5. Jahresbericht der 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 2022. Redaktionsschluss war der 31. Dezember 2022.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Enforcement – Die DSGVO kann auch kraftvoll zubeißen

In der Physik steht der Begriff Kraft dafür, dass auf einen Körper mit der Folge eingewirkt wird, dass dieser seine Geschwindigkeit und/oder Richtung ändert oder sich verformt. Kraft steht also für Veränderung. Wie wir alle in den letzten Jahren erfahren haben, ist Veränderung ein dynamischer Prozess. Sie erfolgt manchmal abrupt und unerwartet, aber manchmal können wir sie auch steuern. Wenn der Europäische Datenschutzausschuss als das Gremium der versammelten europäischen Datenschutzaufsichtsbehörden seinen Rahmen für eine koordinierte Durchsetzung der Datenschutzgrundverordnung (DSGVO) "Coordinated Enforcement" nennt, dann zeigt dies, dass die datenschutzrechtlichen Aufsichtsbehörden in Europa sich für die fortschreitende Kraftentwicklung der DSGVO zumindest mitverantwortlich fühlen.

Wie steht es aber um die Kraft der DSGVO (und der Europäischen Datenschutzrichtlinie für den Strafverfolgungsbereich) viereinhalb Jahre nach ihrem ersten Geltungstag am 25. Mai 2018? Hat sich die Lage des Schutzes personenbezogener Daten in der Europäischen Union zum Guten geändert? Und wenn ja, welchen Beitrag hat das Enforcement der datenschutzrechtlichen Aufsichtsbehörden hierzu geleistet?

In den vergangenen Einleitungen meiner Jahresberichte zur Tätigkeit der bremischen datenschutzrechtlichen Aufsichtsbehörde finden sich Thesen dazu, wie die DSGVO wirkt und wann sie (endlich) damit anfängt: Sie wirkt stetig ansteigend (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 1.2), wo sie wirken wollte (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 1.1), selbst dort, wo sie gar nicht gilt (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 1.3) und sie verhält sich dabei wie ein Tanker, der sich erst langsam in Bewegung gesetzt, irgendwann nicht mehr zu stoppen ist, aber noch lange keine Höchstgeschwindigkeit erreicht hat (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 1.3). Das klingt nach einer langsamen, aber kontinuierlichen Entwicklung und noch nicht sehr kraftvoll. Nach Jürgen Habermas ist die "Androhung rechtsförmig definierter und vor Gericht einklagbarer Sanktionen" Hauptgeltungsquelle "gesatzten Rechts" wie der DSGVO (Faktizität und Geltung, Seite 47). Eine herausgehobene Rolle bei der Schlagkraftentwicklung der DSGVO spielen deshalb die Geldbußen, die nach Artikel 83 DSGVO immer dann im Raum stehen, wenn Verstöße gegen die DSGVO festgestellt wurden.

Insofern kann es im Land Bremen als "Enforcement-Sprung" für die DSGVO angesehen werden, dass es der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) als der personell aufgestockten datenschutzrechtlichen Aufsichtsbehörde im Land Bremen im Berichtsjahr erstmalig gelang, eine namhafte Zahl an Geldbußen nach Artikel 83 DSGVO zu

verhängen (siehe Ziffer 4. dieses Berichts). Nachdem die LfDI kapazitätsbedingt in den ersten beiden Geltungsjahren der DSGVO nur in einem und im Jahr 2021 nur in fünf Fällen Geldbußen nach Artikel 83 DSGVO verhängt hatte, erhielten verantwortliche Stellen, die personenbezogene Daten rechtswidrig verarbeitet hatten, im Jahr 2022 in 21 Fällen Geldbußebescheide. Insgesamt verhängten wir im Berichtsjahr 30 Geldbußen in Höhe von insgesamt 2.073.070 Euro, wobei sich die geringste auf 200 Euro und die höchste auf 1.435.750 Euro belief. Damit konnte die LfDI endlich den anderen europäischen Aufsichtsbehörden nachziehen.

Von der Höchstgeschwindigkeit ist der DSGVO-Tanker immer noch weit entfernt. Die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit hegt jedoch die Hoffnung, dass inzwischen zumindest zur Schrittgeschwindigkeit eine paar Knoten hinzugekommen sind.

Dr. Imke Sommer

2. Zahlen und Fakten

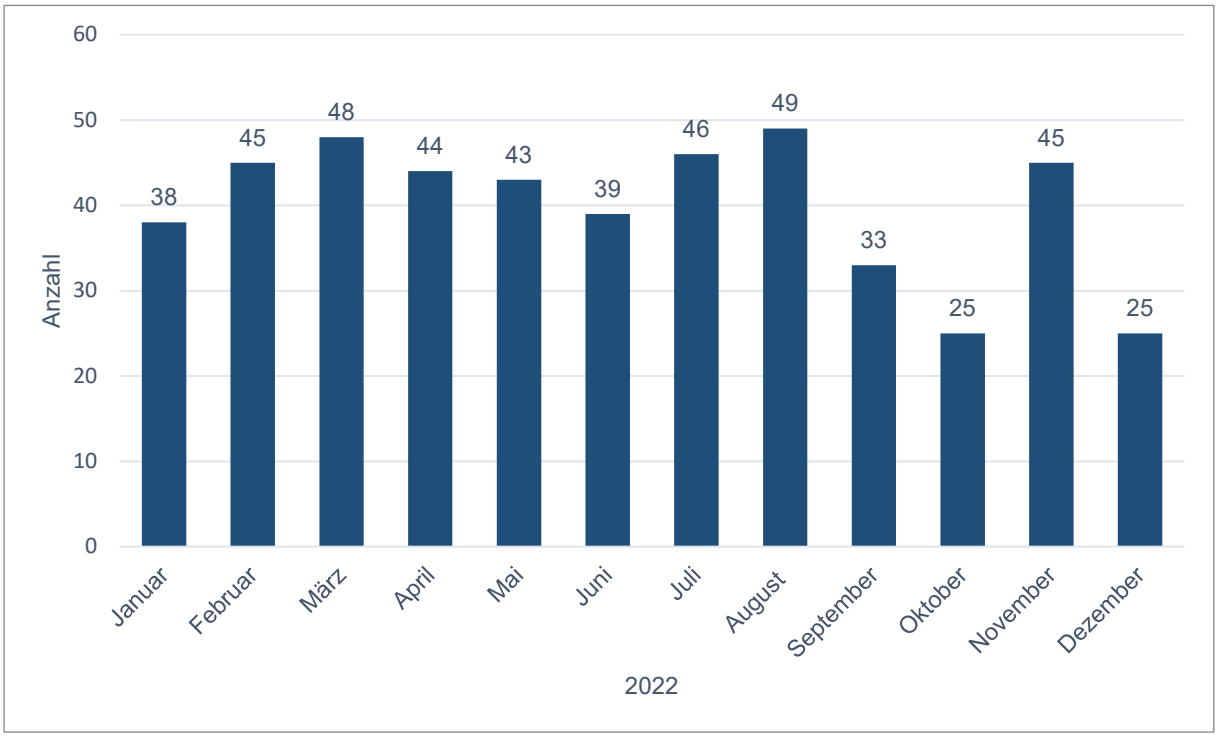
Die Datenschutzgrundverordnung macht es den Aufsichtsbehörden in Artikel 59 zur Pflicht, jährlich über ihre Tätigkeit zu berichten. Um die Transparenz und Vergleichbarkeit innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und für die Öffentlichkeit zu erhöhen, hat die DSK beschlossen, in die jeweiligen Tätigkeitsberichte ein zusätzliches Kapitel aufzunehmen, in dem nach gemeinsam vereinbarten Kriterien Informationen zu bestimmten Kennwerten der jeweiligen Aufsichtsbehörde aufgeführt sind. Die vereinbarten Kriterien sind Beschwerden (siehe Ziffer 2.2 dieses Berichts), Beratungen (siehe Ziffer 2.3 dieses Berichts), Meldungen von Datenschutzverletzungen (siehe Ziffer 2.4 dieses Berichts), Abhilfemaßnahmen (siehe Ziffer 2.5 dieses Berichts), europäische Verfahren (siehe Ziffer 2.6 dieses Berichts) und förmliche Begleitung von Rechtsetzungsvorhaben (siehe Ziffer 2.7 dieses Berichts). Zusätzlich berichten wir über Meldungen über die Bestellung behördlicher und betrieblicher Datenschutzbeauftragter (siehe Ziffer 2.8 dieses Berichts), die datenschutzrechtliche Zertifizierung (siehe Ziffer 2.9 dieses Berichts) und das europäische Binnenmarkt-Informationssystem (siehe Ziffer 2.10 dieses Berichts).

2.1 Auswahl datenschutzrelevanter Sachverhalte, die 2022 an die Landesbeauftragte für Datenschutz und Informationsfreiheit herangetragen wurden

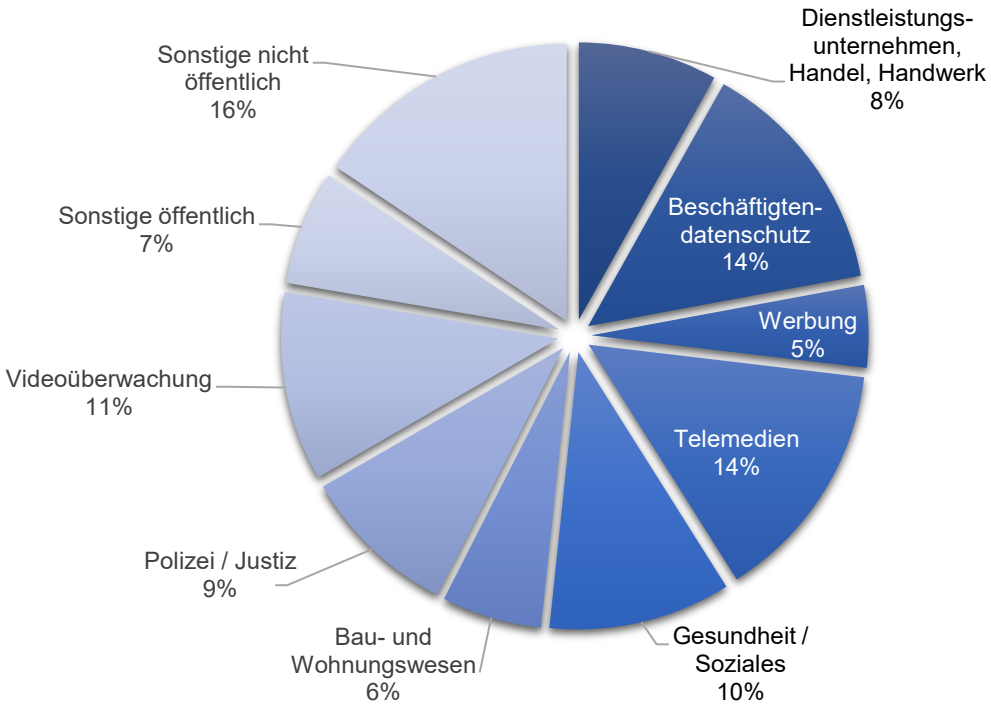
Monat	Beschwerden	Beratungs-anfragen	Meldungen Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte
Januar	38	39	10	44
Februar	45	32	9	24
März	48	44	9	22
April	44	26	20	19
Mai	43	24	10	24
Juni	39	32	13	20
Juli	46	28	10	30
August	49	27	23	25
September	33	47	12	21
Oktober	25	32	22	17
November	45	37	12	24
Dezember	25	19	12	23
Gesamt	**480**	**387**	**162**	**293**

Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

2.2 Beschwerden



In diesem Diagramm sind die monatlichen Beschwerdezahlen des Jahres 2022 dargestellt.

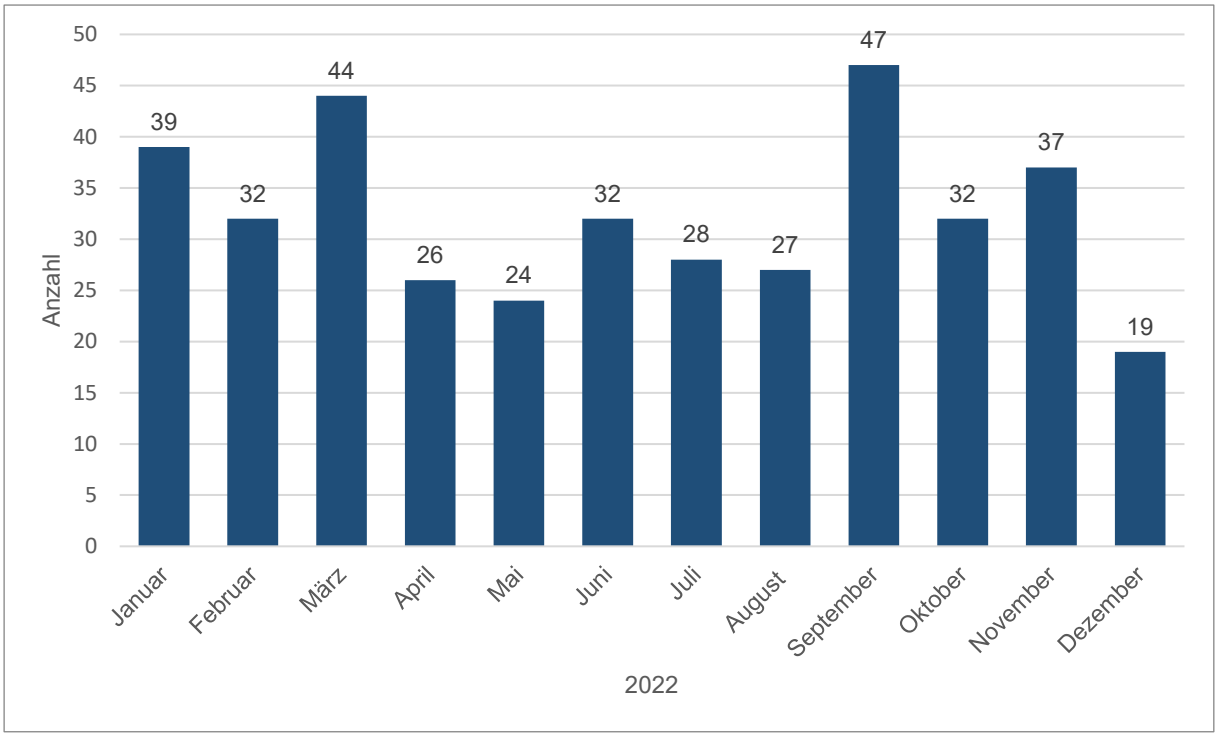


Das Diagramm zeigt die bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2022 nach Themengebieten aufgeschlüsselt.

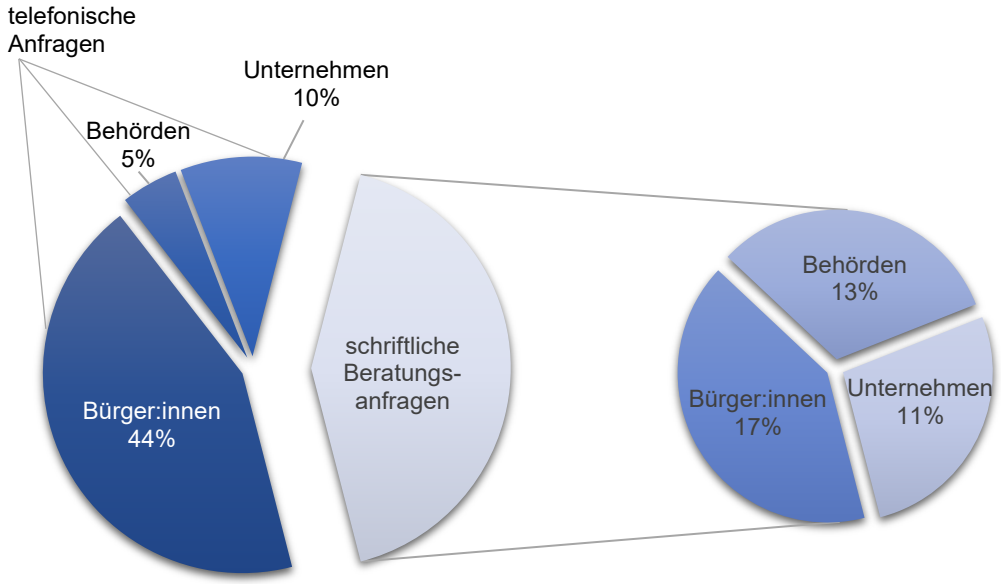
Themengebiet	Absoluter Wert	Relativer Wert
Dienstleistungsunternehmen, Handel, Handwerk	39	8 %
Beschäftigtendatenschutz	67	14 %
Werbung	23	5 %
Telemedien	68	14 %
Bau- und Wohnungsunternehmen	28	6 %
Polizei / Justiz	44	9 %
Videoüberwachung	53	11 %
Sonstiges (nicht öffentlich)	75	15 %
Sonstiges (öffentlich)	32	7 %

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

2.3 Beratungen

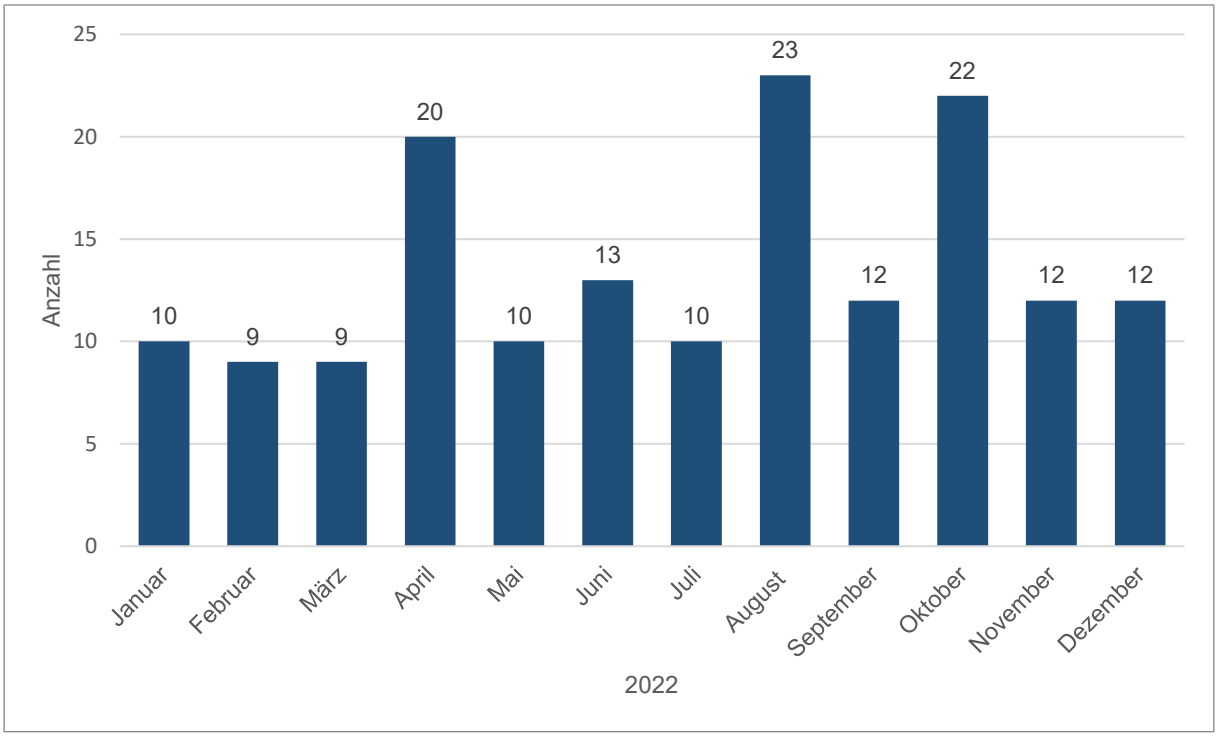


Diese Grafik gibt eine Übersicht über die Anzahl von schriftlichen und telefonischen Beratungen von Verantwortlichen und betroffenen Personen.

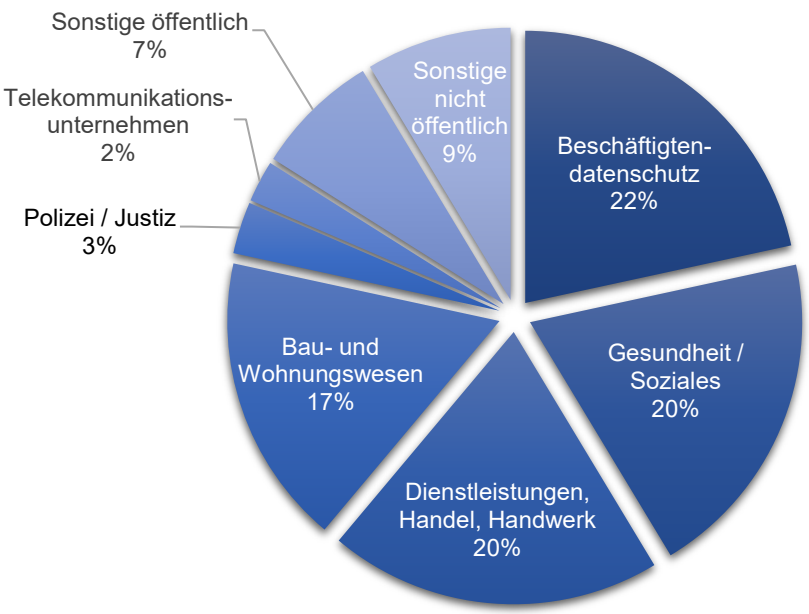


Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2022 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen. Daneben wird danach unterschieden, wer Beratungsanfragen stellt. Dies sind zum einen die Verantwortlichen (Behörden und Unternehmen) und andererseits die von der Verarbeitung personenbezogener Daten betroffenen Grundrechtsträgerinnen und Grundrechtsträger.

2.4 Meldungen von Datenschutzverletzungen



In dieser Grafik sind die monatlichen Meldungen von Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung im Jahr 2022 dargestellt.



Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2022 nach Themengebieten auf.

2.5 Abhilfemaßnahmen

Warnungen

nach Artikel 58 Absatz 2 a DSGVO: Keine

Verwarnungen

nach Artikel 58 Absatz 2 b DSGVO: 15

Anweisungen und Anordnungen

nach Artikel 58 Absatz 2 c-g DSGVO und § 85 BremPolG: Drei

Geldbußen

nach Artikel 58 Absatz 2 i DSGVO: 30

Widerruf von Zertifizierungen

nach Artikel 58 Absatz 2 h DSGVO: Keine

2.6 Europäische Verfahren

Verfahren mit Betroffenheit nach Artikel 56 DSGVO: Acht Fälle

Verfahren mit Federführung nach Artikel 56 DSGVO: Kein Fall

Verfahren gemäß Kapitel VII nach den Artikeln 60ff. DSGVO: Vier Fälle (Artikel 61)

2.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Folgende Beratungen wurden im Berichtsjahr 2022 durchgeführt:

Gesundheit

- Bremisches Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (BremPsychKG)
- Gesetz über das Krebsregister der Freien Hansestadt Bremen (Bremisches Krebsregistergesetz – BremKRG)
- Bremisches Ausführungsgesetz zum Tierische Nebenprodukte-Beseitigungsgesetz (BremAGTierNebG)

Soziales

- Bremisches Wohn- und Betreuungsgesetz (BremWoBeG)

Wissenschaft

- 6. Hochschulreformgesetz (6. HochschulRefG)

Medien und Telemedien

- Zustimmungsgesetz Dritter Medienänderungsstaatsvertrag (§ 63 Nummer 3 BremLMG)

Justiz

- Gesetz über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften in der Justiz der Freien Hansestadt Bremen (IT-Justizgesetz – ITJG)
- Bremisches Gesetz über die Juristenausbildung und die erste juristische Prüfung (JAPG)

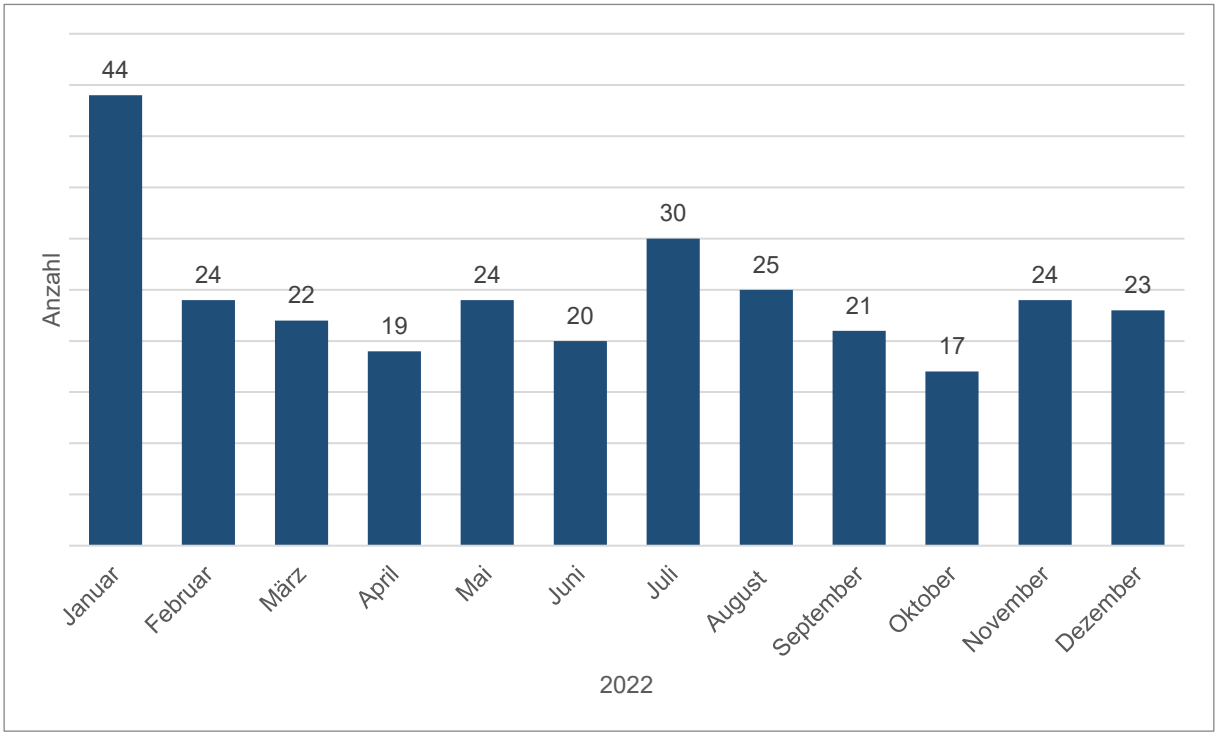
Bau und Wohnen

- Bremische Landesbauordnung (BremLBO)
- Ortsgesetz über die Begrünung von Freiflächen und Flachdachflächen in der Stadtgemeinde Bremen (Begrünungsortsgesetz Bremen – BegrünungsOG)

Verkehr, Umweltschutz und Geodaten

- Bremisches Klimaschutz- und Energiegesetz (BremKEG)
- Zweite Verordnung zur Änderung der Bremischen Landesdüngeverordnung
- Ortsgesetz zur Änderung des Entwässerungsgebührenortsgesetzes
- Verordnung über die Festsetzung eines Wasserschutzgebietes für die Trinkwasserbrunnen des Wasserwerkes Blumenthal der wesernetz Bremen GmbH in Bremen-Vegesack im Land Bremen
- Verwaltungsvereinbarung zum Staatsvertrag im Bereich des ökologischen Landbaus
- Verwaltungsvereinbarung zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen zur Durchführung des Staatsvertrages vom 1./15. Februar 2022 (Niedersächsisches Gesetz- und Verordnungsblatt Nummer 18/2022, Seite 350 und Bremisches Gesetzblatt Nummer 45/2022, Seite 230) zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen im Bereich der beiden EU-Fonds Europäischer Garantiefonds für die Landwirtschaft (EGFL) und Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) sowie nationaler Fördermaßnahmen

2.8 Meldungen über die Bestellung behördlicher und betrieblicher Datenschutzbeauftragter



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

2.9 Datenschutzrechtliche Zertifizierung

Die Förderung von datenschutzspezifischen Zertifizierungsverfahren ist eine Aufgabe der datenschutzrechtlichen Aufsichtsbehörden, die sich direkt aus Artikel 42 Datenschutzgrundverordnung (DSGVO) ergibt. Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) erhielt den Antrag eines bremischen Unternehmens, sich akkreditieren zu lassen und damit sowohl ein von der Aufsichtsbehörde genehmigtes Programm zur Sicherstellung der Zertifizierungsreife datenschutzrechtlicher Prozesse zu nutzen als auch, als Zertifizierungsstelle nach Artikel 43 DSGVO tätig werden zu können. In Zusammenarbeit mit der Deutschen Akkreditierungsstelle (DAkkS) prüfte die LfDI das ihr vorgelegte Konformitätsbewertungsprogramm sowie den dazugehörigen nach Artikel 42 Absatz 5 DSGVO zu genehmigenden Kriterienkatalog. Da wir die eingereichten Unterlagen für grundsätzlich genehmigungsfähig halten, konnte das Verfahren im Berichtsjahr auf nationaler Ebene beendet werden. Der nächste Schritt bestand darin, das Sekretariat des Europäischen Datenschutzausschusses (EDSA) zu informieren und im Rahmen der EDSA-Arbeitsgruppe Compliance, e-Government and Health Expert Subgroup (CEH Subgroup) zwei weitere

europäische Datenschutzaufsichtsbehörden als so genannte Co-Reviewer zu gewinnen, die gemeinsam mit uns die so genannte Kooperationsphase durchführen. In diesem Fall handelt es sich um die italienische Datenschutzaufsichtsbehörde Garante per la Protezione dei Dati Personali und die Berliner Beauftragte für Datenschutz und Informationsfreiheit. Sie erhielten die Gelegenheit die Unterlagen, insbesondere den Katalog der Kriterien, nach dem über die Zertifizierbarkeit entschieden werden soll, ebenfalls zu prüfen, bevor diese in der CEH Subgroup diskutiert und dem EDSA zur Stellungnahme nach Artikel 64 DSGVO vorgelegt werden.

Zusätzlich zu dem oben genannten Verfahren ist die LfDI selbst als Co-Reviewerin tätig und kommentiert gemeinsam mit der norwegischen Datenschutzaufsichtsbehörde Datatilsynet einen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen eingereichten Kriterienkatalog.

2.10 Europäisches Binnenmarkt-Informationssystem

Die Anzahl der zu sichtenden und zu bewertenden E-Mails, die durch das europäische Binnenmarkt-Informationssystem (Internal Market Information System, IMI) versandt wurden, blieb 2022 auf dem Niveau des Vorjahres. Für Verfahren nach den Artikeln 56, 60, 61, 62, 64, 65 und 66 Datenschutzgrundverordnung gingen mehr als 2.500 Benachrichtigungen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit ein. Ein Großteil der Nachrichten betraf die Prüfung der Zuständigkeit.

3. Bremische Bürgerschaft – Ergebnisse der Beratungen des 4. Jahresberichts nach Inkrafttreten der DSGVO

Der Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit (WMDI-Ausschuss) zum 4. Jahresbericht nach der Europäischen Datenschutzgrundverordnung (EU-DSGVO) der Landesbeauftragten für Datenschutz vom 18. März 2022 (Drucksache 20/1403) und zur Stellungnahme des Senats vom 27. September 2022 (Drucksache 20/1608) lag zum Redaktionsschluss noch nicht vor.

4. Geldbußen

4.1 Allgemeines

Zum Ende des Jahres 2021 hatte die zentrale Bußgeldstelle der Landesbeauftragten für Datenschutz und Informationsfreiheit ihre Arbeit aufgenommen und unbefugte Abfragen von Polizist:innen in polizeilichen Informationssystemen ins Zentrum ihrer Tätigkeit genommen (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 2.5). Im

Berichtsjahr lag der Schwerpunkt der aufsichtsbehördlichen Verfahren zur Festsetzung von Geldbußen gemäß Artikel 83 Datenschutzgrundverordnung auf festgestellten Verstößen gegen Vorschriften der Datenschutzgrundverordnung, die im Jahr 2019 stattgefunden hatten.

Im Berichtsjahr ergingen 30 Bescheide zur Verhängung von Geldbußen, welche sich sowohl gegen natürliche Personen als auch gegen Unternehmen richteten. Während bei den Verfahren gegen Unternehmen die Gegenstände der Verstöße aus verschiedenen Bereichen stammten, stand bei den Verfahren gegen natürliche Personen erneut die zweckwidrige Verwendung aus einem beruflichen Kontext stammender personenbezogener Daten für private Zwecke im Vordergrund. Insgesamt wurden Geldbußen in Höhe von 2.073.070 Euro verhängt. Von den 21 erlassenen Bescheiden wurden 19 rechtskräftig, zwei befanden sich zu Redaktionsschluss im Einspruchsverfahren und zwei Verfahren wurden eingestellt.

Im Folgenden wird über ausgewählte Verfahren zur Festsetzung von Geldbußen aus dem Jahr 2022 berichtet.

4.2 Rechtswidrige Verarbeitung von Daten über Mietinteressent:innen

Die höchste von der Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr gegen eine verantwortliche Stelle verhängte Geldbuße gemäß Artikel 83 Datenschutzgrundverordnung belief sich auf insgesamt rund 1,9 Millionen Euro. Ein Wohnungsunternehmen hatte mehr als 9.500 Daten über Mietinteressent:innen ohne Rechtsgrundlage verarbeitet. Sachbearbeiter:innen hatten in einer Datenbank ihre persönlichen Eindrücke über Mietinteressent:innen digital erfasst und dabei unter anderem Informationen über Haarfrisuren, Kleidungsstil, Körpergeruch oder das persönliche Auftreten gespeichert, deren Kenntnis für den Abschluss von Mietverträgen nicht erforderlich sind. Mehr als die Hälfte dieser Daten gehörte wie Hautfarbe, ethnische Herkunft, Religionszugehörigkeit, sexuelle Orientierung und Informationen über den Gesundheitszustand besonderen Kategorien personenbezogener Daten an, die durch die Datenschutzgrundverordnung besonders geschützt sind. Zusätzlich hatte das Wohnungsunternehmen Betroffenen bewusst Transparenz über diese Verarbeitung ihrer Daten erschwert.

Der außerordentlichen Tiefe der Verletzung des Grundrechts auf Datenschutz wäre eine deutlich höhere Geldbuße angemessen gewesen. Weil das Wohnungsunternehmen im datenschutzrechtlichen Aufsichtsverfahren umfassend kooperierte, sich um Schadensminderung, eigene Aufklärung des Sachverhalts und darum bemühte, dass entsprechende Verstöße sich nicht wiederholen, konnte die tatsächlich verhängte Höhe der Geldbuße erheblich reduziert werden.

4.3 GPS-Tracking von Beschäftigten

Gegenstand eines Verfahrens zur Festsetzung einer Geldbuße im fünfstelligen Bereich war der rechtswidrige Einsatz von GPS-Software in Dienstfahrzeugen. Bei einem Global Positioning System (GPS) handelt es sich um eine digitale Möglichkeit der Ortsbestimmung des jeweiligen Fahrzeuges. Eine Aktiengesellschaft, die Dienstfahrzeuge im täglichen Einsatz hat, hatte in diesen GPS eingesetzt und damit eine zeitlich unbeschränkte Überwachung ihrer Beschäftigten ermöglicht. Sie bediente sich einer Software, die unter anderem den Zeitpunkt des Anlassens und Abstellens des Motors jeweils verknüpft mit Ort, Standortgeodaten in Echtzeit, Fahrrouten und die Geschwindigkeit der Fahrzeuge erfasste und sechs Monate lang speicherte. Da aus diesen Daten auf die Aktivitäten und Bewegungen der in den Dienstfahrzeugen sitzenden Beschäftigten geschlossen werden konnte, handelte es sich um Beschäftigtendaten.

Das ununterbrochene GPS-Tracking der Beschäftigten verstieß gegen die Datenschutzgrundverordnung, da dieses weder für das Führen des Fahrtenbuches nach dem Steuerrecht, noch für die Einsatzkoordination, noch für die Fuhrparkverwaltung erforderlich war. Die dauerhafte Ortung zum Führen eines elektronischen Fahrtenbuches nach § 6 Absatz 1 Nummer 4 Einkommenssteuergesetz kann unter engen Voraussetzungen allenfalls in solchen Fällen erforderlich sein, in denen Firmenwagen auch für private Zwecke genutzt werden, was hier nicht der Fall war. Auch eine dauerhafte Ortung zwecks Einsatzkoordination ist nicht erforderlich, wenn der Aufenthaltsort des Firmenfahrzeuges direkt beim Beschäftigten, zum Beispiel mittels Anruf, erfragt werden kann. Auch sind die Informationen über aktuelle und vergangene Standorte der Firmenfahrzeuge für die zukunftsgerichtete Fuhrparkverwaltung planungsunerheblich.

Aufgrund der hohen Eingriffsintensität der GPS-Überwachung im Beschäftigtenbereich über einen Zeitraum von drei Jahren und der langen Speicherdauer wurde gegen das Unternehmen eine Geldbuße im unteren fünfstelligen Bereich verhängt. Zu Gunsten des Unternehmens wirkte sich aus, dass die durch GPS-Ortung erhobenen personenbezogenen Daten der Beschäftigten nicht zur Leistungskontrolle verwendet worden waren.

4.4 Offenlegungen von Beschäftigtendaten

In zwei Fällen verhängte die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) Geldbußen gegen Unternehmen in ihrer Funktion als Arbeitgeberinnen, die personenbezogene Daten ihrer Beschäftigten gegenüber Dritten ohne Rechtsgrundlage offenbart hatten.

In einem Fall versandte eine Arbeitgeberin im Rahmen der Abgabe des Vertriebsgeschäftes und der damit verbundenen betriebsbedingten Kündigungen einen ungeschwärzten Sozialplan an alle betroffenen Beschäftigten, sodass die darin enthaltenen personenbezogenen Daten wie zum Beispiel Geburtsdatum, Alter, Familienstand, Anzahl unterhaltspflichtiger Kinder, Funktion im Unternehmen, Eintrittsdatum, Beschäftigungsdauer, Elternzeit, Betriebsratszugehörigkeit und Schwerbehinderung allen Beschäftigten offenbart wurden. Die Daten der Beschäftigten, die nicht Empfänger:innen des jeweiligen Kündigungsschreibens waren, wurden vor Zustellung der Dokumente an die betroffenen Personen nicht geschwärzt. Eine Offenlegung dieser Daten bedarf wie jede andere Datenverarbeitung einer Rechtsgrundlage nach Artikel 6 Absatz 1 Datenschutzgrundverordnung (DSGVO). Hier fiel auch ins Gewicht, dass die Namensliste unter anderem auch nach Artikel 9 DSGVO besonders geschützte Daten wie zum Beispiel Schwerbehinderung enthielt. Die gegenseitige Kenntnis der offenbarten Daten unter den Beschäftigten durfte nicht vorausgesetzt werden. In diesem Fall verhängte die LfDI eine Geldbuße im unteren fünfstelligen Bereich.

Im Fall eines Unternehmens mit einem etwa dreimal höheren Jahresumsatz übermittelte die ehemalige Arbeitgeberin Gehaltsabrechnungen ihrer Beschäftigten ohne deren Einverständnis an ein anderes Unternehmen, das diese Beschäftigten in der Zukunft weiter beschäftigen sollte. Auf der Grundlage der Kenntnis der übermittelten Gehaltsdaten der Beschäftigten erstellte die neue Arbeitgeberin Arbeitsverträge, in denen die Arbeitnehmer:innen nicht entsprechend ihrer bisherigen Entgeltgruppe und Entgeltstufe übernommen werden sollten, sondern mit niedrigeren Entgelten eingestuft wurden. In diesem Fall wurde eine Geldbuße im hohen fünfstelligen Bereich verhängt. Erheblich sanktionserhöhend wirkten sich dabei gemäß Artikel 83 Absatz 2 Satz 2 Buchstabe a DSGVO die hohe zweistellige Zahl der betroffenen Beschäftigten und der ihnen entstandene Schaden aus. Durch die unrechtmäßige Weitergabe der Gehaltsdaten hatte sich ihre Verhandlungsposition in Bezug auf die neu auszuhandelnden Gehälter deutlich verschlechtert. Der Bescheid zur Verhängung der Geldbuße nach Artikel 83 DSGVO war zu Redaktionsschluss noch nicht rechtskräftig.

4.5 Datenschutzwidriger Umgang mit Bewerbungsdaten

Ein Hackerangriff auf das dienstliche E-Mail-Postfach einer Beschäftigten eines Unternehmens hatte den Abfluss der E-Mail-Adressen von Bewerber:innen ermöglicht. Da das Unternehmen eine Meldung an die Landesbeauftragte für Datenschutz und Informationsfreiheit gemäß Artikel 33 Datenschutzgrundverordnung (DSGVO) unterließ, verhängten wir eine Geldbuße. Den Hinweis auf diesen Sachverhalt hatten wir von einer betroffenen Person erhalten, die sich über die zeitlich weit nach dem Hackerangriff immer noch

erfolgenden Angriffe auf ihr E-Mail-Postfach mittels E-Mail-Adresse einer Beschäftigten des fraglichen Unternehmens beschwerte. Diese Beschwerde hatte sie zunächst beim Unternehmen erhoben. Erst auf unseren Hinweis strukturierte das Unternehmen das elektronische Bewerbungsverfahren um.

In einem anderen Fall wurde Bewerber:innen ein Online-Bewerbungsverfahren auf der Internetseite eines Unternehmens angeboten, ohne dass diese entsprechend den Vorgaben aus den Artikeln 12 und 13 DSGVO über die durch die Nutzung dieses Verfahrens ausgelösten Datenverarbeitungen informiert wurden. Bei der Höhe der von uns verhängten Geldbuße wurden die im dreistelligen Bereich liegende Zahl der betroffenen Bewerber:innen sowie der Zeitraum von einem halben Jahr maßgeblich berücksichtigt.

4.6 Datenschutzwidrige Verarbeitungen einer Personalausweiskopie

In einem weiteren Fall wurde eine Geldbuße gegen ein Medizinisches Versorgungszentrum verhängt, das den Personalausweis eines Kunden gegen dessen Willen eingescannt und die Kopie gespeichert hatte. Als dieser sich dagegen wehrte, wurde dem Kunden mit dem Abbruch der Kundenbeziehung gedroht. Der Personalausweis beinhaltet biometrische Daten, die nach Artikel 9 Absatz 1 Datenschutzgrundverordnung (DSGVO) in Verbindung mit Artikel 4 Nummer 14 DSGVO besonders schutzbedürftig sind und nur unter strengen Voraussetzungen des Artikels 9 Absatz 2 DSGVO von dem Unternehmen verarbeitet werden dürfen. Nach § 20 Absatz 2 Personalausweisgesetz darf ein Personalausweis nur von den jeweiligen Ausweisinhaber:innen oder mit ihrer ausdrücklichen Zustimmung abgelichtet werden. Bei der Zumessung der Geldbuße wurde sanktionserhöhend berücksichtigt, dass der Ausweis gegen den ausdrücklichen Widerspruch des Betroffenen eingescannt worden war.

4.7 Rechtswidrige Verarbeitung von Fotos durch Ladendetektiv

In einem Fall verhängten wir gegen ein Supermarktunternehmen eine Geldbuße nach Artikel 83 Datenschutzgrundverordnung. Ein Ladendetektiv hatte anlässlich eines vermeintlich begangenen Diebstahls in einem Lebensmittelmarkt ein Foto eines Beschwerdeführers angefertigt und dieses vorgeblich zur Durchsetzung des Hausrechts über den Messengerdienst WhatsApp übertragen. Zu den Personen, die von dem Foto Kenntnis nehmen konnten, gehörten neben dem Ladendetektiv der Geschäftsführer, der Filialleiter und zwei Schließkräfte. Später wurden dem Beschwerdeführer die Bildaufnahmen weiterer vermeintlicher Dieb:innen offenbart. Bei der Bemessung der Höhe der Geldbuße berücksichtigten wir nicht nur das rechtsgrundlose Anfertigen und weitere Verarbeiten des Fotos, sondern auch, dass das Foto über den Messengerdienst WhatsApp weitergegeben wurde. Eine über WhatsApp veranlasste Datenverarbeitung findet außerhalb der

Europäischen Union statt und gewährleistet unter anderem deshalb nicht das nach der Datenschutzgrundverordnung erforderliche Datenschutzniveau.

4.8 Zweckwidrige Verwendung von Kontaktdaten über Patient:innen

Im Berichtsjahr verhängten wir zwei Geldbußen nach Artikel 83 Datenschutzgrundverordnung wegen rechtsgrundloser Verwendung von Patient:innendaten. In einem Fall waren die Daten einer Patientin ohne ihr Einverständnis an eine Abrechnungsstelle übermittelt worden. Im anderen Fall nutzte ein Arzt die Kontaktdaten einer Patientin, um zu ihr einen privaten über das Arzt-Patient:innen-Verhältnis hinausgehenden Kontakt herzustellen.

4.9 Verstoß gegen Auskunftspflichten

Wir belegten sowohl ein Unternehmen als auch einen Arzt mit Geldbußen nach Artikel 83 Datenschutzgrundverordnung (DSGVO), weil diese ihren Auskunftspflichten gegenüber betroffenen Personen gemäß Artikel 12 Absatz 3 DSGVO nicht nachgekommen waren. Erst nachdem die betroffenen Personen bei uns als datenschutzrechtliche Aufsichtsbehörde Beschwerden erhoben hatten und wir uns daraufhin an die datenschutzrechtlich verantwortlichen Stellen gewandt hatten, waren den betroffenen Personen die beantragten Auskünfte erteilt worden.

4.10 Ausnutzung der beruflichen Stellung

In den vergangenen drei Jahren gingen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit vermehrt Beschwerden zur Problematik der Ausnutzung einer beruflichen Stellung zur Erhebung personenbezogener Daten und anschließenden Kontaktaufnahme zu den ausschließlich weiblichen betroffenen Personen ohne oder sogar gegen ihren Willen ein. Wegen der damit verbundenen Verstöße gegen Artikel 6 Absatz 1 Datenschutzgrundverordnung (DSGVO) verhängten wir in diesen Fällen Geldbußen gegen natürliche Personen. Bei der Zumessung der jeweiligen Geldbußen berücksichtigten wir jeweils die Ausnutzung der beruflichen Stellung sanktionserhöhend.

Eine Beschwerdeführerin hatte uns berichtet, dass sie nach einem Restaurantbesuch, im Zuge dessen sie nach der Corona-Verordnung dazu verpflichtet gewesen war, ihre Kontaktdaten inklusive privater Mobilfunknummer, in eine Kontaktverfolgungsliste einzutragen, am nächsten Tag von einem sie am Vortag bedienenden Kellner des Restaurants per Messenger kontaktiert worden war.

In einem anderen Fall berichtete eine Beschwerdeführerin, dass sie von einem Mitarbeiter eines Corona-Testzentrums am auf ihre Testung folgenden Tag via Instagram angeschrieben

worden war. Der betreffende Mitarbeiter hatte den Namen und Nachnamen der Betroffenen aus dem Patient:innendatensystem entnommen und die Betroffene mittels dieser Daten in dem sozialen Netzwerk Instagram ausfindig gemacht.

Beide Fälle charakterisieren sich dadurch, dass die Verantwortlichen personenbezogene Daten der Betroffenen dem ursprünglich für die Zugriffsberechtigung ursächlichen Kontext entrissen und diese zu eigennützigen Zwecken verwendeten. Die Restaurantbesucherin war aufgrund der Vorgaben der damals geltenden Corona-Verordnung zur Offenlegung ihrer Kontaktdaten verpflichtet. Auch die Patientinnen, die einen Corona-Test durchführen lassen wollten, mussten ihre personenbezogenen Daten zwecks Vertragsdurchführung mitteilen.

Die Mitarbeiter nutzen ihre berufliche Stellung als Kellner und Mitarbeiter eines Testzentrums, um an die persönlichen Daten der Beschwerdeführerinnen zu gelangen und diese für eigene Zwecke zu verwenden. Dies stellt einen so genannten Mitarbeiter:innenexzess dar, bei dem das eigennützige Handeln der Beschäftigten nicht den jeweiligen Arbeitgeber:innen zugerechnet wird. Die ihre berufliche Stellung zu privaten Zwecken ausnutzenden Beschäftigten müssen deshalb selbst als Verantwortliche im Sinne des Artikel 4 Nummer 7 DSGVO für die durch sie begangenen Datenschutzverletzungen einstehen.

5. Datenschutzbeauftragte und Allgemeines öffentliche Stellen

5.1 Benennungspflicht bei Videoüberwachungsmaßnahmen

Wiederholt waren wir mit der Frage befasst, ob ein Unternehmen, bei dem in der Regel weniger als 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst ist, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennen muss, weil es Videoüberwachungsmaßnahmen durchführt. Im Berichtsjahr handelte es sich unter anderem um einen Gastronomiebetrieb, der die für seine Gäste zugänglichen gastronomischen Bereiche mit Videokameras überwachte, und um eine Firma, die auf ihrem Betriebsgelände Aufnahmen zur Überwachung ihrer Beschäftigten machte.

Gemäß § 38 Absatz 1 Satz 2 Bundesdatenschutzgesetz in Verbindung mit Artikel 37 Absatz 4 Datenschutzgrundverordnung (DSGVO) sind unabhängig von der Anzahl der mit der Verarbeitung personenbezogener Daten beschäftigten Personen Datenschutzbeauftragte zu benennen, wenn die oder der Verantwortliche oder die Auftragsverarbeiterin beziehungsweise der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO unterliegen. Eine Abschätzung der Folgen der vorgesehenen Datenverarbeitungsvorgänge ist gemäß Artikel 35 Absatz 1 DSGVO durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der

Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Da die Daten von Beschäftigten, die im Beschäftigungskontext verarbeitet werden, als besonders schutzwürdig zu betrachten sind und eine besondere Sensibilität aufweisen, ist für deren Verarbeitung bei Vorliegen der Voraussetzungen nach Artikel 35 Absatz 1 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen, was bei einer permanenten Videoüberwachung der Fall ist. Gemäß Artikel 35 Absatz 3 Buchstabe c DSGVO ist eine Datenschutz-Folgenabschätzung insbesondere bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche erforderlich. Das ist der Fall, wenn eine unbestimmte Zahl von Gästen in Räumen der Gastronomie überwacht werden.

In den genannten Videoüberwachungsfällen hätten daher Datenschutz-Folgenabschätzungen durchgeführt und Datenschutzbeauftragte benannt werden müssen.

5.2 Benennung von Datenschutzbeauftragten durch Betreuer:innen

Wir erhielten eine Beratungsanfrage darüber, ob gesetzlich bestellte Betreuer:innen von Privatpersonen Datenschutzbeauftragte benennen müssen. Die Anfragende wies dabei darauf hin, dass Betreuer:innen im Rahmen ihrer Tätigkeit oftmals eine Vielzahl unterschiedlicher personenbezogene Daten der von ihnen betreuten Person verarbeiten, die wie zum Beispiel Steuerdaten, die Herkunft oder Gesundheitsdaten häufig eine hohe Sensibilität aufweisen.

Gemäß Artikel 37 Absatz 1 Buchstabe c Datenschutzgrundverordnung (DSGVO) müssen nicht öffentliche Verantwortliche und Auftragsverarbeiter:innen Datenschutzbeauftragte benennen, wenn ihre Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO besteht. Hierunter fallen zum Beispiel Gesundheitsdaten, Daten über die Hautfarbe, politische, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit oder zum Sexualleben oder der sexuellen Orientierung. Für die Frage, ob es sich um umfangreiche Verarbeitungen handelt, sind insbesondere die große Menge der verarbeiteten personenbezogenen Daten, die lange Dauer der Verarbeitung und die hohe Anzahl der betroffenen Personen von Bedeutung. Sind mehrere dieser Faktoren gegeben, so spricht dies für eine "umfangreiche" Verarbeitung.

Erfolgt die Verarbeitung personenbezogener Daten durch einzelne selbstständige Betreuer:innen besteht regelmäßig keine Benennungspflicht, weil es sich nicht um eine umfangreiche Datenverarbeitung handelt. Liegen die vorstehend genannten Faktoren vor, beispielsweise bei einer Anzahl von zu Betreuenden, die erheblich über den durchschnittlichen Betroffenenkreis hinausgeht, kann aber bereits eine einzelne Betreuerin beziehungsweise ein einzelner Betreuer verpflichtet sein, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Für eine Pflicht zur Benennung einer oder eines Datenschutzbeauftragten spricht es, wenn bei einem privaten Betreuungsbüro oder -verein mehrere Personen mit der Erfüllung von Betreuungsaufgaben befasst sind und das Büro oder der Verein für die personenbezogene Datenverarbeitung verantwortlich ist. Die Benennungspflicht liegt in diesem Fall beim Betreuungsbüro oder dem Betreuungsverein. Nach § 38 Absatz 1 Bundesdatenschutzgesetz müssen Datenschutzbeauftragte benannt werden, wenn in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, auch wenn die Voraussetzungen für die Pflicht zur Benennung einer beziehungsweise eines Beauftragten nach Artikel 37 Absatz 1 DSGVO nicht vorliegen. Ist die Betreuung von einer Behörde oder anderen öffentlichen Stelle wahrzunehmen, muss diese gemäß Artikel 37 Absatz 1 Buchstabe 1 Datenschutzgrundverordnung eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benennen.

5.3 Benennung von Datenschutzbeauftragten im Justizressort

Der Präsident des Landesarbeitsgerichts Bremen unterrichtete uns im Mai des Berichtsjahres darüber, dass die Verfahren zur Benennung von zentralen Datenschutzbeauftragten der Gerichte in der Justiz Bremen abgeschlossen seien. Es handele sich um zwei Datenschutzbeauftragte, die ihre Tätigkeit nunmehr aufgenommen hätten. Die Beauftragten seien bei der Wahrnehmung ihrer Funktion weisungsfrei, könnten sich unmittelbar an die Gerichtsleitungen wenden und seien bei der Aufgabenerfüllung von den Gerichten zu unterstützen.

Wir wiesen den Präsidenten des Landesarbeitsgerichts darauf hin, dass von jedem Gericht jeweils nur eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter zu benennen ist. Die Bestimmungen der Datenschutzgrundverordnung (DSGVO) lassen die Benennung weiterer Datenschutzbeauftragter durch die Verantwortliche beziehungsweise den Verantwortlichen und eine Aufteilung der Beauftragtenfunktion auf mehrere Personen nicht zu. Die sich aus der DSGVO ergebenden Aufgaben und Verantwortlichkeiten können nur rechtskonform umgesetzt werden, wenn sie lediglich an eine Person gebunden sind. Wir baten, die bislang getroffenen Regelungen an die Vorgaben der Datenschutzgrundverordnung anzupassen. Das Justizressort schloss sich unserer Auffassung an und ordnete die Datenschutzbeauftragten jeweils einzelnen Gerichten zu. Der Präsident des Landesarbeitsgerichts kündigte im Oktober an, die Präsident:innen der anderen Gerichte um ein den Anforderungen des Artikels 37 DSGVO entsprechendes Benennungsverfahren bitten zu wollen.

5.4 Anwalt eines Unternehmens gleichzeitig Datenschutzbeauftragter

Nachdem uns ein Unternehmen, das seinen Kund:innen die Durchführung von Corona-Tests anbot, gemäß Artikel 37 Absatz 7 Datenschutzgrundverordnung (DSGVO) den von ihm benannten externen Datenschutzbeauftragten gemeldet hatte, stellten wir bei einem von uns zu bearbeitenden die gleiche Firma betreffenden Beschwerdevorgang fest, dass der Datenschutzbeauftragte in diesem Vorgang auch als rechtlicher Vertreter des Unternehmens auftrat, was er mit einer entsprechenden Vollmacht belegte.

Die Tätigkeit rechtlicher Vertreter:innen eines Unternehmens ist wie die der Rechtsanwält:innen nach der Datenschutzgrundverordnung mit der Funktion der Datenschutzbeauftragten des jeweiligen Unternehmens nicht zu vereinbaren, weil sie die Datenschutzbeauftragte oder den Datenschutzbeauftragten in eine Situation bringen, die ihre oder seine ordnungsgemäße und unabhängige Aufgabenerfüllung in Frage stellen kann. Bei der Beurteilung datenschutzrechtlicher Sachverhalte im Hinblick auf die Umsetzung und Einhaltung datenschutzrechtlicher Vorgaben müssen Beauftragte in ihren Positionen und Entscheidungen frei und unabhängig von der Unternehmensleitung sein. Sofern die beziehungsweise der Datenschutzbeauftragte gleichzeitig die Position der verantwortlichen Stellen einnähme, stießen im aufsichtsrechtlichen Verfahren zwei gegensätzliche Interessen aufeinander. Auch gehört es zu den Aufgaben der Datenschutzbeauftragten nach Artikel 39 Absatz 1 Buchstabe d DSGVO, mit der Datenschutzaufsichtsbehörde im Hinblick auf die Umsetzung und Einhaltung der Verordnung in der verantwortlichen Stelle zusammen zu arbeiten. Diese Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde kann mit der rechtlichen Vertretung von Unternehmensinteressen kollidieren. Die Datenschutzbeauftragten dürfen daher in Angelegenheiten der personenbezogenen Datenverarbeitung nicht als Rechtsvertreter:innen ihrer Unternehmen tätig werden. Wir wiesen das Unternehmen auf die Rechtslage hin und verbanden dies mit der Aufforderung, den Datenschutzbeauftragten von seiner Funktion zu entbinden, sofern daran festgehalten werden solle, dass dieser das Unternehmen auch in Angelegenheiten der Verarbeitung personenbezogener Daten rechtlich vertrete. Das Unternehmen widersprach unserer Aufforderung und teilte uns mit, dass der Betreffende in seiner Eigenschaft als Datenschutzbeauftragter bei einem anderen Unternehmen beschäftigt sei als demjenigen, für das er als rechtlicher Vertreter der von der Beschwerde betroffenen Firma tätig werde. Eine Unvereinbarkeit bestehe daher nicht. An der bestehenden Situation wolle man festhalten. Nachdem wir darauf hingewiesen hatten, dass die von uns dargelegte Rechtslage unabhängig davon besteht, ob die Betreffenden in ihren unterschiedlichen Funktionen beim selben oder bei unterschiedlichen Arbeitgeber:innen angestellt sind, verzichtete das Unternehmen auf die rechtliche Vertretung durch den Datenschutzbeauftragten.

5.5 VIS-Einheitsmandant

In unserem 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 5.16 berichteten wir über das Vorhaben, den so genannten VIS-Einheitsmandanten einzuführen. Der Senator für Finanzen arbeitet unter Mitwirkung verschiedener Ressorts und des externen Datenschutzbeauftragten an der Umsetzung dieses Projekts mit dem Ziel der Verbesserung der digitalen Zusammenarbeit innerhalb der öffentlichen Verwaltung der Freien Hansestadt Bremen und der Stärkung der ressortübergreifenden Zusammenarbeit. Dabei soll das digitale Schriftgut der bremischen Verwaltung im elektronischen Dokumentenmanagementsystem (VISkompakt) in nur einem einzigen Mandanten gebündelt werden.

Wir äußerten uns im Berichtsjahr mit einer ausführlichen Stellungnahme zu den durch die Schaffung eines VIS-Einheitsmandanten aufgeworfenen komplexen datenschutzrechtlichen Problematiken, wobei das Hauptproblem vor allem in der mit dem Einheitsmandanten ermöglichten Übermittlung personenbezogener Daten zwischen den verschiedenen verantwortlichen Stellen besteht. Wir forderten, dass alle in unserer Stellungnahme aufgezeigten datenschutzrechtlichen Risiken durch das Ergreifen technischer Maßnahmen, die durch organisatorische Maßnahmen flankiert werden, vermieden werden. Auch müssen alle Beschäftigten, die den VIS-Einheitsmandanten nutzen, für dessen datenschutzrechtliche Problematiken sensibilisiert und geschult werden. Nach intensivem Austausch wurde das Konzept maßgeblich geändert und angepasst. Auch für die erforderliche Erarbeitung der technischen und organisatorischen Maßnahmen für die Umsetzung eines datenschutzkonformen VIS-Einheitsmandanten haben wir unsere Beratung angeboten.

5.6 Zugriffsberechtigungen im Dokumentenmanagementsystem

Wie in den Vorjahren erhielten wir auch in diesem Berichtsjahr von verschiedenen Dienststellen Anfragen zum Thema Zugriffsberechtigungen im eingesetzten Dokumentenmanagementsystem VISkompakt (VIS) in der bremischen Verwaltung. Häufig ging es dabei um die Konstellation, in der übergeordnete Abteilungen im Wege des Erhalts von so genannten Geschäftsgangverfügungen (GGVen) eine pauschale Zugriffsberechtigung auf verschiedene Ablagen im VIS forderten.

Das Ablagensystem des in der bremischen Verwaltung eingesetzten Systems VIS ermöglicht es grundsätzlich sicherzustellen, dass nur berechtigte Beschäftigte Zugriff auf entsprechendes Schriftgut haben. Mit der Erteilung einer Geschäftsgangverfügung (GGV) erweitern sich die Zugriffsrechte der Adressat:innen dieser GGV jedoch, sofern diese Beschäftigten zuvor keinen Zugriff auf das betreffende Schriftgut (Akte, Vorgang, Dokument) hatten. Sofern das Schriftgut auf einer Ablage gespeichert ist, für die die GGV-empfangende Person regulär keine

Zugriffsberechtigung besitzt, erlischt die Zugriffsberechtigung bei der aktuell in Bremen eingesetzten VIS-Version erst mit der Erledigung der GGV. Die beschriebene Möglichkeit der GGV-Erteilung führt damit zur Erteilung temporärer Zugriffsrechte, deren zeitliche Länge von den Adressat:innen der GGVen gesteuert wird. Daher muss durch organisatorische Regelungen gewährleistet werden, dass GGVen spätestens dann als erledigt markiert werden, wenn der Zugriff auf das entsprechende Schriftgut nicht mehr erforderlich ist. Sofern der Zugriff zu einem späteren Zeitpunkt erneut erforderlich wird, muss bei den zuständigen Beschäftigten eine erneute Zugriffsberechtigung angefragt werden.

Für eine datenschutzrechtliche Bewertung des Zugriffs auf Ablagen ist entscheidend, ob auf diesen Ablagen zumindest auch personenbezogene Daten verarbeitet werden. Falls keine personenbezogenen Daten verarbeitet werden, finden die datenschutzrechtlichen Vorschriften keine Anwendung. Eine projektbezogene Zusammenarbeit oder Abstimmungsprozesse zwischen mehreren Referaten/Abteilungen, bei denen keine über die Daten durch VIS selbst verarbeiteten Beschäftigtendaten (zum Beispiel Namen der Bearbeiter:innen) hinausgehenden personenbezogenen Daten enthalten sind, können auf entsprechenden speziellen Ablagen wie Projektablagen stattfinden, auf die potenziell alle Beschäftigten der Behörde zugreifen können.

Werden personenbezogene Daten Externer wie von denjenigen Menschen, die sich mit einem Anliegen an die Verwaltung gewandt haben, verarbeitet, ist ein Zugriff aller Beschäftigten auf die betreffenden Ablagen unzulässig. Dies gilt in besonderem Maße bei der Verarbeitung besonderer Kategorien personenbezogener Daten, etwa Gesundheitsdaten. In diesen Konstellationen muss in jedem Einzelfall geprüft werden, ob eine GGV erteilt werden darf, die die beschriebene Rechteerweiterung zur Folge hat. Pauschale fallunabhängige Zugriffsrechte für nicht zuständige Beschäftigte und Leitungsebenen dürfen nicht bestehen. Soweit die Verarbeitung personenbezogener Daten zum Zwecke der Aufgabenerfüllung im öffentlichen Bereich durch mehrere Beschäftigte oder die (nächsthöhere) Leitungsebene erforderlich ist, ist die GGV-Erteilung demgegenüber datenschutzrechtlich begründet. Hierbei kann es sich im Einzelfall auch um mehrere Personen im selben Referat beziehungsweise in derselben Abteilung handeln. Auch eine referats- beziehungsweise abteilungsübergreifende Bearbeitung kann erforderlich sein. Neben den funktional zuständigen Beschäftigten können ausschließlich die direkten Vorgesetzten ebenfalls Zugriffsrechte erhalten. Die nächsthöheren Vorgesetzten erhalten grundsätzlich keine Zugriffsrechte, sondern müssen sich für die Berechtigungserteilung via GGV an die jeweiligen direkten Vorgesetzten wenden. Direkte Vorgesetzte fungieren somit als vermittelnde Stelle zwischen den einzelnen Beschäftigten und den übergeordneten Leitungsebenen.

Sofern nicht personenbezogene Daten, sondern Unternehmensdaten verarbeitet werden, greifen die datenschutzrechtlichen Vorgaben nicht, da Betriebs- und Geschäftsgeheimnisse nicht dem Grundrecht auf informationelle Selbstbestimmung unterfallen. Bei der Verarbeitung von Daten Einzelgewerbetreibender, Freiberufler:innen oder so genannten Ein-Personen-GmbHs kann es sich aber um personenbezogene Daten handeln.

5.7 Deutschland online – Datenschutzcockpit

Die Verpflichtung von Bund und Ländern, ihre Verwaltungsdienstleistungen auch in elektronischer Form über Verwaltungsportale anzubieten, wurde bereits in dem 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 5.17 erläutert. Das Gesetz zur Registermodernisierung (RegMoG) sieht die Einführung einer Identifikationsnummer und des so genannten Datenschutzcockpits vor. Bürger:innen sollen unter Nutzung der Identifikationsnummer nachvollziehen können, welche öffentlichen Stellen Daten über sie gespeichert haben, um welche Daten es sich handelt und wann, von wem und zu welchem Zweck auf die personenbezogenen Daten zugegriffen wurde.

Das Datenschutzcockpit, das deutschlandweit eingesetzt werden soll, wird in Bremen pilotiert. Im ebenfalls in Bremen pilotierten Projekt ELFE (Einfach Leistungen für Eltern), das es ermöglicht, mit einem einzigen Online-Antrag die Geburtsanzeige, die Namensbestimmung, das Eltern- und das Kindergeld zu beantragen, werden personenbezogene Daten zwischen verschiedenen Stellen ausgetauscht. Deshalb kann die Funktionsweise des Datenschutzcockpits im ELFE-Projekt gut getestet werden.

In dem regelmäßig stattfindenden Steuerungskreis, an welchem neben Vertreter:innen der Freien Hansestadt Bremen, des Bundesministeriums des Innern und für Heimat, des Bundesamtes für Sicherheit in der Informationstechnik und des Bundesverwaltungsamts auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit teilnehmen, werden Projektfortschritte und offene Fragen beraten. Dazu zählen auch Fragestellungen der Vertreter:innen der Register, die an das Datenschutzcockpit angebunden werden sollen. Sie beziehen sich beispielsweise auf die datenschutzrechtliche Verantwortung, darauf, dass die Register auch unrichtige Daten enthalten, und Vorbehalte gegen Einsichtsmöglichkeiten in die Registerdaten.

6. Inneres

6.1 Meldung der Verletzung des Schutzes personenbezogener Daten

Aus dem Bereich Inneres erreichten uns insgesamt vier Meldungen der Verletzung des Schutzes personenbezogener Daten. Eine Meldung erfolgte aufgrund einer fehlerhaften Versendung einer Meldebescheinigung durch das Bürgeramt Bremen. Die drei weiteren Meldungen stammen von der Polizei. Wiederum einer dieser drei Meldungen liegt ein unberechtigter Zugriff im polizeilichen Informationssystem @rtus zu Grunde, der zweiten Meldung ein Abstellen von Unterlagen aus der Polizeiausbildung an einer Straße und die dritte Meldung der Polizei erfolgte aufgrund eines technisch bedingten Verlustes von Online-Anzeigen und Online-Bewerbungen.

6.2 Videoüberwachungen

Polizeiliche Überwachungsmaßnahmen prägten in diesem Jahr verstärkt unsere Tätigkeit. Im Folgenden wird ein Überblick über die zentralen Maßnahmen gegeben.

6.2.1 Maritime Tage 2022

Wie bereits im letzten Jahr (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.4.1) nutzte die Ortspolizeibehörde Bremerhaven die Rechtsgrundlage des § 32 Absatz 3 Satz 1 Nummer 2 Bremisches Polizeigesetz (BremPolG) für eine Videoüberwachung der Maritimen Tage in Bremerhaven vom 17. August bis 21. August 2022.

Wir wurden frühzeitig in die Planung einbezogen, besprachen die Standorte der Kameras und die erfassten Bereiche wurden gemeinsam mit Vertretern der Ortspolizeibehörde Bremerhaven besprochen. Die Ortspolizeibehörde Bremerhaven informierte die Öffentlichkeit durch Hinweisschilder um das Veranstaltungsgelände herum sowie über verschiedene (Online-)Kanäle. Des Weiteren erstellte die Ortspolizeibehörde Bremerhaven eine Datenschutz-Folgenabschätzung nach § 84 BremPolG, zu der wir Stellung nahmen. Zusammen mit der Einrichtungsanordnung nach § 32 Absatz 3 BremPolG war unsere Stellungnahme auch Gegenstand einer Sitzung der staatlichen Deputation für Inneres.

Die Rechtsgrundlage des § 32 Absatz 3 Satz 1 Nummer 2 BremPolG wurde vom bremischen Gesetzgeber geschaffen, um eine Überwachung von Großveranstaltungen wie den Maritimen Tagen, den Freimärkten oder auch den Weihnachtsmärkten in Bremen und Bremerhaven zu ermöglichen. § 32 Absatz 3 Satz 1 Nummer 2 BremPolG setzt für die Rechtmäßigkeit der Überwachungsmaßnahme keine konkrete Gefahrenprognose voraus, dennoch steht die

Zulässigkeit der Überwachung unter dem Vorbehalt der Verhältnismäßigkeit. Die Rechtmäßigkeit der Überwachung setzt somit voraus, dass der mit ihr einhergehende staatliche Eingriff in das von der Verfassung garantierte allgemeine Persönlichkeitsrecht und in das europäisch garantierte Grundrecht auf Datenschutz vor dem Hintergrund der mit der Überwachungsmaßnahme verfolgten Ziele angemessen erscheint. Die Ortspolizeibehörde Bremerhaven sah die Verhältnismäßigkeit der Überwachungsmaßnahme als gegeben an. Im Rahmen unserer Stellungnahme zur Datenschutz-Folgenabschätzung positionierten wir uns hierzu erneut kritisch. Aus unserer Sicht sollte der bremische Gesetzgeber in § 32 Absatz 3 Satz 1 Nummer 2 BremPolG das Erfordernis einer konkreten Gefahrenprognose ergänzen.

6.2.2 Drohnen

Die Polizei Bremen übermittelte uns eine Datenschutz-Folgenabschätzung zum Einsatz von Drohnen. Nach unserer Auffassung ist ein Einsatz der Drohnen im präventiven Bereich der polizeilichen Tätigkeit im Regelfall nicht möglich.

Der offene Einsatz von Drohnen richtet sich nach § 32 Bremisches Polizeigesetz (BremPolG). Als sinnvolles Einsatzszenario kommt dabei im Regelfall nur ein solches in Betracht, das unter § 32 Absatz 3 Nummer 2 BremPolG fällt, wie etwa die Überwachung des Kulturfestivals Breminale, des Freimarktes oder des Weihnachtsmarktes (siehe hierzu Ziffer 6.2.1 dieses Berichts). In diesen Fällen steht einem Drohneneinsatz regelmäßig der Grundsatz der Verhältnismäßigkeit entgegen. Eine hoheitliche Maßnahme – wie der Einsatz von Drohnen – ist nur verhältnismäßig, wenn kein milderes aber gleich effektives Mittel zur Verfügung steht und die Maßnahme an sich angemessen erscheint. Als milderes und gleich effektives Mittel dürften bei den denkbaren Einsatzszenarien regelmäßig feststehende Kameras in Betracht kommen. Sie können wie Drohnen das Veranstaltungsgelände erfassen (gleich effektives Mittel) und ermöglichen es, die Erfassung bestimmter Bereiche sicher auszuschließen, beispielsweise durch Schwärzungen. So kann etwa die Erfassung von Privatwohnungen durch entsprechende Ausrichtungen der Kameralinsen oder durch Schwärzungen ausgeschlossen werden. Bei Drohnen wird dies indes regelmäßig nicht mit gleicher Sicherheit der Fall sein (Kameras als milderes Mittel). Der mit der polizeilichen Überwachung einhergehende Grundrechtseingriff gebietet es daher, auf feststehende Kameras als milderes aber gleich effektives Mittel zurückzugreifen, sodass der Einsatz von Drohnen unzulässig ist.

Die Rechtmäßigkeit einer verdeckten Drohnenobservation würde sich hingegen nach § 40 Absatz 2 Satz 2 BremPolG bestimmen. § 40 Absatz 2 Satz 2 BremPolG legitimiert jedoch nicht den Einsatz (besonderer) technischer Mittel. Solche dürften nur für längerfristige Observationen nach § 40 Absatz 1 BremPolG herangezogen werden. Drohneneinsätze können hingegen aufgrund der eingesetzten Technik nur kurzfristige Maßnahmen sein. So

sind etwa die Akkukapazitäten begrenzt. Daher könnte ein verdeckter Drohneneinsatz nicht durch § 40 BremPolG legitimiert werden.

Da das Bremische Polizeigesetz den Drohneneinsatz aktuell nicht legitimiert, sprachen wir nach § 86 Absatz 3 Satz 1 BremPolG im Rahmen unserer Stellungnahme zur Datenschutz-Folgenabschätzung der Polizei die Empfehlung aus, im präventiven Aufgabenbereich keine Drohnen einzusetzen, bis der bremische Gesetzgeber eine entsprechende Rechtsgrundlage geschaffen hat. Sofern der bremische Gesetzgeber planen sollte, eine Rechtsgrundlage für den Einsatz von Drohnen zu schaffen, müssten neben den vor allem technischen Schutzmaßnahmen folgende Punkte berücksichtigt beziehungsweise deren Umsetzbarkeit geprüft werden:

- Möglichkeiten der Unkenntlichmachung von unbeteiligten Dritten auf gespeicherten Aufnahmen, insbesondere, wenn diese sich auf privaten Grundstücken befinden (Artikel 13 Grundgesetz),
- Mindestflughöhe über privaten Grundstücken unbeteiligter Dritter (Artikel 13 Grundgesetz),
- Mindestflughöhe über sensiblen Bereichen (Freibad, Krankenhausanlagen…),
- nachträgliche Information verdeckt aufgenommener Unbeteiligter soweit wie möglich und verhältnismäßig (beispielsweise nachträgliche Informationen an Grundstückbesitzer:innen).

6.2.3 Polizeicontainer

Die Polizei Bremen schaffte im Berichtsjahr einen so genannten Polizeicontainer an, der auf Großveranstaltungen, wie zum Beispiel des Kulturfestivals Breminale, etwa zur Anzeigenaufnahme oder zur Lagebesprechung genutzt werden kann. Der Polizeicontainer ist mit Videoüberwachungstechnik ausgestattet, die dem Zweck dient, Sachbeschädigungen des Containers zu verhindern oder besser aufklären zu können. Zwar wurde uns diese Videotechnik bereits von Vertreter:innen der Polizei Bremen in einem Vor-Ort-Termin vorgeführt. Zum Einsatz konnte diese Technik jedoch noch nicht kommen, da vor jedem Einsatz das unter Ziffer 6.2.1 dieses Berichts beschriebene Anordnungsverfahren durchlaufen werden muss.

6.2.4 Liegenschaften

Im Berichtsjahr erweiterte die Polizei Bremen die bestehende Videoüberwachung an den Revieren Findorff und Schwachhausen. Rechtsgrundlage für die Videoüberwachung und ihre Erweiterung ist § 32 Absatz 3 Satz 1 Nummer 1 Bremisches Polizeigesetz (BremPolG). Bei

beiden Revieren wurden wir frühzeitig in die Planung einbezogen. Gemeinsam mit Vertretern der Polizei Bremen legten wir im Rahmen von Vor-Ort-Terminen die Bereiche fest, die in zulässiger Weise von den Kameras erfasst werden dürfen. In diesem Zuge nahmen wir gemeinsam mit den Vertretern der Polizei Schwärzungen von Bereichen vor, die die Polizei nicht mittels Videotechnik erfassen darf. Zudem besprachen wir die Standorte der Hinweisschilder, über die die Öffentlichkeit, insbesondere Passant:innen über die Videoüberwachung informiert werden. Die Polizei Bremen erstellte jeweils eine Datenschutz-Folgenabschätzung nach § 84 BremPolG, zu der wir Stellung nahmen. Diese Stellungnahme wurde zusammen mit der Einrichtungsanordnung nach § 32 Absatz 3 BremPolG den Mitgliedern der Innendeputation vorgelegt.

Anders als § 32 Absatz 3 Satz 1 Nummer 2 BremPolG (siehe hierzu Ziffer 6.2.1 dieses Berichts) setzt § 32 Absatz 3 Satz 1 Nummer 1 BremPolG für eine zulässige Videoüberwachung voraus, dass an den überwachten Orten vermehrt Straftaten begangen werden oder an ihnen aufgrund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist. Die Polizei Bremen hatte für die beiden Standorte jeweils eine Auflistung vergangener Straftaten erstellt und daneben in einer Prognose erörtert, warum auch zukünftig Straften gegen die Liegenschaften der Polizei zu erwarten seien. Die vorgelegten Dokumente erfüllten den gesetzlichen Tatbestand. Bei der aufsichtsrechtlichen Beurteilung der Rechtmäßigkeit der jeweiligen Kameras ist zusätzlich von zentraler Bedeutung, ob sich die Videoüberwachung durch jede der eingesetzten Kameras auf das tatsächlich Erforderliche beschränkt und transparent erfolgt.

Ergänzend haben wir deshalb und anlässlich einer Beschwerde über eine Kamera der Polizei Bremen begonnen, sämtliche Kameras der Liegenschaften der Polizei Bremen und der Ortspolizeibehörde Bremerhaven zu überprüfen, soweit diese auch öffentlich zugänglichen Bereiche erfassen. In Vor-Ort-Terminen mit Vertreter:innen der beiden Polizeibehörden benannten wir erforderliche Beschränkungen der Erfassungsbereiche und berieten bei der Entwicklung von Standortplänen für die erforderliche und zum Teil noch nicht vorhandene Beschilderung der Überwachungen. Unsere Überprüfung der Kameras dauert ebenso wie die Umsetzung des Besprochenen durch die Polizei Bremen noch an.

6.3 Polizeiliche Informationssysteme

Anlässlich des Überschreitens von Löschfristen im letzten Berichtsjahr (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.2) lassen wir uns in einem fortwährenden Austausch von der Polizei Bremen und von der Ortspolizeibehörde Bremerhaven die genutzten Informationssysteme zeigen und nehmen Einsicht in diese. Dies findet im Rahmen von Vor-Ort-Terminen statt, in denen uns die zuständigen Mitarbeiter:innen

der Polizei den von der Polizei verfolgten Zweck benennen und die Nutzung der Systeme darstellen. Gemeinsam werden anschließend sich ergebene datenschutzrechtliche Fragestellungen erörtert und gegebenenfalls ein Anpassungsbedarf identifiziert, dem die Polizeibehörden nachgehen müssen. Im Berichtsjahr nahmen wir in dieser Weise erneut Einsicht in das übergreifende Polizeiinformationssystem @rtus. Daneben war dies zum Beispiel bei Systemen aus der Unfallsachbearbeitung, Asservatenlisten und der Liste festgenommener Personen der Fall. Einen Anpassungsbedarf identifizierten wir stellenweise etwa bei Löschprotokollen und Lösch-/Anonymisierungsroutinen.

Die Polizei erstellte eine Liste aller genutzter Systeme, die nun fortwährend Gegenstand der Vor-Ort-Termine ist. Nicht nur angesichts der Vielzahl der verwendeten Systeme ist dies ein fortlaufender und andauernder Prozess.

6.4 Auskunftsersuchen

Im 4.Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 5.3 berichteten wir, dass wir uns mit der Polizei Bremen und der Ortspolizeibehörde Bremerhaven in beratender Funktion im Austausch darüber befinden, wie Auskunftsersuchen nach § 73 Bremisches Polizeigesetz (BremPolG) zu beantworten sind.

Gemäß § 73 BremPolG können betroffene Personen von beiden Polizeibehörden im Land Bremen Auskunft darüber verlangen, ob diese Daten über sie verarbeiten. Daneben haben sie das Recht, einige weitere Informationen über die Verarbeitung ihrer personenbezogenen Daten durch die Polizeibehörden zu erlangen. In bestimmten Fällen können die Polizeibehörden die Auskunft einschränken oder ganz verweigern.

Das Auskunftsrecht gegenüber Polizeibehörden ist ein zentrales Recht jeder einzelnen Person. Es umfasst nicht allein das Recht, in Erfahrung bringen zu können, was die Polizeibehörden über die betreffende Person wissen, sondern räumt ihr auch die Möglichkeit ein, Datenverarbeitungsvorgänge auf ihre Rechtmäßigkeit zu überprüfen. Unsere Erfahrungen aus der aufsichtsbehördlichen Praxis zeigen, dass sich Betroffene häufig nach Erhalt konkreter Informationen über eine polizeiliche Speicherung sie betreffender Daten veranlasst sehen, weitere Rechte auszuüben und bei uns eine Beschwerde über die polizeiliche Datenverarbeitung einzulegen. So erreichte uns die Mehrzahl der diesjährigen Beschwerden Betroffener, nachdem diese etwa nach § 58 Absatz 8 BremPolG von den Polizeibehörden über eine (weitere) Speicherung sie betreffender Daten unterrichtet worden waren.

Derzeit befinden wir uns sowohl mit den Aufsichtsbehörden anderer Bundesländer als auch mit den bremischen Polizeibehörden im Austausch darüber, welche Anforderungen an die Beantwortung von Auskunftsersuchen zu stellen sind. Mit der Ortspolizeibehörde

Bremerhaven wurde zwischenzeitlich ein Musterformular entwickelt, mittels dessen den Antragstellenden zumindest auf einer ersten Stufe einige Basisinformationen zur Verfügung gestellt werden können. Die Frage der Beantwortung eines Auskunftsersuchens stellt sich dabei auch immer wieder bei der Prüfung polizeilicher Informationssysteme (siehe Ziffer 6.3 dieses Berichts). In einem Beschwerdefall, in dem wir der Auffassung sind, dass in nicht hinreichender Weise Auskunft erteilt wurde, haben wir eine Beanstandung nach § 85 Absatz 1 BremPolG ausgesprochen.

6.5 Anfragen der Polizei an Unternehmen im Rahmen von Ermittlungen

Im Rahmen unserer Beratungstätigkeit wurden wir mit der Frage konfrontiert, unter welchen Voraussetzungen die Polizei Bremen und die Ortspolizeibehörde Bremerhaven Daten über Kund:innen für ihre Ermittlungstätigkeiten bei Unternehmen erfragen dürfen. Während für die Polizeibehörden in der Strafprozessordnung und im Bremischen Polizeigesetz (BremPolG) Befugnisse für derartige Anfragen und für den mit ihnen verbundenem Datenaustausch geschaffen wurden, ist die Übermittlung von Kund:innendaten an die Polizei für Unternehmen mit besonderen Risiken verbunden. Dies gilt zumindest dann, wenn die Übermittlung nicht auf Grundlage einer verpflichtenden Anordnung erfolgt.

Aufgrund des so genannten Doppeltürmodells des Bundesverfassungsgerichts benötigen nicht nur die Polizeibehörden für die Datenanfrage und den anschließenden Datenzugriff eine Legitimationsgrundlage (erste Tür), sondern auch das Unternehmen für die Datenübermittlung (zweite Tür). Da die Datenübermittlung an Polizeibehörden regelmäßig auch mit einer Zweckänderung verbunden ist, muss zudem auch diese gesetzlich legitimiert werden. Als Legitimationsgrundlage sowohl für die Zweckänderung als auch für die Datenübermittlung durch das Unternehmen kommt grundsätzlich § 24 Absatz 1 Nummer 1 Bundesdatenschutzgesetz (BDSG) in Betracht. Der bremische Gesetzgeber hat zwar mit § 57 BremPolG eine ähnliche Rechtsgrundlage geschaffen, deren Anwendbarkeit und formelle Rechtmäßigkeit mangels Gesetzgebungskompetenz des Landesgesetzgebers jedoch zweifelhaft erscheinen. Der § 24 Absatz 1 Nummer 1 BDSG legt Unternehmen die Pflicht zu einer Interessensabwägung auf. Da Unternehmen jedoch in der Regel nicht beurteilen können, welche personenbezogenen Daten für die Zwecke der Polizei tatsächlich erforderlich sind und wie schwer das polizeiliche Verfolgungsinteresse im Einzelfall wiegt, stellt die Interessensabwägung Unternehmen vor unlösbare, mindestens aber vor sehr schwierige Aufgaben. Wir haben daher mit Vertreter:innen beider Polizeibehörden ein Verfahren entwickelt, über das sichergestellt werden kann, dass die Polizeibehörden an Unternehmen nur solche Anfragen richten, deren Beantwortung durch die Unternehmen auf § 24 Absatz 1 Nummer 1 BDSG gestützt werden kann. Mittels vereinbarter technisch-organisatorischer Maßnahmen vor allem auf Seiten beider Polizeibehörden ist es somit möglich,

Interessensabwägungen in einem entwickelten Anfrageverfahren zu implementieren, sodass Unternehmen von der risikoreichen Interessensabwägung im Einzelfall befreit und gleichzeitig datenschutzrechtliche Beschränkungen des Datenaustausches zum Schutz der Grundrechte und Grundfreiheiten betroffener Personen konsequent beachtet werden.

6.6 Rechtsverordnung zur Prüf- und Speicherfristen

Bereits im 4. Jahresbericht unter Ziffer 5.2 legten wir dar, dass das Bremische Polizeigesetz (BremPolG) noch den Erlass einer Rechtsverordnung zu Prüf- und Speicherfristen der Polizei erfordert. Gemäß § 58 Absatz 6 Satz 1 BremPolG werden die Aussonderungsprüffristen vom Senator für Inneres durch Rechtsverordnung festgelegt, wobei nach unserer Rechtsauffassung auch die Normierung von Speicherfristen zulässig ist, insbesondere dann, wenn sich Aussonderungsprüffristen nicht als praktikabel erweisen. Wir stehen mit Vertreter:innen beider Polizeibehörden sowie des Senators für Inneres im kontinuierlichen Austausch und weisen dort immer wieder auf einen zeitnahen Erlass einer entsprechenden Rechtsverordnung hin.

6.7 Personenkontrolldokumentation

Von der Einführung der Personenkontrolldokumentation (PerKonDo) berichteten wir bereits im letzten Jahr (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.8). Nach § 27 Bremisches Polizeigesetz (BremPolG) können kontrollierte Personen seit September 2021 verlangen, dass ihnen die Polizei Bremen und die Ortspolizeibehörde Bremerhaven eine Bescheinigung über die Identitätsfeststellung und deren Begründung (so genannte Kontrollbescheinigungen) ausstellen. Kerngegenstand der Beratung in diesem Berichtsjahr war der Einsatz einer Ausweisscanfunktion. Die kontrollierenden Beamt:innen sind über diese mit ihrem dienstlichen Smartphone in der Lage, bestimmte Daten der Kontrollierten (vollständiger Name, Geburtsdatum und -ort, Geburtsland, Anschrift) mittels eines Scanners zu erfassen und sie so direkt in das System zur Ausstellung einer Kontrollbescheinigung zu übertragen.

Im Zuge der Beratungstätigkeit kamen wir mit der Polizei überein, dass die Erfassung von Ausweisen zulässig ist, sofern die kontrollierten Personen in das Anfertigen einer digitalen Kopie im Wege des Einscannens eingewilligt haben. Verweigert die kontrollierte Person die Einwilligung, dürfen die Ausweisdaten nicht mittels eines Ausweisscanners erfasst werden. Die Anwendung sieht nunmehr technische Hürden vor, mittels derer sichergestellt wird, dass die Scanfunktion nur eingesetzt wird, wenn eine Einwilligung der kontrollierten Person vorliegt.

6.8 Zuverlässigkeitsüberprüfungen

Anlässlich einer Anfrage der Ortspolizeibehörde Bremerhaven setzten wir uns mit der Frage der Zulässigkeit so genannter Zuverlässigkeitsüberprüfungen nach dem Bremischen Polizeigesetz (BremPolG) auseinander. Anlass für die Anfrage war, dass die Ortspolizeibehörde Bremerhaven die Zuverlässigkeit von Bauarbeiter:innen überprüfen möchte, die beim Neubau des Reviers Geestemünde mit kritischer Infrastruktur in Berührung kommen. Bei einer derartigen Zuverlässigkeitsüberprüfung handelt es sich nicht um eine umfassende Sicherheitsüberprüfung im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG), sondern um eine Abfrage in polizeilichen Informationssystemen auf Grundlage des BremPolG.

Das BremPolG sieht keine speziellen Regelungen für eine Zuverlässigkeitsüberprüfung bei kritischen Anlässen vor. Es kennt lediglich eine Zuverlässigkeitsüberprüfung für Bewerber:innen, Angestellte und Beamt:innen bei Polizeibehörden. Anders sieht dies beispielsweise in Bayern aus. Dort regelt der Artikel 60 a des Bayrischen Polizeiaufgabengesetzes (PAG), wann und unter welchen Voraussetzungen die Polizei Zuverlässigkeitsüberprüfungen bei kritischen Anlässen vornehmen kann. Diese Regelung wurde vom Bayrischen Verfassungsgerichtshof bestätigt (Entscheidung des Bayerischen Verfassungsgerichtshofs vom 17. Mai 2022, Aktenzeichen Vf. 47-VII-21). Auch in anderen Ländern ist die Überprüfung der Zulässigkeit von Fremdpersonen, mithin von Personen, die weder Bewerber:innen noch Angestellte noch Beamt:innen bei Polizeibehörden sind, nicht unbekannt. In Bremen stellt sich hingegen aktuell die Frage, ob eine Zuverlässigkeitsüberprüfung auf Grundlage der Generalklauseln des BremPolG möglich ist. Unsere Prüfung hat dabei ergeben, dass eine derartige Überprüfung zumindest unter Beachtung einer Vielzahl von Einschränkungen und Verfahrensschritten nicht generell ausgeschlossen ist.

Zuverlässigkeitsüberprüfungen sind grundsätzlich problematisch, weil sie in das Grundrecht auf informationelle Selbstbestimmung, in das Grundrecht auf Gewährleistung des Datenschutzrechts sowie daneben in die verfassungsrechtlich garantierte Berufsfreiheit eingreifen. Gleichzeitig ist das augenscheinlich gesteigerte Bedürfnis nach der Vornahme derartiger Überprüfungen zu beobachten. Im Rahmen unserer Aufgabenwahrnehmung nach § 84 Absatz 1 Nummer 3 BremPolG regen wir daher an, dass sich der bremische Gesetzgeber dieser Thematik annimmt. Sollte er die Notwendigkeit derartiger Überprüfungen nach einer kritischen Auseinandersetzung mit der Thematik bejahen, sollten klare Vorgaben zur Durchführung derartiger Prüfungen und damit auch zum Schutz betroffener Personen normiert werden.

6.9 Zensus 2022

Im Mai des Berichtsjahres startete der Zensus 2022. Die Landesbeauftragte für Datenschutz und Informationsfreiheit führte in diesem Zusammenhang einen Prüfungs- und Beratungstermin bei einer Zensus-Erhebungsstelle in Bremerhaven durch.

Auch von Bürger:innen, die von den Zensus-Erhebungsstellen angeschriebenen worden waren, erreichten uns einige Beratungsanfragen und Beschwerden. Gegenstand waren, neben Zweifeln über die allgemeine Rechtmäßigkeit der Zensusdurchführung, auch die Pflicht zur Beantwortung der Zensusformulare gegenüber dem Statistischen Landesamt Bremen.

Auch Berichte beispielsweise über falsch geschriebene Namen konnten wir, wie auch weitere Anfragen, im Austausch mit dem Statistischen Landesamt Bremen aufklären.

7. Justiz inklusive Rechtsanwält:innen

7.1 Gemeldete Datenschutzverletzungen

Im Jahr 2022 wurden von Rechtsanwält:innen und Notar:innen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit zwei Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung gemeldet.

Die Staatsanwaltschaft Bremen als verantwortliche Stelle sowie die Gerichte im Land Bremen meldeten der Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr 2022 keine Verletzungen des Schutzes personenbezogener Daten.

7.2 Novellierung des Bremischen Gesetzes über die Juristenausbildung

Von der Senatorin für Justiz und Verfassung erhielten wir einen Gesetzentwurf zur Novellierung des Bremischen Gesetzes über die Juristenausbildung und die erste juristische Prüfung (JAPG) zur datenschutzrechtlichen Prüfung. Im JAPG sollte geregelt werden, dass bei Einsichtnahme in die Prüfungsakte weitergehende Informationsrechte aufgrund anderer Rechtsgrundlagen für Prüflinge und Dritte ausgeschlossen sein sollten. Diese Regelung hätte dem Recht auf Auskunft nach Artikel 15 Datenschutzgrundverordnung widersprochen.

Die Datenschutzgrundverordnung (DSGVO) gilt auch für die nach Personen und Prüfungsnummer sortierte manuelle und analoge Ordnung und Aufbewahrung von Dokumenten wie juristische Aufsichtsarbeiten. Diese werden mit einer Prüfungsnummer versehen, die jeweils einer bestimmten Person zugeordnet ist, und sind damit personenbezogene Daten. Nach Artikel 15 Absatz 1 DSGVO hat die betroffene Person das Recht vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob ihre

personenbezogenen Daten verarbeitet wurden. Im Fall von Prüfungsleistung bedeutet dies, dass Auskunft über die gesamte Prüfungsleistung und die Bewertung erteilt werden muss. Gemäß Artikel 15 Absatz 3 Satz 1 DSGVO muss die verantwortliche Stelle eine Kopie der Daten zur Verfügung stellen.

Auf die zunächst geplante Regelung wurde verzichtet, sodass nun für Betroffene die Einsichtsrechte aus dem JAPG und aus Artikel 15 DSGVO nebeneinander bestehen.

7.3 Protokollierung von lesenden Zugriffe bei der Staatsanwaltschaft

Schon seit 2015 hat die Landesbeauftragte für Datenschutz und Informationsfreiheit die fehlende Protokollierung im Fachverfahren web.sta bei der Staatsanwaltschaft Bremen angemahnt (siehe hierzu 38. Jahresbericht, Ziffer 6.2; 40. Jahresbericht, Ziffer 6.3 und 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.5). Mit Hilfe von Protokolldaten, die ausweisen, wer wann auf staatsanwaltliche Akten zugreift, kann überprüft werden, ob die Verarbeitung der personenbezogenen Daten ordnungsgemäß erfolgt. Möglicherweise hat eine solche Dokumentation auch eine präventive Funktion und vermag es, missbräuchliche Abrufe zu verhindern.

Die Staatsanwaltschaft Bremen plant seit längerem die Einführung einer solchen Protokollierung (siehe hierzu Stellungnahme des Senats Drucksache 20/1608 Nummer 6.5) und sandte uns einen Entwurf einer internen Hausverfügung zur Protokollierung der lesenden Zugriffe in der elektronischen Fachanwendung zu. In diesem Entwurf fehlen derzeit noch die Verfahrensbeschreibung und die Unterlagen des Auftragsverarbeiters, die Voraussetzungen für eine datenschutzrechtliche Prüfung von unserer Seite sind. Wir hoffen, dass diese datenschutzrechtliche Lücke im Jahr 2023 endlich geschlossen werden wird.

7.4 Insolvenzdaten im Internet einsehbar

Mehrere mit Insolvenzverwaltungen betraute Kanzleien sahen sich im Zusammenhang mit unserer datenschutzrechtlichen Kontrolltätigkeit im Berichtsjahr veranlasst, darauf hinzuwirken, dass die Suchmasken in den von ihnen verwendeten digitalen Gläubigerinformationssystemen datenschutzkonform umprogrammiert wurden (siehe hierzu die Pressemitteilung der Landesbeauftragten für Datenschutz und Informationsfreiheit[1]).

Im Zusammenhang mit einem Beschwerdeverfahren hatten wir Kenntnis darüber erhalten, dass die personenbezogenen Daten von Insolvenzschuldner:innen auf den Internetseiten der Insolvenzkanzleien voraussetzungslos öffentlich für jedermann zugänglich waren. Wir

[1] https://www.datenschutz.bremen.de/aktuelles/kontrolle-der-lfdi-bewirkt-stopp-unzulaessiger-veroeffentlichungen-von-personenbezogenen-insolvenzdaten-18308

überprüften daraufhin im Rahmen einer größeren Kontrolle die Veröffentlichungen dieser Daten in den Gläubigerinformationssystemen der meistbestellten deutschlandweit tätigen Insolvenzkanzleien mit Standort in Bremen. Dabei stellten wir die mangels ausreichender gesetzlicher Grundlage datenschutzwidrigen Veröffentlichungen dieser Daten fest. Die betroffenen Kanzleien zeigten sich größtenteils kooperativ und wirkten erfolgreich auf den Softwareanbieter ein, die verwendete Software anzupassen. Die angepasste Software wird nunmehr bundesweit von fast allen in Deutschland tätigen Kanzleien verwendet.

Die Daten der Insolvenzschuldner:innen können jetzt nur noch von den tatsächlichen Insolvenzgläubiger:innen nach vorheriger Registrierung und Einloggen in den passwortgeschützten Bereich des Gläubigerinformationssystem abgerufen werden. Inwieweit gegen die betreffenden Insolvenzkanzleien aufgrund der datenschutzwidrigen Veröffentlichung der personenbezogenen Daten der Insolvenzschuldner:innen im Internet weitergehende Maßnahmen nach der Datenschutzgrundverordnung in Betracht kommen, wird von uns aktuell noch geprüft.

7.5 Digitale Zugriffsmöglichkeit ehemaliger Beschäftigter

Im Berichtsjahr erhielten wir einen Hinweis über ein mutmaßliches Datenleck bei einem insolventen Unternehmen. Im Rahmen unserer Überprüfung stellten wir fest, dass der verantwortliche Insolvenzverwalter die Kennwörter und Zugriffe einiger ehemaliger Beschäftigter, die im Verlauf des Insolvenzverfahrens aus dem Unternehmen ausgeschieden waren, nicht geändert hatte, sodass diese weiterhin via Fernzugriff auf personenbezogene Daten auf den Servern der Insolvenzschuldnerin zugreifen konnten. Dabei bestand für die ehemaligen Beschäftigen der Insolvenzschuldnerin insbesondere auch eine Zugriffsmöglichkeit auf Daten aller Kund:innen und anderer (ehemaligen) Beschäftigter.

Dies stellte einen datenschutzrechtlichen Verstoß des verantwortlichen Insolvenzverwalters dar, weil personenbezogene Daten grundsätzlich durch geeignete technische und organisatorische Maßnahmen in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Dazu gehört es, die Zugriffmöglichkeiten auf personenbezogenen Daten für ausgeschiedene Beschäftigte technisch auszuschließen. Bei insolventen Unternehmen sind hierfür Insolvenzverwalter:innen verantwortlich, da allein diese über die Zwecke und Mittel der Verarbeitung der bei der Insolvenzschuldnerin beziehungsweise bei dem Insolvenzschuldner vorhandenen personenbezogenen Daten entscheiden. Inwieweit gegen den betreffenden Insolvenzverwalter aufgrund des vorgenannten datenschutzrechtlichen Verstoßes

weitergehende Maßnahmen nach der Datenschutzgrundverordnung in Betracht kommen, wird von uns aktuell noch geprüft.

7.6 Fehlversand anwaltlicher Schreiben

Erfreulicherweise gingen im Jahr 2022 die Beschwerden und Meldungen über Rechtsanwaltskanzleien, die anwaltliche Schreiben an falsche Empfänger:innen versandt hatten, zurück. Hierzu wurden uns im Berichtsjahr nur zwei Fälle gemeldet. Dieser Eindruck bestätigt sich auch bei unseren stichprobenartigen Kontrollen. Die von uns kontrollierten Kanzleien konnten dabei vielfältige präventive Maßnahmen zum datenschutzkonformen Versand anwaltlicher Schreiben nachweisen.

7.7 Vermehrte Beschwerden gegen Webseiten von Rechtsanwält:innen

Im Berichtsjahr mussten wir eine Zunahme von Beschwerden gegen die Online-Präsenz von Rechtsanwält:innen feststellen. In den meisten Fällen gingen gleich mehrere Beschwerden gegen eine Kanzlei in einen engen Zeitraum bei uns ein. Selbst bei nur kursorischen datenschutzrechtlichen Prüfungen der jeweiligen Webseiten zeigte sich, dass die Nutzung von Tracking-Tools und Datenschutzerklärungen nicht den datenschutzrechtlichen Anforderungen der Datenschutzgrundverordnung entsprach.

8. Gesundheit

8.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr wurden uns insgesamt 27 Datenschutzverletzungen gemeldet. Ein Großteil der Meldungen betraf die Ausgabe fehlerhafter Impfzertifikate durch die Impfstellen im Land Bremen. Hierfür waren Namensverwechselungen die häufigste Ursache. Wir konnten erreichen, dass die betroffenen Personen auch in künftigen Fällen stets entsprechend der gesetzlichen Vorgaben durch die Senatorin für Gesundheit, Frauen und Verbraucherschutz als Betreiberin der Impfstellen informiert werden.

8.2 Einrichtungsbezogene Impfpflicht

Mit dem "Gesetz zur Stärkung der Impfprävention gegen COVID-19 und zur Änderung weiterer Vorschriften im Zusammenhang mit der COVID-19-Pandemie" schuf der Bundesgesetzgeber Ende 2021 die so genannte einrichtungsbezogene Impfpflicht. Personen, die in medizinischen Einrichtungen tätig sind, hatten bis zum 15. März 2022 Zeit, gegenüber der Einrichtungsleitung nachzuweisen, dass sie gegen COVID-19 geimpft sind oder dass dies wegen einer Kontraindikation nicht möglich ist. Bei Zweifeln an der Echtheit vorgelegter Dokumente oder

bei Nichtvorlage muss die jeweilige Einrichtung der gesetzlichen Regelung zufolge das zuständige Gesundheitsamt einschalten. Dieses kann die Vorlage des Nachweises anordnen und gegebenenfalls ein Tätigkeitsverbot verhängen.

Die Gesundheitsämter im Land Bremen richteten für die Meldungen digitale Plattformen ein. In gemeinsamen Terminen wurde uns die Plattform vorgestellt. Trotz entsprechender Zusagen stellte uns das Gesundheitsamt Bremen hierzu keine näheren Erläuterungen und Screenshots zur Verfügung. Auch ein Löschkonzept erhielten wir nach mehrmaliger Aufforderung nicht. Anfragen Betroffener zur Sicherheit der digitalen Meldeplattform konnten wir daher bedauerlicherweise nicht vollständig beantworten. Neben Anfragen erreichten uns auch einige Beschwerden betroffener Personen, die der Ansicht waren, dass die Übermittlung sie betreffender Daten an das zuständige Gesundheitsamt oder die Verarbeitung der Daten durch das Gesundheitsamt unzulässig sei. Nach Prüfung der Beschwerden konnten wir keine Verstöße feststellen.

8.3 Zugriff auf Corona-Schnelltestergebnisse wegen Sicherheitslücke

Mehrere Tausend Datensätze zu Corona-Testungen einer Bremer Apotheke lagen aufgrund einer Sicherheitslücke ungeschützt einsehbar im Internet. Auf diesen Umstand wurden wir durch einen Internetnutzer hingewiesen. Nachdem wir uns auf Grundlage dieses Hinweises umgehend mit der Apotheke und deren IT-Dienstleister in Verbindung gesetzt hatten, wurde wir bald darüber informiert, dass die Lücke behoben wurde. Es stellte sich heraus, dass der IT-Dienstleister ohne Kenntnis der Apotheke Systemtests mit den Originaldatensätzen durchgeführt hatte. Dies war nicht von der Vereinbarung zur Auftragsverarbeitung zwischen den beiden Unternehmen gedeckt.

Indem der Dienstleister die Daten eigenständig verwendete, ohne dabei die erforderlichen Maßnahmen zur Datensicherheit zu treffen, machte er sich selbst zum datenschutzrechtlich Verantwortlichen und muss auch für den verursachten Datenschutzverstoß die Verantwortung tragen. An diesem Beispiel zeigt sich wieder einmal deutlich das Risiko, welches besteht, wenn Systemtests mit Originaldaten durchgeführt werden. Im Regelfall ist es nicht erforderlich und damit unzulässig, dass Systeme mithilfe von Echtdaten getestet werden. Vor jedem Softwaretest ist daher zu prüfen, ob der Zweck des Tests nicht ebenso gut mit fiktiven oder anonymisierten Daten erreicht werden kann.

8.4 Umgang mit personenbezogenen Daten in Corona-Testzentren

Bereits im 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 7.8 berichteten wir über zahlreiche Beschwerden, welche die Verarbeitung personenbezogener Daten in Corona-Testzentren betrafen. Diese rissen auch im aktuellen Berichtsjahr nicht ab. Zum Teil

fördert unsere Aufsichtstätigkeit in diesem Bereich erhebliche datenschutzrechtliche Defizite zu Tage. In einem Fall fertigte der Betreiber mehrerer Testzentren bei der Eröffnung von neuen Standorten jeweils eine Kopie der Datenbank mit den Daten der Testpersonen eines anderen Standortes an, die der neue Standort fortführen sollte. Dadurch konnten die Beschäftigten des neuen Standortes auf die personenbezogenen Daten der Testpersonen des anderen Standortes zugreifen, obwohl diese Daten für ihre Tätigkeit nicht erforderlich waren. Der Betreiber sah darin kein Problem. Dieses Verfahren sei eine Erleichterung für die Personen, die sich testen ließen, da sie sich nicht in jedem Standort neu registrieren lassen müssten. Dass diese rechtlich unerhebliche Einschätzung zusätzlich unzutreffend ist, zeigt eine uns vorliegende Beschwerde: Aufgrund einer Namensverwechselung wurde ein Testergebnis an eine Person gesendet, obwohl diese Person keinen Test hatte durchführen lassen. Sie hatte sich lediglich zuvor bei einem anderen Standort des Betreibers registrieren und testen lassen, welcher sich in einer anderen Stadt befindet. Da die Testzentren verpflichtet sind, positive Testergebnisse an das zuständige Gesundheitsamt zu melden, kann eine solche Namensverwechselung weitreichende Folgen für die betroffene Person haben.

Betreiber von Testzentren haben mitunter sehr viele Standorte, die je nach Pandemielage eröffnet und wieder geschlossen werden. Zwar ist der Wunsch nach einer effizienten Verwaltung nachvollziehbar. Dennoch gilt auch für Testzentren die Pflicht, durch geeignete technische und organisatorische Maßnahmen auch innerhalb eines Unternehmens sicherzustellen, dass Beschäftigte nur Zugriff auf solche personenbezogenen Daten haben, die für ihre jeweilige Tätigkeit erforderlich sind.

8.5 Private Kontaktaufnahme zu Patientin durch Arzt

Wiederholt melden uns Patientinnen Vorfälle, in denen ärztliches Personal im Nachgang zu einer Behandlung persönliche Nachrichten an die Patientin sendet (siehe hierzu Ziffer 4.9 dieses Berichts). Der Inhalt der Nachrichten weist dabei häufig keinen Bezug zu der Behandlung auf, sondern muss als persönliche Kontaktaufnahme verstanden werden. Spätestens, wenn auf das sympathische Auftreten der Patientin Bezug genommen wird, verlässt die Nachricht den professionellen Rahmen. Werden Messenger-Dienste eingesetzt, führt dies unter Umständen zusätzlich zu einer Übermittlung der Mobilfunknummer an internationale Konzerne. Ohne eine Einwilligung der Patientin zur Nutzung ihrer Kontaktdaten für private Zwecke sind derartige Kontaktversuche unzulässig. Patient:innen müssen sich darauf verlassen können, dass Behandelnde die im Rahmen der medizinischen Behandlung verarbeiteten Daten ohne anderweitige Absprachen ausschließlich für Zwecke des Behandlungsverhältnisses verwenden.

8.6 Zugriffsberechtigungen in SORMAS

Viele Gesundheitsämter in Deutschland – darunter auch die Gesundheitsämter in Bremen und Bremerhaven – setzten im Verlauf der Pandemie zur Erfassung und Bearbeitung der COVID-19-Fälle auf die vom Bundesgesundheitsministerium geförderte Fallbearbeitungssoftware SORMAS. Dank der Begleitung der Entwickler:innen durch eine Arbeitsgruppe, deren Mitglieder verschiedenen Datenschutzaufsichtsbehörden der Länder und der Behörde des Bundesdatenschutzbeauftragten angehören, wurden in den letzten Jahren wesentliche datenschutzrechtliche Verbesserungen der Software bewirkt. Allerdings geht der Bedarf der Gesundheitsämter stellenweise über die vorgesehene Verwendung der Software hinaus. So sieht die aktuelle Version von SORMAS (SORMAS-X) beispielsweise nicht vor, dass Stellen außerhalb des Gesundheitsamtes Zugriff auf Teilbereiche der in SORMAS gespeicherten Daten erhalten. Eine solche feingranulare Zugriffsberechtigung würde es beispielsweise Ordnungsämtern erlauben, für die Bearbeitung von Entschädigungsansprüchen die in SORMAS hinterlegten Isolationszeiten einzusehen, ohne Einblick in die weiteren Gesundheitsdaten, wie Symptome, Risikofaktoren und klinischer Verlauf, zu erhalten.

Diese softwareseitige Einschränkung nahmen wir zum Anlass, um bei den Gesundheitsämtern Bremen und Bremerhaven zu überprüfen, ob und gegebenenfalls in welchem Umfang externe Stellen Zugriff auf die in SORMAS gespeicherten Daten haben. Dabei stellte sich heraus, dass das Gesundheitsamt Bremerhaven Zugriffsrechte für das Bürger- und Ordnungsamt Bremerhaven geschaffen hatte, um die Einhaltung der Isolationsanordnungen zu überprüfen. Wir erläuterten, dass ein solcher Umfang der Zugriffsrechte zu weit ist und die mit einer informationstechnischen Berechtigung ausgestatteten Personen dadurch Zugriff auf sämtliche in SORMAS hinterlegten personenbezogenen Daten haben. Unsere Beratung führte dazu, dass die Zugriffsberechtigungen für das Bürger- und Ordnungsamt Bremerhaven im Sommer des Berichtsjahres entzogen wurden.

Auch im Gesundheitsamt Bremen bestanden entsprechende Zugriffsberechtigungen für einzelne Beschäftigte des Ordnungsamtes Bremen. Aufgrund der Tatsache, dass der Bund die Finanzierung für SORMAS zum 31. Dezember 2022 einstellte, nutzt das Gesundheitsamt Bremen nunmehr eine andere Software für die Fallbearbeitung, bei der keine Zugriffsrechte für Externe vorgesehen sind. Zu der Frage, ob das Gesundheitsamt Bremerhaven weiterhin an SORMAS festhält, lagen zum Redaktionsschluss noch keine näheren Informationen vor.

8.7 Smartspeaker in Praxisräumen

Im Berichtsjahr erreichte uns die Anfrage einer Arztpraxis zum Einsatz so genannter Smartspeaker in Behandlungszimmern und Büros. Ein Smartspeaker ist ein Lautsprecher, der Musik oder Sprache drahtlos überträgt und mit dem Internet verbunden ist. Die Steuerung des Geräts erfolgt in der Regel per Sprachsteuerung nach Nennung eines Codewortes.

Von der Installation solcher Geräte ist aus datenschutzrechtlicher Sicht insbesondere in Arztpraxen abzuraten. Zum einen enthalten die Geräte zahlreiche Mikrofone, welche dauerhaft aktiv geschaltet sind, damit bei der Nennung des Codewortes ein Befehl ausgeführt werden kann. Es findet somit eine kontinuierliche Datenverarbeitung bezüglich der Personen, die sich in den jeweiligen Räumen aufhalten, statt. Wird das Codewort ausgesprochen, findet eine Aufzeichnung alles Hörbaren und eine anschließende Transkription des Gesagten statt. Zudem wird die Aufnahme in vielen Fällen auf den Servern des Herstellers gespeichert, welche sich zumindest bei den Marktführern in der Regel in den Vereinigten Staaten von Amerika befinden. Für eine Datenübermittlung an eine Stelle außerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums gelten besondere datenschutzrechtliche Anforderungen, die in diesen Fällen regelmäßig nicht erfüllt werden. Die Datenübermittlung bewirkt außerdem, dass die jeweilige Praxis nicht mehr über die aufgezeichneten Daten verfügen kann. Die Daten werden durch den Hersteller unter anderem auch dazu verwendet, um die eigene Anwendung zu trainieren und um personalisierte Nutzer:innenprofile zu erstellen. Darüber hinaus besteht eine Fehleranfälligkeit bei der Erkennung des Codewortes. Dies kann dazu führen, dass ungewollt Gespräche aufgezeichnet und durch die Gerätehersteller verarbeitet werden. Eine Arztpraxis kann daher mitunter nicht mehr für die Vertraulichkeit der gesprochenen Patient:innendaten garantieren. Angesichts der Sensibilität von Gesundheitsdaten sowie der ärztlichen Schweigepflicht ist im Behandlungskontext daher kein Raum für den Einsatz so genannter Smartspeaker.

9. Soziales

9.1 Gemeldete Datenschutzverletzungen

Im Bereich Soziales wurden uns im Berichtsjahr insgesamt sieben Datenschutzverletzungen gemeldet. Die Meldungen betrafen unter anderem Fälle von Fehlsendungen, unbefugter Offenlegung personenbezogener Daten oder Diebstahl von Datenträgern.

9.2 Haus des Jugendrechts

Über eine Beratungsanfrage erhielten wir Kenntnis von dem Vorhaben, in Bremerhaven ein so genanntes Haus des Jugendrechts zu gründen. Ziel dieses Projektes ist es, durch eine engere Zusammenarbeit zwischen der Ortspolizeibehörde Bremerhaven, der Staatsanwaltschaft Bremen und der Jugendgerichtshilfe Bremerhaven die Bekämpfung der Jugendkriminalität zu verbessern. Hierzu soll möglichst schnell und abgestimmt auf Straftaten reagiert, frühzeitig kriminellen Karrieren entgegengewirkt und individuelle Hilfsangebote angeboten werden. Aus der zwischen den beteiligten Stellen geschlossenen Kooperationsvereinbarung geht hervor, dass unter Umständen auch andere Behörden und Institutionen hinzugezogen werden sollen. Der Austausch soll unter anderem in Form von Einzelfallbesprechungen erfolgen. Die Zusammenarbeit im Haus des Jugendrechts umfasst die Verarbeitung von höchst sensiblen personenbezogenen Daten. So richtet sich das Projekt an Minderjährige, deren personengezogene Daten von der Datenschutzgrundverordnung (DSGVO) in besonderer Weise geschützt werden. Darüber hinaus betrifft das Vorhaben Daten über strafrechtliche Verurteilungen und Straftaten sowie Sozialdaten. Auch diese Datenkategorien sind datenschutzrechtlich besonders geschützt.

Aus diesem Grund suchten wir das Gespräch mit Projektbeteiligten, um sie auf die datenschutzrechtlichen Schwierigkeiten hinzuweisen, die mit der geplanten Kooperation verbunden sind. Insbesondere Einzelfallbesprechungen zwischen mehreren Verantwortlichen bergen die Gefahr, dass personenbezogene Daten ausgetauscht werden, ohne dass für jeden Übermittlungsfall eine gesetzliche Grundlage besteht. Gegenüber Behörden vermutet der europäische Gesetzgeber zudem grundsätzlich, dass eine Einwilligung in die Verarbeitung der eigenen Daten nicht freiwillig erteilt werden kann (Erwägungsgrund 43). Mit der Freiwilligkeit würde ein konstitutives Element fehlen, das aus einer Äußerung eine Einwilligung im Sinne der DSGVO machen könnte, die Datenverarbeitungen rechtfertigen könnte. Wir wiesen die Verantwortlichen in diesem Zusammenhang auch darauf hin, dass das Bremische Polizeigesetz nicht vorsieht, dass Polizeibehörden Datenverarbeitungen auf Grundlage von Einwilligungen vornehmen können und rieten dringend dazu, die Verarbeitung personenbezogener Daten auf den Umfang der geltenden gesetzlichen Vorschriften zu beschränken.

Aufgrund der bestehenden Unsicherheiten teilten die Projektverantwortlichen mit, die Zusammenarbeit zunächst auf die Akteure Ortspolizeibehörde Bremerhaven, Staatsanwaltschaft und Jugendgerichtshilfe zu beschränken und weitere Stellen nur dann einzubeziehen, wenn dies im Interesse der betroffenen Personen liege, diesen aus der Einbeziehung in keiner Hinsicht Nachteile entstehen könnten und diese deshalb wirksam darin eingewilligt haben. Dazu sollen nun die hierfür benötigten Einwilligungsformulare erstellt

werden. Für die Klärung der noch offenen datenschutzrechtlichen Fragen sind weitere Gespräche geplant.

9.3 Weitergabe von Sozialdaten einer Beschäftigten

Eine Mitarbeiterin des Amtes für Soziale Dienste wandte sich mit einer Beschwerde an uns. Sie habe erfahren, dass sich Kolleg:innen über eine Mitteilung unterhalten hätten, die sie privat an den Kinder- und Jugendnotdienst gemacht habe. Hierüber zeigte sie sich besonders vor dem Hintergrund irritiert, dass durch interne Weisungen innerhalb des Amtes für Soziale Dienste eindeutig festgelegt ist, welches Sozialzentrum zuständig ist, wenn Beschäftigte selbst betroffen sind. Zuständig ist dann auf keinen Fall das Sozialzentrum, in welchem die betroffene Person tätig ist. Die Regelung dient der Umsetzung des Sozialgeheimnisses, das auch innerhalb eines Sozialleistungsträger zu berücksichtigen ist. Beschäftigte sollen auf die Vertraulichkeit sie selbst betreffender Sozialdaten vertrauen können und vor Stigmatisierung und Diskriminierung am Arbeitsplatz geschützt werden.

Die durch die oben genannte Weisung festgelegte interne Zuweisung wurde in dem berichteten Fall nicht eingehalten. Stattdessen wurde das Sozialzentrum über die Mitteilung an den Kinder- und Jugendnotdienst benachrichtigt, in welchem die betroffene Mitarbeiterin tätig ist. Dies führte dazu, dass unter Vorgesetzten und Kolleg:innen über die Belastungsfähigkeit der betroffenen Mitarbeiterin spekuliert wurde und Mitarbeiter:innen auf eine mögliche Krisensituation im familiären Umfeld der Mitarbeiterin hingewiesen wurden. Somit haben sich die Risiken, die bei rechtswidrigen Verarbeitungen von Sozialdaten von Beschäftigten bestehen, im vorliegenden Fall verwirklicht. Sowohl gegenüber dem Sozialzentrum, in welchem die betroffene Mitarbeiterin beschäftigt ist, als auch gegenüber dem Sozialzentrum, welches entgegen der internen Weisung mit diesem Kontakt aufnahm, stellten wir eine Verletzung des Sozialgeheimnisses fest. Wir gehen davon aus, dass dieser Vorfall das Bewusstsein für die besondere Schutzbedürftigkeit von Sozialdaten im Amt für Soziale Dienste schärfen konnte.

9.4 Projekt FamilienCard

Die bremische Landesregierung beschloss im Frühjahr des Berichtsjahres, allen Kindern und Jugendlichen im Land Bremen eine Guthabenkarte, die so genannte FreiKarte, aufgeladen mit 60 Euro, zur Verfügung zu stellen. Das Guthaben kann in verschiedenen Kultur- und Freizeiteinrichtungen eingelöst werden und soll die erheblichen Nachteile, die gerade die Kinder und Jugendlichen während der Corona-Pandemie erlitten, kompensieren. Wir wurden frühzeitig durch das bei der Senatskanzlei eingerichtete Projektbüro über das Vorhaben informiert und wiesen bereits in der Ausschreibungsphase auf die Vorschriften zu Datenschutz

und Datensicherheit hin. Nachdem ein Auftragnehmer gefunden war, stellte uns die Senatskanzlei die Umsetzung des Projektes vor. Im Zusammenhang mit der Beratung bei der Formulierung der Anschreiben an die Kinder und Jugendlichen fiel uns auf, dass für die Verarbeitung der personenbezogenen Daten der Minderjährigen noch keine Rechtsgrundlage bestand. Da die Anschreiben zunächst die Erhebung der Adressdaten der Minderjährigen bei den Meldeämtern voraussetzten, war es für die betroffenen Personen nicht möglich, vorab in die Datenverarbeitung einzuwilligen. Die Datenschutzgrundverordnung lässt eine Verarbeitung personenbezogener Daten jedoch nur zu, wenn eine Einwilligung erteilt wurde oder eine gesetzliche Verarbeitungsbefugnis existiert. Die Senatskanzlei sah zunächst davon ab, eine gesetzliche Grundlage für die Datenverarbeitung im Zusammenhang mit der FamilienCard zu initiieren, weil sie der Ansicht war, die Geschäftsverteilung des Senats sei hierfür ausreichend. Da die in der Sitzung des Senats am 16. August 2022 beschlossene Änderung der Geschäftsverteilung des Senats keine Rechtsvorschrift im Sinne von § 3 Absatz 1 Nummer 2 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung darstellt, stellten wir gegenüber den beiden verantwortlichen Stellen noch einmal ausdrücklich die Rechtswidrigkeit der geplanten Datenübermittlungen der Meldeämter an die Senatskanzlei sowie deren geplanter Verarbeitung durch die Senatskanzlei ohne vorherige Schaffung einer Rechtsgrundlage fest. In der Folge entschieden diese sich, neben der ohnehin geplanten Änderung der Meldedatenübermittlungsverordnung der Bremischen Bürgerschaft die Schaffung eines "Gesetzes zur Einführung der FamilienCard" vorzuschlagen, das am 15. September 2022 verabschiedet wurde. Die anschließende Verarbeitung der Meldedaten der Kinder und Jugendlichen erfolgte daher rechtmäßig.

Das Thema beschäftigt uns auch weiterhin. Aus Medienberichten erfuhren wir, dass es bei der Verteilung der FamilienCard in Bremerhaven in circa 5.000 Fällen zu fehlerhaften Übermittlungen kam. Wir setzten uns diesbezüglich erneut mit der Senatskanzlei in Verbindung. Zum Redaktionsschluss war die datenschutzrechtliche Aufklärung dieses Sachverhalts noch nicht abgeschlossen.

9.5 Datenerhebung zwecks Beantragung von Unterhaltsvorschuss

Durch einen Hinweis wurden wir auf die Ermittlungspraxis des Amtes für Soziale Dienste zur Prüfung von Ansprüchen nach dem Unterhaltsvorschussgesetz aufmerksam gemacht. Nach diesem Gesetz haben Kinder alleinerziehender Elternteile unter bestimmten Voraussetzungen die Möglichkeit, einen Unterhaltsvorschuss als staatliche Sozialleistung zu erhalten. Vor der Gewährung dieser Leistung hat die hierfür zuständige Abteilung des Amtes für Soziale Dienste unter anderem zu prüfen, ob die Elternteile tatsächlich getrennt leben und nicht in einer Weise Kontakt haben, die einem familiären Zusammenleben gleichkommt. Uns wurden Schreiben des Amtes für Soziale Dienste vorgelegt, in denen die Fragen zur Ermittlung dieses Umstands

derart weit gestellt waren, dass die Betroffenen sich in ihrer Intimsphäre verletzt fühlten. So sollten sie beispielsweise angeben, wie sie und der andere Elternteil zu der Übereinkunft gekommen seien, ein Kind miteinander zu zeugen.

Wir wandten uns daraufhin an das Amt für Soziale Dienste und trugen unsere datenschutzrechtlichen Bedenken vor. Es lag auf der Hand, dass die Fragen weiter eingegrenzt und Antwortmöglichkeiten zur Auswahl vorformuliert werden konnten. Das Amt für Soziale Dienste fragt nunmehr die zur Anspruchsprüfung notwendigen Angaben mithilfe eines einheitlichen Formulars ab, welches bereits vorformulierte Fragen sowie teilweise vorgegebene Antwortmöglichkeiten enthält. Darüber hinaus soll den betroffenen Personen in einem Anschreiben gezielt erläutert werden, zu welchem Zweck die Auskünfte eingeholt werden.

10. Bildung

10.1 Gemeldete Datenschutzverletzungen

Im Bereich Schulen und Bildung gab es im Berichtsjahr zwei Meldungen verantwortlicher Stellen nach Artikel 33 Datenschutzgrundverordnung. Auch erreichten uns erneut diverse telefonische und schriftliche Anfragen von Lehrer:innen, Schüler:innen sowie Erziehungsberechtigten. Hierbei handelte es sich vereinzelt um Beratungsanfragen öffentlicher Stellen, überwiegend jedoch um Anfragen betroffener Personen so wie zum Beispiel zur Datenverarbeitung durch Elternvertretungen oder zur Zulässigkeit der Übermittlung personenbezogener Daten durch Schulen.

10.2 Offen einsehbare personenbezogene Daten im Klassenraum

Gleich in zwei Fällen erreichten uns Eingaben zum Umgang mit personenbezogenen Daten von Schüler:innen. In den beiden unter den Ziffern 10.2.1 und 10.2.2 dieses Berichts geschilderten Fällen waren diese in den Klassenräumen dergestalt aufbewahrt beziehungsweise angebracht, dass auch Unbefugte hiervon Kenntnis nehmen konnten. Grundsätzlich ist der Schulbetrieb so zu gestalten, dass außer der Schulleitung und dem Schulsekretariat nur die jeweils für die Schüler:innen zuständigen Lehrkräfte Zugang zu den personenbezogenen Unterlagen haben. Die Aufbewahrung dieser Unterlagen muss so erfolgen, dass ein Zugriff Unbefugter ausgeschlossen ist.

10.2.1 Atteste et cetera

Die Landesbeauftragte für Datenschutz und Informationsfreiheit erreichte ein Hinweis, dass an einer beruflichen Schule in einem Klassenraum Atteste von Schüler:innen, Klausuren sowie Adresslisten gefunden worden seien. Bei den Dokumenten handelte es sich um Unterlagen mit personenbezogenen Daten, teilweise sogar um besonders schutzwürdige Daten gemäß Artikel 9 Datenschutzgrundverordnung. Entsprechend des Grundsatzes der Integrität und Vertraulichkeit müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Wir wiesen die Schule daher an, die Unterlagen unverzüglich in sichere Verwahrung zu nehmen. Dies wurde uns umgehend bestätigt. Darüber hinaus kündigte die Schule an, im Rahmen einer Dienstbesprechung die Kolleg:innen bezüglich des Umgangs mit personenbezogenen Daten zu sensibilisieren.

10.2.2 Verhaltensampeln

Eine weitere Anfrage betraf die Frage der datenschutzrechtlichen Zulässigkeit des Einsatzes von so genannten Verhaltensampeln im Unterricht. In einem Klassenraum einer Grundschule wurde das Verhalten der Schüler:innen mit Hilfe einer solchen Ampel bewertet, die Fotos der Schüler:innen nutzte. Die neben der Tafel angebrachten Fotos waren für alle Personen sichtbar, die sich in dem Klassenraum aufhielten. Im schulischen Bereich dürfen personenbezogene Daten von Schüler:innen verarbeitet werden, soweit dies zur Erfüllung des Unterrichts- und Erziehungsauftrages erforderlich ist. Hierunter fällt grundsätzlich auch die Bewertung des schulischen Verhaltens der Schüler:innen mit Hilfe solcher Verhaltensampeln. Datenschutzrechtliche Bedenken bestehen jedoch immer dann, wenn der Klassenraum auch von anderen Personen als den Schüler:innen der betreffenden Klasse und den Lehrer:innen, die diese unterrichten, genutzt wird und dadurch ein größerer Personenkreis von den auf der Verhaltensampel befindlichen Informationen Kenntnis erlangt. In diesen Fällen muss durch Maßnahmen wie das Abdecken der Ampel nach Unterrichtsschluss sichergestellt werden, dass nur eine klasseninterne Kenntnisnahme der Verhaltensampel möglich ist.

10.3 Videokonferenzsysteme im Schulkontext

Bereits in den beiden vorangegangenen Jahresberichten wiesen wir darauf hin, dass die Verwendung von Videokonferenzsystemen zu Unterrichtszwecken oder ähnlichen Zwecken im häuslichen Kontext datenschutzrechtlich problematisch ist. Die bereits im 3. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 9.6 aufgeworfenen Fragen wurden seitens der senatorischen Behörde und der Schulen weiterhin nicht oder nur unzureichend gelöst. Die

mehrfach angeforderte Datenschutz-Folgenabschätzung liegt uns mittlerweile vor. Jedoch ist diese nicht geeignet, unsere datenschutzrechtlichen Bedenken auszuräumen. Insbesondere werden die Risiken, die durch den Eingriff in die Privatsphäre und das häusliche Umfeld der überwiegend minderjährigen Nutzer:innen entstehen, nicht ausreichend gewürdigt. Auch fehlt es noch an der erforderlichen Aufklärung der betroffenen Personen zu den Risiken der Nutzung und über entsprechenden Abhilfemöglichkeiten. Insbesondere fehlt ein Hinweis an die Betroffenen bezüglich der Freiwilligkeit der Nutzung, sofern diese aus dem häuslichen Umfeld heraus erfolgt. Entgegen der Annahme der Senatorin für Kinder und Bildung kann die verpflichtende Nutzung des Videokonferenzsystems nicht auf die pandemiebedingte Änderung des § 72 a Bremisches Schulgesetz (BremSchulG) gestützt werden. Dort ist geregelt, dass für den Fall, dass im Schuljahr 2021/2022 aufgrund der Corona-Pandemie kein oder nur eingeschränkter Unterricht in der Schule stattfinden kann oder Schüler:innen, die besonders gefährdet sind, an COVID-19 zu erkranken, die Schule nicht besuchen können, die betroffenen Schüler:innen verpflichtet sind, an dem von der Schule ersatzweise oder ergänzend organisierten Unterricht auf Distanz teilzunehmen und die in diesem Rahmen gestellten Aufgaben zu erledigen. Im Übrigen unterblieb entgegen § 21 Absatz 3 Nummer 2 Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung die Unterrichtung der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) über die geplante Gesetzesänderung. Danach muss die LfDI über geplante Rechts- oder Verwaltungsvorschriften unterrichtet werden, sofern die Einführung oder Änderung einer Rechtsvorschrift die Verarbeitung personenbezogener Daten betrifft. Da die Durchführung von Videokonferenzen im schulischen Kontext offensichtlich auf die Regelung des § 72 a Absatz 2 BremSchulG gestützt werden sollte, hätte die LfDI aufgrund der datenschutzrechtlichen Relevanz an der geplanten Änderung des Schulgesetzes beteiligt werden müssen.

10.4 Microsoft 365 in Schulen

Eine weitere Anfrage betraf die Nutzung von Microsoft-Produkten an Schulen. Wir haben erhebliche datenschutzrechtliche Bedenken in Bezug auf die Nutzung von Microsoft 365, da die Möglichkeit einer datenschutzkonformen Verwendung bislang noch nicht dargelegt werden konnte. Insbesondere die fehlende Transparenz sowie die Vielzahl von verschiedenen Modulen, die diverse Nutzungsdaten erfassen und zumindest teilweise auch in die Vereinigten Staaten von Amerika übermitteln, sind datenschutzrechtlich problematisch (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffern 10.6 und 11.13 sowie 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 10.2).

10.5 Umgang mit personenbezogenen Daten von Elternvertretungen

Eine weitere Anfrage, die uns im Berichtsjahr erreichte, betraf die Datenverarbeitung im Rahmen der Elternvertretung beziehungsweise des Elternbeirates. Im Bremischen Schulverwaltungsgesetz ist geregelt, dass an jeder Schule mit minderjährigen Schüler:innen ein Elternbeirat gebildet wird. Die Beiräte sind nicht nur beratende Gremien, sondern auch Entscheidungsgremien in den Schulen. Personenbezogene Daten der Mitglieder von schulischen Entscheidungsgremien dürfen zu den in § 2 Bremisches Schuldatenschutzgesetz genannten Zwecken verarbeitet werden. Hierbei ist stets der Grundsatz der Erforderlichkeit zu beachten, das heißt die Erhebung, Verarbeitung und Nutzung der Daten ist auf das für die Zweckerreichung notwendige Maß zu beschränken. Eine Veröffentlichung der Namen und Kontaktdaten aller Elternsprecher:innen einer Schule ist daher regelmäßig unzulässig.

Auch in der Elternvertretungsarbeit selbst sind die datenschutzrechtlichen Vorschriften zu beachten. Regelmäßiger Kritikpunkt aus datenschutzrechtlicher Sicht ist hierbei die Nutzung offener E-Mail-Verteiler. Diese ist grundsätzlich unzulässig, da die E-Mail-Adressen personenbezogene Daten darstellen, die nicht ohne Einwilligung der betroffenen Personen offengelegt werden dürfen. Auch bei der Weiterleitung von E-Mails sollte dieser Punkt stets beachtet werden.

11. Wohnen, Verkehr und Umwelt

11.1 Gemeldete Datenschutzverletzungen

Im Bereich Bauen und Wohnen wurden uns in diesem Jahr von datenschutzrechtlich verantwortlichen Stellen 28 Datenschutzverletzungen gemeldet. Die Tendenz ist gegenüber den Vorjahren steigend und zeigt uns, dass in vielen Unternehmen sowie öffentlichen Stellen die technischen und organisatorischen Maßnahmen weiter ausgebaut und teilweise auch Beschäftigte verstärkt sensibilisiert werden müssten, da es sich in vielen Fällen um menschliches Fehlverhalten handelte. Erwähnenswert sind hier häufige Fälle des Fehlversandes von Protokollen, Mietangeboten, Interessent:innenbögen, Wirtschaftsplänen, Kündigungs- und Mietänderungsschreiben.

In den Bereichen Verkehr und Umwelt wurden uns seitens der verantwortlichen Stellen in elf Fällen Datenverletzungen gemeldet. In diesem Zusammenhang weisen wir erneut auf die Meldepflicht und die Meldefrist aus Artikel 33 Datenschutzgrundverordnung hin.

11.2 Rechtswidrige Verarbeitung der Daten von Mietinteressent:innen

Im letzten Jahr berichteten wir über ein datenschutzrechtliches Aufsichtsverfahren gegen eine bremische Wohnungsbaugesellschaft (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 15.2), das wir im Berichtsjahr fortführten. Unsere Prüfung ergab, dass mehr als 9.500 Daten über Mietinteressent:innen in rechtswidriger Weise verarbeitet worden waren. Bei mehr als der Hälfte der Fälle handelte es sich um die rechtswidrige Verarbeitung besonderer personenbezogener Daten wie Hautfarbe, Religionszugehörigkeit, sexuelle Orientierung und über den Gesundheitszustand, die von der Datenschutzgrundverordnung besonders geschützt sind. Auch hatte die Wohnungsbaugesellschaft Anträge Betroffener auf Transparenz über die Verarbeitung ihrer Daten bewusst konterkariert. Wir verhängten gegen die Wohnungsbaugesellschaft eine Geldbuße in Höhe von insgesamt rund 1,9 Millionen Euro (siehe hierzu Ziffer 4.2 dieses Berichts).

11.3 Aufbewahrung der Daten ehemaliger Mieter:innen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit nahm den Fall der rechtswidrigen Verarbeitung der Daten von Mietinteressent:innen (siehe hierzu Ziffer 11.2 dieses Berichts) zum Anlass, vermehrt Vermieter:innen hinsichtlich der Verarbeitung personenbezogener Daten zu sensibilisieren und Mieter:innen vor unrechtmäßigen Datenverarbeitungen zu schützen. Dabei nahmen wir zunächst das Thema Aufbewahrungspflichten der Daten ehemaliger Mieter:innen in unseren Fokus. In diesem Kontext hatten wir eine Beschwerde einer Petentin erhalten, die vermutete, dass sämtliche Ihrer Daten aus einem vor circa vier Jahren beendeten Mietverhältnis noch immer bei einer Wohnungsbaugesellschaft vorlagen.

Auf unsere Nachfrage teilte uns die Vermieterin mit, dass sie die Mieter:innenakten vor dem Hintergrund der Aufbewahrungspflichten nach §§ 147 Abgabenordnung (AO) und 257 Handelsgesetzbuch (HGB) noch zehn Jahre nach Beendigung des Mietverhältnisses aufbewahre. Demgegenüber rechtfertigen die genannten Vorschriften keineswegs die Aufbewahrung der kompletten Mieter:innenakte für die angegebene Dauer.

Die Aufbewahrungspflichten nach §§ 147 AO und 257 HGB beziehen sich vorwiegend auf steuerrelevante Unterlagen und Buchungsbelege. Informationen zu bereits erledigten Reparaturaufträgen und abgeschlossenen Nachbarschaftsstreitigkeiten gehören dazu beispielsweise nicht. In diesen Fällen gibt es keine rechtliche Legitimation, die Informationen bis zu zehn Jahre nach Beendigung eines Mietvertrages aufzubewahren. Vielmehr müssen

entsprechende Informationen spätestens bei Beendigung des Mietverhältnisses gelöscht werden.

Am Thema des Aufbewahrungsverhaltens auf Vermieter:innenseite arbeiten wir mit anderen datenschutzrechtlichen Aufsichtsbehörden zusammen, um eine Auflistung der Daten ehemaliger Mieter:innen zum Standard zu machen, die zur Erfüllung der Aufbewahrungspflichten nach den §§ 147 AO und 257 HGB tatsächlich erforderlich sind. Gemeinsam mit unseren Kolleg:innen aus den anderen Ländern planen wir in diesem Zusammenhang eine Orientierungshilfe mit Informationen und Hinweisen, die Mieter:innen unterstützt und darüber aufklärt, welche ihrer Daten ehemalige Vermieter:innen wie lange speichern dürfen. Auch Kleinvermieter:innen, denen es nicht möglich ist, regelmäßig eine steuerrechtliche Beratung einzuholen, sollen darin Hilfestellungen finden.

11.4 Bundeseinheitliche Gesetzesgrundlage für funkbasierte Messgeräte im Bereich Kaltwasser

Aufgrund ihrer bremischen Erfahrungen zu diesem Thema (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 15.3) schloss sich die Landesbeauftragte für Datenschutz und Informationsfreiheit im Berichtsjahr mit den datenschutzrechtlichen Aufsichtsbehörden aus sechs weiteren Bundesländern zusammen, um Hinweise an den Bundesgesetzgeber für eine datenschutzgerechte spezialgesetzliche Regelung im Bereich der Datenverarbeitung durch funkbasierte Kaltwasserzähler zu formulieren. Das in der Arbeitsgruppe erarbeitete Ergebnis wird der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vorgelegt.

Im Gegensatz zu den Bereichen Strom, Heizung und Warmwasser gibt es für den Bereich der Kaltwasserzähler noch keine spezifische Rechtsgrundlage für die Übertragung personenbezogener Daten per Funk. Im Interesse der Rechtssicherheit sollte dies geändert werden. Aus datenschutzrechtlicher Sicht sollte bundeseinheitlich festgelegt werden, dass nur personenbezogene Daten erhoben und verarbeitet werden dürfen, die für Abrechnungszwecke erforderlich sind oder deren Verarbeitung im öffentlichen Interesse wie dem der Trinkwasserhygiene liegt. Auch sollte normiert werden, dass Betreiber:innen der Funkwasserzähler Verbraucher:innen gegenüber darlegen müssen, welche ihrer personenbezogenen Daten verarbeitet und übermittelt werden, und warum dies zur Erfüllung der Aufgaben der Funkwasserzählerbetreibenden notwendig ist. Die Einhaltung ausreichender technischer und organisatorischer Sicherheitsvorkehrungen für die personenbezogenen Daten muss zur Pflicht gemacht werden, um Missbrauch durch unbefugte Dritte abwenden zu können. Löschfristen müssen gesetzlich bestimmt und klargestellt werden, dass deren Einhaltung verpflichtend ist.

11.5 Digitale Zähler mit integriertem Funkmodul

Zusammen mit einigen anderen Aufsichtsbehörden nahmen wir im Berichtsjahr an einem weiteren Projekt teil, in dem es um die digitale Datenverarbeitung per Funktechnologie in den Bereichen Strom, Heizung sowie Kalt- und Warmwasser ging.

Im Hinblick auf die aktuelle Energiekrise ist die Energieeffizienzrichtlinie (Richtlinie 2012/27/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur Energieeffizienz) stärker in den Fokus geraten. Darin wird auch das Ziel formuliert, den Menschen in der Europäische Union die Einsparung von Energie dadurch zu erleichtern, indem sie ihre jeweiligen aktuellen Energieverbräuche genau mitverfolgen können. Die Energieeffizienzrichtlinie wurde in den Bereichen Strom, Heizung und Warmwasser in Form des Messstellenbetriebsgesetzes, der Heizkostenverordnung und der Fernwärme- oder Fernkälte-Verbrauchserfassungs- und Abrechnungsverordnung bereits in deutsches Recht umgesetzt.

Wir konnten feststellen, dass die Thematik nicht nur bei Mieter:innen, sondern auch bei Vermieter:innen, Eigentümer:innen, Wohnungseigentumsgemeinschaften und Hausverwaltungen, sowie auch bei den Energieversorgen und Ableseunternehmen selbst zu Verunsicherungen führt. Daher haben die datenschutzrechtlichen Aufsichtsbehörden begonnen, datenschutzrechtliche FAQs im Zusammenhang mit der funkgesteuerten Erhebung und Ermittlung personenbezogener Daten zu erstellen, die auch die jeweiligen Unterschiede in den Verbrauchsarten Strom, Heizung, Kalt- und Warmwasser berücksichtigen.

11.6 Mitgliedschaft im Mieterschutzbund ist personenbezogenes Datum

Eine der zahlreichen Beschwerden im Miet- und Wohnbereich, die uns erreichte, stand im Zusammenhang mit einer Mitgliedschaft in einem Mieterschutzbund. Vorab hatten wir die Frage erhalten, ob es sich bei der Information über die Mitgliedschaft in einem Mieterschutzbund um ein personenbezogenes Datum handelt. Dies konnten wir zweifelsfrei bejahen, weil zu den Informationen, die sich auf eine natürliche Person beziehen, selbstverständlich auch sachliche Informationen zu der Person, wie die Mitgliedschaft in einem Mieterschutzbund gehören. Die Verarbeitung dieses personenbezogenen Datums bedarf deshalb nach Artikel 6 Datenschutzgrundverordnung einer Legitimationsgrundlage.

11.7 Frage nach Vermögensverhältnissen von Immobilieninteressent:innen

Eine weitere Fragestellung, die sich im Rahmen unserer Tätigkeit als datenschutzrechtliche Aufsichtsbehörde aufwarf, war die, ob und unter welchen Umständen Immobilienmakler:innen nach den Vermögensverhältnissen von Kaufinteressent:innen fragen dürfen.

Auch wenn die Interessenlagen bei Kauf und Anmietung einer Immobilie nicht vollständig mit denen von Mietinteressent:innen vergleichbar sind, können die Maßstäbe der Orientierungshilfe für Mietinteressent:innen[2] herangezogen werden. Daraus ergibt sich, dass im Falle einer Besichtigung zwecks eventuellen Erwerbs einer Immobilie die Frage nach den Vermögensverhältnissen noch ebenso wenig wie im Falle einer Wohnungsbesichtigung im Rahmen eines angestrebten Mietverhältnisses erforderlich ist.

11.8 Datenübermittlungen in Sachen Zensus 2022

Uns erreichten im Berichtsjahr einige Beschwerden zur Übermittlung personenbezogener Daten von Mieter:innen durch Wohnungseigentümer:innen an Zensusbehörden. In einem anderen Fall beschwerte sich ein Mitglied einer Wohungseigentümer:innengemeinschaft (WEG) bei uns über die Übermittlung von Daten wie unter anderem Adresse, Größe der Wohnung sowie die Heizungsart durch die Verwaltung der WEG an die Zensusbehörde. Diese Übermittlung erfolgte rechtmäßig, weil der WEG-Verwalter nach dem Gesetz zur Durchführung des Zensus im Jahr 2022 (ZensG 2022) hinsichtlich dieser Daten gegenüber der Zensusbehörde auskunftspflichtig war. Der § 24 Absatz 1 ZensG 2022 besagt, dass neben Eigentümer:innen auch Verwalter:innen Auskunftspflichtige für die Gebäude- und Wohnungszählung 2022 sind. Angaben wie Adresse, Größe, Heizungsart und Nettokaltmiete gehören zu den Erhebungsmerkmalen im Rahmen des § 10 ZensG 2022. Daher war die Übermittlung der Daten an die Zensusbehörde datenschutzrechtlich nicht zu beanstanden.

11.9 Massenhafte Fehldrucke im Verkehrsunternehmen

Eine der gemeldeten Datenschutzverletzungen bezog sich auf einen fehlerhaften Druckvorgang in einem Verkehrsunternehmen. Hunderte per Post ausgelieferte Kund:innenschreiben, die als Duplex-Druck erstellt worden waren, enthielten auf den jeweiligen Rückseiten personenbezogene Daten anderer Kund:innen. Die Vorder- und Rückseiten der jeweiligen Kund:innenschreiben passten insofern nicht mehr zusammen. Als

[2] https://www.datenschutz.bremen.de/sixcms/media.php/13/Orientierungshilfe_Mietausk%C3%BCnfte_V.06_20180207.pdf

das Unternehmen bei uns die Datenschutzverletzung meldete, hatte es nach eigenen Angaben die genaue Ursache für die entstandene Datenpanne noch nicht ermitteln können und plante daher, ein Testsystem aufzusetzen und zu versuchen, den fehlerhaften Druck nachzustellen.

In diesem Kontext weisen wir auf die Wichtigkeit umfassender technischer sowie organisatorischer Maßnahmen hin, die das Erstellen und Versenden von Kund:innenschreiben in datenschutzkonformer Weise ermöglichen. Vor Versand der Schreiben empfahlen wir zusätzlich die Sichtung der Schreiben im Vier-Augen-Prinzip, um das Risiko für Datenschutzverletzungen dieses Ausmaßes zu verringern.

11.10 Hackerangriff auf Energiedienstleister

Viele Bremer Vermieter:innen kontaktierten uns im Zusammenhang mit einem Hackerangriff auf einen großen deutschen Energiedienstleister, da Tausende Kund:innendatensätze betroffen waren. Dem Cyberangriff auf das Energieunternehmen, welches in der Regel im Rahmen einer Auftragsverarbeitung nach Artikel 28 Datenschutzgrundverordnung für die Wohnungsunternehmen und Einzelvermieter:innen tätig wird, folgte eine Erpressung des besagten Unternehmens. Folge des Angriffs war, dass es zu starken Beeinträchtigungen der IT-Infrastruktur kam und eine Vielzahl personenbezogener Daten auf einer so genannten Leak-Seite veröffentlicht wurde. Auch tausende Datensätze bremischer Mieter:innen waren betroffen. Dieser Fall führt drastisch vor Augen, wie wichtig es ist, Sicherheitsvorkehrungen im Rahmen der technischen und organisatorischen Maßnahmen zu verstärken und zu aktualisieren, um Angriffe dieser Art besser abwehren zu können.

11.11 Halter:innenabfrage beim Kraftfahrtbundesamt

Wir erhielten auch dieses Jahr wieder Beschwerden im Zusammenhang mit Abfragen über die Halter:innen von Fahrzeugen beim Kraftfahrtbundesamt. Der § 39 Straßenverkehrsgesetz (StVG) besagt, dass unter anderem die im § 39 Absatz 1 StVG aufgeführten Daten durch die Zulassungsbehörde oder das Kraftfahrtbundesamt zu übermitteln sind, wenn die Empfängerin beziehungsweise der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegen kann, dass sie oder er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. In diesen Fällen ist eine entsprechende Abfrage daher datenschutzrechtlich zulässig.

Halter:innenabfragen zu anderen Zwecken, wie zum Beispiel zur privaten Kontaktaufnahme, sind dagegen unzulässig. Im Berichtsjahr erfuhren wir von einem nicht unserer Zuständigkeit

unterliegenden Fall, in dem sich im Nachhinein herausstellte, dass ein Mann den zu einem Kennzeichen gehörenden Namen der Halterin des Kraftfahrzeuges nur erfragt hatte, um persönlichen Kontakt mit ihr aufzunehmen.

11.12 Zulässigkeit der Weitergabe von Luftbildaufnahmen

In unserem 3. Jahresbericht nach der Datenschutzgrundverordnung berichteten wir über die Voraussetzungen der Datenschutzkonformität von Luftbildaufnahmen. Bei diesen so genannten Orthofotografien handelt es sich um maßstabsgetreue Abbildungen der Erdoberfläche von oben, die um Verzerrungen durch Höhenunterschiede und die Erdkrümmung bereinigt wurden. In der Erstellung von Orthofotografien kann eine Verarbeitung personenbezogener Daten liegen, deren Zulässigkeit sich aus den Regelungen des bremischen Vermessungs- und Katastergesetzes bemisst.

Im Berichtsjahr erreichte uns eine Anfrage der zuständigen Behörde hinsichtlich der Weitergabe von Orthofotografien. Die Weitergabe stellt eine Verarbeitung personenbezogener Daten nach der Datenschutzgrundverordnung dar. Da Orthofotografien auch bei einer Pixelgröße von 10 cm je Bildpunkt bei der Wiedergabe von Häusern und Grundstücken noch personenbezogene Daten enthalten können, bedarf es für die Weitergabe einer Rechtsgrundlage. Das Gesetz über den Zugang zu digitalen Geodaten des Landes Bremen (Bremisches Geodatenzugangsgesetz) besagt, dass Orthofotografien grundsätzlich öffentlich bereit zu stellen sind. Bei bestimmten Aufnahmen kann die Veröffentlichung jedoch beschränkt werden, beispielsweise bei militärisch genutzten Gebieten zum Zwecke der Verteidigung oder aus Gründen der öffentlichen Sicherheit. Das Umweltinformationsgesetz schützt personenbezogenen Daten vor Veröffentlichung, sofern aus deren Bekanntgabe eine erhebliche Beeinträchtigung der Interessen der Betroffenen resultieren würde. Aufgrund der gewählten Pixelgrößen und des regelmäßig sehr entfernten Personenbezugs kann diese Gefahr bei Orthofotografien jedoch in den meisten Fällen ausgeschlossen werden. Auch nach dem Gesetz für die Nutzung von Daten des öffentlichen Sektors ergibt sich grundsätzlich keine Einschränkung für die Weitergabe von Orthofotografien.

12. Beschäftigtendatenschutz

12.1 Gemeldete Datenschutzverletzungen

Insgesamt wurden im Bereich Beschäftigtendatenschutz im Jahr 2022 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit 41 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet, wobei 38 Meldungen aus dem nicht öffentlichen Bereich und drei aus dem öffentlichen Bereich stammten. Neben 27 datenschutzrechtlichen Beschwerden erreichten uns zudem zahlreiche Anfragen von

Beschäftigten. Zu Beginn des Jahres betrafen diese überwiegend die Umsetzung der 3G-Regelung vor Betreten des Arbeitsplatzes sowie den Umgang von Arbeitgeber:innen mit den zur Verfügung gestellten 3G-Daten. Im Laufe des Berichtsjahres wurden nicht Pandemie bezogene Themen wieder präsenter. Unter anderem gab es diverse Anfragen, welche die Überwachung der Beschäftigten durch Arbeitgeber:innen betrafen. Insbesondere unzulässige Videoüberwachungen und Überwachungen mit dem weltweiten Positionsbestimmungssystem GPS stellen ein erhebliches Problem für die Beschäftigten dar.

12.2 Digitalisierung der Personalverwaltung

Die Landesbeauftragte für Datenschutz und Informationsfreiheit berät den Senator für Finanzen bei der Durchführung eines Projektes, das sich mit der Digitalisierung der Personalverwaltung befasst. Hinsichtlich der geplanten Einführung von elektronischen Personalakten wiesen wir unter anderem vor dem Start der Pilotierungsphase darauf hin, dass für eine datenschutzrechtlich zulässige Nutzung bereits vorab die Vergabe eindeutig festgelegter Berechtigungen für die Verarbeitung personenbezogener Daten notwendig sind, da der Zugriff auf personenbezogene Daten auf das erforderliche Maß beschränkt sein muss. Grundsätzlich gilt dabei, dass nur die zur Benutzung eines Datenverarbeitungssystems mit personenbezogenen Daten Berechtigten auf die dort zu verarbeitenden personenbezogenen Daten in dem jeweils für die in ihrer individuellen Zuständigkeit zu erbringenden Verarbeitungstätigkeiten erforderlichen Umfang Zugriff haben dürfen. So wird sichergestellt, dass die personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Nur wenn diese Anforderungen erfüllt werden, kann ein datenschutzkonformer Betrieb gewährleistet werden.

12.3 Zugriff auf personenbezogene E-Mail-Postfächer von Beschäftigten

Bei längerer Abwesenheit von Beschäftigten oder auch bei Beendigung des Arbeitsverhältnisses stellt sich regelmäßig die Frage, wie mit dem personalisierten E-Mail-Konto der oder des Beschäftigten zu verfahren ist. Diese Problematik war auch Anlass einer Beschwerde, die eine in der bremischen Verwaltung beschäftigte betroffene Person an uns richtete. Aufgrund einer längeren Abwesenheit war die Dienststelle davon ausgegangen, dass eine Rückkehr an den Arbeitsplatz nicht erfolgen werde. Daraufhin wurde Einsicht in das dienstliche E-Mail-Postfach genommen, weil dies zur Erledigung der dienstlichen Aufgaben als erforderlich angesehen wurde. Eine Regelung zur Vorgehensweise in derartigen Fällen enthält § 13 Absatz 4 und Absatz 5 der Verwaltungsvorschrift zu Kommunikation und Dokumentenverwaltung in der Freien Hansestadt Bremen (VV KommDok). Wir wiesen die Dienststelle daher darauf hin, dass im Fall einer nicht vorhersehbaren Abwesenheit vorrangig und unverzüglich nach Bekanntwerden der Abwesenheit von der in der Dienststelle

zuständigen Person der vorgegebene automatische Antworttext ohne Zugriffsmöglichkeit auf das E-Mail-Postfach über das E-Mail-Kontenpflegetool einzurichten ist. Eine Öffnung des E-Mail-Postfaches und die Einsichtnahme in einzelne E-Mails dürfen nur erfolgen, wenn zwingende dienstliche Gründe vorliegen und den Anforderungen des § 13 Absatz 5 VV KommDok entsprochen wird. Hierbei ist zu beachten, dass die Öffnung des E-Mail-Postfaches nur auf Basis eines vereinbarten Verfahrens erfolgen darf und der betroffenen Person zur Kenntnis zu geben ist. Es müssen zwingende dienstliche Gründe für die Öffnung vorliegen. Die Einsichtnahme in einzelne E-Mails darf nur bei Vorliegen zwingender dienstlicher Gründe und im Vier-Augen-Prinzip erfolgen. Vorrangig ist die Absenderin oder der Absender (falls bekannt) zu bitten, die betreffende E-Mail erneut an eine alternative E-Mail-Adresse (zum Beispiel Stellvertretung oder Funktionspostfach) zu senden. Es muss bei der Einsichtnahme gewährleistet sein, dass die Grundrechte und Grundfreiheiten der betroffenen Person gewahrt werden. Insbesondere sind offensichtlich private oder vertrauliche E-Mails unverzüglich ungeöffnet zu löschen.

12.4 Abfrage und Speicherung des Impfstatus von Beschäftigten

Wie bereits in den letzten beiden Jahren erreichten uns diverse Anfragen und Beschwerden im Pandemiekontext. Diese betrafen vorwiegend die Umsetzung der so genannten 3G-Regelung durch Arbeitgeber:innen. Im November 2021 erfolgte eine Änderung des Infektionsschutzgesetzes, wodurch Arbeitgeber:innen verpflichtet wurden, im Rahmen der Zutrittskontrolle einen 3G-Nachweis zu verlangen. Diese Norm stellt selbst keine Rechtsgrundlage für eine direkte Abfrage des Impfstatus bei den Beschäftigten dar, da der Nachweis einer ausreichenden Impfung nur eine der drei Nachweismöglichkeiten darstellt (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 10.3). Auch wurden vielfach bei der Zutrittskontrolle Daten erhoben, die zur Zweckerreichung nicht erforderlich waren. Bei Impfnachweisen war dies regelmäßig die Angabe des Impfstoffes, bei Testnachweisen war hingegen mehrfach die zu lange Speicherdauer problematisch.

Seit einer weiteren Änderung des § 28 b Infektionsschutzgesetz (IfSG) mit Wirkung zum 20. März 2022 bietet dieser für die Erfassung des 3G-Status durch Arbeitgeber:innen keine Rechtsgrundlage mehr. Auf Beschwerden Beschäftigter hin forderten wir im Anschluss daran diverse Verantwortliche zur Löschung der Daten. Die erfolgte Löschung wurde uns in aller Regel zeitnah bestätigt.

Zu den Themen Zutrittskontrolle und Löschverpflichtungen erhielten wir neben den genannten berechtigten Beschwerden betroffener Beschäftigter auch Beratungsanfragen von Arbeitgeber:innen, sodass in diesen Fällen Rechtsverstöße vermieden werden konnten.

12.5 Datenschutz bei Ressortumfragen

Bei eingeschränkt dienstfähigen Beamtinnen und Beamten erfolgt eine Prüfung einer anderweitigen Verwendungsmöglichkeit vor Versetzung in den Ruhestand. Entsprechende Umfragen müssen unter Einhaltung des Personaldatenschutzes in anonymisierter Form erfolgen, wobei auf Grundlage des amtsärztlichen Gutachtens eine Kurzbeschreibung der gesundheitlichen Einschränkungen vorgenommen werden soll. Eine Formulierung in einer Ressortumfrage, durch die eine konkrete Aussage zu dem Gesundheitszustand getroffen wurde, war Anlass für eine Beschwerde der betroffenen Person. Regelmäßig genügt es bei der Prüfung der anderweitigen Verwendung die konkreten Leistungseinschränkungen mitzuteilen. Eine Offenbarung der Diagnose oder auch von detaillierten Krankheitsbefunden ist hingegen für den Zweck der Suchanfrage als Konkretisierung des gesetzlichen Grundsatzes "Weiterverwendung vor Versorgung" weder erforderlich noch zulässig. Die Dienststellen, denen die Daten übermittelt wurden, wurden daher aufgrund unseres Tätigwerdens vom Senator für Finanzen zur Löschung aufgefordert. Auch wurden wir darüber informiert, dass eine Überprüfung der Formulierungen in dem Rundschreiben des Senators für Finanzen Nummer 08/2016 zum Umgang mit eingeschränkt dienstfähigen Beamtinnen und Beamten erfolgen soll, insbesondere hinsichtlich des Begriffs "gesundheitliche Einschränkungen". Daneben befürworten wir eine klarstellende Formulierung zum Verzicht auf die Mitteilung von Diagnosen und Befunden.

12.6 Video- und Audioüberwachung von Beschäftigten

Gleich in mehreren Fällen erreichten uns Informationen darüber, dass Beschäftigte durch Kameras überwacht wurden. So erfolgte gleich in zwei Fällen eine umfassende Überwachung von Büroräumen, wodurch sich die Beschäftigten einem permanenten Überwachungsdruck ausgesetzt sahen. In anderen Fällen wurden Produktionshallen inklusive der Arbeitsplätze der Beschäftigten gefilmt, um möglichen Verfehlungen von Beschäftigten oder Diebstählen entgegenzuwirken, ohne dass hierfür konkrete Anhaltspunkte vorlagen. Auch in Geschäften wurden Kameras installiert, welche die Beschäftigten durchgehend bei ihrer Arbeit filmten. In einigen Fällen erfolgte die Installation darüber hinaus ohne vorherige Information der Beschäftigten und ohne die erforderliche Beschilderung, welche auf die Videoüberwachung hinweist.

In allen Fällen wiesen wir darauf hin, dass grundsätzlich personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Insbesondere die Erforderlichkeit des Einsatzes von Kameras konnte von den Verantwortlichen regelmäßig nicht dargelegt werden. Eine dauerhafte Videoüberwachung am

Arbeitsplatz greift erheblich in die Persönlichkeitsrechte der Beschäftigten ein, auch entsteht hierdurch ein unzulässiger Überwachungsdruck. Daher dürfen dauerhafte Arbeitsplätze oder Bereiche, in denen sich Beschäftigte über längere Zeiträume aufhalten, grundsätzlich nicht kameraüberwacht werden. Eine Videoüberwachung zum Zweck der Verhaltens- oder Leistungskontrolle ist gänzlich unzulässig. Wird als Zweck der Überwachung die Prävention von Diebstählen durch Beschäftigte angegeben, so ist zu beachten, dass zur Aufdeckung von Straftaten personenbezogene Daten von Beschäftigten nur nach der Maßgabe des § 26 Absatz 1 Satz 2 Bundesdatenschutzgesetz (BDSG) verarbeitet werden dürfen. Eine Datenverarbeitung ist daher allenfalls dann zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffenen Personen im Beschäftigungsverhältnis eine Straftat begangen haben, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt. Eine Videoüberwachung zu dem Zweck, befürchteten Verfehlungen von Beschäftigten zu begegnen ist hingegen unzulässig. Auch kann eine dauerhafte Videoüberwachung nicht auf § 26 Absatz 1 Satz 2 BDSG gestützt werden.

Durch unser Tätigwerden konnte in zwei Fällen erreicht werden, dass die beanstandeten Videoüberwachungsanlagen zeitnah abgeschaltet wurden. In den anderen Fällen führten wir unter anderem Vor-Ort-Kontrollen durch und wirken weiter auf die Einhaltung der datenschutzrechtlichen Vorgaben hin.

12.7 Nutzung von WhatsApp im betrieblichen Kontext

Bereits in unserem vorherigen Jahresbericht informierten wir darüber, dass die Nutzung von WhatsApp für die Übermittlung von Beschäftigtendaten in jedem Fall unzulässig ist, da hierdurch Kontaktdaten ohne ausreichende Rechtsgrundlage auf Server außerhalb der Europäischen Union übermittelt werden (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 10.4). Dennoch erreichten uns auch in diesem Jahr wieder Anfragen und Beschwerden betroffener Beschäftigter zur Nutzung von WhatsApp im Beschäftigungsverhältnis.

In einem Fall informierte die Geschäftsführung die Beschäftigten eines Unternehmens in einer WhatsApp-Gruppe über die Krankmeldung einer Kollegin. Hier war neben der Nutzung des problematischen Übermittlungsmediums auch die Übermittlung der personenbezogenen Daten selbst mangels Rechtsgrundlage rechtswidrig. Zwar ist die betriebsinterne Information über Abwesenheitszeiten grundsätzlich für die Durchführung des Beschäftigungsverhältnisses erforderlich, nicht erforderlich und damit unzulässig ist jedoch die Information über konkrete Abwesenheitsgründe, wie zum Beispiel Krankheit oder Urlaub. Da die übermittelte Information über die Krankmeldung ein Gesundheitsdatum zum Gegenstand hatte, das zu den

besonderen Kategorien personenbezogener Daten nach Artikel 9 Datenschutzgrundverordnung gehört, handelte es sich um eine schwerwiegende Rechtsverletzung.

13. Medien, Telemedien, Digitalisierung

13.1 Gemeldete Datenschutzverletzungen

Von datenschutzrechtlich verantwortlichen Stellen aus den Bereichen Medien und Telemedien wurden uns im Berichtsjahr vier Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet.

13.2 Koordinierte Prüfung der Webseiten von Medienunternehmen

Im 3. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 18.2 und im 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 17.2 berichteten wir über die koordinierte Prüfung der Webseiten von Medienunternehmen, an der die Landesbeauftragte für Datenschutz und Informationsfreiheit gemeinsam mit den datenschutzrechtlichen Aufsichtsbehörden aus zehn weiteren Bundesländern teilnahm. Während der gesamten Laufzeit dieser koordinierten Prüfung wurden gemeinsame Prüfkriterien, vor allem zum Thema Tracking, entwickelt und verschiedene Dienste, die auf sämtlichen Webseiten eingebunden werden, gemeinsam geprüft.

Die meisten von uns angeschriebenen Medienunternehmen nahmen entsprechende Änderungen vor und passten Einstellungen ihrer Webseite an. Noch nicht zufriedenstellend sind die meisten so genannten Cookie-Banner. Häufig ist es Nutzer:innen der Webseiten nur unter erschwerten Bedingungen möglich, deutlich zu machen, dass sie die Verwendung von Cookies ablehnen. Die Möglichkeit zum Erteilen sowie zum Ablehnen einer Einwilligung sollte jedoch gleichwertig gestaltet sein. Aus Sicht der Nutzenden darf es nicht komplizierter oder aufwändiger sein, die Einwilligung abzulehnen als sie zu erteilen. Dabei ist es grundsätzlich durchaus möglich, Cookie-Banner mehrschichtig zu gestalten, also detailliertere Informationen erst auf einer zweiten Ebene des Banners mitzuteilen, zu der die Nutzenden über einen Button oder Link gelangen. Wenn jedoch bereits auf der ersten Ebene des Cookie-Banners ein Button existiert, mit dem eine (informierte) Einwilligung für verschiedene Zwecke erteilt werden kann, sollte auch auf dieser ersten Ebene die Möglichkeit bestehen, die Einwilligung abzulehnen. Wichtig ist, dass die beiden Optionen Akzeptieren oder Ablehnen gleichwertig gestaltet werden. Zu betonen ist in diesem Zusammenhang, dass technisch nicht notwendige Dienste beim Aufruf einer Webseite ohnehin nicht von Beginn an aktiviert sein dürfen, da die Datenschutzgrundverordnung für die Einwilligung eine zeitlich vor der Datenverarbeitung

liegende unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung voraussetzt.

13.3 So genannte Facebook-Fanpages

Mit Schreiben vom 25. April 2022 wiesen wir diejenigen obersten Landesbehörden der Freien Hansestadt Bremen an, die eine so genannte Facebook-Fanpage betreiben, auf die derzeitige Rechtslage und Rechtsprechung zum Thema "Betreiben einer Facebook-Fanpage" hin. Das Betreiben einer solchen Fanpage ist noch immer nicht datenschutzkonform möglich. Die Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 5. Juni 2018, Aktenzeichen C-210/16) und die sich daran anschließenden Urteile des Bundesverwaltungsgerichts (Urteil vom 11. September 2019, Aktenzeichen 6 C 15.18) und des Oberverwaltungsgerichts Schleswig (Urteil vom 25. November 2021, Aktenzeichen 4 LB 20/13) bestätigten allesamt, dass ein datenschutzkonformer Betrieb einer Facebook-Fanpage unter den aktuellen Umständen nicht möglich ist. Wir informierten die betreffenden Stellen unter anderem über das Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 18. März 2022 (aktualisiert im November 2022), das eine Unzulässigkeit des Fanpagebetriebes aufgrund von Verstößen gegen Datenschutzvorschriften feststellt. Demzufolge wiesen wir die angeschriebenen Landesbehörden auf die Erforderlichkeit der Deaktivierung der von ihnen betriebenen Facebook-Fanpages hin und machten diese insbesondere darauf aufmerksam, dass eine datenschutzrechtliche Mitverantwortung der Betreiber:innen von Facebook-Fanseiten besteht. Für den Fall des Weiterbetriebs der Fanpages über den 1. Juli 2022 hinaus behielten wir uns weitere aufsichtsbehördliche Mittel vor.

Die Senatskanzlei übersandte uns eine ausführliche Stellungnahme, der sich die anderen angeschriebenen Landesbehörden anschlossen. Sie teilte mit, dass sich die bremische Senatskanzlei mit den anderen Ländern und insbesondere mit dem vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) ebenfalls in dieser Sache angeschriebenen Bundespresseamt im engen Austausch stehe, um für die aufgeworfene Problematik eine Lösung zu finden. Das Bundespresseamt befinde sich noch im Prüfungsverfahren und werde den eigenen Facebook-Auftritt bis zur Klärung sämtlicher Sach- und Rechtsfragen weiterhin aufrechterhalten. Die bremische Senatskanzlei sei an datenschutzkonformen Lösungen interessiert, halte aber gleichzeitig ein bundeseinheitliches Vorgehen für angemessen, weil sich die Fragen in der gesamten Bundesrepublik Deutschland gleichermaßen stellten. Aus diesem Grund lehne sie die Deaktivierung der Fanpages allein durch die bremischen Behörden ab und werde das Ergebnis der Prüfung des Bundespresseamtes abwarten. Wir stellen mittlerweile fest, dass das Bundespresseamt als

erste Reaktion auf die Löschungsaufforderung des BfDI seit kurzem Informationen zumindest auch auf dem datenschutzfreundlichen Dienst Mastodon[3] teilt.

13.4 Dark Patterns

Am 14. März 2022 nahm der Europäische Datenschutzausschuss (EDSA) in seiner 62. Sitzung die Leitlinien[4] zu so genannten Dark Patterns bei der Oberflächengestaltung sozialer Netzwerke an. Unter dem Ausdruck Dark Patterns ist die Gestaltung von Webseiten 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. Meist ist hier nicht von einer freiwilligen und informierten Einwilligung auszugehen, wie sie von der Datenschutzgrundverordnung gefordert wird, um die Verarbeitung personenbezogener Daten zu rechtfertigen.

Bekannte Manipulationspraktiken sind Cookie-Banner, bei denen die Auswahl-Buttons in unterschiedlichen Größen oder Farben dargestellt werden (Beispiel: Der Akzeptieren-Button ist groß und grün, der Ablehnen-Button ist deutlich kleiner oder versteckt und in einer unscheinbaren Farbe hinterlegt). Die Option Ablehnen muss 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. Häufig ist es Nutzenden nicht einmal möglich, Cookies auf erster Ebene abzulehnen. Stattdessen müssen sie sich durch komplizierte Datenschutz-Einstellungen klicken, um ablehnen zu können. Auch stellen wir bei vielen Webseiten fest, dass personenbezogene Daten der Nutzenden bereits beim Aufruf der Webseite an Drittanbieter übermittelt werden, ohne dass der Cookie-Banner von den Nutzenden überhaupt bedient worden wäre.

Durch diese (teilweise unbewussten) Manipulationen werden Nutzende in ihrem Verhalten und ihrer Fähigkeit, ihre Daten effektiv zu schützen, erheblich beeinträchtigt. Häufig verstoßen diese Praktiken gegen die Datenschutzgrundverordnung, wobei jeder Fall im Einzelnen geprüft werden muss. Beschwerden zu solchen Dark Pattern-Fällen häufen sich und wir erhalten von Nutzenden viele entsprechende Hinweise. Außerdem erfahren wir auch auf anderen Wegen von Dark Pattern. Unsere Erfahrung ist, dass viele Webseitenbetreibende ihre Webseiten umgehend umgestalten, nachdem wir ein datenschutzrechtliches Prüfverfahren eingeleitet haben. Leider gibt es aber auch andere Webseitenbetreibende, die entweder nicht reagieren

[3] https://social.bund.de/@Bundespresseamt
[4] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en

oder an ihrer Webseite keine datenschutzrechtlichen Änderungen vornehmen. In diesen Fällen machen wir von unseren datenschutzrechtlichen Befugnissen Gebrauch.

13.5 2G/3G-Kontrollen von digitalen Zertifikaten / CovPass-App

Auch noch im Berichtsjahr als dem dritten Pandemiejahr erreichten uns mehrere Beschwerden, die die 2G/3G-Kontrollen digitaler Zertifikate in der so genannten CovPass-App betrafen. Dabei handelte es sich um einige Vorfälle beim 2G-Check auf dem Weihnachtsmarkt und im Behördenzentrum in der Stresemannstraße. Alle Betroffenen gaben an, dass für die Kontrolle der digitalen Zertifikate nicht die dafür vorgesehene CovPassCheck-App genutzt worden war. Anstatt die QR-Codes zu scannen, hätten die Beschäftigten des Sicherheitsdienstes auf den Bildschirmen der persönlichen Smartphones der Betroffenen gescrollt und die Daten mit dem Lichtbildausweis abgeglichen. Mit dieser Art und Weise der Kontrolle wurden folglich mehr Daten (etwa Geburtsdatum und Datum der Impfung) unfreiwillig preisgegeben als erforderlich war.

Wir schrieben die verantwortlichen Stellen an und informierten sie über die Rechtslage und wiesen dabei insbesondere darauf hin, dass es sich bei den abgerufenen Informationen um sensible Gesundheitsdaten handelt. Dass Beschäftigte des Sicherheitsdienstes auf dem Smartphone der Betroffenen herumwischen und -tippen, stellt bei Nichtvorliegen einer Einwilligung der Betroffenen einen Verstoß gegen Datenschutzrecht dar. Das Scannen des QR-Codes gibt weniger Informationen preis als die Abfrage der Detailangaben, da insbesondere nicht mitgeteilt wird, ob eine Impfung oder Genesung vorliegt. Zudem wird nicht übermittelt, wann das jeweilige Ereignis eingetreten ist. Für das wegen der Möglichkeit der Nutzung der Scanfunktion nicht erforderliche Aufrufen der Detailangaben eines Zertifikats in der CovPass-App ist keine Rechtsgrundlage ersichtlich. Zudem ist diese Art der Überprüfung nicht mit dem Grundsatz der Datenminimierung zu vereinbaren. Die CovPass-App wurde unter anderem gerade aus dem Datensparsamkeits-Gedanken heraus entwickelt und eingesetzt. Viele Menschen nutzen diese App primär aus Datenschutzgründen. Selbst in der Arbeitshilfe des Senators für Finanzen, die uns vorgelegt wurde, wird erklärt, dass vorrangig die digitalen Zertifikate mit dem digitalen Check der CovPass-App einzulesen sind. Nur wenn kein digitales Zertifikat vorliegt, sollen der Impfausweis beziehungsweise ein anderer manueller Nachweis eingesehen werden dürfen.

13.6 Mitschnitt eines Telefonats und Veröffentlichung im Internet

Uns erreichte eine Beschwerde wegen der Veröffentlichung eines Mitschnittes eines privaten Telefonates über einen Anbieter im Internet, der anschließend über soziale Medien verbreitet worden war. Wir kontaktierten die hierfür verantwortliche Person und konnten erreichen, dass

der Telefonatsmitschnitt von der Anbieterseite entfernt wurde. Nach unserem Kenntnisstand wird parallel zu dem bei uns durchgeführten datenschutzrechtlichen Aufsichtsverfahren durch die Polizei ermittelt, da die betroffene Person Strafanzeige erstattet hatte.

13.7 Verbot Veröffentlichung Sitzungsmitschnitte von Beiräten

Das Verwaltungsgericht Bremen bestätigte mit Urteil vom 10. Oktober 2022 Löschungsanordnungen der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI), die die Veröffentlichung von Mitschnitten und Screenshots von per Online-Videokonferenz abgehaltenen Beiratssitzungen betrafen.

Die LfDI hatte den Kläger unter anderem aufgefordert, auf der von ihm betriebenen Internetseite veröffentlichte YouTube-Videos und Screenshots zu löschen. Diese betrafen Mitschnitte einer per Videokonferenz abgehaltenen Beiratssitzung. Das Verwaltungsgericht bestätigte die Rechtmäßigkeit dieser Anordnungen. Der Kläger habe nicht aus einem berechtigten Interesse heraus gehandelt. Ein solches werde nicht bereits dann verfolgt, wenn eine Privatperson eine eigene Internetseite betreibe und auf dieser ihre eigene Meinung darbiete. Auch spreche gegen ein solches Interesse, dass die Inhalte primär darauf abzielten, die beteiligten Personen zu diffamieren. Angesichts der öffentlichen digitalen Zugänglichkeit der Beiratssitzung, der Protokollierung von Beiratssitzungen und der Tatsache, dass diese der Öffentlichkeit im Internet zur Verfügung gestellt werde, sei die Veröffentlichung durch den Kläger nicht zur Information der Öffentlichkeit erforderlich. Zusätzlich überwögen die Interessen und Grundrechte der abgebildeten Beiratsmitglieder, die durch Veröffentlichungen im Internet besonders gefährdet seien, weil die veröffentlichten Informationen auf diese Weise einem unkontrollierbaren und unbeschränkbaren Personenkreis zur Verfügung gestellt würden. Das Verwaltungsgericht erklärte auch die Anordnungen für rechtmäßig, die den Kläger dazu verpflichten, entsprechende Veröffentlichungen auch in Zukunft zu unterlassen.

14. Werbung

14.1 Gemeldete Datenschutzverletzungen

Von Unternehmen aus dem Bereich Werbung erhielten wir im Berichtsjahr keine Meldungen über Verletzungen des Schutzes personenbezogener Daten. Dagegen erreichten uns 24 Beschwerden, die solche Unternehmen betrafen.

14.2 Betroffenenrechte

Im Bereich Werbung und Adresshandel erreichten uns erneut zahlreiche Beratungsanfragen Betroffener. Dabei ging es insbesondere um die Abbestellung von Newslettern, den

unerwünschten Erhalt von Kundenzufriedenheitsbefragungen und Fragen zum Umfang der Rechte der von Datenverarbeitungen durch Unternehmen der Werbe- und Adresshandelsbranche Betroffenen. Bei diesen in der Datenschutzgrundverordnung (DSGVO) verankerten Rechten handelt es sich zum Beispiel um Auskunftsrechte der betroffenen Personen und das Recht auf Löschung personenbezogener Daten.

Wir informierten die Betroffenen in diesem Zusammenhang darüber, dass Verantwortliche verpflichtet sind, den Betroffenen unter anderem Auskunft darüber zu erteilen, welche ihrer Daten verarbeitet werden, zu welchem Zweck dies geschieht, für welche Dauer die Daten gespeichert werden und woher die Daten stammen. Zudem machten wir sie darauf aufmerksam, dass es sich auch bei dem Erhalt von so genannten Kundenzufriedenheitsbefragungen um Werbung handelt, sodass die genannten Rechte uneingeschränkt gelten.

Im Zusammenhang mit so genannter Direktwerbung, also der Kontaktaufnahme von Unternehmen, Parteien, Verbänden oder Vereinen mit ihren Vertragspartner:innen oder Mitgliedern, die dazu dienen, den Absatz zu steigern oder die Ziele dieser Stellen zu fördern, wiesen wir auf Artikel 21 DSGVO hin. Danach haben die Betroffenen das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einzulegen. Widersprechen die Betroffenen der Verarbeitung für Zwecke der Direktwerbung, dürfen ihre personenbezogenen Daten von den verantwortlichen Stellen nicht mehr hierfür verarbeitet werden.

14.3 Direktwerbung mit Einwilligung

Wir erhielten erneut Beschwerden über Unternehmen, insbesondere aus dem Online-Versandhandel, die Betroffene zu Werbezwecken telefonisch oder per E-Mail kontaktiert hatten, obwohl die Betroffenen hierfür keine Einwilligung erteilt hatten.

Bereits im 4. Jahresbericht nach der Datenschutzgrundverordnung unter Ziffer 14.3 hatten wir zu diesem Thema auf eine Entscheidung des Oberverwaltungsgerichts Saarlouis vom 16. Februar 2021 hingewiesen, wonach die wettbewerbsrechtlichen Bewertungsmaßstäbe des Gesetzes gegen den unlauteren Wettbewerb (UWG) auch im Rahmen der Interessenabwägung nach Artikel 6 Absatz 1 Buchstabe f Datenschutzgrundverordnung zu berücksichtigen sind. Diese Entscheidung hat mittlerweile auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder aufgegriffen und die Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutzgrundverordnung[5] unter

[5] https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf

Einbeziehung der wettbewerbsrechtlichen Vorschriften angepasst. Danach ist Werbung mit einem Telefonanruf bei Verbraucher:innen ohne deren vorherige ausdrückliche Einwilligungen oder bei sonstigen Marktteilnehmer:innen ohne deren zumindest mutmaßliche Einwilligung stets unzulässig. Werbung per E-Mail ohne die vorherige Einwilligung der Betroffenen ist nur noch unter den engen Voraussetzungen des § 7 Absatz 3 UWG möglich. Vor diesem Hintergrund raten wir den Werbenden dringend, die vorherige Einwilligung der jeweiligen Betroffenen einzuholen.

14.4 Internationale Zusammenarbeit datenschutzrechtlicher Aufsichtsbehörden

Im Berichtsjahr 2022 erreichten uns Beschwerden über den Erhalt von Werbung per E-Mail durch Werbevermittlung aus nicht der Europäischen Union (EU) angehörenden Ländern wie zum Beispiel aus der Türkei oder (seit dem Brexit) aus Großbritannien. Bei der werblichen Ansprache handelt es sich meist um Werbung durch so genannte Werbevermittler. In diesen Fällen haben die Unternehmen, die für sich und ihre Produkte werben wollen, keine Kenntnisse über die personenbezogenen Daten der Werbungsempfänger:innen , weil sie lediglich die Werbung in Auftrag geben und nicht wissen, an wen diese versandt wird. Hier kann kein datenschutzrechtlicher Verstoß im Inland festgestellt werden, weil es nicht das im Land Bremen ansässige Unternehmen ist, das die Verarbeitung personenbezogener Daten vornimmt, sondern es sich um eine Verarbeitung durch ein Unternehmen handelt, das nicht dem örtlichen Anwendungsbereich der Datenschutzgrundverordnung unterfällt.

In diesen Fällen setzen wir uns mit den Aufsichtsbehörden in dem jeweiligen Drittland in Verbindung und versuchen die Beschwerde in Absprache mit den Betroffenen weiter zu verfolgen. Anders als für die Zusammenarbeit unter den datenschutzrechtlichen Aufsichtsbehörden innerhalb der EU gibt es hierfür keine festgelegten Verfahren.

15. Videoüberwachung im nicht öffentlichen Bereich

15.1 Gemeldete Datenschutzverletzungen

Im Bereich Videoüberwachung gab es im Berichtsjahr keine Meldungen der Verletzung des Schutzes personenbezogener Daten nach Artikel 33 der Datenschutzgrundverordnung. Hingegen erhielten wir im Berichtszeitraum 54 Beschwerden, die sich auf Videoüberwachungen durch private Stellen bezogen.

15.2 Videoüberwachung im Restaurant

Uns erreichten mehrere Beschwerden von Restaurantbesucher:innen, wonach in den jeweils aufgesuchten Restaurants der Verdacht bestand, dass die Sitzbereiche mit Videokameras überwacht wurden. Im Zuge der Prüfung bei den jeweiligen Restaurants konnten wir feststellen, dass diese Befürchtungen zutrafen. Darüber hinaus waren weder Datenschutzbeauftragte bestellt noch einsehbare Verzeichnisse über Verarbeitungstätigkeiten oder Aufzeichnungen über durchgeführte Datenschutz-Folgenabschätzungen vorhanden. Es stellte sich heraus, dass sich die Gastwirt:innen über die datenschutzrechtlichen Vorgaben nicht im Klaren waren. Wir erläuterten, dass die Erhebung personenbezogener Daten mit Videotechnik nur zulässig ist, soweit sie unter anderem zur Wahrung berechtigter Interessen erforderlich ist und sofern nicht schutzwürdige Interessen der betroffenen Personen überwiegen. Die Schutzwürdigkeit der Interessen der von der Videoüberwachung betroffenen Personen in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, ist besonders hoch einzustufen. Dies trifft auf Sitzbereiche, durch die zu einem längeren Aufenthalt eingeladen werden soll, im besonderen Maße zu. In beiden Fällen überwogen daher die schutzwürdigen Interessen der Besucher:innen gegenüber den berechtigten Interessen der Restaurantbetreiber:innen. Ebenso haben Beschäftigte einen Anspruch, bei Ausübung ihrer beruflichen Tätigkeit keiner ständigen Arbeits- und Leistungskontrolle durch die Arbeitgeberin oder den Arbeitgeber zu unterliegen. Letztlich zeigten sich beide Gastronom:innen einsichtig und setzten die von uns aufgegebenen Maßnahmen um, um eine datenschutzgerechte Videoüberwachung zu gewährleisten.

15.3 Schwerpunkte im Berichtsjahr

Ein nicht unerheblicher Teil der Beschwerdefälle bezog sich in diesem Berichtszeitraum auf Überwachungskameras an Privathäusern, wobei eine Zunahme der anonymen Beschwerden zu verzeichnen war. In vielen Fällen konnten wir keine Datenschutzverstöße feststellen. Oftmals schien es bei den anonymen Beschwerden darum zu gehen, die datenschutzrechtliche Aufsichtsbehörde in einem privaten Nachbarschaftsstreit zum Nachteil einer beziehungsweise eines Beteiligten zu instrumentalisieren.

Auch stellen wir fest, dass wir zunehmend erheblich mehr Aufwand betreiben müssen, um die für unsere rechtliche Zulässigkeitsprüfung erforderlichen Daten zu erhalten. Hierzu gehören beispielsweise Erfassungsbereich, Zweck der Verarbeitung oder die technischen Gegebenheiten. In den Beschwerden wurden häufig nur unvollständige Angaben zum Namen und zur Adresse der für die Videoüberwachung Verantwortlichen gemacht. Ebenso fehlten Angaben darüber, welche Bereiche die betreffende Kamera mutmaßlich überwacht und wo

der exakte Standort der Kamera war. Anders als in den Vorjahren wurden unsere Anfragen an die verantwortlichen Personen zunehmend nur schleppend beantwortet, waren vielfach wenig aussagefähig und unvollständig.

16. Kredit-, Versicherungs- und allgemeine Wirtschaft

16.1 Gemeldete Datenschutzverletzungen

Von Kredit- und anderen Wirtschaftsunternehmen wurden uns im Berichtsjahr vor allem Fälle der fehlerhaften Übermittlung personenbezogener Daten basierend insbesondere auf individueller Unachtsamkeit bei der Adressierung postalischer beziehungsweise elektronischer Nachrichten oder bei der Sortierung zu versendender Unterlagen gemeldet. Hierunter fielen auch wieder einige wenige Fälle des E-Mail-Versandes unter Nutzung des offenen Adressverteilerfeldes Cc (siehe hierzu 4. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 12.7). Mittlerweile sollte dahingehend ein entsprechendes Datenschutzbewusstsein der Verantwortlichen beziehungsweise ihrer Beschäftigten vorhanden sein und es existieren am Markt technisch geeignete Lösungen, um einen unbefugten Versand mit offenem E-Mail-Verteiler zu verhindern. Daher ahnden wir derartige Verstöße mittlerweile regelmäßig mit einer Maßnahme im Sinne der Datenschutzgrundverordnung.

Daneben erreichten uns leider auch wieder etliche Meldungen zu technischen Angriffen auf die IT-Infrastruktur von Verantwortlichen, sei es in Form erfolgreicher Phishing-Mails oder durch Einsatz sonstiger Schadware wie etwa Verschlüsselungssoftware. Hierbei handelt es sich um eine weiterhin zunehmende Problematik. Wir empfehlen betroffenen Verantwortlichen neben der Meldung bei uns regelmäßig auch eine – auch anonym mögliche – Meldung beim Bundesamt für Sicherheit in der Informationstechnik sowie eine Strafanzeige bei der Polizei oder Staatsanwaltschaft. Präventiv ist es für sämtliche Unternehmen empfehlenswert, in die Sicherheit der IT-Infrastruktur zu investieren sowie regelmäßig Sicherheitsupdates, Sicherheits-Backups und Schulungen der Beschäftigten durchzuführen.

Aus dem Bereich der Versicherungswirtschaft wurden uns im Berichtsjahr keine Meldungen von Datenschutzverletzung nach Artikel 33 Datenschutzgrundverordnung zugeleitet.

16.2 Erforderlichkeit eines Einwilligungsnachweises

Ein Maklerunternehmen hatte im Rahmen der Vermittlung eines Kaufgeschäfts Daten zur Person eines Käufers an verschiedene Versicherungsgesellschaften zwecks Versicherungsangebotserstellung für den Kaufgegenstand weitergegeben. Die Käuferseite erhielt dann in der Folge Versicherungsangebote, woraufhin sie sich nach einiger Zeit bei uns

über die Datenübermittlung an die Versicherungsgesellschaften beschwerte. Das Unternehmen erklärte auf unsere Nachfrage, dass es sich um eine übliche Serviceleistung für Käufer:innen handele; da dies Zusatzaufwand für das Unternehmen bedeute, werde sie aber nur auf ausdrücklichen Wunsch erbracht. Die Käuferseite habe mündlich ihr Einverständnis erklärt. Die Käuferseite bestritt eine Einwilligung.

Wir konnten mit den verfügbaren Aufklärungsmöglichkeiten bei vertretbarem Aufwand den tatsächlichen Sachverhaltsablauf nicht hinreichend sicher aufklären. In diesem Fall gilt nach der Datenschutzgrundverordnung (DSGVO): Ist eine "Einwilligung" im Sinne des Artikels 4 Ziffer 11 DSGVO Grundlage für die Verarbeitung der personenbezogenen Daten eines Betroffenen, so muss im Streitfall die Einwilligungserteilung seitens der datenverarbeitenden Stelle nachgewiesen werden können, Artikel 7 Absatz 1 DSGVO in Verbindung mit Artikel 5 Absatz 2 DSGVO (Rechenschaftspflicht). Das Risiko der Nichterweislichkeit der Erteilung einer Einwilligung trifft also nach den materiell-rechtlichen Regelungen der DSGVO die datenverarbeitende Stelle.

16.3 Anfertigung einer Personalausweiskopie bei Paketabholung?

Hin und wieder erhalten wir Beschwerden, weil die Betroffenen bei der Abholung eines an sie adressierten Paketes in einem Paketshop nicht nur zur Vorlage ihres Personalausweises aufgefordert wurden, sondern sogar zur Aushändigung zwecks Anfertigung einer Kopie.

Das Postgesetz enthält hierzu eine spezielle Regelung: Um sicherzustellen, dass die Abholenden die angegebenen Adressat:innen sind, darf die Vorlage eines amtlichen Ausweises erbeten werden. Um darüber hinaus auch später nachweisen zu können, dass das Paket ordnungsgemäß ausgehändigt wurde, dürfen lediglich die Art des Ausweises, die Ausstellungsbehörde und das Ausstellungsdatum sowie die Ausweisnummer gespeichert werden. Für diese Daten ist eine Löschfristregelung festgeschrieben. Derartigen berechtigten Beschwerde können wir nicht selbst abhelfen. Soweit bei der geschäftsmäßigen Erbringung von Postdienstleistungen Daten verarbeitet werden, ist allein der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständige Datenschutzaufsichtsinstanz.

16.4 Identitätsverwechslung bei Kontovollmacht

Eine Kundin eines Kreditinstituts wandte sich an uns und teilte mit, dass bei dem Kreditinstitut durch ihr namensähnliche Vollmachtgeberin für ihr Konto eine Vorsorgevollmachtsurkunde zugunsten eines ihr unbekannten Dritten (Vollmachtnehmer) erstellt worden sei. Die Vorsorgevollmacht sei auch in elektronischer Version im Postfach ihres Online-Kontos hinterlegt worden, worüber sie im Online-Konto benachrichtigt worden sei. Weiter teilte sie mit,

dass die Vorsorgevollmacht unterschrieben worden sei, die auf dem Dokument enthaltene Unterschrift im Feld Vollmachtgeber jedoch nicht ihrer Unterschrift entspreche.

Die Verantwortliche räumte auf unsere Aufforderung zur Stellungnahme hin den vorstehenden Sachverhalt weitestgehend ein und teilte mit, dass es bei Erstellung der Vorsorgevollmachtsurkunde offenbar zu einer Namensverwechselung (Eintragung des falschen Namens) durch den bearbeitenden Mitarbeiter gekommen sei. Auch die Vollmachtgeberin habe bei Unterzeichnung nicht bemerkt, dass die Urkunde nicht ihren, sondern den falschen Namen aufgewiesen habe. Der Vollmachtnehmer habe dadurch kurzzeitig Einblick auf das Konto der Kundin, die sich bei uns gemeldet hatte, nehmen können.

Nach Bekanntwerden des Sachverhaltes entzog das verantwortliche Kreditinstitut umgehend die Online-Vollmacht und damit die eingerichtete Zugriffsmöglichkeit auf das falsche Konto und informierte die kontoführende Filiale, sodass die fehlerhafte Vollmachtsurkunde noch am selben Tag vernichtet wurde. Eine solche sofortige Abhilfe ist von der Datenschutzgrundverordnung gefordert.

16.5 Unbefugte Kontodatenzugriffe

Wir erhielten im Berichtsjahr unter anderem auch einen Hinweis darauf, dass bereits bei einer einmaligen Tagesnutzung einer Wellnesseinrichtung für den nutzenden Gast ohne Mitgliedsstatus ein Kundenkonto erstellt werde. Mittels eines auszufüllenden Formulars würden zwingend Vor- und Nachname und Geschlecht erfragt sowie ein Personenfoto erbeten, daneben zur Abgabe weiterer Daten (Wohnort, Geburtstag, Telefon, E-Mail-Adresse) gedrängt.

Um den Sachverhalt zu verifizieren und näher aufzuklären, wandten wir uns mit einem Fragenkatalog an das verantwortliche Unternehmen. In Reaktion hierauf erhielten wir jedoch die Antwort, dass Tagesgäste nunmehr wieder anonym und ohne Angabe personenbezogener Daten die Einrichtung nutzen könnten. Die Erhebung wurde mit einem Testlauf erklärt; die erhobenen Informationen zu Tagesgästen seien bereits wieder gelöscht.

Wir nahmen dies zur Kenntnis und unterstrichen dabei nachdrücklich, dass eine Verarbeitung personenbezogener Echtdaten nur probehalber, also ohne dass die gesetzlichen Voraussetzungen hierfür vorliegen, in der Datenschutzgrundverordnung nicht vorgesehen ist.

16.6 Information durch Inkassounternehmen

Im Rahmen der Einziehung einer titulierten Forderung gegen eine betroffene Schuldnerin hatte sich ein Inkassounternehmen per Brief an die Vermieterin der Schuldnerin gewandt, dieser mitgeteilt, dass eine Pfändung gegen die Schuldnerin bevorstehe und um Auskunft zu einigen Fragen gebeten, wobei sie sich unter anderem erkundigt hatte, wie hoch das Mietdeponat sei.

Das Inkassounternehmen unterließ es in diesem Zusammenhang, die Vermieterin als Drittschuldnerin über die Verarbeitung ihrer Daten im Sinne von Artikel 14 Datenschutzgrundverordnung (DSGVO) zu informieren. Dies beanstandeten wir gegenüber dem Inkassounternehmen, das uns daraufhin mitteilte, dass das Verfahren umgestellt worden sei, sodass in zukünftigen vergleichbaren Fällen die jeweiligen Drittschuldner:innen nach Artikel 14 DSGVO informiert würden. Trotz der sofortigen Abhilfe belegten wir das verantwortliche Inkassounternehmen aufgrund der Wichtigkeit der Datenschutzinformation nach Artikel 13 und Artikel 14 DSGVO mit einer Verwarnung im Sinne der Datenschutzgrundverordnung.

16.7 Auskunftserteilung durch Verantwortliche

Zahlreiche Beschwerden erreichten uns im Berichtsjahr über nicht oder unvollständig erteilte Auskünfte nach Artikel 15 Datenschutzgrundverordnung (DSGVO). Nicht immer waren die Beschwerden begründet: So konnten wir in einem Fall feststellen, dass die Auskunft von der verantwortlichen Stelle fristgerecht innerhalb eines Monats erteilt worden war, allerdings aufgrund individueller Einstellungen im Spam-Ordner des E-Mail-Postfaches des Betroffenen gelandet war, sodass dieser die Auskunft übersehen hatte.

Dennoch wiesen und weisen wir in diesem Zusammenhang die datenschutzrechtlich Verantwortlichen ausdrücklich darauf hin, dass sie die Beweislast für den Zugang etwaiger Auskunftserteilungen tragen und es sich daher empfiehlt, diesen möglichst genau zu dokumentieren. Die Dokumentation des Versandes von E-Mails reicht dafür nicht aus, da sich hiermit noch nicht nachweisen lässt, dass diese tatsächlich in den Herrschaftsbereich (auch das E-Mail-Postfach) der Betroffenen gelangt sind. Entgegen der Ansicht des Betroffenen im eingangs genannten Beschwerdefall besteht aber grundsätzlich kein durchsetzbares Wahlrecht, die Auskunftserteilung nach Artikel 15 DSGVO per Post zu erhalten. Für die Auskunftserteilung ist in den einschlägigen Artikeln 12 und 15 DSGVO keine bestimmte Form vorgeschrieben; sie darf schriftlich, gegebenenfalls auch elektronisch oder in anderer Form erteilt werden. Bei gesicherter Identität der betroffenen Person darf dies auf Wunsch sogar mündlich erfolgen. Es stellte daher keinen datenschutzrechtlichen Verstoß dar, dass sich die

Verantwortliche im vorgenannten Fall entschieden hatte, die Auskunft nicht per Post, sondern gesichert per E-Mail zur Verfügung zu stellen.

16.8 Unfreiwillige Pseudo – Einwilligung im Versicherungsbereich

Zum Abschluss eines Versicherungsvertrages oder zur Abwicklung von Versicherungsleistungen holen Versicherungen häufig von den betroffenen Personen vermeintliche Einwilligungen zur Verarbeitung von Gesundheitsdaten ein. Verweigern die Betreffenden die Verarbeitung der personenbezogenen Daten, kommt es laut Versicherungsverträgen nicht zu einem Vertragsabschluss oder zu einer Leistung der Versicherung in einem Schadensfall. Daher kann hier nicht von einer freiwilligen Einwilligung nach Artikel 7 Datenschutzgrundverordnung (DSGVO) ausgegangen werden. Die Betroffenen können die erteilte vermeintliche Einwilligung auch nicht ohne weiteres widerrufen, da es bei einer Versicherungsleistung vorgeschriebene Aufbewahrungspflichten gibt.

Der Bundesgesetzgeber könnte in diesem Zusammenhang über die Schaffung einer Regelung im Sinne des Artikel 9 Absatz 2 Buchstabe g DSGVO nachdenken, die einen strengen gesetzgeberischen Rahmen dafür festlegen könnte, welche personenbezogenen Daten aus Gründen eines erheblichen öffentlichen Interesses für die Zwecke der Leistungsprüfungen in der Versicherungswirtschaft erforderlich sind. Gegenwärtig wird den Versicherungsnehmer:innen suggeriert, sie hätten eine Wahlmöglichkeit zur freiwilligen Einwilligung in die Verarbeitung ihrer Daten, was nicht der Fall ist.

16.9 Speicherung von Impf- und Genesungsnachweisen in Fitnessstudios

Im Zuge der Corona-Pandemie waren Betreiber:innen von Sportstudios verpflichtet worden, sicherzustellen, dass alle Besucher:innen des Studios entweder negativ auf das Corona-Virus getestet, genesen oder geimpft waren (siehe zuletzt: § 3 Absatz 1, 3, 4 Nr. 2 Dreißigste Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 [Dreißigste Coronaverordnung] der Freien Hansestadt Bremen). Diese Verpflichtung wurde mit der Ersten Basis Schutzverordnung vom 22. März 2022 (Erste Verordnung zum Basisschutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 [Erste Corona-Basisschutzmaßnahmenverordnung]) aufgehoben.

Viele Betreiber:innen von Sportstudios hatten Kopien der Impf- und Genesungsnachweise in ihren Systemen gespeichert, um es geimpften und genesenen Besucher:innen zu ersparen, bei jedem Aufsuchen des Sportstudios einen entsprechenden Nachweis vorlegen zu müssen. Beim Einchecken von Besucher:innen wurde Beschäftigten des Studios die Information angezeigt, dass die Besucher:innen die gesetzliche Anforderungen erfüllten, sodass die Besucher:innen den Check-In-Prozess absolvieren konnten, ohne einen entsprechenden

Impf- beziehungsweise Genesenennachweis vorlegen zu müssen. Nach dem Wegfall der Verpflichtung, sicherzustellen, dass alle Besucher:innen von Sportstudios entweder negativ auf das Corona-Virus getestet, genesen oder geimpft waren, schrieben wir 30 Sportstudiobetreiber:innen an und forderten diese auf, vorhandene Impf- und/oder Genesungsnachweis zu löschen oder Einwilligungserklärungen nachzuweisen, die die Speicherung der Nachweise gegebenenfalls auch nach dem Wegfall der dargelegten Verpflichtung legitimieren können. Der größte Teil unserer aufsichtsrechtlichen Verfahren konnte zwischenzeitlich abgeschlossen werden, da die entsprechenden Sportstudiobetreiber:innen die gespeicherten Impf- und/oder Genesungsnachweise auf unsere Aufforderung hin löschten. Ein Verfahren wird aktuell noch betrieben.

17. Internationales und Europa

17.1 Homeoffice aus Drittländern

Da die Datenschutzgrundverordnung (DSGVO) in allen Mitgliedsstaaten der Europäischen Union, Norwegen, Island und Liechtenstein gilt, unterfällt eine Homeoffice-Tätigkeit aus diesen Ländern heraus der DSGVO. Dies gilt grundsätzlich auch bei einem Aufenthalt von im Homeoffice tätigen Beschäftigten in Ländern, für die ein so genannter Angemessenheitsbeschluss existiert – wie zum Beispiel für Israel, Vereinigtes Königreich und die Schweiz –, weil diesen Ländern von der Europäischen Kommission ein mit der DSGVO vergleichbares Datenschutzniveau bescheinigt wurde.

Technisch gesehen ist die Wahrnehmung von Tätigkeiten aus dem Homeoffice aber natürlich auch aus Nicht-Europäischen Ländern heraus möglich, für die es – wie zum Beispiel für die Vereinigten Staaten von Amerika – keinen Angemessenheitsbeschluss gibt. Bei einem Aufenthalt von Beschäftigten in solchen Drittländern müssen für jede Übermittlung personenbezogener Daten, also für jeden Zugriff der Beschäftigten auf die für die Erfüllung ihrer Aufgaben erforderlichen Daten, zusätzliche Garantieren bestehen. Hier ergibt sich unter anderem das Problem, dass Garantien zur Drittlandübermittlung wie Standardvertragsklauseln nicht dafür konzipiert wurden, zwischen Arbeitgeber:innen und Beschäftigten zu wirken.

Fehlen geeignete Garantien zur Übermittlung, liegt ein Verstoß gegen die DSGVO vor. Daher ist davon abzuraten, Beschäftigten, die sich in Drittländern ohne Angemessenheitsbeschluss aufhalten, den Zugriff auf personenbezogene Daten zu erlauben. In jedem Fall der Tätigkeit von Beschäftigten aus dem Homeoffice heraus sollten technisch-organisatorische Maßnahmen zur Risikominimierung getroffen werden.

17.2 Privacy Shield 2.0 in Aussicht?

Das EU-U.S. Privacy Shield umfasste Absprachen über das Datenschutzrecht zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA). Er beinhaltete Zusicherungen der US-amerikanischen Bundesregierung und einen Angemessenheitsbeschluss der Europäischen Kommission. Am 16. Juli 2020 hatte der Europäische Gerichtshof (EuGH) diesen Angemessenheitsbeschluss der Kommission für die USA in seinem so genannten Schrems-II-Urteil für ungültig erklärt. Seitdem konnten Übermittlungen personenbezogener Daten in die USA nicht mehr auf Artikel 45 Absatz 1 Datenschutzgrundverordnung (DSGVO) gestützt werden.

Zum Ende des Berichtsjahres könnte die Nachfolgeregelung für das Privacy Shield, das Privacy Shield 2.0 nahe bevorstehen, das den Namen "EU-U.S. Data Privacy Framework" erhalten und frühestens im Frühjahr 2023 in Kraft treten soll. Am 7. Oktober 2022 unterzeichnete der Präsident der Vereinigten Staaten von Amerika die Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities (Executive Order). Sie soll die Grundlage dafür schaffen, dass auch europäische Unternehmen, die keine geeigneten Garantien im Sinne des Artikels 45 DSGVO vorsehen, personenbezogene Daten in die USA übermitteln können, ohne gegen die DSGVO zu verstoßen. Die Executive Order soll allen Kritikpunkten des EuGH am Privacy Shield begegnen.

Nach Auffassung der Europäischen Kommission kann die Executive Order jedoch ein zentrales Problem nicht lösen: Die US-Sicherheitsgesetze ermöglichen eine Massenüberwachung der in der EU lebenden Menschen, wenn ihre Daten von Konzernen aus den USA verarbeitet werden. Deshalb entspreche der Datenschutzstandard in den USA auch nach der Executive Order nicht dem in der EU. Ob die Europäische Kommission nach dieser Feststellung ein angemessenes Datenschutzniveau der USA attestieren wird, ist ungewiss. Max Schrems, der mit seiner Klage Auslöser für das EuGH-Urteil war, geht davon aus, dass das neue Abkommen genauso fehlerhaft wie das alte sein wird und deutet an, dass der EuGH auch mit dem EU-U.S. Data Privacy Framework befasst werden wird.

17.3 Kein Verstoß von US-Cloud Diensten gegen die Datenschutzgrundverordnung

Wie unter Ziffer 17.2 diese Berichts bereits thematisiert, erklärte der Europäische Gerichtshof (EuGH) 2020 die Datenschutzvereinbarung EU-U.S. Privacy Shield für ungültig. Seitdem gelten die Vereinigten Staaten von Amerika (USA) nicht mehr als Drittland mit einem angemessenen Datenschutzniveau. Als Reaktion hierauf eröffneten einige Dienstleister aus den USA europäische Firmensitze zum Beispiel für ihre Cloud-Dienste.

Nach einem Beschluss der Vergabekammer Baden-Württemberg vom 13. Juli 2022 ist auch die Übermittlung personenbezogener Daten an die europäischen Standorte der US-Dienstleister rechtswidrig, weil ein latentes Risiko besteht, dass eine unzulässige Übermittlung personenbezogener Daten stattfinden kann. Demgegenüber dürfen europäische Unternehmen nach dem rechtskräftigen Urteil des Oberlandesgerichts Karlsruhe vom 7. September 2022 personenbezogene Daten an Tochterfirmen von US-Unternehmen in die USA grundsätzlich übermitteln, sofern diese Daten auf europäischen Servern verbleiben. Ohne das Vorliegen konkreter Anhaltspunkte dürfe nicht davon ausgegangen werden, dass eine solche Datenübermittlung rechtswidrig sei.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit rät Unternehmen mit Sitz im Land Bremen, in jedem Fall ausreichende Sicherheitsmechanismen zu treffen, um zu gewährleisten, dass keine Datenübermittlungen personenbezogener Daten in die USA stattfinden.

18. Die Beschlüsse des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) ist die Organisationsform, in der die datenschutzrechtlichen Aufsichtsbehörden in Europa gemeinsam handeln. Hierzu beschließt der EDSA unter anderem Leitlinien, Empfehlungen und bewährte Verfahren zur Datenschutzgrundverordnung[6] und trifft verbindliche Beschlüsse in Einzelfällen.

19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2022

19.1 Wissenschaftliche Forschung – selbstverständlich mit Datenschutz

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. März 2022)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unterstreicht, dass wissenschaftliche Forschung und Datenschutz miteinander vereinbar sind.

Auch der europäische Verordnungsgeber hat die Bedeutung der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung gesehen. So privilegiert die Datenschutzgrundverordnung (DSGVO) die wissenschaftliche Forschung an vielen Stellen. Dazu gehört beispielsweise die Regelung in Artikel 5 Absatz 1 Buchstabe b

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

DSGVO, wonach Forschungszwecke vereinbar mit dem ursprünglichen Zweck sein können, zu dem die Daten einmal erhoben wurden.

Dies entspricht dem politischen Ziel der Europäischen Union, den wissenschaftlichen Fortschritt zu fördern sowie ihre wissenschaftlichen und technologischen Grundlagen dadurch zu stärken, dass ein europäischer Forschungsraum geschaffen wird.

Die DSGVO zielt daher darauf ab, einen Ausgleich zwischen der Forschungsfreiheit auf der einen Seite und dem Recht des Einzelnen auf Achtung seines Grundrechts auf Datenschutz zu schaffen. So weist Artikel 89 DSGVO darauf hin, dass Verarbeitungen von personenbezogenen Daten für die wissenschaftliche Forschung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne der DSGVO unterliegen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet werden muss. Die DSK unterstützt daher nachdrücklich die Förderung und Erforschung von Methoden, Forschungsdaten so zu verarbeiten, dass Persönlichkeitsrechte der Bürgerinnen und Bürger bestmöglich geschützt werden. Soweit ein Zugriff auf identifizierende Angaben nicht durch geeignete innovative Methoden ausgeschlossen werden kann, sollten Anonymisierung, Pseudonymisierung, Datentreuhänderschaften und andere Instrumente vorgesehen werden.

Die DSK begrüßt die Überlegungen der Bundesregierung, ein allgemeines Forschungsdatengesetz auf den Weg zu bringen, das das Recht auf informationelle Selbstbestimmung wahrt. Flankiert werden sollte dieses allgemeine Forschungsdatengesetz durch Forschungsregelungen in einzelnen Bereichen. Insbesondere erkennt die DSK die Pläne der Bundesregierung an, ein datenschutzgerechtes Gesundheitsdatennutzungsgesetz auf den Weg zu bringen, um die Besonderheiten bei der wissenschaftlichen Forschung mit Gesundheitsdaten zu berücksichtigen. Die Erschließung von Gesundheitsdaten in medizinischen Registern für die wissenschaftliche Forschung durch ein geplantes Registergesetz kann allerdings nur unter Beachtung der datenschutzrechtlichen Anforderungen erfolgen.

Insoweit weist die DSK vor allem auf ihre Entschließung vom 25./26. März 2004[7] hin und fordert den Gesetzgeber auf sicherzustellen, dass auch bei und nach der Übermittlung geschützter personenbezogener medizinischer Daten ein strafrechtlicher Schutz vor Offenbarung und Beschlagnahmeschutz im Strafverfahren gewährleistet ist.

[7] vergleiche https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/67DSK-EinfuehrungEinesForschungsgeheimnissesFuerMedizinischeDaten.pdf

Aus diesem Grund hält sie es insbesondere für erforderlich,

- in § 203 Strafgesetzbuch (StGB) die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53 a Strafprozessordnung (StPO) für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forschende und ihre Berufshelfenden zu schaffen und
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die DSK bietet eine konstruktive Beratung bei der Weiterentwicklung der Nationalen Forschungsdateninfrastruktur an, sofern dabei personenbezogene Daten betroffen sind. Dies gilt auch im europäischen Kontext, soweit etwa im Bereich des Europäischen Gesundheitsdatenraums personenbezogene Daten, insbesondere Gesundheitsdaten, für die wissenschaftliche Forschung bereitgestellt werden sollen.

Die DSK beabsichtigt zeitnah weitere Vorschläge zum Thema Forschungsdaten zu veröffentlichen. Ziel ist es, neben der Rechtsklarheit für die Nutzung von Forschungsdaten insbesondere auch den nachhaltigen Schutz für die personenbezogenen Daten der Bürgerinnen und Bürger zu gewährleisten.

19.2 Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. März 2022)

In den vergangenen Jahren gab es zahlreiche Parlamentarische Untersuchungsausschüsse im Bundestag und in den Landtagen, die das Handeln von Polizei- und Sicherheitsbehörden untersucht haben. Prominente Beispiele sind die Untersuchungsausschüsse zur "Terrorgruppe nationalsozialistischer Untergrund" (so genannte NSU).

Die Untersuchungsausschüsse möchten eine für die Aufklärung notwendige Datengrundlage sicherstellen. Deshalb fordern sie die Behörden regelmäßig auf, sämtliche personenbezogenen Daten weiterhin zu speichern, die in irgendeinem Bezug zum Untersuchungsgegenstand stehen können (etwa zum Thema "Rechtsextremismus"). Diese Daten sind dann für die Arbeit des Untersuchungsausschusses vorzuhalten. Dies soll auch

solche Daten umfassen, die nach den gesetzlichen Regeln eigentlich zu löschen wären (so genanntes Löschmoratorium).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hält das Interesse der Parlamentarischen Untersuchungsausschüsse an dem Erhalt personenbezogener Daten für nachvollziehbar und gewichtig, um den Untersuchungsauftrag umzusetzen. Es ist ihr insbesondere bewusst, dass dem parlamentarischen Informationsinteresse ein besonders hohes Gewicht zukommt, soweit es um die Aufdeckung möglicher Rechtsverstöße und vergleichbarer Missstände geht. Gleichzeitig gilt es allerdings zu berücksichtigen, dass dadurch erheblich in Grundrechte der betroffenen Personen eingegriffen wird, insbesondere dann, wenn diese Personen tatsächlich in keinerlei Bezug zum Untersuchungsgegenstand stehen beziehungsweise gesetzliche Löschungsverpflichtungen suspendiert werden.

Um parlamentarischen Kontrollrechten und Grundrechten betroffener Personen gleichermaßen Geltung zu verschaffen, weist die Konferenz auf folgende Punkte hin:

- Ohne die förmliche Einsetzung eines Untersuchungsausschusses und Anforderungen von Beweisunterlagen gibt es keine Rechtsgrundlage dafür, die gesetzlich vorgeschriebene Löschung personenbezogener Daten zu suspendieren.

  Hierzu gehört, dass der Untersuchungsgegenstand klar definiert ist und die Beweisbeschlüsse hinreichend bestimmt formuliert sind (Bundesverfassungsgericht, Beschluss vom 17. Juni 2009 – 2 BvE 3/07). Zudem müssen die Ausnahmen zeitlich auf die Arbeit des Untersuchungsausschusses begrenzt sein. Nur auf diese Weise können unnötige Datenspeicherungen und die damit verbundenen Risiken für die Rechte der betroffenen Personen vermieden werden.

- "Löschreife" Daten, die die Behörden für Zwecke eines Untersuchungsausschusses zur Verfügung halten, dürfen sie im weiteren Verwaltungsvollzug nicht nutzen. Die DSK hält es daher für erforderlich, diese Daten in Anlehnung an § 58 Absatz 3 Bundesdatenschutzgesetz in ihrer Verarbeitung zu beschränken. Hierfür sollte der jeweilige Gesetzgeber Voraussetzungen und Grenzen präzise beschreiben. Einige Landesgesetzgeber haben dies bereits umgesetzt.

Die DSK appelliert deshalb an die Gesetzgeber des Bundes und der Länder, den Sicherheitsbehörden klare gesetzliche Vorgaben zum Umgang mit zu löschenden Daten zu machen. Diese müssen den Untersuchungsausschüssen den Zugriff auf die Daten sichern. Gleichzeitig ist sicherzustellen, dass die Daten dem Verwaltungsvollzug der Behörden

entzogen sind. So werden das Untersuchungsinteresse der Parlamentarischen Untersuchungsausschüsse und die Grundrechte der betroffenen Personen gewahrt.

19.3 Die Zeit für ein Beschäftigtendatenschutzgesetz ist "Jetzt"!

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2022)

Die voranschreitende technische Entwicklung ermöglicht eine immer weitergehende Überwachung von Beschäftigten. Deshalb forderte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits 2014 die Schaffung eines Beschäftigtendatenschutzgesetzes.[8]

Die sich dynamisch entwickelnde Digitalisierung führt zu tiefgreifenden Veränderungen in der Arbeitswelt. Auch vor diesem Hintergrund hat das Bundesministerium für Arbeit und Soziales (BMAS) den interdisziplinären Beirat Beschäftigtendatenschutz eingesetzt, der seinen Abschlussbericht im Januar 2022 fertiggestellt hat. Auch er kommt darin zu dem Schluss, dass – neben weiteren Maßnahmen – ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.[9]

Das europäische Recht ermöglicht es den Mitgliedstaaten spezifischere Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen. Eine erste Regelung hat der deutsche Gesetzgeber mit Erlass des § 26 Bundesdatenschutzgesetz (BDSG) getroffen und sich zugleich weitergehende Regelungen ausdrücklich vorbehalten (Bundestag-Drucksache 18/11325, Seite 97). Die DSK begrüßt, dass sich im Koalitionsvertrag auf Bundesebene explizit zur Schaffung von Regelungen zum Beschäftigtendatenschutz bekannt wird (Koalitionsvertrag "Mehr Fortschritt wagen", Seite 17).

Die DSK ist der Auffassung, dass weitergehende Regelungen notwendig und überfällig sind: § 26 BDSG ist nicht hinreichend praktikabel, normenklar und sachgerecht[10]. Die Norm ist als Generalklausel formuliert und eröffnet weite Interpretationsspielräume. Dadurch führt sie zu Unklarheiten über die Zulässigkeit von Verarbeitungen personenbezogener Daten im Beschäftigungskontext für Arbeitgeberinnen und Arbeitgeber, Beschäftigte, Bewerberinnen und Bewerber, Personalvertretungen oder Gerichte.

---

[8] Entschließung vom 27. März 2014, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20140327_en_Beschaeftigtendatenschutzgesetz.pdf

[9] Beiratsbericht, Seiten 6, 9, abrufbar unter: https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergebnisse-beirat-beschaeftigtendatenschutz.pdf;jsessionid=0A2E14EA95F12CD2F926680929CDC8C5.delivery2-master?__blob=publicationFile&v=3)

[10] Siehe Stellungnahme der DSK zur Evaluierung des BDSG vom 2.3.2021, Seite 8 folgende, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf

Gerade im Zeitalter der Digitalisierung muss ein Beschäftigtendatenschutzgesetz hinreichend flexibel sein, ein hohes Datenschutzniveau gewährleisten sowie Rechtsklarheit für alle Akteure der Arbeitswelt ermöglichen. Zudem hat es insbesondere vor dem Hintergrund der Risiken technischer Entwicklungen einen angemessenen Ausgleich zwischen den grundrechtlich geschützten Interessen der Arbeitgeberinnen und Arbeitgeber sowie dem Recht auf informationelle Selbstbestimmung der Beschäftigten zu schaffen.

Daher fordert die DSK den Gesetzgeber auf, im Rahmen eines eigenständigen Beschäftigtendatenschutzgesetzes mindestens in den folgenden Bereichen gesetzliche Regelungen zu schaffen:

– Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI)

Die Grenzen und Rahmenbedingungen des Einsatzes algorithmischer Systeme im Beschäftigungs- und Bewerbungskontext sollten gesetzlich geregelt werden. Dabei spielt die Schwere, Tiefe und Breite der Grundrechtseingriffe, die der Einsatz algorithmischer Systeme im Beschäftigungskontext typischerweise verursacht, eine wesentliche Rolle. Zudem sind die Hambacher Erklärung der DSK[11] und die von der Datenethikkommission entwickelte "Kritikalitätspyramide"[12] zu berücksichtigen. Je höher die "Kritikalität", also das Schädigungspotenzial eines algorithmischen Systems ist, desto strenger sind demnach die Anforderungen an dessen Einsatz. Im Beschäftigungs- und Bewerbungsverhältnis fallen zahlreiche aussagekräftige Daten an. Die Beschäftigten sowie Bewerberinnen und Bewerber sind wegen ihres Abhängigkeitsverhältnisses besonders schutzbedürftig. Zugleich sollen alle Beteiligten von den Chancen des KI-Einsatzes profitieren können. Korrektur- und Kontrollinstrumente wie Zulassungsverfahren, Vorabprüfungen, Antidiskriminierungs- oder Transparenzvorgaben sowie verbesserte Möglichkeiten der Rechtsdurchsetzung bedürfen daher gesetzlicher Normierung. Besonders eingriffsintensive Datenverarbeitungen sollten verboten werden: So fordert die DSK, auch im Beschäftigungskontext die Profilbildung als solche dem Verbot mit Erlaubnisvorbehalt des Artikels 22 der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung – DSGVO) zu unterstellen. Es hat sich gezeigt, dass Artikel 22 DSGVO, dessen Wortlaut nur automatisierte Entscheidungen verbietet, im Beschäftigungskontext nicht ausreichend Schutz gewährleistet. Zum Schutz der betroffenen Bewerberinnen und Bewerber sowie Beschäftigten ist darüber hinaus regelmäßig der Einsatz von KI im Beschäftigungskontext auf der Grundlage einer Einwilligung zu untersagen.

[11] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf
[12] Gutachten der Datenethikkommission, Seite 177 fortfolgende, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

– Grenzen der Verhaltens- und Leistungskontrolle

Die Grenzen der Verhaltens- und Leistungskontrolle bedürfen gesetzlicher Eckpunkte.

Heimliche Kontrollen im Beschäftigungsverhältnis oder Dauerüberwachungen des Verhaltens der Beschäftigten sollten grundsätzlich, im Betrieb ebenso wie im "Home Office", verboten sein. Die Einzelfallkasuistik der arbeitsgerichtlichen Rechtsprechung und § 26 Absatz 1 Satz 2 BDSG sind im Rahmen einer normenklaren Ausnahmeregelung zu berücksichtigen. Dabei bedarf die Frage, ob § 26 Absatz 1 Satz 2 BDSG auch bei groben Pflichtverletzungen entsprechend Anwendung finden darf, einer gesetzlichen Klarstellung. Gesetzliche Eckpunkte, die zum Beispiel auch Transparenz- und Zertifizierungsanforderungen für technische Anwendungen vorgeben können, sind insbesondere zu folgenden Aspekten nötig: Grenzen des Zugriffs auf und der Auswertung von E-Mails, Internetdienstdaten und weiteren IT-Daten der Beschäftigten durch Arbeitgeberinnen und Arbeitgeber, Regelungen zum Einsatz von Videoüberwachungssystemen sowie Grenzen des Einsatzes von Geoinformationssystemen (GPS-Tracking) und biometrischen Verfahren im Beschäftigungsverhältnis. Hintergrund ist, dass der Einsatz und die Auswertung von Informations- und Kommunikationstechnologie gerade bei computergebundenen Arbeitsplätzen weitreichende Möglichkeiten der Leistungsüberwachung der Beschäftigten eröffnet, die durch gesetzliche Regelungen beschränkt werden müssen. Auch die Auswertung und Analyse von mit GPS ausgestatteten Fahrzeugen hat hohes Überwachungspotenzial und bedarf einer Regulierung. Besonders schützenswerte persönliche Merkmale wie biometrische Daten von Beschäftigten dürfen nur in Ausnahmefällen, die der Gesetzgeber definieren sollte, für Zwecke des Beschäftigungsverhältnisses genutzt werden.

– Ergänzungen zu den Rahmenbedingungen der Einwilligung

Die DSK befürwortet eine Ergänzung der Regelungen des § 26 Absatz 2 BDSG unter Berücksichtigung der Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung, wonach die Einwilligung im Beschäftigungsverhältnis wegen des bestehenden Machtungleichgewichts grundsätzlich kritisch zu sehen ist[13]. Zudem sollte die entsprechende Regelung die Formulierung von Regelbeispielen beziehungsweise Bedingungen enthalten, in welchen Fällen Einwilligungen im Beschäftigungs- und Bewerbungsverhältnis unzulässig sein sollen.

[13] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4.5.2020, Randnummer 21 fortfolgende, abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf

- Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen

Die DSK fordert den Gesetzgeber auf klarzustellen, ob und inwieweit mit Kollektivvereinbarungen einschließlich Betriebsvereinbarungen zusätzliche Rechtsgrundlagen für Datenverarbeitungen im Beschäftigungsverhältnis geschaffen werden können. Der Wortlaut von Artikel 88 Absatz 1 DSGVO und § 26 Absatz 1 Satz 1 BDSG ist in dieser Hinsicht unklar.

- Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Artikel 6 und 9 DSGVO

Die DSK empfiehlt, eindeutige konkretisierende Regelungen für die Verarbeitung von besonderen Kategorien personenbezogener Daten, wie zum Beispiel Gesundheitsdaten, im Beschäftigungsverhältnis zu schaffen. Denn die Anwendungsbereiche der Regelungen des § 22 BDSG und des § 26 BDSG überschneiden sich: Unklar ist, welcher der beiden Paragrafen den Vorrang genießt. Nach § 22 Absatz 1 Nummer 1 Buchstabe b BDSG ist beispielsweise die Verarbeitung besonderer Kategorien personenbezogener Daten "für die Beurteilung der Arbeitsfähigkeit des Beschäftigten" zulässig. Dieser steht hinsichtlich des Anwendungsbereiches nicht im Einklang mit § 26 Absatz 3 BDSG, der die Verarbeitung besonderer Kategorien von personenbezogenen Daten im Beschäftigungsverhältnis an weitere Bedingungen knüpft.

Unklar ist darüber hinaus auch das Verhältnis zu Artikel 6 Absatz 1 und Artikel 9 Absatz 2 DSGVO hinsichtlich der Frage, inwiefern auf die Ermächtigungsgrundlagen aus der DSGVO zurückgegriffen werden darf, wenn die Verarbeitung gemäß § 26 BDSG ausgeschlossen ist. Es ist hinsichtlich der neu zu schaffenden bereichsspezifischen Rechtsgrundlagen daher notwendig, ihr Verhältnis zu den Rechtsgrundlagen der DSGVO klarzustellen.

- Beweisverwertungsverbote

Die DSK befürwortet die gesetzliche Normierung eines Beweisverwertungsverbots für rechtswidrig verarbeitete Beschäftigtendaten. Diese Regelung sollte klare Kriterien für das Vorliegen eines Beweisverwertungsverbotes enthalten.

- Datenverarbeitung bei Bewerbungs- und Auswahlverfahren

Die DSK ist der Ansicht, dass gesetzliche Regelungen zur Datenverarbeitung in der Bewerbungsphase erforderlich sind. Geregelt werden sollten die Möglichkeiten und Grenzen der Verarbeitung von direkt bei Bewerberinnen und Bewerbern sowie bei Dritten oder aus öffentlich zugänglichen Quellen in Bezug auf die Bewerberinnen und Bewerber erhobenen

Daten. Darunter fallen insbesondere die folgenden Themenkomplexe: Fragerecht der Arbeitgeberinnen und Arbeitgeber, Anforderung polizeilicher Führungszeugnisse, ärztliche Untersuchungen und Eignungstests, Datenerhebung aus Drittquellen (zum Beispiel bei vorherigen Arbeitsstellen), Umgang mit sozialen Netzwerken oder das so genannte Active Sourcing. Wesentlich sind in dieser Phase auch Regelungen zur Transparenz und klare Löschfristen.

19.4 Petersberger Erklärung – zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24. November 2022)

Vorbemerkung

Die wissenschaftliche Forschung mit Gesundheitsdaten, also mit Informationen über den Gesundheitszustand von Personen, kann dazu dienen, Erkenntnisse über die Ursachen von Krankheiten zu gewinnen, effiziente Therapien zu entwickeln und Behandlungsmöglichkeiten zu verbessern.

Damit steht sie im essentiellen Interesse der Allgemeinheit und sollte gerade bei der Verfolgung dieser Ziele bestmöglich gefördert werden. Allerdings ist dabei zu beachten, dass die hierfür relevanten Datenkategorien von der Europäischen Datenschutzgrundverordnung (DSGVO) in besonderer Weise geschützt werden und einem besonders hohen Schutzbedarf unterliegen. Eine unsachgemäße Verwendung sensibler Gesundheitsdaten kann zu gravierenden Folgen führen, wie zum Beispiel soziale Stigmatisierung oder sogar Diskriminierung für die betroffenen Personen etwa auf dem Arbeits- und Versicherungsmarkt.

Datenverarbeitung für Zwecke der wissenschaftlichen Forschung genießt schon heute in der Datenschutzgrundverordnung und den nationalen Datenschutzgesetzen eine weitgehende Privilegierung. Es ist daher eine wichtige Herausforderung, Wege und Lösungen zu finden, um die Verarbeitung von Gesundheitsdaten zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken zu ermöglichen und ihre Vorzüge nutzbar zu machen. Gleichzeitig ist den damit verbundenen Risiken konsequent zu begegnen, um den Betroffenen einen adäquaten Grundrechtsschutz zu gewähren.

Mit begründetem Vertrauen der betroffenen Personen in die Einhaltung ethischer, rechtlicher und technischer Standards wächst ihre Motivation, die Forschung zu unterstützen. Deshalb ist es für Bürgerinnen und Bürger unerlässlich, darauf vertrauen zu können, dass ihre personenbezogenen Daten im Einklang mit den sie schützenden datenschutzrechtlichen

Vorgaben und unter Wahrung ihrer informationellen Selbstbestimmung verarbeitet werden. Auch deshalb ist Datenschutz eine Voraussetzung für eine menschenzentrierte wissenschaftliche Forschung mit Gesundheitsdaten.

Grundlage für eine solche datenschutzkonforme effektive Gesundheitsdatenforschung ist neben einer weitreichenden Transparenz vor allem eine hohe Rechtsklarheit für alle Beteiligten sowie die Sicherstellung eines nachhaltigen Schutzes personenbezogener Daten, wie bereits in ihrer Entschließung vom 23. März 2022 "Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" von der Datenschutzkonferenz (DSK) gefordert.

In Konkretisierung dieser Forderungen hat sich die DSK auf die folgenden Empfehlungen im Zusammenhang mit der Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung verständigt:

1. **Die Menschen stehen im Mittelpunkt der Forschung. Sie dürfen nicht zum bloßen Objekt der Datenverarbeitung gemacht werden. Entsprechende Verarbeitungsprozesse müssen daher rechtmäßig sowie für betroffene Personen stets transparent und nachvollziehbar sein. Auch wenn eine Verarbeitung ihrer Daten im öffentlichen Interesse gesetzlich erlaubt und nicht auf ihre Einwilligung gestützt wird, sind die betroffenen Personen in geeigneter Form einzubinden. Digitale Managementsysteme sollen Informations-, Kontroll- und Mitwirkungsmöglichkeiten sicherstellen. Gesetzliche Regelungen müssen wirksam den Schutz des Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen.**

2. **Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten genutzt werden.**

3. **Zu den grundlegenden Garantien und Maßnahmen gehören die Verschlüsselung, die Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung. Zusätzlich sind besondere Anforderungen bei Verarbeitungen in Drittländern zu beachten. Anonyme Datensätze, die die Re-Identifikation auch für Personen mit Zusatzwissen irreversibel ausschließen, können Forschende umfassend nutzen.**

4. **Auswertungen anhand von Falldaten greifen insbesondere dann besonders tief in die Rechte und Freiheiten der betroffenen Personen ein, wenn Datensätze aus verschiedenen Quellen verknüpft werden. Daher müssen die Art und der Umfang der**

Bereitstellung, der Zweck der Auswertung und die Forschenden persönlich besondere Schutzanforderungen erfüllen. Geeignete Verfahren müssen gewährleisten, dass rechtliche und technische Voraussetzungen für den Datenzugang erfüllt sind. Die datenschutzrechtliche Verantwortlichkeit ist lückenlos festzulegen, damit betroffene Personen ihre Datenschutzrechte ausüben können.

5. **Mit einem zentralen Registerverzeichnis sollten die Nutzung der in den verschiedenen Registern gespeicherten Daten für alle Beteiligten transparent gestaltet und mehrfache Datensammlungen vermieden werden. Dabei sind Qualitätsanforderungen verbindlich vorzugeben, zu prüfen und auszuweisen. Zudem sollte eine zentrale koordinierende Stelle mit Lotsenfunktion geschaffen werden, die Datennutzungsanträge veröffentlicht und die Nutzenden zur Publizierung der Forschungsergebnisse in anonymer Form verpflichtet. Dies schafft sowohl Wissen im Allgemeininteresse als auch Schutz für die betroffenen Personen.**

6. **Durch eine gesetzliche Regelung des Forschungsgeheimnisses ist der Umgang mit personenbezogenen medizinischen Forschungsdaten für wissenschaftlich Forschende auch in strafrechtlicher und prozessualer Sicht klarzustellen und damit ein wichtiger Beitrag zum Schutz dieser Daten zu leisten.**

7. **Die Datenschutzbehörden müssen die Einhaltung datenschutzrechtlicher Anforderungen umfassend und effektiv überwachen und durchsetzen können. Hierfür ist auch erforderlich, gegenüber öffentlichen Stellen den sofortigen Vollzug von Maßnahmen anordnen zu können. Zur Erleichterung der Kontrolle sollten standardisierte Anforderungen unter anderem an die Dokumentation der Datenverarbeitungsprozesse festgelegt werden.**

Grundlage für die Datenverarbeitung

Generell gilt: Die Einzelperson darf nicht zum bloßen Objekt der Datenverarbeitung gemacht werden.

Ungeachtet der gesondert zu führenden Diskussionen zum Europäischen Gesundheitsdatenraum und zur Nutzung von Gesundheitsdaten zu Forschungszwecken auf europäischer Ebene, besteht nach Auffassung der DSK auch auf nationaler Ebene Bedarf, die Regelungen für die Nutzung von Forschungsdaten näher zu spezifizieren und kohärent auszugestalten. Ziel dabei sollte eine länderübergreifende, einheitliche Regelung zur Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken sein, die Forschungsverbünden mit Partnern in unterschiedlichen Bundesländern das Einhalten der datenschutzrechtlichen Anforderungen erleichtert.

Soweit Ärztinnen und Ärzte und andere Berufsgeheimnisträger ermächtigt werden sollen, personenbezogene Daten zu Forschungszwecken zu übermitteln, muss die Regelung mit dem Berufsrecht in Einklang stehen.

Die datenschutzrechtliche Einwilligung als Grundlage für die Datennutzung kann dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen. Sie muss freiwillig erfolgen, setzt eine umfassende Information voraus und ist jederzeit widerruflich.

Es ist Aufgabe des Gesetzgebers, im Allgemeininteresse liegende Forschung mit Gesundheitsdaten zu ermöglichen, aber auch ihre Grenzen festzulegen und die Interessen der betroffenen Personen zu wahren. Der Gesetzgeber darf diese komplexen Fragestellungen nicht vollständig auf die betroffenen Personen und die Forschenden verlagern.

Sofern eine gesetzliche Regelung Rechtsgrundlage einer Datenverarbeitung zu Forschungszwecken sein soll, muss sie in jedem Fall normenklar wirksam den Schutz des Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen. Eine solche Regelung kann bei der Nutzung von Daten aus anderen Quellen, beispielsweise Behandlungsdaten aus Krankenhäusern, aus medizinischen Registern oder auch aus anderen Forschungsprojekten (so genannte Sekundärnutzung) datenschutzkonforme Forschung ermöglichen oder erleichtern, wenn das Einholen einer ausdrücklichen Einwilligung nicht durchführbar wäre oder das Forschungsvorhaben ernsthaft beeinträchtigen würde.

Zweck der wissenschaftlichen Forschung

Eine gesetzliche Grundlage für die Nutzung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken muss einen Ausgleich insbesondere zwischen den verfassungsrechtlich geschützten Interessen schaffen: dem Recht der betroffenen Personen auf Kontrolle über ihre Daten (so genanntes "informationelles Selbstbestimmungsrecht") einerseits und der Forschungsfreiheit der Wissenschaftler und wissenschaftlichen Einrichtungen andererseits.

Eine gesetzliche Grundlage für die Verarbeitung personenbezogener Daten zu Forschungszwecken sollte im Rahmen der Interessenabwägung unter anderem Gemeinwohlinteressen – insbesondere das öffentliche Interesse an den Erkenntnissen und den Nutzen für die Allgemeinheit – berücksichtigen. Es bedarf der näheren Bestimmung durch den Gesetzgeber, was inhaltlich der Forschung im Gemeinwohlinteresse entspricht und welche weiteren Anforderungen an das Verfahren und die Durchführung der Forschung gestellt werden.

Geeignete Garantien für die Rechte und Freiheiten betroffener Personen

Eine gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten muss angemessene Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen enthalten.

Die Privilegierung der Forschung als Zweck der Verarbeitung personenbezogener Daten in der Datenschutz-Grundverordnung wird flankiert von zusätzlichen Anforderungen, vor allem zur Datenminimierung und zur frühestmöglichen Anonymisierung. Da die Anonymisierung den besten Schutz für die Rechte und Freiheiten der betroffenen Personen bietet, ist die Umsetzung dieser Schutzmaßnahme immer vorrangig zu prüfen.

Soweit der Forschungszweck mit anonymisierten Daten erreicht werden kann, dürfen nur anonymisierte Daten verarbeitet werden. Dabei bestehen hohe Anforderungen an die Anonymisierung personenbezogener Daten. Soweit zur Erreichung des Forschungszwecks eine vollständige Anonymisierung nicht möglich ist, sind effektive Maßnahmen der Pseudonymisierung vorzusehen. Darüber hinaus sind technische und organisatorische Schutzmaßnahmen entsprechend dem für die bei Gesundheitsdaten gesteigerten Anforderungen gemäß dem Stand der Technik zu treffen, darunter solche zur Pseudonymisierung und Verschlüsselung der Daten.

Falls Datenverarbeitungen auch in Ländern außerhalb des Europäischen Wirtschaftsraums stattfinden sollen, entstehen dadurch Risiken, denen mit besonderen Garantien zu begegnen ist. Dies ist nach der DSGVO gewährleistet mit Beschlüssen nach Artikel 45 DSGVO und bei Garantien nach Artikel 46 DSGVO einschließlich gebotener ergänzender Maßnahmen. Auch in allen anderen Fällen sollten Pseudonymisierungen oder Verschlüsselungen ausschließen, dass die Daten im Drittland einer spezifischen Person zugeordnet werden können.

Pseudonymisierung durch Vertrauensstellen

Die Aufgabe der Pseudonymisierung der Gesundheitsdaten sollte gesetzlich an unabhängige und eigenverantwortliche Vertrauensstellen übertragen werden. Dafür ist entscheidend, diese Stellen völlig unabhängig auszugestalten und insbesondere Weisungen von wissenschaftlich Forschenden bezüglich der von den Vertrauensstellen verarbeiteten Daten auszuschließen. Die konkreten Aufgaben, Rechte und Pflichten der Vertrauensstellen sind zu definieren. Je nach Ausgestaltung ist zudem die eigene Verantwortlichkeit dieser Stellen für die Datenverarbeitung im Interesse der Wahrung der Betroffenenrechte festzulegen.

Kontrolle durch die betroffenen Personen: Mitwirkung und Widerspruch

Will der Gesetzgeber die Verarbeitung zu Forschungszwecken nicht auf eine Einwilligung, sondern auf eine gesetzliche Grundlage stellen, sollte er die Einbindung der betroffenen

Personen vorsehen. Dabei ist zumindest sicherzustellen, dass die betroffene Person in der Regel einer Verarbeitung der personenbezogenen Daten zu Forschungszwecken voraussetzungslos widersprechen kann. Ausnahmen können nur für gesetzlich konkret bestimmte Einzelfälle vorgesehen werden, wenn dieses Recht den Forschungszweck unmöglich macht oder ernsthaft beeinträchtigt. Das Verfahren ist so auszugestalten, dass der Widerspruch möglichst unkompliziert ausgeübt werden kann.

Die betroffenen Personen müssen über die Verarbeitungsschritte informiert werden sowie Gelegenheit erhalten, sich leicht zu informieren. Digitale Methoden oder Managementsysteme, wie Datencockpit, Dashboard oder Portal, sollen dabei Information, Kontrolle und Mitwirkung vereinfachen, indem sie Nachrichten übermitteln und digitale Einwilligungserklärungen zulassen. Durch entsprechende Vorgaben sollten Lösungen erreicht werden, die Bürgerinnen und Bürgern einheitliche und leicht zugängliche Wege bieten, ihre Kontrollrechte auszuüben.

Sichere Datenbereitstellung

Zunächst ist ein Verfahren festzulegen, in dem zuverlässig überprüft werden kann, ob ein Zugriff auf die Daten datenschutzrechtlich zulässig ist (Use-and-Access-Verfahren). Bei der Bereitstellung von personenbezogenen Daten für Forschende müssen besondere technische und organisatorische Anforderungen vorgeschrieben werden. So sollte ein Zugang zu den Daten vorrangig in einer sicheren Umgebung der Zugangsstelle vorgesehen werden. Ein Zugriff oder Abruf sollte nur dann möglich sein, wenn Forschende zuvor nachweisen, dass sie angemessene technische und organisatorische Maßnahmen implementiert haben und den Stand der Technik einhalten.

Um den Verantwortlichen Hilfestellung zur Beachtung einheitlicher Mindeststandards zu geben, sollten generelle Risiken der Verarbeitung im Wege einer gesetzlichen Datenschutz-Folgenabschätzung ermittelt und berücksichtigt sowie grundlegende Maßnahmen zur Risikominimierung unmittelbar gesetzlich geregelt werden. Unabhängig davon ist von den Verantwortlichen eine Datenschutz-Folgenabschätzung für jeweils bevorstehende Forschungsvorhaben durchzuführen.

Verknüpfung von Datensätzen

Sofern eine gesetzliche Grundlage geschaffen werden sollte, um Datensätze aus verschiedenen Quellen, beispielsweise aus medizinischen Registern, zu verknüpfen, sind besondere Sicherheits- und Schutzmaßnahmen vorzusehen. Die Verknüpfung erhöht das Risiko für die Rechte und Freiheiten natürlicher Personen, wenn sie anhand der zusammengeführten Informationen leichter zu identifizieren sind. Sie verstärkt darüber hinaus

das Risiko, dass Zweckbindungen nicht eingehalten werden, dass zusätzliche, nicht zur Erreichung des Forschungszwecks erforderliche Informationen in einer für die betroffenen Personen wenig überschaubaren Weise generiert oder auch unrichtige Informationen erzeugt werden. Es sind besondere Record-Linkage-Verfahren vorzusehen, die nur eine anlassbezogene und temporäre Zusammenführung zulassen sollten. Die betroffenen Personen sollten über ein Einwilligungsmanagementsystem die Gelegenheit haben, in Kenntnis der Risiken der Zusammenführung aktiv zuzustimmen. Alternativ müssen technische Methoden oder Maßnahmen sicherstellen, dass die Reidentifizierung der betroffenen Person trotz der Verkettung ausgeschlossen ist.

Bei der Verarbeitung von Daten zu Forschungszwecken muss stets unter Beachtung der vorliegenden Risiken geprüft werden, ob und inwieweit Daten zentral oder dezentral gespeichert oder verarbeitet werden. Soweit dies vom Forschungszweck her möglich ist, sollten die Daten am Ort der Speicherung ausgewertet werden, sodass den Ort der sicheren Speicherung nur anonyme Ergebnisse der Datenauswertung verlassen. Dabei ist eine Mehrfachspeicherung zu vermeiden.

Partizipation und Teilnahme

Im Zusammenhang mit der Gesundheitsforschung gibt es bereits vielfältige Ansätze zur Partizipation der betroffenen Personen. Einige Forschungsvorhaben und Register ermöglichen den betroffenen Personen, sich über Vorhaben und daraus resultierende Erkenntnisse zum Beispiel zu Behandlungsalternativen oder Therapien zu informieren, darüber zu diskutieren und sich bestimmte Forschungsthemen zu wünschen. Diese Partizipation sollte gesetzlich verankert werden.

Denkbar sind Webportale mit weiterführenden Informationen über konkrete Forschungsprojekte sowie einzelne darauf bezogene Krankheitsbilder und in diesem Zusammenhang stehende Therapieziele, Diskussionsforen, Newsletter oder Veröffentlichungen von Datenauswertungen.

Klare Verantwortlichkeiten

Die DSK empfiehlt, gesetzlich zu bestimmen, wer datenschutzrechtlich für einzelne Verarbeitungsschritte verantwortlich ist. Die datenschutzrechtliche Verantwortlichkeit ist lückenlos zu regeln, insbesondere bei der Übermittlung zwischen Forschungseinrichtungen, um sicherzustellen, dass die betroffenen Personen ihre Datenschutzrechte ausüben können. Es sind rechtsklare Regelungen zur Aufbewahrungsdauer und Löschung von Forschungsdaten festzulegen, die sowohl das Recht auf informationelle Selbstbestimmung der betroffenen Personen als auch das Interesse der wissenschaftlichen Forschung an einer

späteren Überprüfbarkeit der Forschungsergebnisse berücksichtigen. Die aus Sicht des Datenschutzes besonders relevanten Instrumente der Verschlüsselung, Pseudonymisierung und Anonymisierung sollten vom Gesetzgeber präzisiert werden.

Daten aus medizinischen Registern

Eine gesetzliche Regelung zur Nutzung von personenbezogenen Daten für Forschungszwecke sollte zudem spezifische Vorgaben für medizinische Register schaffen. Sie sollte einheitliche Anforderungen für die Datenverarbeitung in den Registern enthalten.

Hierzu sollte zunächst ein laufendes, zentrales Verzeichnis der bestehenden Register im Gesundheitsbereich errichtet werden, um eine strukturierte Übersicht über vorhandene Daten zu bieten. Dies schafft für die betroffenen Personen ebenso wie für die Forschenden Transparenz. Zugleich vermeidet dies mehrfache Datensammlungen mit gleichen Inhalten und fördert so den Grundsatz der Datenminimierung.

Weiter sind Standards für die Qualität medizinischer Register und der dortigen Verarbeitung festzulegen, die auch Vorgaben zum Datenschutz und zur Datensicherheit enthalten müssen. So sollten die von den Registern einzuhaltenden technisch-organisatorischen Maßnahmen harmonisiert werden. Zugleich sollte ein Verfahren vorgesehen werden, mit dem die Einhaltung dieser Standards – in regelmäßigen Abständen wiederholt – geprüft und nachgewiesen wird.

Eine Datenverarbeitung in den Registern ist stets nur zulässig, wenn die Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet ist. Eine Befugnis zur Übermittlung von personenbezogenen Daten, insbesondere Patientendaten, in ein Register setzt dabei mindestens die normenklare Definition des Datenkranzes und die Erforderlichkeit der Erfassung aus medizinisch-fachlicher Sicht voraus. Eine ausdrückliche Meldepflicht ist nur in besonderen Ausnahmefällen denkbar und muss aus verfassungsrechtlichen Gründen gesetzlich festgelegt sein.

Sollte eine zentrale, koordinierende Stelle vorgesehen werden, könnte diese hinsichtlich der Betroffenenrechte eine Beratungs- und Lotsenfunktion wahrnehmen. Um die zuverlässige Durchführung dieser Aufgaben zu gewährleisten, ist eine öffentliche Stelle hiermit zu betrauen und die datenschutzrechtliche Verantwortlichkeit der Stelle ebenso wie die datenschutzrechtliche Aufsicht eindeutig festzulegen.

Normenklare Regelung eines Forschungsgeheimnisses

Bereits mit ihrer Entschließung im Jahr 2004 hat die 67. DSK die Einführung eines Forschungsgeheimnisses gefordert und diese Forderung im März 2022 bekräftigt. Hierdurch

sollte die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe gestellt, deren Beschlagnahme verboten und ein Zeugnisverweigerungsrecht für wissenschaftlich Forschende und ihre Berufshelfer geschaffen werden. Die DSK erinnert eindringlich an diese Forderung und ist bereit, entsprechende Vorhaben beratend zu begleiten.

Überwachung und Aufsicht

Die unabhängigen Datenschutzaufsichtsbehörden müssen die Einhaltung der datenschutzrechtlichen Regelungen zur Verarbeitung personenbezogener Gesundheitsdaten im Forschungskontext lückenlos überwachen und durchsetzen können. Sie müssen auch gegenüber öffentlichen Stellen mit Befugnissen ausgestattet werden, erforderliche Anordnungen durchsetzen zu können. Dazu gehört auch die – europarechtlich ohnehin gebotene und in Deutschland bisher ausgeschlossene – Möglichkeit, sofortigen Vollzug von Maßnahmen anordnen zu können.

Um eine effektive und konstruktive Aufsicht zu gewährleisten, sind konkrete Anforderungen an die prüffähige Dokumentation der Verarbeitungsschritte und die zu implementierenden technischen und organisatorischen Maßnahmen vorzusehen. Ebenso sind die forschenden Einrichtungen mit ausreichendem datenschutzrechtlichen Sachverstand auszustatten.