Der Landesbeauftragte
für Datenschutz

Freie
Hansestadt
Bremen

7. Jahresbericht

des Landesbeauftragten für Datenschutz
nach der Europäischen Datenschutzgrundverordnung

Bremerhaven, den 28. März 2025

Impressum:

Für die Inhalte dieser Ausgabe des 7. Jahresberichtes zum Datenschutz nach der Datenschutzgrundverordnung ist verantwortlich:

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Dr. Timo Utermark

Arndtstraße 1
27570 Bremerhaven
Telefon: 04 71 / 5 96 – 20 10 oder 04 21 / 3 61 – 20 10
E-Mail: office@datenschutz.bremen.de

Durch Kippen des Jahresberichtes kommen Sie zur Informationsfreiheit.

© Foto: Magistratspressestelle/Felix Schulke

7. Jahresbericht
des Landesbeauftragten für Datenschutz
nach der Europäischen Datenschutzgrundverordnung

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats meinen Bericht im Sinne des Artikels 59 der Europäischen Datenschutzgrundverordnung über das Ergebnis der Tätigkeit im Jahr 2024. Redaktionsschluss war der 31. Dezember 2024.

Bremerhaven, den 28. März 2025

Dr. Timo Utermark

Der Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Relevante Entwicklungen

In der Entwicklung des Datenschutzrechtes trat im vergangenen Jahr die zentrale Bedeutung des Schutzes der informationellen Selbstbestimmung durch das Grundgesetz wieder hervor. 2024 ergingen drei grundlegende Entscheidungen des Bundesverfassungsgerichtes zum Verhältnis des Schutzes der informationellen Selbstbestimmung aus Artikel 2 Absatz 1 Grundgesetz (GG) in Verbindung mit Artikel 1 Absatz 1 GG, des Fernmeldegeheimnisses aus Artikel 10 GG beziehungsweise des Grundrechtes auf Unverletzlichkeit der Wohnung aus Artikel 13 GG zu den Rechtsgütern der inneren und äußeren Sicherheit. Den Entscheidungen kommt auch eine Bedeutung für die Freie Hansestadt Bremen zu. Zunächst erklärte das deutsche Verfassungsgericht mit einem Beschluss vom 17. Juli 2024 (Aktenzeichen 1 BvR 2133/22) zentrale Vorschriften des Hessischen Verfassungsschutzgesetzes für unvereinbar mit dem Grundgesetz. Mit dem Gesetz über das Bundeskriminalamt und die Zusammenarbeit der Länder in kriminalpolizeilichen Angelegenheiten befasste sich das Bundesverfassungsgericht sodann in seinem Urteil vom 1. Oktober 2024 (Aktenzeichen 1 BvR 1160/19, siehe hierzu Ziffer 5.7 dieses Berichtes). Zu verfassungsrechtlichen Fragen im Zusammenhang mit der strategischen Inland-Ausland-Fernmeldeaufklärung äußerte sich das Bundesverfassungsgericht schließlich in einem am 8. Oktober 2024 ergangenen Beschluss (Aktenzeichen 1 BvR 1743/16 und 1 BvR 2539/16). Da sich der Beschluss zum Hessischen Verfassungsschutzgesetz auf Landesrecht bezieht, verdient er in Hinblick auf die Freie Hansestadt Bremen besondere Beachtung.

Neben diesen verfassungsrechtlichen Entscheidungen brachte das Jahr 2024, wie bereits in den Vorjahren, die europäische Gesetzgebung neue relevante Entwicklungen. Auf europäischer Ebene ist nämlich am 1. August 2024 die Verordnung über künstliche Intelligenz in Kraft getreten, die große Auswirkungen auf die Gewährleistung des Datenschutzes in der Zukunft haben wird. Mit diesem Gesetzgebungsakt wird ein weiterer Baustein des europäischen Datenrechtes auch auf den Schutz der informationellen Selbstbestimmung der Bürgerinnen und Bürger ausgerichtet.

Schließlich hat sich auch in der Freien Hansestadt Bremen eine Änderung in Bezug auf den Datenschutz ergeben: Am 13. Dezember 2024 habe ich mein Amt als Landesbeauftragter für Datenschutz und Informationsfreiheit angetreten. Dafür, dass ich Teil dieser Behörde sein darf, bin ich sehr dankbar. Meine Mitarbeiterinnen und Mitarbeiter stehen für einen außerordentlichen Sachverstand, demonstrieren immer wieder aufs Neue „Haltung“, wenn es darum geht, das Grundrecht auf informationelle Selbstbestimmung durchzusetzen, und suchen gleichzeitig stets serviceorientiert, kooperativ und verständig nach praktischen Lösungen. Täglich engagieren sie sich mit hohem Einsatz für den Schutz der persönlichen Daten der Bürgerinnen und Bürger in der Freien Hansestadt Bremen. Einen besonderen Dank möchte ich Herrn Bothe

und Frau Binner ausdrücken, die in der Zwischenzeit, als es keine Leitung gab, die Arbeit der Stellvertretung praktisch ausgefüllt haben und die Behörde durch das auch schwierige Fahrwasser gesteuert haben. Auch meiner Vorgängerin im Amt, Frau Dr. Sommer, möchte ich dafür danken, dass sie mir den Einstieg in jeder Hinsicht leichtgemacht hat und mit Rat und Tat zur Seite steht. Ihr gebührt Anerkennung für ihren großen Einsatz für den Schutz personenbezogener Daten in der Freien Hansestadt Bremen, in Deutschland und in Europa.

1.1 Beschluss zum Hessischen Verfassungsschutzgesetz

Gegenstand des Beschlusses des Bundesverfassungsgerichtes vom 17. Juli 2024 (Aktenzeichen 1 BvR 2133/24) zum Hessischen Verfassungsschutzgesetz waren verschiedene Verfassungsbeschwerden, in denen sich die Beschwerdeführer unmittelbar gegen einzelne Bestimmungen des Hessischen Verfassungsschutzgesetzes wendeten, die es dem hessischen Landesamt für Verfassungsschutz ermöglichten, insbesondere in das Recht auf informationelle Selbstbestimmung von Bürgerinnen und Bürgern einzugreifen. Die Verfassungsbeschwerden umfassten zunächst die Erlaubnis zur Ortung von Mobilfunkendgeräten durch § 9 Hessisches Verfassungsschutzgesetz, wodurch auch die Möglichkeit geschaffen wurde, Persönlichkeitsprofile zu erstellen, einen Eingriff, der mit einer gegebenenfalls „hohen Persönlichkeitsrelevanz“ verbunden ist (Bundesverfassungsgericht [BverfG], Beschluss vom 17. Juli 2024 [Aktenzeichen 1 BvR 2133/24] Randnummer 129), Zudem wurde die in § 10 Hessisches Verfassungsschutzgesetz geschaffene Ermächtigungsgrundlage angegriffen, bei Flügen im Einzelfall Auskünfte über die Passagiere einzuholen. Ferner standen unter anderem die Weitergabe von personenbezogenen Daten an Strafverfolgungsbehörden nach § 20a Hessisches Verfassungsschutzgesetz und die Übermittlung von personenbezogenen Daten, die das hessische Landesamt für Verfassungsschutz zuvor erhoben hatte, an andere öffentliche Stellen nach § 20b Hessisches Verfassungsschutzgesetz im Zentrum des Verfahrens.

Bei der Beurteilung der Frage, ob die gesetzlichen Ermächtigungen, auf deren Grundlage die Verfassungsschutzbehörden in das Grundrecht auf informationelle Selbstbestimmung eingreifen können, verhältnismäßig sind, nimmt das Bundesverfassungsgericht auf die Besonderheiten der Verfassungsschutzbehörden Rücksicht und stellt andere Anforderungen als an die polizeilichen Tätigkeiten (BVerfG, am angegebenen Ort [aaO], Randnummer 87). Es erkennt ebenfalls an, dass die Verfassungsschutzbehörden das Ziel verfolgen, besonders hochrangige Rechtsgüter zu schützen (BVerfG, aaO, Randnummer 93). Zudem verfügen die Verfassungsschutzbehörden nicht über die „operativen Anschlussbefugnisse“ der Polizeibehörden, was dazu führt, dass die Eingriffe in das Recht auf informationelle Selbstbestimmung durch die Verfassungsschutzbehörden geringer als diejenigen aus polizeilicher Tätigkeit sind. Denn das Gewicht eines Eingriffes bestimmt sich auch danach, was mit den erlangten Informationen

getan werden kann (BVerfG, aaO, Randnummer 89). Für die Übermittlung von Daten der Verfassungsschutzbehörden an Polizei- und Strafverfolgungsbehörden folgt hieraus ein „informationelles Trennungsprinzip“, weil die teilweise höheren Anforderungen an die Datenerhebung durch die Polizei- und Strafvollstreckungsbehörden nicht umgangen werden dürfen (BVerfG, aaO, Randnummer 92).

Auf der Grundlage dieser allgemeinen Erwägungen stellt das Bundesverfassungsgericht klar, dass auch Standortermittlungen von Mobilfunkdaten, die ermöglichen, ein Bewegungsprofil zu erstellen, und damit zu schwerwiegenden Grundrechtseingriffen ermächtigen, unter engen Voraussetzungen verfassungsrechtlich zulässig sind (BVerfG, aaO, Randnummer 136 fortfolgende). Insbesondere muss in der Ermächtigungsgrundlage für eine so weitgehende Standortermittlung von Mobilfunkdaten die gesteigerte Beobachtungsbedürftigkeit bereits in einer dem Bestimmtheitsgrundsatz genügenden Art und Weise beschrieben werden (BVerfG, aaO, Randnummern 140 folgende). Auch ist eine unabhängige Vorabkontrolle unverzichtbar (BVerfG, aaO, Randnummer 158). Da die hessische Regelung des § 9 Hessisches Verfassungsschutzgesetz diesen Anforderungen nicht genügte, wurde sie für mit dem Grundgesetz unvereinbar erklärt. Allerdings ist mit dieser grundlegenden Entscheidung auch verfassungsrechtlich geklärt, dass ein Verzicht auf die Nutzung von Standortdaten von Mobilfunkgeräten, wie sie § 33 Bremisches Verfassungsschutzgesetz (BremVerfSchG) vorsieht, nicht zwingend ist. Die Entscheidung gibt dem bremischen Gesetzgeber insofern eine verlässliche Grundlage, in diesem Teilbereich das Verhältnis von Sicherheitsbelangen und dem Grundrecht auf informationelle Selbstbestimmung sowie dem Fernmeldegeheimnis neu abzuwägen.

Auch eine Ermächtigungsgrundlage, die es einem Landesamt für Verfassungsschutz gestattet, Auskünfte von Verkehrsunternehmen zu Fluggastdaten einzuholen, ist verfassungsrechtlich nach dem Beschluss des Bundesverfassungsgerichtes möglich, sofern die gesetzliche Regelung den verfassungsschutzspezifischen Anforderungen genügt (BVerfG, aaO, Randnummer 170). Mit dem Beschluss des Bundesverfassungsgerichtes ist daher auch in diesem Bereich präzise definiert, unter welchen Voraussetzungen der Gesetzgeber entsprechende Befugnisse schaffen kann. Im konkreten Fall war die Vorschrift des § 10 Absatz 2 Nummer 1 Hessisches Verfassungsschutzgesetz verfassungswidrig, weil die verfassungsrechtlich geforderte hinreichende Eingriffsschwelle von der Vorschrift nicht gewahrt wurde. Da das Bremische Verfassungsschutzgesetz keine Ermächtigungsgrundlage, entsprechende Auskünfte einzuholen, vorsieht, ermöglicht der Beschluss auch hier dem Gesetzgeber, gegebenenfalls notwendige gesetzliche Vorschriften verfassungskonform neu zu schaffen.

Intensiv setzt sich die Entscheidung anhand von § 20a Hessisches Verfassungsschutzgesetz mit den Voraussetzungen auseinander, unter denen Informationen durch das Landesamt für

Verfassungsschutz an die Strafverfolgungsbehörden übermittelt werden dürfen. Jede Datenübermittlung stellt einen neuen eigenständigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar und bedarf daher einer eigenständigen gesetzlichen Grundlage (BVerfG, aaO, Randnummer 194). Verfassungsrechtlich ist in diesen Sachverhaltskonstellationen eine Übermittlung von Daten nur dann zulässig, wenn diese dem Schutz eines herausragenden öffentlichen Interesses dient. Zusätzlich ist stets erforderlich, dass die Übermittlung personenbezogener Daten nur zur Verfolgung von besonders schweren Straftaten erfolgt (BVerfG, aaO, Randnummer 199). In Bezug auf den Verdachtsgrad fordert das Bundesverfassungsgericht daneben „konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis“ (BVerfG, aaO, Randnummer 199). Diese engen Voraussetzungen ergeben sich aus dem Kriterium der hypothetischen Datenneuerhebung, das danach fragt, wann eine Datenerhebung durch die Strafverfolgungsbehörden verfassungsrechtlich zulässig wäre (BVerfG, aaO, Randnummer 198).

In seiner neuen Entscheidung stellt das Bundesverfassungsgericht nunmehr klar, dass es auch nicht genügt, wenn im Gesetz als Voraussetzung für die Übermittlung von Daten lediglich genannt ist, dass diese der Verfolgung der in § 74a Gerichtsverfassungsgesetz (GVG) und § 120 GVG aufgeführten Delikten (Staatsschutzdelikten) dienen. Vielmehr muss auch in diesen Fällen gesetzlich definiert werden, dass es sich um besonders schwere Straftaten handelt (BVerfG, aaO, Randnummer 208). Insoweit § 20a Hessisches Verfassungsschutzgesetz daher ausreichen ließ, dass sich die Straftaten gegen ein Schutzgut der Verfassung richteten und nicht auch eine besonders schwere Straftat verlangte, genügt die Vorschrift daher nach der Entscheidung des Bundesverfassungsgerichtes nicht den verfassungsrechtlichen Anforderungen (BVerfG, aaO, Randnummer 214). Entsprechend ist es auf der Grundlage dieser neuen Rechtsprechung fraglich, ob § 21 Absatz 1 Nummer 1 BremVerfSchG, der ebenfalls nur an eine Straftat gemäß § 74a GVG und § 120 GVG anknüpft und ebenfalls nicht eine besonders schwere Straftat erfordert, den verfassungsrechtlichen Anforderungen genügt. Auch § 21 Absatz 1 Nummer 2 BremVerfSchG erfüllt diese Anforderungen möglicherweise nicht, weil in der Vorschrift nur von „sonstigen Straftaten, bei denen auf Grund ihrer Zielrichtung, des Motivs des Täters oder dessen Verbindung zu einer Organisation anzunehmen ist, dass sie sich gegen die in § 3 Absatz 1 Satz 1 BremVerfSchG genannten Schutzgüter wenden“, gesprochen wird. Auch hier muss erwogen werden, dass zusätzlich das Kriterium der besonders schweren Straftat aufgenommen wird.

Auf der anderen Seite lässt es das Bundesverfassungsgericht genügen, wenn die Übermittlung zur Strafverfolgung nach dem Hessischen Verfassungsschutzgesetz in Bezug auf Delikte erfolgt, die mit einer Höchststrafe von 10 Jahren Freiheitsstrafe sanktioniert werden können (BVerfG, aaO, Randnummer 203). Zudem darf auch eine Übermittlung von personenbezoge-

nen Informationen erfolgen, wenn dies der Strafverfolgung von Straftaten, die mit einer Höchststrafe von 5 Jahren Freiheitsstrafe bewährt sind, dient und dies auf Grund des jeweils geschützten Rechtsgutes, dessen Bedeutung für die Rechtsgemeinschaft und unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar ist (BVerfG, aaO, Randnummer 205). Auch in Bezug auf die Übermittlung von personenbezogenen Daten zur Strafverfolgung zeigt die Entscheidung daher Wege auf, wie das Grundrecht auf informationelle Selbstbestimmung und das Erfordernis der Strafverfolgung sachgerecht zum Ausgleich gebracht werden können. Da das Bremische Verfassungsschutzgesetz in § 21 BremVerfSchG von entsprechenden Weitergabemöglichkeiten bislang keinen Gebrauch macht, ist auch hier zu überprüfen, ob die Ermächtigungsnorm zur Weitergabe von Informationen entsprechend ergänzt werden sollte.

Schließlich präzisiert das Bundesverfassungsgericht auch die Anforderungen von Datenweiterleitungen an sonstige öffentliche Stellen. Auch hier ist Ausgangspunkt der Anforderungen an die gesetzlichen Ermächtigungsnormen das Kriterium der hypothetischen Datenneuerhebung (BVerfG, aaO, Randnummer 221). Daher gelten, soweit die empfangende Stelle über „operative Befugnisse“ verfügt, grundsätzlich dieselben Voraussetzungen wie bei der Weitergabe an Polizeibehörden (BVerfG, aaO, Randnummer 222). Da § 20b Hessisches Verfassungsschutzgesetz diesen Anforderungen nicht genügt, ist die Norm nach der Entscheidung des Bundesverfassungsgerichtes mit dem Grundgesetz unvereinbar. Die Auswirkungen auf die Vorschrift des § 20 BremVerfSchG, die einen vergleichbaren Sachverhalt regelt, sind daher ebenfalls zu bewerten.

Die Entscheidung zeigt, gerade wenn man die Regelungen des Bremischen Verfassungsschutzgesetzes an ihr misst, dass die verfassungsrechtlichen Vorgaben auch in der Freien Hansestadt Bremen eine angemessene Reaktion auf die Herausforderungen der aktuellen Sicherheitslage ermöglichen. Hierzu müssen aber einerseits die Gestaltungsräume, die sich verfassungsrechtlich ergeben, ohne Vorfestlegungen abgewogen und andererseits die neuen zwingenden Vorgaben, die aus der Rechtsprechung folgen, beachtet werden.

1.2 Verordnung über künstliche Intelligenz

Nach einer langen politischen Diskussion wurde auf europäischer Ebene die Verordnung über künstliche Intelligenz vom Europäischen Parlament am 13. März 2024 und vom Rat der Europäischen Union am 21. März 2024 beschlossen. Der endgültige Text wurde am 12. Juli 2024 verkündet und trat sodann 20 Tage später in Kraft. Mit dem Inkrafttreten beginnt nunmehr die Phase der Umsetzung dieses Gesetzgebungsaktes in Deutschland und in der Freien Hansestadt Bremen. Die Verordnung wird vollständig ab dem 2. August 2026 (Artikel 113 Verordnung über künstliche Intelligenz [KI-VO]), aber insbesondere das Verbot von einzelnen Prak-

tiken im KI-Bereich gemäß Artikel 5 KI-VO bereits ab dem 2. Februar 2025 gelten. Die Verordnung, die einen Gesetzesakt gemäß Artikel 289 Absatz 3 Vertrag über die Arbeitsweise der Europäischen Union darstellt, gilt in allen Mitgliedstaaten der Europäischen Union unmittelbar und es bedarf insofern keiner weiteren Umsetzungsakte; dem nationalen Gesetzgeber bleibt lediglich ein geringer Gestaltungsspielraum, etwa in Hinblick auf die Bestimmung der national zuständigen Behörden.

Mit der Verordnung über künstliche Intelligenz ist ein weiterer Baustein der Digital- und Datenregulierung der Europäischen Union in Kraft getreten. Die Verordnung über künstliche Intelligenz verfolgt den Zweck, „das Funktionieren des Binnenmarktes zu verbessern und die Einführung einer auf den Menschen ausgerichteten und vertrauenswürdigen künstlichen Intelligenz zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und die in der Charta verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, vor schädlichen Auswirkungen von KI-Systemen zu gewährleisten und die Innovationen zu unterstützen“ (Artikel 1 KI-VO). Die Verordnung ist daher dem Produktsicherheitsrecht zuzuordnen. Dementsprechend liegt der Verordnung über künstliche Intelligenz ein sehr differenziertes Risikoprogramm entsprechend der Gefährlichkeit des Einsatzes der künstlichen Intelligenz zu Grunde.

Besonders gefährliche Praktiken im KI-Bereich werden durch Artikel 5 KI-VO verboten. Dies betrifft etwa Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person (vergleiche Artikel 5 Absatz 1 Buchstabe a) KI-VO). Sodann werden unterschiedliche Regeln entsprechend der Gefährlichkeit der KI-Systeme etabliert. So führt die Einordnung als „Hochrisiko-KI-System“ (Artikel 6 KI-VO) zu strengen Anforderungen an das KI-System (Artikel 8 fortfolgende KI-VO). Zudem knüpfen sich weitere Pflichten der Anbieter, Händler und Betreiber an diese Einstufung (Artikel 16 fortfolgende KI-VO). Für KI-Systeme mit einem begrenzten Risiko sieht die Verordnung über künstliche Intelligenz vor allem Transparenzpflichten vor (Artikel 50 KI-VO). Aus Anlass von ChatGPT hat der europäische Gesetzgeber überdies Anforderungen und Pflichten für KI-Modelle mit allgemeinen Verwendungszwecken aufgenommen (Artikel 51 fortfolgende KI-VO). Sofern von KI-Systemen lediglich ein niedriges Risiko ausgeht, sieht die Verordnung über künstliche Intelligenz freiwillige Verhaltenskodizes vor (Artikel 95 KI-VO).

Ergänzend zur Verordnung über künstliche Intelligenz verfolgt die Datenschutzgrundverordnung das Ziel, „den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ zu gewährleisten (Artikel 1 Absatz 1 Datenschutzgrundverordnung [DSGVO]). Da von KI-Systemen auch in großem Umfang personenbezogene Daten verarbeitet werden, greifen auch die Pflichten und Rechte ein, die sich aus der Datenschutzgrundverordnung ergeben

(Artikel 2 Absatz 7 KI-VO). Dies gilt insbesondere für das Recht aus Artikel 22 DSGVO, wonach eine betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Bei der nationalen Gesetzgebung zur Verordnung über künstliche Intelligenz ist darauf zu achten, dass der Schutz des Rechts auf informationelle Selbstbestimmung nicht relativiert, sondern weiterhin auf der Grundlage der Datenschutzgrundverordnung umfassend gewährleistet wird. Eine möglichst starke Rolle der Landesdatenschutzbeauftragten bei der Umsetzung der Verordnung würde daher sowohl dem föderalen Charakter Deutschlands als auch den Erfordernissen des Schutzes der informationellen Selbstbestimmung entsprechen. Überdies ist der Anwendungsvorrang des Europarechtes zu beachten. Unabhängig davon stellen die neuen Entwicklungen auch den Landesbeauftragten für Datenschutz und Informationsfreiheit in der Freien Hansestadt Bremen vor neue Anforderungen, die zu den bereits bestehenden Aufgaben hinzutreten (siehe hierzu Ziffer 12.9 dieses Berichtes).

Die Fragen der Aufsicht und Regulierung dürfen dabei nicht den Blick dafür verstellen, dass der Einsatz künstlicher Intelligenz große Chancen für die Freie Hansestadt Bremen, ihre Gesellschaft und Wirtschaft bietet, die ergriffen werden müssen.

2. Bremische Bürgerschaft – Ergebnisse der Beratungen des 6. Jahresberichtes und des 5. Jahresberichtes nach Inkrafttreten der Datenschutzgrundverordnung

Der Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung (WMDID-Ausschuss) zum 6. Jahresbericht nach der Europäischen Datenschutzgrundverordnung der Landesbeauftragten für Datenschutz vom 18. März 2024 (Drucksache 21/341) und zur Stellungnahme des Senats vom 3. September 2024 (Drucksache 21/739) lag zum Redaktionsschluss noch nicht vor.

Der Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung (WMDID-Ausschuss) zum 5. Jahresbericht nach der Europäischen Datenschutzgrundverordnung vom 8. Februar 2024 (Drucksache 21/280) ist gemeinsam mit dem 5. Jahresbericht der Landesbeauftragten für Datenschutz vom 24. März 2023 (Drucksache 20/1835) und der Stellungnahme des Senats vom 27. Juni 2023 (Drucksache 21/3) von der Bürgerschaft (Landtag) in seiner Sitzung am 29. und 30. Mai 2024 zur Kenntnis genommen worden.

Von den im 5. Jahresbericht dargestellten Verstößen gegen die Datenschutzgrundverordnung bewertet der Ausschuss für Wissenschaft, Medien, Datenschutz, Informationsfreiheit und Digitalisierung als problematisch, dass die Wohnungsbaugesellschaft BREBAU GmbH in mehr als 9.500 Fällen personenbezogene Daten von Mietinteressentinnen und Mietinteressenten rechtswidrig, nämlich ohne Einwilligung beziehungsweise sonstige Grundlage, verarbeitet hat. Die Landesbeauftragte für Datenschutz und Informationsfreiheit informierte den Ausschuss darüber, dass sie eine Geldbuße in Höhe von 1,9 Millionen Euro verhängt habe. Der Ausschuss nahm positiv zur Kenntnis, dass die BREBAU GmbH neben der Löschung der unrechtmäßig erhobenen Daten weitere Maßnahmen zur Beseitigung der Missstände ergriffen hat.

3. Geldbußen

3.1 Allgemeines

Im Berichtsjahr 2024 lag der Schwerpunkt der aufsichtsbehördlichen Verfahren zur Festsetzung von Geldbußen gemäß Artikel 83 Datenschutzgrundverordnung (DSGVO)

- auf gegen Unternehmen festgestellte datenschutzrechtliche Verstöße aus den Jahren 2021 und 2022 sowie

- auf Einstellungen von Verfahren zur Festsetzung von Geldbußen.

Im Berichtsjahr hat der Landesbeauftragte für Datenschutz und Informationsfreiheit sein Ermessen wiederholt dahingehend ausgeübt, Verfahren aus Opportunitätsgründen einzustellen, und von der Verfolgung von datenschutzrechtswidrigen Verstößen abgesehen.

Es ergingen im Berichtsjahr gegen Unternehmen und natürliche Personen 13 Bescheide zur Verhängung von Geldbußen, die insgesamt 73 Geldbußen enthielten. Die Anzahl der verhängten Geldbußen divergiert mit der Anzahl der Bescheide, weil gegen eine verantwortliche Stelle in einem Bescheid mehrere Geldbußen verhängt werden können. Insgesamt wurden im Berichtsjahr Geldbußen in Höhe von 207.702,00 Euro verhängt. Hauptaugenmerk waren Verantwortliche im Bereich Insolvenzverwaltungen, die personenbezogene Daten von Bürgerinnen und Bürgern im Internet zu lange veröffentlicht hatten. Darüber hinaus gibt es Veröffentlichungen im bundesweiten Insolvenzregister, deren Datenumfang und Veröffentlichungsdauer präzise geregelt sind. Von den 13 erlassenen Bescheiden wurden neun im Berichtsjahr rechtskräftig. Aus dem Berichtsjahr befinden sich drei Bescheide zu Redaktionsschluss im Einspruchsverfahren. In 60 Fällen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit von der Verhängung einer Geldbuße in diesem Berichtsjahr abgesehen.

Im Berichtsjahr verteilten sich die Geldbußen nach Artikel 83 DSGVO auf die folgenden Bereiche: Fünf Bescheide gegen natürliche Personen und acht Bescheide gegen Unternehmen, davon vier Bescheide im Bereich Beschäftigtendatenschutz, zwei Bescheide im Bereich Soziales und zwei Bescheide gegen Rechtsanwaltsgesellschaften.

3.2 Ausnutzung der Patientendaten zur privaten Kontaktaufnahme mittels WhatsApp

Der Landesbeauftragte für Datenschutz und Informationsfreiheit verhängte im Berichtsjahr eine Geldbuße gegen einen Arzt, der unter Ausnutzung seiner beruflichen Stellung die Tele-

fonnummer seiner Patientin aus der Patientenakte entnahm, um mit ihr privat mittels Messenger-Dienst WhatsApp in Kontakt zu treten. Patientinnen- und Patientendaten dürfen ausschließlich zu Behandlungszwecken verwendet werden. Jede über diesen Zweck hinausgehende Nutzung der Patientinnen- und Patientendaten ist grundsätzlich untersagt und bedarf im Falle einer privaten Kontaktaufnahme einer ausdrücklichen Einwilligung, die in diesem Fall zu keinem Zeitpunkt von der Patientin erteilt wurde.

3.3 Rechtswidrige Verarbeitung der Daten von Schulungsteilnehmenden

Ferner sanktionierte der Landesbeauftragte für Datenschutz und Informationsfreiheit ein Weiterbildungsunternehmen im Jahr 2024 mit drei Geldbußen wegen unbegrenzter und intransparenter Verarbeitung personenbezogener Daten der Schulungsteilnehmerinnen und Schulungsteilnehmer.

Das verantwortliche Unternehmen verwendete zwecks Datenverwaltung ein IT System, das keine Löschung der Daten vorsah. Stattdessen wurden die Datensätze nach Ablauf der Aufbewahrungsfrist lediglich als „deaktiviert“ gekennzeichnet. Zum Zeitpunkt der von dem Landesbeauftragten für Datenschutz und Informationsfreiheit durchgeführten Vor-Ort-Prüfung waren im IT-System mindestens 2.600 deaktivierte Datensätze ehemaliger Schulungsteilnehmerinnen und Schulungsteilnehmer enthalten, die nach Ablauf der vorgegebenen Aufbewahrungsfristen bereits hätten gelöscht werden müssen.

Ferner verstieß das Weiterbildungsunternehmen gegen das Transparenzgebot gemäß Artikel 12 Absatz 1 Datenschutzgrundverordnung (DSGVO) und verletzte seine Informationspflichten gegenüber den Schulungsteilnehmerinnen und Schulungsteilnehmern gemäß Artikel 13 DSGVO, weil die Schulungsverträge keine ausreichenden und zum Teil widersprüchliche Informationen über die Verarbeitung personenbezogener Daten der Schulungsteilnehmerinnen und Schulungsteilnehmer enthielten. Insbesondere fehlten eindeutige Angaben zur Dauer der Speicherung.

3.4 Unberechtigter Zugriff auf personenbezogene Daten

Der Landesbeauftragte für Datenschutz und Informationsfreiheit ahndete zudem mehrere Fälle des unberechtigten Zugriffes auf personenbezogene Daten durch Personen, die auf Grund ihrer beruflichen Stellung Zugang zu diesen Daten hatten.

In vier Fällen wurden im Jahr 2024 gegen natürliche Personen Geldbußen wegen Ausnutzung ihrer beruflichen Stellungen verhängt. Zwei Bankmitarbeiter griffen auf die Umsatzdaten einer Kundin zu, ohne dass hierfür ein dienstlicher Grund vorlag. Eine Mitarbeiterin des Jobcenters griff auf den Datensatz eines Kunden zu und verwendete die darin enthaltenen Informationen

zur Höhe der Auszahlungen zu Privatzwecken, um einen Kommentar zu einem beim Instagram geposteten Beitrag zu verfassen.

Eine Polizeibeamtin tätigte 50 unberechtigte Abfragen zu ihrem Ex-Ehemann in den polizeilichen Informationssystemen ohne Anweisung durch Vorgesetzte und ohne dienstliches Interesse.

3.5 Mangelnde technisch-organisatorische Maßnahmen bei der Verarbeitung von Beschäftigtendaten

Im Berichtsjahr erging außerdem ein Bescheid gegenüber einem Unternehmen in der Freien Hansestadt Bremen wegen des unrechtmäßigen Umgangs mit personenbezogenen Beschäftigtendaten. Aufgrund der Anzahl und des Umfanges der betroffenen Daten wurden gegenüber der verantwortlichen Stelle Geldbußen im insgesamt fünfstelligen Bereich verhängt.

Von einem leitenden Beschäftigten der verantwortlichen Stelle wurden parallele Ordnerstrukturen geschaffen. Auf die als Kopie erstellten Ordner konnten mehr Beschäftigte als erforderlich zugreifen. Circa 40 Beschäftigte konnten dadurch unbefugt umfangreiche Beschäftigten- und Gesundheitsdaten nutzen. In den Ordnern befanden sich unter anderem Anträge auf Höhergruppierungen, Excel-Tabellen mit Abwesenheitszeiten, Listen mit Wünschen für Überstunden, Dokumente zur Pandemiebekämpfung, Dokumente zu Gesundheit und Gesundheitsquoten, Protokolle von Mitarbeitendengesprächen, Gleitzeitsalden, Einschätzungen über Beschäftigte sowie E-Mail-Verläufe. Außerdem wurde von der verantwortlichen Stelle in drei Fällen keine Informationen hinsichtlich der in den oben genannten Ordnern enthaltenen personenbezogenen Daten nach Artikel 15 Datenschutzgrundverordnung beauskunftet.

4. Datenschutzbeauftragte und Allgemeines öffentliche Stellen

4.1 Gleichzeitige Benennung von Datenschutzbeauftragten durch Verantwortliche

Im Berichtszeitraum erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit erneut einige Beratungsanfragen bezüglich der Benennungen von zwei oder mehreren gleichrangigen Datenschutzbeauftragten durch dieselbe verantwortliche Stelle. Zu diesem Thema gab es auch eine entsprechende Umfrage im Arbeitskreis Gesundheit und Soziales der Datenschutzaufsichtsbehörden in Bezug auf die Frage, ob eine Krankenkasse zwei gleichrangige Datenschutzbeauftragte benennen darf.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist der Auffassung, dass die verantwortliche Stelle oder die Auftragsverarbeitenden gemäß Artikel 37 Absatz 1 Buchstabe a) Datenschutzgrundverordnung (DSGVO) nur eine natürliche Person als Datenschutzbeauftragte oder Datenschutzbeauftragten benennen darf. Die Benennung von zwei oder mehr gleichrangigen Datenschutzbeauftragten mit identischen Aufgaben ist unzulässig. Die beziehungsweise der Datenschutzbeauftragte muss ihre oder seine Aufgaben gemäß Artikel 38 Absatz 3 DSGVO weisungsfrei und unabhängig ohne Beeinflussung ihrer oder seiner Bewertungen wahrnehmen können. Die gleichrangige Benennung von zwei oder mehr Datenschutzbeauftragten könnte unter anderem zu Interessenkonflikten und auch unterschiedlichen Bewertungen führen, bei deren Vorliegen die Verantwortlichen oder die Auftragsverarbeitenden die ihr beziehungsweise ihm genehmere Variante berücksichtigen könnten und hierdurch die oder der andere Beauftragte geschwächt würde.

Allerdings schließt der Landesbeauftragte für Datenschutz und Informationsfreiheit die Benennung von mehreren Datenschutzbeauftragten nicht gänzlich aus, wobei eine konkrete Abgrenzung der Zuständigkeiten für unterschiedliche Bereiche zu erfolgen hat. Durch die Abgrenzung dürfen die zu gewährleistende Weisungsfreiheit und Unabhängigkeit nicht beeinträchtigt sein. Für die Aufsichtsbehörde muss eine bestimmte Ansprechpartnerin oder ein bestimmter Ansprechpartner für einen konkreten Aufgabenbereich bei ihr gemeldet sein.

Ein weiteres denkbares Szenario für die Benennung einer beziehungsweise eines zweiten Datenschutzbeauftragten bestände, wenn das Amt der oder des Datenschutzbeauftragten für einen längeren Zeitraum ruht und die beziehungsweise der Zweitbeauftragte in dieser Zeit vollwirkend die Aufgaben mit den gleichen Rechten und Pflichten bis zur Rückkehr der beziehungsweise des primär bestellten Datenschutzbeauftragten übernimmt.

4.2 Aktuelle Fälle aus dem Berichtsjahr im Hinblick auf die Umsetzung von Artikel 37 Datenschutzgrundverordnung

Im Jahr 2024 erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit von Verantwortlichen und Auftragsverarbeitenden rund 359 Meldungen nach Artikel 37 Absatz 7 Datenschutzgrundverordnung (DSGVO) im Hinblick auf die Benennung von behördlichen und betrieblichen Datenschutzbeauftragten. Wie bereits in den Vorjahren erfolgten die Meldungen der Datenschutzbeauftragten größtenteils über das Meldeformular der Homepage des Landesbeauftragten für Datenschutz und Informationsfreiheit, das er allen Meldepflichtigen zur Einhaltung ihrer oder seiner Meldeverpflichtung anbietet. Grundsätzlich werden alle eingegangenen Meldungen zum Zweck der Einhaltung der Vorschriften der Datenschutzgrundverordnung von dem Landebeauftragten für Datenschutz und Informationsfreiheit auf die Konformität der Benennung geprüft und verwaltet. Aber auch bereits im Vorfeld der Benennung einer beziehungsweise eines Datenschutzbeauftragten prüft der Landesbeauftragte für Datenschutz und Informationsfreiheit, ob diese zulässig ist.

Trotz der in Artikel 38 Absatz 6 DSGVO geforderten Vermeidung von Inkompatibilitäten erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit mehrfach Meldungen, die auf einen etwaigen Interessenkonflikt im Einzelfall geprüft werden mussten. Hat die oder der Beauftragte neben der Beauftragtenfunktion andere Aufgaben und Pflichten, die sie oder er zusätzlich erfüllen muss, kann dies die Wahrnehmung der Aufgaben der oder des Datenschutzbeauftragten erheblich beeinträchtigen, sodass diese nicht, wie es die Datenschutzgrundverordnung verlangt, möglich ist. Dies ist insbesondere der Fall, wenn die Beauftragte oder der Beauftragte in anderer Funktion getroffene Entscheidungen hinsichtlich der Datenverarbeitung selbst kontrollieren muss. Nicht mit der Funktion der oder des Datenschutzbeauftragten betraut werden können daher Personen, die als Leitungsperson einen Zuständigkeitsbereich haben, der unter anderem personenbezogene Datenverarbeitungen umfasst.

In Bezug auf die erforderliche Benennung einer oder eines Datenschutzbeauftragten bei einem kleinen Verein, von dem Gesundheitsdaten verarbeitet werden, klärte der Landesbeauftragte für Datenschutz und Informationsfreiheit somit im Berichtszeitraum unter anderem gemeinsam mit dem Verein, wer dort die Aufgaben der oder des Datenschutzbeauftragten wahrnehmen kann. Da sich keine interne Lösung anbot, wurde letztlich ein externer Datenschutzbeauftragter benannt.

Hinsichtlich eines Unternehmens ist gegenwärtig in einem Fall zu prüfen, ob dort der Prokurist zum Datenschutzbeauftragten benannt werden darf. In diesem Fall ist zu klären, in welchem Umfang die Prokura erteilt wurde und ob sie auch Entscheidungsbefugnisse hinsichtlich der

personenbezogenen Datenverarbeitung des Unternehmens umfasst, was mit einem umfangreichen Schriftwechsel verbunden ist. Hierbei ist zu beachten, dass der Datenschutzbeauftragte nicht gleichrangig zum Geschäftsführer steht und wie dieser gleichermaßen entscheidend für das Unternehmen tätig wird. Eine abschließende Klärung steht in diesem Fall noch aus.

4.3 Deutschland online – Datenschutzcockpit

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat gemeinsam mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Entwicklung des Datenschutzcockpits begleitet. In dem Datenschutzcockpit können Bürgerinnen und Bürger sehen, welche öffentlichen Stellen aus welchem Grund ihre persönlichen Daten unter Verwendung der Identifikationsnummer nach dem Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung (Identifikationsnummerngesetz) ausgetauscht haben. Unter Einhaltung der Datenschutzbestimmungen sowie nach der expliziten Zustimmung der betroffenen Personen dürfen bestimmte öffentliche Stellen diese Daten wiederverwenden und untereinander austauschen; dieses soll den Bürgerinnen und Bürgern ersparen, ihre Daten mehrfach anzugeben. Als Beispiel kann hier der Online-Service ELFE (Einfach Leistungen für Eltern) aufgeführt werden. So können verschiedene Leistungen bei unterschiedlichen Behörden gleichzeitig beantragt werden, in diesem Fall beispielsweise die Geburtsurkunde sowie das Eltern- und Kindergeld.

In einem regelmäßigen konstruktiven Austausch, an dem neben dem Landesbeauftragten für Datenschutz und Informationsfreiheit und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit auch der Senator für Finanzen, das Bundesministerium des Innern und für Heimat, das Bundesverwaltungsamt, das Bundesamt für Sicherheit in der Informationstechnik und Entwicklerinnen und Entwickler des Datenschutzcockpits teilnehmen, werden unterschiedliche Themen, zum Beispiel zur technischen Ausgestaltung und zu verschiedenen Rechtsfragen, besprochen und über den Projektfortschritt informiert. Durch das Einbinden der Datenschutzaufsichtsbehörden konnte bereits seit Projektbeginn unter anderem auf die Einhaltung des Datenschutzgrundsatzes „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ (Artikel 25 Datenschutzgrundverordnung) geachtet werden.

Das Datenschutzcockpit wurde im Berichtsjahr in Betrieb genommen und kann unter https://datenschutzcockpit.bund.de von allen Bürgerinnen und Bürgern mit Hilfe des elektronischen Personalausweises genutzt werden. Allerdings sind noch nicht alle registerführenden Stellen an dieses System angebunden. Daher wird nicht zeitnah gewährleistet sein, dass die

Bürgerinnen und Bürger ihre Informations-, Kontroll- und Mitwirkungsmöglichkeiten vollständig wahrnehmen können.

4.4 Microsoft 365

Immer wieder wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtsjahr zur Rechtmäßigkeit der Nutzung von Microsoft 365 befragt. Durch die große Anzahl an unterschiedlichen Versionen – alleine zwei unterschiedliche Versionen für Privatpersonen, vier unterschiedliche Versionen für Unternehmen („Business“), drei Versionen für Großunternehmen („Enterprise“), drei Versionen für Bildungseinrichtungen sowie jeweils eine Version für die öffentliche Verwaltung („Government“) und für gemeinnützige Organisationen („Nonprofit“) – ist es kaum möglich, fundierte Aussagen zu jeder Anfrage zu treffen. Dazu müsste neben der rechtlichen Prüfung der Verträge auch eine technische Untersuchung durchgeführt werden, die insbesondere bei proprietärer Software, sogenannter geschlossener Software, deren Quellcode nicht einsehbar ist und deren Benutzerinnen und Benutzer auf die Vorgaben des Herstellers angewiesen sind, nur mit unverhältnismäßig hohem Aufwand zu gewährleisten wäre.

Die Tatsache, dass eine Prüfung nur sehr schwer bis unmöglich ist, bedeutet jedoch nicht, dass es keine weiteren Kritikpunkte gibt. So ist die Übertragung von personenbezogenen Daten in Drittstaaten trotz des bestehenden Angemessenheitsbeschlusses nach wie vor sehr problematisch; die KI-gestützten Funktionen in den Office-Modulen „Delv“ und „Workplace Analytics“ können große Datenmengen analysieren, um produktive Arbeitsmuster zu erkennen, und so detaillierte Einblicke in das Verhalten und die Leistung einzelner Mitarbeiterinnen und Mitarbeiter liefern; die Erhebung von Metadaten durch Microsoft zu Analysezwecken und zur Weiterentwicklung von Diensten könnte unter anderem ein Verstoß gegen den Datenschutzgrundsatz der Zweckbindung sein.

Aufgrund der Komplexität des Systems und der Tatsache, dass sich dieses beispielsweise durch Updates jederzeit verändern kann, sowie der nach wie vor nicht geklärten – oben dargestellten – Kritikpunkte wird die Nutzung zum jetzigen Zeitpunkt als nicht datenschutzkonform angesehen.

4.5 VIS Einheitsmandant

Im Berichtsjahr wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit seitens des Gesamtpersonalrats im Rahmen des Mitbestimmungsverfahrens zum VIS Einheitsmandanten um Stellungnahme gebeten, insbesondere mit dem Schwerpunkt auf die Verarbeitung von Beschäftigtendaten. Die Freie Hansestadt Bremen hat das Ziel, die digitale und vor allem auch ressortübergreifende Zusammenarbeit zu verbessern, auszubauen und zu stärken. Zu

diesem Zweck wird das digitale Schriftgut der bremischen Verwaltung übergreifend in einem einzigen – technischen – Mandanten dem sogenannten „Einheitsmandanten“ im Dokumentenmanagement-System VIS gebündelt gespeichert und verarbeitet.

Im Einheitsmandanten werden zum Zweck der dienststellenübergreifenden Zusammenarbeit stets Geschäftsgangverfügungen genutzt. Darüber können Akten, Vorgänge oder Dokumente „zur Bearbeitung“ oder „zur Kenntnis“ Mitarbeitenden auch dann zugänglich gemacht werden, wenn diese eigentlich keine Zugriffsberechtigung auf diese Objekte haben. Dies gilt unabhängig davon, ob die Adressaten einer Dienststelle angehören oder in anderen Dienststellen beschäftigt sind. Geschäftsgangverfügungen, die Adressaten bei anderen Verantwortlichen gemäß Artikel 4 Absatz 1 Nummer 7 der Datenschutzgrundverordnung (DSGVO) zum Ziel haben, stellen im Sinne des Datenschutzes eine Übermittlung personenbezogener Daten dar. Dazu bedarf es gemäß Artikel 6 DSGVO stets einer Rechtsgrundlage.

Dies betrifft zunächst personenbezogene Inhaltsdaten in Word-Dokumenten, PDF-Dateien oder E-Mails des zugehörigen VIS-Objektes, zum Beispiel Akte, Vorgang, Dokument, aber auch vollumfänglich die stets in den Metadaten des VIS-Objektes enthaltenen personenbezogenen oder personenbeziehbaren Daten zu Beschäftigten, die sogenannten Beschäftigtendaten. Alle diese personenbezogenen Daten werden in jedem Fall im Rahmen einer Geschäftsgangverfügung den Adressaten offenbart. Auch wenn in den Inhaltsdaten keine personenbezogenen Daten enthalten sein sollten, sind Beschäftigtendaten betroffen. Personenbezogene Daten aller VIS-Nutzenden, die an dem jeweiligen VIS-Objekt aktiv tätig waren, sind mit dem VIS-Objekt verbunden. Daher ist für die Entscheidung, ob eine Übermittlung personenbezogener Daten zulässig ist, im Rahmen von Geschäftsgangverfügung sowohl die Übermittlung der Inhaltsdaten als auch die Übermittlung der Metadaten zu prüfen.

Die Verarbeitung von Beschäftigtendaten ist auf Grundlage von § 12 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) in Verbindung mit § 85 Bremisches Beamtengesetz (BremBG) zulässig, soweit dies im Rahmen der Personalverwaltung oder Personalwirtschaft, insbesondere zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, einschließlich zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist und dadurch schutzwürdige Belange der betroffenen Person nicht beeinträchtigt werden oder eine Rechtsvorschrift dies erlaubt. Eine Übermittlung von Beschäftigtendaten im Rahmen von Geschäftsgangverfügungen kann hierauf jedoch nicht gestützt werden.

Zudem ist folgendes zu beachten: Da in dem elektronischen Aktensystem VISkompakt alle berechtigten Personen, auch verantwortlichenübergreifend, also, wenn zwei oder mehr Verantwortliche gemäß Artikel 4 Absatz 1 Nummer 7 DSGVO involviert sind, die im VIS-Objekt

gespeicherten Daten im Sinne des Artikel 4 Absatz 1 Nummer 2 DSGVO verarbeiten können, ändern sich damit mit jeder einzelnen Aktion Art und Umfang der im VIS-Objekt gespeicherten personenbezogenen Daten. Das kann dazu führen, dass die Übermittlung des Datenbestandes damit ab diesem Zeitpunkt unzulässig wird. Technisch ist durch zeitlich vorher liegende „alte“ Geschäftsgangverfügungen dann die Vergabe der Zugriffsberechtigungen bereits geschehen. Durch jede dieser Aktionen erfolgt dann zwangsläufig eine Offenbarung von personenbezogenen Daten gegenüber Dritten. Dies gilt im Übrigen für beide „Richtungen“: Auch auf der Seite des eine Geschäftsgangverfügung empfangenden Verantwortlichen ist stets vor Verarbeitung im Sinne des Artikel 4 Absatz 1 Nummer 2 DSGVO zu prüfen, ob die Übermittlung der personenbezogenen Daten zulässig ist.

Durch die Geschäftsgangverfügung erfolgt eine Übermittlung personenbezogener Daten, aber keine technische Datenübertragung. Es gibt daher niemals eine klar definierte, klar abgegrenzte Menge personenbezogener Daten, die übermittelt werden. Vielmehr handelt es sich um einen Datenbestand, der einer fortwährenden Wandlung unterliegt. Die Menge personenbezogener Daten wächst dabei stetig an, selbst bei VIS-Objekten, in deren Inhaltsdaten gar keine personenbezogenen Daten enthalten sind, weil hier die Menge personenbezogener Daten im Hinblick auf Beschäftigtendaten mit jeder Aktion stetig ansteigt.

Hier kommt daher ein Verstoß gegen die Anforderungen des Artikel 5 Absatz 2 (Rechenschaftspflicht) in Verbindung mit Artikel 5 Absatz 1 Buchstaben a) (Rechtmäßigkeit), b) (Zweckbindung), c) (Datenminimierung) sowie f) (Integrität und Vertraulichkeit) DSGVO sowie gegen Artikel 6 DSGVO in Betracht.

Für eine vollständige elektronische Aktenführung ist eine umfangreiche Verarbeitung von Beschäftigtendaten erforderlich. Es sind bislang keine ausreichenden Maßnahmen oder Mechanismen technischer oder organisatorischer Art erkennbar, mit denen den sich aus der Verarbeitung der Beschäftigtendaten ergebenden Fragestellungen begegnet werden könnte und die eine datenschutzkonforme Datenverarbeitung mehrerer Verantwortlicher in einem einzigen Mandanten ermöglichen.

Das Systemdesign des zugrundeliegenden VISkompakt ist nicht ohne Weiteres geeignet, um eine datenschutzkonforme, gemeinsame Nutzung des Systems in einem Einheitsmandanten zu realisieren. In einem gemeinsam von mehr als einem Verantwortlichen genutzten Mandanten ist es datenschutzrechtlich unzulässig, Geschäftsgangverfügungen über die Grenzen der jeweils einzelnen Verantwortlichen hinweg zu verwenden, sofern keine ausreichende datenschutzrechtliche Ermächtigung vorliegt.

Zudem ist es äußerst komplex, die Betroffenenrechte nach Artikel 15 fortfolgende DSGVO zu gewährleisten. In VISkompakt fehlt eine Möglichkeit, systematisch die personenbezogenen

Daten, die zum Zeitpunkt der Recherche im Zugriff aller Beschäftigten eines Verantwortlichen liegen, zu durchsuchen. Demzufolge kann der Verantwortliche seiner Pflicht nicht nachkommen, Betroffenen eine umfassende, vollständige und korrekte Auskunft zu geben. Eine effektive Datenschutzkontrolle durch eigene behördliche Datenschutzbeauftragte oder die Aufsichtsbehörde ist ebenfalls gegenwärtig nicht gewährleistet; die Anforderungen aus Artikel 5 Absatz 2 DSGVO (Rechenschaftspflicht) können aktuell nicht erfüllt werden.

5. Inneres

5.1 Gemeldete Datenschutzverletzungen

Im Bereich Inneres sind von den Polizeibehörden sowie den Bürger- und Ordnungsämtern insgesamt neun Meldungen von Verletzungen des Schutzes personenbezogener Daten eingegangen. Diesen Meldungen lag überwiegend eine fehlerhafte Versendung von Briefen und E-Mails zugrunde.

5.2 Polizeiliche Videoüberwachungen

In den vergangenen Jahresberichten (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.2 sowie 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.2) hat die Landesbeauftragte für Datenschutz und Informationsfreiheit die Ausweitung der polizeilichen Videoüberwachungen sehr kritisch begleitet. Dieses Berichtsjahr wurde die Überwachung von Volksfesten (Osterwiese, Breminale, Maritime Tage, Freimarkt, Weihnachtsmarkt) ausgedehnt und die Anzahl der überwachten öffentlichen Plätze (Bürgermeister-Koschnik-Platz, Hillmannplatz) in der Stadt Bremen erhöht.

Die polizeiliche Überwachung von Volksfesten und öffentlichen Plätzen stellt einen Eingriff von erheblichem Gewicht in die Rechte und Freiheiten betroffener Personen dar, der mit dem angenommenen Nutzen der Überwachung aufgewogen werden muss. So muss die Überwachung etwa zum Erreichen der verfolgten Ziele hinreichend geeignet sein.

Dies kann nach der Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit in Hinblick auf die konkrete Ausgestaltung der Maßnahme in ihrer Anwendung dazu führen, dass ihre Geeignetheit zu verneinen, zumindest aber zu bezweifeln ist. Wenn etwa auf der Osterwiese oder der Breminale nur eine Überwachung von kleinen Ausschnitten erfolgt und es infolgedessen vom Zufall abhängt, ob eine Tat von den Kameras erfasst wird, ist kritisch zu hinterfragen, ob von einer Erhöhung der Sicherheit auf Volksfesten gesprochen werden kann. Vergleichbar stellt sich die Situation am Hillmannplatz dar: Wenn die Kameras den eigentlichen Kriminalitätsschwerpunkt gar nicht erfassen, können sie die Sicherheit auf und um den Platz nicht erhöhen und führen infolgedessen zu einem unverhältnismäßigen Grundrechtseingriff auf Seiten der betroffenen Personen. Im Einzelfall können aber auch generalpräventive Effekte in die Beurteilung einbezogen werden.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit und nunmehr der Landesbeauftragte für Datenschutz und Informationsfreiheit haben bei der Überprüfung der Umsetzung der Überwachungsmaßnahmen datenschutzrechtliche Defizite feststellt (siehe zum Bremer Weihnachtsmarkt 2023 bereits 6. Jahresbericht nach der Datenschutzgrundverordnung,

Ziffer 6.2.2; Silvester 2023/2024: keine Schwärzungen von Wohnungen der Grohner Dühne, Nichtbeachtung der Tatbestandsvoraussetzungen des § 32 Absatz 1 Bremisches Polizeigesetz (BremPolG); Osterwiese 2024: Unvollständigkeit der übermittelten Protokolldaten; Weihnachtsmarkt 2024: kein Abschalten der Kameras während einer Versammlung).

Der Landesbeauftragte für Datenschutz und Informationsfreiheit fordert daher weiterhin, dass die Videoüberwachung in quantitativer Hinsicht auf wenige Fälle beschränkt wird. Insbesondere bei der Überwachung von Volksfesten ist aus der Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit eine Gesetzesänderung mit dem Inhalt notwendig, dass diese nur zulässig ist, wenn eine ausreichende Gefahrprognose für diese Feste vorliegt. In qualitativer Hinsicht ist ferner eine Verbesserung erforderlich, insbesondere durch den Einsatz besserer Technik, um die Geeignetheit der Überwachung zur Verfolgung der avisierten Ziele sicherzustellen.

Des Weiteren fordert der Landesbeauftragte für Datenschutz und Informationsfreiheit die Berücksichtigung milderer Maßnahmen. So bietet es sich an Orten, für die die Videoüberwachung geprüft wird, möglicherweise an, zunächst auf eine Umgestaltung zu setzen, bevor auf die eingriffsintensive Maßnahme der Videoüberwachung zurückgegriffen wird.

5.3 Evaluation Bremisches Polizeigesetz

Gemäß § 150 Satz 1 Bremisches Polizeigesetz (BremPolG) alte Fassung, in Kraft vom 5. Dezember 2023 bis 28. Juni 2024, war die praktische Anwendung der §§ 41 bis 44 BremPolG bis zum 31. August 2023 zu evaluieren. Die Gültigkeit der Vorschriften (§ 41: Datenerhebung durch den verdeckten Einsatz technischer Mittel, § 42: Telekommunikationsüberwachung und Eingriff in die Telekommunikation, § 43: Verkehrs-, Nutzungs- und Standortdatenerhebung, § 44: Bestandsdatenerhebung) war nach § 152 Absatz 4 BremPolG alte Fassung bis zum 30. Juni 2024 beschränkt. Entgegen der gesetzlichen Vorgaben fand die Evaluation erst in der ersten Jahreshälfte 2024 statt. Zwecks Evaluation wurden vom Senator für Inneres und Sport zwei Gutachten in Auftrag gegeben. Diese sowie ein an die Evaluation anknüpfender Entwurf zur Änderung des Bremischen Polizeigesetzes wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit zur Stellungnahme übermittelt.

Aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit ist insbesondere zu kritisieren, dass nach der gutachterlichen Darstellung keine hinreichende polizeiliche Dokumentation der genannten Maßnahmen erfolgte und die Einhaltung der jeweiligen Tatbestandsvoraussetzungen sowie die Erfüllung der jeweiligen Benachrichtigungspflichten nicht durchgehend nachvollziehbar waren. Diese skizzierten Zweifel konnten nach der Lesart des Landesbeauftragten für Datenschutz und Informationsfreiheit bislang nicht vollständig in belegbarer Weise ausgeräumt werden. So heißt es in dem Gutachten von Herrn Professor

Stauch: „[…] in 4 Fällen könnten Zweifel an der Eingriffsschwelle bestehen […].“ (Stauch, Evaluation nach § 150 BremPolG, Seite 10). Und weiter: „Nur in einem der 75 Fälle lässt sich aufgrund der Dokumentation feststellen, ob die Betroffenen von der durchgeführten Maßnahme benachrichtigt und über ihre Rechte belehrt wurden“ (Stauch, am angegebenen Ort, Seite 15). Der Landesbeauftragte für Datenschutz und Informationsfreiheit fordert daher zu einer ordnungsgemäßen Dokumentation auf, aus der sich unmittelbar ergibt, dass die Eingriffsschwellen bei diesen zum Teil sehr eingriffsintensiven Maßnahmen eingehalten und die Betroffenenrechte gewahrt werden. In seiner Beratungsfunktion hat der Landesbeauftragte für Datenschutz und Informationsfreiheit seine Unterstützung bei Optimierung der Dokumentationsprozesse angeboten.

Des Weiteren hat sich aus den Gutachten zwar ergeben, dass die Polizeibehörden auf die evaluierten Befugnisse angewiesen sind, weshalb der Landesbeauftragte für Datenschutz und Informationsfreiheit sich auch nicht gegen eine Verlängerung dieser Befugnisse ausgesprochen hat, eine angedachte Erweiterung der Befugnisse wurde von ihm jedoch kritisch bewertet. Er begrüßt daher, dass die Erweiterung nicht, wie im Gesetzesentwurf zunächst vorgesehen, stattgefunden hat.

Anlass für seine kritische Positionierung ist dabei nicht nur die unzureichende Dokumentation, sondern auch, dass nach seiner Bewertung der Evaluationsprozess kein Bedürfnis einer umfangreichen Erweiterung aufgezeigt hat. Insbesondere die Subsidiaritätsklausel aus § 43 Absatz 3 Satz 1 BremPolG, nach der der Standort eines Mobilfunktelefons nur ermittelt werden darf, wenn die Ermittlung des Aufenthaltsortes der betroffenen Person auf andere Weise weniger erfolgversprechend oder erschwert wäre, ist aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit unter allen Umständen beizubehalten. Die Maßnahme der Standortdatenerhebung nach § 43 Absatz 3 BremPolG ist im Vergleich zu den übrigen von den Gutachtern genannten Maßnahmen die eingriffsintensivste und sollte daher auch zukünftig erst zur Anwendung gelangen, wenn anderweitig die Ermittlung des Aufenthaltsortes weniger erfolgsversprechend oder erschwert ist.

5.4 Datenschutzgrundverordnung und Parlamente, Datenaustausch zur Beantwortung parlamentarischer Anfragen

Mit Urteil vom 16. Januar 2024 (Aktenzeichen C-33/22) hat der Europäische Gerichtshof entschieden, dass die Datenschutzgrundverordnung grundsätzlich auch auf Landtage Anwendung findet und für sie die regulären Bestimmungen zur datenschutzrechtlichen Aufsicht gelten. Im Zuge dessen hat der Europäische Gerichtshof insbesondere die Frage verneint, ob, wie zum Teil bislang auf nationaler Ebene vertreten, die parlamentarische (Kern-)Tätigkeit unter die Ausnahme des Artikel 2 Absatz 1 Buchstabe a) Datenschutzgrundverordnung

(DSGVO) fällt. Nach Artikel 2 Absatz 1 Buchstabe a) DSGVO wird eine Verarbeitung personenbezogener Daten ausnahmsweise nicht von der Datenschutzgrundverordnung erfasst, wenn sie im Rahmen einer Tätigkeit erfolgt, die nicht in den Anwendungsbereich des Unionsrechtes fällt. Der Europäische Gerichtshof möchte diesen Ausnahmetatbestand jedoch vor allem auf Angelegenheiten der nationalen Sicherheit beschränken und hat hinsichtlich der parlamentarischen Tätigkeit die Anwendbarkeit der Datenschutzgrundverordnung bejaht.

Aufgrund dieser Entscheidung hat sich der Landesbeauftragte für Datenschutz und Informationsfreiheit am Anfang des Berichtsjahres an die Präsidentin der Bremischen Bürgerschaft gewandt und sie auf das Urteil sowie dessen Auswirkungen hingewiesen. Infolge des Urteils ist § 2 Absatz 4 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG), der bislang die Bremische Bürgerschaft von der Anwendung dieses Gesetzes und der Datenschutzgrundverordnung ausnimmt, nicht mehr anzuwenden und zu streichen. Des Weiteren hält der Landesbeauftragte für Datenschutz und Informationsfreiheit es für notwendig, die Verarbeitung personenbezogener Daten durch die Bremische Bürgerschaft, ihre Mitglieder, ihre Gremien, die Deputationen sowie durch die Fraktionen und Gruppen ausdrücklich im Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung zu regeln. Außerdem spricht er sich für eine gesetzliche Regelung der datenschutzrechtlichen Aufsicht über die Bremische Bürgerschaft aus. Auch unter diesem Aspekt erachtet der Landesbeauftragte für Datenschutz und Informationsfreiheit daher eine Anpassung des Bremischen Ausführungsgesetzes zur EU-Datenschutz-Grundverordnung für sachgerecht. Bis zur Einrichtung einer derartigen Kontrollstelle nach den Vorgaben der Datenschutzgrundverordnung übt der Landesbeauftragte für Datenschutz und Informationsfreiheit die datenschutzrechtliche Aufsicht nach Artikel 55 DSGVO, § 40 Bundesdatenschutzgesetz, § 21 Absatz 1 BremDSGVOAG über die Bremische Bürgerschaft aus.

Das Urteil bestärkt zugleich den Landesbeauftragten für Datenschutz und Informationsfreiheit auch in seiner Auffassung zum behördlichen Datenaustausch zwecks Beantwortung parlamentarischer Anfragen. Im 6. Jahresbericht nach der Datenschutzgrundverordnung legte die Landesbeauftragte für Datenschutz und Informationsfreiheit unter Ziffer 6.8 dar, dass dieser Datenaustausch unter die Datenschutzgrundverordnung und gegebenenfalls unter die Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates (EU-Richtlinie) falle, mangels entsprechender Rechtsgrundlagen aber derzeit gegebenenfalls rechtswidrig ist. Vor dem Hintergrund, dass nach der Rechtsprechung des Europäischen Gerichtshofes nunmehr sogar die parlamentarische Tätigkeit unter die Datenschutzgrundverordnung fällt, gilt diese Schlussfolgerung erst recht.

5.5 Telenotarzt

Im Berichtsjahr begleitete der Landesbeauftragte für Datenschutz und Informationsfreiheit die Einführung des sogenannten Telenotarztes durch den Senator für Inneres und Sport. Bei Rettungseinsätzen können nunmehr anstelle von Notärztinnen sowie Notärzten vor Ort Telenotärztinnen sowie Telenotärzte hinzugezogen werden. Die Zuschaltung erfolgt via Video. Die hinzugezogenen Telenotärztinnen sowie Telenotärzte sitzen entweder in der Rettungsleitstelle in Bremen oder aber in Goslar. Derartige neue Versorgungsformen können während der Erprobungsphase auf die Experimentierklausel des § 30b Bremisches Hilfeleistungsgesetz gestützt werden, der nach der Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit auch die mit ihnen verbundenen Datenverarbeitungsvorgänge legitimieren kann. Sobald die Versorgungsform ihren experimentellen Charakter jedoch verliert und in einen regulären Standardbetrieb überführt wird, bedarf es spezieller gesetzlicher Grundlagen im Bremischen Hilfeleistungsgesetz zur Legitimation der Verarbeitungsvorgänge.

Vor allem bei grenzüberschreitenden Formen der Zusammenarbeit ist zudem erforderlich, dass die datenschutzrechtlichen Verantwortlichkeiten von Anfang an geklärt sind. Dies hat auch dieses Projekt wieder gezeigt. Die beteiligten Akteure haben am Anfang eines gemeinsamen Projektes zu eruieren, in welcher datenschutzrechtlichen Beziehung sie zueinander stehen. Regelmäßig ist zu überprüfen, ob ein Auftragsverhältnis oder eine gemeinsame Verantwortlichkeit vorliegt.

5.6 Ordnungsamt – pmOWi-App zur Ahndung von Verkehrsverstößen

Im Berichtsjahr erfuhr der Landesbeauftragte für Datenschutz und Informationsfreiheit über eine Pressemitteilung, dass die Bremer Ordnungsdienste seit Jahresbeginn 2024 mithilfe einer App, nämlich der pmOWi, auf den dienstlichen Smartphones ihrer Außendienstkräfte Ordnungsverstöße ahnden können. Die Außendienstkräfte könnten über eine sichere Datenverbindung Daten übermitteln und auch Bezahlvorgänge abwickeln. Die Anwendung pmOWi dient nach Auskunft des Dienststellenleiters des Ordnungsamtes der Beschleunigung der Arbeitsvorgänge und auch der Entlastung des Ordnungsdienstes insgesamt. Die geplante Einführung der Software war dem Landesbeauftragten für Datenschutz und Informationsfreiheit vorab nicht bekannt, und es wurde im Vorwege der Einführung auch keine Datenschutzfolgenabschätzung zur Prüfung und Stellungnahme durch die Dienststellenleitung des Ordnungsamtes vorgelegt.

Nach Aufforderung zur Einreichung einer Datenschutzfolgenabschätzung erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit im Juli 2024 Unterlagen des Herstellers sowie einige Leistungsbeschreibungen. Jedoch fehlten im Kontext der schwerpunktmäßigen

Anwendung der Software für Ordnungswidrigkeitenverfahren klare Aussagen zur Anwendbarkeit der Datenschutzgrundverordnung in Abgrenzung zur Anwendbarkeit der JI-Richtlinie[1]. Die eingereichten Unterlagen entsprachen daher nicht den Anforderungen einer Datenschutzfolgenabschätzung, infolgedessen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit um Vorlage einer vollständigen Datenschutzfolgenabschätzung gebeten. Diese wurde ihm Ende Oktober 2024 vorgelegt. Die Prüfung der Unterlagen dauert noch an. Ein Vor-Ort-Termin zur Inaugenscheinnahme der Anwendungen hat beim Ordnungsamt stattgefunden, im Rahmen dessen die Nutzung der Anwendung und die Verarbeitung der Daten begutachtet werden konnten.

Gemäß Artikel 1 Absatz 1 in Verbindung mit Artikel 2 Absatz 1 der JI-Richtlinie findet die JI-Richtlinie Anwendung bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden unter anderem zum Zwecke der Verfolgung von Straftaten. Mithilfe der Anwendung der pmOWi werden allgemeine Ordnungswidrigkeiten sowie Verkehrsordnungswidrigkeiten geahndet; somit ist aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit für die verarbeiteten Ordnungswidrigkeiten die JI-Richtlinie anstelle der Datenschutzgrundverordnung anzuwenden. Folglich hält er für den Einsatz der pmOWi-App eine Datenschutzfolgenabschätzung gemäß § 67 Absatz 1 Bundesdatenschutzgesetz (BDSG) für erforderlich, bei der gemäß § 67 Absatz 4 BDSG auf die einzelnen Verarbeitungstätigkeiten detailliert eingegangen werden muss. Außerdem sind die Rechtsgrundlagen für die Durchführung der Verarbeitungstätigkeiten zu nennen, und eine Risikoabschätzung zu den einzelnen Tätigkeiten ist erforderlich.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat in diesem Verfahren klargestellt, dass es bei so weitreichenden Softwarelösungen, bei denen personenbezogene Daten von Bürgerinnen und Bürgern auf neuartige Weise elektronisch verarbeitet werden, unerlässlich ist, die Datenschutzbehörde vorab zu informieren oder wenigstens eine erforderliche Datenschutzfolgenabschätzung vor dem Beginn der Nutzung neuer Verfahren zur Stellungnahme vorzulegen.

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

Bereits im 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 5.2, im 5. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 6.6 sowie im 6. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 6.7 legte die Landesbeauftragte für

[1] Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.

Datenschutz und Informationsfreiheit dar, dass das Bremische Polizeigesetz den Erlass einer Rechtsverordnung zu Prüf- und Speicherfristen der Polizei erfordert. Gemäß § 58 Absatz 6 Satz 1 Bremisches Polizeigesetz (BremPolG) werden die Aussonderungsprüffristen der Polizei vom Senator für Inneres und Sport durch Rechtsverordnung festgelegt, wobei nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit auch die Normierung von Speicherfristen zulässig ist, insbesondere dann, wenn sich Aussonderungsprüffristen nicht als praktikabel erweisen. Obgleich wiederholt die Dringlichkeit des Erlasses einer praktikablen Rechtsverordnung betont wurde, kam es auch in diesem Berichtsjahr nicht zu dem Erlass einer entsprechenden Verordnung.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit sieht sich daher auch in diesem Berichtsjahr veranlasst, den zeitnahen Erlass einer entsprechenden Rechtsverordnung zu fordern. Nur sie kann zum einen auf der Seite der Rechtsanwenderinnen und Rechtsanwender Klarheit über die zulässige Speicherdauer polizeilicher Daten schaffen und zum anderen dem Landesbeauftragten für Datenschutz und Informationsfreiheit einen klaren Prüfungsmaßstab an die Hand geben.

Mit dem Urteil des Bundesverfassungsgerichtes zum Bundeskriminalamtgesetz vom 1. Oktober 2024 (Aktenzeichen1 BvR 1160/19) hat sich die Dringlichkeit, eine solche Rechtsverordnung zu erlassen, noch einmal erhöht. Das Bundesverfassungsgericht hat festgestellt, dass insbesondere die zweckändernde vorsorgliche polizeiliche Speicherung von Daten, die vormals zu Zwecken der Strafverfolgung erhoben wurden, nur dann zulässig ist, wenn sie auch von gesetzlich geregelten Speicherfristen flankiert wird. Dazu bedarf es nach dem Bundesverfassungsgericht eines gesetzlich ausgestalteten Regelungskonzeptes. Nicht ausreichend ist es hingegen, wenn es der Polizeibehörde selbst überlassen bleibt, die Prüf- und Speicherfristen in einem eigenen, behördeninternen Regelungskonzept auszugestalten (Bundesverfassungsgericht [BVerfG], Urteil vom 1. Oktober 2024 [Aktenzeichen 1 BvR 1160/19], Randnummern 200 fortfolgende). So verhält es sich jedoch derzeit nach dem Bremischen Polizeigesetz, das auch die zweckändernde vorsorgliche polizeiliche Speicherung von Daten legitimiert. Nach § 50 Absatz 4 BremPolG dürfen die Polizeibehörden personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten über eine tatverdächtige Person und in Zusammenhang damit über Dritte rechtmäßig erhoben haben, zweckändernd auch zur Abwehr von Gefahren und zur Verhütung erheblicher Straftaten verarbeiten. Diese Befugnis zur zweckändernden Datenverarbeitung wird bislang nicht, wie vom Bundesverfassungsgericht gefordert, von gesetzlich geregelt Speicherfristen flankiert.

Da die Rechtsverordnung zu den Prüf- und Speicherfristen noch nicht existiert, ist derzeit allein das polizeiinterne Regelungskonzept zum Vorgangbearbeitungssystem @rtus maßgeblich.

Dieses hat indes nicht den Charakter eines Gesetzes. Das Bundesverfassungsgericht formuliert insoweit, dass „es ein[es] hinreichend ausdifferenzierte[n] Regelungskonzeptes zur Speicherdauer“ (BverfG, am angegebenen Ort [aaO], Randnummer 200) bedürfe, dass durch den Gesetzgeber „ausgestaltet“ werden müsse (BverfG, aaO, Randnummer 203). Mithin ist das Bremische Polizeigesetz in dieser Hinsicht kritisch anhand der Vorgaben des Bundesverfassungsgerichtes zu überprüfen.

6. Justiz

6.1 Gemeldete Datenschutzverletzungen (inklusive Rechtsanwältinnen und Rechtsanwälten, Steuer- und Rechnungswesen)

Im Jahr 2024 wurden von Rechtsanwältinnen und Rechtsanwälten sowie Notarinnen und Notaren bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit vier Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung gemeldet. Es handelt sich um eine außerordentlich niedrige Zahl. Den Gründen für diese außerordentlich niedrige Zahl wird der Landesbeauftragte für Datenschutz und Informationsfreiheit nachgehen.

Zwei Fälle hatten fehlerhafte Übermittlung von personenbezogenen Daten an einen unberechtigten Empfänger zum Gegenstand.

Durch die Staatsanwaltschaft Bremen als verantwortliche Stelle wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit im Jahr 2024 19 Datenschutzverletzungen gemeldet. In zehn der Fälle waren auf dem Postweg Ermittlungsakten verloren gegangen; in den anderen Fällen waren Akten zunächst nicht auffindbar, wurden später jedoch im Hause wiedergefunden.

Im Berichtsjahr wurden durch die Finanzverwaltung sowie durch die Angehörigen der steuerberatenden Berufe neun Fälle von Datenschutzverletzungen gemeldet. In den meisten Fällen war Ursache der Datenschutzverletzungen der Fehlversand von Briefpost oder E-Mails an falsche Empfängerinnen und Empfänger. In einem Fall verschickte ein Steuerbüro einen Serienbrief an mehrere Mandantinnen und Mandanten, der personenbezogene Daten eines Mandanten enthielt.

Durch das Amtsgericht (Grundbuchamt) wurde eine Datenschutzverletzung dem Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet. Der Meldung lag die versehentliche Versendung personenbezogener Daten eines Grundstückseigentümers an einen unzuständigen Notar zugrunde.

6.2 Fortentwicklung E-Mail-Verschlüsselung bei Rechtsanwältinnen und Rechtsanwälten

Das Thema E-Mail-Verschlüsselung bei Rechtsanwältinnen und Rechtsanwälten beschäftigte den Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtszeitraum erneut. Ihn erreichten insoweit zahlreiche kritische Nachfragen, aber auch positive Rückmeldungen

von Rechtanwältinnen und Rechtsanwälten, die die E-Mail-Kommunikation mit Mandanten bereits datenschutzkonform aufgestellt hatten und zum Beispiel aus Wettbewerbsgründen ihre Zustimmung zu seinem Vorgehen äußerten.

Vorsorglich weist der Landesbeauftragte für Datenschutz und Informationsfreiheit nochmals darauf hin, dass auch die Einholung von Erklärungen der Kommunikationspartnerinnen beziehungsweise Kommunikationspartner der Rechtsanwältinnen und Rechtsanwälte, sie seien mit der Übersendung per E-Mail einverstanden, nicht zu einer datenschutzrechtlichen Rechtmäßigkeit einer unverschlüsselten oder transportverschlüsselten E-Mail-Kommunikation führt. Denn bei der Verschlüsselung von E-Mails handelt es sich um technisch-organisatorische Maßnahmen, die gerade nicht zur Disposition des Einzelnen stehen.[2]

Im Übrigen wurde die Erörterung der Thematik mit der Hanseatischen Rechtsanwaltskammer Bremen fortgesetzt. Seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit wurde die von einigen Kanzleisoftware-Produkten angebotene sogenannte Portal-Variante als gute Lösung zur Erfüllung der datenschutzrechtlichen Anforderungen und somit als Alternative zur reinen E-Mail-Kommunikation vorgestellt. Hierbei richtet die Rechtsanwältin oder der Rechtsanwalt mittels Kanzleisoftware ein Aktenportal ein, in das sie oder er Nachrichten und Aktenbestandteile einstellen kann, die sie oder er der Mandantin oder dem Mandanten übermitteln will. Die Mandantin beziehungsweise der Mandant erhält Zugangsdaten, mit denen sie oder er sich in das Portal einloggen kann. Die Unterrichtung über eine im Portal hinterlegte Nachricht erfolgt über eine E-Mail, die allerdings außer dem Hinweis, dass eine Nachricht bereitliege, keinen weiteren Inhalt enthält. Alternativ wies der Landesbeauftragte für Datenschutz und Informationsfreiheit auch darauf hin, dass eine Ende-Zu-Ende-Verschlüsselung von E-Mails, insbesondere via Secure / Multipurpose Internet Mail Extensions (S/MIME) oder Pretty Good Privacy (PGP), akzeptabel sei.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wird die Angelegenheit auch in Zukunft konsequent weiterverfolgen. Dem Schutz personenbezogener Daten im Bereich der Rechtsanwältinnen und Rechtsanwälte kommt nach seiner Auffassung eine hohe Bedeutung zu.

[2] Vergleiche dazu auch DSK-Beschluss vom 24. November 2021, zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Artikel 32 Datenschutzgrundverordnung auf ausdrücklichen Wunsch betroffener Personen, dort Ziffer 2, https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf.

6.3 Vorsitz des Unterarbeitskreises Rechtsanwälte

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat im Jahr 2024 den Vorsitz des neuen länderübergreifenden Unterarbeitskreises Rechtsanwälte übernommen. Im Rahmen dieses Unterarbeitskreises sollen zukünftig datenschutzrechtliche Themen aus dem Bereich der Rechtsanwältinnen und Rechtsanwälte unter der Federführung des Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen erörtert werden.

6.4 Aufsichtsbefugnisse des Landesbeauftragten für Datenschutz und Informationsfreiheit im Anwendungsbereich der StPO und des OWiG

Im Rahmen von datenschutzrechtlichen Beschwerden gegen die Staatsanwaltschaft Bremen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit bei dieser um die Erteilung von Auskünften gebeten. Als Rechtsgrundlage für sein Auskunftsbegehren hat er § 500 Absatz 1, Absatz 2 Nummer 2 Strafprozessordnung (StPO) in Verbindung mit § 16 Absatz 4 Satz 1 Nummer 2 Bundesdatenschutzgesetz (BDSG) angeführt. Die Staatsanwaltschaft Bremen verwies jedoch darauf, dass § 500 StPO sich lediglich auf den 3. Teil des BDSG beziehe, § 16 BDSG hingegen im 1. Teil dieses Gesetzes stehe.

Diese am Wortlaut des § 500 StPO orientierte Auslegung steht im Widerspruch zu dem Inhalt eines Gesprächsprotokolls, das eine abweichende Sichtweise enthält, die die Landesbeauftragte für Datenschutz und Informationsfreiheit mit der Senatorin für Justiz und Verfassung im Jahr 2022 geteilt hat. Zwischen der Landesbeauftragten für Datenschutz und Informationsfreiheit und der Senatorin für Justiz und Verfassung bestand Übereinstimmung, dass § 500 StPO derart zu lesen sei, dass sich seine Verweisung auch auf § 16 BDSG erstrecke. Eine weitere Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates (JI-Richtlinie) im Bereich der Strafverfolgung ist in der Freien Hansestadt Bremen bisher auch nicht erfolgt.

Legt man die Haltung der Staatsanwaltschaft Bremen zu Grunde, wie sie aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit nach erneuter Prüfung gut vertretbar ist, fehlt gegenwärtig eine Regelung, die den Landesbeauftragten für Datenschutz und Informationsfreiheit ausdrücklich als zuständige Aufsichtsbehörde im Sinne des Artikel 41 JI-Richtlinie benennt (anders als beispielsweise in Niedersachen, siehe dort § 57 Niedersächsisches Datenschutzschutzgesetz). Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat aus diesem Grund nach Redaktionsschluss dieses Berichtes angeregt, eine Änderung im Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung vorzuneh-

men, um diese Regelungslücke zu schließen. In Hinblick auf die seitens der Staatsanwaltschaft Bremen vorgetragenen Gründe hält er an der seinerzeit im Jahr 2022 mit der Senatorin für Justiz und Verfassung geteilten Sichtweise nicht mehr fest.

6.5 Umsetzung der Protokollierungspflicht nach § 76 BDSG durch die Staatsanwaltschaft Bremen

Bereits seit 2023 befasste sich die Landesbeauftragte für Datenschutz und Informationsfreiheit mit der Umsetzung der Protokollierungspflicht nach § 76 Bundesdatenschutzgesetz (BDSG) durch die Staatsanwaltschaft Bremen bei den Zugriffen auf die spezifischen Fachverfahren. Jede Stelle, die Tätigkeiten im Rahmen der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten ausübt, muss den Vorgaben des § 76 BDSG genügen und die Zugriffe auf ihre Systeme derart protokollieren, dass alle Zugriffe auf die verarbeiteten Daten nachprüfbar sind.

Im Frühjahr 2024 wurde dem Landesbeauftragten für Datenschutz und Informationsfreiheit seitens der Staatsanwaltschaft Bremen ein Entwurf einer Hausverfügung bezüglich des Umgangs mit der Protokollierungsverpflichtung übersandt, zu dem der Landesbeauftragte für Datenschutz und Informationsfreiheit Rückfragen hatte und ergänzende Vorschläge unterbreitet hat. Insbesondere schien die darin anvisierte Speicherfrist von nur drei Monaten im Widerspruch zu den Vorgaben des § 76 Absatz 4 BDSG zu stehen, der eine deutlich längere Speicherfrist vorsieht: Löschung am Ende des Folgejahres. Er hat angeregt, den Entwurf der Hausverfügung unter Berücksichtigung seiner Anmerkungen anzupassen.

Aktuell sind die Vorgaben des § 76 BDSG noch nicht in den Fachverfahren der Staatsanwaltschaft Bremen implementiert und werden daher seitens der Staatsanwaltschaft Bremen noch nicht umgesetzt. Die finale Umsetzung der angepassten Protokollierungspflichten soll in der Fachanwendung web.sta bis Ende Mai 2026 abgeschlossen sein. Der Landesbeauftragte für Datenschutz und Informationsfreiheit wird die Umsetzung der Protokollierungspflicht nach § 76 BDSG bei den Zugriffen auf die spezifischen Fachverfahren durch die Staatsanwaltschaft Bremen weiter eng begleiten.

6.6 Protokollierung von Zugriffen auf E-Akten beim Landgericht Bremen

Im Rahmen einer Beschwerde wegen der Nichtverfügbarkeit einer elektronischen Prozessakte hat der Landesbeauftragte für Datenschutz und Informationsfreiheit beim Landgericht Bremen angefragt, ob es Störungen hinsichtlich der Zugriffsmöglichkeiten gab – konkret am Tag der mündlichen Verhandlung – und ob die Zugriffe auf die E-Akten protokolliert werden. Der Landesbeauftragte für Datenschutz und Informationsfreiheit erhielt die Auskunft, dass die Zu-

griffsrechte – nach Auffassung des Landgerichtes Bremen ordnungsgemäß – im elektronischen Aktensystem VISkompakt hinterlegt seien. Die Speicherfristen von 44 Tagen für die tatsächlichen Zugriffe wird jedoch seitens des Landesbeauftragten für Datenschutz und Informationsfreiheit als zu kurz bewertet.

Es wird ein weiterer Austausch mit dem Landgericht Bremen erfolgen, um eine datenschutzkonforme und datensparsame Lösung zu entwickeln.

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

Von der Senatorin für Justiz und Verfassung erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit einen Gesetzesentwurf für das Bremische Gesetz über die Sicherheit in Justizgebäuden. Der Entwurf enthielt eine Befugnis der Dienststellenleitung für eine Anordnung, nach der die Personalien aller Personen, die Zutritt zu einem Gerichtsgebäude begehren, zum Beispiel, um als Zuschauerin und Zuschauer an einer Verhandlung teilzunehmen, durch den Justizwachdienst an die Polizei weiterzugeben sind.

Mit dieser Vorgehensweise sollte erreicht werden, objektiv beurteilen zu können, ob eine polizeiliche Unterstützung für den Verhandlungstag erforderlich ist. In seiner Stellungnahme wies der Landesbeauftragte für Datenschutz und Informationsfreiheit auf § 1 Absatz 1 Bremisches Polizeigesetz (BremPolG) in Verbindung mit § 2 Nummer 1 BremPolG hin, woraus sich ergibt, dass nur Polizeivollzugsbeamte, nicht jedoch Bedienstete des Justizwachdienstes die Aufgabe haben, Gefahren für die öffentliche Sicherheit abzuwehren. Aus diesem Grund lehnte er die genannte Norm als Ermächtigungsgrundlage für die Erhebung und Verarbeitung der personenbezogenen Daten zur Einlasskontrolle durch die Justizvollzugsbediensteten als nicht einschlägig ab.

Außerdem gab es ohne das Vorliegen einer Gefahr, die entsprechend dem Gewicht des Eingriffes vom Gesetzgeber zu definieren ist, keinen ausreichenden Anlass für den Justizwachdienst, personenbezogene Daten von Besucherinnen und Besuchern der Gerichtsgebäude an die Polizei weiterzuleiten. Ohne das Vorliegen einer den verfassungsrechtlichen Anforderungen genügenden Gefahr würden anlasslose Überprüfungen durchgeführt.

Unabhängig von der fehlenden Ermächtigung hält der Landesbeauftragte für Datenschutz und Informationsfreiheit die Übermittlung der Personalien der einlassbegehrenden Besucherinnen und Besucher für unverhältnismäßig und eine unzulässige Einschränkung des in § 169 Absatz 1 Satz 1 Gerichtsverfassungsgesetz normierten Grundsatzes der Öffentlichkeit der Ver-

handlung. Die Schaffung einer Rechtsgrundlage für die Kontrolle von Zuschauerinnen und Zuschauern erachtet der Landesbeauftragte für Datenschutz und Informationsfreiheit daher für unzulässig.

Die Senatorin für Justiz und Verfassung erhielt die Stellungnahme des Landesbeauftragten für Datenschutz und Informationsfreiheit im ersten Halbjahr 2024. Die Verabschiedung des Gesetzes steht noch aus.

7. Gesundheit

7.1 Gemeldete Datenschutzverletzungen

Im vorliegenden Berichtsjahr haben Verantwortliche aus dem Bereich Gesundheit bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit 24 Datenschutzverletzungen gemeldet. Ein Großteil der Meldungen betraf Fehlsendungen von medizinischen Daten an unbefugte Personen sowie mögliche Kenntnisnahmen von Gesundheitsdaten durch Dritte bei Einbrüchen oder Diebstählen.

Darüber hinaus erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit auch Fälle, in denen Beschäftigte unbefugt Patientinnen- beziehungsweise Patientendaten in Krankenhausinformationssystemen abfragten und zu privaten Zwecken an Dritte weitergaben. Da es sich um Daten des jeweiligen Krankenhauses handelt, unterliegen die Einrichtungen in solchen Fällen der Meldepflicht nach Artikel 33 Datenschutzgrundverordnung. Es wird je nach Fallkonstellation zudem gegebenenfalls auch gegen die Beschäftigten ein Verfahren eröffnet, wenn bei der Prüfung der Meldung festgestellt wird, dass sie sich durch ihr Verhalten selbst zu datenschutzrechtlichen Verantwortlichen aufgeschwungen haben.

7.1.1 Einbrüche in Außenstellen des Gesundheitsamtes Bremen

Das Gesundheitsamt Bremen verfügt über 17 Außenstellen, die im gesamten Stadtgebiet verteilt sind. Dort sind die Stadtteilteams des Kinder- und Jugendgesundheitsdienstes untergebracht, die unter anderem für Schuleingangsuntersuchungen oder für Früherkennungsuntersuchungen (U6-U9) zuständig sind. Wiederholt kam es in der letzten Zeit zu Einbrüchen, zuletzt berichtete die Landesbeauftragte für Datenschutz und Informationsfreiheit über vergleichbare Vorfälle in ihrem 6. Jahresbericht nach der Datenschutzgrundverordnung (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 8.1.1). Aufgrund festgestellter Mängel hinsichtlich der getroffenen Maßnahmen zur Datensicherheit forderte die Landesbeauftragte für Datenschutz und Informationsfreiheit das Gesundheitsamt Bremen damals auf, personenbezogene Daten nur in abschließbaren Schränken zu lagern und Schlüssel nur an die Beschäftigten auszuhändigen, die die Daten für die Erfüllung ihrer Aufgaben benötigen.

Bedauerlicherweise musste der Landesbeauftragte für Datenschutz und Informationsfreiheit in diesem Berichtsjahr feststellen, dass die Aufforderung nicht in allen Außenstellen umgesetzt worden war. Ihm wurde erneut ein Einbruch in eine Außenstelle gemeldet, in welcher Akten in unverschlossenen Schränken gelagert wurden. Zwar fanden sich keine Anhaltspunkte dafür, dass die Schränke im Zuge des Einbruchs durchsucht wurden. Dennoch entspricht eine solch

nachlässige Aufbewahrung von höchst sensiblen Daten Minderjähriger nicht den datenschutzrechtlichen Anforderungen. Der Landesbeauftragte für Datenschutz und Informationsfreiheit forderte das Gesundheitsamt Bremen daher auf, sämtliche Außenstellen auf die jeweils getroffenen technischen und organisatorischen Maßnahmen der Datensicherheit zu überprüfen und Mängeln unverzüglich abzuhelfen. Neben dem offensichtlichen Nachbesserungsbedarf in der betroffenen Außenstelle führte die Prüfung weitere Fälle ans Licht, bei denen Schlüssel abhandengekommen waren oder Akten nicht in abschließbaren Schränken aufbewahrt wurden. Das Gesundheitsamt Bremen teilte mit, dass nunmehr in allen Standorten Schlüsseltresore installiert wurden und das Schulungsangebot für die Beschäftigten nachgebessert wurde.

7.1.2 Fehlgeleitete Faxsendungen

Im Gegensatz zu anderen Bereichen spielt das Faxgerät im Gesundheitsbereich zur Datenübermittlung nach wie vor eine nicht unbeachtliche Rolle. Der Grund hierfür mag zum einen sein, dass staatlicherseits geschaffene Alternativlösungen über die Telematik-Infrastruktur noch nicht die gewünschte Zuverlässigkeit aufweisen. Zum anderen wird häufig noch angenommen, es handele sich bei der Übertragung via Fax um eine sichere Methode, die vor allem bei zeitkritischen Vorgängen alternativlos sei.

Dass ein herkömmliches Fax aus technischer Sicht etwa so sicher ist wie der Versand einer offenen Postkarte, wurde in früheren Berichten bereits ausführlich dargelegt (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.1). Ebenso bietet das Fax im Internetzeitalter keinen zeitlichen Vorteil mehr. Online-Lösungen, etwa über verschlüsselte E-Mails oder Portallösungen, die ein sicheres Hoch- und Herunterladen von Inhalten ermöglichen, sind hingegen in der Lage, die Defizite des Faxes auszugleichen, indem selbst sensibelste Daten sowohl sicher als auch schnell übertragen werden können.

Es steht außer Frage, dass eine einheitliche Lösung, wie etwa über die Telematik-Infrastruktur, das Ziel sein sollte. Bis diese flächendeckend für alle Einrichtungen im Gesundheitsbereich in dem geforderten Umfang zur Verfügung steht, sind Verantwortliche gefordert, eigene Lösungen bereitzustellen.

Im vorliegenden Berichtsjahr erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit mehrere fehlgeleitete Faxsendungen mit Patientinnen- und Patientendaten. Beim Versand wurde offenbar versehentlich die Faxnummer seiner Behörde in das Empfängerfeld eingetragen. In keinem der Fälle fiel der Fehler bei der oder dem Verantwortlichen auf, sondern gelangte dieser beziehungsweise diesem erst durch die Kontaktaufnahme des Landesbeauftragten für Datenschutz und Informationsfreiheit zur Kenntnis. Selbst ohne Berücksichtigung von Möglichkeiten Dritter, den Inhalt der Sendung auszuspähen, machen diese Fälle bereits deutlich, wie gering der Schutz vor einer unbefugten Offenlegung bei der Übermittlung via Fax

ist. Da die versendeten Gesundheitsdaten bei einer Fehlsendung ohne Weiteres durch die unbefugte Empfängerin beziehungsweise den unbefugten Empfänger zur Kenntnis genommen werden können, sind solche Vorfälle als Datenschutzverletzung der zuständigen Aufsichtsbehörde zu melden.

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

In ihrem 6. Jahresbericht berichtete die Landesbeauftragte für Datenschutz und Informationsfreiheit über ihren Austausch mit dem Gesundheitsamt Bremen hinsichtlich der Datenverarbeitung im Zusammenhang mit der Durchführung von HPV-Impfungen bei Schülerinnen und Schülern in der Stadtgemeinde Bremen (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 8.5). Sie forderte damals einige Anpassungen, damit sichergestellt ist, dass die Impfung freiwillig erfolgt. In seiner Stellungnahme zu dem Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit kündigte der Senat an, die verwendeten Dokumente zeitnah mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit abzustimmen, um diese beim Schulimpfprogramm im Sommer 2024 zu verwenden.

Bedauerlicherweise konnte das Gesundheitsamt Bremen den angekündigten Zeitplan nicht halten. Die Umsetzung der Anmerkungen der Landesbeauftragten für Datenschutz und Informationsfreiheit vom September 2023 und die Überarbeitung des Verfahrens erfolgten erst im Frühjahr 2024. Da sich aus dem Entwurf nur noch ein geringer Überarbeitungsbedarf und wenige Rückfragen ergaben, wäre eine rechtzeitige Finalisierung zu diesem Zeitpunkt weiterhin möglich gewesen. Allerdings wurde das Verfahren im Nachgang erneut angepasst. Hintergrund war die Einbindung des Robert Koch-Instituts in die Auswertung des Impfprogramms, die anfangs nicht vorgesehen war und erst im Juli 2024 umgesetzt wurde. Zudem konnten die Bedenken hinsichtlich der Übermittlung von Klassenlisten durch die Senatorin für Kinder und Bildung an das Gesundheitsamt Bremen weiterhin nicht ausgeräumt werden. Für eine Anpassung der Dokumente und Klärung der Fragen war zu diesem Zeitpunkt jedoch kein Raum mehr. Das Gesundheitsamt Bremen entschied daher, auf eine finale Abstimmung der Dokumente zu verzichten. Diesen Umstand bedauert der Landesbeauftragte für Datenschutz und Informationsfreiheit. Er wird den Prozess weiterhin begleiten und erwartet, dass die Zeit bis zur nächsten Durchführung des Impfprogramms genutzt wird, um das Verfahren datenschutzkonform zu gestalten.

7.3 Rechtsprechung zur kostenfreien Kopie der Patientenakte

Der Europäische Gerichtshof hat mit seinem Urteil vom 26. Oktober 2023 (Aktenzeichen C-307/22) wichtige Fragen im Hinblick auf den Auskunftsanspruch von Patientinnen und Patienten geklärt und damit mehr Rechtsklarheit geschaffen. In seiner Entscheidung befasste sich der Europäische Gerichtshof mit der widersprüchlichen Rechtslage, nach der Ärztinnen und Ärzte einerseits gemäß Artikel 15 Absatz 3 Datenschutzgrundverordnung eine kostenfreie Kopie der Patientenakte bereitstellen müssen und andererseits gemäß § 630g Absatz 2 Bürgerliches Gesetzbuch eine Kostenerstattung verlangen dürfen. Das Urteil fiel zugunsten der Patientinnen und Patienten aus, die ein Recht auf eine unentgeltliche erste Kopie ihrer Akten haben. Der Bundesgesetzgeber sowie die Landesärztekammern sind nun gefordert, entgegenstehende Regelungen des Bürgerlichen Gesetzbuches sowie der Berufsordnungen anzupassen. Den Änderungsbedarf hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 11. September 2024 im Einzelnen beschrieben (siehe hierzu Ziffer 18.2 dieses Berichtes).

Der Europäische Gerichtshof stellte außerdem klar, dass die Motivation, die eine Patientin oder ein Patient mit einem Auskunftsantrag verfolgt, unbeachtlich ist. Es ist daher auch nicht erforderlich, dass der Antrag begründet wird.

Die Auskunft muss für die betroffene Person zudem verständlich sein und ihr ermöglichen, die Richtigkeit und Vollständigkeit der Daten zu überprüfen. Hierfür ist es laut Europäischen Gerichtshofes erforderlich, dass die betroffene Person jedenfalls eine vollständige Kopie derjenigen Dokumente ihrer Patientenakte erhält, die Informationen, wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärztinnen und Ärzte und Angaben zu an ihr vorgenommenen Behandlungen oder Eingriffen, umfasst.

7.4 Datenschutzrechtliche Verantwortlichkeit von gerichtlich bestellten Sachverständigen

Verschiedene Eingaben bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit zeigen, dass sich Psychologinnen und Psychologen, die als Sachverständige in familiengerichtlichen Verfahren tätig sind, häufig in Bezug auf datenschutzrechtliche Anforderungen einer gewissen Unsicherheit ausgesetzt sehen. Diese resultiert vornehmlich daraus, dass sie im Auftrag des Gerichtes tätig werden und das Gericht die Art und den Umfang des Auftrages festlegt. Hieraus schließen Sachverständige zum Teil, dass das Gericht für die Datenverarbeitung verantwortlich sei und über alle damit zusammenhängenden Fragen entscheiden müsse.

Nach der Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit liegt die datenschutzrechtliche Verantwortlichkeit in familiengerichtlichen Verfahren bei den beauftragten Sachverständigen selbst. Im gerichtlich festgelegten Rahmen arbeiten sie eigenverantwortlich und genießen wissenschaftliche Unabhängigkeit. Sie entscheiden im Regelfall selbst, welche personenbezogene Daten zur Beantwortung der Beweisfrage erhoben werden und wie die Verarbeitung erfolgt. Außerdem sind Sachverständige nicht Teil des Gerichtes und üben somit keine justizielle Tätigkeit gemäß Artikel 55 Absatz 3 Datenschutzgrundverordnung (DSGVO) aus.

Die Einordnung als datenschutzrechtlich Verantwortliche hat zur Folge, dass die Sachverständigen die Vorgaben der Datenschutzgrundverordnung einzuhalten haben und diesbezüglich einer Rechenschaftspflicht (Artikel 5 Absatz 2 DSGVO) unterliegen. Die Rechtsgrundlage für die Datenverarbeitung ergibt sich dabei regelmäßig aus gesetzlichen Befugnissen, sodass auf die Einholung einer Einwilligung verzichtet werden kann. Zu den datenschutzrechtlichen Pflichten gehört insbesondere, die betroffenen Personen über die Datenverarbeitung zu informieren (Artikel 13, 14 DSGVO) und ihnen auf Antrag eine Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erteilen (Artikel 15 DSGVO). Des Weiteren müssen Maßnahmen der Datensicherheit sowie ein Löschkonzept entwickelt und umgesetzt werden.

7.5 Unzulässige Speicherung von Arztbriefen im Krankenhaus

Für Beschäftigte im Krankenhaus ergeben sich immer dann besondere Risiken, wenn sie selbst Patientinnen und Patienten beim eigenen Arbeitgeber werden oder in der Vergangenheit waren und das Krankenhaus aus diesem Grund Gesundheitsdaten von ihnen verarbeitet. Krankenhäuser müssen auf diese Fallgestaltung vorbereitet sein und im Krankenhausinformationssystem Möglichkeiten vorsehen, um diese Daten in besonderem Maße zu schützen – etwa vor der Neugier der Kolleginnen und Kollegen. Dies gilt ebenso für Patientenakten, die nicht oder noch nicht vollständig digital geführt werden.

Bei einem Krankenhaus im Zuständigkeitsbereich des Landesbeauftragten für Datenschutz und Informationsfreiheit führte die Nachlässigkeit bei der Vergabe von Zugriffsrechten dazu, dass eine Beschäftigte oder ein Beschäftigter, die oder der von einer früheren psychiatrischen Behandlung einer Kollegin oder eines Kollegen wusste, Einsicht in ihren oder seinem Entlassungsbrief nahm. Der Vorfall wurde von dem betroffenen Krankenhaus ordnungsgemäß als Datenschutzverletzung gemeldet, weil es für die Aufgaben der oder des Beschäftigten nicht erforderlich war, Einsicht in die Patientenakte zu nehmen.

Bei der Prüfung des Falles stellte der Landesbeauftragte für Datenschutz und Informationsfreiheit fest, dass die unbefugte Einsichtnahme über einen digitalen Ordner möglich war, in welchem seit 2006 die Entlassungsbriefe aller Patientinnen und Patienten abgelegt wurden.

Zugriffsberechtigt waren alle examinierten Mitarbeiterinnen und Mitarbeiter des Pflegedienstes sowie des Ärztlichen Dienstes. Nach Ansicht des Krankenhauses war der Zugriff notwendig, damit bei Aufnahmen von Patientinnen und Patienten am Wochenende oder in der Nacht ein Zugriff auf die Medikationsdaten bestand.

Aus mehreren Gründen widersprach dieses Vorgehen den datenschutzrechtlichen Vorgaben: Zum einen sieht § 43 Absatz 3 Bremisches Krankenhausgesetz vor, dass automatisiert verarbeitete Patientendaten nach Abschluss der Behandlung für die Möglichkeit des Direktabrufes zu sperren sind. Zwar führte das betreffende Krankenhaus die Behandlungsdokumentation grundsätzlich papierbasiert, jedoch fällt der in Frage stehende Ordner unter die genannte Vorschrift. Da ein Vollzugriff auf den Ordner bestand und auch ältere Berichte nicht für den Direktabruf gesperrt waren, stellte dies eine Verletzung der Regelung dar.

Zum anderen war nach der Bewertung des Landesbeauftragten für Datenschutz und Informationsfreiheit ein Zugriff auf die Entlassungsberichte für alle Pflegekräfte sowie alle Ärztinnen und Ärzte nicht erforderlich. Aus den Berichten ergibt sich nicht zwingend die aktuelle Medikation der betroffenen Person, weil diese im Rahmen von späteren Behandlungen im ambulanten Bereich oder von stationären Aufenthalten in anderen Krankenhäusern verändert worden sein könnte. Die Daten bieten somit keine medizinische Verlässlichkeit und sind damit für den angegebenen Verwendungszweck ungeeignet.

Nach dem gemeldeten Vorfall und dem Tätigwerden des Landesbeauftragten für Datenschutz und Informationsfreiheit löschte das Krankenhaus einen Großteil der abgelegten Entlassungsbriefe und beschränkte die Zugriffsrechte auf das ärztliche Personal. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit wurde mitgeteilt, dass gerade die Umstellung auf ein elektronisches Krankenhausinformationssystem erfolge und zukünftig auf den Ordner verzichtet werden könne. Bei einem gemeinsamen Termin verschaffte er sich ein Bild von der Situation vor Ort und erörterte die Problematik mit dem Verantwortlichen. Hierbei erfuhr er, dass es seit der Beschränkung der Zugriffsrechte keine konkreten Anfragen auf Freigabe der Daten gab. Dies bestätigt nach Auffassung des Landesbeauftragten für Datenschutz und Informationsfreiheit, dass die Daten für Behandlungszwecke nicht erforderlich sind. Er forderte das Krankenhaus daher auf, den Ordner zu löschen. Dieses hielt jedoch weiterhin an dem Ordner fest. Es führte nunmehr an, der Schreibdienst, welcher für die Bearbeitung von Anfragen zu früheren Behandlungsfällen zuständig sei, benötige weiterhin Zugriff auf die Daten.

Diese Begründung überzeugt aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit nicht. Zwar wurden bis zum Frühjahr des Berichtsjahres papiergebundene Patientenakten geführt, sodass ein Zugriff auf abgeschlossene Behandlungsfälle aufgrund der Archivierung der Akten zeitaufwändig ist. Doch auch bei digitalen Patientendaten darf es keine dauerhafte Möglichkeit des Direktabrufs geben und es muss im Zweifel ein erhöhter zeitlicher

Aufwand in Kauf genommen werden. Der Umweg über den angelegten Dateiordner widerspricht den gesetzlichen Vorgaben und ist aus diesem Grund unzulässig.

7.6 Stichprobenhafte Prüfung bei Trägern stationärer Pflegeeinrichtungen

Bei einem Großteil der von dem Landesbeauftragten für Datenschutz und Informationsfreiheit geführten aufsichtsrechtlichen Verfahren wird er aufgrund einer Beschwerde von einer betroffenen Person, einer Meldung über eine Datenschutzverletzung oder eines Hinweises aus der Bevölkerung tätig. Es gibt allerdings auch Bereiche, aus denen ihn vergleichsweise wenig Beschwerden von Betroffenen erreichen, weil diese etwa wegen körperlicher oder sprachlicher Einschränkungen hierzu nicht in der Lage sind oder es ein erhebliches Abhängigkeitsverhältnis zu der verantwortlichen Stelle gibt. Hierzu gehört unter anderem der Pflegebereich. Insbesondere Personen, die in einer stationären Pflegeeinrichtung wohnen, sind auf erhebliche Unterstützung angewiesen, um ihren Alltag meistern zu können. Selbst wenn ihnen oder ihren Angehörigen mögliche Datenschutzverletzungen bei der Verarbeitung ihrer sensiblen Gesundheitsdaten auffielen, ist die Hürde einer Beschwerde bei der Datenschutzaufsichtsbehörde häufig sehr hoch. Umso mehr müssen sich die betroffenen Personen darauf verlassen können, dass die Verarbeitung ihrer Daten gemäß den gesetzlichen Vorgaben erfolgt.

Vor diesem Hintergrund hat der Landesbeauftragte für Datenschutz und Informationsfreiheit eine stichprobenhafte Prüfung bei Trägern stationärer Pflegeeinrichtungen in der Freien Hansestadt Bremen durchgeführt. Anhand der Anzahl der Bewohnerinnen und Bewohner in den jeweiligen Einrichtungen wählte der Landesbeauftragte für Datenschutz und Informationsfreiheit insgesamt zehn Träger in Bremen und Bremerhaven aus. Diesen sandte er zunächst einen Fragenkatalog mit der Bitte um Beantwortung zu und forderte Dokumentationen zum Datenschutz an.

Die Auswertung der Rückmeldungen zeigte ein insgesamt positives Bild. Alle Träger konnten die angeforderten Informationen und Dokumentationen bereitstellen. Jedoch stellte der Landesbeauftragte für Datenschutz und Informationsfreiheit an einigen Stellen auch Nachbesserungsbedarf fest. Er ließ sich beispielsweise Einwilligungserklärungen vorlegen, die für solche Datenverarbeitungsvorgänge eingeholt werden müssen, die aufgrund einer gesetzlichen Grundlage nicht zulässig sind. Hierbei stieß er teils auf zu pauschale und teils auf missverständliche Formulierungen. Außerdem stellte er fest, dass die Träger teilweise sehr unterschiedliche Aufbewahrungsfristen anführten und sich hierbei auf unterschiedliche gesetzliche Grundlagen bezogen. Seine Nachfragen lösten bei einigen Trägern bereits eine Überprüfung

und Überarbeitung der Einwilligungsformulare beziehungsweise der Datenschutzdokumentation aus, ohne dass es einer expliziten Aufforderung bedurfte. In anderen Fällen wies er auf Unzulänglichkeiten hin und bat um Nachbesserung.

Auffällig war darüber hinaus, dass keiner der ausgewählten Träger besondere Anstrengungen unternimmt, um den betroffenen Personen die Wahrnehmung ihrer Betroffenenrechten zu erleichtern. Dies nahm die Landesbeauftragte für Datenschutz und Informationsfreiheit zum Anlass, um den Trägern Vorschläge an die Hand zu geben, die Hürden für Betroffene beziehungsweise deren rechtliche Vertreterinnen beziehungsweise Vertreter abzubauen. So ist es empfehlenswert, dass Ansprechpartnerinnen oder Ansprechpartner für den Bereich Datenschutz auch vor Ort zu erreichen sind und nicht nur telefonisch oder per E-Mail. Diese könnte man mit einer Checkliste mit Antworten zu den häufigsten Fragen ausstatten, sodass kein besonderes Fachwissen erforderlich ist. Weitergehende Anliegen können dann an den betrieblichen oder externen Datenschutzbeauftragten weitergeleitet werden.

Die Prüfung hat gezeigt, dass der stationäre Pflegebereich in der Freien Hansestadt Bremen datenschutzrechtlich bereits gut aufgestellt ist, aber an einigen Stellen noch Unsicherheit herrscht und es an der nötigen Transparenz gegenüber den Betroffenen fehlt.

8. Soziales

8.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden dem Landesbeauftragten für Datenschutz und Informationsfreiheit im Bereich Soziales insgesamt 16 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. Der Großteil der Meldungen betraf eine Sicherheitslücke bei einer Kindertagesbetreuungs-App (siehe hierzu Ziffer 8.4 dieses Berichtes) sowie den Verlust von Laptops und Smartphones.

8.2 Kommunikation durch unverschlüsselter E-Mails durch Sozialbehörden

Im Berichtsjahr gingen bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit mehrere Beschwerden bezüglich der Kommunikation mithilfe von unverschlüsselten E-Mails durch das Amt für Soziale Dienste ein. Die Thematik der sicheren Übertragungswege bei elektronischer Kommunikation durch das Amt für Soziale Dienste wurde durch die Landesbeauftragte für Datenschutz und Informationsfreiheit bereits in ihrem 34. Jahresbericht aus dem Jahr 2011 angesprochen (siehe hierzu 34. Jahresbericht, Ziffer 7.4). Leider scheint es seitdem keine Sensibilisierung bei den Sozialbehörden bezüglich dieser Thematik gegeben zu haben.

Problematisch ist dies, weil es sich bei den hierbei versendeten Daten oftmals um Sozialdaten handelt, die dem besonderen Schutz des Sozialgeheimnisses unterliegen. Zwar ist das Interesse der Sozialbehörden an einer unkomplizierten und schnellen Kommunikation mit den Bürgerinnen und Bürgern verständlich, jedoch kann bei der Versendung per unverschlüsselter E-Mail die Absenderin beziehungsweise der Absender nicht sicherstellen, dass Unbefugte keine Kenntnis von den Inhalten der E-Mail erhalten. Die Sicherheit der Sozialdaten kann daher bei einer solchen Kommunikationsmethode nicht sichergestellt werden.

Vielmehr sollten die Sozialbehörden, sofern sie Daten über digitale Kommunikationswege übersenden wollen, auf eine der vielfach vorhandenen sicheren Möglichkeiten zurückgreifen, um Dateien an Bürgerinnen und Bürger oder private Trägerinnen und Träger zu senden. So stellt beispielsweise die Kommunikation, bei der Dateitransferplattformen in Kombination mit einer Ende-zu-Ende-Verschlüsselung oder einem Passwortschutz gewährleistet werden, einen sicheren Weg der Kommunikation dar.

Zum Berichtszeitpunkt lag dem Landesbeauftragten für Datenschutz und Informationsfreiheit noch keine Stellungnahme der Sozialbehörden vor, wie diese zukünftig planen, dem besonderen Schutz von Sozialdaten bei der Versendung über das Internet nachzukommen. Er wird das Thema weiterverfolgen.

8.3 Datenbank Haaranalysen

Nachdem die Landesbeauftragte für Datenschutz und Informationsfreiheit über mehrere Jahre auf datenschutzrechtliche Mängel bei der Umsetzung der vom Amt für Soziale Dienste betriebenen Datenbank zur Verwaltung von Daten aus Gutachten zu Haaranalysen hingewiesen hatte (siehe hierzu zuletzt 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 9.6 – mit weiteren Nachweisen zu den zahlreichen Beanstandungen in der Vergangenheit), kam es im Berichtsjahr zu neuen Entwicklungen. In der von dem Amt für Soziale Dienste betriebenen Datenbank werden Daten aus Gutachten zu Haaranalysen zum Drogenkonsum drogenabhängiger und/oder substituierter Eltern und deren Kinder verwaltet.

Da die von der Senatorin für Arbeit, Soziales, Integration und Jugend angekündigte Prüfung der Überführung der Datenbank in ein Fachverfahren weiterhin nicht abgeschlossen werden konnte, kündigte der Landesbeauftragte für Datenschutz und Informationsfreiheit im Frühjahr 2024 einen Vor-Ort-Termin an, um den aktuellen Betrieb der Datenbank zu prüfen. Nach dieser Ankündigung wurde im Amt für Soziale Dienste die Entscheidung getroffen, die Datenbank zu löschen. Die Ergebnisse der Analysen sollen zukünftig nicht mehr zentral, sondern nur noch in den einzelnen Verfahrensakten gespeichert werden.

Da der Landesbeauftragte für Datenschutz und Informationsfreiheit auch darüber hinaus Anpassungsbedarf bei der Datenverarbeitung im Zusammenhang mit Haaranalysen feststellte, forderte er das Amt für Soziale Dienste auf, die Verfahren sowie die hierzu bestehende fachliche Weisung anzupassen. Seitens der Senatorin für Arbeit, Soziales, Jugend und Integration wurde mitgeteilt, dass die Überprüfung der Verfahren bereits angestoßen worden sei und, basierend auf den Ergebnissen, Anpassungen vorgenommen werden sollten. Es wurde zugesagt, den Landesbeauftragten für Datenschutz und Informationsfreiheit in diesen Prozess einzubeziehen und das zukünftige Verfahren mit ihm abzustimmen.

8.4 Vermehrte Nutzung von Apps in der Kindertagesbetreuung

Der Landesbeauftragte für Datenschutz und Informationsfreiheit bemerkte im Berichtsjahr einen vermehrten Anstieg bei der Nutzung von Apps im Bereich der Kindertagesbetreuung. Diese Apps werden vornehmlich zur internen Organisation in den Einrichtungen und zur Kommunikation mit den Sorgeberechtigten eingesetzt.

Hierbei wird jedoch eine Vielzahl von personenbezogenen Daten der Kinder und Sorgeberechtigten in die Systeme der App eingepflegt, was insbesondere im Hinblick auf den gebotenen besonderen Schutz von personenbezogenen Daten von Kindern entsprechende technische und organisatorische Maßnahmen erfordert.

Dass diese jedoch nicht immer etabliert sind, wurde durch einen Datenschutzvorfall bei einem Anbieter einer solchen App deutlich. Hier waren durch die fehlerhafte Konfiguration eines Servers die personenbezogenen Daten von Kindern sowie Sorgeberechtigten aus dem Internet frei abrufbar. Der Anbieter der App selbst hat seinen Sitz in Baden-Württemberg, die Kitaträger haben mit diesem Anbieter Auftragsverarbeitungsverträge abgeschlossen, die Prüfung bezüglich des Vorfalles bei der App wurde daher durch den Landesbeauftragten für Datenschutz und Informationsfreiheit nicht durchgeführt. Alleine in der Freien Hansestadt Bremen war hiervon über ein Dutzend Einrichtungen betroffen.

Für die Kitaträger als Verantwortliche stellt sich in einem solchen Fall die Frage, ob und wenn ja welche personenbezogenen Daten abgeflossen sind. Sofern der Verantwortliche im Rahmen seiner Ermittlung zu dem Ergebnis kommt, dass personenbezogene Daten abgeflossen sind, damit ein unbefugter Zugriff auf die Daten nicht ausgeschlossen werden kann und daher ein hohes Risiko für die Kinder und Sorgeberechtigten als betroffene Personen vorliegt, muss eine entsprechende Information an die Betroffenen erfolgen. Im Rahmen der eingegangenen Meldungen bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit wies er mehrere Verantwortliche auf diese Informationspflicht hin.

Auch sollte bei der Indienststellung der App der Zweck, der mit der Datenverarbeitung in der App erfüllt werden soll, beachtet und nur die personenbezogenen Daten in der App erfasst werden, die zur Erfüllung dieses Zweckes erforderlich sind. Eine darüber hinaus gehende Verarbeitung von personenbezogenen Daten ist nicht mit den datenschutzrechtlichen Vorgaben vereinbar.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit konnte auch feststellen, dass in manchen Fällen die entsprechende Information an die Sorgeberechtigten bezüglich der Datenverarbeitung in der App nicht den gesetzlichen Anforderungen entsprach. Auch hierbei sollten Kitaträger darauf achten, dass die Sorgeberechtigten vollumfänglich über die Verarbeitungsvorgänge im Zusammenhang mit der App informiert werden.

Im Berichtsjahr wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit auch auf die Einführung einer solchen App bei KiTa Bremen hingewiesen. Leider wurde er nicht direkt im Einführungsprozess beteiligt und konnte die App beziehungsweise die Dokumentation zu dieser nur nach Einführung überprüfen. Dabei zeigte sich, dass zumindest die Dokumentation nicht ausreichend beziehungsweise fehlerhaft war.

9. Bildung

9.1 Gemeldete Datenschutzverletzungen

Im Bereich Schulen und Bildung gab es im Berichtsjahr zwölf Meldungen verantwortlicher Stellen nach Artikel 33 Datenschutzgrundverordnung an den Landesbeauftragten für Datenschutz und Informationsfreiheit. Fünf Meldungen betrafen dabei Schulen, sieben weitere die Hochschulen in der Freien Hansestadt Bremen.

In den meisten Fällen im Schulbereich waren Einbrüche sowie Verlust von Dienstgeräten Gründe für die gemeldeten Datenschutzverletzungen. Neben diesen Meldungen gingen auch zehn Beschwerden bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit ein, wobei neun Beschwerden den Schulbereich und eine Beschwerde den Hochschulbereich betrafen. Es erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit zudem diverse Anfragen von Betroffenen, die sich zumeist auf die Übermittlung personenbezogener Daten von Schülerinnen sowie Schülern und Lehrkräften bezogen.

9.2 Vergabe von Passwörtern bei itslearning

Den Landesbeauftragten für Datenschutz und Informationsfreiheit erreichte ein Hinweis, dass an einer Grundschule für die SuBITI[3] Konten der Schülerinnen und Schüler, mit denen unter anderem die Anmeldung auf der Lernplattform itslearning erfolgt, sämtliche Passwörter identisch vergeben worden seien. Seitens der Schule sei darüber hinaus eine Änderung der Passwörter nicht gewünscht gewesen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies die Schule daher darauf hin, dass Passwörter, die den Schülerinnen und Schülern Zugang zu schulseitig angebotenen internetbasierten IT-Anwendungen gewähren, die den Zugriff auf personenbezogene Daten ermöglichen, wie zum Beispiel itslearning, so vergeben werden müssen, dass ein möglichst hoher Schutz vor unberechtigter Anmeldung gewährleistet ist. Die personenbezogenen Daten Minderjähriger sind nämlich in der Regel besonders schützenswert. Dabei müssen die Passwörter der Kinder nicht nur anderen Schülerinnen und Schülern oder Dritten gegenüber unbekannt bleiben, auch den Lehrkräften dürfen die individuellen Passwörter nicht bekannt sein. Dies ist bei der Vergabe identischer Passwörter offensichtlich nicht der Fall, sodass ein solches Vorgehen datenschutzrechtlich unzulässig ist. Auch sollten Schülerinnen und Schüler zum regelmäßigen Wechsel ihrer Passwörter ermuntert werden.

[3] SuBITI ist das „Service- und Betriebskonzept für die IT-Infrastruktur“ der senatorischen Behörde für die Schulen der Stadtgemeinde Bremen.

9.3 Einsatz von Telepräsenzrobotern in Schulen

Im Berichtsjahr erreichte den Landesbeauftragten für Datenschutz und Informationsfreiheit eine Anfrage zur datenschutzrechtlichen Einschätzung bezüglich des Einsatzes von Telepräsenzrobotern, sogenannten Schul-Avataren, in bremischen Schulen. Telepräsenzroboter ermöglichen Schülerinnen und Schülern, die aufgrund einer Langzeiterkrankung nicht regelmäßig am Präsenzunterricht teilnehmen können, sich zum Unterricht zuzuschalten. Die Geräte werden im Klassenzimmer auf dem Platz der betroffenen Schülerin beziehungsweise des betroffenen Schülers aufgestellt, haben eine eingebaute Kamera und ein Mikrofon, um den Präsenzunterricht per Live-Stream zu übertragen. Mit einem Endgerät steuert die Schülerin beziehungsweise der Schüler den Telepräsenzroboter, dreht seinen Kopf, sieht den Stream und hört, was um das Gerät herum geschieht. Über eine Leuchtfunktion am Gerät ist erkennbar, ob das Gerät aktiv ist. Die Lehrkräfte haben die Möglichkeit, wie im Präsenzunterricht, ausgleichend einzugreifen und den sogenannten Telepräsenzroboter an anderer Stelle zu positionieren, sofern der Einsatz des Gerätes zu einer Belastung für Mitschülerinnen und Mitschüler, beispielsweise Sitznachbarinnen und Sitznachbarn, führen sollte.

Die Einsatzbedingungen von Telepräsenzrobotern entsprechen damit grundsätzlich denen eines Videokonferenzsystems. Im Rahmen ihrer Aufgabenerfüllung muss die Schule entscheiden, ob ihr Einsatz für den von ihr zu erfüllenden gesetzlichen Bildungs- und Erziehungsauftrag erforderlich ist und inwieweit hiervon Gebrauch gemacht wird. Dabei sind in jedem Fall auch die gesundheitlichen Belange der betroffenen erkrankten Schülerin beziehungsweise des Schülers in den Blick zu nehmen. Zudem muss die Schule gewährleisten, dass das Recht der erkrankten Schülerin oder des erkrankten Schülers auf Bildung in Gemeinschaft, mag dieses Recht auch nur digital vermittelt verwirklicht werden können, umfassend zur Geltung kommen muss. Der hohe Rang dieses Rechtes der erkrankten Schülerin beziehungsweise des erkrankten Schülers ist auch bei der Lösung eines möglichen Konfliktes mit dem Recht auf informationelle Selbstbestimmung zu berücksichtigen.

Um zu verhindern, dass unbefugte Dritte Zugriff auf den Audio- und Videostream erhalten oder die Steuerung des Gerätes übernehmen, muss die Schule auch für eine ausreichende Sicherheit bei dem von den betroffenen Schülerinnen und Schülern eingesetzten mobilen Endgeräten (Tablet, Smartphone) sorgen. Die betroffenen Schülerinnen und Schüler nutzen hier von der Schule bereitgestellte und verwaltete Endgeräte, die verpflichtende Regelungen erfordern.

Aktuell fehlt es im Bremischen Schuldatenschutzgesetz an einer entsprechenden Rechtsgrundlage. Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies die Senatorin für Kinder und Bildung daher darauf hin, dass er die Nutzung von Telepräsenzrobotern für eine

Übergangszeit auch auf der Grundlage von Einwilligungen, die von den Erziehungsberechtigten der Mitschülerinnen und Mitschüler erteilt werden müssen, für möglich erachte, es jedoch zukünftig einer gesetzlichen Regelung im Bremischen Schuldatenschutzgesetz bedarf, um klare Voraussetzungen für den Einsatz zu schaffen.

10. Bau, Wohnen, Umwelt, Energie und Verkehr

10.1 Gemeldete Datenschutzverletzungen

Aus dem Bereich Bau, Wohnen, Umwelt, Energie und Verkehr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr 15 Meldungen über Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung. Auffällig ist hierbei, dass sich die Zahl der Meldungen von sogenannten Datenpannen an ihn im Vergleich zum Vorjahr – insgesamt 21 eingegangene Meldungen – deutlich verringert hat. Die Gründe für diese geringere Anzahl an Meldungen sind bislang offen.

10.2 Sichere Datenübermittlung bei Beantragung einer Bauakte

In dem letzten Berichtsjahr äußerte die Landesbeauftragte für Datenschutz und Informationsfreiheit im Zusammenhang mit einer bei ihr eingegangen Beschwerde unter anderem ihre Bedenken hinsichtlich der Gestaltung der Website im Rahmen der Online-Beantragung einer Bauakte.

Als nicht datenschutzkonform erachtete die Landesbeauftragte für Datenschutz und Informationsfreiheit, dass in den auf ihren Hinweis hin erstellten Kontaktformularen auf der Website mehrere Kontaktmöglichkeiten, wie Adresse, E-Mail und Telefonnummer, parallel abgefragt wurden. Sie wies darauf hin, dass die Verarbeitungen im Rahmen des Datenminimierungsgrundsatzes der Datenschutzgrundverordnung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden müssten, und hielt es für die Beantragung einer Bauakte für ausreichend, wenn entweder Post- oder E-Mail-Adresse angefordert würden. Die Abfrage einer Telefonnummer hielt die Landesbeauftragte für Datenschutz und Informationsfreiheit für entbehrlich. Zudem wies sie darauf hin, dass nicht die Möglichkeit einer persönlichen Vorlage des Ausweisdokumentes bei der Behörde bestanden habe. Ebenfalls für verbesserungswürdig erachtete sie in diesem Zusammenhang einzelne Aspekte der Hochladefunktion für Ausweisdokumente (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 11.6).

Wie in der Stellungnahme des Senats zum 6. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung über den Datenschutz im Jahr 2023 in der Freien Hansestadt Bremen dargestellt, kam es zu positiven Entwicklungen.

Als begrüßenswert erachtet der Landesbeauftragte für Datenschutz und Informationsfreiheit zunächst, dass eine Abfrage der Telefonnummer nicht mehr als Pflichtangabe, sondern nur noch im Rahmen einer freiwilligen Angabe für den Eintritt der Notwendigkeit bei kurzfristigen Klärungen abgefragt wird und dass die Hochladefunktion für Ausweisdokumente auf ihre Vereinbarkeit mit der Datenschutzgrundverordnung überprüft werden soll.

Auch den geplanten Hinweis auf der Website der Behörde, dass der Personalausweis bei dieser persönlich oder per Brief zur Kenntnis gegeben werden könne, betrachtet der Landesbeauftragte für Datenschutz und Informationsfreiheit als richtigen Schritt, um zukünftig die Betroffenenrechte und den Grundsatz der Datenminimierung zu wahren.

Weiterhin Gegenstand der Diskussion zwischen dem Landesbeauftragten für Datenschutz und Informationsfreiheit und dem Ressort ist jedoch die Auffassung des Ressorts, dass für eine vollständige Bearbeitung des Vorganges eine E-Mail-Adresse notwendig sei. Hierzu führt das Ressort aus: Die anzugebende E-Mail-Adresse werde für die elektronische Übermittlung der Datei mit der Bauakte und die vollstreckungsfähige Adresse des Kostenschuldners bei Zahlungsverzug benötigt. Die elektronische Bearbeitung in einem durchgängig digitalen Geschäftsprozess sei zudem ohne Angabe einer E-Mail-Adresse nicht durchführbar.

Für eine Kontaktaufnahme mit der beantragenden Person sowie etwaige Vollstreckungsansprüche gegen diese bei Zahlungsverzug ist demgegenüber die Anforderung der postalischen Adresse nach Einschätzung des Landesbeauftragten für Datenschutz und Informationsfreiheit die zu präferierende Kontaktmöglichkeit.

Die Angabe der E-Mail-Adresse sollte allenfalls als freiwillige Angabe bei der Antragsstellung gelten, beziehungsweise für den Fall, dass die Zusendung der Bauakte auf elektronischem Wege gewünscht wird. Keineswegs sollte den Antragstellenden jedoch der Weg der postalischen Anforderung versperrt werden. Denkbar wäre, dass einigen von ihnen eine Transportverschlüsselung nicht hinreichend sicher sein könnte und Bedenken hinsichtlich unbefugter Zugriffe auf das E-Mail-Postfach bestehen könnten. Zudem ist durchaus vorstellbar, dass nicht jede Antragstellerin beziehungsweise jeder Antragsteller über einen Schlüssel für eine Ende-zu-Ende-Verschlüsselung verfügt, geschweige denn weiß, wie dieser eingerichtet wird.

Ungeachtet dessen sollte auch Personen, die aktuell über keinen funktionsfähigen Drucker oder ähnliche Mittel verfügen, die Möglichkeit der Anforderung in Papierform nicht verwehrt werden. Dass die elektronische Bearbeitung des Antrages ohne Angabe der E-Mail-Adresse nicht möglich sei, erschließt sich dem Landesbeauftragten für Datenschutz und Informationsfreiheit – auch aus technischer Sicht – nicht.

10.3 Veröffentlichung von Immobilienfotos im Zusammenhang mit Online-Immobilieninseraten

Den Landesbeauftragten für Datenschutz und Informationsfreiheit erreichte die Beschwerde eines Petenten, der in Bezug auf Veröffentlichung eines Immobilieninserates zum Verkauf eines Nachbarshauses zufällig darauf gestoßen war, dass auch seine Immobilie mit auf dem

Online-Inserat zu sehen war. Da auf der Anzeige ebenfalls noch ein Gewerbebetrieb mit abgebildet war, dessen Adresse man problemlos, beispielsweise per Internetrecherche, ermitteln konnte, ermöglichte eine anschließende Suche über Google Street View oder Apple Look Around die Herstellung eines Personenbezuges zu seiner Immobilie, weil diese räumlich zugeordnet werden konnte.

Die Veröffentlichung der Immobilie erfolgte ohne eine entsprechende Einwilligung des Petenten nach Artikel 7 Absatz 1 Datenschutzgrundverordnung (DSGVO) und der Immobilienmakler versäumte es ebenfalls, eine Verpixelung des beschwerdegegenständlichen Hauses vorzunehmen, mit der eine Identifizierung der Immobilie des Betroffenen und somit ein datenschutzrechtlicher Verstoß hätte verhindert werden können.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit empfiehlt in diesem Zusammenhang Immobilienmaklerinnen und Immobilienmaklern, vor einer Veröffentlichung von Lichtbildaufnahmen – insbesondere bewohnter Immobilien – weiterhin, eine Einwilligung der Betroffenen einzuholen, die den Voraussetzungen des Artikel 7 DSGVO entspricht (im Optimalfall schriftlich), um die Risiken etwaiger Datenschutzverstöße zu vermeiden oder zumindest zu minimieren. Zu den Immobilien zählen, für die eine entsprechende Einwilligung eingeholt werden muss, wie in dem eingangs geschilderten Beschwerdesachverhalt, auch nicht zum Verkauf angebotene, benachbarte Immobilien, soweit diese nicht verpixelt wurden.

Zum Thema Einholung einer Einwilligung bei Veröffentlichung von Immobilienfotos weist der Landesbeauftragte für Datenschutz und Informationsfreiheit in diesem Kontext noch auf das Urteil des Landgerichtes Frankenthal vom 4. Juni 2024 (Aktenzeichen 3 O 300/23) hin. In diesem Verfahren hat das Landgericht Frankenthal eine Klage auf Schadensersatz mit der Begründung abgewiesen, dass die Kläger, Mieter einer zum Verkauf angebotenen Wohnung, durch ihr Dabeisein bei den Lichtbildaufnahmen in ihrer Wohnung konkludent nicht nur in die Anfertigung der Aufnahmen, sondern auch in die Veröffentlichung dieser zwecks Verkauf, was bei Immobilieninseraten üblicherweise zu erwarten ist, eingewilligt hätten. Eine stillschweigende Einwilligung reiche in einer solchen Konstellation, so das Landgericht Frankenthal, aus und bedürfe daher auch keiner weiteren insbesondere schriftlichen Form. Danach sei eine Einwilligung auch jede bestätigende Handlung, mit der die betroffene Person zu verstehen gebe, dass sie mit der Verarbeitung der sie betroffenen Daten einverstanden sei. Eine dementsprechende Einwilligung sei in dem vom Landgericht Frankenthal entschiedenen Fall durch die Kläger erteilt worden. Indem sie die Mitarbeiterinnen und Mitarbeiter der Beklagten in die Wohnung gelassen und diesen erlaubt hätten, die Lichtbildaufnahmen anzufertigen, hätten sie unmissverständlich und konkludent ihre Einwilligung dazu gegeben. Zudem räumten sie ein, dass ihnen bewusst gewesen sei, dass die Fotos im Rahmen des Verkaufes der streitgegenständlichen Immobilie angefertigt worden seien.

10.4 Verbändeanhörung zur überarbeiteten Orientierungshilfe für Mietinteressentinnen und Mietinteressenten

Im 6. Jahresbericht nach der Datenschutzgrundverordnung berichtete die Landesbeauftragte für Datenschutz und Informationsfreiheit über ihre Teilnahme an einem bundesweiten Unterarbeitskreis zur Überarbeitung der Orientierungshilfe für Mietinteressentinnen und Mietinteressenten, die sowohl ein Leitfaden für Menschen, die planen, Wohnraum anzumieten, als auch eine Hilfestellung für Vermieterinnen und Vermieter sein soll (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 11.3). Nach Erstellung der nunmehr überarbeiteten Fassung wurde die Orientierungshilfe im Berichtsjahr im Auftrag der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder durch den Arbeitskreis Wirtschaft zur Stellungnahme an sieben Bundesverbände, die Interessen von mietenden sowie vermietenden Parteien vertreten, versendet. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit lag bei Redaktionsschluss eine Stellungnahme vor, hinsichtlich einer weiteren wurde um Fristverlängerung gebeten. Eine Auswertung der Verbändestellungnahmen wird somit voraussichtlich im nächsten Berichtsjahr erfolgen.

Die Neufassung der Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressentinnen und Mietinteressenten inklusive eines Musterfragebogens als Anlage ist auf der Homepage des Landesbeauftragten für Datenschutz und Informationsfreiheit abrufbar.[4]

10.5 Datenschutzkonformität von smarten Rauchwarnmeldern

In den Vorberichtsjahren setzte sich die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen mit der Datenschutzkonformität von digitalen Zählern mit Funkmodul, insbesondere im Bereich Kaltwasser, auseinander, weil es hier – im Gegensatz zu den Bereichen Strom, Heizung und Warmwasser – bisher weiterhin noch keine spezifische Rechtsgrundlage für die Übertragung von personenbezogenen Daten per Funk gibt, die einen ausreichenden Schutz für das Grundrecht auf informationelle Selbstbestimmung gewährleistet.

Eine ähnliche Problematik ergibt sich nun im Bereich von Rauchwarnmeldern, weil ein deutschlandweit tätiges Wohnungsunternehmen anlässlich der zehnjährigen Austauschpflicht in Wohngebäuden nun smarte Modelle einbauen möchte, die neben der herkömmlichen Brandmeldefunktion unter anderem auch die Datenverarbeitung für ein Raum- und Klimamo-

[4] https://www.datenschutz.bremen.de/sixcms/media.php/13/2024-01-24_DSK-OH_Mietinteresse_V1.0.pdf.

nitoring ermöglichen und Bewegungsprofile erstellen können. Dies hat zur Folge, dass tiefergehende Rückschlüsse auf das Wohnverhalten und die Lebensgewohnheiten der jeweiligen Personen möglich sind. Beispielsweise kann das Gerät ermitteln, in welchem Raum sich eine Person gerade aufhält oder anhand von Informationen zu Temperatur und Luftfeuchtigkeit feststellen, ob ausreichend gelüftet wird, und gegebenenfalls sogar Tipps für ein richtiges Lüftungsverhalten erteilen.

Bei temporär abweichendem Heiz- und Lüftungsverhalten sind auch Rückschlüsse darüber möglich, ob Mieterinnen und Mieter über einen gewissen Zeitraum abwesend sind, beispielsweise sich im Urlaub befinden.

Beim Ausbleiben hinreichend technischer und organisatorischer Sicherheitsmaßnahmen, insbesondere beim Datenübertragungsprozess, kann auch die Gefahr unbefugter Zugriffe durch Dritte nicht mit hinreichender Sicherheit ausgeschlossen werden.

In der Freien Hansestadt Bremen ist der Einbau der smarten Rauchwarnmelder durch das besagte Unternehmen zwar derzeit nicht vorgesehen, dennoch befindet sich der Landesbeauftragte für Datenschutz und Informationsfreiheit in einem aktiven Austausch- und Beratungsprozess mit weiteren datenschutzrechtlichen Aufsichtsbehörden im Rahmen eines bundesweiten Arbeitskreises. Er sieht angesichts der hohen Eingriffsintensität die Installation von smarten Rauchmeldern sehr kritisch, weil ein hohes Gefährdungspotenzial besteht, wenn Daten über Mieterinnen und Mieter zu deren Wohnverhalten erhoben werden.

11. Beschäftigtendatenschutz

11.1 Gemeldete Datenschutzverletzungen

In diesem Berichtsjahr wurden bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit im Bereich Beschäftigtendatenschutz 62 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. 48 Meldungen stammten dabei aus dem nicht öffentlichen Bereich, 14 Meldungen hingegen aus dem öffentlichen Bereich. Neben diesen Meldungen erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit insgesamt 65 Beschwerden über den Umgang der Verantwortlichen mit Beschäftigtendaten, wobei 15 Beschwerden dem öffentlichen Bereich und die restlichen 50 Beschwerden dem nicht öffentlichen Bereich zuzuordnen waren. Darüber hinaus erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit im Bereich des Beschäftigtendatenschutzes viele telefonische Anfragen, die besonders häufig die Überwachung der Beschäftigten sowie die Weitergabe von Beschäftigtendaten betrafen. Weiterhin stellen unzulässige Videoüberwachungen und Überwachungen mit dem Ortungssystem GPS ein erhebliches Problem für die Beschäftigten dar.

11.2 Stellenausschreibung – Einsicht in die Personalakte

Durch eine Beschwerde wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit darauf aufmerksam gemacht, dass verschiedene Dienststellen in ihren Stellenausschreibungen Bewerberinnen und Bewerber dazu auffordern, ihrer Bewerbung eine Einverständniserklärung zur Einsichtnahme in eine etwaig vorhandene Personalakte beizufügen.

Hinsichtlich der Einsichtnahme in die Personalakte bereits zu einem so frühen Zeitpunkt des Bewerbungsverfahrens bestehen jedoch erhebliche datenschutzrechtliche Bedenken. So enthält die Personalakte neben der Grundakte auch Teil- und Nebenakten.

Die Erforderlichkeit der Einsichtnahme in die gesamte Personalakte bereits zu Beginn des Bewerbungsverfahrens konnte nicht dargelegt werden. Für das Treffen einer Auswahlentscheidung ist darüber hinaus die Anforderung der Grundakte daher grundsätzlich ausreichend.

Die aufgrund der Beschwerde angeschriebenen Dienststellen teilten daraufhin mit, dass sie das Tätigwerden des Landesbeauftragten für Datenschutz und Informationsfreiheit zum Anlass genommen haben, das bisherige Verfahren abzuändern. Hierzu zählt unter anderem, dass Einwilligungen zur Einsichtnahme in die Grundakte nur noch von denjenigen Bewerberinnen und Bewerbern erbeten werden, die nach der Vorauswahl dem engeren Kreis der Bewerberinnen und Bewerber angehören.

11.3 Videoüberwachung im Beschäftigtenverhältnis

In diesem Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit erneut mehrere Beschwerden zur Videoüberwachung im Beschäftigtenverhältnis. Der Umfang der Überwachung war dabei sehr unterschiedlich. So erfolgte unter anderem in einem Fall eine komplette Überwachung der Büroräume, in einem weiteren Fall hingegen wurde das gesamte Außengelände sowie die Produktionshallen mittels Videokameras überwacht. Häufig waren hierbei auch die Speicherfristen problematisch, weil in einigen Unternehmen die Aufnahmen erst nach 20 Tagen gelöscht wurden.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies in allen Fällen darauf hin, dass die Videoüberwachung im Beschäftigtenverhältnis aufgrund des dort bestehenden Über- beziehungsweise Unterordnungsverhältnisses sehr hohen Anforderungen unterliegt. Es ist daher immer eine Prüfung der Zulässigkeit im Einzelfall erforderlich. Grundsätzlich gilt, dass der Einsatz von Kameras zum Zweck der Verhaltens- und Leistungskontrolle nicht erlaubt ist. Dementsprechend dürfen auch dauerhafte Arbeitsplätze oder Bereiche, in denen sich Beschäftigte über längere Zeit aufhalten, grundsätzlich nicht überwacht werden. Dies gilt ebenfalls für Pausen-, Sozial- und Aufenthaltsräume und insbesondere für sensible Bereiche, wie Umkleidekabinen oder Sanitärräume.

In jedem Fall, auch wenn Bereiche überwacht werden, in denen sich Beschäftigte nur vorübergehend oder gelegentlich aufhalten, ist vor Einsatz der Videoüberwachung eine Interessenabwägung durchzuführen. Hierbei ist unter anderem auch zu berücksichtigen, ob den Beschäftigten ein kontrollfreier und unbeobachteter Arbeitsbereich verbleibt. Je weniger Rückzugsraum zur Verfügung steht, desto eher überwiegen die schutzwürdigen Interessen der Beschäftigten.

Bezüglich der Speicherdauer ist stets zu beachten, dass die Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zweckes nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Hierbei wird regelmäßig eine Speicherdauer von 72 Stunden für zulässig erachtet. Wird seitens des Verantwortlichen eine darüberhinausgehende Speicherdauer für erforderlich gehalten, so sind der Zweck und die Notwendigkeit der längeren Speicherung für jede Kamera einzeln umso ausführlicher zu begründen.

Durch sein Tätigwerden konnte der Landesbeauftragte für Datenschutz und Informationsfreiheit in mehreren Fällen erreichen, dass die beanstandeten Videoüberwachungsanlagen abgeschaltet wurden. In weiteren Fällen konnte eine Anpassung der durchgeführten Videoüberwachungen an die datenschutzrechtlichen Vorgaben erreicht werden.

11.4 Bewerbung per WhatsApp

In diesem Berichtsjahr wurde der Landesbeauftragte für Datenschutz und Informationsfreiheit durch einen Pressebericht darauf aufmerksam, dass ein Unternehmen in der Freien Hansestadt Bremen eine Bewerbungsmöglichkeit über den Messenger-Dienst WhatsApp eingeführt hat. Aufgrund der bestehenden datenschutzrechtlichen Bedenken hat der Landesbeauftragte für Datenschutz und Informationsfreiheit den Verantwortlichen daher zunächst zur Stellungnahme aufgefordert und auf die bestehenden Bedenken hingewiesen. Der Verantwortliche teilte ihm daraufhin mit, dass ein vertraglich gebundener Auftragsverarbeiter aus Deutschland genutzt werde, sodass die verarbeiteten Daten ausschließlich auf zertifizierten und verschlüsselten Servern in Deutschland gehostet würden und kein Zugriff durch WhatsApp (Meta Plattforms Incorporated) auf konkrete Nachrichteninhalte möglich sei.

In diesem Zusammenhang wies der Landesbeauftragte für Datenschutz und Informationsfreiheit den Verantwortlichen darauf hin, dass eine WhatsApp-Nutzung über einen Dienstleister, der die Kommunikationsdaten selbst hoste, demnächst voraussichtlich nicht mehr möglich sein werde und die Daten spätestens ab diesem Zeitpunkt durch die Meta Plattforms Incorporated (WhatsApp) gehostet würden. Er regte daher an, die Bewerbungsmöglichkeit über WhatsApp vorsorglich erneut zu überprüfen und erforderlichenfalls einzustellen.

12. Medien, Telemedien, Digitalisierung

12.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden im Bereich Medien, Telemedien und Digitalisierung insgesamt drei Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung an den Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet.

12.2 In-Real-Life Streams

Im Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit Beschwerden zu Live-Streams auf internationalen Streaming Plattformen aus dem öffentlichen Raum. In den Aufnahmen dieser Streams konnten personenbezogene oder personenbeziehbare Daten, wie Personen oder KfZ-Kennzeichen, ausgemacht werden.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit ist mit der verantwortlichen Stelle in den Austausch gegangen und hat darauf hingewiesen, dass technische Maßnahmen zu treffen sind, um die personenbezogenen Daten von Unbeteiligten zu schützen. Er hat Kenntnis von weiteren Live-Streams, die ohne technische Maßnahmen erfolgt sind.

Der Vorgang ist noch nicht abgeschlossen.

12.3 Live-Streams aus Nachtschichten in Pflegeeinrichtungen auf Tik-Tok

Im Berichtsjahr hat der Landesbeauftragte für Datenschutz und Informationsfreiheit davon Kenntnis erhalten, dass auf der chinesischen Plattform Tik-Tok eine zunehmende Menge an Live-Streams aus Pflegeeinrichtungen veröffentlicht wird. Dies sieht er kritisch, weil im Umfeld sensible personenbezogene Daten sichtbar sein könnten.

Bei den Recherchen zu diesem Thema ist der Landesbeauftragte für Datenschutz und Informationsfreiheit auf einen Fall aus der Freien Hansestadt Bremen gestoßen. Die konkrete Pflegeeinrichtung, aus der diese Streams erfolgten, fiel unter die Zuständigkeit der Aufsichtsbehörde der Evangelischen Kirche in Deutschland. Der Vorgang wurde an die zuständige Aufsichtsbehörde abgegeben und es bleibt abzuwarten, ob bei der Bearbeitung ein sogenannter Mitarbeiterexess festgestellt wird, also eine Verarbeitung personenbezogener Daten in einer Art und Weise, die nicht in dem Arbeitsvertrag vorgegeben ist. In diesem Fall würde die Zuständigkeit an die Aufsichtsbehörde fallen, in der der entsprechende Mitarbeiter wohnhaft ist.

12.4 Dark Patterns in Cookie-Bannern

Wie schon in dem 5. Jahresbericht nach der Datenschutzgrundverordnung befasste sich der Landesbeauftragte für Datenschutz und Informationsfreiheit auch dieses Jahr erneut mit so genannten Dark Patterns (siehe hierzu 5. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 13.4). Unter dem Ausdruck Dark Patterns ist die Gestaltung von Websites zu verstehen, durch die Nutzende teilweise in aufdringlicher Weise dazu bewegt werden, Entscheidungen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zu treffen, die sie ohne diese suggestiven Gestaltungen nicht getroffen hätten. Dadurch ist hierbei zumeist nicht von einer freiwilligen und informierten Einwilligung auszugehen.

Den Landesbeauftragten für Datenschutz und Informationsfreiheit erreichte hierzu im Laufe des Berichtsjahres eine Beschwerde zu einem Cookie-Banner bei einer Website, bei der die Möglichkeit zum Ablehnen in einem Fließtext versteckt war, während der Button zur Einwilligung in die Datenverarbeitung in auffallender Farbe gestaltet war. Tatsächlich muss die Möglichkeit zum Ablehnen als Alternative zum Akzeptieren eindeutig erkennbar, leicht wahrnehmbar und unmissverständlich sein. Entscheidend ist, dass die verschiedenen Optionen gleichwertig dargestellt und diese von den Nutzenden wahrgenommen werden können. Dies war hier jedoch nicht der Fall. Der im Fließtext versteckte Button war für die Nutzenden kaum wahrnehmbar, insbesondere nicht als gleichwertige Alternative zum Akzeptieren-Button.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies den Verantwortlichen auf diese nicht mit den datenschutzrechtlichen Vorgaben vereinbare Gestaltung seines Cookie-Banners hin und konnte im Rahmen eines kooperativen Austausches erreichen, dass das Cookie-Banner nunmehr eine gleichwertige Möglichkeit zum Ablehnen auf der ersten Ebene bereithält.

12.5 Weiterhin fehlende oder fehlerhafte Datenschutzerklärungen

Auch in diesem Berichtsjahr erreichte den Landesbeauftragten für Datenschutz und Informationsfreiheit wieder eine Vielzahl von Beschwerden aufgrund von fehlenden oder fehlerhaften Informationen nach Artikel 13 Datenschutzgrundverordnung auf Websites (siehe hierzu bereits 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 13.3). Wie auch schon bei den nicht mit den datenschutzrechtlichen Vorgaben zu vereinbarenden Cookie-Bannern ist es auch bei den fehlenden oder fehlerhaften Datenschutzerklärungen aus Sicht des Landesbeauftragten für Datenschutz und Informationsfreiheit unverständlich, wie diese in einer solchen Vielzahl im siebten Jahr nach Inkrafttreten der Datenschutzgrundverordnung auftreten können.

12.6 Veröffentlichungen von personenbezogenen Daten in Google Rezensionen

Im Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit erneut mehrere Beschwerden zu in Google Rezensionen veröffentlichten personenbezogenen Daten (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 13.4). Daher wird er die wiederholten Verstöße gegen die Datenschutzgrundverordnung in diesen Sachverhaltskonstellationen zum Anlass nehmen, um die Ärztekammer Bremen für diese Problematik zu sensibilisieren.

Die Offenlegung erfolgte in allen Fällen durch die Inhaber von Arzt- beziehungsweise Tierarztpraxen im Rahmen von deren Antwort auf vermeintlich zu negative oder falsche Rezensionen von Patientinnen und Patienten beziehungsweise Kundinnen und Kunden. In allen Fällen wurden die Rezensionen von den betroffenen Personen unter einem Pseudonym abgegeben, jedoch durch die verantwortliche Stelle in deren Antwort unter Nennung des vollständigen Namens der betroffenen Person beantwortet und so die Identität der betroffenen Personen offengelegt.

Auch erfolgte jeweils eine weitere Offenlegung von personenbezogenen Daten. So wurden in einem Fall die Anschrift der betroffenen Person in der Antwort auf die Rezension genannt. In einem anderen Fall erfolgte gar eine Offenlegung der medizinischen Behandlungsgeschichte der betroffenen Person.

In allen Fällen konnte durch das Tätigwerden des Landesbeauftragten für Datenschutz und Informationsfreiheit erreicht werden, dass die in Frage stehenden Antworten auf die Google Rezensionen gelöscht wurden.

12.7 App-Angebote durch Behörden

In dem Berichtsjahr erreichte den Landesbeauftragten für Datenschutz und Informationsfreiheit eine Beratungsanfrage zu einer entwickelten App von einer Behörde. Die Prüfung dieser App ist noch nicht vollständig abgeschlossen. Problematisch ist für die Behörden in der Freien Hansestadt Bremen, dass die Ausschreibung für die Entwickler von Apps durch den IT-Dienstleister der Freien Hansestadt Bremen erfolgt.

Bei der Beratung der Behörden ist der Landesbeauftrage für Datenschutz und Informationsfreiheit auf Probleme in dem Entwicklungs- und Beschaffungsprozess für die konkreten Apps gestoßen. Die Behörden wenden sich an den IT-Dienstleister der Freien Hansestadt Bremen. Dieser IT-Dienstleister schreibt dann für die Behörde die zu entwickelnde App aus und sucht

aus den Angeboten einen geeigneten Dienstleister heraus. Der Dienstleister entwickelt dann die App für die Behörde.

Datenschutzrechtlich steht der Landesbeauftragte für Datenschutz und Informationsfreiheit hier vor zwei Schwierigkeiten: Einerseits besteht zwischen den Behörden und dem IT-Dienstleister kein Auftragsverarbeitungsvertrag. Dies kann problematisch sein, falls die App über die IT-Infrastruktur des IT-Dienstleisters läuft und dort personenbezogene Daten verarbeitet werden. Andererseits sind die Informationen, die der Landesbeauftragte für Datenschutz und Informationsfreiheit für die Beratung benötigt, nicht in der Detailtiefe bei der verantwortlichen Behörde vorhanden.

12.8 Veröffentlichungen auf Instagram

Am Ende des Berichtszeitraumes erreichte den Landesbeauftragten für Datenschutz und Informationsfreiheit eine Beschwerde zu einer Veröffentlichung eines Videos auf Instagram. In diesem Fall habe ein Gastronomie-Betrieb Videos von der Eröffnungsfeier ohne Einwilligung der Kunden aufgezeichnet und auf dem geschäftlichen Instagram-Account veröffentlicht. Der Landesbeauftragte für Datenschutz und Informationsfreiheit steht mit der verantwortlichen Stelle in Kontakt. Der Vorgang ist noch nicht abgeschlossen.

12.9. Gründung des Arbeitskreises Künstliche Intelligenz

Im November des Jahres 2024 wurde von der Datenschutzkonferenz der Arbeitskreis „Künstliche Intelligenz“ gegründet, an dem der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen sich aktiv beteiligt. In dem Arbeitskreis wird die allgemeine Entwicklung verfolgt und es werden unter anderem Positionspapiere sowie Handlungsempfehlungen zum Umgang mit Künstlicher Intelligenz entwickelt. Um der Schnelllebigkeit der technischen Entwicklung Genüge zu tun, gibt es regelmäßige Treffen und kleinere, agilere Unterarbeitsgruppen. Für die Unterarbeitsgruppe „Forschung und neuere Entwicklungen“ hat der Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen auf der konstituierenden Sitzung, die am 23. und 24. Januar 2025 nach Redaktionsschluss dieses Jahresberichtes stattfand, die Leitung übernommen.

13. Werbung

13.1 Gemeldete Datenschutzverletzungen

Von Unternehmen aus dem Bereich Werbung erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtsjahr eine Meldung über Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung.

Dagegen erreichten ihn 36 Beschwerden über Unternehmen, die aus Sicht der Beschwerdeführenden im Zusammenhang mit Werbemaßnahmen gegen die Datenschutzgrundverordnung verstoßen hatten. Die hohe Diskrepanz zwischen der Anzahl der gemeldeten Verletzungen des Schutzes personenbezogener Daten einerseits und der Anzahl der Beschwerden andererseits legt nahe, dass es weiterhin eine hohe Dunkelziffer bei den Meldungen in Bezug auf Verletzungen des Schutzes personenbezogener Daten im Werbebereich gibt (siehe hierzu 6. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 14.1).

13.2 Unverzügliche Eintragung von Werbewidersprüchen

Im Berichtsjahr erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit darüber hinaus zahlreiche Beschwerden über die Nichtumsetzung von Werbewidersprüchen.

Gemäß den Vorgaben der Datenschutzgrundverordnung sind Werbewidersprüche von den jeweiligen Verantwortlichen unverzüglich umzusetzen. Im Falle der postalischen Werbung hat die oder der jeweilige Verantwortliche zusätzlich darauf zu achten, dass im Rahmen der unverzüglichen Umsetzung von Werbewidersprüchen sichergestellt wird, dass keine neuen Verarbeitungsaufträge, wie zum Beispiel neue Drucke und deren Versand, gestartet werden.

13.3 Hinweispflicht auf Möglichkeit zum Werbewiderspruch

Im Bereich Werbung erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit weitere Anfragen und Beschwerden, insbesondere in Bezug auf die Abbestellung von Newslettern. Gemäß den Vorgaben der Datenschutzgrundverordnung muss die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf ihr Werbewiderspruchsrecht hingewiesen werden.

Der Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen, um eine faire und transparente Verarbeitung zu gewährleisten. Eine Abmeldung sollte daher bei E-Mail-Werbung beispielsweise mit einem Anklicken des Abmelde-Links in der werblichen E-Mail ohne zusätzliche Erschwernisse möglich sein.

Exemplarisch kann ein Fall aus dem Berichtszeitraum genannt werden. In diesem Fall fehlte der Abmelde-Link in der Werbe-E-Mail vollständig. Der Landesbeauftragte für Datenschutz und Informationsfreiheit wirkte erfolgreich auf die betreffende verantwortliche Stelle ein, ihre Werbe-E-Mails zukünftig in jeder Hinsicht gemäß den Vorgaben der Datenschutzgrundverordnung zu gestalten.

14. Videoüberwachung im nicht öffentlichen Bereich

14.1 Gemeldete Datenschutzverletzungen

Auch in diesem Berichtsjahr gab es im Bereich Videoüberwachung keine gemeldeten Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung. Allerdings stieg die Zahl der Beschwerden erneut an und lag in diesem Jahr bei 106 Beschwerden. Der hohe Beratungsbedarf im Bereich der Videoüberwachung durch nicht öffentliche Stellen spiegelt sich auch in der Anzahl der telefonischen und schriftlichen Beratungsanfragen wieder.

14.2 Videoüberwachung im privaten Bereich – Haushaltsausnahme

Der überwiegende Teil der Beschwerdefälle bezog sich in diesem Berichtszeitraum auf an Fassaden von Privathäusern und Eigentumswohnanlagen angebrachte Überwachungskameras. Die Verantwortlichen gaben oft an, die Kameras zum Schutz des Eigentums installiert zu haben. Dabei gingen viele davon aus, dass solch eine Videoüberwachung als ausschließlich persönliche oder familiäre Tätigkeit einzuordnen und die Datenschutzgrundverordnung auf solche Datenverarbeitungen nicht anwendbar sei (sogenannte Haushaltsausnahme gemäß Artikel 2 Absatz 2 Buchstabe c) Datenschutzgrundverordnung). Bei einem solchen Vorgehen wird jedoch oft übersehen, dass dabei möglicherweise auch der öffentliche Verkehrsraum miterfasst wird und die Datenverarbeitung somit gerade nicht unter die Haushaltsausnahme fällt.

In allen Fällen wurden die Verantwortlichen auf die rechtlichen Zulässigkeitsvoraussetzungen hingewiesen. Kamerabetreiberinnen und -betreiber können sich nur auf dem eigenen Grundstück auf das Hausrecht beziehungsweise die Haushaltsausnahme im Sinne der Datenschutzgrundverordnung berufen. Eine Videoüberwachung hat grundsätzlich an der Grenze des eigenen Grundstücks zu enden. Öffentliche Verkehrsbereiche sowie nachbarliche Grundstücke dürfen hingegen im Regelfall nicht mit überwacht werden, weil dort grundsätzlich die schutzwürdigen Interessen der betroffenen Personen überwiegen.

14.3 Einsatz von Klingelkameras

Eine Beschwerde, die ebenfalls dem Bereich der Videoüberwachung durch Privatpersonen zuzurechnen ist, betraf die Installation einer Klingelkamera in einem Mehrfamilienhaus durch den Vermieter. Auch Tür- und Klingelkameras stellen optisch-elektronische Einrichtungen dar, mithilfe derer personenbezogene Daten, zum Beispiel Bilddaten, verarbeitet werden. Vorliegend war die Klingelanlage derart konfiguriert, dass das Kamerabild gezeigt wurde, wenn von außen die Klingel oder von innen der Überwachungsmodus betätigt wurde. In beiden Fällen schaltete sich die Kamera nach etwa 40 Sekunden automatisch ab.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit wies den Verantwortlichen daher darauf hin, dass Kameras in Klingelanlagen so geschaltet sein müssen, dass nur die Bewohner auf die Bilder zugreifen können, bei denen geklingelt wird, und forderte zu einer entsprechenden Anpassung auf. Das Klingelsystem muss technisch so eingerichtet sein, dass eine Bildübertragung erst nach Betätigung der Klingel ermöglicht und räumlich nicht mehr abgebildet wird, als ein Blick durch einen Türspion gewähren würde. Darüber hinaus muss die Übertragung nach einigen Sekunden automatisch unterbrochen werden. Auch darf keine Übertragung des Livebildes über das Internet oder eine Aufzeichnung der Bilder erfolgen. Eine Tür- und Klingelkamera, die manuell aktiviert werden kann und dabei auch Gemeinschaftsflächen erfasst, erfüllt die rechtlichen Anforderungen an eine Videoüberwachung hingegen nicht.

15. Kredit-, Versicherungs- und allgemeine Wirtschaft

15.1 Gemeldete Datenschutzverletzungen

Die Anzahl der Meldungen nach Artikel 33 Datenschutzgrundverordnung (DSGVO) von Unternehmen aus den hier betrachteten Branchen veränderte sich gegenüber dem vorigen Berichtszeitraum nur wenig. Auch inhaltlich betrafen die Meldungen – bei abstrakter Betrachtung – im Wesentlichen die bereits in den vorherigen Jahresberichten geschilderten Fallgestaltungen. Auch wenn ein Verantwortlicher von einer Meldung absehen kann, sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, empfiehlt der Landesbeauftragte für Datenschutz und Informationsfreiheit weiterhin eine Meldung. Denn das Unterlassen einer Meldung bei einem tatsächlich meldepflichtigen Vorfall kann mit einer Geldbuße nach Artikel 83 DSGVO geahndet werden.

Lediglich eine Meldung erfolgte in diesem Berichtsjahr zur mannigfachen Offenlegung von personifizierten E-Mail-Adressen infolge Nutzung des offenen E-Mail-Adressfeldes „An“ bei einem Nachrichtenversand. Ob dies auf ein mittlerweile generell bei den Versendern elektronischer Nachrichten vorhandenes Problembewusstsein zur Nutzung eines offenen E-Mail-Verteilers zurückzuführen ist oder lediglich weitere derartige Vorfälle nicht bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet wurden, bleibt jedoch offen.

Die schwerwiegendsten Schadensereignisse, die dem Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet wurden, hatten neuerlich wieder externe Angriffe auf die IT-Infrastruktur von Unternehmen zum Gegenstand, wie zum Beispiel Ransomware-Attacken oder Phishing-Mail-Attacken. Mit derartigen Angriffen aus den Tiefen des World Wide Web geht im Erfolgsfalle für diejenigen, deren personenbezogene Daten betroffen sind, nahezu ausnahmslos ein irreversibler Kontrollverlust über ihre personenbezogenen Daten einher; mit den Folgen werden die Betroffenen dann seitens der eigentlichen (Daten-)Verantwortlichen nach der Erfahrung des Landesbeauftragten für Datenschutz und Informationsfreiheit aber allzu oft alleine gelassen. Dies wiegt umso schwerer, je unabänderlicher die abgeflossenen Informationen, etwa (biometrische) Identitätsdaten sind.

Weitere Vorfallsmeldungen hatten – auch dies eine Konstante – die versehentliche Offenlegung personenbezogener Informationen aufgrund fehlerhaft erfasster oder veralteter postalischer wie auch elektronischer Kontaktdaten eines Adressaten zum Gegenstand.

15.2 Höchstrichterliche Präzisierungen des Schadensersatzanspruchs Betroffener bei Cyberangriffen auf Unternehmen

Nach Artikel 82 Datenschutzgrundverordnung (DSGVO) steht einer Person, die wegen eines Verstoßes gegen datenschutzrechtliche Rechtsvorschriften einen materiellen oder immateriellen Schaden erlitten hat, grundsätzlich ein Anspruch auf Schadensersatz gegen die verantwortliche Stelle beziehungsweise deren Auftragsverarbeiter zu. Derjenige, der Schadensersatz begehrt, muss freilich das Vorliegen eines Verstoßes gegen die Datenschutzgrundverordnung, seinen materiellen beziehungsweise immateriellen Schaden sowie einen Kausalzusammenhang zwischen dem Schaden und dem Verstoß darlegen und gegebenenfalls beweisen (vergleiche Europäischer Gerichtshof, Urteil vom 25. Januar 2024, Aktenzeichen C-687/21, Randnummer 58).

In Bezug auf erfolgreiche Cyberattacken Dritter auf ein Unternehmen, das die Daten eines Betroffenen verarbeitet, erfolgte zwischenzeitlich eine wichtige Präzisierung dieses Schadensersatzanspruchs Betroffener durch eine höchstrichterliche Entscheidung des Europäischen Gerichtshofes. Mit Urteil vom 14. Dezember 2023 in der Rechtssache C-340/21 entschied der Europäische Gerichtshof insoweit insbesondere Folgendes:

Allein daraus, dass es zu einem unbefugten Zugang Dritter zu bei einem Verantwortlichen gespeicherten personenbezogenen Daten gekommen ist, kann noch nicht abgeleitet werden, dass die technischen beziehungsweise organisatorischen Sicherungsmaßnahmen des Verantwortlichen ungeeignet gewesen sind; denn, jegliches Risiko im Vorfeld durch Sicherungsmaßnahmen auszuschließen, kann das geltende Recht vernünftigerweise nicht verlangen.

Allerdings muss der Verantwortliche selbst aufgrund seiner grundlegenden gesetzlichen Rechenschaftspflicht (vergleiche Artikel 5 Absatz 2 DSGVO, Artikel 24 Absatz 1 Satz 1 DSGVO) darlegen und beweisen, dass er zur Absicherung der Datenverarbeitung geeignete und angemessene technische beziehungsweise organisatorische Maßnahmen implementiert hatte. Nicht die Anspruchstellerin oder der Anspruchsteller muss das Gegenteil beweisen und darlegen.

Der Umstand, dass ein Schaden durch unbefugten Zugang zu personenbezogenen Daten allein auf der Handlung eines möglicherweise kriminellen Dritten beruht, genügt im Rahmen der Exkulpationsmöglichkeit (Artikel 82 Absatz 3 DSGVO) nicht, um den Verantwortlichen schon von seiner Haftung zu befreien. Ebenso wenig kann sich der Verantwortliche nach einer weiteren Entscheidung des Europäischen Gerichtshofes grundsätzlich von seiner Haftung

allein dadurch befreien, dass er geltend macht, der Schaden sei durch ein fahrlässiges Fehlverhalten einer ihm unterstellten Person verursacht worden (Europäischer Gerichtshof, Urteil vom 11. April 2024, Aktenzeichen C-741/21).

Da ein Schaden im Sinne der Datenschutzgrundverordnung bereits im Verlust der Kontrolle über eigene Daten liegen kann, kann auch die Befürchtung eines Betroffenen, seine abgeflossenen Daten würden durch die Hacker missbräuchlich verwendet, bereits einen ersatzfähigen immateriellen Schaden darstellen, selbst wenn konkret noch keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil des Betroffenen erfolgt sein sollte. Allerdings muss diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person hinreichend begründet sein; dies dürfte allerdings bei einem zielgerichteten Angriff zur Erlangung beispielsweise von Identitäts- oder Zahlungsmitteldaten häufig darzulegen sein.

In einer weiteren Rechtssache stellte der Europäische Gerichtshof mit Urteil vom 14. Dezember 2023 (Aktenzeichen C-456/22) zudem nochmals klar, dass nach einem erwiesenen Verstoß gegen Bestimmungen der Datenschutzgrundverordnung der von der betroffenen Person geltend gemachte immaterielle Schaden keine Bagatellgrenze überschreiten beziehungsweise keinen besonderen Schweregrad aufweisen muss, um ersatzfähig zu sein.

15.3 Mitteilung eines Gläubigers an Arbeitgeber des Schuldners über einzuziehende Forderung

Ein Betroffener bat den Landesbeauftragten für Datenschutz und Informationsfreiheit um eine Einschätzung, ob es eine Rechtsgrundlage dafür gebe, dass ein Inkassounternehmen im Wege eines formlosen Anschreibens an seinen, des Betroffenen, Arbeitgeber herantrete, diesem das Vorhandensein einer titulierten Forderung gegen den Betroffenen mitteile und um Angabe zu pfändbaren Forderungen des Betroffenen bitte.

Oftmals, so auch hier, hängt die datenschutzrechtliche Bewertung von den Regelungen anderer Rechtsmaterien ab. Unter maßgeblicher Berücksichtigung der einschlägigen Regelungen der Zivilprozessordnung zur Forderungsvollstreckung (§§ 828 fortfolgende Zivilprozessordnung [ZPO]) kam der Landesbeauftragte für Datenschutz und Informationsfreiheit vorliegend zu dem Ergebnis, dass eine derartige Mitteilung datenschutzrechtlich nicht zu beanstanden sein dürfte.

Rechtsgrundlage für die Offenlegung der Existenz einer titulierten Forderung gegenüber dem Arbeitgeber des Betroffenen kann nur Artikel 6 Absatz 1 Buchstabe f) Datenschutzgrundverordnung sein. Es bedarf also einer Abwägung des berechtigten Interesses des im Auftrag des

Titelgläubigers handelnden Inkassounternehmens einerseits und des schutzwürdigen Interesses des betroffenen Titelschuldners andererseits.

Das berechtigte Interesse der verantwortlichen Stelle, also des Inkassounternehmens, besteht hier in der Durchsetzung einer gerichtlich festgestellten zivilrechtlichen Forderung des Inkasso-Auftraggebers und Titelgläubigers. Dem steht das Interesse des Betroffenen und Titelschuldners, etwa Gründe des Ansehens, gegenüber, dass der Arbeitgeber von Schulden des Arbeitnehmers nichts von den titulierten Forderungen erfährt.

In die Interessensabwägung spielen nun die zivilprozessualen Wertungen hinein. Im Rahmen einer zwangsweisen Durchsetzung einer titulierten Forderung im Wege der Forderungspfändung (Vollstreckung in Forderungen, vergleiche §§ 828 fortfolgende ZPO) wäre es grundsätzlich zulässig und gegebenenfalls auch notwendig, etwaige sogenannte Drittschuldner zu kontaktieren. Als Drittschuldner bezeichnet man in diesem Kontext Personen oder Stellen, gegen die der Titelschuldner wiederum selbst eine Geldforderung hat. Hier ist das zum Beispiel die Lohnforderung des Arbeitnehmers gegen den Arbeitgeber. Der Titelgläubiger hätte insoweit nach § 845 ZPO im Rahmen einer sogenannten Vorpfändung die Möglichkeit, durch den Gerichtsvollzieher einem Drittschuldner – hier also dem Arbeitgeber – und dem Titelschuldner selbst die Benachrichtigung zustellen zu lassen, dass eine Forderungspfändung bevorstehe. Der Drittschuldner erführe dann also aufgrund dieser Benachrichtigung im Rahmen der Vorpfändung von einer Forderung eines Titelgläubigers gegen den Titelschuldner.

Da die Vorpfändung ein Zahlungsverbot für den Drittschuldner gegenüber dem Titelschuldner im Umfang der bevorstehenden Pfändung begründet, muss der Drittschuldner nicht nur über die Existenz einer Forderung, sondern auch über deren Höhe in Kenntnis gesetzt werden. Denn wüsste der Drittschuldner, hier also der Arbeitgeber, nicht, in welcher Höhe die Arbeitslohnforderung seines Arbeitnehmers, des Titelschuldners, gepfändet wäre, vergleiche zur Lohnpfändung § 832 ZPO, könnte er nicht beurteilen, inwieweit er über den von Pfändung gesetzlich freigestellten Arbeitseinkommensteil hinaus überhaupt noch eine Lohnzahlung an den Arbeitnehmer und Titelschuldner vornehmen dürfte. Zudem könnte der Titelgläubiger ohnehin im Rahmen einer sogenannten Drittschuldnererklärung (§ 840 ZPO) umfangreiche Auskünfte des Drittschuldners verlangen, hier also des den Arbeitslohn zahlenden Arbeitgebers, was dann immanent Kenntnis des Drittschuldners von der Titelforderung voraussetzt.

Die Position des Titelschuldners – im vorliegenden Fall also des Arbeitnehmers – verschlechtert sich also durch das informelle Schreiben des im Auftrag des Titelgläubigers handelnden Inkassounternehmens an den Arbeitgeber im Vergleich zu einer förmlichen Forderungsvollstreckung unter Einsatz eines Gerichtsvollziehers nicht. Vielmehr dürfte die Stigmatisierungswirkung im Falle des Tätigwerdens eines Gerichtsvollziehers eher weitergehen, als dies bei einem formlosen Anschreiben zur Klärung von pfändbaren Forderungen der Fall ist. Zudem

würde eine Zustellung über den Gerichtsvollzieher dem Titelschuldner weitere, vermeidbare Kosten verursachen.

Ein Überwiegen des schutzwürdigen Interesses des Betroffenen sah der Landesbeauftragte für Datenschutz und Informationsfreiheit daher nicht.

15.4 Anwesenheitsliste einer Vereinsmitgliederversammlung als Protokollanhang

Im Berichtszeitraum erhielt der Landesbeauftragte für Datenschutz und Informationsfreiheit einen Hinweis darauf, dass der Vorstand eines Vereins im Zusammenhang mit einer Mitgliederversammlung auch eine Liste der Mitglieder des Vereins veröffentlicht habe, obwohl dies von einem oder mehreren Mitgliedern nicht gewünscht gewesen sei.

Um den Sachverhalt aufzuklären, wandte sich der Landesbeauftragte für Datenschutz und Informationsfreiheit an den Vorstand des Vereins. Bei dieser Rücksprache stellte sich heraus, dass nicht eine Mitgliederliste veröffentlicht worden war, sondern dass dem an die Vereinsmitglieder versandten Protokoll der Versammlung eine Anwesenheitsliste beigefügt gewesen war. Darin waren die bei der Versammlung anwesenden Vereinsmitglieder mit Vor- und Nachnamen aufgeführt.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hatte in Bezug auf die mitversandte Anwesenheitsliste keine grundlegenden datenschutzrechtlichen Bedenken, unabhängig von der diskussionswürdigen, hier aber unerheblichen Frage, ob man die Rechtsgrundlage dieser Offenlegung der Mitgliedschaft wie auch Versammlungsanwesenheit in Artikel 6 Absatz 1 Buchstabe b) Datenschutzgrundverordnung (DSGVO) sieht oder nur Artikel 6 Absatz 1 Buchstabe f) DSGVO als einschlägig erachtet und insoweit grundsätzlich – vorbehaltlich besonderer persönlicher Situationen eines einzelnen Vereinsmitglieds – kein überwiegendes schutzwürdiges Interesse des betroffenen Vereinsmitglieds erkennt.

Grundsätzlich gilt nämlich nach gefestigter Rechtsprechung, dass aus dem Mitgliedschaftsrecht ein Anspruch eines jeden Vereinsmitglieds auf Kenntnis des Namens und gegebenenfalls von Kontaktdaten der „Co-Mitglieder" folgt, soweit diese Daten zur Wahrnehmung von Mitgliedschaftsrechten benötigt werden und nicht ganz ausnahmsweise überwiegende Gegeninteressen des Vereins beziehungsweise des einzelnen Mitgliedes an einer Geheimhaltung erkennbar sind – zum Beispiel bei einem Selbsthilfeverein von anonym bleiben wollenden Suchterkrankten denkbar –, was vorliegend nicht zu erkennen war. Jede Person geht bei einem Vereinsbeitritt wissentlich und willentlich eine Verbindung zu den anderen Vereinsmitgliedern ein und kann daher im Regelfall nicht mit einem Anonymbleiben rechnen.

Soweit nun als Anhang des gesetzlich vorgesehenen Protokolls einer Vereinsmitglieder-Versammlung (vergleiche §§ 31 fortfolgende Bürgerliches Gesetzbuch [BGB]) eine auf den Nach- und Vornamen beschränkte Anwesenheitsliste beigefügt war, ermöglichte diese – auch für an einer Versammlungsteilnahme verhinderte Mitglieder – eine Kontrolle der Ordnungsgemäßheit von etwaigen Beschlüssen der Mitgliederversammlung (Quoren, Stimmrechtsausschlüsse; vergleiche § 32 BGB bis § 34 BGB) und eben auch eine Nachkontrolle gegenüber dem Vorstand zur tatsächlichen Anwesenheit von Mitgliedern. Über den Vornamen werden Verwechslungen bei Namensgleichheiten ausgeschlossen. Das Vorgehen des Vereins war daher zulässig.

15.5 Allgemeines zu Versicherungswirtschaft

Im Bereich der Versicherungswirtschaft erreichte den Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtszeitraum eine Meldung nach Artikel 33 Datenschutzgrundverordnung zu einer möglichen Datenschutzverletzung einer Verantwortlichen.

Bei der Meldung handelte es sich um einen Sachverhalt, der lediglich vorsorglich bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet wurde, bei dem sich letztendlich nach Abschluss der forensischen Untersuchungen aber herausgestellt hat, dass keine Verletzung des Schutzes personenbezogener Daten im Sinne der Datenschutzgrundverordnung vorlag, sodass dieser Vorfall eigentlich nicht meldepflichtig gewesen wäre. Daneben erreichten den Landesbeauftragten für Datenschutz und Informationsfreiheit insgesamt sieben Beschwerden von Bürgerinnen und Bürgern. Dies ist ein deutlicher Anstieg im Vergleich zu den Vorjahren.

15.6 Mindestanforderungen an das Beschwerdevorbringen Betroffener

Immer wieder wenden sich Personen an den Landesbeauftragten für Datenschutz und Informationsfreiheit und werfen einer datenverarbeitenden Stelle pauschal Datenschutzrechtsverstöße vor, ohne aber nähere Angaben zu dem aus ihrer Sicht gegebenen Datenschutzrechtsverstoß zu machen.

Zwar gibt es nach der Datenschutzgrundverordnung keine Formvorgaben für ein Beschwerdevorbringen, schon um eine wirksame Wahrnehmung durch Jedermann zu ermöglichen. Inhaltlich bedarf es jedoch zur Prüfbarkeit des Vorwurfes hinreichender Angaben in Form nachvollziehbarer, ausreichender Tatsachendarlegungen. Denn allein auf den pauschalen Vorwurf „Datenschutzrechtsverstoß“ hin kann der Landesbeauftragte für Datenschutz und Informationsfreiheit in der Regel noch keine Ermittlungen gegen einen Verantwortlichen quasi ins Blaue hinein aufnehmen. Damit der Landesbeauftragte für Datenschutz und Informations-

freiheit also ein Vorbringen als Beschwerde bearbeiten kann, muss sich dem Beschwerdevorbringen zumindest entnehmen lassen, wer die betroffene Person ist, die sich beschwert, welcher datenverarbeitenden Stelle ein Rechtsverstoß zur Last gelegt wird, der durch den Landesbeauftragten für Datenschutz und Informationsfreiheit nach dem erkennbaren Willen der beschwerdeführenden Person überprüft werden soll, und wenigstens ansatzweise, welcher tatsächliche Verarbeitungsvorgang in Bezug auf ihre personenbezogenen Angaben zu einer Datenschutzrechtsverletzung geführt haben soll beziehungsweise noch führen wird.

16. Internationales und Europa

16.1 Neue Beschwerdemöglichkeiten bei internationalen Datenschutzverstößen

Am 10. Juli 2023 hat die Europäische Kommission den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework verabschiedet. Dies hat zur Folge, dass personenbezogene Daten aus der Europäischen Union (EU) wieder an die Vereinigten Staaten von Amerika (USA) übermittelt werden dürfen, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind. Der Landesbeauftragte für Datenschutz und Informationsfreiheit hofft, dass die erzielten Fortschritte in Bezug auf die Verwirklichung des Schutzes personenbezogener Daten erhalten bleiben.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 4. September 2023 Anwendungshinweise zum Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework vom 10. Juli 2023 veröffentlicht und dazu eine Pressemitteilung herausgegeben. Diese Hinweise richten sich an Verantwortliche, die personenbezogene Daten an die USA übermitteln, und an betroffene Personen, die sich über ihre Rechtsschutzmöglichkeiten informieren möchten.

Ein Bestandteil des Angemessenheitsbeschlusses ist ein neuer Beschwerdemechanismus bei möglichen Verstößen gegen den EU-U.S. Data Privacy Framework durch zertifizierte U.S.-Unternehmen / U.S.-Organisationen.

Wenn eine Beschwerdeführerin beziehungsweise ein Beschwerdeführer somit der Meinung ist, dass ein unter dem EU-U.S. Data Privacy Framework zertifiziertes U.S.-Unternehmen, an welches personenbezogene Daten von ihr oder ihm übermittelt worden seien, gegen seine Pflichten aus dem EU-U.S. Data Privacy Framework verstoßen habe oder die Rechte, die ihr oder ihm nach dem EU-U.S. Data Privacy Framework zustünden, verletzt habe, kann die Beschwerdeführerin beziehungsweise der Beschwerdeführer sich mit einer Beschwerde direkt an den Landesbeauftragten für Datenschutz und Informationsfreiheit wenden. Der Europäische Datenschutzausschuss hat dafür ein Beschwerdeformular entwickelt. Dieses Formular ist auf der Internetseite des Landesbeauftragten für Datenschutz und Informationsfreiheit veröffentlicht.[5]

[5] https://www.datenschutz.bremen.de/sixcms/media.php/13/EU-US%20DPF%20Beschwerdeformular%20gewerbliche%20Angelegenheiten.pdf.

Je nach Sachlage kann es erforderlich sein, dass der Landesbeauftragte für Datenschutz und Informationsfreiheit die Beschwerde an das „Informelle Gremium der EU-Datenschutzbehörden“ oder an U.S.-Unternehmen beziehungsweise U.S.-Organisationen oder die zuständigen U.S.-Behörden weiterleitet. Die Arbeitsweise des Gremiums ist in einer Geschäftsordnung beschrieben, welche ebenfalls auf der Internetseite des Landesbeauftragten für Datenschutz und Informationsfreiheit zu finden ist.[6]

Es gibt darüber hinaus eine weitere Möglichkeit der Beschwerde mit Blick auf von der Beschwerdeführerin beziehungsweise von dem Beschwerdeführer angenommene Zugriffe auf ihre beziehungsweise seine personenbezogenen Daten für Zwecke der nationalen Sicherheit durch U.S.-amerikanische Geheimdienste oder Sicherheitsbehörden. Dieses Beschwerdeverfahren beruht auf U.S.-amerikanischem Recht und ist daher für Fälle gedacht, in denen eine Person annimmt oder es für möglich hält, dass die U.S.-Nachrichtendienste bei einem etwaigen Zugriff auf ihre Daten für Zwecke der nationalen Sicherheit gegen die hierfür geltenden Vorgaben des U.S.-amerikanischen Rechts verstoßen habe.

Zur Vereinfachung des Verfahrens für Personen in der Europäischen Union nehmen alle Datenschutzbehörden der EU-Mitgliedstaaten diese Beschwerden entgegen und leiten diese anschließend über das Sekretariat des Europäischen Datenschutzausschusses an die zuständigen Stellen in den Vereinigten Staaten weiter. Dort werden die Beschwerden geprüft und entschieden. Zu dieser Beschwerdemöglichkeit gibt es ebenfalls ein vom Europäischen Datenschutzausschuss entwickeltes Beschwerdeformular auf der Internetseite des Landebeauftragten für Datenschutz und Informationsfreiheit.[7]

16.2 Europäisches Binnenmarkt-Informationssystem

Da den Landesbeauftragten für Datenschutz und Informationsfreiheit auch Beschwerden erreichen, die sich auf Verantwortliche beziehen, die ihren Sitz in anderen europäischen Ländern haben, muss er nach Artikel 56 fortfolgende Datenschutzgrundverordnung (DSGVO) mit den jeweils für diese verantwortliche Stelle federführenden europäischen Aufsichtsbehörden zusammenarbeiten. Diese Zusammenarbeit wird durch das Binnenmarkt-Informationssystem (Internal Market Information System, IMI), das von der Europäischen Kommission entwickelt worden ist, ermöglicht und vereinfacht. Das Binnenmarkt-Informationssystem dient einer präzisen Zuständigkeitsverteilung zwischen den jeweiligen betroffenen europäischen Behörden.

[6] https://www.datenschutz.bremen.de/sixcms/media.php/13/EU-US%20DPF%20Gesch%C3%A4ftsordnung%20Informelles%20Gremium%20der%20EU-Datenschutzbeh%C3%B6rden.pdf.
[7] https://www.datenschutz.bremen.de/sixcms/media.php/13/EU-US%20DPF%20Beschwerdeformular%20Nachrichtendienste.pdf.

Die Anzahl der zu sichtenden und zu bewertenden E-Mails, die durch das europäische Binnenmarkt-Informationssystem versandt wurden, ist 2024 im Vergleich zum Vorjahr leicht angestiegen. Für Verfahren nach den Artikeln 56, 60, 61, 62, 64, 65 und 66 DSGVO gingen mehr als 3.000 Benachrichtigungen bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit ein. Ein Großteil der Nachrichten betraf die Prüfung der Zuständigkeit. Es gab allerdings auch diverse Beschlussmitteilungen der europäischen Aufsichtsbehörden und Benachrichtigungen bezüglich der eigenen Verfahren des bremischen Landesbeauftragten für Datenschutz und Informationsfreiheit.

17. Die Beschlüsse des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss ist die Organisationsform, in der die datenschutzrechtlichen Aufsichtsbehörden in Europa gemeinsam handeln. Hierzu beschließt der Europäische Datenschutzausschuss (EDSA) unter anderem Leitlinien, Empfehlungen und bewährte Verfahren zur Datenschutzgrundverordnung[8] und trifft verbindliche Beschlüsse in Einzelfällen.

Im Zusammenhang mit der am 12. Juli 2024 verkündeten Verordnung über künstliche Intelligenz beschloss der Europäische Datenschutzausschuss auf seiner Plenartagung am 16. Juli 2024 eine Erklärung zur Rolle der Datenschutzbehörden im Rahmen des Gesetzes über künstliche Intelligenz (KI-Gesetz). In dieser hob der Europäische Datenschutzausschuss insbesondere hervor, dass es sachgerecht sei, wenn die Datenschutzbehörden zumindest in einer Reihe von Fällen als Marktaufsichtsbehörde benannt würden. Dies gelte vor allem für die sogenannten Hochrisiko-KI-Systeme, soweit sich die Zuständigkeit der Datenschutzbehörden als Marktaufsichtsbehörden nicht bereits aus der Verordnung über künstliche Intelligenz ergebe. Denn die Datenschutzbehörden verfügten bereits über Fachwissen und Erfahrung im Bereich der künstlichen Intelligenz.

[8] https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de.

18. Die Entschließungen der Datenschutzkonferenzen im Jahr 2024

18.1 Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 15. Mai 2024)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert sowohl alle relevanten Stakeholder – insbesondere Leitungen, Träger und Interessenvertretungen der Krankenhäuser – als auch die verantwortlichen Akteure in Politik und Verwaltung sowie die Gesetzgeber des Bundes und der Länder dazu auf, sich frühzeitig mit den datenschutzrechtlich relevanten Auswirkungen der für die Zukunft zu befürchtenden weiteren Krankenhausschließungen zu befassen.

In den vergangenen Monaten hat die Zahl an Schließungen und Insolvenzen von Krankenhäusern bundesweit stark zugenommen. Die Datenschutzkonferenz nimmt dies insbesondere im Hinblick auf die in den Einrichtungen vorgehaltenen besonders schutzbedürftigen Behandlungsdokumentationen der Patientinnen und Patienten mit Sorge zur Kenntnis. Wiederholt wurden die Datenschutzaufsichtsbehörden mit Fällen konfrontiert, in denen eine sichere Aufbewahrung und der Zugang der Betroffenen zu den Patientendaten nicht gewährleistet waren. Teilweise bestand sogar die Gefahr, dass sich Unbefugte Zugang zu den Krankenakten verschaffen konnten.

Die Datenschutzkonferenz weist in diesem Zusammenhang auf Folgendes hin:

Datenschutzrelevante Herausforderungen für Klinikbetreiber und Insolvenzverwalter im Zusammenhang mit Krankenhausschließungen

Die Erfahrungen der Aufsichtsbehörden zeigen, dass mangels Insolvenzmasse die Kosten zur weiteren Aufbewahrung der Patientenakten häufig ab einem gewissen Zeitpunkt nicht mehr durch den Insolvenzverwalter getragen werden können. Hat die Suche nach anderen rechtlich Verantwortlichen keinen Erfolg, gibt es im Bereich der Krankenhausbehandlung keine bundes- oder landesgesetzlichen Festlegungen, durch wen und in welcher Form die weitere Aufbewahrung einschließlich der Löschung der Patientendaten erfolgen muss und in welcher Weise die Patientinnen und Patienten Zugang zu den sie betreffenden Behandlungsdokumentationen erhalten. Insbesondere fehlen hier vergleichbare Regelungen, wie sie sich vereinzelt in Heilberufsgesetzen der Länder finden, in denen unter bestimmten Voraussetzungen eine Notverantwortung der Heilberufskammern bei der Schließung ambulanter Arztpraxen festgelegt

wurde (zum Beispiel § 22 Absatz 2 Heilberufsgesetzes des Landes Rheinland-Pfalz, § 4 Absatz 1 Satz 4 fortfolgende Heilberufe-Kammergesetz des Landes Baden-Württemberg, § 7 Absatz 3 Sächsisches Heilberufekammergesetz).

Aus Sicht der Datenschutzkonferenz hat dieser Zustand starke nachteilige Auswirkungen auf den datenschutzrechtlich gebotenen Schutz der Gesundheitsdaten und die effektive Wahrnehmung der Betroffenenrechte der Patientinnen und Patienten:

Patientenakten enthalten Gesundheitsdaten im Sinne von Artikel 4 Nummer 15 der Datenschutzgrundverordnung (DSGVO), die eine besondere Kategorie personenbezogener Daten nach Artikel 9 DSGVO darstellen. Aufgrund ihrer Sensibilität muss ihnen ein besonderer Schutz zukommen. Dies ist derzeit im Falle der Insolvenz von Krankenhausträgern oder ungeplanter Schließungen von einzelnen Einrichtungen nur unzureichend rechtlich geregelt.

Nur sofern ein Insolvenzverfahren läuft, können Patientinnen und Patienten regelmäßig über den Insolvenzverwalter Einsicht in ihre Akte erlangen. Sobald das Insolvenzverfahren jedoch beendet ist oder mangels Masse nicht eröffnet wird, ist aufgrund fehlender Regelungen offen, durch wen und unter welchen technisch-organisatorischen Anforderungen Krankenhausakten aufzubewahren, datenschutzkonform zu löschen und wie Patientenrechte zu gewährleisten sind. Dies ist sowohl aus datenschutzrechtlicher Sicht als auch im Interesse einer im Einzelfall gebotenen medizinischen Weiterbehandlung nicht hinzunehmen. Es bedarf deshalb zeitnaher effektiver Lösungen, die den weiteren Umgang sowohl mit papiergebundenen als auch mit elektronisch geführten Patientenakten im Falle von Klinikschließungen datenschutzkonform festlegen. Denn die datenschutzrechtlichen Vorgaben, wie sie beim fortlaufenden Krankenhausbetrieb zu beachten sind, gelten auch nach einer Betriebseinstellung fort.

Denkbare Lösungsansätze aus datenschutzrechtlicher Sicht

Die Datenschutzkonferenz hält unter anderem folgende Bausteine für geeignet, um eine datenschutzkonforme Lösung der aufgezeigten Problematik zu finden:

- In Anlehnung an bereits bestehende Regelungen in den Landeskrankenhausgesetzen von Nordrhein-Westfalen (§ 34c Absatz 1 Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen (KHGG NRW)) und Hessen (§ 12 Absatz 5 Hessisches Krankenhausgesetz) sollten die Krankenhäuser bundesweit dazu verpflichtet werden, entsprechende Konzepte zur weiteren Verwahrung der Patientenakten für den Fall der Insolvenz oder der ungeplanten Schließung anzufertigen. Diese sollten der zuständigen Fachaufsicht vorgelegt werden.

- Aufgrund der aufgezeigten Probleme im Kontext von Insolvenzen regt die Datenschutzkonferenz an, dass sich die Länder mit einer Finanzierungs-Lösung befassen, damit in

dringenden Fällen Aufbewahrungen und Sicherungen von Patientenakten für einen Übergangszeitraum weiter finanziert werden können. So sieht zum Beispiel das Krankenhausgestaltungsgesetz des Landes Nordrhein-Westfalen in § 34c Absatz 2 bis Absatz 6 KHGG NRW die Einrichtung von Patientenaktensicherungsfonds vor.

- Solange keine geeigneten landesrechtlichen Regelungen existieren, sollten die relevanten Stakeholder, insbesondere Leitungen, Träger und Interessenvertretungen der Krankenhäuser, gemeinsam datenschutzkonforme Lösungen entwickeln, um im Bedarfsfall die kurzfristige sichere Aufbewahrung von Patientenakten geschlossener Kliniken sicherzustellen. Dabei könnten auch Vertreter der Datenschutzaufsicht beratend beteiligt werden.

- Die Datenschutzkonferenz regt an, dass sich die Gesundheitsministerkonferenz bei ihrer nächsten Zusammenkunft mit der Thematik befasst und Lösungsmöglichkeiten erarbeitet. Dabei sollte eine lückenlose Regelung der Notverantwortung für Patientendaten geschlossener Krankenhäuser angestrebt werden – etwa wie dies in den Heilberufsgesetzen oder Pflegekammergesetzen einzelner Länder durch die Zuständigkeit der Kammern geschehen ist.

Die Datenschutzkonferenz appelliert nachdrücklich an die Entscheidungsträger, bestehende Regelungslücken zu schließen und im Interesse der betroffenen Patientinnen und Patienten für Rechtsklarheit und Rechtssicherheit zu sorgen.

18.2 Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. September 2024)

In seinem Urteil vom 26. Oktober 2023 (Aktenzeichen C-307/22) hat sich der Europäische Gerichtshof zum Verhältnis des Rechts auf Einsicht in die Patientenakte aus § 630g Bürgerliches Gesetzbuch (BGB) und des Rechts auf Kopie personenbezogener Daten aus Artikel 15 Absatz 3 Datenschutzgrundverordnung (DSGVO) geäußert.

Das Gericht stellte fest, dass der Patient oder die Patientin einen Anspruch auf eine unentgeltliche erste Kopie seiner oder ihrer Akte hat. Durch eine nationale Regelung wie § 630g Absatz 2 Satz 2 BGB darf dem Patienten oder der Patientin keine Kostenlast hierfür auferlegt werden. Der Verantwortliche kann jedoch für alle weiteren Kopien ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen.

Zwar kann nach den Ausführungen des Europäischen Gerichtshofes eine nationale Regelung, die vor dem Inkrafttreten der Datenschutzgrundverordnung erlassen wurde, in den Anwendungsbereich des Artikel 23 Absatz 1 Buchstabe i) DSGVO fallen und damit den Umfang der unter anderem in Artikel 15 DSGVO vorgesehenen Pflichten und Rechte einschränken. Eine solche Möglichkeit erlaubt es jedoch nicht, eine nationale Regelung zu erlassen beziehungsweise eine bestehende Regelung anzuwenden, die der betroffenen Person zum Schutz der wirtschaftlichen Interessen des Verantwortlichen die Kosten für eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung durch den Verantwortlichen sind, auferlegt.

Im Übrigen stellte der Europäische Gerichtshof fest, dass der Antrag des Patienten oder der Patientin nicht zu begründen ist. Nach Ausführungen des Europäischen Gerichtshofes kommt es nicht auf die Motivation des Antragstellers oder der Antragstellerin auf den Erhalt der Kopie an.

Die deutschen Aufsichtsbehörden weisen darauf hin, dass nach dem Urteil des Europäischen Gerichtshofes nicht nur dringender Handlungsbedarf für den Bundesgesetzgeber besteht, § 630g Absatz 2 Satz 2 BGB den Vorgaben der Datenschutzgrundverordnung anzupassen. Auch die Berufsordnungen der Heilberufskammern enthalten regelmäßig entsprechende Regelungen zur Kostenerstattung für die Herausgabe von Kopien aus der Patientenakte (vergleiche § 10 Absatz 2 am Ende Muster-Berufsordnung der Bundesärztekammer; § 12 Absatz 4 Muster-Berufsordnung der Bundeszahnärztekammer; § 11 Absatz 1 Muster-Berufsordnung der Bundespsychotherapeutenkammer), die den Vorgaben der Datenschutzgrundverordnung und der Rechtsprechung des Europäischen Gerichtshofes widersprechen.

Während der Bundesgesetzgeber eine Änderung des Bürgerlichen Gesetzbuches noch in dieser Legislaturperiode vornehmen wird, ist offen, ob und gegebenenfalls wann es auch zu den notwendigen berufsrechtlichen Anpassungen kommen wird. Im Sinne eines möglichst einheitlichen Rechtsrahmens und aus Gründen der Rechtsklarheit fordern die deutschen Aufsichtsbehörden daher die Heilberufskammern auf, die berufsrechtlichen Regelungen zeitnah an die Vorgaben aus der Datenschutzgrundverordnung anzupassen. Die bestehenden zivil- und berufsrechtlichen Regelungen, die für die Bereitstellung einer Erstkopie eine Kostenpflicht für den Patienten oder die Patientin vorsehen, sind nicht anwendbar. Bis eine Änderung der jeweiligen Berufsordnung erfolgt ist, sind die Kammermitglieder über die Entscheidung des Europäischen Gerichtshofes zum Anspruch der Patientin beziehungsweise des Patienten auf eine kostenlose Kopie der Patientenakte zu informieren und zu einem rechtskonformen Vorgehen anzuhalten

18.3 Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. September 2024)

Bereits jetzt setzen einige Behörden automatisierte biometrische Gesichtserkennungssysteme im öffentlichen Raum ein und berufen sich dabei auf unspezifische strafprozessuale Normen.[9] Hierbei werden nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) der einschlägige Rechtsrahmen und die Freiheitsrechte der Betroffenen – also potentiell aller Bürgerinnen und Bürger – nicht hinreichend beachtet. Die bestehenden Regelungen in der Strafprozessordnung bieten für biometrische Gesichtserkennung im öffentlichen Raum keine Grundlage. Aktuell gibt es zudem Bestrebungen der Politik, das Instrument der automatisierten biometrischen Gesichtserkennung in unterschiedlichen rechtlichen Zusammenhängen zu erlauben.

Eine Regelung durch den Gesetzgeber wäre hierbei nur in einem engen Rahmen mit den europäischen und nationalen Grundrechten der betroffenen Personen vereinbar.

Der Einsatz von Gesichtserkennungssystemen kann ein sehr intensiver Eingriff in die Grundrechte der betroffenen Personen sein. Die Intensität hängt insbesondere von der Art der ausgewerteten Daten, der eingesetzten Technik und dem Grad der Automatisierung ab. Von besonderer Bedeutung ist die Streubreite der Maßnahme, wie zum Beispiel beim Einsatz von Gesichtserkennungssystemen im öffentlichen Raum. Erfasst die Analyse viele Menschen und zudem solche, die dafür keinerlei Anlass gegeben haben, führt dies zu einem noch intensiveren Eingriff. Relevant sind ferner eine eventuelle Heimlichkeit der Maßnahme und das erhebliche Risiko von Fehlerkennungen. Diese können auch für unschuldige Menschen zu intensiven Folgeeingriffen, wie zum Beispiel Freiheitsentziehungen, führen.

Aus diesem Grund hat der europäische Gesetzgeber in der KI-Verordnung[10] bestimmte Anwendungen ausgeschlossen und für andere Anwendungen enge Grenzen bestimmt.

---

[9] So wurde etwa im Frühjahr 2024 bekannt, dass eine sächsische Polizeidirektion über ein Gesichtserkennungssystem verfügt, welches bereits für Ermittlungsverfahren in verschiedenen Bundesländern genutzt wurde. Als Rechtsgrundlagen wurden §§ 100h, 163f Strafprozessordnung (StPO) für die Aufzeichnung von Bildern auf öffentlichen Straßen und § 98a StPO für den Abgleich mittels automatisierter Gesichtserkennung herangezogen.

[10] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

Sofern nach der KI-Verordnung und dem Verfassungsrecht ein Regelungsspielraum für den nationalen Gesetzgeber verbleibt und er den entsprechenden Einsatz als zwingend erforderlich betrachtet, muss er spezifische, verhältnismäßige Rechtsgrundlagen für den Einsatz von Gesichtserkennungssystemen schaffen. Hierin sind in Abhängigkeit von der Eingriffsintensität hinreichende Eingriffsschwellen, ausreichende Anforderungen an den Rechtsgüterschutz und zusätzliche Schutzmechanismen festzulegen.

Zu dieser Thematik hat der Europäische Datenschutzausschuss Leitlinien erlassen. Auch nach Ansicht des Europäischen Datenschutzausschusses darf Gesichtserkennungstechnologie nur unter strikter Einhaltung des einschlägigen Rechtsrahmens und ausschließlich in solchen Fällen verwendet werden, in denen die Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit belegbar erfüllt sind.

Sofern und soweit der Gesetzgeber den entsprechenden Einsatz nach sorgfältiger Prüfung als unbedingt erforderlich betrachtet, fordert die Datenschutzkonferenz, sich mit den rechtlichen Vorgaben intensiv auseinanderzusetzen und diese zu beachten.

18.4 Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen![11]

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 19. Dezember 2024)

Die Gesetzgeber und Regierungen der Europäischen Union, des Bundes und der Länder streben einen digitalen Wandel an, in dessen Mittelpunkt der Mensch steht (siehe zum Beispiel Europäische Erklärung zu den digitalen Rechten und Grundsätzen in der digitalen Dekade; 2023/C 23/1). Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) erkennt das Potential, das der digitale Wandel in allen Lebensbereichen für Wirtschaft und Gesellschaft birgt. Sie unterstützt deswegen das Leitbild einer menschenzentrierten Digitalisierung als ein wichtiges politisches Ziel in der Europäischen Union. Seine Umsetzung und Verwirklichung durch unterschiedliche Akteure muss das Grundrecht auf informationelle Selbstbestimmung im Blick behalten und insbesondere die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten beachten. Speziell in der Daseinsvorsorge sieht die Datenschutzkonferenz daher die Notwendigkeit, diesen menschenzentrierten Ansatz zum Schutz derjenigen, die nicht digital agieren können oder wollen, gesetzlich zu flankieren.

[11] Der Bayerische Landesbeauftragte für den Datenschutz und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit haben die Entschließung abgelehnt.

Seien es zentrale Verkehrsdienstleistungen, die Energie- oder Wasserversorgung oder öffentlich geförderte kulturelle Dienstleistungen, der Trend zur Digitalisierung hält überall Einzug. Wenn für die Inanspruchnahme solcher Dienstleistungen die Nutzung elektronischer Kommunikationswege (zum Beispiel Internet), die Eröffnung eines digitalen Kontos oder die Nutzung einer Smartphone-App vorausgesetzt werden, kann das dazu führen, dass bestimmte Menschen von der Inanspruchnahme solcher Daseinsvorsorgeleistungen ausgeschlossen werden. Das betrifft all diejenigen, die aufgrund körperlicher oder geistiger Beeinträchtigung, ihres Alters (Minderjährige ebenso wie Ältere), Technikferne oder fehlender Mittel nicht in der Lage sind, die digitale Technik zu nutzen, oder die in Ausübung ihres Grundrechts auf informationelle Selbstbestimmung ihre Daten nicht preisgeben wollen. Dieser Trend ist auch eine Herausforderung für die Grundrechte auf Datenschutz und Achtung des Privatlebens aus Artikel 8 und Artikel 7 der Charta der Grundrechte der Europäischen Union (GRCh) sowie auf informationelle Selbstbestimmung gemäß Artikel 2 Absatz 1 Grundgesetz (GG) in Verbindung mit Artikel 1 Absatz 1 GG in ihrem jeweiligen Anwendungsbereich.

Vor diesem Hintergrund weist die Datenschutzkonferenz darauf hin, dass bei der Leistungserbringung gemäß Artikel 6 Absatz 1 Buchstabe b) Datenschutzgrundverordnung (DSGVO) nur die Verarbeitung der für einen Vertrag erforderlichen personenbezogenen Daten zulässig ist. Die Erforderlichkeit der Datenverarbeitung bezieht sich auf den Hauptgegenstand des Vertrags – sie muss also für die Inanspruchnahme der Leistung der Daseinsvorsorge unerlässlich sein. Außerdem ist der Grundsatz der Datenminimierung gemäß Artikel 5 Absatz 1 Buchstabe c) DSGVO zu berücksichtigen, wobei die Verarbeitung auf den für den Zweck erforderlichen Umfang zu begrenzen ist. Bei einer auf Einwilligung basierenden Datenverarbeitung ist deren Freiwilligkeit und mithin die Rechtmäßigkeit der Verarbeitung in Frage zu stellen, wenn die betroffenen Personen einer sozialen oder ökonomischen Drucksituation ausgesetzt sind, die ihnen eine „echte oder freie Wahl“ (vergleiche Erwägungsgrund 42 Satz 5 DSGVO) unmöglich machte.

Vor diesem Hintergrund macht die Datenschutzkonferenz auch auf die besondere Bedeutung der Prinzipien von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Data Protection by Design and Default) nach Artikel 25 DSGVO aufmerksam. Der Verantwortliche hat bereits bei der Planung von Digitalisierungsprojekten, aber auch bei ihrer Realisierung insbesondere geeignete Maßnahmen zur Datenminimierung zu treffen. Die Datenschutzkonferenz unterstreicht, dass solche Maßnahmen nachhaltig zur Vertrauenswürdigkeit digitaler Angebote beitragen können. Zugleich sind die in Artikel 25 DSGVO verbindlich ausgestalteten Prinzipien kein optionales Angebot der Verantwortlichen, sondern die notwendige Voraussetzung für ein datenschutzkonformes digitales Angebot der Daseinsvorsorge.

Allein mit Mitteln des Datenschutzes sind allerdings befriedigende Lösungen für die Menschen, die wegen fehlender digitaler Möglichkeiten von wichtigen Leistungen der Daseinsvorsorge ausgeschlossen sind, nicht erreichbar. Zum einen kann die rechtliche Durchsetzung des Datenschutzes in möglichen gerichtlichen Auseinandersetzungen viel Zeit in Anspruch nehmen, in denen Betroffene keine schnelle Teilhabe erhalten. Zum anderen sind auch nicht alle gesellschaftspolitischen Aspekte einer menschenzentrierten Digitalisierung an Datenschutzregelungen gebunden. Es bedarf hier vielmehr klarer gesetzlicher Leitplanken, um die menschenzentrierte Digitalisierung voranzubringen. Die Notwendigkeit solcher Maßnahmen aus Verbraucherschutzsicht hat jüngst die 20. Verbraucherschutzministerkonferenz vom 14. Juni 2024 unterstrichen (vergleiche Beschluss Nummern 25 und 27: Sicherstellung einer nicht-digitalen Kundenkommunikation und analogen Teilhabe am wirtschaftlichen Leben).

Die Datenschutzkonferenz appelliert an die Gesetzgeber von Bund und Ländern, flankierende gesetzliche Maßnahmen im Bereich der Daseinsvorsorge zu prüfen, die die Rahmenbedingungen einer fairen Teilhabe derjenigen regeln, die keinen digitalen Zugang zu unverzichtbaren Dienstleistungen der Daseinsvorsorge haben oder nicht haben wollen.

19. Zahlen und Fakten

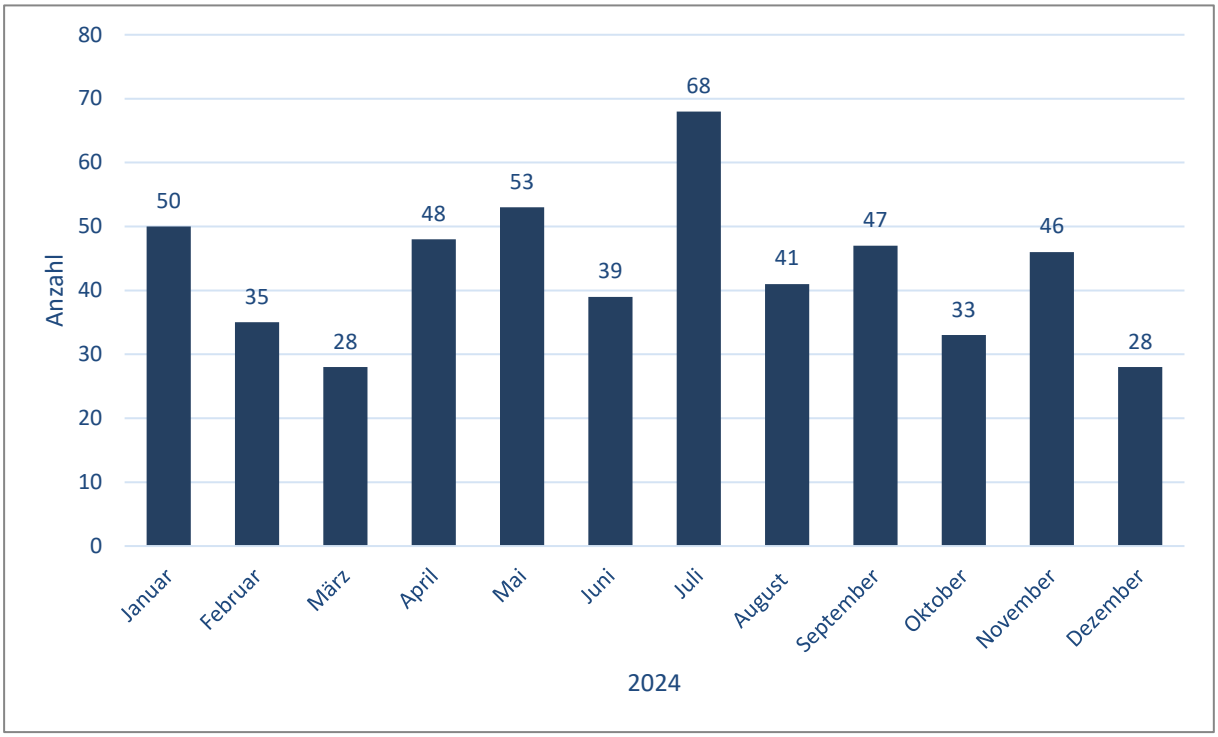
19.1 Auswahl datenschutzrelevanter Sachverhalte, die 2024 an den Landesbeauftragten für Datenschutz und Informationsfreiheit herangetragen wurden

Monat	Beschwerden	Beratungs-anfragen	Meldungen Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte
Januar	50	31	11	55
Februar	35	21	24	29
März	28	30	16	29
April	48	27	19	49
Mai	53	17	19	29
Juni	39	29	15	34
Juli	68	30	15	22
August	41	26	19	35
September	47	20	19	21
Oktober	33	25	8	13
November	46	38	21	8
Dezember	28	25	19	35
Gesamt	**516**	**319**	**205**	**359**

Tabelle 1

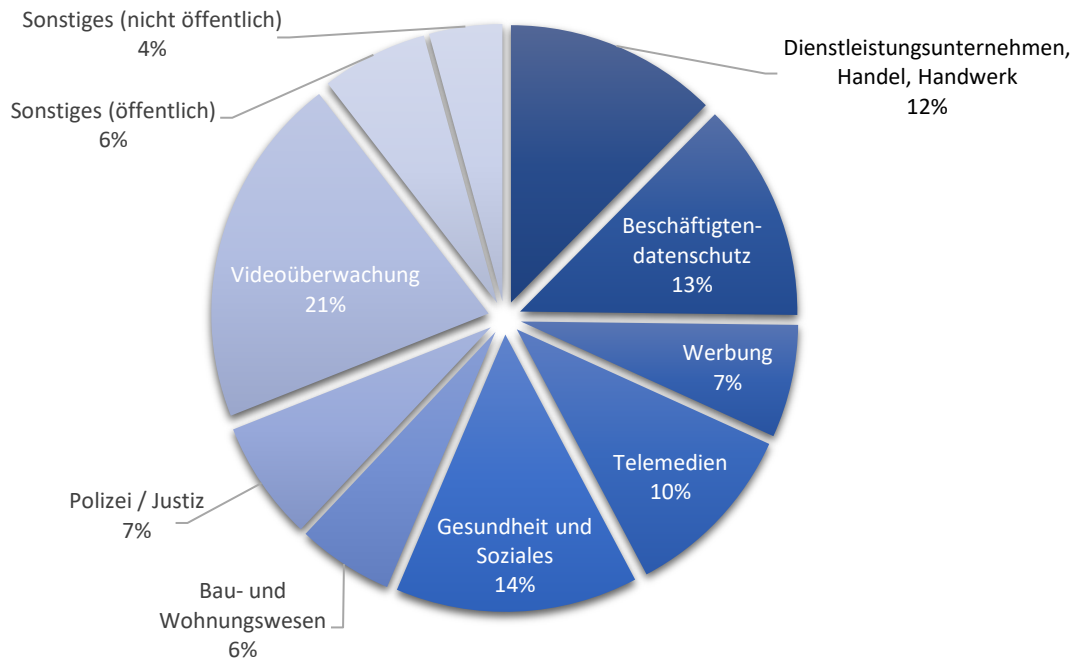
Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

19.2 Beschwerden



Säulendiagramm 1

In diesem Diagramm sind die monatlichen Beschwerdezahlen des Jahres 2024 dargestellt.



Tortendiagramm 1

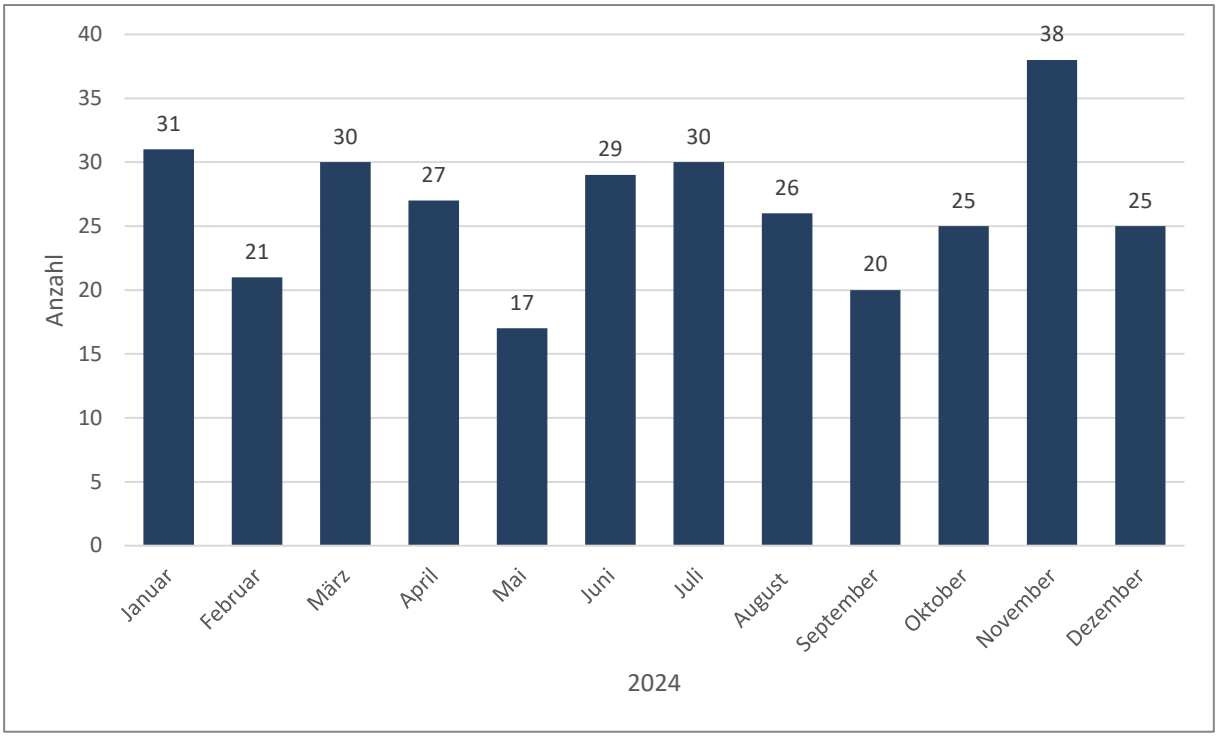
Das Diagramm zeigt die bei dem Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2024 nach Themengebieten aufgeschlüsselt.

Themengebiet	Absoluter Wert	Relativer Wert
Dienstleistungsunternehmen, Handel, Handwerk	64	12 %
Beschäftigtendatenschutz	66	13 %
Werbung	34	7 %
Telemedien	54	10 %
Gesundheit und Soziales	73	14 %
Bau- und Wohnungsunternehmen	29	6 %
Polizei / Justiz	36	7 %
Videoüberwachung	106	21 %
Sonstiges (nicht öffentlich)	22	6 %
Sonstiges (öffentlich)	32	4 %

Tabelle 2

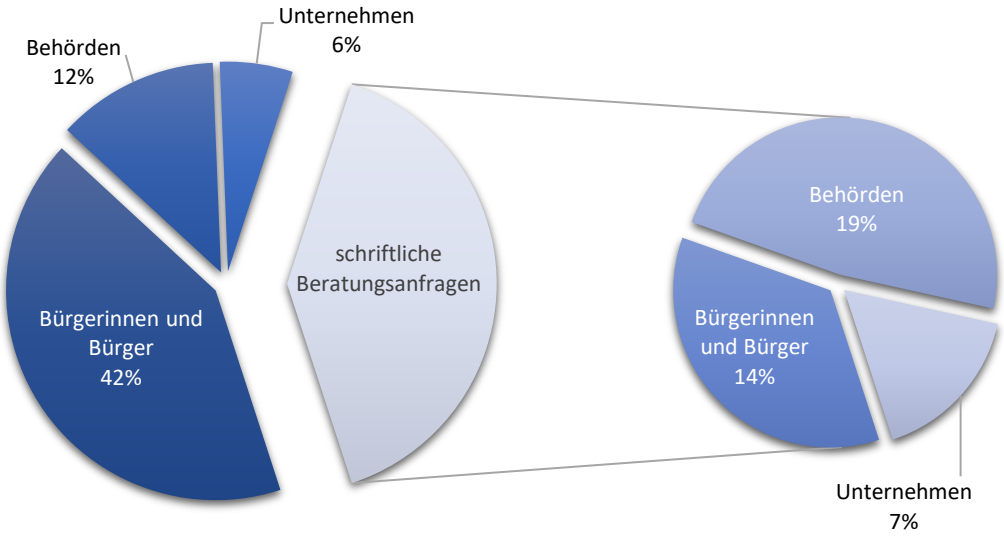
Die Tabelle stellt die absoluten und relativen Werte der unterschiedlichen Themengebiete der Beschwerden dar.

19.3 Beratungen



Säulendiagramm 2

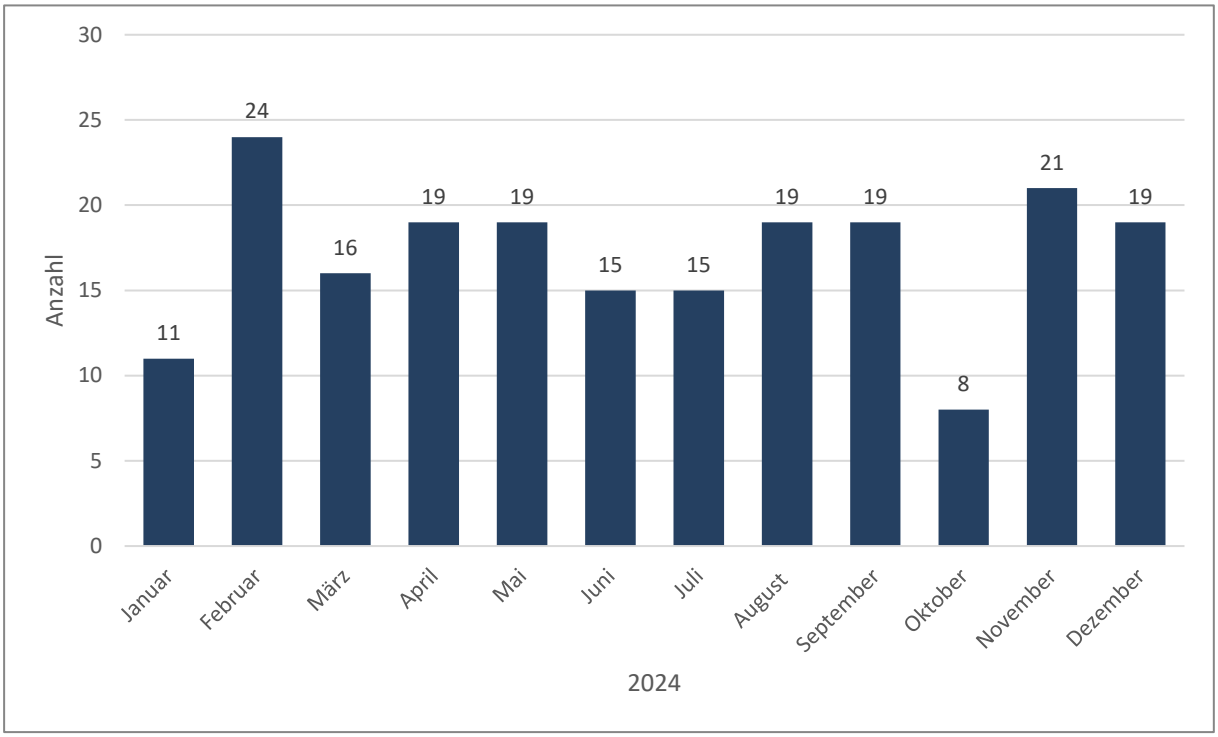
Diese Grafik gibt eine Übersicht über die Anzahl schriftlicher und telefonischer Beratungen von Verantwortlichen und betroffenen Personen.



Tortendiagramm 2

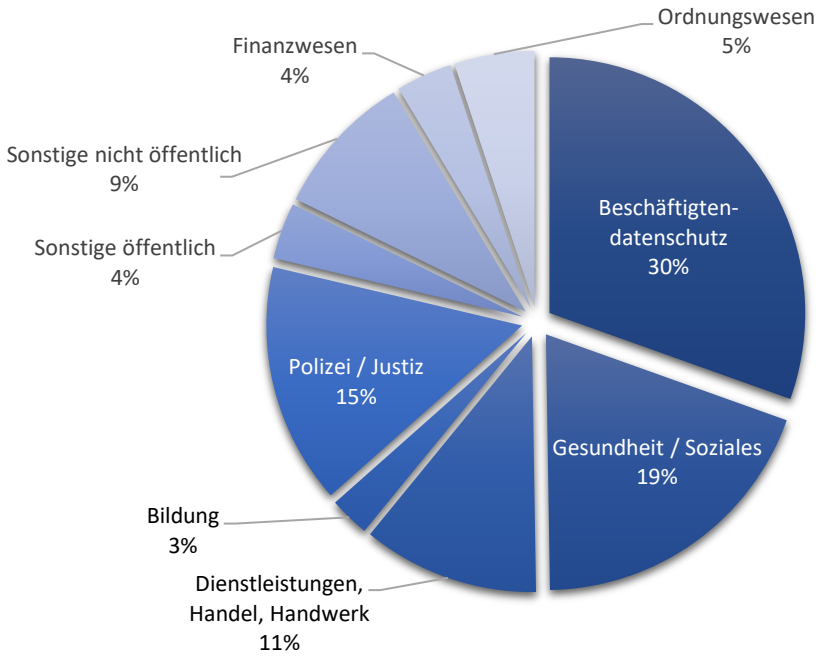
Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2024 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen. Daneben wird danach unterschieden, wer Beratungsanfragen stellt. Dies sind zu einem die Verantwortlichen (Behörden und Unternehmen) und andererseits die von der Verarbeitung personenbezogenen Daten betroffenen Grundrechtsträgerinnen und Grundrechtsträger.

19.4 Meldungen von Datenschutzverletzungen



Säulendiagramm 3

In dieser Grafik sind die monatlichen Meldungen von Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung im Jahr 2024 dargestellt.



Tortendiagramm 3

Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2024 nach Themengebieten auf.

19.5 Abhilfemaßnahmen

Warnungen

nach Artikel 58 Absatz 2 Buchstabe a) Datenschutzgrundverordnung (DSGVO): Keine

Verwarnungen

nach Artikel 58 Absatz 2 Buchstabe b) DSGVO: Sieben

Anweisungen und Anordnungen

nach Artikel 58 Absatz 2 Buchstaben c) bis g) DSGVO und § 85 BremPolG: Eine

Geldbußen

nach Artikel 58 Absatz 2 Buchstabe i) DSGVO: 73

Widerruf von Zertifizierungen

nach Artikel 58 Absatz 2 Buchstabe h) DSGVO: Keine

19.6 Europäische Verfahren nach der Datenschutzgrundverordnung

Verfahren mit Betroffenheit nach Artikel 56 DSGVO:	Sieben Fälle
Verfahren mit Federführung nach Artikel 56 DSGVO:	Kein Fall
Verfahren gemäß Kapitel VII nach den Artikeln 60 ff. DSGVO:	Ein Fall (Artikel 60)
	Drei Fälle (Artikel 61)
	Ein Fall (Artikel 64)

19.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Inneres

- Cybersicherheitsbasisgesetz
- Gesetz zur Änderung des Bremischen Polizeigesetzes (BremPolG)
- Änderung des Bremischen Hilfeleistungsgesetzes
- Bremisches Sicherheitsüberprüfungsgesetz (BremSÜG-ÄndG)

- Bremische Sicherheitsüberprüfungsgesetz-Durchführungsverordnungsverordnung (BremSÜDDVO)

- Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB)

Justiz

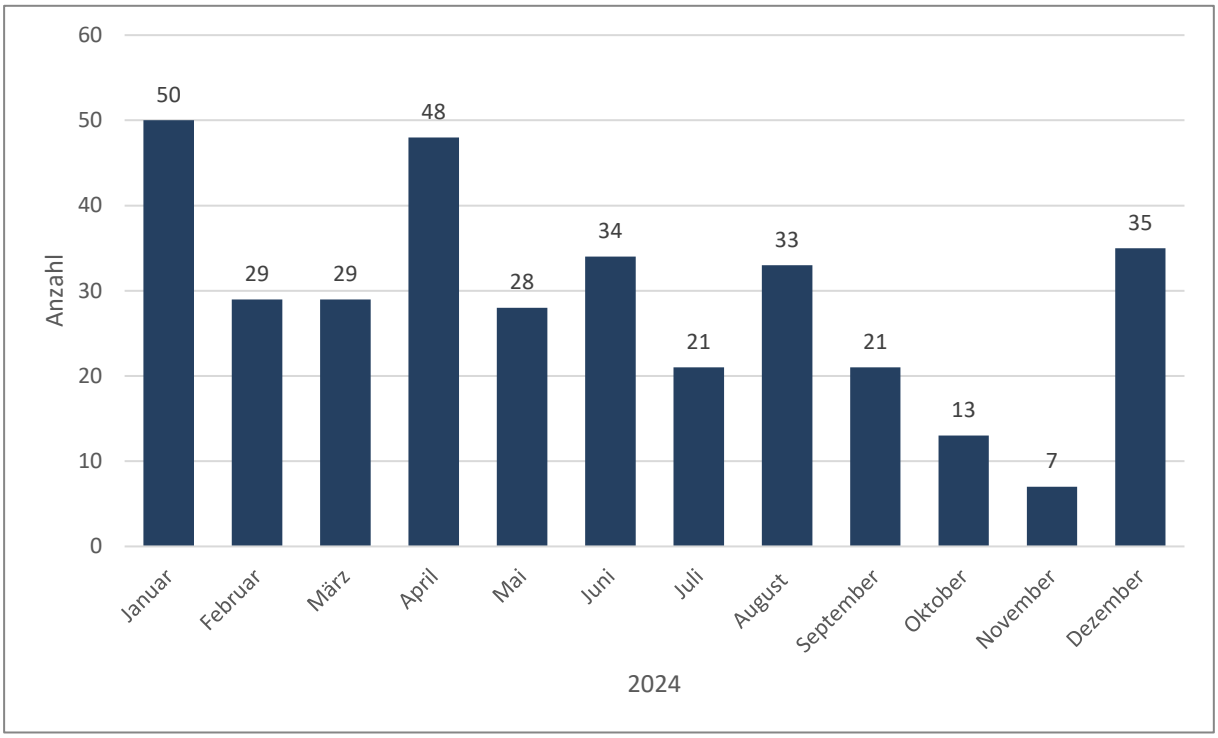
- Bremisches Gesetz über die Sicherheit in Justizgebäuden (Bremisches Justizgebäudegesetz – BremJustizGG)

- Hausverfügung zur Einhaltung des behördlichen Datenschutzes – Protokollierung lesender Zugriffe auf die Fachanwendung web.sta

Beschäftigtendatenschutz

- Verordnung zur Durchführung des Gesetzes eines Ausbildungsunterstützungsfonds im Land Bremen

19.8 Meldungen über die Bestellung behördlicher und betrieblicher Datenschutzbeauftragter



Säulendiagramm 4

Nach Artikel 37 Datenschutzgrundverordnung müssen die behördlichen und betrieblichen Datenschutzbeauftragten an die zuständige Aufsichtsbehörde gemeldet werden. Diese Grafik zeigt die Anzahl der jeweiligen Meldungen pro Monat.

19.9 Datenschutzrechtliche Zertifizierung

Im Jahr 2018 erreichte ein erster Antrag eines bremischen Unternehmens auf Akkreditierung zur datenschutzrechtlichen Zertifizierungsstelle die Landesbeauftragte für Datenschutz und Informationsfreiheit. Als zuständige Datenschutzaufsichtsbehörde prüfte der Landesbeauftragte für Datenschutz und Informationsfreiheit in Zusammenarbeit mit der Deutschen Akkreditierungsstelle GmbH das vorgelegte Konformitätsbewertungsprogramm sowie den dazugehörigen nach Artikel 42 Absatz 5 Datenschutzgrundverordnung (DSGVO) zu genehmigenden Kriterienkatalog.

Die datenschutzrechtliche Zertifizierung nach Artikel 42 und 43 DSGVO ist ein Nachweis, dass eine Organisation, ein Dienst oder ein Prozess die Anforderungen der Datenschutzgrundverordnung erfüllt. Die Zertifizierung wird von einer akkreditierten Zertifizierungsstelle ausgestellt, also einer Stelle, deren Kompetenz und Integrität zuvor von der zuständigen Datenschutzaufsichtsbehörde und der Deutschen Akkreditierungsstelle GmbH geprüft wurde. Dieses Verfahren ist anspruchsvoll und langwierig: Nachdem der Landesbeauftragte für Datenschutz und Informationsfreiheit den nationalen Kriterienkatalog des bremischen Unternehmens für grundsätzlich genehmigungsfähig gehalten hatte, begann die Prüfung des Europäischen Datenschutzausschusses.

In der ersten, sogenannten informellen Phase prüfen neben der zuständigen Datenschutzaufsichtsbehörde zwei weitere Aufsichtsbehörden die Kriterien. In diesem Fall handelte es sich dabei um die italienische Datenschutzaufsichtsbehörde Garante per la Protezione die Dati Personali und die Berliner Beauftragte für Datenschutz und Informationsfreiheit, bevor im Anschluss alle europäischen Datenschutzaufsichtsbehörden einbezogen wurden. Die entsprechenden Rückmeldungen der Aufsichtsbehörden wurden dem antragstellenden Unternehmen zur Kenntnis gegeben und mit der Möglichkeit zur Nachbesserung mitgeteilt.

Die zweite (formelle) Phase ist mit ihren Fristen in der Datenschutzgrundverordnung geregelt. Hier haben neben der Berliner Beauftragten für Datenschutz und Informationsfreiheit auch die Österreichische Datenschutzbehörde als „Co-Rapporteure“ mitgewirkt. In der zweiten Phase konnte die italienische Datenschutzaufsichtsbehörde auf Grund beschränkter Ressourcen das Prüfverfahren nicht weiter begleiten, sodass die österreichische Aufsichtsbehörde an deren Stelle trat. Nachdem der Kriterienkatalog in der Arbeitsgruppe des Europäischen Datenschutzausschusses „Compliance, E-Government and Health Expert Subgroup“ ausführlich thematisiert worden ist, wurde dieser dem Europäischen Datenschutzausschuss zur Stellungnahme

nach Artikel 64 DSGVO vorgelegt. Dieser hat in der „Opinion of the Board 26/2024“ festgestellt, dass der eingereichte Kriterienkatalog gemäß Artikel 42 DSGVO grundsätzlich genehmigungsfähig ist.

Die aufgeführten Empfehlungen des Europäischen Datenschutzausschusses wurden von dem bremischen Unternehmen implementiert. Das Verfahren befindet sich nun in der finalen Phase des Genehmigungsprozesses.