BREMISCHE BÜRGERSCHAFT **Drucksache 21/1352**
Landtag (zu Drs. 21/1108)
21. Wahlperiode 16.09.2025

Mitteilung des Senats vom 16. September 2025

Stellungnahme des Senats zum 7. Jahresbericht des Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung über den Datenschutz im Jahr 2024 im Land Bremen

Der Senat übermittelt der Bürgerschaft (Landtag) seine nachfolgende Stellungnahme zum 7. Jahresbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit nach der Europäischen Datenschutzgrundverordnung (DSGVO) (Berichtszeitraum: 1. Januar 2024 bis 31. Dezember 2024) mit der Bitte um Kenntnisnahme.

Die Sicherung der verfassungsrechtlich verbürgten informationellen Selbstbestimmung der Bürger:innen 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 der Landesbeauftragte für Datenschutz und Informationsfreiheit berechtigte Kritik übte. Der Senat hat zur Lösung dieser Fälle in Abstimmung mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Maßnahmen zum Schutz personenbezogener Daten ergriffen und bekräftigt seine Absicht, dies auch künftig zu tun.

Artikel 59 Datenschutzgrundverordnung verpflichtet den Landesbeauftragten für Datenschutz und Informationsfreiheit zur jährlichen Berichterstattung.

Der Jahresbericht soll bezüglich der Tätigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit Transparenz schaffen. Folglich muss der Jahresbericht einen Überblick über die Wahrnehmung der Aufgaben nach Artikel 57 Datenschutzgrundverordnung 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 dem Landesbeauftragten für Datenschutz und Informationsfreiheit die Möglichkeit ein, die Arten der gemeldeten Verstöße sowie der getroffenen Maßnahmen zu veröffentlichen. Von dieser

Möglichkeit hat der Landesbeauftragte für Datenschutz und Informationsfreiheit im vorliegenden 7. Jahresbericht Gebrauch gemacht.

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

4. Datenschutzbeauftragte und Allgemeines öffentliche Stellen

4.4 Microsoft 365

Die vom Landesbeauftragten für Datenschutz und Informationsfreiheit dargestellten datenschutzrechtlichen Herausforderungen hat der Senator für Finanzen ebenfalls erkannt.

Daher wird der Senator für Finanzen sich zusätzlicher Maßnahmen bedienen, mit der ein datenschutzkonformer Einsatz von Microsoft 365 in der bremischen Verwaltung erfolgen kann. Er wird auch die Erfahrungen aus anderen Ländern bei der Einführung von Microsoft 365 nutzen. Daraus ergeben sich folgende Maßnahmen:

— Abschluss eines gesonderten Auftragsverarbeitungsvertrags mit Microsoft, mit dem die Einhaltung europäischen Rechts gewährleistet wird.

— Eine weitestgehende Einhaltung der „EU Boundary“, nach der Daten den europäischen Wirtschaftsraum grundsätzlich nicht verlassen. Dazu hält Microsoft im europäischen Wirtschaftsraum ausreichende Rechenzentrumskapazitäten vor.

— Die Beibehaltung der bisherigen Speicherorte, insbesondere für personenbezogene Daten, das heißt vor Ort im Rechenzentrum von Dataport.

— Die Nutzung von Online-Speichern (insbesondere One Drive oder Sharepoint Online) soll bis auf weiteres nicht für einen Schutzbedarf oberhalb von „normal“ erfolgen und technisch unterbunden werden. Damit dieses nachhaltig geschieht, erfolgt der Einsatz nur im gemanagten BASIS Umfeld.

In Bereichen, in denen ein Einsatz von Microsoft 365 unter den genannten Gesichtspunkten nicht empfehlenswert ist, können die Dienststellen auf die klassische „Office 2024“ zurückgreifen.

Der Senator für Finanzen prüft zudem die Notwendigkeit, inwieweit bestehenden Restrisiken in einer Datenschutzfolgeabschätzung mit weiteren Maßnahmen entgegenzuwirken ist.

4.5 VIS Einheitsmandant

Allgemeines:

Der Senator für Finanzen hat den Landesbeauftragten für Datenschutz und Informationsfreiheit bereits seit dem Jahr 2018, also vor Beginn des Projektes für den VIS-Einheitsmandanten, initiativ einbezogen und auch in den Folgejahren regelmäßig über den Stand des Projekts informiert. Die Stellungnahmen des Landesbeauftragten für Datenschutz und Informationsfreiheit wurden in jeder Phase des Projektes berücksichtigt und sind in die umfangreichen technischen und organisatorischen Maßnahmen eingeflossen, die zur Verwirklichung des Einheitsmandanten vorgenommen worden sind.

Bislang hat der Landesbeauftragte für Datenschutz und Informationsfreiheit den VIS-Einheitsmandanten unter bestimmten Voraussetzungen für grundsätzlich umsetzbar erachtet (vergleiche etwa 4. Jahresbericht Datenschutz zum Berichtsjahr 2021, Seite 34). In der Endphase des Projektes hat er diese Einschätzung kurzfristig geändert und vertritt seitdem die im 7. Jahresbericht dargelegte Auffassung, wonach der Einheitsmandant datenschutzrechtlich grundsätzlich nicht zulässig sei.

Im Einzelnen:

Im Hinblick auf die Speicherung von Schriftgut wird im 7. Jahresbericht ausgeführt, dass das digitale Schriftgut der bremischen Verwaltung übergreifend in einem einzigen Mandanten gebündelt gespeichert und verarbeitet werde. Hierzu sei das Systemdesign von VIS nicht ohne Weiteres geeignet, eine datenschutzkonforme, gemeinsame Nutzung in einem Einheitsmandanten zu realisieren. Mit diesen Ausführungen erweckt der Landesbeauftragte für Datenschutz und Informationsfreiheit den Eindruck, der Einheitsmandant bündele alle innerhalb der Behörden anfallenden Informationen; folglich würden alle personenbezogenen Daten wie von einer „Datenkrake“ zusammengezogen. Diese Auffassung verkennt nach Auffassung des Senators für Finanzen, dass auf dem Einheitsmandanten nur ein Teil der Verwaltungsdokumente bearbeitet wird. Der weitaus größere Teil der personenbezogenen Daten wird in speziellen Fachverfahren, in eigenen Mandanten sowie in anderen Systemen verarbeitet, ohne Verbindung zum Einheitsmandanten herzustellen. Innerhalb des Einheitsmandanten sind umfangreiche technische und organisatorische Vorkehrungen getroffen worden, welche die datenschutzkonforme Nutzung sicherstellen.

Im Hinblick auf die Zusammenarbeit innerhalb des aktenführenden Systems wird im 7. Jahresbericht ausgeführt, dass mit sogenannten Geschäftsgangverfügungen Schriftgut für Adressaten der eigenen Dienststelle und für Adressaten anderer Dienststellen zugänglich gemacht

werden könnte, obwohl für die adressierten Beschäftigten keine Zugriffsberechtigung bestünde.

Es trifft zu, dass Geschäftsgangverfügungen erlassen werden können, die über Dienststellengrenzen hinweg Zugriffe erlauben. Darin besteht gerade der Hauptzweck des Einheitsmandanten. Der Hauptzweck stellt das Arbeiten in einem sicheren und geschützten System dar, welches für eine dienststellenübergreifende Kommunikation nicht verlassen werden muss. Für dieses dienststellenübergreifende Arbeiten wurden umfangreiche datenschutzrechtliche Vorkehrungen getroffen, wie zum Beispiel das Prinzip der Vier-Augen-Prüfung. Entsprechende getroffene datenschutzrechtliche Vorkehrungen bleiben jedoch im 7. Jahresbericht unerwähnt.

Soweit der Landesbeauftragte für Datenschutz und Informationsfreiheit im 7. Jahresbericht das Fehlen einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Bürger:innen sowie der Beschäftigten der bremischen Verwaltung im VIS-Einheitsmandanten anmahnt, gilt Folgendes:

Die Rechtsgrundlage zur Verarbeitung personenbezogener Daten im VIS-Einheitsmandanten ergibt sich aus § 3 Absatz 1 Nummer 2 des Bremischen Ausführungsgesetzes zur EU-Datenschutzgrundverordnung in Verbindung mit dem Geschäftsverteilungsplan des Senats, der auf Artikel 120 der Landesverfassung beruht. Keine Rechtsgrundlage stellt dagegen § 85 des Bremischen Beamtengesetzes dar, da sich die Vorschrift auf Personalaktendaten bezieht. Dies wurde im weiteren Projektverlauf gegenüber dem Landesbeauftragten für Datenschutz und Informationsfreiheit auch mehrfach dargelegt.

Bei der Nutzung des VIS-Einheitsmandanten sind alle Dienststellen, also sowohl der „Absender“ als auch der „Adressat“ einer Geschäftsgangverfügung, an die zwingenden rechtlichen Vorgaben für die Datenverarbeitung innerhalb der Verwaltung gebunden, da es sich um ein rein verwaltungsinternes System handelt. Geschäftsgangverfügungen sind – anders als zum Beispiel die bisher notwendigen Abstimmungen per E-Mail – aus sich heraus nachvollziehbar und revisionssicher und verhindern Dritten, die außerhalb der Verwaltung stehen, den Einblick in die Unterlagen. Ein Einblick durch Dritte außerhalb der Verwaltung ist auch dann nicht möglich, wenn als Adressat einer Geschäftsgangverfügung versehentlich eine solche externe Person eingetragen würde. Auch hierdurch zeigt sich, dass die Nutzung des VIS-Einheitsmandanten gegenüber bisherigen elektronischen Abstimmungsprozessen in der bremischen Verwaltung, die zum Beispiel über einen E-Mail-Verkehr erfolgt sind, aus datenschutzrechtlicher Sicht einen deutlichen höheren Standard des Datenschutzes gewährleistet.

Soweit im 7. Jahresbericht keine ausreichenden Maßnahmen gegen mögliche Verstöße gegen die Datenschutzgrundverordnung durch die Nutzung des VIS-Einheitsmandanten angemahnt werden, gilt Folgendes:

Die für den Einheitsmandanten getroffenen technischen und organisatorischen Maßnahmen waren insbesondere zentrale Bestandteile des Projektes und des fortwährenden Austauschs mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit.

Der Hinweis im 7. Jahresbericht, wonach die Kontrolle durch die behördlichen Datenschutzbeauftragten im Hinblick auf die Verarbeitung personenbezogener Daten im VIS-Einheitsmandanten nicht gewährleistet sei, ist nicht nachvollziehbar. Bislang sind keine Anhaltspunkte bekannt, wonach die Nutzung des VIS-Einheitsmandanten die Kontrollrechte der behördlichen Datenschutzbeauftragten eingeschränkt hätten.

Abschließend ist festzustellen, dass der Senator für Finanzen die im 7. Jahresbericht dargestellten datenschutzrechtlichen Bedenken des Landesbeauftragten für Datenschutz und Informationsfreiheit zum VIS-Einheitsmandanten ausdrücklich nicht teilt. Vielmehr sieht der Senator für Finanzen in der Nutzung des VIS-Einheitsmandanten eine datenschutzkonforme Nutzung von Abstimmungsprozessen innerhalb der bremischen Verwaltung.

5. Inneres

5.1 Gemeldete Datenschutzverletzungen

Im Jahr 2024 wurden seitens der Polizei Bremen drei Verletzungen des Schutzes personenbezogener Daten gemeldet.

Dabei handelte sich um folgende Vorgänge:

1. Eine dienstliche E-Mail mit dem Inhalt der Meldung wichtiger Ereignisse erreichte aufgrund eines Büroversehens vier Beschäftigte des bremischen öffentlichen Dienstes außerhalb des polizeilichen Adressatenkreises. Die E-Mail wurde zurückgerufen und die vier betroffenen Beschäftigten wurden zusätzlich gebeten, die E-Mail unverzüglich zu löschen. Zudem wurde der behördliche Datenschutzbeauftragte unverzüglich über den Vorfall informiert. Dieser veranlasste in Abstimmung mit der Behördenleitung sodann eine Meldung an den Landesbeauftragten für Datenschutz und Informationsfreiheit. Die Beschäftigten wurden im Rahmen der Aufklärung des Vorgangs erneut auf die Einhaltung der datenschutzrechtlichen Bestimmungen hingewiesen.

2. Ebenfalls aufgrund eines Büroversehens wurde seitens der Polizei Bremen bei der Übersendung eines monatlich erscheinenden Newsletters über Präventionsthemen an circa 1 100 Abonnentinnen und

Abonnenten nicht - wie eigentlich erforderlich - die Funktion „Bcc“ genutzt, sodass alle E-Mail-Adressen allen Beziehern des Newsletters zur Kenntnis gelangen konnte. Selbstverständlich hat sich der Versender des Newsletters für sein Versäumnis bei den Betroffenen entschuldigt. Zudem wurde das Thema in der Organisationseinheit besprochen, um weiteren Verstößen vorzubeugen. Künftig wird für die Versendung des Newsletters eine Kollegin fest eingesetzt. Der behördliche Datenschutzbeauftragte wurde über den Vorgang unverzüglich informiert. Dieser veranlasste sodann in Abstimmung mit der Behördenleitung eine Meldung an den Landesbeauftragten für Datenschutz und Informationsfreiheit.

3. Schließlich wurde ein für den Kriminaldauerdienst vorgesehenes Protokoll aus dem Einsatzleitsystem versehentlich von einem Beschäftigten der Leitstelle an eine private E-Mail-Adresse einer Person mit dem gleichen Namen des Mitarbeiters der Leitstelle übersandt. Der Fehler erfolgte bei der Versendung einer beabsichtigten Test-E-Mail an die eigene persönliche Dienst-Mailadresse um die Möglichkeit einer Versendung aus dem System zu überprüfen. Hierbei wurde aufgrund eines Büroversehens statt der Endung „@polizei.bremen.de“ die Endung „@gmx.de“ in die Adresszeile eingefügt. Der betroffene Beschäftigte der Polizei verfügt selbst über eine private E-Mail-Adresse mit der Endung „@gmx.de“. Der Empfänger der E-Mail hat sich telefonisch bei der Polizei Bremen gemeldet und zugesichert, dass er die E-Mail unverzüglich gelöscht hat.

   Die Ortspolizeibehörde Bremerhaven hat im Jahr 2024 eine Datenschutzverletzung an den Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet. In diesem Zusammenhang wurde eine nicht verschlüsselte Festplatte mit Videosequenzen aus vermeintlich strafrechtlich relevanten Sachverhalten auf dem Postweg versandt. Später wurde festgestellt, dass die Festplatte nicht beim Empfänger eingetroffen ist. Interne Maßnahmen zum Auffinden der Festplatte verliefen negativ. Bisher hat die Ortspolizeibehörde Bremerhaven keine Kenntnis über die Folgen der Verletzung des Schutzes personenbezogener Daten erlangt. Der Vorgang wurde zum Anlass genommen den Umgang mit Datenträgern innerhalb der Ortspolizeibehörde Bremerhaven neu zu bewerten.

   Seitens des Bürgeramts Bremen wurden im Berichtsjahr Datenschutzverstöße im niedrigen einstelligen Bereich dem Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet.

   Seitens des Ordnungsamtes Bremen war im Berichtszeitraum ein Vorgang dem Landesbeauftragten für Datenschutz und Informationsfreiheit zu melden. Danach hatte eine Kollegin des Ordnungsamts infolge eines lokalen Drucks des Anschreibens an den

Bürger die Beweisbildanlage eines Schreibens versehentlich einem anderen Schriftstück beigefügt. Die Empfängerin der fälschlicherweise übermittelten Bilder wurde unverzüglich aufgefordert, diese zu vernichten.

5.2 Polizeiliche Videoüberwachungen

Allgemeines:

Wichtigster Auftrag der bremischen Polizeibehörden ist die Gewährleistung der öffentlichen Sicherheit und Ordnung sowie der Schutz der verfassungsmäßig garantierten Rechte und Freiheiten der Bürger:innen. In diesem Rahmen trifft die Polizei Bremen alle erforderlichen und verhältnismäßigen Maßnahmen unter Beachtung der gesetzlichen Vorgaben. Dabei orientiert sie sich an den Grundsätzen der Rechtsstaatlichkeit. Zur Wahrung der öffentlichen Sicherheit ist die Videoüberwachung ein wesentliches Instrument und dient insbesondere der Prävention sowie der schnellen Intervention im Falle sicherheitsrelevanter Ereignisse.

Die Polizei Bremen steht hinsichtlich ihrer durchgeführten und in Planung befindlichen Videoüberwachungsmaßnahmen in einem fortwährenden Austausch mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit und gewährleistet dabei stets ihre volle Kooperationsbereitschaft.

Zu den im 7. Jahresbericht seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit geäußerten Bedenken zur polizeilichen Videoüberwachung auf Volksfesten sowie an öffentlichen Plätzen gilt Folgendes:

Ausdehnung der Videoüberwachung auf Volksfesten und öffentlichen Plätzen:

Die polizeiliche Videoüberwachung stellt eine eingriffsintensive Maßnahme dar. Aus diesem Grund führt die Polizei Bremen im Vorfeld einer vorgesehenen Videoüberwachungsmaßnahme umfangreiche Prüfungen unter Berücksichtigung des Grundsatzes der Erforderlichkeit und Verhältnismäßigkeit durch. Darüber hinaus erfolgt eine kontinuierliche Evaluierung bestehender Maßnahmen.

Der Schutz der öffentlichen Sicherheit auf stark frequentierten (Groß-) Veranstaltungen wie zum Beispiel der Osterwiese, der Breminale, dem Freimarkt oder den Weihnachtsmärkten hat insbesondere vor dem Hintergrund vergangener (inter-)nationaler Schadensereignisse im Zusammenhang mit Volksfesten höchste Priorität. Dabei wird jeder Einsatz einer Videoüberwachung nach den Vorgaben des Bremischen Polizeigesetzes (§ 32 Absatz 3 Satz 1 Nummer 2 Bremisches Polizeigesetz [BremPolG]) durchgeführt und ist stets durch eine Gefahrenprognose

gestützt. Vor der Implementierung einer Videoüberwachung erfolgt eine umfassende Rechtsgüterabwägung, bei der die widerstreitenden Interessen und Grundrechte gegeneinander abgewogen werden. Bei den bereits realisierten Maßnahmen überwogen dabei höherrangige Rechtsgüter wie beispielsweise die körperliche Unversehrtheit und der Schutz des Eigentums gegenüber dem Recht auf informationelle Selbstbestimmung.

Darüber hinaus setzt die Polizei Bremen Videoüberwachungsmaßnahmen auf Grundlage des § 32 Absatz 3 Satz 1 Nummer 1 Bremisches Polizeigesetz ausschließlich an Standorten ein, die als Kriminalitäts-brennpunkte identifiziert wurden oder an denen aufgrund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist. Die Feststellung eines Kriminalitätsbrennpunktes erfolgt grundsätzlich auf Grundlage polizeilicher Erkenntnisse sowie eingegangener Bürger-beschwerden, die auf eine erhöhte sicherheitsrelevante Gefahrenlage in einem bestimmten Bereich hinweisen. Nach der ersten Bewertung der polizeilichen Lage erfolgt ein interner Entscheidungsprozess, welche polizeilichen Maßnahmen zur Reduzierung der Kriminalität durchgeführt werden können. Zur fundierten Beurteilung der Notwendigkeit wird eine Kriminalitätsanalyse erstellt. Ergibt diese eine signifikant sicherheits-relevante Belastung, wird neben anderen polizeilichen Maßnahmen auch eine Videoüberwachung in Erwägung gezogen. Bei der Entscheidung für eine Videoüberwachung erfolgen, neben der Erstellung eines Planungskonzeptes, umfangreiche Abstimmungen sowohl mit dem Senator für Inneres und Sport als auch mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Die Abstimmung umfasst unter anderem die Erstellung einer Datenschutzfolgeabschätzung, die Einholung von Stellungnahmen sowie die mündliche Einbindung in den Planungssachstand.

Die Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit, wonach die Geeignetheit der Videoüberwachung zur Erhöhung der Sicherheit auf Volksfesten und öffentlichen Plätzen grundsätzlich in Zweifel zu ziehen sei, wird nicht geteilt und ist auch durch empirische Forschung nicht belegt. Denn es sind auch generalpräventive Zwecke bei der Bewertung zu berücksichtigen. Der Normzweck des § 32 Bremisches Polizeigesetz und die darauf basierende Einrichtung einer Videoüberwachung dienen gerade der Abschreckung potenzieller Täterinnen und Täter und der damit verbundenen präventiven Verhinderung von Straftaten. Die repressive Wirkung der Maßnahme ist demgegenüber nachrangig.

Dazu lautet es in der einschlägigen Gesetzesbegründung zum Bremischen Polizeigesetz (vergleiche Bürgerschaftsdrucksache 20/511):

„Diese Maßnahmen der Videoüberwachung sind in erster Linie der Gefahrenvorsorge zuzurechnen. Insbesondere im Vorfeld terroristischer Straftaten sind Überwachungsmaßnahmen auch dann zulässig, wenn noch

kein konkretisiertes und zeitlich absehbares strafbares Geschehen oder eine konkrete Gefahr erkennbar ist. Der Staat darf bereits im Vorfeld von konkreten Gefahren Aktivitäten entfalten, um die Entstehung von Gefahren zu verhindern […]“.

Die bloße Präsenz einer Videoüberwachung, unabhängig von den konkret erfassten Sichtbereichen der jeweiligen Kameras, entfaltet grundsätzlich auch eine generalpräventive Wirkung. In Verbindung mit der entsprechenden Beschilderung, die außerhalb der jeweiligen Kamerasichtfelder auf eine offene Videobeobachtung hinweist, ist davon auszugehen, dass Personen – einschließlich potenzieller Tatbeteiligter – beim Betreten des überwachten Bereichs Kenntnis von der Videoaufzeichnung erlangen. Dieser Umstand kann eine präventiv abschreckende Wirkung entfalten.

Ein Beispiel hierfür stellt der mobile Videoanhänger der Polizei Bremen dar, dessen physische Präsenz schwer zu übersehen ist. Zwar könnten potenzielle Tatbeteiligte versuchen, sich der Erfassung gezielt zu entziehen und Straftaten außerhalb der überwachten Bereiche zu begehen. Gleichwohl deuten praktische polizeiliche Erfahrungen darauf hin, dass bereits die Wahrnehmung einer möglichen Videoüberwachung eine präventiv abschreckende Wirkung entfalten und die Tatbegehung im überwachten Nahbereich verringern kann. Dieser Effekt wurde evidenzbasiert zum Beispiel am Hillmannplatz festgestellt, wo die registrierten Straftaten während der Einsatzzeiten der Videoüberwachung um etwa 40 Prozent zurückgingen. Allein dies zeigt, dass die Videoüberwachung zur Erhöhung der Sicherheit beiträgt und deshalb als geeignet anzusehen ist.

Die Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit, wonach es bei einer Implementierung von Videoüberwachung in kleinen Ausschnitten vom Zufall abhänge, ob eine Tat von den Kameras erfasst würden, greift zu kurz. Die Platzierung der Videoüberwachung erfolgt nicht willkürlich, sondern basiert auf polizeilichen Erkenntnissen. Dadurch wird sichergestellt, dass Überwachungsmaßnahmen gezielt dort zum Einsatz kommen, wo mit einer erhöhten Wahrscheinlichkeit strafbare Handlungen zu erwarten sind. Tatbeteiligte wählen ihre Tatorte oft strategisch, sodass an bestimmten Örtlichkeiten oder im Rahmen von (Groß-) Veranstaltungen typischerweise eine höhere Delikt-wahrscheinlichkeit besteht. Die gezielte Videoüberwachung solcher Bereiche erhöht folglich die Wahrscheinlichkeit, sicherheitsrelevante Ereignisse aufzuzeichnen, erheblich. Zudem wird erneut auf die präventive Wirkung der Videoüberwachung hingewiesen.

Zudem ist angesichts der begrenzten Haushaltsmittel eine flächendeckende Videoüberwachung bereits finanziell nicht realisierbar. Insofern müssen die verfügbaren Ressourcen gezielt eingesetzt werden, um die öffentliche Sicherheit bestmöglich zu schützen. Eine vollständige Videoüberwachung von (Groß-) Veranstaltungen oder aller Bereiche in

einem Kriminalitätsbrennpunkt sind daher oft nicht realisierbar, sodass die Polizei gezwungen ist, punktuelle Maßnahmen zu ergreifen, die auf spezifische Gefahrenbereiche fokussiert sind. Dadurch wird die polizeiliche Videoüberwachung jedoch nicht ungeeignet.

Nach alledem bleibt festzuhalten, dass die Forderung des Landesbeauftragten für Datenschutz und Informationsfreiheit nach einer Änderung des Bremischen Polizeigesetzes dahingehend, dass eine Videoüberwachung von Volksfesten nur bei einer „ausreichenden Gefahrprognose“ zulässig sein soll, dem Willen des bremischen Gesetzgebers widerspricht. Zudem würde die Forderung des Landesbeauftragten für Datenschutz und Informationsfreiheit einer Gesetzesänderung zu einer Einschränkung die Flexibilität der Gefahrenabwehrmaßnahmen führen. Vielmehr sieht die derzeitige Gesetzeslage eine sorgfältige Prüfung vor und erfordert eine dokumentierte Begründung jeder Videoüberwachungsmaßnahme.

Bestehende Verfahrensprozesse zur Sicherstellung der Datenschutzkonformität:

Um die datenschutzrechtlichen Anforderungen zu erfüllen, werden die folgenden Prozesse vor einer Videoüberwachungsmaßnahme durchgeführt:

— Einbindung des behördlichen Datenschutzbeauftragten und der Zentralstelle für Datenschutz (Z 133) der Polizei Bremen in die Einsatzplanung bei datenschutzrelevanten Themen.

— Durch den behördlichen Datenschutzbeauftragten erfolgt eine Einbindung des Landesbeauftragten für Datenschutz und Informationsfreiheit.

— Vereinbarung von Vor-Ort-Terminen, um den Einsatzstandort zu bestimmen und datenschutzrechtlich zu bewerten.

— Erstellung einer Datenschutzfolgenabschätzung und einer Verfahrens- oder Dienstanweisung.

— Enge Begleitung der Fachabteilung zur Reduzierung von unbeabsichtigten Fehlern.

— Endabnahme aller datenschutzrelevanter Belange durch den behördlichen Datenschutzbeauftragten mithilfe einer Checkliste.

Einzelfälle zur Videoüberwachung der Polizei Bremen im Berichtsjahr 2024:

Zum Jahreswechsel 2023/2024 wurde der mobile Videoanhänger der Polizei Bremen an der Grohner Düne eingesetzt. Im vorliegenden Fall wurden die Gebäudebereiche (Fenster und Türen) nicht geschwärzt. Dies wurde im Rahmen der Nachbereitung aufgegriffen und wird bei künftigen

Maßnahmen berücksichtigt. Zudem wurde unverzüglich die Löschung der Aufzeichnungen beauftragt. Hinsichtlich der vorgeworfenen Nichtbeachtung der Tatbestandsvoraussetzungen des § 32 Absatz 1 Bremisches Polizeigesetz vertritt die Polizei Bremen die Rechtsauffassung, dass die Ereignisse in der Silvesternacht die Aktivierung der Videoüberwachung gerechtfertigt haben.

Bei der Bremer Osterwiese 2024 wurde erneut der mobile Videoanhänger der Polizei Bremen eingesetzt. Bei der Erhebung und der Übermittlung der Protokolldaten an den Landesbeauftragten für Datenschutz und Informationsfreiheit wurde durch diesen festgestellt, dass die Protokolle unvollständig waren. Trotz umfassender Prüfungen durch die Zentrale Polizeidirektion konnten die technischen Ursachen nicht abschließend geklärt oder im Detail rekonstruiert werden, sodass eine eindeutige Fehleranalyse nicht möglich war. Künftig wird der betreffende Prozess noch engmaschiger begleitet, um ein erneutes Auftreten fehlerhafter Protokolldatenübermittlungen frühzeitig zu erkennen und entsprechend gegensteuern zu können.

Im Rahmen einer sich bildenden Versammlung auf dem Bremer Marktplatz während des Weihnachtsmarkts stellten die Beschäftigten der Videoleitstelle der Polizei Bremen fest, dass sie nicht über die erforderliche technische Berechtigung verfügten, die Videoüberwachung zu deaktivieren oder in den „Demomodus“ zu versetzen. Sobald dieser Umstand bekannt wurde, wurden unverzüglich geeignete Maßnahmen ergriffen, wie das Herausschwenken der betroffenen Kamera sowie die Abschaltung der betreffenden Bildschirme, um eine Aufzeichnung oder eine Live-Übertragung der Versammlung zu verhindern. Eine vollständige Verhinderung der Aufzeichnung war jedoch nicht möglich, da ein Großteil der eingesetzten Kameras nicht schwenkbar war. Infolge dessen wurden die Versammlungsteilnehmenden zu Beginn der Veranstaltung durch Polizeibeamt:innen auf die bestehende Videoüberwachung hingewiesen. Der Veranstaltungsleiter nahm diese Information zur Kenntnis und erklärte, dass die Videoüberwachung die Durchführung der Veranstaltung in keiner Weise beeinträchtige. Im Anschluss an diesen Vorfall wurde das Berechtigungskonzept innerhalb der Polizei Bremen unverzüglich angepasst, sodass die Beschäftigten der Videoleitstelle in die Lage versetzt wurden, die einzelnen Kameras im Bedarfsfall deaktivieren zu können. Der Landesbeauftragte für Datenschutz und Informationsfreiheit wurde durch die Polizei Bremen über den Vorfall in Kenntnis gesetzt.

Durch die Ortspolizeibehörde Bremerhaven wurde eine Videoüberwachungsmaßnahme bei den Maritimen Tagen 2024 durchgeführt. Hierzu lässt sich feststellen, dass die Maßnahme zum Erreichen der verfolgen Ziele geeignet war. Die Kamerastandorte wurden auf Grundlage einer entsprechenden Gefährdungsbewertung ausgewählt. Der Einsatz zusätzlicher Kameras wird fortlaufend bewertet und steht in

Abhängigkeit der örtlichen Gegebenheiten (zum Beispiel Stromversorgung und Ressourcenzuweisungen).

5.3 Evaluation Bremisches Polizeigesetz

Nach § 150 des Bremischen Polizeigesetzes alte Fassung war der Bremischen Bürgerschaft ein Evaluationsbericht über die Auswirkungen der nach §§ 41 bis 44 Bremisches Polizeigesetz möglichen Anordnungen sowie zur Anwendung des § 27 Absatz 1 Satz 2 Bremisches Polizeigesetz vorzulegen. Schwerpunkte des Berichts sollten die Wirksamkeit sowie die praktische Anwendung der Befugnisnormen und der Verfahrensvorschriften sein. Der Senat hat den Evaluationsbericht unter Mitwirkung von Herrn Prof. Stauch und Herrn Prof. Dr. Hartmann erarbeitet und der Bremischen Bürgerschaft zugeleitet. Der Senator für Inneres und Sport hat die Evaluation eng begleitet. Bereits die Evaluationsarbeiten selbst und auch die Ergebnisse der Gutachter haben in der Folge zu einem intensiven Austausch zwischen dem Senator für Inneres und Sport und den Behörden des Polizeivollzugsdienstes geführt, in dessen Verlauf auch Verbesserungen in Bezug auf die Dokumentation eingeleitet wurden.

Hinsichtlich der Subsidiaritätsklausel in § 43 Absatz 3 Bremisches Polizeigesetz teilt der Senator für Inneres und Sport die übereinstimmende Auffassung beider Gutachter, nach der eine Absenkung der Subsidiaritätsschwelle erforderlich ist. Die Standortermittlung bezieht sich allein auf ein einziges Datum, den aktuellen oder vor kurzem innegehabten Standort einer Person. Es werden hiermit keine besonders schutzwürdigen Daten erhoben. Diesem – punktuellen – Eingriff in das Recht auf informationelle Selbstbestimmung stehen nur wenige höchstwertigste Rechtsgüter, insbesondere das Recht auf Leben und körperliche Unversehrtheit der betroffenen Person, gegenüber, welche durch den Staat zu schützen sind. Die Fälle des § 43 Absatz 3 Bremisches Polizeigesetz gebieten angesichts der von der Norm vorausgesetzten gegenwärtigen Gefahr in der Regel unverzügliches Handeln, insbesondere zur Lebensrettung.

Zudem können in der Vergangenheit liegende unzureichende Dokumentationen nicht dazu führen, dass notwendige Gesetzesänderungen nicht vorgenommen würden. Die Verknüpfung der Erweiterung dringend benötigter polizeilicher Befugnisse mit früheren verwaltungstechnischen Versäumnissen in der Dokumentation wäre sachfremd. Gerade auch der Vorrang einer aufwändigen Öffentlichkeitsfahndung – und damit drohender Stigmatisierung betroffener Personen, deren Bilder samt zugehörigem Sachverhalt veröffentlicht und durch alle gespeichert werden können – dürfte nach Darstellung im Evaluationsgutachten kaum im Interesse Betroffener sein im Vergleich zur einmaligen, im Hintergrund stattfindenden Feststellung des (letzten) Standortes des mitgeführten Mobilfunktelefons.

5.4 Datenschutzgrundverordnung und Parlamente, Datenaustausch zur Beantwortung parlamentarischer Anfragen

Die Bürgerschaftskanzlei teilt die Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit, wonach aufgrund des Urteils des Europäischen Gerichtshofs (EuGH) vom 16. Januar 2024 eine Anpassung der Regelungen des Bremischen Ausführungsgesetzes zur EU-Datenschutzgrundverordnung zur Vermeidung von Rechtsunsicherheiten erforderlich ist. Die Bürgerschaftskanzlei steht bezüglich der Umsetzung bereits im engen Austausch mit dem Senatskommissar für den Datenschutz und dem Landesbeauftragten für Datenschutz und Informationsfreiheit. Zur Umsetzung der Rechtsprechung des Europäischen Gerichtshofs ist es sinnvoll, zunächst im Rahmen eines Gesetzgebungsverfahrens die Streichung des § 2 Absatz 4 Bremisches Ausführungsgesetz zur EU-Datenschutzgrundverordnung aus Klarstellungsgründen umzusetzen. In einem weiteren Schritt wäre zu überlegen, ob die Datenschutzordnung der Bremischen Bürgerschaft in das Bremische Ausführungsgesetz zur EU-Datenschutzgrundverordnung zu überführen ist. Hierzu wäre die Datenschutzordnung auf DSGVO-Konformität zu überprüfen und gegebenenfalls bestehender Änderungsbedarf zu erfassen. Vor diesem Hintergrund sind auch die Datenverarbeitungsvorgänge der Fraktionen zu berücksichtigen. Zu diesem Thema hat bereits ein erstes Gespräch stattgefunden.

Hinsichtlich der Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit besteht nach Auffassung der Bürgerschaftskanzlei hingegen kein zwingender Regelungsbedarf. Dieser ist nach der geltenden Gesetzeslage für den gesamten parlamentarischen Bereich zuständig. Von den Fraktionen wurde der Wunsch geäußert, diesen als Aufsichtsbehörde beizubehalten.

Darüber hinaus wird derzeit geprüft, ob bezüglich eines Datenaustausches zwischen den Behörden zwecks Beantwortung von parlamentarischen Anfragen eine gesetzliche Regelung im Bremischen Ausführungsgesetz zur EU-Datenschutzgrundverordnung zu schaffen wäre.

5.5 Telenotarzt

Die seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit angemahnte, gesonderte rechtliche Grundlage, der es bedarf, sobald ein Versorgungskonzept aus der Erprobungsphase in den Regelbetrieb geht, wurde durch Artikel 1 des Gesetzes zur Novellierung des Bremischen Hilfeleistungsgesetzes (BremHilfeG) vom 1. April 2025 (Brem.GBl. S. 261) mit Wirkung vom 1. März 2025 bereits geschaffen

Gemäß § 32 Absatz 9 Bremisches Hilfeleistungsgesetz können telemedizinische Anwendungen zur Unterstützung rettungsdienstlichen Personals im Einsatz genutzt werden. Durch die Einführung des § 86 Absatz

1 Nummer 4 Bremisches Hilfeleistungsgesetz wurde die Verarbeitung von erhobenen und gespeicherten personenbezogenen Daten spezifiziert. So dürfen im automatisierten und im nichtautomatisierten Verfahren erhobene und gespeicherte personenbezogene Daten aus aufgabenbezogenen Anlässen übermittelt werden, wenn die Weitergabe an eine andere angeschlossene Telenotärztin oder einen anderen angeschlossenen Telenotarzt erfolgen oder von der hiesigen Telenotärztin oder von dem hiesigen Telenotarzt übernommen werden soll. Hierdurch wurde die geforderte, gesonderte rechtliche Grundlage geschaffen, dass datenschutzkonform neben den bremischen Telenotärzt:innen auch entsprechend qualifiziertes Personal aus anderen Standorten (wie zurzeit Telenotärzt:innen aus Goslar) in diese Aufgabe mit eingebunden werden können.

Dank der Einbindung und Unterstützung des Landesbeauftragten für Datenschutz und Informationsfreiheit bei der Entwicklung dieser grenzüberschreitenden Zusammenarbeit, welche die bedarfsgerechte und kosteneffiziente Arbeit ermöglicht, konnten von Beginn an die datenschutzrechtlichen Verantwortlichkeiten mitgedacht werden. Die bei der Ausarbeitung als notwendig identifizierten Veränderungen konnten gemeinsam im laufenden Projekt nachgesteuert werden.

5.6 Ordnungsamt – pmOWi-App zur Ahndung von Verkehrsverstößen

Der Senator für Inneres und Sport bedauert die unterbliebene Beteiligung des Landesbeauftragten für Datenschutz und Informationsfreiheit im Rahmen der Einführung der Softwarelösung im Ordnungsamt Bremen und wird zukünftig sicherstellen, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit rechtzeitig beteiligt wird. Im Hinblick auf die Erstellung der Datenschutzfolgeabschätzung steht das Ordnungsamt im engen Austausch mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit.

5.7 Rechtsverordnung zu den Prüf- und Speicherfristen nach dem Bremischen Polizeigesetz

Die Normierung von Speicherungsfristen im Rahmen einer Rechtsverordnung durch den Senat auf der gesetzlichen Grundlage des § 58 Absatz 6 Satz 1 des Bremischen Polizeigesetzes ist derzeit nicht möglich. Nach Auffassung der Senatorin für Justiz und Verfassung wäre eine entsprechende Regelung von der Ermächtigungsnorm des § 58 Absatz 6 Satz 1 Bremisches Polizeigesetz nicht erfasst. Der Senat als Verordnungsgeber folgt der fachlichen Einschätzung der Senatorin für Justiz und Verfassung als zuständiges Ressort für die formelle und materielle Prüfung von Gesetz- und Verordnungsentwürfen des Landes und der Stadtgemeinde Bremen.

Im Rahmen der anstehenden Novellierung des Bremischen Polizeigesetzes wird der Senat der Bürgerschaft (Landtag) einen Gesetzentwurf vorlegen, der auch eine Rechtsgrundlage zum Erlass einer Rechtsverordnung vorsehen wird, die auch die Regelung von Speicherungsfristen ermöglicht. Soweit die Bürgerschaft (Landtag) den Gesetzentwurf beschließt, kann der Senat eine entsprechende Rechtsverordnung schnellstmöglich erlassen.

6. Justiz

6.4 Aufsichtsbefugnisse des Landesbeauftragten für Datenschutz und Informationsfreiheit im Anwendungsbereich der Strafprozessordnung (StPO) und des Ordnungswidrigkeitengesetzes (OWiG)

Soweit der Landesbeauftragte für den Datenschutz nach der Europäischen Datenschutzgrundverordnung wie bereits im 3. Jahresbericht (dort unter Ziffer 6.5) die aus seiner Sicht nicht erfolgte Umsetzung des Artikel 41 der EU-Datenschutzrichtlinie zur Zusammenarbeit im Bereich Justiz und Inneres (JI-Richtlinie) rügt, hält die Senatorin für Justiz und Verfassung an der bereits in ihrer Stellungnahme zum 3. Jahresbericht vertretenen Rechtsauffassung ausdrücklich fest, wonach eine rechtskonforme Umsetzung des Artikel 41 der JI-Richtlinie bereits erfolgt ist. Bei der Anwendung des Strafgesetzbuches (StGB) und der Strafprozessordnung wenden die Gerichte und Staatsanwaltschaften Bundesrecht an. Dem entspricht es, dass zuvörderst der Bundesgesetzgeber für die Umsetzung der europäischen Datenschutzvorgaben im Tätigkeitsbereich der Strafgerichte und Staatsanwaltschaften zuständig ist. Dementsprechend wurde zum Ende des Jahres 2019 die Vorschrift des § 500 Strafprozessordnung durch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 in die Strafprozessordnung eingefügt (vergleiche Bundestagsdrucksache 19/4671, Seite 71). Soweit öffentliche Stellen der Länder im Anwendungsbereich der Strafprozessordnung personenbezogene Daten verarbeiten und soweit die Strafprozessordnung nichts Abweichendes bestimmt, erfolgt eine Rechtsfolgenverweisung in Teil 3 des Bundesdatenschutzgesetzes (BDSG). An die Stelle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt für die Freie Hansestadt Bremen der Landesbeauftragte für Datenschutz und Informationsfreiheit (vergleiche § 500 Absatz 2 Nummer 2 Strafprozessordnung).

§ 500 Strafprozessordnung soll die bundeseinheitliche Ausgestaltung des Datenschutzrechts für das Strafverfahren gewährleisten (vergleiche Bundestagsdrucksache 19/4671, Seite 71). Das Bundesdatenschutzgesetz findet im Grundsatz subsidiär Anwendung, wenn die Spezialgesetze keine besondere Regelung treffen (vergleiche § 1 Absatz 2 Satz 1, 2 Bundesdatenschutzgesetz). Die Strafprozessordnung und das Bundesdatenschutzgesetz stehen insoweit in Ergänzung zueinander

(vergleiche auch Beckscher Online-Kommentar Strafprozessordnung/von Häfen, 39. Edition 1.1.2021, § 500 Randnummer 4). Namentlich bezüglich besonderer Schutzvorschriften für die sogenannten besonderen Kategorien personenbezogener Daten, bezüglich Auskunftsrechten einer von der Datenverarbeitung betroffenen Person, hinsichtlich Löschungs- und Berichtigungspflichten sowie hinsichtlich der Anforderungen an Datensicherheit, Technik und förmliche Gestaltung ist das Bundesdatenschutzgesetz insoweit neben der Strafprozessordnung von besonderer Bedeutung (vergleiche Puschke, Systematischer Kommentar zur Strafprozessordnung, 5. Auflage 2020, § 500 Randnummer 2 fortfolgende).

Wie aus § 500 Absatz 2 Nummer 2 Strafprozessordnung folgt, kommen dem Landesbeauftragten für Datenschutz und Informationsfreiheit Kontrollbefugnisse hinsichtlich des technisch-organisatorischen Datenschutzes bei den Gerichten beim Umgang mit personenbezogenen Daten im Rahmen der sogenannten Eigenverwaltung, bei Justizverwaltungsakten und bezüglich der Tätigkeit der Geschäftsstellen zu (vergleiche Puschke, Systematischer Kommentar zur Strafprozessordnung, 5. Auflage 2020, § 500 Randnummer 8, mit weiteren Nachweisen). Gleiches gilt für die Staatsanwaltschaften bezüglich Justizverwaltungsakten, der Wahrnehmung schlichter Verwaltungsaufgaben und bei der Verarbeitung personenbezogener Daten im Rahmen ihrer Ermittlungstätigkeit. Nach Auffassung der Senatorin für Justiz und Verfassung ist § 500 Strafprozessordnung im Ordnungswidrigkeitenverfahren sinngemäß anzuwenden. Wie aus vorstehenden Ausführungen folgt, haben die europarechtlichen Vorgaben bereits eine Umsetzung erfahren.

Die Senatorin für Justiz und Verfassung wird in Kürze eine Überarbeitung des Einführungsgesetzes zur Strafprozessordnung vorlegen, welche deklaratorisch die vorgenannte Rechtslage zusammenfasst.

6.6 Protokollierung von Zugriffen auf E-Akten beim Landgericht Bremen

Die Darstellung der Protokollierung von Zugriffen auf E-Akten am Landgericht Bremen ist im Grundsatz zutreffend, allerdings etwas verkürzt dargestellt.

Grundsätzlich haben nur diejenigen Beschäftigten Zugriff auf die elektronische Akte der jeweiligen Abteilung, die in der entsprechenden Abteilung laut Geschäftsverteilungsplan zuständig sind. Dabei wird die Erteilung beziehungsweise Löschung der Berechtigung, auf die elektronische Akte Zugriff nehmen zu können, wie folgt dokumentiert:

In den Gerichten wird in den verschiedenen Abteilungen mit unterschiedlichen IT-Verfahren gearbeitet. In Zivilsachen wird mit einer elektronischen Akte (e-Akte) gearbeitet (Software „e²A“), die wiederum mit einem Fachverfahren verbunden ist. Die Erteilung von Berechtigungen im Fachverfahren, die wiederum auf die e-Akte durchschlagen, erfolgt in einem

geregelten – formalisierten – Prozess über sogenannte Benutzeraufträge. Wenn einer oder einem Beschäftigten die Zuständigkeit in diesem Fall für Zivilsachen nach dem Geschäftsverteilungsplan zugewiesen wird, dann erfolgt ein entsprechender Auftrag über spezielle auftragsberechtigte Personen in der Verwaltung über ein Formular an die IT-Stelle Justiz. Nur die IT-Stelle kann die Berechtigungen in den Fachverfahren vergeben. Alle so erteilten Aufträge werden von der IT-Stelle in der Verwaltungsakte VIS dokumentiert und können über einen längeren Zeitraum nachvollzogen werden. Auch die Löschung von Berechtigungen wird entsprechend dokumentiert, wenn eine Aufgabe wieder abgegeben wird.

Das Fachverfahren und auch die e-Akte werden bei Dataport im sogenannten Datacenter Justiz betrieben. Hierfür wurden sogenannte „Security Service Level Agreements“ abgeschlossen und damit ein sehr hohes Sicherheitsniveau eingekauft.

Neben der beschriebenen Berechtigungsdokumentation bestehen auch hinsichtlich der Anwendung als solche die in Datenbanken üblichen Möglichkeiten, auf Protokollierungsdateien zuzugreifen. So ist es auf Anfrage bei dem IT-Dienstleister Dataport auch über diese Daten möglich, konkrete Personen zu identifizieren, die Zugriff auf die e-Akte genommen haben. Gegenwärtig werden die entsprechenden Log-Dateien nach 14 Tagen gelöscht. Eine Rücksicherung aus dem Backup ist maximal innerhalb der letzten 30 Tage möglich.

Zudem ist zu berücksichtigen, dass viele Tätigkeiten in der e-Akte, wie etwa die Erstellung von Dokumenten, die elektronische Signatur, die Anlegung von Aufgaben oder der Versand von Dokumenten bereits jetzt in zahlreichen Metadaten über den eigentlichen Verfahrensabschluss hinaus unter Einhaltung der gesetzlichen Aufbewahrungsfristen eingesehen werden können und müssen. Diese Möglichkeit der Nachverfolgung der Bearbeitung der Akte geht über die rein technische Protokollierung hinaus.

6.7 Gesetzentwurf über die Befugnisse in Justizgebäuden auf der Grundlage des Hausrechtes

Die Senatorin für Justiz und Verfassung hat zum Entwurf eines Bremischen Gesetzes über die Sicherheit in Justizgebäuden bereits in der Phase der Erarbeitung des Gesetzentwurfs den Landesbeauftragten für Datenschutz und Informationsfreiheit beteiligt und gebeten, zu der datenschutzrechtlichen Zulässigkeit einer gesetzlichen Bestimmung zur Erfassung personenbezogener Daten im Zusammenhang mit konfliktträchtigen Gerichtsverhandlungen Stellung zu nehmen. Mit der Anfrage sollte in einem sehr frühen Stadium geklärt werden, ob eine entsprechende Befugnisnorm datenschutzrechtlich zulässig ist. Die Mitteilung des Landesbeauftragten für Datenschutz und Informationsfreiheit, wonach eine entsprechende Regelung aus seiner Sicht gegen geltendes Datenschutzrecht verstoße, wurde zur Kenntnis genommen. Die Senatorin für Justiz und Verfassung

wird diese Ausführungen bei der weiteren Erstellung des beabsichtigten Gesetzesentwurfes mit anderen Argumenten abwägen und erforderlichenfalls den Landesbeauftragten für Datenschutz und Informationsfreiheit im Rahmen der gesetzlichen Bestimmungen die Möglichkeit zur weiteren Stellungnahme einräumen.

Der bisherige Ablauf dieser Angelegenheit bietet insoweit Anlass, die Trennlinien zwischen einem informatorischen Vorfeldaustausch auf Referentenebene und der gesetzlich vorgesehenen Befassung des Landesbeauftragten für Datenschutz und Informationsfreiheit zu Entwürfen von Rechts- und Verwaltungsvorschriften zu erörtern.

7. Gesundheit

7.1 Gemeldete Datenschutzverletzungen

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz wird im Rahmen der Rechtsaufsicht gem. § 33 in Verbindung mit § 38 des Bremischen Krankenhausgesetzes die Krankenhäuser zeitnah um Mitteilung bitten, wie das Berechtigungsmanagement im Hinblick auf die Verarbeitung personenbezogener Gesundheitsdaten der Krankenhäuser ausgestaltet ist und wie die regelmäßige Überprüfung sichergestellt wird. Des Weiteren wird die Senatorin für Gesundheit, Frauen und Verbraucherschutz prüfen, in welchem Umfang regelmäßige Datenschutzschulungen der Beschäftigten in den Krankenhäusern, die aufgrund ihrer Aufgaben rechtmäßigen Zugriff auf die Patientendaten nach § 38 Absatz 2 des Bremischen Krankenhausgesetzes haben, erfolgen.

7.1.1 Einbrüche in Außenstellen des Gesundheitsamtes Bremen

Alle 17 Außenstellen des Gesundheitsamtes Bremen wurden in Hinblick auf die Umsetzung technischer und organisatorischer Maßnahmen im Sinne von Artikel 32 der EU-Datenschutzgrundverordnung überprüft. Alle Außenstellen besitzen nun Schlüsseltresore, um die personenbezogenen Daten, insbesondere die personenbezogenen Gesundheitsdaten zu schützen. Zudem wurden die Schulungen im Gesundheitsamt Bremen nachgebessert. Das Schulungskonzept enthält nun eine thematische Einheit zum Umgang mit personenbezogenen Daten. Darin enthalten sind konkrete Fallbeispiele aus dem Gesundheitsamt, um allen Beschäftigten die Thematik so nachvollziehbar wie möglich zu vermitteln.

7.1.2 Fehlgeleitete Faxsendungen

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz nimmt diesen Bericht zum Anlass, die Gesundheitsämter Bremen und Bremerhaven im Rahmen der Fachaufsicht zu kontaktieren und für einen sicheren Umgang mit personenbezogenen (Gesundheits-) Daten zu sensibilisieren. Darüber hinaus wird auf die Nutzung von datenschutzrechtlich sichereren Online-Lösungen zur Übermittlung von Patientendaten verwiesen. Hier werden die

erwähnten verschlüsselten E-Mails oder Portallösungen benannt, um die Möglichkeit aufzuzeigen, die Defizite des Faxes zu umgehen. Zusätzlich wird auf die Kassenärztliche Vereinigung Bremens und Kassenzahnärztliche Vereinigung Bremens zugegangen, mit der Bitte diese Sensibilisierung auch an die niedergelassenen Ärzt:innen heranzutragen.

7.2 Angebot an Bremer Schülerinnen und Schüler zur Durchführung von HPV-Impfungen durch das Gesundheitsamt Bremen

Der bereits im 6. Jahresbericht benannten Kritik hat sich das Gesundheitsamt Bremen umfassend gestellt und aktiv an der Verbesserung der damals für verbesserungswürdig zu bewertenden Unterlagen gearbeitet.

Gleichwohl hat sich durch die Einbindung des Robert-Koch-Instituts (RKI) eine Veränderung im Verfahren ergeben. Der Veränderung im Verfahren musste durch organisatorische Maßnahmen Rechnung getragen werden. Hierbei wurde auch der behördliche Datenschutzbeauftragte des Gesundheitsamtes Bremen einbezogen.

Die Klärung der Frage der Übermittlung von Klassenlisten durch die Senatorin für Kinder und Bildung an das Gesundheitsamt Bremen konnte bislang nicht erfolgen. Die Klärung wird jedoch zeitnah nachgeholt. Dabei sieht sich das Gesundheitsamt Bremen in der Verantwortung, ihre durch Recht und Gesetz zugewiesenen Aufgaben datenschutzkonform wahrzunehmen. Folglich wird der Vorgang priorisiert. Die nächsten geplanten Schritte zur Umsetzung sind dabei die Abstimmung mit der Senatorin für Kinder und Bildung im Hinblick auf die datenschutzkonforme Übermittlung der Klassenlisten und die Abstimmung der Unterlagen mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit.

7.5 Unzulässige Speicherung von Arztbriefen im Krankenhaus

Zu unbefugten Einsichtnahmen kann es nur kommen, wenn die Daten – entgegen der Vorgaben – nicht pseudonymisiert wurden oder die Daten auf einer gesonderten Ablage gespeichert waren, die nicht über die technischen Möglichkeiten eines Klinikinformationssystems verfügt.

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz wird im Rahmen der Rechtsaufsicht gem. § 33 in Verbindung mit § 38 des Bremischen Krankenhausgesetzes die Krankenhäuser auffordern, ihre Beschäftigten anzuweisen, Daten beschäftigter Personen grundsätzlich immer zu pseudonymisieren oder zu anonymisieren. Außerdem werden die Krankenhäuser im Rahmen der Rechtsaufsicht darauf hingewiesen, dass Datenablagen außerhalb eines Krankenhausinformationssystems nicht zu erfolgen haben.

7.6 Stichprobenhafte Prüfung bei Trägern stationärer Pflegeeinrichtungen

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz hat das Thema Datenschutz und die Hinweise des Landesbeauftragten für Datenschutz und Informationsfreiheit im Landespflegeausschuss im Mai 2025 thematisiert. Die Hinweise zur Verbesserung wurden von den Mitgliedern des Landespflegeausschusses zur Kenntnis genommen und der allgemein eher positive Stand zum Datenschutz in der Pflege begrüßt. Eine Vertreterin des Landesbeauftragten für Datenschutz und Informationsfreiheit, die an der Ausschusssitzung teilgenommen hat, hat den Mitgliedern des Landespflegeausschusses bei Bedarf weitere Unterstützung angeboten.

8. Soziales

8.1 Gemeldete Datenschutzverletzungen

Die Senatorin für Arbeit, Soziales, Jugend und Integration ist ihrer Pflicht nach Artikel 33 Datenschutzgrundverordnung durch die Meldungen an den Landesbeauftragten für Datenschutz und Informationsfreiheit nachgekommen. Die abhandengekommenen Laptops und Smartphones waren passwortgeschützt und verschlüsselt, sodass die gespeicherten Daten vor dem Zugriff Dritter geschützt waren und auch weiterhin sind.

8.2 Kommunikation durch unverschlüsselte E-Mails durch Sozialbehörden

Den Beschäftigten der Senatorin für Arbeit, Soziales, Jugend und Integration ist der besondere Schutzbedarf von Sozialdaten sehr bewusst. Die Senatorin für Arbeit, Soziales, Jugend und Integration ist aktuell mit Dataport im Gespräch, welche technischen Möglichkeiten künftig zum Einsatz kommen könnten.

8.3 Datenbank Haaranalysen

Das Amt für Soziale Dienste speichert die Daten aus den Gutachten zur Haaranalysen zum Drogenkonsum drogenabhängiger und beziehungsweise oder substituierter Eltern und Kindern im Fachverfahren und wird den Landesbeauftragten für Datenschutz und Informationsfreiheit bei Anpassungen und Weisungen bezüglicher der Datenspeicherung einbeziehen und diese mit ihm abstimmen.

8.4 Vermehrte Nutzung von Apps in der Kindertagesbetreuung

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wurde bei der Auswahl der Kita-App durch den Eigenbetrieb Kita Bremen beteiligt. Der Auswahlprozess erstreckte sich über einen mehrmonatigen Zeitraum.

Der Eigenbetrieb Kita Bremen nutzt die Kita-App lediglich zur Kommunikation mit den Sorgeberechtigten.

Zur Nutzung von Kita-Apps im Allgemeinen:

Eine Expertise des Staatsinstituts für Frühpädagogik (IFP) gibt einen aktuellen Überblick über die am Markt verfügbaren Kita-Apps für mittelbare pädagogische Aufgaben in der Kindertagesbetreuung. Dabei werden auch Hinweise zum Praxiseinsatz sowie Hinweise über die Datenschutzanforderungen dargestellt (Konzeption und Anwendung webbasierter Kita-Apps in der 3. Auflage, Mai 2025). Auf diese Expertise des Staatsinstituts für Frühpädagogik soll kurzfristig im Rahmen der auf der Grundlage des § 78 des Achten Buches Sozialgesetzbuch eingesetzten Arbeitsgruppe hingewiesen werden, um die Träger der Kindertagesbetreuung für das Thema zu sensibilisieren und sie in ihrer Auswahl von Kita-Apps zu unterstützen.

9. Bildung

9.2 Vergabe von Passwörtern bei itslearning

Die initiale Passwortvergabe für Schüler:innen stellt insbesondere in Grundschulen eine nicht ganz einfache Herausforderung dar. Gelegentlich greifen Lehrkräfte zu pragmatischen Lösungen, um den Schüler:innen zunächst den Zugang zu Plattformen wie itslearning zu ermöglichen. Gleichwohl ist nach der ersten Anmeldung sicherzustellen, dass jedes Kind ein individuelles, sicheres und geheimes Passwort erhält.

Die Senatorin für Kinder und Bildung legt großen Wert darauf, dass diese Vorgehensweise umgesetzt wird. Zu diesem Zweck stehen auf der Plattform itslearning unterstützende Materialien zur Verfügung. Darüber hinaus gibt es Fortbildungsangebote sowie Informationsschreiben zum Schuljahresbeginn für die Lehrkräfte.

Die Bedeutung individueller, sicherer Passwörter ist mittlerweile an allen Schulen bekannt. Die Vorgaben werden regelmäßig umgesetzt. Gleichwohl lassen sich Einzelfälle, in denen die Vorgaben nicht entsprechend umgesetzt werden, nicht vollständig ausschließen.

9.3 Einsatz von Telepräsenzrobotern in Schulen

Das Gesetz zur Änderung des Bremischen Schulgesetzes und des Bremischen Schuldatenschutzgesetzes vom 1. April 2025 (Brem.GBl. S. 326) ist am 2. April 2025 in Kraft getreten.

Mit der Novellierung wurde eine Rechtsgrundlage für den Distanzunterricht inklusive des Einsatzes von Telepräsenzrobotern (Avataren) geschaffen. Vor dem Einsatz eines Avatars erfolgt eine umfangreiche Beratung aller beteiligten Personen, die auch die datenschutzrechtlichen Aspekte umfasst.

10. Bau, Wohnen, Umwelt, Energie und Verkehr

10.2 Sichere Datenübermittlung bei Beantragung einer Bauakte

Die Senatorin für Bau, Mobilität und Stadtentwicklung wird im nächsten Wartungszyklus des Onlinedienstes „Einsicht in abgeschlossene Bauakten“ folgenden Punkt überarbeiten:

Das Pflichtfeld der E-Mail-Adresse wird zukünftig als optionales Feld geführt.

Das optionale Feld wird um einen Hinweis ergänzt, dass die E-Mail-Adresse für den elektronischen Versand erforderlich ist. Alternativ kann die Bauakte vor Ort eingesehen werden.

11. Beschäftigtendatenschutz

11.2 Stellenausschreibung – Einsicht in die Personalakte

Der Senator für Finanzen hat bereits mit seinem Rundschreiben Nummer 04/2020 „Änderung personalaktenrechtlicher Vorschriften aufgrund der Datenschutz-Grundverordnung“ Hinweise für die Personalstellen zur Übermittlung von Personalakten im Rahmen eines Auswahlverfahrens gegeben. Hierbei wurde auch auf das Gebot der Erforderlichkeit bei der Datenverarbeitung auch im Rahmen von Auswahlverfahren und den Zeitpunkt Anforderung der Personalakte hingewiesen. Danach ist die Erforderlichkeit in der Regel erst dann gegeben. wenn die sich bewerbende Person in die engere Auswahl genommen worden ist. Auf das genannte Rundschreiben werden die Personalreferent:innen seitens des Senators für Finanzen erneut hingewiesen.

Das Zentrale Personalbüro des Senators für Finanzen, zuständig für die Dienststellen des Senators für Finanzen, der Finanzämter und der Landeshauptkasse, verfährt bereits entsprechend. Hierzu wurde die Bitte um Erteilung der Einwilligung zur Einsichtnahme dahingehend konkretisiert, dass sich die Einsichtnahme ausschließlich auf die Grundakte sowie Hauptakte bezieht und nicht auf Nebenakten.

12. Medien, Telemedien, Digitalisierung

12.7 App-Angebote durch Behörden

Der Senator für Finanzen nimmt zur Problematik der Ausschreibung von App-Entwicklungen durch den IT-Dienstleister der Freien Hansestadt Bremen, Dataport, wie folgt Stellung:

Aus haushalts- und vergaberechtlicher Sicht ist die Bündelung der IT-Dienstleistungen, einschließlich der Entwicklung von Apps, durch den zentralen IT-Dienstleister sinnvoll, um Synergieeffekte zu nutzen, Kosten zu reduzieren und eine einheitliche Qualität sicherzustellen. Gleichzeitig ist

sicherzustellen, dass bei der Auftragsvergabe Transparenz und ein faires Wettbewerbsverfahren gewährleistet sind.

Im Kontext des Gesetzes zur Gewährleistung der digitalen Souveränität der Freien Hansestadt Bremen - Land und Stadtgemeinde - ist es zudem von großer Bedeutung, dass die Entwicklung und Nutzung von Apps unter Berücksichtigung der digitalen Unabhängigkeit und der Sicherheit der IT-Infrastruktur erfolgt.

Der Senator für Finanzen unterstützt daher die Prüfung und Sicherstellung, dass alle Ausschreibungen und Beschaffungen im IT-Bereich die Vorgaben dieses Gesetzes einhalten, insbesondere hinsichtlich Datenschutz, Datensicherheit und Vermeidung von Abhängigkeiten von nichtsouveränen IT-Dienstleistern.