BREMISCHE BÜRGERSCHAFT **Drucksache 20/1103**
Landtag **(zu Drs. 20/891)**
20. Wahlperiode **14.09.2021**

Mitteilung des Senats

Stellungnahme des Senats zum 3. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung

Mitteilung des Senats
an die Bremische Bürgerschaft (Landtag)
vom 14. September 2021

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum 3. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung (Berichtszeitraum: 1. Januar 2020 bis 31. Dezember 2020) 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.

Durch die ab dem 25. Mai 2018 unmittelbar anzuwendende Europäische Datenschutzgrundverordnung (DSGVO) wurde die Berichtspflicht der Landesbeauftragten für Datenschutz und Informationsfreiheit mit Art. 59 DSGVO auf eine neue rechtliche Grundlage gestellt. Art. 59 DSGVO verpflichtet die Landesbeauftragte für Datenschutz und Informationsfreiheit zur jährlichen Berichterstattung. Die jährliche Berichtspflicht wurde im Land Bremen bereits durch § 33 Abs. 1 des Bremischen Datenschutzgesetzes in der bis zum 24. Mai 2018 geltenden Fassung sichergestellt.

Der Jahresbericht soll bezüglich der Tätigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit Transparenz schaffen. Folglich muss der Jahresbericht einen Überblick über die Wahrnehmung der Aufgaben nach Art. 57 DSGVO enthalten. Im Jahresbericht kann sowohl über maßgebliche Entwicklungen in der Datenverarbeitung als auch über die Wahrnehmung der Rechte der Betroffenen berichtet werden. Der Jahresbericht räumt der Landesbeauftragten für Datenschutz und Informationsfreiheit die Möglichkeit ein, die Arten der gemeldeten Verstöße sowie der getroffenen Maßnahmen zu veröffentlichen. Von dieser Möglichkeit hat die Landesbeauftragte für Datenschutz und Informationsfreiheit im vorliegenden 3. Jahresbericht Gebrauch gemacht.

Gemäß § 22 des Bremischen Ausführungsgesetzes zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) vom 8. Mai 2018 (Brem.GBl. S. 131) legt der Senat der Bremischen Bürgerschaft (Landtag) seine Stellungnahme zu dem Tätigkeitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit vor.

Die Stellungnahme zum 3. Jahresbericht der Landesbeauftragten für Datenschutz ist als Anlage beigefügt

Beschlussempfehlung:

Anlage(n):
1. Anlage Stellungnahme Datenschutz

4. Datenschutzbeauftragte

4.2 Befristung der Benennung von Datenschutzbeauftragten

Der von der Landesbeauftragten für Datenschutz und Informationsfreiheit beschriebene Fall in Bremerhaven fällt nicht in den Zuständigkeitsbereich des Magistrats. Vielmehr ist eine eigenständige öffentliche Einrichtung in Bremerhaven betroffen. Diese nimmt zum konkreten Einzelfall wie folgt Stellung:
Die Tätigkeit der oder des Datenschutzbeauftragten wurde zunächst von einer beschäftigten Person der Einrichtung wahrgenommen. Nachdem diese das Amt niedergelegt hatte, wurde eine Firma mit der Wahrnehmung der datenschutzrechtlichen Aufgabe betraut und das Auftragsverhältnis zunächst auf ein Jahr befristet. Zwischenzeitlich konnte man sich von den Leistungen der Firma überzeugen, so dass ein langfristiger Vertrag abgeschlossen werden soll.

4.3 Kündigungsschutz des Datenschutzbeauftragten bei bremischen öffentlichen Stellen

Der Senatskommissar für den Datenschutz wird die Änderungsbitte der Landesbeauftragten für Datenschutz und Informationsfreiheit zum BremDSGVOAG bezüglich der Übernahme der Regelung des § 6 Abs. 4 des Bundesdatenschutzgesetzes ins Landesrecht prüfen und der Landesbeauftragten das Prüfergebnis zuleiten.

5. Inneres

5.1 Gemeldete Datenschutzverletzungen

Zur Protokollierung des Zugriffs auf polizeiliche Informationssysteme gilt Folgendes:

INPOL-Land stellt ein zentrales polizeiliches Informationssystem für die Polizei Bremen und die Ortspolizeibehörde Bremerhaven dar. Um eine eindeutige Identifizierung der abfragenden Person zu gewährleisten, wurde vor Jahren ein Authentifizierungsprotokoll implementiert, das in der Lage ist sowohl Anfragen der Polizei Bremen als auch Anfragen der Ortspolizeibehörde Bremerhaven zu verarbeiten.

Die im Juni des Berichtsjahres entdeckte Sicherheitslücke erlaubt Mitarbeitenden, die über erweiterte Rechte verfügen, sich unter einer fremden Kennung bei INPOL-Land anzumelden und Anfragen abzusetzen. Das genutzte Authentifizierungsprotokoll (Finger) übergibt die am PC angemeldete Nutzerkennung an die Fachanwendung. Dabei wird allerdings ein weniger privilegierter Systemparameter genutzt, der nicht auf Fernzugriffe reagiert und auch nicht mit Administrationsrechten manipuliert werden kann. Neben der Nutzerauthentifizierung protokolliert INPOL zusätzlich die IP-Adresse des abfragenden PC-Arbeitsplatzes. Über diese kann der Rechner eindeutig identifiziert werden. Aufgrund der lokalen Protokollierung auf dem identifizierten PC wird die Ermittlung der im Zeitpunkt der Abfrage angemeldeten nutzenden Person ermöglicht. Somit kann eine Nachverfolgbarkeit des Zugriffs über Umwegen und mit einem höheren Prüfaufwand erfolgen. Gleichwohl muss die Problematik der Protokollierung von Zugriffen nachhaltig gelöst werden. Hierzu ist bereits ein Projekt zur Ablösung des veralteten Authentifizierungsprotokolls geplant.

Zum zwischenzeitlichen Verlust von Online-Strafanzeigen im Zusammenhang mit der Online-Wache gilt Folgendes:

Der zwischenzeitliche Verlust von 22 Strafanzeigen, die online gestellt wurden, war auf eine Kommunikationsstörung zwischen den lokalen E-Mail-Postfächern der Polizei Bremen sowie den Servern beim Dienstleister Dataport zurückzuführen. Die Ursache für die Kommunikationsstörung konnte zwischen den Beteiligten Dataport, der Brekom und der Polizei Bremen im Ergebnis nicht ermittelt werden. Die Administratoren der Polizei Bremen haben durch eine Anpassung der internen Konfiguration der betroffenen E-Mail-Postfächer diese für die externen Server des Dienstleisters Dataport wieder erreichbar gemacht. Durch eine Auswertung der Protokolldateien konnten alle Anzeigenden erfolgreich kontaktiert und um eine wiederholte Anzeige gebeten werden.

5.2 Mobile Datenverarbeitung bei der Polizei

Das angeführte Rechte- und Rollenkonzept zum sog. digitalen Notizbuch wurde der Landesbeauftragten für Datenschutz und Informationsfreiheit zwischenzeitlich in der novellierten Fassung (Version 1.1) zur Prüfung zur Verfügung gestellt.

Zudem wurde der Ausweisscan, der Empfehlung der Landesbeauftragten folgend, bisher nicht in den Testbetrieb eingeführt. An einer datenschutzrechtlich abgestimmten Lösung wird im Projekt @rtus-Mobile weiterhin gearbeitet. Zunächst ist jedoch ein generelles Hemmnis der Bereitstellung, der für den Ausweisscan vorgesehenen Software / Applikation, zu beseitigen. Sobald sich eine Lösung abzeichnet, wird der begonnene Dialog mit der Landesbeauftragten für Datenschutz und Informationsfreiheit und den behördlichen Datenschutzbeauftragten der beteiligten Dienststellen mit dem Ziel der Etablierung einer datenschutzkonformen Lösung für einen Ausweisscan fortgesetzt.

5.3 Das neue Polizeirecht

Das Bremische Polizeigesetz wurde aus der Mitte der Bremischen Bürgerschaft in das parlamentarische Verfahren gegeben und nicht als Gesetzentwurf des Senats. Folglich wären die von der Landesbeauftragten für Datenschutz und Informationsfreiheit geäußerten verfassungsrechtlichen Bedenken in der Bürgerschaft (Landtag) zu erörtern.

Ungeachtet dessen orientieren sich die Vorschriften des Bremischen Polizeigesetzes an den Vorschriften des Bundeskriminalamtgesetzes und der hierzu ergangenen Rechtsprechung des Bundesverfassungsgerichts. Dies steht im Einklang mit der Vorgehensweise in allen anderen Bundesländern und ist dem Informationsverbund geschuldet, der insbesondere vom Bundeskriminalamt geprägt wird.

Zu neu geschaffenen Regelungen zur Überwachung von Telekommunikation (TKÜ) gilt Folgendes:

Der Landesbeauftragten für Datenschutz und Informationsfreiheit wurde vom Senator für Inneres bereits dargelegt, zuletzt im August 2020 mit der Bitte um Bewertung der TKÜ-Verwaltungskooperation, dass sich die von ihr angesprochenen Mängel tech-

nisch nicht beheben lassen. Die Konstruktion der Telekommunikationsanlage ermöglicht die von der Landesbeauftragten für Datenschutz und Informationsfreiheit geforderten Anforderungen nicht. Der rechtliche Hinweis der Landesbeauftragten, die Telekommunikationsanlage bis zur Aufhebung der Mängel nicht zu nutzen, hätte zur Folge, dass für strafprozessuale und ggf. polizeiliche Telekommunikationsmaßnahmen etwa im Bereich des politischen Extremismus oder der Organisierten Kriminalität die Freie Hansestadt Bremen keine Maßnahmen mehr beziehungsweise – sofern überhaupt aus Kapazitätsgründen oder technisch möglich – allenfalls über andere Länder (sofern dort die Mandantentrennung möglich wäre) nachrangig diese Maßnahmen durchführen könnte.

Aufgrund der Kündigung des Supports durch den Anlagenhersteller „Syborg“ können notwendige größere Änderungen an Hard- und Software der Anlage nicht mehr vorangetrieben werden. Mithin befindet sich die Inbetriebnahme einer neuen TKÜ-Anlage im Rahmen des RDZ (Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer) in der Umsetzungsphase. Die aus der Nutzung des vorherigen TKÜ-Systems „Syborg“ verbliebenen datenschutzbezogenen Mängel sollten durch die Implementierung der neuen TKÜ-Anlage im Rahmen des RDZ behoben werden. Entgegen ursprünglicher Planungen verzögert sich die Aufnahme des Wirkbetriebes der datenschutzkonformen Technik des RDZ jedoch mindestens bis zum November 2022.

Durch den verspäteten Start des RDZ wird die Syborg-Anlage für die Umsetzung von TKÜ-Maßnahmen auf Grundlage der Strafprozessordnung weiterhin genutzt. Andere oder tiefergreifendere Verstöße gegen die datenschutzrechtlichen Vorgaben sind für TKÜ-Maßnahmen nicht ersichtlich. Die Notwendigkeit einer datenschutzrechtlichen Unterscheidung zwischen Maßnahmen nach der Strafprozessordnung und dem Bremischen Polizeigesetz ist aus fachlicher Sicht insofern nicht geboten.

Zu der Nutzung von sog. Bodycams gilt Folgendes:

Bei der Ermöglichung des sog. Pre-Recording körpernah getragener Videoaufzeichnungsgeräte (Bodycams) in Wohnungen durch das Bremische Polizeigesetz handelt es sich um eine bewusste Entscheidung des bremischen Gesetzgebers, der das Gesetz aus der Mitte der Bürgerschaft in das Gesetzgebungsverfahren eingebracht hat. Die amtliche Gesetzesbegründung, wonach hiermit insbesondere Fällen der häuslichen Gewalt besser begegnet werden soll, ist schlüssig. Die Maßnahme steht unter dem Vorbehalt, Leib und Leben von Personen zu schützen.

Gem. Ziffer 4.3 der entsprechenden Dienstanweisung zur Nutzung der sog. Bodycams tragen alle kameraführenden Beamt:innen eine Weste mit dem Aufdruck „Videodokumentation“ oder haben entsprechende Schilder an ihrer Dienstkleidung befestigt. Dem polizeilichen Gegenüber sowie unbeteiligten Dritten wird somit umgehend optisch mitgeteilt, dass die jeweiligen Beamt:innen entsprechende Bild- und Tonaufzeichnungen vornehmen. Die sichtbar angebrachte Bodycam erweckt bei Dritten somit bereits den Eindruck, dass Aufzeichnungen erfolgen. Eine verdeckte Aufzeichnung findet demnach nicht statt.

Die Nutzung des Pre-Recordings dient ausschließlich dazu, die Annäherung an einen unklaren Sachverhalt aufzuzeichnen. Vor dem Einschalten der Pre-Recording

Funktion müssen die rechtlichen Voraussetzungen zur Anfertigung von Bildaufzeichnungen gegeben sein. Tatsächlich gelangen die Daten in einen sogenannten „flüchtigen Datenspeicher“ der sich alle 60 Sekunden selbst überschreibt. Die Daten sind somit nach 60 Sekunden grundsätzlich automatisch gelöscht. Soweit Bildaufnahmen gesichert werden sollen, muss die Aufnahmetaste gedrückt werden. Nach Drücken der Aufnahmetaste werden die Bildaufnahmen der letzten 60 Sekunden nicht gelöscht, sondern selbständig durch die Bodycam von der eigentlichen, sich regelmäßig überschreibenden Aufnahme kopiert und gespeichert.

Gemäß Ziffer 5 der Dienstanweisung zur Nutzung der Bodycams ist das anlasslose Filmen während der Dienstverrichtung untersagt. Das Aktivieren der Bodycam ist grundsätzlich anzukündigen, sofern die oder der Adressat:in der Maßnahme auch kommunikativ ansprechbar ist. Die Ankündigung, die Bodycam einzuschalten, erfolgt grundsätzlich vor einer entsprechenden Einsatzsituation, spätestens jedoch im Zeitpunkt des Beginns der Aufzeichnung.

5.5 Projekt Deradikalisierung und Extremismusprävention mit Schwerpunkt Islamismus/Salafismus

In einer Arbeitsgruppe wird unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit sowie Vertreter:innen der Senatorin für Kinder und Bildung und der Senatorin für Justiz und Verfassung eine Mustervorlage einer Einwilligungserklärung und einer Schweigepflichtentbindungserklärung erarbeitet. Die Mustervorlage wird den betroffenen Institutionen abschließend zur Verfügung gestellt.

5.7 Vertraulichkeit der Corona-Quarantänekontrolle

Das von der Landesbeauftragten für Datenschutz und Informationsfreiheit beschriebene Spannungsfeld ist im Ordnungsamt bekannt und ebenfalls festgestellt worden. Die Mitarbeitenden wurden zwischenzeitlich entsprechend sensibilisiert und geschult beim Umgang mit den besonders schützenswerten Gesundheitsdaten der Quarantäneverpflichteten.

5.8 Einsatz von Security-Unternehmen in BürgerServiceCentern

Es liegt eine gemeinsame Verantwortlichkeit im Sinne des Art. 26 DSGVO vor. Das Bürgeramt ist im Rahmen einer Vereinbarung über die gemeinsamen Verantwortlichkeiten nach Art. 26 Abs. 1 Satz 3 DSGO die einheitliche Anlaufstelle und Ansprechpartner für alle datenschutzrechtlichen Fragestellungen und stimmt die weiteren Verfahren ab. Dies gilt auch für den Bereich des Sicherheitsdienstes, der im Auftrag der senatorischen Dienststelle und Immobilien Bremen seine Aufgaben in der Gebäudesicherung versieht.

5.9 Alternierende Telearbeit bei der Polizei Bremen

Zur Problematik der alternierenden Telearbeit bei der Polizei Bremen gilt Folgendes:

Die alternierende Telearbeit startete 2018 im Rahmen einer Testphase mit 6 Teilnehmer:innen. Mit Überführung in die „Allgemeine Ablauf Organisation“ (AAO) und Einstellung eines Koordinators Telearbeit wurde die Telearbeit bei der Polizei sukzessive ausgebaut. Mittlerweile nehmen rund 50 Mitarbeiter:innen am Arbeitsmodell der

alternierenden Telearbeit teil. Die zukünftige Ausgestaltung und ein etwaiger Ausbau der alternierenden Telearbeit bei der Polizei Bremen sind aktuell Gegenstand interner Prüfungen.

6. Justiz

6.2 Gemeldete Datenschutzverletzungen

Die Senatorin für Justiz und Verfassung nimmt aufgrund der Zuständigkeit ihres Geschäftsbereichs für aufsichtsrechtliche Maßnahmen für die bremischen Notar:innen nach § 92 der Bundesnotarordnung wie folgt Stellung:

Der von der Landesbeauftragten für Datenschutz und Informationsfreiheit gezogenen Schlussfolgerung, allein aus der geringen Zahl der von Notar:innen proaktiv gemeldeten Verletzungen nach Art. 33 DSGVO auf eine angebliche Verletzung der gesetzlichen Pflicht zur Meldung von Datenpannen zu schließen, kann nicht gefolgt werden. Vielmehr hat der europäische Verordnungsgeber die Notwendigkeit gesehen, die Meldepflicht unter den Vorbehalt einer Qualifizierung des Datenschutzverstoßes zu stellen und die Meldung nicht für jede Verletzung einer Datenschutzregelung vorzusehen, sondern nur für eine solche Verletzung, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Demnach bedarf es einer Prognose zu den Folgen des Datenschutzverstoßes durch die meldepflichtige verantwortliche Stelle.

Die Senatorin für Justiz und Verfassung geht somit davon aus, dass die bremischen Notar:innen ihrer Meldepflicht nach Art. 33 DSGVO vollumfänglich nachgekommen sind. Anhaltspunkte, die auf Gegenteiliges schließen lassen könnten, sind nicht ersichtlich und wurden von der Landesbeauftragten für Datenschutz und Informationsfreiheit auch nicht angezeigt. Es ist außerdem darauf hinzuweisen, dass die Notar:innen berufsrechtlich zu besonderer Verschwiegenheit verpflichtet sind und ein besonders sorgsamer Umgang mit personenbezogenen Daten zur Routine in der notariellen Tätigkeit zählt und daher eine besondere Sensibilität für dieses Thema besteht.

Für die Staatsanwaltschaft und die bremischen Gerichte – soweit die nicht justizielle Tätigkeit betroffen ist - gilt Folgendes:

Auch hier darf nicht aufgrund nicht gemeldeter Fälle auf einen Verstoß gegen Art. 33 DSGVO ohne Vorliegen weiterer Anhaltspunkte geschlossen werden.

Die Tätigkeiten in den Gerichten und Staatsanwaltschaften werden unterstützt durch IT-Fachverfahren, die das Schreibwerk für die Verfahrensbeteiligten erstellen, wodurch Fehler weitgehend ausgeschlossen werden. Auch die Mitarbeiter:innen in den Dienststellen sind sich der besonderen Schutzbedürftigkeit der verarbeiteten personenbezogenen Daten bewusst und gehen verantwortungsvoll damit um.

Für die Gerichte besteht für den justiziellen Bereich, der den Hauptteil der Verarbeitung personenbezogener Daten ausmacht, gemäß Art 55 Abs. 3 DSGVO auch gar

keine Meldepflicht gegenüber der Landesbeauftragten für den Datenschutz und Informationsfreiheit, so dass sich insofern erst Recht der Schluss von ausbleibenden Meldungen auf potentielle Verstöße verbietet.

6.4 Auskunftsanspruch bei der Staatsanwaltschaft

Die Staatsanwaltschaft Bremen hat nach Aufklärung des Sachverhalts der Landesbeauftragten für Datenschutz und Informationsfreiheit mit Schreiben vom 17. März 2021 entsprechend berichtet. Folglich ist der Vorgang aus dem Jahr 2020 abgeschlossen.

Hinsichtlich des Vorgangs aus dem Jahr 2018 hat die Staatsanwaltschaft Bremen ebenfalls zwischenzeitlich mit Schreiben vom 30. April 2021 gegenüber der Landesbeauftragten für Datenschutz und Informationsfreiheit ausführlich Stellung genommen.

Die Mitarbeiter:innen der Staatsanwaltschaft werden regelmäßig im Rahmen von Einarbeitungen, Besprechungen und Fortbildungen im Hinblick auf die Anwendung der IT-Fachverfahren und der Verarbeitung personenbezogener Daten datenschutzrechtlich sensibilisiert.

Zudem hat die Generalstaatsanwältin infolge der zwei Beanstandungen aus den Jahren 2018 und 2020 im Rahmen der Dienstaufsicht eine ordnungsgemäße Sachbearbeitung von Auskunftsersuchen und Anfragen der Landesbeauftragten für Datenschutz und Informationsfreiheit gegenüber dem Leitenden Oberstaatsanwalt angemahnt.

Die Aufarbeitung des Vorgangs aus dem Jahr 2020 hat gezeigt, dass die Staatsanwaltschaft die Anfragen der Petentin durchaus angemessen bearbeitet hat, so dass keine weitergehenden Maßnahmen veranlasst sind.

6.5 Umsetzung der Richtlinie (EU) 2016/680 für den Strafvollzug, die Strafgerichte und die Staatsanwaltschaft

Zur Abstimmung der Entwurfsfassung des Bremischen Justizvollzugsdatenschutzgesetzes gilt Folgendes:

Die Notwendigkeit zur Beteiligung und Abstimmung der entsprechenden Senatsvorlage richtet sich nach § 8 der Geschäftsordnung des Senats und den in der Geschäftsverteilung im Senat geregelten und hier betroffenen Ressortzuständigkeiten. Zu dem seinerzeit bestehenden Entwurf eines Bremischen Justizvollzugsdatenschutzgesetzes wurden der Senator für Inneres, der Senator für Finanzen, die Senatorin für Gesundheit, Frauen und Verbraucherschutz, die Justizvollzugsanstalt Bremen, die Landesbeauftragte für Datenschutz und Informationsfreiheit und das Hanseatische Oberlandesgericht in Bremen frühzeitig angehört und beteiligt. Die Abstimmung erfolgte zuletzt abschließend mit dem Senatskommissar für den Datenschutz. Sofern danach noch strittige Punkte verblieben, wurden diese gemäß § 18 Abs. 3 der Geschäftsordnung des Senats in der Senatsvorlage dargestellt.
Eine formelle Abstimmung in allen Einzelheiten mit der Landesbeauftragten für Datenschutz und Informationsfreiheit bedurfte es aus Rechtsgründen schon nicht. Hiervon unabhängig wurde in der Senatsvorlage 396/20 (vgl. Sitzung des Senats am

7. April 2020) aus Transparenzgründen auf die umfangreiche Beteiligung der Landesbeauftragten für Datenschutz und Informationsfreiheit und ihre weiter bestehenden Kritikpunkte vollumfänglich hingewiesen.

Bezüglich des Entwurfs eines Bremischen Strafjustizdatenschutzgesetzes gilt Folgendes:

Im Bereich der Strafgerichte und der Staatsanwaltschaft erfolgte mit der Einführung des § 500 der Strafprozessordnung (StPO) mit Wirkung vom 26. November 2019 eine Umsetzung der JI-Richtlinie durch Bundesrecht. Eine Anpassung durch den Bundesgesetzgeber war auch erforderlich, da die Gerichte und Staatsanwaltschaften im Hinblick auf das Strafgesetzbuch und die StPO Bundesrecht anwenden. Die Frage, ob neben der bereits erfolgten vollständigen Umsetzung der JI-Richtlinie weiterer Normierungsbedarf durch landesrechtliche Vorschriften im Bereich des Justizdatenschutzrechts angezeigt sein könnte, ist Gegenstand von politischen Erörterungen zwischen den zuständigen Ressorts.

7. Gesundheit

7.2 Unzulässige Weitergabe von Corona-Daten durch die Gesundheitsämter an die Polizei

Seit dem 8. April 2020 werden personenbezogene Daten oder pseudonymisierte Daten über Listen von Covid-19-infizierten Personen nicht mehr vom Gesundheitsamt Bremen an die Polizei Bremen übermittelt. Personenbezogene Daten erhält ausschließlich das zuständige Ordnungsamt. Die an die Polizei Bremen übermittelten Datensätze wurden nach schriftlicher Mitteilung des betreffenden Lagezentrums des Krisenstabes aus den polizeilichen Systemen vollständig gelöscht; sie liegen bei der Polizei Bremen nicht mehr vor, so dass die möglichen nachteiligen Auswirkungen der Datenübermittlung abgemildert werden konnten. Alle betroffenen Personen wurden im April 2020 vom Gesundheitsamt Bremen schriftlich über die Übermittlung ihrer Daten an die Polizei Bremen informiert.

7.3 Veröffentlichung von Corona-Fallzahlen

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz veröffentlicht alle 14 Tage Corona-Fallzahlen auf Stadtteilebene. Zu Beginn wurden die Fallzahlen auf der räumlichen Ebene von Postleitzahlen veröffentlicht. Da sich diese räumliche Einheit nicht mit den administrativen Grenzen von Stadtteilen deckt, wurde auf die Darstellung auf Stadtteilebene gewechselt. Bei der Veröffentlichung der Zahlen werden die datenschutzrechtlichen Empfehlungen umgesetzt. Fallzahlen von weniger als 5 pro räumliche Einheit werden nicht veröffentlicht und nicht in die Berechnung gewichteter Zahlen mit aktuellen Bevölkerungszahlen einbezogen. Zudem ist die Bevölkerungszahl in den bremischen Stadtteilen ausreichend hoch, so dass kein Personenbezug mehr hergestellt werden kann. In Stadtteilen mit niedrigen Einwohnerzahlen

werden keine Fallzahlen veröffentlicht. Hierzu zählen die Stadtteile Häfen, Seehausen und Strom.

7.4 Nutzung von Corona-Daten zu Forschungszwecken

In beiden genannten Forschungsvorhaben, durchgeführt durch das Leibniz-Institut für Präventionsforschung und Epidemiologie (BIPS) in Bremen, wurden die datenschutzrechtlichen Empfehlungen umgesetzt. Bei beiden Projekten wird sichergestellt, dass personenbezogene Daten ausschließlich von autorisiertem Personal im Gesundheitsamt verarbeitet und nicht an das BIPS übermittelt werden.

7.5 Meldung von negativen Corona-Testergebnissen

Derzeit werden von den Laboren die „Negativ-Meldungen“ kumuliert an das Robert-Koch-Institut gemeldet. Weder das Gesundheitsamt Bremen noch das Landeskompetenzzentrum Infektionsepidemiologie erhalten die Meldungen über das System Demis aus den Laboren. Eine namentliche Einzelmeldung ist auch im Ergebnis nicht zielführend. Allerdings hilft die Gesamtzahl der durchgeführten Tests, also auch die Zahl der negativ ausgefallenen Tests, die Lage generell zu beurteilen, da es einen Unterschied macht, ob 5 von 100 oder 5 von 1.000 Tests positiv sind.

7.6 Fund des Belegungsplanes einer psychiatrischen Station auf offener Straße

Infolge des festgestellten Datenschutzverstoßes, der ausschließlich aufgrund einer individuellen Nachlässigkeit erfolgt ist, wurden folgende Maßnahmen umgesetzt, um ein entsprechendes individuelles Fehlverhalten zukünftig ausschließen zu können:

- In den Besprechungen und bei Übergaben erfolgen regelmäßig und vermehrt Hinweise auf den Datenschutz.
- Es wurden Prozessanweisungen bezüglich des Umgangs mit Verlegungslisten erarbeitet.
- Es erfolgen zweimal jährlich Datenschutzschulungen für das Klinikpersonal.
- Die Direktionsleitung des Krankenhauses hat an alle Mitarbeiter:innen datenschutzrechtliche Merkblätter ausgegeben.

8. Soziales

8.1 Gemeldete Datenschutzverletzungen

Die Senatorin für Soziales, Jugend, Integration und Sport nimmt die Stellungnahme der Landesbeauftragten für Datenschutz und Informationsfreiheit zum Anlass zu prüfen, ob es im Ressort zu unterlassenen Meldungen von Datenschutzverstößen nach Art. 33 DSGVO gekommen ist. Diesbezüglich steht das Ressort im engen Austausch

mit dem Datenschutzdienstleister Datenschutz Nord GmbH. Die Prüfung ist noch nicht abgeschlossen.

8.4 Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte

Zu dem Vorgang nimmt die Senatorin für Soziales, Jugend, Integration und Sport wie folgt Stellung:

Freitextfeld:

Die Anpassung des Freitextfeldes wurde mit Release vom 8. Februar 2021 in der Testumgebung umgesetzt. Da diese Version in einigen Punkten nicht den Anforderungen genügte, mussten vom Hersteller noch Verbesserungen vorgenommen werden. Inzwischen liegt eine überarbeitete Version vor, die bereits produktiv gesetzt wurde.

Speicherung der Essensdaten:

Seit dem 1. Februar 2021 werden die Essensdaten bereits nach 96 Stunden gelöscht, statt wie bisher nach 14 Tagen.

Aufbewahrungsfristen, Fachverfahren der Zentrale Aufnahmestelle für Asylbewerber und Flüchtlinge im Land Bremen (ZASt), Datenschutzkonzept und Löschkonzept:

Nach § 7 Abs. 1 des Asylgesetzes dürfen die mit der Ausführung des Asylgesetzes betrauten Behörden zum Zwecke der Ausführung des Gesetzes personenbezogene Daten erheben, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.
Da die ZASt ihre Aufgaben nur in enger Kooperation mit anderen Behörden auf Landes- und Bundesebene erfüllen kann, die am Asylverfahren und an Verfahren nach § 15 a Aufenthaltsgesetz (AufenthG) beteiligt sind, beträgt die Aufbewahrungsfrist für die elektronischen Fallakten der ZASt nach Auffassung der Senatorin für Soziales, Jugend, Integration und Sport - analog zu den Aufbewahrungsfristen des Bundesamtes für Migration und Flüchtlinge und der Ausländerbehörden - 10 Jahre (vgl. § 91 AufenthG).

Ab dem 1. Januar 2022 haben alle Behörden des Landes ihre Akten elektronisch zu führen (vgl. § 6 des Gesetzes zur Förderung der elektronischen Verwaltung in Bremen vom 20. März 2018). Durch die Einführung von Bewohner- und Quartiersmanagementsoftware (BQM) als Fachverfahren und E-Akte wurde hierzu für den Aufgabenbereich der ZASt die Voraussetzung geschaffen.

Diese und andere Rechtsgrundlagen zu diesem Vorgang wurden der Landesbeauftragten für Datenschutz und Informationsfreiheit seit 2019 mehrfach, zuletzt mit Schreiben vom 5. Januar 2021, mitgeteilt.

Die vom Dienstleister Datenschutz Nord GmbH überarbeitete Version des Datenschutzkonzepts wurde mit Schreiben vom 26. April 2021 der Landesbeauftragten für

Datenschutz und Informationsfreiheit zwischenzeitlich zugeleitet. Die Nutzung bestimmter BQM-Daten im Fachverfahren für die ZASt wurde in die überarbeitete Version des Datenschutzkonzeptes aufgenommen.

Das geforderte Löschkonzept ist inzwischen ebenfalls fertiggestellt. In diesem werden die Rechtsgrundlagen ebenfalls thematisiert.

Ortsbesichtigungstermin in der Landeserstaufnahmestelle (LASt):

Die im Bericht angesprochene Ortsbesichtigung am 11. September 2019 fand in der Landeserstaufnahmestelle in der Lindenstraße statt. Es ging bei diesem Treffen nicht um die Arbeitsabläufe in der ZASt, sondern um Fragen an die Einrichtungsleitung der AWO und an den Sicherheitsdienst bezüglich des Umgangs mit Bewohner:innendaten.

9. Bildung

9.2 Digitale Lernplattform

Die Nutzer:innenzahlen sind durch die Corona-Pandemie und die damit verbundene Situation um das acht- bis neunfache angestiegen. Von der Stabsstelle Digitalisierung sind zahlreiche Unterstützungsangebote in verschiedenen Formen (Sprechstunden, Handreichungen, Selbstlernpfade, Erklär-Videos) entwickelt und weit über 100 Fortbildungen durchgeführt worden. Die Sicherheit der Lehrkräfte im Umgang mit der Plattform ist dadurch signifikant gestiegen.

Das Datenschutzkonzept wird an den notwendigen Stellen zeitnah überarbeitet und an die aktuellen Anforderungen angepasst.

9.3 YouTube-Inhalt als verpflichtender Hausaufgabenbestandteil

Auf YouTube finden sich viele qualitativ hochwertige Erklär-Videos, die Schüler:innen Unterrichtsinhalte didaktisch sinnvoll vermitteln. Gleichzeitig ist der Abfluss der Nutzer:innendaten in die USA problematisch. Die Stabsstelle Digitalisierung weist in Fortbildungen regelmäßig auf dieses Problem hin und stellt mit medien.online ein reichhaltiges Angebot an Bildmaterial datenschutzkonform zur Verfügung. Parallel dazu ist eine vergleichbare Streaming-Plattform im Rahmen des DigitalPakt Schule in Planung.

9.5 Datenschutzwidriger Umgang mit Klassenbüchern in Papierform

Die Senatorin für Kinder und Bildung und der behördliche Datenschutzbeauftragte der senatorischen Dienststelle haben von dem konkreten Sachverhalt keine Kenntnis und können den Vorgang deshalb auch nicht rechtlich bewerten.

9.6 Videokonferenzsysteme im Schulkontext

Mit der Einführung von Cisco Webex als einheitlicher Videokonferenzlösung für die öffentlichen Schulen der Freien Hansestadt Bremen wurde eine sichere und datenschutzkonforme Lösung implementiert.

9.7 Unzulässiges schulisch organisiertes "Freundebuch" der Klasse

Die Senatorin für Kinder und Bildung und der behördliche Datenschutzbeauftragte der senatorischen Dienststelle haben von dem konkreten Sachverhalt keine Kenntnis. Gleichzeitig teilen die Senatorin für Kinder und Bildung und der behördliche Datenschutzbeauftragte die von der Landesbeauftragten für Datenschutz und Informationsfreiheit dargelegten datenschutzrechtlichen Bedenken uneingeschränkt. Für eine Prüfung des Sachverhaltes ist allerdings relevant, wer eigentlicher Initiator dieser Maßnahme gewesen ist und ob gegebenenfalls sogar dafür eine Einwilligung seitens der Schule bei den Erziehungsberechtigten eingeholt wurde und wie eingehend das Privatleben der Kinder und ihrer Eltern in den Tagebucheinträgen beschrieben wurde. Daher ist die Senatorin für Kinder und Bildung hier auf weitere Informationen zum Sachverhalt angewiesen.

9.8 iPads für Schülerinnen und Schüler

Auf Grundlage der Beratung der Landesbeauftragten für Datenschutz und Informationsfreiheit wurden in Zusammenarbeit mit dem Dienstleister Datenschutz Nord GmbH, dem behördlichen Datenschutzbeauftragten der Senatorin für Kinder und Bildung und den öffentlichen Schulen entsprechende Prozesse, Formblätter, Informationsschreiben und Auftragsdatenverarbeitungsverhältnisse erstellt, um den Datenschutzanforderungen im Rahmen der schulischen iPad-Nutzung gerecht zu werden.

9.9 Nutzung eigener privater Endgeräte für schulische Zwecke

Durch die flächendeckende Ausstattung der Schüler:innen und Lehrkräfte der öffentlichen Schulen mit iPads besteht die Notwendigkeit der Nutzung privater Endgeräte für schulische Zwecke nicht mehr.

9.10 Online-Portal zur Leseförderung

Die Schulen sind angehalten, die Namen der Schüler:innen so zu anonymisieren, dass durch Externe kein Rückschluss auf einzelne Personen erfolgen kann. Zukünftig soll hierfür eine automatische Anonymisierung über eine Schnittstelle zum Identitätsmanagementsystem der Schulen realisiert werden. Des Weiteren rät die Stabsstelle Digitalisierung den Schulen dazu, die Eltern über die Nutzung von Antolin zu informieren. Einer Einwilligung durch die Schüler:innen bzw. deren Erziehungsberechtigte bedarf es nicht, weil nach § 4 Abs. 1 Satz 1 des Bremischen Schuldatenschutzgesetzes die Datenverarbeitung für die Erfüllung des Unterrichts- und Erziehungsauftrages an der Schule erforderlich ist.

9.11 Datenweitergabe für schulische Wettbewerbe an die Veranstalter

Welchen mathematischen Wettbewerb die Landesbeauftragte für Datenschutz und Informationsfreiheit im konkreten Fall anspricht, ist der Senatorin für Kinder und Bildung nicht bekannt. Ungeachtet dessen gilt Folgendes:

Grundsätzlich ist die Teilnahme von Schüler:innen an Wettbewerben gewünscht (vgl. Richtlinie für Schülerwettbewerbe vom 29. Juni 2015); sie sind Teil der Strategie der Bildungsbehörde zur Förderung leistungsstarker und besonders leistungsfähiger Schüler:innen. Nach Inkrafttreten der DSGVO haben die Anbieter:innen der von der Kultusministerkonferenz empfohlenen Wettbewerbe (vgl. Liste vom 1. März 2018 im Anhang der Empfehlung der Kultusministerkonferenz „Qualitätskriterien für Schülerwettbewerbe“ vom 17. September 2009) ihre Teilnahmebedingungen sorgfältig überarbeitet und an die Vorschriften der DSGVO angepasst. Dies gilt auch für die dort aufgeführten Mathematik-Wettbewerbe. In der Regel wird nunmehr bereits im (Online-)Anmeldevorgang die Einwilligung der Schüler:innen bzw. der Erziehungsberechtigten zur Datennutzung/Bildrechten u.a. abgefragt. Ohne diese Einwilligung ist eine Teilnahme am Wettbewerb entsprechend nicht möglich. Bei Aufgabenwettbewerben, die im Klassenverband absolviert werden, können Schüler:innen, die keine Einwilligung erteilt haben, zwar Aufgaben lösen. Diese werden aber nicht zur Wettbewerbsteilnahme eingesendet. Die Datenschutzregelungen werden bei Wettbewerben, für die die Bildungsbehörde Landeskoordinator:innen einsetzt, von diesen zusätzlich an die Lehrkräfte und Teilnehmenden kommuniziert. Trotz anfänglich großer Herausforderungen etabliert sich in der Praxis mittlerweile ein zunehmend selbstverständlicher und akzeptierender Umgang mit den durch die DSGVO erforderlichen neuen Prozessen.

10. Beschäftigtendatenschutz

10.2 Microsoft 365

Microsoft 365 wird im Rahmen der Bereitstellung von BASIS.bremen-PC nicht eingesetzt. Die durch Microsoft 365 im speziellen bereitgestellten zusätzlichen Dienste, wie z. B. die Geräte- und Anwendungsverwaltung oder Identitäts- und Zugriffsverwaltung, die für den Einsatz der hier beschriebenen Module eine Voraussetzung darstellen, werden im Rahmen von BASIS.bremen und SIS.bremen durch den Dienstleister Dataport selbst betrieben.

10.3 Nutzung privater Endgeräte im Beschäftigungskontext

In der Verwaltung der Freien Hansestadt Bremen (Land und Stadtgemeinde Bremen) werden sowohl im stationären (Arbeitsplatzcomputer) als auch im mobilen Bereich (Notebooks, Smartphones, Tablets) für dienstliche Zwecke ausschließlich dienstliche IT-Endgeräte eingesetzt.

10.4 Nutzung privater Telefonnummern im Rahmen von Heimarbeit und Telearbeit

Die Auffassung der Landesbeauftragten für Datenschutz und Informationsfreiheit wird geteilt. Ergänzend wird darauf hingewiesen, dass eine Herausgabe der privaten Telefonnummer von Beschäftigten an Dritte im Rahmen der Erfüllung ihrer Pflichten aus dem Arbeitsverhältnis beziehungsweise Dienstverhältnis aufgrund der Möglichkeit einer Rufumleitung vom Diensttelefon auf das Privattelefon in der Regel ohnehin nicht notwendig ist. Unabhängig davon sollten die Personalstellen der Dienststellen und im Rahmen der Corona-Pandemie die jeweiligen Vorgesetzten jedoch Kenntnis der privaten Telefonnummer der Beschäftigten haben, um diese im Bedarfsfall anrufen zu

können. Bei Anrufen vom privaten Telefon besteht die Möglichkeit, die Rufnummernunterdrückung einzuschalten, so dass die private Telefonnummer nicht sichtbar wird. Eine Nutzung der ausschließlich dienstlichen Rufnummern im Homeoffice (ein- und abgehend) wäre dann zu gewährleisten, wenn die Rufnummern durchgehend auf fünfstellige Durchwahlnummern im zentralen Telekommunikationssystem der bremischen Verwaltung umgestellt wären. Die Umsetzung dieses Rufnummernkonzeptes ist im Aufbau, so dass diese Funktion derzeit nur teilweise zur Verfügung gestellt werden konnte. Des Weiteren können die Dienststellen ihren Mitarbeitenden dienstliche Smartphones mit Flatrates aus den Verträgen des zentralen Dienstleisters zur Kommunikation mit dem zentralen Telekommunikationssystem der bremischen Verwaltung zur Verfügung stellen.

Die Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau teilt für ihre Dienststelle ergänzend mit, dass aufgrund des akuten Infektionsgeschehens die Mitarbeitenden kurzfristig gebeten wurden, möglichst im Homeoffice zu arbeiten. Kurzfristig konnte das Problem der Nutzung privater Telefonnummern aus technischen und lizenzrechtlichen Gründen jedoch nicht gelöst werden. Deshalb wurden die Mitarbeitenden per Rundmail diesbezüglich sensibilisiert und darum gebeten, an ihren Endgeräten die Rufnummernübertragung auf “anonym“ zu stellen.

Der Bevollmächtigte Bremens beim Bund führt hierzu aus, dass im Falle des Homeoffice und der nicht zur Verfügung stehenden dienstlichen Telefongeräte entsprechende Rückrufbitten über E-Mails erfolgen, so dass private Telefonnummern der Beschäftigten nicht herausgegeben werden müssen.

10.5 OpenTouch Conversation in Behörden

Die Landesbeauftragte für Datenschutz und Informationsfreiheit stellt fest, dass ihres Wissens weder ein Datenschutzkonzept noch eine Dienstvereinbarung zu den Status-Einstellungen der CTI-Software OpenTouch Conversation (OTC) existieren. Der Senator für Finanzen erläutert hierzu, dass er im Herbst 2016 ein Mitbestimmungsverfahren gemäß „Dienstvereinbarung über die Gestaltung und Nutzung von Telekommunikationsanlagen, Sprachübertragung über das Kommunikationsnetz der bremischen Verwaltung und Mobilfunkgeräten“ (Anlage 1b) hinsichtlich der Nutzung der CTI-Funktionen für Standard-Büroarbeitsplätze sowie die freiwillige Nutzung der Präsenzinformationen des Telekommunikationssystems durchgeführt hat.
Alle Dienststellen sowie die Schulen der Freien Hansestadt Bremen wurden mit Rundschreiben 02/2017 vom 20. Januar 2017 vom Senator für Finanzen über die Ergebnisse dieses Verfahrens und über die Status-Einstellmöglichkeiten bei OTC informiert. Die Kommunikation zwischen den Dienststellen findet weiterhin über das im Einsatz befindliche zentrale E-Mail-System statt. Für weitere Systeme oder Funktionstools liegen derzeit keine zentral verbindlichen Vorgaben zur Nutzung im Regelbetrieb vor.

16. Bauen und Wohnen

16.4 Luftbildaufnahmen

Die zuständige Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau prüft, ob die von der Landesbeauftragten für Datenschutz und Informationsfreiheit geforderten Mitteilungen an die Betroffenen bezüglich der Bildflüge

seitens des Landesamtes für Geoinformation erfolgt ist. Dabei wird auch die bestehende Verwaltungspraxis im Land Bremen hinsichtlich der behördlich veranlassten Bildüberflüge abzuklären und gegebenenfalls datenschutzkonform anzupassen sein. Über das Ergebnis der Prüfung wird die Landesbeauftragte für Datenschutz und Informationsfreiheit unverzüglich unterrichtet.

17. Verkehr und Umwelt

17.2 Ausbau A 281 – Datenweitergabe durch Projektverantwortliche

Der im Jahresbericht geschilderte Vorgang beinhaltete die Weitergabe von Adressen der betroffen Bürger:innen zur Durchführung von Beweissicherungsmaßnahmen im Zuge des Baus der A 281. Die Stabstelle der Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau hat seinerzeit den Sachverhalt aufgeklärt und dabei keine datenschutzrechtlichen Verstöße festgestellt. Dabei war die Frage zu prüfen, ob die Zuständigkeit für die Behandlung der Beschwerde bei der Landesbeauftragten für Datenschutz und Informationsfreiheit oder beim Bundesbeauftragten für den Datenschutz lag.

Hinsichtlich der Frage der datenschutzrechtlichen Verantwortlichkeiten im Hinblick auf das Bauprojekt der A 281 gilt Folgendes:

Zum 1. Januar 2021 ist die Zuständigkeit für die Bundesfernstraßen auf die Autobahngesellschaft des Bundes bzw. auf das Fernstraßenbundesamt übergangen. Dieser Zuständigkeitswechsel hat sämtliche bisher bestehenden Vertragsregelungen zwischen der Freien Hansestadt Bremen und der Projektverantwortlichen DEGES beinhaltet. Eine neue Vereinbarung nach Art. 26 DSGVO zwischen dem Bundesverkehrsministerium als Bauherrin, der DEGES und der Senatorin für Klimaschutz, Umwelt, Mobilität, Stadtentwicklung und Wohnungsbau ist nach Auffassung der senatorischen Behörde nicht notwendig.

18. Telemedien

18.3 Überprüfung des Einsatzes von Analyse-Tools

Hierzu wird auf die Stellungnahme des Senats zum 2. Jahresbericht der Landesbeauftragten für Datenschutz nach der EU-Datenschutzgrundverordnung zu Ziffer 18.2 „Verwendung von Trackingtools und Analysetools auf Webseiten“ verwiesen.