Mitteilung des Senats
an die Bremische Bürgerschaft (Landtag)
vom 28. August 2018

Stellungnahme des Senats zum „40. Jahresbericht der Landesbeauftragten für Datenschutz“

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum „40. Jahresbericht der Landesbeauftragten für Datenschutz“ (Berichtszeitraum: 1. Januar bis 31. Dezember 2017) 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 40. Jahresberichts nimmt der Senat unter Bezugnahme auf die Nummerierung im Jahresbericht wie folgt Stellung:

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 39. Jahresberichts

Mit der Einführung des Vorgangsbearbeitungssystems (VBS) @rtus am 7. Januar 2014 für die Polizei Bremen und Bremerhaven wurden die Lösch- und Verwaltungsfristen im VBS pauschal, über alle Vorgangsarten hinweg, auf fünf Jahre heraufgesetzt. Die Verlängerung der Löschfristen war notwendig, um eine Datenbasis für eine fachlich begründete längere Datenhaltung zu erlangen. Um die gesetzlichen Vorgaben nach differenzierten Löschfristen zu gewährleisten, wurde das Lösch- und Verwaltungskonzept technisch und fachlich angepasst und in der Version 4.0 am 10. Oktober 2017 eingeführt. Die Löschroutinen sind derzeit noch ausgesetzt, bis die endgültigen Ergebnisse aus den Teilprojekten „Betrieb“ (fachliche Anpassungen des Lösch- und Verwaltungskonzeptes), „Daten“ (Fristennachberechnung der Alt-Daten, Aufbau einer Auswertedatenbank) und „Berechtigungskonzept“ vorliegen. Mit der Umsetzung des Gesamtprojektes wird auch der gesamte Datenbestand (seit 7. Januar 2014) des VBS @rtus anhand des datenschutzrechtlich abgestimmten Lösch- und Verwaltungskonzeptes nachberechnet und automatisiert bereinigt.

Aufgrund der Abhängigkeiten, der zunächst im VBS @rtus erfassten PIAV-Daten, gelten auch für den PIAV-Prozess die Regelungen aus dem Lösch- und Verwaltungskonzept für das automatisierte Vorgangsbearbeitungssystem @rtus. Ziel ist die Harmonisierung der Lösch- und Verwaltungskonzepte für das VBS @rtus und PIER.

Beide Systeme sind Quellen für die an PIAV anzuliefernden Daten und sollen daher gewährleisten, dass mit der Löschung der Quelldaten auch die erforderlichen Löschaufträge an PIAV erstellt werden. Deshalb wird eine systemübergreifende und

automatisierte Löschung, ausgehend vom VBS @rtus über PIER bis zu PIAV angestrebt. Die Berücksichtigung der gesetzlichen Regelungen des § 36 k Abs. 4 des Bremischen Polizeigesetzes, des § 484 Abs. 4 der Strafprozessordnung und der KpS-Richtlinien stehen im Mittelpunkt der Harmonisierung.

3. Datenschutzbeauftragte

3.2 Zentrale behördliche Datenschutzbeauftragte im Innenressort

Der Senator für Inneres bedauert, dass die Informationen hinsichtlich der Meldung der Bestellung der behördlichen Datenschutzbeauftragten die Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtsjahr nicht erreicht haben. Mit Schreiben vom 20. März 2018 wurde die erforderliche Meldung nachgeholt.

3.3 Organisatorische Anbindung der behördlichen Datenschutzbeauftragten

Im Bereich der Dienststelle der Senatorin für Finanzen wurde zwischenzeitlich ein regelmäßiger Jour-Fixe-Termin des behördlichen Datenschutzbeauftragten der Senatorin für Finanzen mit dem Staatsrat zum Vortrag von Anregungen und Kritik eingerichtet. Die Überlegungen über die zukünftige Berichterstattung gegenüber der Dienststellenleitung sind noch nicht abgeschlossen.

Die Senatorin für Kinder und Bildung hat seit Mitte 2018 die datenschutz nord GmbH beauftragt.

3.5 Arbeitsgruppe "Prüfung bei Dataport"

Die von der Senatorin für Finanzen unterstützte Arbeitsgruppe der behördlichen Datenschutzbeauftragten hat ihre Ergebnisse am 6. Dezember 2017 im Treffen der behördlichen Datenschutzbeauftragten dargelegt. Die Ergebnisse der Arbeitsgruppe fassen die Beobachtungen aus dem Besuch in einer Präsentation und einem Auditbericht zusammen.

Aus dem Aufgabenbereich des Supports bei Dataport wurden von der Arbeitsgruppe folgende Beobachtungen kritisch gewürdigt:

Der Hinweis, dass der User Help Desk (UHD) im Dialog ist, wird während des Dialogs nicht im Vordergrund als Hinweis für die Nutzerin oder den Nutzer eingeblendet.

Die Screenshots, die aus der Sitzung angefertigt werden (wenn sie notwendig sind), bleiben in der Regel bis auf weiteres auf dem PC der UHD-Mitarbeiterin oder des UHD-Mitarbeiters, weil für das Löschen eine Löschroutine fehlt.

Die von der Landesbeauftragten für Datenschutz im Jahresbericht genannten Mängel beim „Support und der Auftragserteilung von Dataport an Subauftragnehmer“ entsprechen nicht den von der Senatorin für Finanzen wahrgenommenen Kritikpunkten der Arbeitsgruppe und damit auch nicht der Grundaussage des Auditberichts. Vielmehr hat die Senatorin für Finanzen aus den Treffen der Arbeitsgruppe und der Vorstellung der Ergebnisse am 6. Dezember 2017 als Ergebnis übernommen, dass die behördlichen Datenschutzbeauftragten die von Dataport zum Schutz der Daten getroffenen technischen und organisatorischen Maßnahmen sehr positiv bewerten.

4. Verwaltungsübergreifende Verfahren

4.1 SAP – Einheitskreditor/Einheitsdebitor

Der Entwurf der Einheitspersonenkontoverordnung ist abgeschlossen und befindet sich derzeit in der Abstimmung mit dem für das IT-Datenschutzrecht zuständigen Referat 40 der Senatorin für Finanzen. Es wird eine Senatsbefassung bis Ende August bzw. Anfang September 2018 angestrebt.

4.2 Länderübergreifende Zusammenarbeit im IT-Bereich

Die Landesbeauftragte für Datenschutz beschreibt zutreffend den aufwendigen Prozess der Abstimmung der Dokumentation gemeinsam genutzter Infrastrukturen zwischen Dataport, den Trägerländern und den zuständigen Datenschutzbehörden. Dieser macht sich an der „Mandantenproblematik“ fest. Auch wenn der Begriff im Jahresbericht hier nicht verwendet wird, geht es um die angemessene Trennung der Verarbeitung von personenbezogenen Daten. Das führt zu einer detailtiefen technischen Diskussion, ohne dass sich an dem Tatbestand etwas ändert.

Der Senat sieht in gemeinsam vorgehaltenen Infrastrukturen die Möglichkeit, die Potenziale moderner Informationstechnik für den Einsatz in der bremischen Verwaltung zu heben.

Die Senatorin für Finanzen begrüßt die Mitarbeit der Landesbeauftragten für Datenschutz in den gemeinsamen Gremien der Datenschutzbehörden der Trägerländer. Ihre Mitarbeit trägt wesentlich dazu bei, dass die technischen Möglichkeiten moderner Rechenzentren in Übereinstimmung mit den rechtlichen Anforderungen des Datenschutzes ausgeschöpft werden können. Verbesserungsmöglichkeiten entstehen auch mit der seit dem 25. Mai 2018 unmittelbar anzuwendenden EU-Datenschutzgrundverordnung, die auch den Betrieb von Verfahren durch gemeinsame Auftraggeber regelt. Die Senatorin für Finanzen begrüßt daher auch die Initiative von Dataport, in den Ausführungsgesetzen der Trägerländer zur Umsetzung der EU-Datenschutzgrundverordnung vergleichbare Formulierungen hierzu aufzunehmen.

4.3 Microsoft Office 365

Die Landesbeauftragte für Datenschutz hält den Einsatz von Microsoft Office 365 in Cloud-Diensten für datenschutzrechtlich ungeklärt. Dies beruht auf dem Diskussionsstand der verschiedenen Arbeitsgruppen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Mittlerweile hat Microsoft Azure Deutschland als Cloud-Dienst ein Testat nach den Anforderungen des Anforderungskatalogs Cloud Computing (Cloud Computing Compliance Controls Catalogue, C5) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erhalten (vgl. Pressemitteilung des BSI vom 15. August 2017). Die Senatorin für Finanzen geht daher von einer datenschutzkonformen Bereitstellung von Microsoft Office 365 in der Deutschland-Cloud aus. Inwieweit die bremische Verwaltung dieses oder ein vergleichbares Cloud-Angebot für „Software as a Service“ (SaaS) künftig nutzt, hängt jedoch auch von weiteren Fragen, wie der Wirtschaftlichkeit im Einzelfall, der Integration von Fachverfahren der Verwaltung sowie dem Auf-

wand zur Anpassung von verwendeten Formatvorlagen und den Remanenzkosten bestehender Infrastrukturen ab.

5. Inneres

5.1 Allgemeines zu den Polizeiverfahren

Zum Vorgangsbearbeitungssystem (VBS) @rtus gilt Folgendes:

Ziel des Projektes „Datenschutzphase 2“ ist auch die Beschränkung der derzeit offenen Zugriffsstruktur innerhalb des Vorgangsbearbeitungssystems (VBS) @rtus. Das Teilprojekt „Berechtigungskonzept“ wurde beauftragt, ein fachlich-technisches Berechtigungskonzept im Kontext des Lösch- und Verwaltungskonzeptes zu erstellen. Im Rahmen der Projektarbeit sollen bestehende Berechtigungsstrukturen unter den datenschutzrechtlichen Gesichtspunkten des Konzeptes betrachtet und aufbereitet werden. Die Entwicklung eines Konzeptes zur Antragstellung für die Erweiterung von Zugriffsrechten auf das VBS @rtus soll auch die Einbindung des behördlichen Datenschutzes berücksichtigen. Das Konzept wird im Rahmen des Projektes „Datenschutzphase 2“ umgesetzt, so dass mit einer Etablierung in den Prozessen im Januar 2019 zu rechnen ist.

Zum Löschkonzept für die Falldatei Rauschgift gilt Folgendes:

Die Überführung der Falldatei Rauschgift erfolgt in drei Stufen. Zunächst werden vom Bundeskriminalamt lokalisierte Daten in die Falldatei „PIAV Rauschgiftkriminalität“ migriert. Weitere lokalisierte Datenbestände werden anonymisiert an „PIAV Strategisch“ überführt. Die Restdatenbestände werden nach der Migration vom Bundeskriminalamt gelöscht. Eine Speicherung von Daten in die Falldatei Rauschgift ist seit dem 17. April 2018 nicht mehr möglich. Die Falldatei Rauschgift Kriminalaktennachweise in der Anwendung INPOL Zentral (Bundeskriminalamt) werden durch den jeweiligen Datenbesitzer gelöscht. Hilfestellungen zur automatisierten Löschung werden mit dem Bundeskriminalamt derzeit erarbeitet.

Zum Datenschutzkonzept für das Verfahren INPOL Land gilt Folgendes:

Die Datenanlieferung an INPOL Land Bremen erfolgt unter den rechtlichen Voraussetzungen der datenschutzrechtlichen Bestimmungen, des Bremischen Polizeigesetzes und des Bundeskriminalamtsgesetzes. Zweck der Speicherungen, Speicherdauer und Art der zu speichernden / verarbeitenden Daten in INPOL werden über die auf Bundesebene festgeschriebenen Verfahrensbeschreibungen und Errichtungsanordnungen der Datengruppen geregelt. Gleichzeitig ergeben sich Vorgaben über das sogenannte „INPOL Manual“ und einschlägige Polizeidienstverordnungen (Bsp. PDV 384.1 und 384.2 – Fahndungen) und die Verfahrensbeschreibung „INPOL Land Bremen“. Die überwiegende Datenanlieferung an INPOL Land Bremen erfolgt über die elektronische Schnittstelle aus dem VBS @rtus heraus. Diese Datenbestände werden dementsprechend über das Lösch- und Verwaltungskonzept des VBS @rtus geregelt. Die Bereinigung von Datensätzen, die nicht über die Schnittstelle angeliefert werden, erfolgt automatisiert über eingetragene Löschfristen. Derzeit liegt eine aktuelle Verfahrensbeschreibung für INPOL Land vor und ein Benutzerkonzept ist erstellt. Eine Schutzbedarfsfeststellung befindet sich derzeit im Fachbereich INPOL in Bearbeitung.

Bezüglich der allgemeinen Zugriffsrechte durch externe Dienstleister ist festzustellen, dass das Hosting von INPOL Land durch einen Staatsvertrag geregelt und von der Firma Dataport als Gesellschaft des öffentlichen Rechts wahrgenommen wird. Mittlerweile erfolgte bei Dataport eine Zentralisierung der Aufgaben. Die Mitarbeiterinnen und Mitarbeiter von Dataport, die für das Verfahren INPOL Land Bremen zuständig sind, betreuen u.a. auch das INPOL Verfahren für die Länder Schleswig-Holstein, Sachsen-Anhalt und Hamburg. Die Mitarbeiterinnen und Mitarbeiter sind den Sicherheitsrichtlinien entsprechend eingestuft und verfügen grundsätzlich für alle Verfahren über dieselben administrativen Zugriffsrechte. Für das Verfahren Bremen gelten insofern die Datenschutzvorgaben analog zu den anderen Ländern.

Zum Datenschutzkonzept bezüglich des Umgangs mit DNA von Geschädigten im Rahmen der Spurensicherung und –auswertung des Landeskriminalamtes gilt Folgendes:

Nach § 81c der Strafprozessordnung (StPO) können im laufenden Strafverfahren auch Körperzellen bei anderen Personen als dem Beschuldigten erhoben werden. Dies ist ohne eine Einwilligung rechtlich möglich, wenn die Personen als Zeugen in Betracht kommen und wenn sich an ihrem Körper eine bestimmte Spur oder Folge einer Straftat befindet. Zum anderen können nach § 81c Abs. 2 S. 1 StPO Blutproben bei anderen Personen als Beschuldigte zum Zwecke der Untersuchung entnommen werden, ohne dass es sich bei dieser um einen Zeugen handelt. Im Gegensatz zu § 81c Abs. 1 StPO gilt nicht der Zeugen- und Spurengrundsatz, sondern lediglich der Aufklärungsgrundsatz. Auch der Fall einer Probenentnahme bei der geschädigten Person, obwohl DNA-Spuren am Tatort noch nicht aufgefunden worden sind, war bereits Gegenstand einer gerichtlichen Entscheidung. Das seinerzeit mit dieser Frage befasste Landgericht Offenburg hielt in seinem Beschluss vom 10. Juli 2002 (III Qs 29/02) fest, dass die Entnahme einer Speichelprobe zum Zwecke der Durchführung eines DNA-Vergleichs schon dann richterlich angeordnet werden dürfe, wenn die begründete Erwartung bestehe, dass auf sichergestellten Spurenträgern Vergleichsmaterial festgestellt werden könne (vgl. hierzu auch LG Ravensburg, NStZ-RR 2010, 18).

Eine unzulässige Vorratshaltung der DNA-Untersuchungsanordnung ist nur dann anzunehmen, wenn sich das Verfahren in einem Stadium befindet, in dem kein sachliches Bedürfnis dafür zu erkennen ist, die Untersuchung anzuordnen oder noch völlig ungewiss ist, ob die oder der Betroffene jemals für eine Entnahme zur Verfügung steht (vgl. dazu BGH, NStZ 2000, 212; NStZ-RR 2003, 289).

Ungeachtet der Möglichkeit einer unter Zwang durchgeführten DNA-Entnahme, bedarf die Anordnung der Entnahme einer DNA-Probe nach § 81c StPO keiner Befugnis, wenn die Maßnahme mit der Einwilligung der in Anspruch genommenen Person durchgeführt wird. Voraussetzung ist, dass die oder der Betroffene ordnungsgemäß belehrt wurde. Die Belehrung hat im Hinblick auf die konkret durchzuführende Maßnahme sowie dem Umstand zu erfolgen, dass die Maßnahme ohne Einwilligung der oder des Betroffenen nicht zulässig ist und dass die einmal erklärte Einwilligung bis zur Beendigung der Untersuchung jederzeit widerrufen werden kann.

Da ein Hinweis über die Widerrufsmöglichkeit in der Anlage „Einverständniserklärung / Belehrung DNA“ fehlte, wurde die Anlage mit einem entsprechenden Hinweis zwi-

schenzeitlich ergänzt. Die oder der Betroffene wird nunmehr auf die Möglichkeit hingewiesen, ihre oder seine Erklärung zu widerrufen.

Hinsichtlich der Vorabkontrollen zu Intrapol gilt Folgendes:

Die bislang erforderlichen Vorabkontrollen entfallen mit der neuen europäischen Regelung. Gleichwohl sind die erforderlichen Verfahrensverzeichnisse für die entsprechenden Anwendungen im Intrapol zu erstellen, zu aktualisieren und vorzulegen. Die behördliche Datenschutzbeauftragte wird mit der Landesbeauftragten für Datenschutz die weiteren Schritte hierzu festlegen.

5.2 Online-Wache

Die folgenden Planungen sollen bis Ende August 2018 umgesetzt werden:

Das Internetformular ist https verschlüsselt und das ausgefüllte Formular wird an einen Server gesendet, der sich auf einer Serverfarm der Brekom befindet. Dort wird aus den Formulardaten eine E-Mail generiert, die an das Postfach OnlineWache@polizei.bremen.de adressiert ist. Die von der Polizei Bremen angebotenen Internetformulare enthalten bereits alle Vorkehrungen für eine PGP-Verschlüsselung. Zurzeit bereitet die Polizei Bremen den technischen Weg der Entschlüsselung über das vorgegebene Governikus Programm vor. Dies umfasst u. a. die Anschaffung von Hard- und Software (Governikus) sowie die Implementierung des Systems in die „Demilitarisierte Zone“ (DMZ) der Polizei Bremen.

Das technische Konzept wurde der Landesbeauftragten für Datenschutz und Informationsfreiheit bereits vorgestellt. Bislang wurden keine datenschutzrechtlichen Bedenken geäußert:

- Verschlüsselung des Internetformulars inklusive der Anlagen mit PGP.
- Entschlüsselung in der DMZ der Polizei Bremen durch einen Server mit dem Programm Governikus.
- Weiterleitung der E-Mail an das Empfängerpostfach.
- Abarbeitung der eingehenden personenbezogenen Daten in eine Anwendung im Polizeinetz.

5.3 Rahmendatenschutzkonzept

Der Entwurf eines Rahmendatenschutzkonzeptes für die Polizei Bremen liegt der Landesbeauftragten für Datenschutz und Informationsfreiheit vor. Aufgrund eines Zuständigkeitswechsels und der Veränderung von Personalressourcen konnte eine abschließende Fassung bisher nicht erstellt werden. Eine priorisierte Bearbeitung wird noch in 2018 angestrebt.

5.4 BodyCam

Der 40. Jahresdatenschutzbericht zitiert den Abschlussbericht der Polizei Bremen mit der Bewertung, dass 98 % der vom Einsatz der BodyCam betroffenen Personen „stark alkoholisiert“ waren oder unter dem Einfluss von Betäubungsmitteln standen und in diesen Fällen kein präventiver oder deeskalierender Effekt erreicht werden kann. Hier wurde der Abschlussbericht nicht richtig wiedergegeben, da durch die

Evaluation lediglich festgestellt wurde, dass 98 % der betroffenen Personen unter Alkohol und/oder Drogeneinfluss standen. Ebenfalls wurde festgestellt, dass je höher der Grad an Beeinflussung durch Alkohol oder Betäubungsmitteln war, desto geringer sich die Wirkung der Bodycam zeigte. Der Anteil der Einsätze, bei denen aufgrund starken Alkoholkonsums oder aufgrund von Betäubungsmitteln kein präventiver oder deeskalierender Effekt festzustellen war, lag bei unter 40 %. Hierbei ist anzumerken, dass der Einsatz der BodyCams im Rahmen des Probelaufs nur in den Bereichen der Diskomeile und des Sielwalls durchgeführt wurde und die Kameras dort im Rahmen von Schwerpunktmaßnahmen überwiegend zur Nachtzeit („Partyzeit“) eingesetzt wurden.

Die Ankündigung, die Bodycam einzuschalten, erfolgt grundsätzlich vor einer entsprechenden Einsatzsituation und wird spätestens dann ausgesprochen, wenn die Kamera beginnt zu filmen. Die betroffene Person wird von den durchgeführten Maßnahmen unmittelbar in Kenntnis gesetzt. Die Maßnahme erfolgt somit offen im Sinne des § 29 Abs. 5 des Bremischen Polizeigesetzes.

Abweichend von der Darstellung im 40. Jahresdatenschutzbericht waren 118 Fälle ohne Relevanz. Diese Aufnahmen werden im Rahmen der rechtlichen Voraussetzungen nach Ablauf von zwei Monaten gelöscht. Eine Löschung vor Ablauf dieser Frist wäre aus polizeilicher Sicht zwar möglich. Gleichwohl schöpft die Polizei Bremen diesen Zeitrahmen im Interesse der oder des Betroffenen aus. Dies scheint angemessen, damit die oder der Betroffene der Maßnahme ausreichend Zeit hat, um rechtliche Beratung einzuholen und ggf. einen Beweisantrag zu stellen. Die Nutzung einer BodyCam wird auch als Beweismittel zugunsten der oder des Betroffenen eingesetzt.

Material, welches „als relevant markiert“ wurde, ist für Zwecke des Ermittlungsverfahrens vorzuhalten. Die Löschung von Aufzeichnungen ist derzeit im Datenschutzkonzept BodyCam geregelt. Danach sind die Daten nach derzeitigem Rechtsstand unverzüglich zu löschen, soweit nicht ihre Aufbewahrung im Einzelfall für die Verfolgung von Straftaten oder Ordnungswidrigkeiten weiterhin erforderlich ist. Vorbehaltlich einer endgültigen Regelung wird dies derzeit durch die Polizei Bremen wie folgt ausgelegt: Die Löschung erfolgt auf Weisung der Staatsanwaltschaft nach Abschluss des Verfahrens oder als relevantes Beweismaterial bei Vergehen nach 5 Jahren bzw. bei Verbrechen nach 10 Jahren.

Der Umgang mit polizeilichem Videomaterial wird derzeit im Rahmen eines Projektes überarbeitet. Ziel ist es, eine Dienstanweisung zu erstellen. Hierbei werden auch die Löschungsfristen beschrieben und mit der Landesbeauftragten für Datenschutz und Informationsfreiheit abgestimmt.

Die Aufnahmen der Polizei mittels BodyCam erfolgen grundsätzlich auf Grundlage des Bremischen Polizeigesetzes. Erfolgen die Aufnahmen nach den Voraussetzungen des Bremischen Polizeigesetzes und entwickelt sich aus der Situation eine strafrechtliche Relevanz, können die zu präventiven Zwecken angefertigten Aufzeichnungen im Strafverfahren hinzugezogen werden. Es bleibt im Einzelfall innerhalb des Ermittlungsverfahrens zu prüfen, ob ein Beweisverwertungsverbot besteht. Die strafrechtliche Würdigung steht jedoch nicht der Polizei Bremen zu, sondern obliegt ausschließlich der Staatsanwaltschaft bzw. den zuständigen Strafgerichten.

5.5 Telekommunikationsüberwachung

Der Hersteller der derzeitigen Telekommunikationsüberwachungsanlage (TKÜ) aus der Kooperation der Bundesländer Niedersachsen und Bremen hat sein Produkt aufgekündigt, so dass die derzeitig genutzte TKÜ-Anlage mit Ablauf des Jahres 2020 nicht weiter genutzt werden kann. Hierdurch bedingt sind faktisch die Mängel abgestellt, da keine weitere polizeiliche Nutzung zur Überwachung in der jetzigen Form erfolgen wird. Aufgrund dessen wird eine völlig neue TKÜ-Anlage in der Kooperation des Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung (RDZ) unter ständiger Begleitung des behördlichen Datenschutzbeauftragten konzeptioniert und unter den bisher gewonnenen Erkenntnissen und Vorgaben entwickelt. Selbstverständlich liegt es auch im Interesse der Polizei Bremen, den datenschutzrechtlichen Belangen Rechnung zu tragen. Eine Anpassung an diese Belange kann nur in enger Zusammenarbeit mit dem Landeskriminalamt Niedersachsen umgesetzt werden, da dort der technische Betrieb erfolgt.

5.7 Entwurf zur Änderung des Bremischen Polizeigesetzes

Auf die Kritik der Landesbeauftragten für Datenschutz und Informationsfreiheit zum Entwurf zur Änderung des Bremischen Polizeigesetzes (Entwurfsfassung: November 2017) wurde im Dezember 2017 bereits durch den Senator für Inneres reagiert.

Zur Umsetzung der Rechtsprechung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz (BKAG) nimmt der Senator für Inneres wie folgt Stellung:

Das Bundesverfassungsgericht hat die Verfassungsmäßigkeit verdeckter präventiver Datenerhebungsmaßnahmen nicht auf Maßnahmen zur Bekämpfung des internationalen Terrorismus beschränkt. Gegenstand der erwähnten Entscheidung des Bundesverfassungsgerichts war § 4a Absatz 1 Satz 2 BKAG a.F. Deshalb hat sich das Bundesverfassungsgericht zu den dort genannten terroristischen Straftaten geäußert und den Bezug für verfassungsgemäß erklärt. Eine Beschränkung sämtlicher verdeckter präventiver Befugnisse und Datenerhebungen in den Landespolizeigesetzen auf Terrorabwehrmaßnahmen hat das Bundesverfassungsgericht damit nicht festgestellt. Dies wird auch aus den allgemeinen Anforderungen deutlich, die das Bundesverfassungsgericht an den Rechtsgüterschutz, die Gefahrenschwellen und die weiteren Voraussetzungen stellt. In Anlehnung an den bereits bestehenden Begriffen „Straftat“ und „Straftat von erheblicher Bedeutung“ soll mit dem Begriff der „terroristischen Straftat“ ein weiterer Begriff zur Präzisierung und Bezugnahme in das Bremische Polizeigesetz (BremPolG) eingeführt werden. Insoweit handelt es sich lediglich um eine Präzisierung des Begriffs aus polizeirechtlicher Sicht, ohne dass hiermit die Gesetzgebungskompetenz des Bundes verletzt wäre. Nach Artikel 74 Absatz 1 Nr. 1 Grundgesetz unterfällt das Strafrecht der konkurrierenden Gesetzgebung. Mit der Definition der terroristischen Straftat wird – ebenso wenig wie mit den seit vielen Jahren im Bremischen Polizeigesetz vorhandenen Definitionen der „Straftat von erheblicher Bedeutung“ (§ 2 Nr. 5 BremPolG) oder der „Straftat“ (§ 2 Nr. 4 BremPolG) – Strafrecht normiert, sondern Polizeirecht. Die Straftatenverhütung ist als Gefahrenabwehr Kernaufgabe des polizeilichen Handelns (vgl. § 1 Abs. 1 S. 1 und 2 BremPolG). Die Abwehr der Gefahren des internationalen Terrorismus‘ fällt daher nicht ohne weiteres in den Zuständigkeitsbereich des Bundeskriminalamtes. Die Zuständigkeit ist nur gegeben, wenn es sich um eine länderübergreifende Gefahr

handelt, die Zuständigkeit der Polizei Bremen nicht erkennbar ist oder der Senator für Inneres um die Übernahme durch das Bundeskriminalamt ersucht (vgl. § 5 BKAG 2018).

5.7.1 Probleme der länderübergreifenden Telekommunikationsüberwachung

Neben Bremen haben nur zwei weitere Bundesländer keine Befugnisse im Bereich der Telekommunikationsüberwachung zum Zwecke der Gefahrenabwehr. In den beiden anderen Bundesländern besteht jedoch die Absicht, ebenfalls Regelungen aus dem Bereich der Telekommunikationsüberwachung einzuführen. Die Befugnis zur präventiven Telekommunikationsüberwachung ist nicht vom Bestand des neuen Rechen- und Dienstleistungszentrums abhängig.

5.7.2 Teilumsetzung der Bundesverfassungsgerichtsentscheidung

Der Senator für Inneres ist der Auffassung, dass der angesprochene Grundsatz nicht die Gesetzgebung, sondern die Verwaltung bindet. Das Bundesverfassungsgericht verlangt nicht, dass eine Regelung existiert, in welcher die Kumulation verdeckter Maßnahmen geregelt wird. Vielmehr verlangt es eine Dokumentation von Eingriffen und die Sicherstellung, dass nicht verschiedene zuständige Stellen unabhängig voneinander doppelt in die Grundrechte eingreifen (vgl. BVerfG, Urteil vom 12. April 2005 – 2 BvR 581/01, juris Rn. 61 ff.). Diesen Anforderungen wird bereits durch vielfältige Dokumentationsverpflichtungen und Abstimmungen zwischen den Sicherheitsbehörden hinreichend Rechnung getragen. Das Bundesverfassungsgericht hat – sogar vor dem Hintergrund der weiter reichenden Befugnisse des Bundeskriminalamtgesetzes – hierzu ausgeführt: „Keinen Bedenken unterliegt allerdings, dass das Gesetz keine ausdrückliche Regelung enthält, die mit Blick auf das Zusammenwirken der verschiedenen Befugnisse das Verbot der Rundumüberwachung näher ausformt.“ (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 u.a., juris, Rn. 254). Dass sich der Überarbeitungsbedarf der Benachrichtigungspflicht aus der Entscheidung des Bundesverfassungsgerichts ergäbe, kann nicht nachvollzogen werden. Die Formulierung im Entwurf entspricht den Anforderungen dieser Rechtsprechung.

5.7.3 Vorbehalt der Anordnung präventiven Polizeihandelns durch Amtsgerichte

Der Gesetzesentwurf zum Bremischen Polizeigesetz bleibt in der bestehenden Systematik. Sofern im Bremischen Polizeigesetz andere Eingriffsbefugnisse dem Richtervorbehalt unterliegen, sind die ordentlichen Gerichte für die Entscheidung zuständig. Die Zuordnung der richterlichen Anordnung zur Verwaltungsgerichtsbarkeit stellt in den Bundesländern derzeit den seltenen Ausnahmefall dar. Da in aller Regel die Bundesländer ebenfalls die Anordnung verdeckter Maßnahmen der ordentlichen Gerichtsbarkeit zuordnen, besteht aufgrund dieser identischen Zuordnung eher die Möglichkeit, Rechtsprechung zu den Befugnissen aus den anderen Bundesländern für die Überprüfung der Befugnisse nach dem Bremischen Polizeigesetz auszuwerten und zu nutzen.

5.7.4 Ausstehende Umsetzung der JI-Richtlinie und der DSGVO

Der Anwendungsbereich der EU-Datenschutzgrundverordnung und der Datenschutzrichtlinie (VO 2016/679 bzw. RL 2016/680) ist strittig. Ob und in welchem Umfang die

EU-Datenschutzgrundverordnung auf hoheitliche Tätigkeiten der Polizei Anwendung findet, wird im zweiten Gesetzesänderungspaket zur Umsetzung des europäischen Datenschutzrechts ausgearbeitet. Der Gesetzentwurf soll der Bürgerschaft (Landtag) noch in 2018 zugeleitet werden.

5.8 Elektronische Akte beim Verfassungsschutz

Hinsichtlich der Einführung einer elektronischen Akte beim Verfassungsschutz bestehen keine Kritikpunkte seitens der Landesbeauftragten für Datenschutz und Informationsfreiheit. Mit den Regelungen werden die Belange des Datenschutzes deutlich gestärkt, u.a. in dem die konkrete Nutzung des Systems protokolliert wird. Die Formulierungen des Gesetzestextes sind dabei weitgehend mit den Regelungen des Bundesrechts identisch.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit kritisiert, dass hinsichtlich der Personenspeicherungen die Altersgrenze bei Minderjährigen von 16 Jahren auf 14 Jahre herabgestuft wurde und damit ihrer Ansicht nach mehr Personen gespeichert werden. Minderjährige konnten gemäß § 12 des Bremischen Verfassungsschutzgesetzes bisher im Regelfall erst ab dem 16. Lebensjahr vom Verfassungsschutz erfasst werden. Diese Schwelle hat sich als zu hoch erwiesen, wie nicht nur mehrere extremistische Anschläge von jüngeren Tätern deutlich bestätigen. Sowohl der Bund als auch die Länder haben daher inzwischen fast ausnahmslos entweder auf eine Altersgrenze verzichtet oder diese im Kern zumindest auf das 14. Lebensjahr herabgesetzt. Diese nunmehr auch für das bremische Recht vorgesehene Regelung gewährleistet damit auch den Informationsaustausch zwischen den Verfassungsschutzbehörden. Der besondere datenschutzrechtliche Schutz Minderjähriger bleibt dabei vollständig erhalten; die entsprechenden Altersgrenzen werden nicht abgesenkt und die verstärkten Prüfungsanforderungen für die Erforderlichkeit der Speicherung bleiben bestehen. Auch die Vorschriften der Polizei sehen eine Speicherung von Tatverdächtigen ab dem 14. Lebensjahr vor.

Die Kritik der Landesbeauftragten für Datenschutz und Informationsfreiheit zur Streichung der gesetzlichen Verpflichtung zur Evaluierung wird nicht geteilt.
Der Bund hat seine entsprechenden Regelungen wissenschaftlich umfassend evaluiert und abermals befristet. Vor dem Hintergrund einer bundesrechtlich vorgesehenen Befristung und der Evaluation einer weitaus größeren Datengrundlage des Bundes bietet eine abermalige bremische Evaluierung absehbar keinen Mehrwert zur Frage, ob die identischen bremischen Regelungen zukünftig weitergelten sollen. Im Hinblick darauf sieht der Entwurf eine weitere befristete Geltung der Vorschriften für fünf Jahre vor, verzichtet jedoch auf eine eigene bremische Evaluation. Im Einvernehmen mit dem Deutschen Bundestag ist das Institut für Gesetzesfolgenabschätzung und Evaluation (InGFA) in Speyer erneut mit der wissenschaftlichen Expertise beauftragt worden.

6. Justiz

6.3 Protokollierung lesender Zugriffe bei der Staatsanwaltschaft

Die Protokollierung des lesenden Zugriffs im Fachverfahren web.sta ist nach wie vor technisch nicht möglich. Für eine Änderung dieses Zustandes ist eine einvernehmliche Beauftragung zur Erweiterung des Fachverfahrens durch alle Trägerländer not-

wendig. Durch die Neufassung des Bundesdatenschutzgesetzes ist dieses Thema erneut auf die Agenda des Anwenderkreises web.sta (Beschlussgremium der web.sta-Trägerländer) gesetzt worden. Es wird seitens der betroffenen Behörde mit einer baldigen Beauftragung zur Umsetzung dieser Datenschutzanforderung gerechnet. Solange die Möglichkeit der Protokollierung indes nicht besteht, kann bei Pflichtverletzungen, wie sie in dem hier geschilderten Fall möglicherweise vorliegen, nur konkret reagiert werden, wenn der betroffenen Behörde auch Hinweise auf die Mitarbeiterin oder den Mitarbeiter, die oder der den Datenschutzverstoß begangen haben soll, übermittelt werden oder sonst vorliegen. Aufgrund des vorgetragenen Sachverhalts hat der zuständige Behördenleiter mangels solcher Anhaltspunkte im vorliegenden Fall ein Ermittlungsverfahren gegen Unbekannt eingeleitet. Das Ermittlungsverfahren wird unter dem Geschäftszeichen 272 UJs 31176/18 geführt.

Generell werden neue Mitarbeiterinnen bzw. Mitarbeiter zum Dienstantritt grundsätzlich auf das Datengeheimnis verpflichtet. Der Leiter der betroffenen Behörde hat den vorgetragenen Vorfall zudem zum Anlass genommen, sämtliche Bedienstete der Staatsanwaltschaft erneut darauf aufmerksam zu machen, dass Recherchen in den Fachanwendungen der Staatsanwaltschaft nur zu dienstlichen Zwecken erfolgen dürfen. Seitens der betroffenen Behörde soll dies auch unmittelbar an die Landesbeauftragte für Datenschutz und Informationsfreiheit zurückgemeldet werden. Weitere organisatorische Maßnahmen, wie zum Beispiel die Beschränkung des Zugriffs auf die Daten, die nur den eigenen Zuständigkeitsbereich betreffen, erscheinen aus hiesiger Sicht nicht angezeigt. Das innerhalb der Staatsanwaltschaft offene System, das allen Mitarbeiterinnen und Mitarbeitern erlaubt, Sachstände auch aus anderen Zuständigkeitsbereichen zu erlangen, ermöglicht u.a. ein effizientes Abarbeiten der außerordentlich hohen Anzahl von Ermittlungsverfahren und sonstigen Vorgängen. Eine Abkehr von dieser Möglichkeit würde einen erheblichen Mehraufwand allein durch interne Sachstandsanfragen erfordern, die innerhalb der Behörde notwendig werden würden.

7. Gesundheit

7.1 Formulare für Schweigepflichtentbindungserklärungen

Der Magistrat Bremerhaven nimmt hierzu wie folgt Stellung:

Die Handlungsanweisung wird derzeit, auch vor dem Hintergrund der europäischen Datenschutzgrundverordnung, überarbeitet. Aus organisatorischen und personellen Gründen konnte diese Überarbeitung leider noch nicht abgeschlossen werden. Im Zusammenhang mit den Freitextfeldern wird, auch beim elektronischen Muster, auf diese Handlungsanweisung verwiesen werden. Sobald alle erforderlichen Arbeiten abgeschlossen sind, werden die entsprechenden Unterlagen der Landesbeauftragten für Datenschutz und Informationsfreiheit zur Prüfung zugeleitet.

7.4 Verfahrensbeschreibungen Gesundheitsamt Bremen

Die Verfahrensbeschreibungen werden im Zuge der Migration der Fachverfahren zu Dataport unter Berücksichtigung der Vorgaben der Landesbeauftragten für Datenschutz und Informationsfreiheit aktualisiert. Diese Migration ist angelaufen und soll bis Ende 2019 abgeschlossen werden. Wie angekündigt wird an diesem Prozess die Landesbeauftragte für Datenschutz und Informationsfreiheit beteiligt, so dass die ak-

tualisierten und erweiterten Verfahrensbeschreibungen gemäß Projektfortschritt an sie übermittelt werden. Der nähere Zeitplan ergibt sich aus den Meilensteinen der Projektskizze zum bereits angelaufenen Projekt D37 „Einheitliche und zukunftsfähige IT-Organisation im Bereich des Öffentlichen Gesundheitsdienstes (hier: Gesundheitsamt Bremen)“ sowie aus dem Handlungsfeld „Digitalisierung und Bürgerservice“ und lautet wie folgt:

- M 1 Start des Projektes am 1. Oktober 2017
- M 2 Start Migration Fachverfahren in das RZ von Dataport 31. März 2018
- M 3 Fertigstellung der GUI des Prototypens für das Userinterface 30. Juni 2018
- M 4 Fertigstellung Aktualisierung Schnittstelle VISKompakt to Office 31. Dezember 2018
- M 5 Start Aufbau Datawarehouse 1. Januar 2019
- M 6 Fertigstellung Datawarehouse 31. Dezember 2019.

8. Bildung und Soziales

8.1 Aufnahme von Gesundheitsdaten im Abschlusszeugnis

Die im 40. Jahresdatenschutzbericht erwähnte Schule hat, wie von der Landesbeauftragten für Datenschutz und Informationsfreiheit gefordert, dem Schüler ein Abschlusszeugnis ohne den Hinweis auf die Gewährung von Notenschutz zwischenzeitlich erteilt.

8.2 Datenbank Haaranalyse

Hinsichtlich der Entwicklung einer neuen Datenbank Haaranalysen liegen ein Datenschutzkonzept sowie ein Konzept zur technischen Sicherheit vor. Mit der Umsetzung der Entwicklung der Datenbank konnte trotz weiterer durch die Landesbeauftragte für Datenschutz und Informationsfreiheit konkret formulierter Anforderungen hinsichtlich der technischen Sicherheit, die bei der Entwicklung berücksichtigt werden müssen, begonnen werden. Dies erfolgte in Rücksprache mit der Landesbeauftragten für Datenschutz und Informationsfreiheit. Zurzeit wird das technische Sicherheitskonzept umgesetzt. Die inhaltliche Datenstruktur wird aufgebaut und die fachlichen Fragen werden mit der Landesbeauftragten für Datenschutz und Informationsfreiheit kommuniziert.

Zu den Vorlagen für ein Lösch- und ein Auswertungskonzept wurde seitens der Landesbeauftragten für Datenschutz und Informationsfreiheit am 29. Juni 2018 Stellung genommen. Entsprechend dieser Stellungnahme wird das weitere Verfahren angepasst.

Bezüglich einer Verbindung der Datenbank zur Nachfolgesoftware OK-JUG kann noch keine Aussage getroffen werden. Zum jetzigen Zeitpunkt läuft das Testungs- und Auswahlverfahren für die neue Software. Eine Entscheidung hierüber steht daher noch aus. Die Einarbeitung der Datenbank Haaranalyse wird zu einem späteren Zeitpunkt als Anforderung formuliert werden.

8.3 Verarbeitung bei der Haaranalyse im Amt für Soziale Dienste

Die „Einwilligungs- und Schweigepflichtentbindungserklärung zur Durchführung einer Haaranalyse“ in Verbindung mit den Anlagen „Einwilligungserklärung zur Erfassung von Sozialdaten von substituierten bzw. drogenabhängigen Eltern und deren Kindern in der Datenbank Haaranalysen des Amtes für Soziale Dienste/ Abteilung Kinder- und Jugendnotdienst des Jugendamtes“ und „Protokoll über die Entnahme einer Haarprobe“ wurde am 24. Januar 2018 mit der Landesbeauftragten für Datenschutz und Informationsfreiheit abgestimmt und als Fachliche Mitteilung „F04 2018 Einwilligungs- und Schweigepflichtentbindungserklärung“ für die Durchführung einer Haaranalyse mit ausfüllbaren Anlagen im Handbuch „Hilfen zur Erziehung“ hinterlegt. Die Einarbeitung des Löschkonzeptes für die Datenspeicherung in der Datenbank Haaranalyse wird in einem zweiten Schritt angepasst, sobald die neue Datenbank in Betrieb genommen wird.

8.5 Vergabe von Mitteln des Europäischen Sozialfonds (ESF)

Die ESF-Prüfbehörde ist organisatorisch der Senatorin für Finanzen zugeordnet und nimmt zu dem aus dem Jahr 2015 stammenden Vorgang wie folgt Stellung:

Bezüglich der Ausführungen zur ESF-Prüfbehörde ist der Sachverhalt in Ziffer 8.5 des 40. Jahresdatenschutzberichts unzutreffend dargestellt.

Die ESF-Prüfbehörde erlässt keinerlei Regelungen für die Förderung aus dem ESF-Fonds. Sie richtet ihre Prüftätigkeiten gemäß Artikel 127 der VO (EU) 1303/2013 an den Regularien der Europäischen Kommission und den nationalen Bestimmungen für die Gewährung von Zuwendungen aus und prüft deren Einhaltung durch die Verwaltungsbehörde, deren zwischengeschalteter Stelle und den Zuwendungsempfängerinnen und Zuwendungsempfängern. Gegenüber den Zuwendungsempfängerinnen und Zuwendungsempfängern besteht gemäß Artikel 127 der VO (EU) 1303/2013 i. V. m. Artikel 27 der VO (EU) 480/2014 ein Prüfrecht der ESF-Prüfbehörde. Darüber hinaus steht die Prüfbehörde in keinerlei Verbindung zu den Zuwendungsempfängerinnen und Zuwendungsempfängern oder den Maßnahmeteilnehmern.

Die ESF-Prüfbehörde hat aus den oben genannten Gründen kein eigenes Interesse an personenbezogenen Daten der Maßnahmeteilnehmer. Insofern ist es unzutreffend, dass die ESF-Prüfbehörde eine Vereinbarung mit den Beratungsstellen getroffen habe, mit der die Prüfbehörde bis zu zehn Prozent anonyme Beratungen akzeptiere. Eine solche Regelung wäre nicht mit den geltenden Bestimmungen der Europäischen Kommission und auch nicht mit den Bestimmungen der Bremischen Landeshaushaltsordnung vereinbar. Nach Auskunft der ESF-Verwaltungsbehörde hat die Europäische Kommission eine entsprechende Abrechnung anonymer Beratungen im ESF-Fonds abgelehnt.

Auch die Aussage, wonach die Prüfbehörde keine Möglichkeit habe, „datenschutzfreundlichere Lösungen umzusetzen“, ist falsch, da die Prüfbehörde nicht für die Verwaltung der Fondsmittel und den damit in Zusammenhang stehenden organisatorischen Maßnahmen zuständig ist.

Ebenso ist die in Ziffer 8.5 des 40. Jahresberichts der Landesbeauftragten für Datenschutz genannte Zusage der ESF-Prüfbehörde, eine Überarbeitung des Informationsblattes für Teilnehmerinnen und Teilnehmer durchzuführen, nicht mit dem durch die Europäische Kommission definierten Aufgabengebiet der Prüfbehörden vereinbar und würde einen unbefugten Eingriff in das Aufgabengebiet der ESF-Verwaltungsbehörde darstellen.

8.8 Jugendberufsagentur

Die Landesbeauftragte für Datenschutz und Informationsfreiheit wurde von Anfang an in die Planungen und Überlegungen zum Modelprojekt eingebunden, um eine rechtskonforme Ausgestaltung des Projekts sicherzustellen. Die Senatorin für Kinder und Bildung hat sich intensiv mit der Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit zu einem ersten Projektzielbild, das die Bundesagentur für Arbeit im Oktober 2017 vorlegte, auseinandergesetzt und ihrerseits zu den Anmerkungen der Landesbeauftragten Stellung genommen. Inzwischen hat die Bundesagentur für Arbeit Vertragsentwürfe übersandt, die von der Senatorin für Kinder und Bildung überarbeitet bzw. kommentiert wurden. Dabei wurden bereits einigen der von der Landesbeauftragten für Datenschutz und Informationsfreiheit im Vorfeld geäußerten Bedenken Rechnung getragen. Beide Varianten liegen der Landesbeauftragten für Datenschutz mit der Möglichkeit der Stellungnahme vor. Es ist auch aus Sicht der Senatorin für Kinder und Bildung weiterhin angezeigt, die Landesbeauftragte für Datenschutz eng in den Verfahrensgang miteinzubinden.

8.9 Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte

Seit Einführung der Software für das Bewohner- und Quartiersmanagement besteht ein laufender Kontakt zur Landesbeauftragten für Datenschutz und Informationsfreiheit. Dies wird in dem Bericht deutlich. Auch hinsichtlich der noch bestehenden datenschutzrechtlichen Bedenken ist dies der Fall und es werden alle Anstrengungen unternommen, auf Hinweise zeitnah zu reagieren.

Im Einzelnen:

Schaffung einer Möglichkeit der anonymen Speicherung der Essendaten:

Eine Speicherung der Essensdaten ohne Personenbezug ist zurzeit noch nicht möglich. Der Hersteller des Programms wurde mit der Lösung dieses Problems beauftragt, so dass zeitnah mit einer Anonymisierung der Daten zu rechnen ist.

Abschaffung des Moduls zur Speicherung der Anwesenheitsdaten von Mitarbeiterinnen und Mitarbeitern:

Wie im Bericht vermerkt, wird diese Möglichkeit der Datenspeicherung von den Einrichtungen bislang nicht genutzt. Der Hinweis wurde jedoch aufgenommen und mit den Trägern der Einrichtungen besprochen. Die Abschaltung dieses Moduls wurde dabei vereinbart bzw. veranlasst.

Speicherung von Gesundheitsdaten/Speicherung der Religionszugehörigkeit:

Datenschutzrechtliche Bedenken bestehen hinsichtlich des uneingeschränkten Zugriffs auf das Freitexteingabefeld „andere Behinderungen“ und auf die Erfassung der Religionszugehörigkeit. Eine Umbenennung des Textfeldes „andere Behinderungen“ in „andere Einschränkungen“ ist bereits umgesetzt und steht seit dem Update am 6. April 2018 zur Verfügung. Die im 40. Jahresdatenschutzbericht angeregte Maßnahme, für beide Felder den Zugriff auf die Leitung der jeweiligen Unterkunft zu beschränken, kann nicht umgesetzt werden, da diese Informationen für die Planung der Belegung der Unterkünfte unbedingt erforderlich sind.

Löschroutinen der vorhandenen Datensätze:

An der Lösung des Problems wird weiterhin gearbeitet.

9. Beschäftigtendatenschutz

9.1 Beschäftigtendatenschutz nach DSGVO und BDSG-neu

Die Ausführungen der Landesbeauftragten für Datenschutz und Informationsfreiheit zur Datenverarbeitung im Beschäftigungskontext nach dem Bundesdatenschutzgesetz betreffen gemäß dessen Geltungsbereich die Beschäftigten in der öffentlichen Verwaltung des Bundes sowie die Beschäftigten privater Arbeitgeberinnen und Arbeitgeber. Die Verarbeitung von personenbezogenen Daten im Beschäftigungskontext der Beschäftigten des bremischen öffentlichen Dienstes erfolgt gemäß § 12 des Bremischen Ausführungsgesetzes zur EU-Datenschutzgrundverordnung nach Maßgabe der personalaktenrechtlichen Vorschriften des Bremischen Beamtengesetzes.

Die Anpassung der personalaktenrechtlichen Vorschriften des Bremischen Beamtengesetzes an die EU-Datenschutzgrundverordnung wird derzeit mit dem Entwurf eines Gesetzes zur Änderung dienstrechtlicher Vorschriften zur Anpassung an die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) sowie zur Änderung weiterer dienstrechtlicher Vorschriften verfolgt. Die zweite und abschließende Senatsbefassung zu dem Entwurf ist im September 2018 geplant, sodass der Gesetzentwurf vom Senat voraussichtlich noch in der zweiten Jahreshälfte 2018 der Bremischen Bürgerschaft (Landtag) zugeleitet werden kann.

9.2 Zugriff auf Personalaktendaten

Die von der Landesbeauftragten für Datenschutz und Informationsfreiheit angesprochenen Mängel wurden kurzfristig abgestellt. Nunmehr ist das Modul „Personalverwaltung“ einer umfassenden Personalmanagementsoftware (PMS) im Wirkbetrieb. Mit der PMS lassen sich die erforderlichen Maßnahmen zum Datenschutz sowie zur Kommunikations- und Datensicherheit einheitlich und zentral durchführen. Die Nutzung der PMS erfolgt innerhalb des Rahmens einer Verfahrensbeschreibung, die mit einer zwischen der Amtsleitung und dem Personalrat der Feuerwehr Bremen abgeschlossenen Dienstvereinbarung eingeführt wurde. Die PMS ist noch nicht vollumfänglich importiert, weil ein störungsfreier Betrieb nur mit einer schrittweisen Einführung gewährleistet werden kann. Das Verfahren soll noch im diesen Jahr abgeschlossen werden. Die behördliche Datenschutzbeauftragte ist in den Prozess eng mit eingebunden.

9.3 Aufzeichnung von Telefongesprächen

Die Feuerwehr Bremen hat die Aufzeichnungen sämtlicher bei der Feuerwehr Bremen über den Amtsanschluss (3030-0) eingehenden Telefongespräche gestoppt. Da eine Aufzeichnung bei bestimmten Rufnummern im Einzelfall zwingend erforderlich ist, wird zurzeit gemeinsam mit der behördlichen Datenschutzbeauftragten an einer Lösung gearbeitet. Eine entsprechende Verfahrensbeschreibung wird derzeit erarbeitet. Sobald nähere Einzelheiten vorliegen, wird die Landesbeauftragte für Datenschutz und Informationsfreiheit in das Verfahren mit eingebunden.

13. Verkehr und Umwelt

13.1 Personenbezogene Daten in automatisierten und vernetzten Fahrzeugen

13.1.3 Kooperative intelligente Verkehrssysteme

Hinsichtlich der Nutzung kooperativer intelligenter Verkehrssysteme für Verkehrslenkung und zur Verkehrssicherheit als Aufgaben der Polizei Bremen besteht im Land Bremen derzeit kein konkreter Planungsstand.