, um den Unterrichtsbetrieb sicherzustellen.
Die Frage, welcher Umgang mit den Namenskürzeln der Lehrkräfte in diesem Zusammenhang aus datenschutzrechtlicher Sicht geboten ist, wird zeitnah mit der Landesbeauftragten für Datenschutz und Informationsfreiheit zu diskutieren sein, um den Schulen eine handhabbare Vorgabe für ihr Handeln zu geben.

13.2.3 Telekommunikationsregelungen und Medienregelungen für Beschäftigte und Studierende in der Jacobs University

Bei der Jacobs University handelt es sich um eine private Einrichtung, die über eine eigene Organisationshoheit verfügt. Der im Rahmen der Rechtsaufsicht zu verfolgende Verstoß ist durch die Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit abgestellt worden, so dass kein weiterer Handlungsbedarf besteht.

15. Videoüberwachung

15.5 Videoüberwachung eines Studentenwohnheimes

In den vom Studentenwerk betriebenen Wohnheimen ist eine Videoüberwachung nicht erfolgt; es sind weder Kameras in der Vergangenheit eingesetzt worden noch ist beabsichtigt, dies in der Zukunft vorzusehen. Es muss sich um einen Vorgang in einem privat betriebenen Wohnheim handeln.

20 Die Entschließungen der Datenschutzkonferenzen im Jahr 2011

20.11 Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen

Die Senatorin für Finanzen bewertet die Einführung von IPv6 nicht grundsätzlich anders als die Landesbeauftragte für Datenschutz und Informationsfreiheit. Sie wird im Rahmen ihrer Aufträge bei der Brekom bis auf weiteres keine Umsetzung von IPv6 in den lokalen Netzen vornehmen lassen. Eine Änderung in dieser Vorgehensweise wird

sie mit der Landesbeauftragten für Datenschutz und Informationsfreiheit abstimmen, insbesondere auch bei der Nutzung anderer Technologien z.B. Voice over IP.
In Verbundnetzen (z.B. DOI) wird IPv6 zur Zeit implementiert. Hier bestehen die von der Landesbeauftragten für Datenschutz und Informationsfreiheit gesehenen Risiken in Bezug auf den Datenschutz nicht.