**BREMISCHE BÜRGERSCHAFT** **Drucksache 19 / 44**
Landtag (zu Drs. 18/1795)
19. Wahlperiode 11. 08. 15

# Mitteilung des Senats vom 11. August 2015

## Stellungnahme des Senats zum 37. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum 37. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit (Berichtszeitraum: 1. Januar bis 31. Dezember 2014) 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 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 37. Jahresberichts nimmt der Senat unter Bezugnahme auf die Nummerierung im Jahresbericht wie folgt Stellung:

### 1.5.3 Zugangserschwerungen durch Verschlüsselung und Co.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit hat in diesem Abschnitt als Unterabschnitt zu „Smart Cities“ das Thema der Bearbeitung personenbezogener Daten aufgegriffen.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit schlägt eine Verschlüsselung als technisch-organisatorische Maßnahme der „Zugangserschwerung“ vor. Ein Verweis auf die technisch-organisatorischen Maßnahmen im Bremischen Datenschutzgesetz (§ 7 BremDSG) ist daher naheliegend.

Die Kommunikation mit E-Mails ist jetzt schon weitgehend verschlüsselt. Allerdings ist es nur eine Leitungsverschlüsselung auf Teilstrecken (z. B. zwischen dem PC und dem Mail-Server). Eine darüber hinausgehende Verschlüsselung (d. h. Bürgerin-zu-Amt bzw. Bürger-zu-Amt bzw. Fachbereich) findet noch nicht statt.

Weitere technisch-organisatorische Maßnahmen werden zurzeit im Rahmen der Überarbeitung bestehender Regelungen geprüft. Dazu gehören:

— Vermeidung von E-Mail-Adressen als Kontaktadressen in sensiblen Fachbereichen,

— Verweis auf entsprechende Werkzeuge (z. B. Governikus Communicator als Nachfolger des elektronischen Gerichts- und Verwaltungspostfachs – EGVP),

— formularbasierte Verfahren zur Kommunikation und die

— Integration des immer noch weit verbreiteten Verschlüsselungsprogramms „Pretty Good Privacy“ (PGP) in die EGVP-Strukturen.

Darüber hinaus bietet die Senatorin für Finanzen im Rahmen eines Pilotprojekts die Kommunikation über PGP mit den Bürgerinnen und Bürgern an.

## 3. Behördliche Beauftragte für den Datenschutz

### 3.1 Gesetzeskonforme Bestellung behördlicher Datenschutzbeauftragter

Die Landesbeauftragte für Datenschutz und Informationsfreiheit stellt fest, dass sie einer bremischen Dienststelle im Zusammenhang mit der Bestellung einer oder eines externen Datenschutzbeauftragten Hinweise bezüglich der Anforderungen zur Ausgestaltung eines entsprechenden Geschäftsbesorgungsvertrags dargelegt hat. Die betroffene Dienststelle stellt hierzu klar, dass der Vertrag zur Bestellung des behördlichen Datenschutzbeauftragten bereits im April 2013 unter Berücksichtigung der Empfehlungen der Landesbeauftragten für Datenschutz und Informationsfreiheit angepasst wurde.

Des Weiteren zeigt die Landesbeauftragte für Datenschutz und Informationsfreiheit an, dass eine bremische Dienststelle mit zahlreichen Verfahren personenbezogener Datenverarbeitungen nunmehr bis Oktober 2015 die Bestellung eines behördlichen Datenschutzbeauftragten sichergestellt hat. Darüber hinaus wird eine ressortinterne Bündelung der Aufgaben des behördlichen Datenschutzbeauftragten derzeit im Rahmen des Ressortprojekts „Zentralisierung von Querschnittsaufgaben“ geprüft. Die dazugehörigen Untersuchungsergebnisse werden in Kürze vorliegen. Eine Entscheidung des Lenkungsausschusses über die Umsetzung wird spätestens für September 2015 erwartet.

## 4. Verwaltungsübergreifende Verfahren

### 4.1 BASIS.Bremen

Die mit der Landesbeauftragten für Datenschutz und Informationsfreiheit vereinbarte Kette von Maßnahmen (vergleiche dazu auch die Stellungnahmen der Senatorin für Finanzen zu den letzten Datenschutzberichten) wird zurzeit umgesetzt. Bis zum Sommer 2015 ist der Abschluss einer Reihe von Workshops hierzu beabsichtigt. Ausstehende Regelungen zur Verwaltung der IT-Systeme durch Dataport sind erarbeitet worden. Die Inkraftsetzung soll umgehend erfolgen.

Anhand von Mustern zur Erfassung der Geschäftsprozesse, der Schutzbedarfsfeststellung und der Risikobetrachtung können die Dienststellen die notwendigen und angemessenen Maßnahmen zur Realisierung ihrer Anforderungen ableiten, selbst vornehmen bzw. abrufen. Die Umsetzung orientiert sich am IT-Grundschutz. Die Umsetzung des Grundschutzes im Bremer Verwaltungsnetz (BVN) und im zentralen Verzeichnisdienst (Active Directory) vollzieht sich im Rahmen entsprechender Aufgabenverlagerungen auf Dataport.

Die Senatorin für Finanzen prüft gegenwärtig, ob der Nachweis sowie die entsprechende Fortschreibung der Einhaltung der Vorgaben des Grundschutzes im Rahmen des von der Landesbeauftragten für Datenschutz und Informationsfreiheit angeregten Sicherheits-Service Level Agreements (SLA) bei Dataport beauftragt werden kann. Dies würde auch die Managementprozesse bei Dataport für BASIS.Bremen abdecken.

Die Beauftragung würde ab 2016 beginnen, da sich dann eine gemeinsame Bedarfslage der Dataport-Trägerländer ergeben wird, die auch eine Teilung der Aufwände ermöglicht.

### 4.2 Sichere Administrationsumgebung bei Dataport

Die Senatorin für Finanzen hat die Unterlagen zu den beiden Administrationsumgebungen geprüft, die es am Standort Bremen und am Standort des neuen Rechenzentrums von Dataport, das auf zwei Standorte in Norddeutschland verteilt ist (RZ 2), gibt.

Im Bereich des „RZ 2“ werden im dritten Quartal 2015 von Dataport die Ergebnisse der Zertifizierung neu vorgelegt (Erneuerungsaudit).

Im Bereich der Administrationsplattform sind die Unterlagen geprüft worden. Eine erste Bewertung hat ergeben, dass im Rahmen der internen Prozesse von Dataport diese Plattform auch für „hohen Schutzbedarf“ ausgelegt ist. Offen ist jedoch, inwieweit hierzu weitere technische Maßnahmen gehören, wie die bislang für die Administrationsplattform der Freien Hansestadt Bremen nicht beauftragte Videoprotokollierung.

Da die Migration in das neue Rechenzentrum (RZ 2) Ende 2015 beginnen soll und voraussichtlich 2016 in großem Umfang vorangetrieben wird, ist zu prüfen, in welchem Umfeld (alt oder neu) diese Anforderungen umzusetzen sind.

### 4.3 Flächendeckende Einführung des Dokumentenmanagementsystems VISkompakt

Die Senatorin für Finanzen prüft und ergänzt im Lauf des Jahres 2015 die Konzepte für die elektronische Akte, insbesondere hinsichtlich der Protokollierung, zum zentralen Rechte- und Rollenkonzept und zum Löschen in VISkompakt.

Eine Abgrenzung des zentralen zu den dezentralen Datenschutzkonzepten erfolgt exemplarisch anhand des dezentralen Datenschutzkonzepts der Senatorin für Soziales, Jugend, Frauen, Integration und Sport.

Bereits in der aktuell zum Einsatz kommenden Version von VISkompakt wurde umgesetzt, dass eine durch Geschäftsgang vorgenommene Rechteerweiterung nach Erledigung des Geschäftsgangs wieder zurückgenommen wird.

Das Konzept zur Verschlüsselung von Daten mit hohem Schutzbedarf wird erarbeitet und gegebenenfalls noch in 2015 pilotiert. Das Datenschutzkonzept wird entsprechend ergänzt.

Zur Frage der Mandantenfähigkeit und der Trennung auf Ablagenebene bestehen noch unterschiedliche Auffassungen. Die Senatorin für Finanzen wird die geltende Regelung prüfen und das Verfahren für die Einrichtung von Mandanten und Ablagen gegebenenfalls neu definieren.

Das Restrisiko einer fehlerhaften Rechtevergabe lässt sich nicht komplett ausschließen. Grundsätzlich sollen Berechtigungen in VISkompakt an Gruppen vergeben werden, die im Active Directory (AD) angelegt werden. Dennoch ist es theoretisch denkbar, dass ein AD-Administrator eine falsche Person zu einer Gruppe zuordnet. Die Pflege des AD hat daher mit besonderer Sorgfalt zu erfolgen. Die Senatorin für Finanzen erarbeitet dazu organisatorische Regelungen, insbesondere auch hinsichtlich der Vorgaben zur Dokumentation.

Für die elektronische Handakte werden die bestehenden Konzepte überprüft und gegebenenfalls angepasst. Aus Sicht der Senatorin für Finanzen handelt es sich beim Export einer Akte oder Bestandteilen einer Akte zunächst nicht um eine Weitergabe der Daten, sondern lediglich um eine lokale Kopie für den berechtigten Nutzer. Eine Protokollierung an dieser Stelle ist daher nicht erforderlich.

Die Bewertung des Schutzbedarfs von Schriftgut kann allerdings nur dezentral erfolgen. Daraus abzuleitende Regelungen für den Schutzbedarf „Hoch“ müssen daher im Wesentlichen in den dezentralen Datenschutz- bzw. Nutzungskonzepten Berücksichtigung finden.

### 4.4 Anforderungen an den Betrieb von SAP

Das Projekt ReBe soll die gesamten Berechtigungen für den SAP-Produktivmandanten FP2/100 im SAP reorganisieren und neue Benutzerrollen schaffen, die genau auf die Tätigkeiten im SAP zugeschnitten sind, die Anwenderinnen und Anwender für ihren Aufgabenbereich benötigen.

Da die Umstellung auf die neuen Berechtigungskonzepte für die Anwender weitreichende Konsequenzen haben kann, findet zurzeit eine intensive und umfassende Testphase der neuen Berechtigungen in der Test- und Qualitätssicherungsumgebung FQ2 statt.

Bis zur Produktivsetzung aller Rollen nach den neuen Berechtigungskonzepten besitzen die Anwender weiterhin ihre bisher vorhandenen Berechtigungen. Dabei greift das grundsätzliche Prinzip der minimalen Berechtigungsvergabe, dass jedem Anwender nur die Zugriffe im System erlaubt, die erforderlich sind. Dies gilt für alle SAP-Bereiche, auch für den Zahlungsverkehr und den Umgang mit Debitoren und Kreditorenstämmen in FQ2.

Begleitend zum Projekt ReBe hat im Juni 2014 Dataport das Tool SAP Test Data Migration Server (TDMS) der Fachlichen Leitstelle SAP Bremen bei einem Treffen vorgestellt. Ziel der Einführung von TDMS ist, in nicht produktiven Systemen der Bremer SAP-Landschaft Kopien der produktiven Mandan-

ten FP2/100 (Senatorin für Finanzen) bzw. FP2/150 (Universität) optional mit anonymisierten personenbezogenen Stammdaten und/oder zeitlich reduziertem Bewegungsdatenbestand aufzubauen. Die so bereitgestellten Systeme sollen für Test, Support bzw. Entwicklungszwecke genutzt werden.

Dataport hat ein entsprechendes Angebot erstellt.

Auf Basis dieses Angebots klärt die Fachliche Leitstelle SAP der Senatorin für Finanzen zurzeit die mögliche Finanzierung des Einführungsprojekts und der laufenden Betriebskosten.

Im Zuge der geplanten strukturellen und funktionalen Weiterentwicklung des SAP-Verfahrens durch Projekte der Senatorin für Finanzen ist auch die Aktualisierung der Datenschutzdokumentenlage zur SAP-Nutzung beabsichtigt, um interne und externe Prüf- und Kontrollziele erfüllen zu können.

Der von den Vertretern der Landesbeauftragten für Datenschutz und Informationsfreiheit in Gesprächen geäußerte Ergänzungs-, Erklärungs- und Vervollständigungsbedarf zur konzipierten Nutzung eines Ticketmanagements für das SAP-Verfahren und dem darin integrierten Prozess zur Kennwortrücksetzung durch die Benutzer wurde gemeinsam strukturiert. Anhand des daraus resultierenden Fragenkataloges wurden die relevanten Projektdokumente durch die Fachliche Leitstelle SAP überarbeitet und der Landesbeauftragten für Datenschutz und Informationsfreiheit sowie dem behördlichen Datenschutzbeauftragten zur erneuten Prüfung übergeben.

Dataport plant im Auftrag der Senatorin für Finanzen für die Verbindung des SAP-Systems, z. B. mit BreKAT, die SAP-Komponente Process Integration (PI) zu nutzen. Das SAP PI-System wird länderübergreifend eingesetzt. Zur Umsetzung des Trennungsgebots bei der PI-Nutzung hat Dataport ein Mandantenkonzept zur Abschottung der länderspezifischen Datenströme entwickelt, das der Landesbeauftragten für Datenschutz und Informationsfreiheit seit Januar 2015 zur Prüfung vorliegt. Länderübergreifend nutzt Dataport außerdem das SAP-System Solution Manager, z. B. für die technische Versorgung der länderspezifischen Solution Manager und SAP ERP-Systeme sowie für die technische Kommunikation mit SAP.

### 4.5 Elektronischer Einkaufskatalog BreKAT

Die Darstellung der Landesbeauftragten für Datenschutz wird geteilt und den Empfehlungen wird gefolgt.

## 5. Inneres und Sport

### 5.1 Mikrozensus

Der von der Landesbeauftragten für Datenschutz festgestellte Sachverhalt ist zutreffend, jedoch als Einzelfall zu werten, dessen Wiederholung aufgrund zwischenzeitlich erfolgter Maßnahmen nicht mehr zu erwarten ist.

Nachdem der Mitarbeiter des Statistischen Landesamtes die erhobenen Daten im Laptop erfasst hat, wurden die handschriftlichen Unterlagen ordnungsgemäß von ihm vernichtet. Das Statistische Landesamt hat dem Interviewer nochmals erläutert, dass seine Vorgehensweise nicht den gesetzlichen Anforderungen entspricht und ihn angewiesen, für die Befragung ab sofort gemäß gesetzlicher Regelung des § 6 Abs. 1 Mikrozensusgesetz 2005 (MZG 2005) bzw. des § 11 Bundesstatistikgesetz (BStatG) entweder den Laptop einzusetzen oder den amtlichen Mikrozensus-Fragebogen zu verwenden.

Die ehrenamtlich eingesetzten Mikrozensus-Interviewer werden vom Statistischen Landesamt geschult und über ihre Rechte und Pflichten belehrt. Als Erhebungsbeauftragte (§ 6 MZG 2005 in Verbindung mit § 14 BStatG ) haben sie die Anweisungen des Statistischen Landesamtes zu befolgen. Mit dem Schreiben zur Bestellung zum ehrenamtlichen Erhebungsbeauftragten erhalten die Interviewer ein Merkblatt zur Belehrung über die Wahrung der statistischen Geheimhaltung und die sich aus dem Bremischen Datenschutzgesetz (BremDSG) ergebenden Pflichten, dessen Empfang sie schriftlich bestätigen müssen.

### 5.2 Telekommunikationsüberwachung durch die Polizeien

Das technische Verfahren der Telekommunikationsüberwachung durch die Polizeien in Bremen und Niedersachsen wird durch das Land Niedersachsen betrieben. Ein weiterer Fortgang in der Angelegenheit konnte dort noch nicht erreicht werden. Auch eine Unterzeichnung des Verwaltungsabkommens steht noch aus.

### 5.3 Allgemeines zu den Polizeiverfahren

Die Polizei Bremen arbeitet derzeit an der Erstellung der von der Landesbeauftragten für Datenschutz und Informationsfreiheit geforderten entsprechenden Unterlagen bzw. Datenschutzkonzepte. Die Arbeiten zur Fertigstellung, insbesondere eines zusammenfassenden Rahmendatenschutzkonzepts, werden priorisiert geführt, andere Konzeptionen stehen in Abhängigkeit noch ausstehender Prüfergebnisse. Offene Detailfragen werden dabei im Dialog mit der Landesbeauftragten für Datenschutz und Informationsfreiheit geklärt.

### 5.4 Data Center Polizeien

Der Hinweis der Landesbeauftragten für Datenschutz und Informationsfreiheit bezüglich des Trennungsgebots gemäß § 7 Absatz 4 Satz 2 Nummer 8 Bremisches Datenschutzgesetz und eines länderübergreifenden Datenaustausches wird im Zuge der künftigen Regelungen berücksichtigt.

### 5.5 Einsatzleitzentrale der Ortspolizeibehörde Bremerhaven

Die Verfahrensbeschreibung der Einsatzleitstelle ist weiterhin in der Bearbeitung. Das Rahmendatenschutzkonzept, auf das die Verfahrensbeschreibung bezüglich der technischen und organisatorischen Maßnahmen hinweist, befindet sich derzeit in der abschließenden Abstimmung. Danach wird das Rahmendatenschutzkonzept der Landesbeauftragten für Datenschutz und Informationsfreiheit unverzüglich zugeleitet.

Der Bitte der Landesbeauftragten für Datenschutz und Informationsfreiheit an den behördlichen Datenschutzbeauftragten der Ortspolizeibehörde Bremerhaven, die Protokollierung auf Gewährleistung der Eingabekontrolle nach § 7 Bremisches Datenschutzgesetz zu prüfen, wurde zwischenzeitlich nachgekommen.

### 5.6 Auskunftsbegehren und Löschbegehren von Bürgerinnen und Bürgern gegenüber der Polizei Bremen

Die Polizei erteilt regelmäßig Bürgerinnen und Bürgern Auskünfte über die Daten, die zu ihrer Person gespeichert sind. Wird darüber hinaus auch eine Löschung der Daten begehrt, prüft die Polizei, ob dies unter Berücksichtigung fachlicher Belange möglich ist. Sofern einem Antrag nicht unmittelbar entsprochen werden kann, wird aber jedenfalls ein voraussichtlicher Löschungstermin mitgeteilt. Ferner werden die Gründe, die gegen eine sofortige Löschung sprechen, dargelegt. Auch in dem von der Landesbeauftragten für Datenschutz und Informationsfreiheit dargestellten Fall hat die Polizei eine einzelfallbezogene Löschung geprüft. Im Hinblick auf die Vielzahl der Vorfälle ist dies jedoch nicht befürwortet worden. Die Polizei Bremen hat den Betroffenen allerdings ausdrücklich auf die Möglichkeit hingewiesen, sich an die Landesbeauftragte für Datenschutz und Informationsfreiheit wenden zu können. Von dieser Möglichkeit hat der Betroffene Gebrauch gemacht. Nach einer abweichenden Einschätzung der Landesbeauftragten für Datenschutz und Informationsfreiheit ist die Polizei Bremen deren Einschätzung gleichwohl gefolgt und hat eine Löschung der Daten durchgeführt. In Bezug auf die Rückmeldung von Verfahrensausgängen an die Polizei Bremen ist festzustellen, dass mit der Einführung des neuen Vorgangsbearbeitungssystems „Artus“ eine deutliche Verbesserung zu verzeichnen ist.

### 5.8 Erweiterte Führungszeugnisse in Sportvereinen

Dem Senatsressort Sport ist nicht bekannt, dass sich Vereine und Verbände über Führungszeugnisse von Personen gegenseitig im Bedarfsfall informieren. Die betroffene Person legt ihr Führungszeugnis nur dem Verein/Verband vor, für den sie tätig ist. Dabei sollte vorausgesetzt werden, dass diese Angaben vertraulich sind und nicht weitergegeben werden.

Nach Auskunft des Landessportbunds wird unter den Vereinen und Verbänden keine Weitergabe und Information über vorliegende Führungszeugnisse praktiziert, da es sich hierbei um ein sehr sensibles Thema handelt. Das Senatsressort Sport hält es für sinnvoll, keine Ausnahmen zu machen und grundsätzlich keine Aussagen oder Angaben an andere weiterzugeben.

## 6. Gesundheit

### 6.1 Aufbau eines klinisch-epidemiologischen Krebsregisters in Bremen

Ein Teil der geäußerten Kritik der Landesbeauftragten für Datenschutz und Informationsfreiheit konnte im Rahmen des förmlichen Beteiligungsverfahrens zum Entwurf eines Gesetzes zur Neuregelung des Krebsregisterrechts (BremKRG) aufgegriffen und im Gesetzentwurf umgesetzt werden. Das Gesetz ist am 1. Mai 2015 in Kraft getreten (Brem.GBl. S. 241). Gleichwohl konnte nicht allen Bedenken der Landesbeauftragten gefolgt werden.

Mit dem BremKRG werden die bundesrechtlichen Regelungen des § 65c SGB V zur Einrichtung von klinischen Krebsregistern in den Ländern umgesetzt. Es gibt darin keine Vorgaben zur Struktur oder Organisation eines klinischen Krebsregisters, wohl aber zum Aufgabenprofil der klinischen Krebsregister wie auch zur personenbezogenen Erfassung von Daten. Um den Personenkreis zu begrenzen, der Zugang zu Identitätsdaten von Krebspatienten hat, führen in Bremen eine Vertrauensstelle und eine Auswertungsstelle mit einer gemeinsamen ärztlichen Leitung die Aufgaben der Krebsregistrierung aus. Aufgaben, die keinen Personenbezug erfordern, erfolgen in der Auswertungsstelle. Eine gemeinsame ärztliche Leitung, wie sie bereits für das seit Jahren bestehende epidemiologische Krebsregister gesetzlich geregelt war, wird es aufgrund der guten Erfahrungen weiterhin geben. Zudem benötigt das Bremer Krebsregister einen Funktionsträger, der das Register nach außen vertritt. Insbesondere vor dem Hintergrund der ärztlichen Schweigepflicht erscheint das im Berichtsentwurf erwähnte „erhöhte Missbrauchsrisiko“ durch eine gemeinsame Leitung irritierend.

Die Forderung, die Möglichkeit einer Übertragung von Aufgaben der Vertrauensstelle auf einen privaten Dritten im Gesetz nicht zu ermöglichen, beruht auf der unzutreffenden Annahme, bei einer privatrechtlich organisierten Stelle bestehe im Fall einer Beleihung generell ein Interessenkonflikt und damit einhergehend eine Missbrauchsgefahr bezüglich der gespeicherten Daten. Die gesetzlichen Bestimmungen werden insgesamt als ausreichend angesehen, ein hohes Datenschutzniveau sicherzustellen.

Ferner bemängelt die Landesbeauftragte für Datenschutz und Informationsfreiheit, dass die betroffene Person keine Möglichkeit hat, die Erhebung, Verarbeitung und Nutzung ihrer Daten durch Einlegung eines Rechtsmittels zu verhindern. Tatsächlich sieht das Gesetz zwar die Möglichkeit vor, Einwendungen gegen die Datenverarbeitung zu erheben, dies führt jedoch nicht zu einem Verarbeitungs- oder Nutzungsverbot, sondern zieht die Pflicht zur unverzüglichen Pseudonymisierung der Daten nach sich. Diese Lösung erscheint angemessen und sachgerecht, weil sie gleichermaßen die Datenschutzinteressen der betroffenen Person, deren Identität durch die Pseudonymisierung geheim bleibt, gewährleistet, und das Interesse an einer möglichst vollständigen flächendeckenden Erfassung von Daten über Krebserkrankungen, die der Verbesserung der onkologischen Versorgung der Bevölkerung dient, sicherstellt.

Der Forderung der Landesbeauftragten für Datenschutz und Informationsfreiheit nach Regelungen für einwilligungsunfähige Personen wurde nicht nachgekommen, da diese umfassend in allgemein geltenden Vorschriften geregelt sind und daher in einem Spezialgesetz, wie es das Gesetz zur Neuregelung des Krebsregisterrechts ist, nicht gesondert aufgeführt werden müssen.

Ein weiterer Kritikpunkt ist das Auskunftsrecht. Nach § 3 Abs. 1 BremKRG hat eine betroffene Person das Recht, jederzeit einen Antrag auf Auskunftserteilung über ihre Daten an das Bremer Krebsregister zu stellen. Diese Daten umfassen auch alle Verarbeitungsschritte, wie z. B. eine Codierung, sodass ein vollumfängliches Auskunftsrecht gewährleistet wird.

Der Forderung, das Pseudonymisierungsverfahren im Gesetz festzulegen, wurde nicht entsprochen. Im Gesetz wird vielmehr der Grundsatz geregelt, dass für eine Verarbeitung und Nutzung von Daten technische und organisatorische Maßnahmen zu treffen sind, die den geltenden Standards der Sicherheitstechnik entsprechen.

Weiter ist es insbesondere zur Durchführung kleinräumiger Untersuchungen im Umfeld potenzieller Emittenten krebserzeugender Stoffe erforderlich, dass die Auswertungsstelle Angaben über die Zugehörigkeit der erfassten Person zu einem Ortsteil und ausschließlich für diese Analysen temporär auch Angaben über deren Anschrift erhält. Der Forderung der Landesbeauftragten für Datenschutz und Informationsfreiheit, diese Datenübermittlung nicht zuzulassen, wurde nicht entsprochen, da andernfalls solche Auswertungen nicht möglich wären.

Auch die in § 16 Absatz 1 BremKRG vorgesehene Möglichkeit, Daten nicht nur – wie bisher – zu wissenschaftlichen Zwecken, sondern auch zu anderen Zwecken an Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung zu übermitteln, wird von der Landesbeauftragten für Datenschutz und Informationsfreiheit kritisiert. Hierzu ist jedoch festzuhalten, dass es sich bei diesen Daten ausschließlich um pseudonymisierte Daten handelt, die – entgegen der Annahme der Landesbeauftragten für Datenschutz und Informationsfreiheit – nicht direkt an Wirtschaftsunternehmen übermittelt werden dürfen, sondern nur an Forschungseinrichtungen, die mit diesen Daten auch im Auftrag von Wirtschaftsunternehmen mit Methoden, die den wissenschaftlichen Standards entsprechen, zu nicht rein wissenschaftlichen Zwecken forschen dürfen. Dem Datenschutz wird auf diese Weise angemessen Rechnung getragen.

Schließlich kritisiert die Landesbeauftragte für Datenschutz und Informationsfreiheit das Verfahren der im Rahmen der Qualitätssicherung des Mammographie-Screening-Programms bundesrechtlich geregelten Übermittlung von Befundunterlagen vom behandelnden Arzt an das zuständige Referenzzentrum, wenn beim Abgleich zwischen Daten des Bremer Krebsregisters und des Mammographie-Screening-Programms ein potenzielles Intervallkarzinom ermittelt wurde.

In den „Tragenden Gründen“ des Gemeinsamen Bundesausschusses zum Beschluss der Durchführung des Abgleichverfahrens wird nach Erfahrungen aus den Modellprojekten ausdrücklich für eine „Nichtanwendung der Einwilligungslösung“ bei der Übermittlung von personenbezogenen Befunddaten votiert.

Um in Bremen ein möglichst hohes datenschutzrechtliches Niveau zu erzielen, werden vor der Übermittlung Angaben, die einen Bezug zur Person zulassen, aus den Befundunterlagen gelöscht. In Bremen wird lediglich eine Kommunikationsnummer mit den Befundunterlagen übermittelt.

### 6.2 Kinder- und jugendpsychiatrische Versorgungsdokumentationen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit fordert vom Gesundheitsamt und dem Klinikum Bremen-Ost die Umsetzung der vorgeschlagenen Änderungen im Bereich der jugendpsychiatrischen Versorgungsdokumentation, die Erstellung einer Verfahrensbeschreibung nach dem Bremischen Datenschutzgesetz und die Erarbeitung der erforderlichen Einwilligungserklärungen und Schweigepflichtentbindungserklärungen von Betroffenen. Die von der Landesbeauftragten für Datenschutz und Informationsfreiheit geforderte Löschung der Identitätsdaten der Betroffenen in der Auswertungsstelle des Klinikums Bremen-Ost ist bereits erfolgt. Hinsichtlich der Umsetzung der übrigen Anforderungen werden die Gespräche mit der Landesbeauftragten für Datenschutz und Informationsfreiheit fortgesetzt. Die Gespräche zur Klärung der datenschutzrechtlichen Problematik sind aus terminlichen Gründen noch nicht zustande gekommen. Der Senator für Gesundheit ist bestrebt, zeitnah eine abschließende Klärung des Sachverhalts zu erreichen.

## 7. Soziales

### 7.1 Kindergarten Online [Ki ON]

Mit der Landesbeauftragten für Datenschutz und Informationsfreiheit fand zwischenzeitlich ein Meinungsaustausch statt.

Hierzu ist festzustellen, dass die Tagesbetreuung sowohl für unter dreijährige Kinder als auch für Kindergartenkinder vom öffentlichen Jugendhilfeträger in Zusammenarbeit mit verschiedenen Trägern von Tageseinrichtungen in Bremen gewährleistet wird. Neben den stadteigenen Kindergärten, die durch KiTa Bremen als Eigenbetrieb in öffentlicher Trägerschaft betrieben werden, leistet eine Vielzahl freier Träger aufgrund 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 im Tätigkeitsbericht angesprochene Fachverfahren zur Verwaltung ihrer Einrichtungen ein und sind somit datenschutzrechtlich verantwortliche Stellen. Daher haben die Träger jeweils einen eigenständigen Vertrag mit dem Softwaredienstleister.

Weiter wird die Auffassung vertreten, dass die Zusammenarbeit zwischen öffentlichen und freien Trägern in § 4 des Achten Buches Sozialgesetzbuch (SGB VIII) ausdrücklich geregelt ist. 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 Selbstständigkeit der freien Träger auch in Bezug auf die Durchführung ihrer Aufgaben sowie in der Gestaltung ihrer Organisationsstruktur zu achten. Die Zusammenarbeit ist partnerschaftlich auszugestalten. Eine Garantenpflicht des Jugendhilfeträgers nach § 61 Abs. 3 SGB VIII besteht nicht, da die freien Träger aufgrund eigener Initiative gleichberechtigt neben dem öffentlichen Träger eigene Einrichtungen betreiben. Der öffentliche Träger kann nicht in die Tätigkeit der freien Träger eingreifen und diese durch Verwaltungshandeln verpflichten, sich den für öffentliche Träger geltenden, sozialdatenschutzrechtlichen Spezialvorschriften zu unterwerfen und damit die Einschaltung von externen Dienstleistern anhand der für den staatlichen Bereich geltenden Vorschrift des § 80 Abs. 5 Zehntes Buch Sozialgesetzbuch (SGB X) auszurichten. Ein Eingriff in die Trägerautonomie ist weder gesetzlich geboten, noch möglich.

Hinsichtlich der im Jahresbericht angesprochenen Punkte der Datenerhebung sowie technischer und organisatorischer Maßnahmen verweist die Senatorin für Soziales, Jugend, Frauen, Integration und Sport auf die Ausführungen des Senats zum 36. Jahresdatenschutzbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit.

### 7.3 Das neue BAföG-System

Die Landesbeauftragte für Datenschutz und Informationsfreiheit hat erst im Oktober 2014 über Änderungsvorschläge bezüglich des Fachdatenschutzkonzepts „Einführung der Software Dialog 21“ unterrichtet. Folglich war eine Reaktion des Studentenwerks bis Ende des Berichtsjahres 2014 in zeitlicher Hinsicht nicht mehr möglich, da ein externer Dienstleister zur Umsetzung der Vorgaben beauftragt werden musste. Das Datenschutzkonzept wurde zwischenzeitlich überarbeitet und die von der Landesbeauftragten für Datenschutz und Informationsfreiheit angemahnten Änderungsvorschläge vollumfänglich umgesetzt.

## 8. Bildung, Wissenschaft und Kultur

### 8.1 Übermittlung von Schülerdaten an Verlagsportal

Der von der Landesbeauftragten für Datenschutz und Informationsfreiheit dargestellte Sachverhalt ist korrekt. Der erwähnte und vom Senatsressort Bildung angestrebte Abschluss eines gesonderten Vertrags konnte nicht realisiert werden, da die online zu lesenden Vertragsbedingungen den Anforderungen aus Sicht des Verlags bereits entsprechen und dieser daher keinen Handlungsbedarf mehr sieht.

Gleichwohl wird die Senatorin für Kinder und Bildung darauf achten, dass die Schulen in regelmäßigen Abständen auf die sich aus der Arbeit mit Online-Portalen ergebenden möglichen Risiken hingewiesen werden, um die Eltern entsprechend zu informieren und so die Gefahr einer Wiederholung der Nennung von Klarnamen zu minimieren. Dies wird durch jährliche Verfügung geschehen.

### 8.2 Facebook-Präsenz auf der Homepage einer Schule

Die Berichterstattung ist sachlich richtig; der Einzelfall konnte im Sinne der Hinweise der Landesbeauftragten für Datenschutz und Informationsfreiheit gelöst werden.

Um zu gewährleisten, dass eine Handlungssicherheit auf der Basis des Datenschutzes bei den Schulleitungen vorhanden ist und die notwendigen Informationen auch bei neuen Schulleitungen präsent sind, wird in bestimmten zeitlichen Abständen auf die bestehende Verfügung hinzuweisen sein. Dies wird mit dem Zusatz versehen, die Informationen über Gesamtkonferenzen oder andere Informationswege auch neuen Lehrerinnen und Lehrern zur Verfügung zu stellen.

### 8.3 Zusammenarbeit zwischen Schule, Jugendhilfe, Gesundheitsamt und ReBUZ

Der Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit gibt den Sachverhalt richtig wieder. Die Vereinbarung zur Zusammenarbeit zwischen Schule, Jugendhilfe, Gesundheitsamt und Regionalen Beratungs- und Unterstützungszentren (ReBUZ) ist mittlerweile abgeschlossen worden.

### 8.5 E-Mail-Nutzung bei der Senatorin für Bildung und Wissenschaft

Die E-Mail hat sich in den letzten Jahren als zentrales Kommunikationsmedium des Bildungs- und Wissenschaftsressorts etabliert. Den Themen Datenschutz und Informationssicherheit wird deshalb eine besondere Bedeutung beigemessen und eine kontinuierliche Verbesserung der technischen und organisatorischen Maßnahmen zu deren Absicherung angestrebt.

Die E-Mailsysteme im Bildungsnetz sind so ausgelegt, dass bei der internen Kommunikation (d. h. alle Sender und Empfänger nutzen ausschließlich E-Mail-Konten des Bildungsnetzes) die erforderlichen technischen Maßnahmen automatisch ergriffen werden. Sobald externe Adressaten involviert sind und sensible Daten im Text oder im Anhang einer E-Mail ausgetauscht werden sollen, müssen diese explizit verschlüsselt werden. Hierfür können im Einzelfall User-Zertifikate für eine Ende-zu-Ende-Verschlüsselung von E-Mails ausgestellt werden oder Informationen können auf Dateiebene (z. B. mit ZIP-Containern) verschlüsselt werden. Die erforderlichen Werkzeuge und Informationen hierfür stehen in allen Dienststellen und Schulen zur Verfügung.

Der rechtliche Ordnungsrahmen ist definiert und es wird derzeit erwogen, ihn im Rahmen einer Dienstvereinbarung zur Nutzung der E-Mail-Konten im Bildungsnetz bis 2016 zu konkretisieren.

## 9. Bau und Umwelt

### 9.1 Umgang mit Bauvorlagen beim Senator für Umwelt, Bau und Verkehr

Entsprechend des Gesprächsergebnisses zwischen der Landesbeauftragten für Datenschutz und Informationsfreiheit und dem Senator für Umwelt, Bau und Verkehr konnte nach Abschluss der Prüfung des Vorgangs einvernehmlich festgestellt werden, dass dem Nachbarn im Regelfall ein berechtigtes Interesse an der Einsichtnahme in Bauakten unterstellt werden kann, um ihm die anschließende Möglichkeit einzuräumen, eine konkrete Beeinträchtigung nachbarlicher Belange geltend machen zu können. Aus diesem Grund ist im Vorfeld keine besondere Begründung für die Akteneinsicht erforderlich. In jedem Fall der Akteneinsicht ist zukünftig durch die Bauaufsichtsbehörde jedoch zu dokumentieren, wer welche Dokumente einsieht, um der Auskunftsverpflichtung gemäß § 21 Absatz 1 Nummer 4 BremDSG nachkommen zu können.

## 10. Finanzen

### 10.1 Umstellung von bargeldlosen Zahlungen auf SEPA

Die Dokumentation zu TransX befindet sich in der Überarbeitung durch die Landeshauptkasse (LHK) bezüglich der Anmerkungen durch die Landesbeauftragten für Datenschutz und Informationsfreiheit. Gleiches gilt für die Datenschutzdokumentation für das Verfahren SEPA, welche komplett neu zu erstellen ist. Betroffen ist hier das Großrechnerverfahren SEPA-Überweisung, dass das Giro-Verfahren aus den Siebzigerjahren abgelöst hat.

Die Fertigstellung der geforderten Dokumentationen wird voraussichtlich bis Ende September 2015 erfolgen.

Die durch das SEPA-Lastschriftverfahren neu zu definierende Mandatsverwaltung obliegt grundsätzlich der Behörde, dem Eigenbetrieb oder der Gesellschaft, die die Lastschrifteinzüge verantwortet, es sei denn, diese Aufgaben wurden vertraglich anderweitig geregelt und einer anderen Einheit übertragen.

Die Lastschriftmandate müssen vom Zahlungspflichtigen in Papierform erteilt werden. Diese Erteilung erfolgt gegenüber der Behörde, dem Eigenbetrieb oder der Gesellschaft, der gegenüber eine Verbindlichkeit besteht. Für alle SEPA-Lastschriften, die durch Zahlläufe der LHK erzeugt werden, sind die erteilten Mandate in der LHK aufzubewahren. Dies betrifft bisher die SAP Buchungskreise des Kernhaushalts, der KiTa Bremen (3250) und dem Landesuntersuchungsamt für Chemie, Hygiene und Veterinärmedizin (2225).

Im SAP werden die zahlungsrelevanten Informationen hinterlegt, dazu gehört unter anderem IBAN, BIC, die Kennzeichnung, ob ein Mandat vorliegt, die Angabe des zu verwendenden Zahlwegs (z. B. E für Lastschriften) oder die Mandatsreferenznummer. Dies ermöglicht, dass Lastschriften, die bis zur Einführung von SEPA ebenfalls über das alte Giro-Verfahren abgewickelt wurden, nunmehr mit Mandatsreferenznummer und Gläubiger-ID im SAP erzeugt und jetzt über eine sichere Verbindung mit der Software Sfirm 3.0 durch Mitarbeitende des Referats 20 (Zahlungsverkehr) der LHK direkt an die Bremer Landesbank übermittelt werden.

Für das Verfahren FIKuS hat es seit Einführung keine Datenschutzdokumentation gegeben, da keine personenbezogenen Daten gemäß § 2 Abs. 1 BremDSG verarbeitet werden. Deshalb hält die Senatorin für Finanzen eine Datenschutzdokumentation für nicht erforderlich.

Im Projekt ReBe werden die gesamten Berechtigungen für den SAP-Produktivmandanten FP2/100 im SAP reorganisiert und neue Rollen geschaffen, die genau auf die Tätigkeiten im SAP zugeschnitten sind, die Anwenderinnen und Anwender für ihren Aufgabenbereich benötigen (siehe auch Stellungnahme zu Ziffer 4.4).

### 10.2 Zentrale Zuwendungsdatenbank

Der beschriebene Abstimmungsprozess mit dem behördlichen Datenschutzbeauftragten der Senatorin für Finanzen ist noch nicht abgeschlossen. Die Hinweise und Anmerkungen werden zurzeit in die Datenschutzdokumentation und in das Rollen- und Rechtekonzept eingearbeitet, soweit sie unstrittig sind. Es ist davon auszugehen, dass noch verbliebene offene Punkte bis Ende 2015 geklärt werden können.

Ebenfalls werden die Hinweise zur Schnittstelle zwischen den Fachverfahren ZEBRA Bremen und SAP aufgenommen. Das Verfahren befindet sich derzeit in der Abstimmung mit der Kassenaufsicht; es wird angestrebt, die Produktivsetzung der Schnittstelle so zeitnah wie möglich zu erreichen

## 13. Videoüberwachung

### 13.2 Justizvollzugsanstalt

Die von der Landesbeauftragten für Datenschutz und Informationsfreiheit bemängelten Kameraeinstellungen wurden überprüft und teilweise geändert. Soweit einige Änderungen unter Hinweis auf Sicherheitsanforderungen von der Anstaltsleitung abgelehnt wurden, sind noch weitere Gespräche zwischen der Landesbeauftragten für Datenschutz und Informationsfreiheit und der Anstaltsleitung vorgesehen. Dabei wird aus Sicht des Senators für Justiz und Verfassung zu berücksichtigen sein, dass die Videoüberwachung des äußeren Anstaltsgeländes ein zentrales Element zur Erhöhung der Sicherheit und Ordnung der Anstalt ist, da hierdurch Mauerüberwürfe aufgeklärt und reduziert werden können. Das dazugehörige Datenschutzkonzept wurde von der Justizvollzugsanstalt zwischenzeitlich in allen von der Landesbeauftragten für Datenschutz und Informationsfreiheit beanstandeten Punkten überarbeitet oder ergänzt und zur Prüfung übersandt.

### 13.3 Eigensicherung der Polizeien

Unter Berücksichtigung der Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit wurden die Inhalte der Verfahrensbeschreibung nunmehr überarbeitet. Die angepasste Version der Verfahrensbeschreibung geht der Landesdatenschutzbeauftragten in Kürze zu.

### 13.4 Lehrerausbildung

Am 30. Januar 2015 fand ein Gespräch zwischen der Landesbeauftragten für Datenschutz und Informationsfreiheit, der Senatorin für Bildung und Wissenschaft und der Universität Bremen statt. Die Beteiligten haben sich in diesem Gespräch auf ein Muster für eine Einwilligungserklärung bei der Durchführung von Videografien verständigt. Ebenso erfolgte eine Verständigung darüber, wie der Einsatz von Videografien in den Modulbeschreibungen im Handbuch „Schulpraktische Studien“ dargestellt wird. Eine gesonderte Erklärung, in der die Studierenden ihre Zustimmung zur Durchführung von Videografien geben, entfällt damit. Mit diesen Dokumenten und Maßnahmen wurden die Bedenken der Landesbeauftragten für Datenschutz und Informationsfreiheit aufgegriffen und zwischen allen Beteiligten eine einvernehmliche Lösung entwickelt.

Druck: Anker-Druck Bremen