4. 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 2021. Redaktionsschluss war der 31. Dezember 2021.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Basta? Wie und wo die DSGVO tatsächlich wirkt

Wenn diese Zeilen veröffentlicht werden, gilt die Datenschutzgrundverordnung (DSGVO) seit 46 Monaten. Am 25. Mai 2022 werden es vier Jahre sein. Auch wenn dies nach einem langen Zeitraum klingt, ist es doch für ein Gesetzeswerk nur ein Wimpernschlag. Jedenfalls noch nicht lange genug, um eine "gewachsene Faktizität eingewöhnter und tradierter Lebensformen" entfaltet zu haben, wie sie Habermas für die soziale Geltung von Normen voraussetzt (Faktizität und Geltung, Seite 47).

Um auch für die DSGVO überall die "faktisch zu erwartende Akzeptanz im Kreise der Rechtsgenoss:innen" herzustellen, muss es daher noch ein Weilchen bei der "Androhung rechtsförmig definierter und vor Gericht einklagbarer Sanktionen" als der Geltungsquelle "gesatzten Rechts" bleiben. Auch im Land Bremen ist es jetzt deshalb mit der Verhängung von Administrative Fines (Verwaltungsbußgeldern) für Verstöße gegen die DSGVO losgegangen. Die datenschutzrechtlichen Aufsichtsbehörden in der Europäischen Union (EU) sind nach Artikel 83 DSGVO angewiesen, diese Administrative Fines in jedem Einzelfall in wirksamer, verhältnismäßiger und abschreckender Höhe zu verhängen. Davon, dass dies überall in der EU geschieht, zeugt eine Webseite, die öffentlich zugängliche Informationen über verhängte Administrative Fines sammelt und zum Redaktionsschluss 960 Einträge aufwies, von denen der höchste bei 746 Millionen Euro lag. Meine Kollegin aus Luxemburg hatte diese Administrative Fine im Juli 2021 gegen Amazon Europe verhängt. Im September war eine Administrative Fine in Höhe von 225 Millionen Euro gegen WhatsApp Ireland Ltd. hinzugekommen, nachdem die französische Kollegin bereits im Jahr 2019 eine Administrative Fine in Höhe von 50 Millionen Euro gegen Google LLC verhängt hatte. Im Oktober schloss sich mein hamburgischer Kollege mit der bislang vierthöchsten Administrative Fine an, die er in Höhe von 35,3 Millionen Euro wegen der Überwachung mehrerer hundert Mitarbeiter:innen eines H&M Servicecenters verhängte.

Aber das "Enforcement", also die nachdrückliche und bekräftigende Durchsetzung der Normen der DSGVO ist nicht das einzige Element, an dem abzulesen ist, ob und wie die Akteur:innen bei der Verarbeitung personenbezogener Daten die Regeln der DSGVO kennen und befolgen. Die DSGVO wirkt in vielfacher Weise. Das lässt sich auch an der datenschutzrechtlichen Entwicklung der letzten dreieinhalb Jahre im Land Bremen ablesen. Illustriert wird dies an den Zahlen der Beschwerden Betroffener (siehe hierzu Ziffer 1.1 dieses Berichts), der von verantwortlichen Stellen gemeldeten Datenschutzverletzungen (siehe hierzu Ziffer 1.2 dieses Berichts) und den im Land Bremen aber auch anderswo zu beobachtenden Fernwirkungen der DSGVO (siehe hierzu Ziffer 1.3 dieses Berichts). Und dann ist da noch ein Aspekt: Obwohl der europäische Gesetzgeber für die DSGVO im Großen und Ganzen diejenigen Normen verwendete, die er in der Vorgängerrichtlinie und in den mitgliedsstaatlichen Umsetzungsnormen vorgefunden hatte, gibt es einige Neuerungen, deren Innovationskraft

erst langsam aufscheint und die noch stärker Eingang in die informationstechnischen und juristischen Diskussionen finden sollten, um die "Rechtsgenoss:innen" von ihrer Strahlkraft zu überzeugen. Hierzu zählt auf jeden Fall die Forderung nach Transparenz über "die involvierte Logik" von Algorithmen (siehe hierzu Ziffer 1.4 dieses Berichts).

1.1 Die DSGVO wirkt, wo sie wirken wollte: Beschwerden

Der europäische Gesetzgeber nennt in Erwägungsgrund 10 die in Zeiten fortschreitender Digitalisierung notwendig gewordene "Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten", als Motivation für die Normierung der Datenschutzgrundverordnung (DSGVO). Dafür, dass diese Botschaft bei den Menschen angekommen ist, spricht der starke Anstieg von Beschwerden Betroffener auch bei der bremischen Datenschutzaufsichtsbehörde, der Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI).

Waren vor Geltung der DSGVO im Jahr 2012 – 196, im Jahr 2013 – 219, im Jahr 2014 – 209, im Jahr 2015 – 221, im Jahr 2016 – 247 und im Jahr 2017 – 281 Beschwerden bei der bremischen LfDI eingegangen, stieg diese Zahl seit dem ersten Geltungstag der DSGVO am 25. Mai 2018 sprunghaft an und verbleibt seitdem ungefähr auf diesem um zwei Fünftel angestiegenen Niveau. Im Jahr 2018 waren es 395 Beschwerden, von denen nur 86 aus den Monaten Januar bis April stammten. Im Jahr 2019 erreichten die LfDI 567 Beschwerden, im Jahr 2020 waren es 544 und im Berichtsjahr 2021 483. Damit wurden allein im Land Bremen in den letzten Jahren mindestens neun Beschwerden pro Woche erhoben.

Der Berichtsbitte des Abgeordneten Dr. Yazici im Ausschuss der Bremischen Bürgerschaft für Wissenschaft, Medien, Datenschutz und Informationsfreiheit an die LfDI ist es zu verdanken, dass wir für den Zeitraum von Januar 2016 bis August 2021 genauere Zahlen über unsere datenschutzrechtliche Aufsichtstätigkeit über öffentliche Stellen erhoben haben. Daraus ergeben sich auch Erkenntnisse in Bezug auf unsere beschwerdebezogenen Aufgaben im Allgemeinen.

1.1.1 Beschwerdegetriebene Aufsichtsarbeit

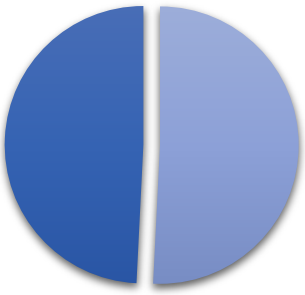
Insgesamt bezogen sich bei der Landesbeauftragten für Datenschutz und Informationsfreiheit im Erhebungszeitraum von Januar 2016 bis August 2021 797 datenschutzrechtliche Aufsichtsverfahren auf öffentliche Stellen. Davon betrafen die meisten Verfahren (212) Sachverhalte aus dem Bereich Inneres. 199 Aufsichtsverfahren bezogen sich auf die Bereiche Gesundheit/Soziales, 117 auf die Bereiche Umwelt/Verkehr/Wohnen, 75 auf die Bereiche Bürger- und Ordnungsämter und sonstige öffentliche Stellen, 68 auf den Bereich Justiz, 63 auf

die Bereiche Hochschulen/Kultur/öffentliche Kreditinstitute/Gewerbeaufsicht und ebenfalls 63 Aufsichtsverfahren betrafen den Beschäftigtendatenschutz bei öffentlichen Stellen. Von den 797 Aufsichtsverfahren gingen 391 und damit etwa die Hälfte auf Beschwerden zurück, die Betroffene bei uns erhoben hatten. Dies zeigt, dass unsere Aufsichtsarbeit gegenwärtig außerordentlich beschwerdegetrieben ist und sich damit stark daran orientiert, welche Rechtsverletzungen die Grundrechtsträger:innen selbst uns zutragen. Dass dies im Sinne der Datenschutzgrundverordnung (DSGVO) ist, zeigt der Umstand, dass die Rolle der Beschwerdeführenden in den Artikeln 77 und 78 DSGVO sehr stark ausgestaltet ist.

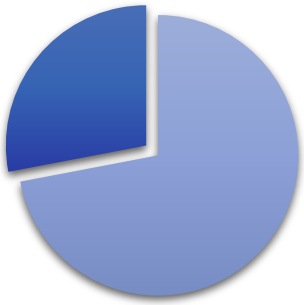
1.1.2 Beschäftigtendatenschutz bei Verletzungsgrad an der Spitze

Dank der erhobenen Zahlen lässt sich für die unterschiedlichen öffentlichen Fachbereiche feststellen, in wie vielen der durchgeführten Aufsichtsverfahren Verstöße festgestellt oder von den verantwortlichen Stellen im Wege der Meldung angezeigt wurden. Hier ragt der Bereich des Beschäftigtendatenschutzes hervor: Von 63 Aufsichtsverfahren wurden in 31 Fällen, also in der Hälfte der Fälle, datenschutzrechtliche Verletzungen festgestellt oder angezeigt. In den Bereichen Bürger- und Ordnungsämter/sonstige öffentliche Stellen wurden von 75 Verfahren 21 und in den Bereichen Hochschulen/Kultur/öffentliche Kreditinstitute/Gewerbeaufsicht von 63 Verfahren 19, also jeweils etwa in einem Drittel der Fälle, Datenschutzverletzungen festgestellt oder angezeigt. Im Bereich Inneres war es mit 49 von 212 Verfahren ein Viertel. In den Bereichen Gesundheit/Soziales waren es mit 40 von 199 ein Fünftel, in den Bereichen Umwelt/Verkehr/Wohnen mit 18 von 117 Verfahren ein Sechstel und im Bereich Justiz mit fünf von 68 ungefähr ein Vierzehntel der datenschutzrechtlichen Aufsichtsverfahren, in denen Rechtsverstöße festgestellt oder angezeigt wurden.

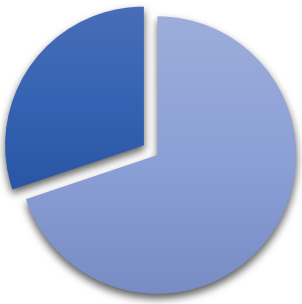
Verletzungsgrad: Beschäftigtendatenschutz



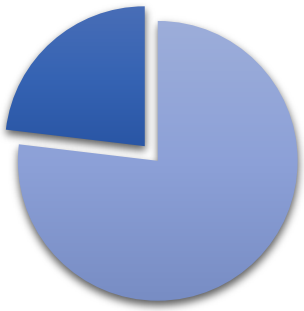
Verletzungsgrad: Bürger- und Ordnungsämter / sonstige öffentliche Stellen



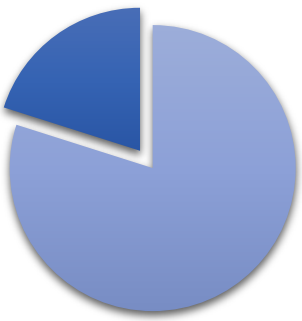
Verletzungsgrad: Hochschulen / Kultur / öffentliche Kreditinstitute / Gewerbeaufsicht



Verletzungsgrad: Inneres



Verletzungsgrad: Gesundheit / Soziales

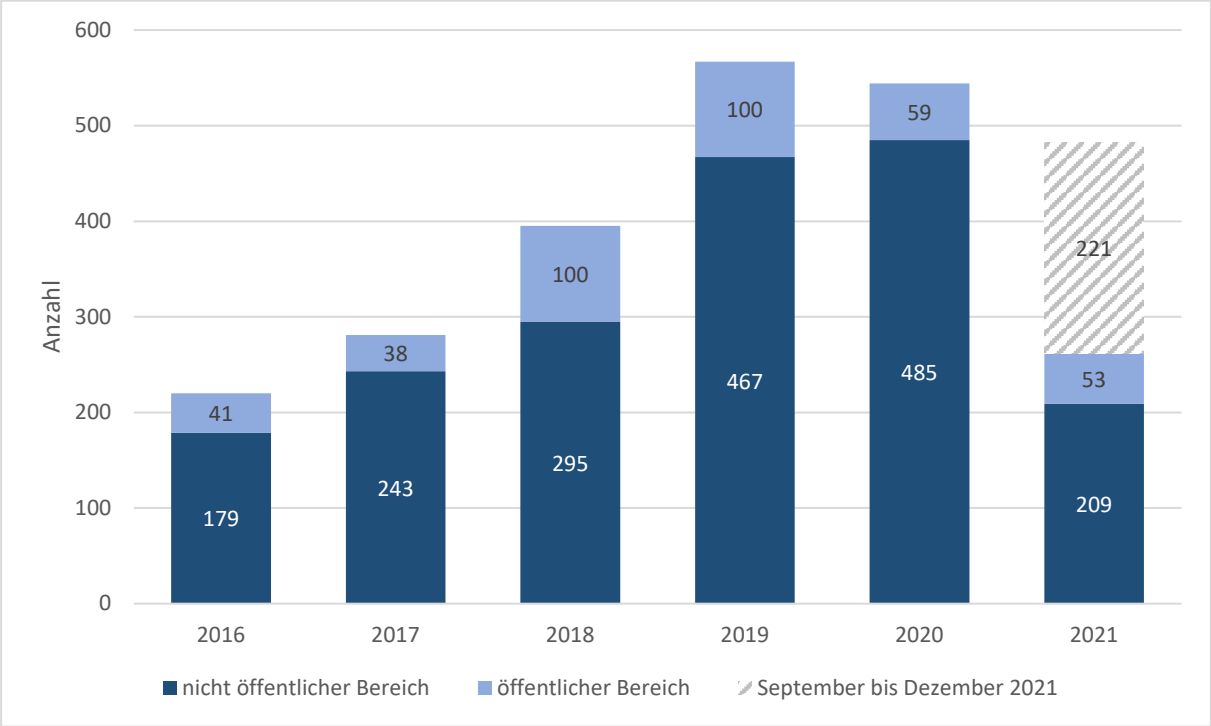


Verletzungsgrad: Umwelt / Verkehr / Wohnen

Verletzungsgrad: Justiz

1.1.3 Deutliches Überwiegen von Beschwerden über private Stellen

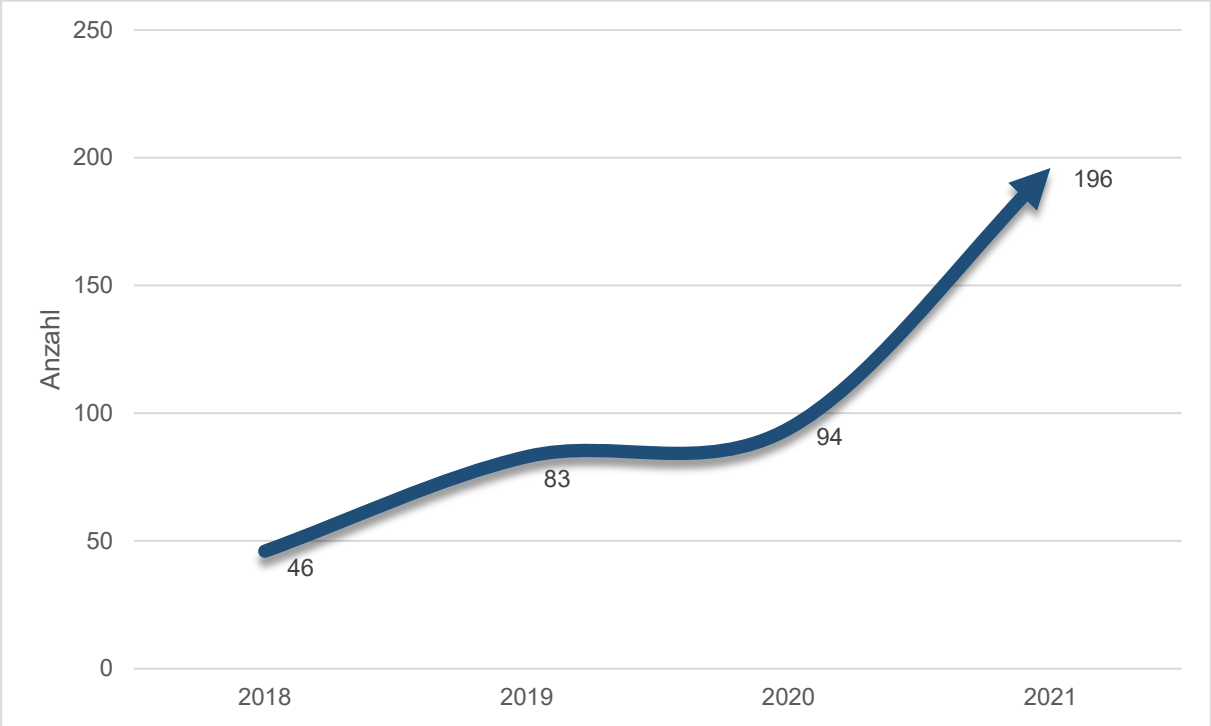
Aus den erhobenen Zahlen ergibt sich auch das Verhältnis des Anteils von Beschwerden über öffentliche Stellen zu Beschwerden über private Stellen. Von den 220 Beschwerden im Jahr 2016 bezogen sich 41, also etwa ein Fünftel, auf öffentliche Verantwortliche, also Behörden wie die Polizei, sonstige Teile der Kernverwaltung und andere öffentliche Stellen. Im Jahr 2017 waren es von 281 Beschwerden 38, also circa ein Sechstel; im Jahr 2018 von 395 Beschwerden 100, also circa ein Viertel; im Jahr 2019 von 567 ebenfalls 100, also etwa ein Sechstel; im Jahr 2020 waren es von 544 Beschwerden 59, also etwa ein Zehntel. In den ersten acht Monaten des Jahres 2021 waren es von 262 Beschwerden 53, also circa ein Fünftel.



Zu beobachten ist damit, dass der Anteil der Beschwerden, die sich auf nicht öffentliche verantwortliche Stellen bezieht, deutlich höher liegt als der Beschwerdeanteil über öffentliche Verantwortliche. Die Geltung der Datenschutzgrundverordnung hat hier keine signifikante Veränderung ergeben. Nach wie vor sind es relativ konstant etwa drei Viertel bis zu fünf Sechstel der Beschwerden, die private verantwortliche Stellen personenbezogener Daten betreffen. Das Jahr 2020, in dem es eine große Zahl von Beschwerden gegen die pandemiebedingte Kontaktdatenverarbeitung durch Dienstleistungsbetriebe wie Gaststätten gab, wies mit neun Zehnteln der Beschwerden einen noch höheren Anteil auf.

1.2 Die DSGVO wirkt stetig ansteigend: Datenpannen

Ein Bereich, in dem sich der kontinuierliche Geltungsanstieg der Datenschutzgrundverordnung (DSGVO) deutlich zeigt, ist der Bereich der von datenschutzrechtlich Verantwortlichen selbst gemeldeten Datenschutzverletzungen. Artikel 33 DSGVO verpflichtet Verantwortliche, der zuständigen Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden zu melden. Der bei uns zu verzeichnende Anstieg dieser Meldungen von 46 im Jahr 2018, wovon nur eine sich auf den Zeitraum vor Geltung der DSGVO bezog, auf 83 im Jahr 2019, 94 im Jahr 2020 und jetzt 196 im Berichtsjahr 2021, zeigt, dass diese Rechtspflicht von einer zunehmenden Anzahl von Verantwortlichen erfüllt wird.



Angesichts der erwähnten festgestellten Rechtsverstöße allein im öffentlichen Bereich erscheinen diese Zahlen immer noch gering. Da die Frage, wie ein datenschutzrechtlicher Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang die beziehungsweise der Verantwortliche oder die Auftragsverarbeiterin beziehungsweise der Auftragsverarbeiter den Verstoß mitgeteilt hat, nach Artikel 83 Absatz 2 Satz 2 Buchstabe h DSGVO bei der Bemessung der Höhe der Administrative Fine (Verwaltungsgeldbuße) zu berücksichtigen ist, ist es wahrscheinlich, dass die Zahl der uns gemeldeten Datenschutzverstöße weiter steigen wird.

1.3 Die DSGVO wirkt selbst dort, wo sie gar nicht gilt

Bei der Datenschutzgrundverordnung (DSGVO) ist es wie beim Sähen: Die Samen gehen gelegentlich an anderen Stellen auf, als an denen, an denen sie verstreut wurden. Inner- und außerhalb Europas entfaltet die DSGVO auch außerhalb ihres sachlichen und örtlichen Anwendungsbereiches Fernwirkungen.

1.3.1 Überraschende Fernwirkung im Bereich der JI-Richtlinie

Vom sachlichen Anwendungsbereich der Datenschutzgrundverordnung (DSGVO) ist ausweislich ihres Artikels 2 Absatz 2 Buchstabe d die Verarbeitung personenbezogener Daten "durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" ausgenommen. Dieser Bereich blieb jedoch nicht ungeregelt, da der europäische Gesetzgeber die sogenannte JI-Richtlinie ("Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung") erließ. Als Richtlinie musste diese europäische Norm bis zum 6. Mai 2018 in mitgliedstaatliches Recht umgesetzt werden. Im Land Bremen erfolgte diese Richtlinienumsetzung erst deutlich später.

Gleichwohl entstand in der Zwischenzeit selbst in der datenschutzrechtlichen Aufsichtspraxis nicht der Eindruck eines Normenvakuums. Die DSGVO, die seit 25. Mai 2018 für diejenigen Verarbeitungen personenbezogener Daten durch Polizei, Strafjustiz, Staatsanwaltschaft und Strafvollzug galt, die nicht der Strafverfolgung und der Prävention von Straftaten dienen, entfaltete hier auch in den anderen Tätigkeitsbereichen dieser Verantwortlichen offensichtlich eine Art Fernwirkung. Nicht nur deshalb regte die Landesbeauftragte für Datenschutz und Informationsfreiheit (leider vergeblich) in ihren Stellungnahmen zu den auf die Umsetzung der JI-Richtlinie gerichteten Gesetzen die landesgesetzgeberische Normierung genau dieser bereits "eingeübten" DSGVO-Normen an. Ob es für die Rechtsanwendenden beispielsweise in der Polizei und bei den sozialen Diensten der Justiz, für deren JI-Richtlinienbezogene Tätigkeiten seit dem 8. Dezember 2020 das Bremische Polizeigesetz gilt, nicht doch übersichtlicher wäre, wenn sie nicht – wie es nun der Fall ist – vor jeder Verarbeitung personenbezogener Daten jeweils entscheiden müssten, ob sie sich im Anwendungsbereich der DSGVO oder der JI-Richtlinie befinden, bleibt fraglich. Da es sich bei der JI-Richtlinie um eine durch mitgliedstaatliche Rechtsakte umzusetzende Richtlinie handelt, bei der die mitgliedstaatlichen Gesetzgeber einen Regelungsspielraum haben, bleibt es dem bremischen Gesetzgeber weiterhin unbenommen, jederzeit weite Teile des derzeitig geltenden Polizeigesetzes durch den einfachen Satz "Für alle Verarbeitungen personenbezogener Daten im Anwendungsbereich dieses Gesetzes gilt die DSGVO" zu ersetzen.

1.3.2 Weltstandard

Ihre Fernwirkung besteht aber auch darin, dass sich die Datenschutzgrundverordnung (DSGVO) in datenschutzrechtlicher Hinsicht auch außerhalb ihres territorialen Anwendungsbereichs mehr und mehr zum Weltstandard entwickelt. Dies gilt nicht nur deshalb, weil Staaten, für die – wie dies bereits für Japan, das Vereinigte Königreich und die Republik Korea der Fall war – Angemessenheitsbeschlüsse der Kommission ergehen, nach Artikel 45 DSGVO ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten aufweisen müssen. Die DSGVO dient auch als Vorbild anderer datenschutzrechtlicher Normierungsinitiativen. So orientierte sich Brasilien bei der Formulierung seines seit 2020 geltenden Datenschutzgesetzes ebenso an der DSGVO, wie es beim 2019 in Kraft getretenen kenianischen Datenschutzgesetz und beim 2020 in Kraft getretenen kalifornischen Consumer Privacy Act der Fall war. In der Schweiz wird Mitte 2022 ein Datenschutzgesetz in Kraft treten, das ebenso wie ein in Indien diskutierter Gesetzesentwurf einige Ähnlichkeiten mit der DSGVO aufweist. Und auch, wenn Lob für die DSGVO aus den Mündern der Konzernchefs der üblichen verdächtigen Internetgiganten irritierend wirkt, zeigt sich daran doch, dass es für weltweit agierende Firmen zweckmäßig ist, sich an den Regeln der DSGVO zu orientieren, um nicht für mehrere Weltregionen unterschiedliche Anwendungen programmieren zu müssen.

1.4 Transparenz über die involvierte Logik von Algorithmen

All diese Entwicklungen zeigen zum einen, dass die "Rechtsgenoss:innen" bremen-, deutschland-, europa- und weltweit mehr und mehr Akzeptanz für die Datenschutzgrundverordnung (DSGVO) als Regelungswerk entwickeln. Gleichzeitig wird aber deutlich, dass es für den weltweiten Schutz personenbezogener Daten äußerst wichtig ist, auch bei der Rechtsanwendung innerhalb der Europäischen Union die in den Normtexten der DSGVO vorhandenen Potenziale in grundrechtsfreundlicher Hinsicht vollständig auszuschöpfen. Nur so kann es gelingen, dass die DSGVO ein Europa- und Weltstandard ist und bleibt, der dem genannten selbstformulierten Anspruch des europäischen Gesetzgebers gerecht wird, die Rechte der betroffenen Personen zu stärken und präzise festzulegen und die Verpflichtungen für die datenschutzrechtlich Verantwortlichen zu verschärfen.

Bei der Frage nach der "präzisen Festlegung" der Rechte der betroffenen Personen ist jedoch in einigen Fällen noch Luft nach oben. Das gilt beispielsweise für die Verpflichtung zur Transparenz über "die involvierte Logik" von Algorithmen. In ihren Artikeln 13 und 14 (jeweils Absätze 2 Buchstabe f beziehungsweise g) verpflichtet die DSGVO Verantwortliche, im Falle automatisierter Entscheidungsfindungen aussagekräftige Informationen über "die involvierte Logik" sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person ("meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject") zur

Verfügung zu stellen. Dieser durch die DSGVO eingeführte Begriff bedarf der Konkretisierung. Gemeint ist damit nämlich gerade nicht das pure Offenlegen der unzähligen Rechenoperationen. Eine solche unstrukturierte Transparenz würde in Zeiten von Giant Data nur zu sinnlosen Informationsfluten führen, die für Nicht-Informatiker:innen zudem unverständlich wären. Stattdessen brauchen wir sinnvoll strukturierte Filter, die die Parameter erkennen lassen, nach denen künstliche Intelligenz trainiert. Und weil Artikel 12 der DSGVO dazu verpflichtet, die Informationen "in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu übermitteln, müssen sich die Betroffenen dabei nicht mit Konvoluten kryptischer Kauminformationen abspeisen lassen.

Auch im Kommissionsvorschlag für den Digital Services Act findet sich in Artikel 12 der Gedanke der Verpflichtung zur auch für Nicht-Informatiker:innen verständlichen Offenlegung der wesentlichen Informationen im Zusammenhang mit algorithmischen Entscheidungsfindungen. Nach dem vorgeschlagenen Artikel 23 müssen Online-Plattformen über die "etwaige Verwendung automatisierter Mittel zur Moderation von Inhalten, mit Angabe der genauen Zwecke, mit Indikatoren für die Genauigkeit der automatisierten Mittel bei der Erfüllung dieser Zwecke und mit angewandten Schutzvorkehrungen" informieren. "Sehr große Online-Plattformen" müssen nach dem geplanten Artikel 29 in ihren allgemeinen Geschäftsbedingungen in klarer, barrierefreier und leicht verständlicher Weise die wichtigsten Parameter darlegen, die in ihren Empfehlungssystemen verwendet werden, sowie alle Optionen, die sie den Nutzer:innen zur Verfügung stellen, damit diese die wichtigsten Parameter ändern oder beeinflussen können, darunter mindestens eine Option, die nicht auf Profiling beruht.

Die Europäische Union ist also nicht davon abgekehrt, Stellen, die die datenschutzrechtliche Verantwortung für die Verarbeitung personenbezogener Daten mit Hilfe von Algorithmen tragen, dazu zu verpflichten, allgemeinverständlich Rösse, Reiter:innen und Reiseziele zu benennen.

Es bleibt noch viel zu tun.

Dr. Imke Sommer

2. Zahlen und Fakten

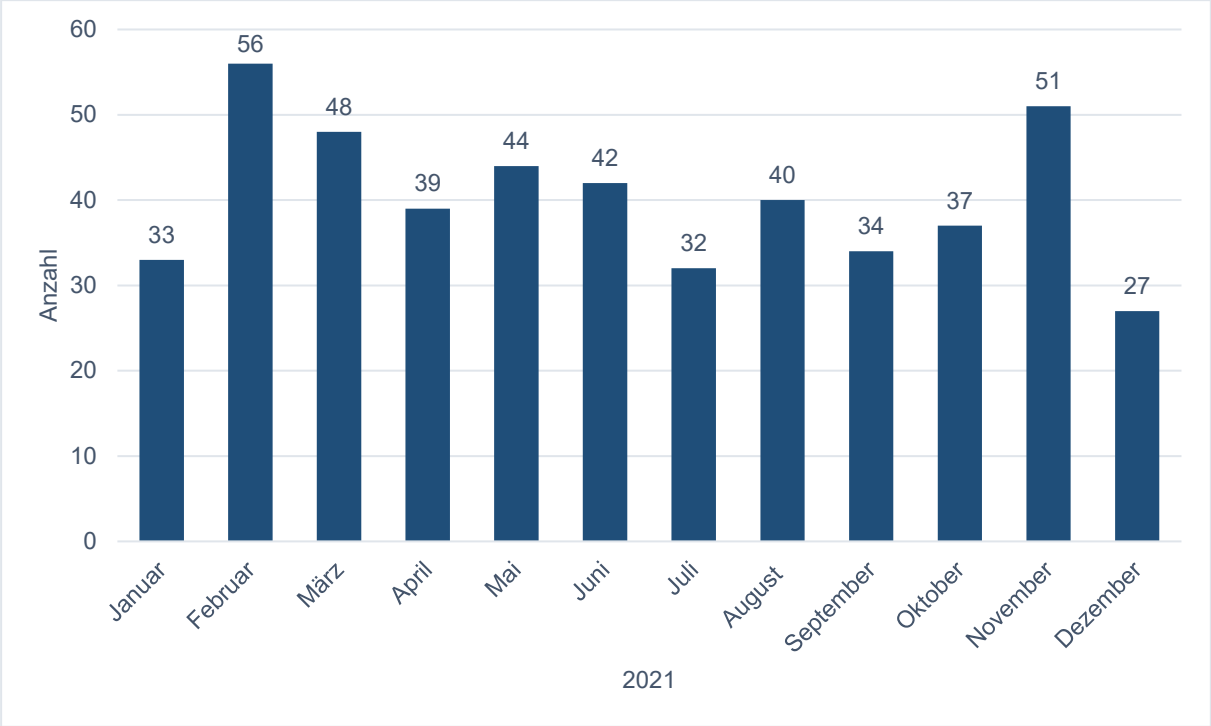
Die Datenschutzgrundverordnung macht es den Aufsichtsbehörden in Artikel 59 zur Pflicht, jährlich über ihre Tätigkeit zu berichten. Um die Transparenz und Vergleichbarkeit innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und für die Öffentlichkeit 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 Akkreditierung von Zertifizierungsverfahren und Zertifizierungsstellen (siehe Ziffer 2.9 dieses Berichts) und das Europäische Binnenmarkt-Informationssystem (siehe Ziffer 2.10 dieses Berichts).

2.1 Auswahl datenschutzrelevanter Sachverhalte, die 2021 an die Landesbeauftragte für Datenschutz und Informationsfreiheit herangetragen wurden

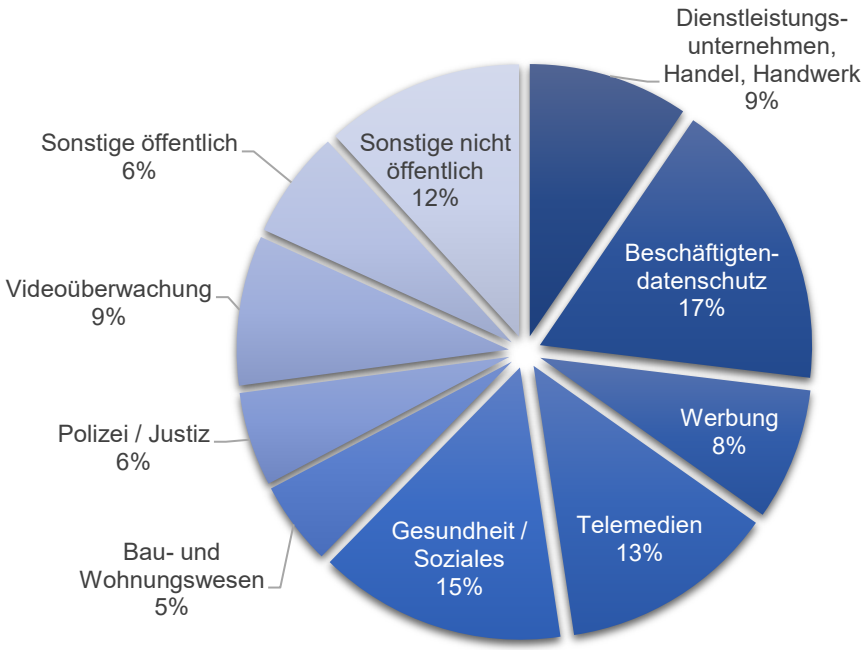
Monat	Beschwerden	Beratungs-anfragen	Meldungen Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte
Januar	33	35	9	39
Februar	56	36	15	24
März	48	44	42	24
April	39	28	13	25
Mai	44	44	12	20
Juni	42	49	13	32
Juli	32	25	15	27
August	40	27	13	25
September	34	30	17	13
Oktober	37	34	12	27
November	51	37	18	40
Dezember	27	28	17	10
Gesamt	**483**	**417**	**196**	**306**

Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

2.2 Beschwerden



In diesem Diagramm sind die monatlichen Beschwerdezahlen des Jahres 2021 dargestellt.

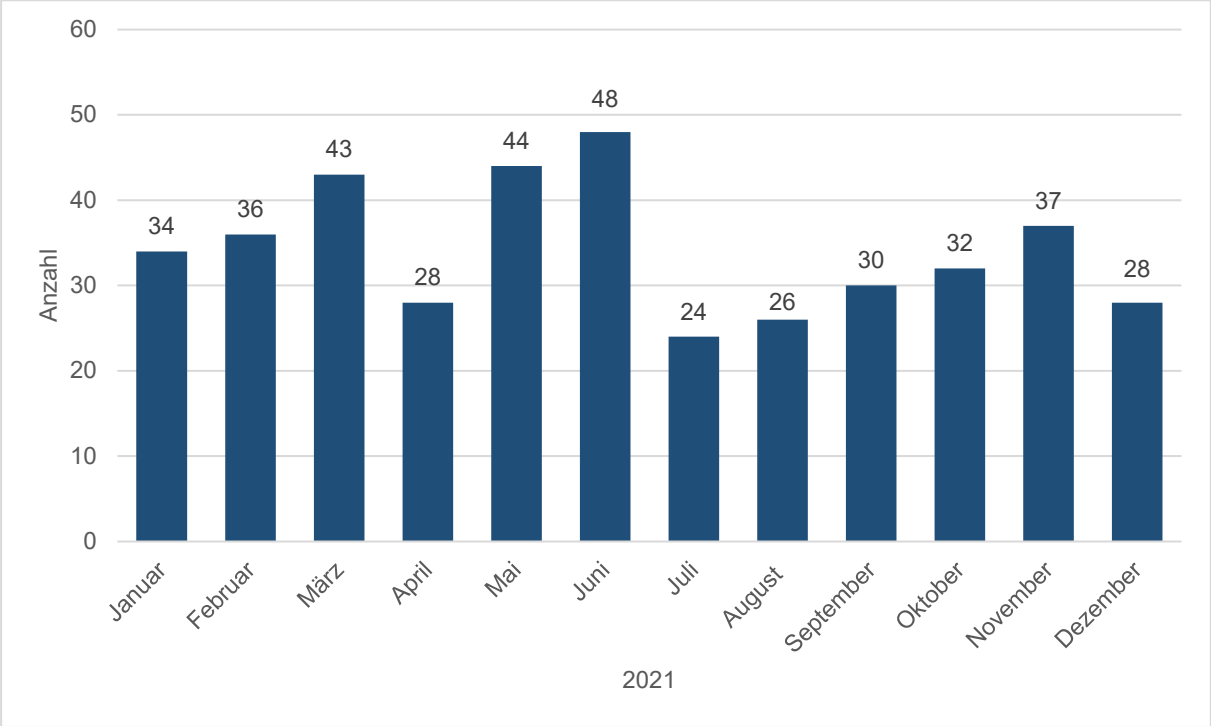


Das Diagramm zeigt die bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2021 nach Themengebieten aufgeschlüsselt.

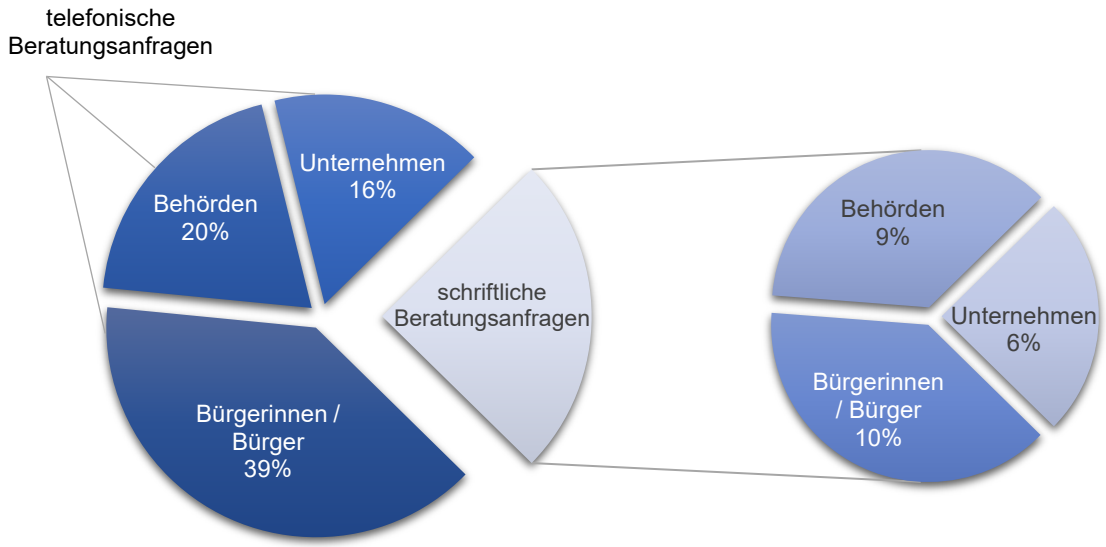
Themengebiet	AW	RW	Themengebiet	AW	RW
Dienstleistungsunternehmen, Handel, Handwerk	46	10 %	Bau- und Wohnungsunternehmen	24	5 %
Beschäftigtendatenschutz	84	17 %	Polizei / Justiz	27	6 %
Werbung	38	8 %	Videoüberwachung	43	9 %
Telemedien	62	13 %	Sonstiges (nicht öffentlich)	57	11 %
Gesundheit und Soziales	71	15 %	Sonstiges (öffentlich)	31	6 %

Die Tabelle stellt die absoluten Werte (AW) und relativen Werte (RW) der unterschiedlichen Themengebiete der Beschwerden dar.

2.3 Beratungen

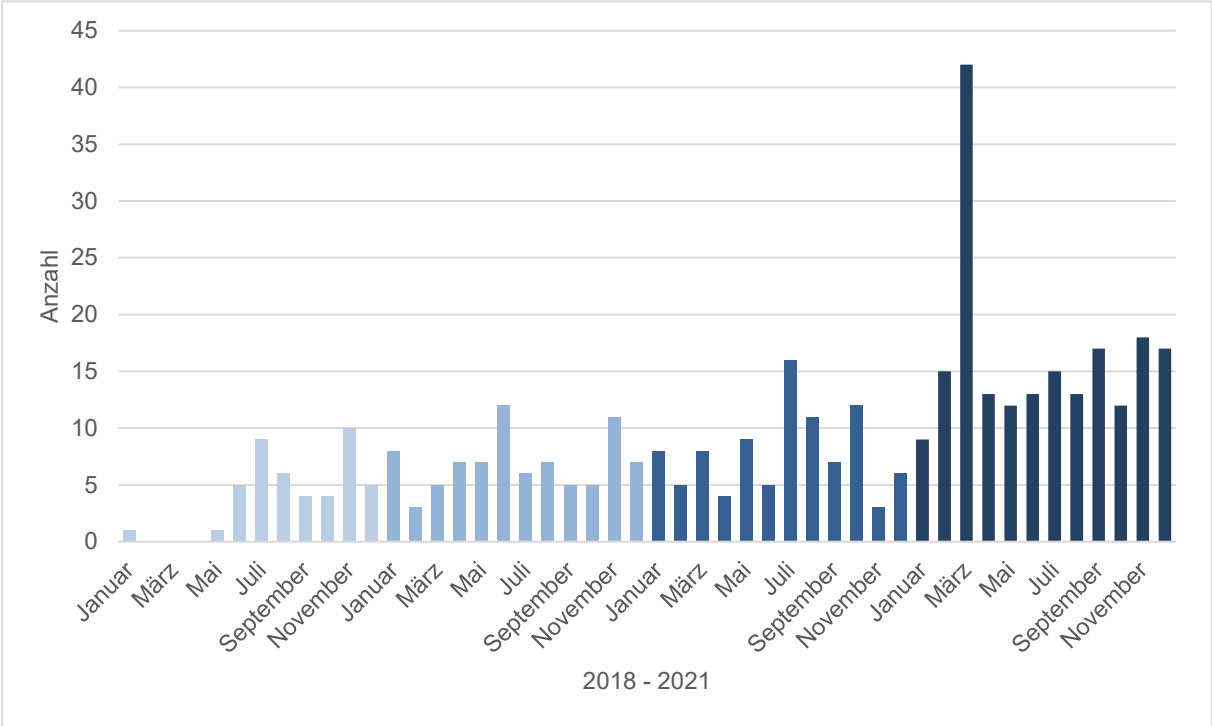


Diese Grafik gibt eine Übersicht über die Anzahl von schriftlichen und telefonischen Beratungen von Verantwortlichen und betroffenen Personen.

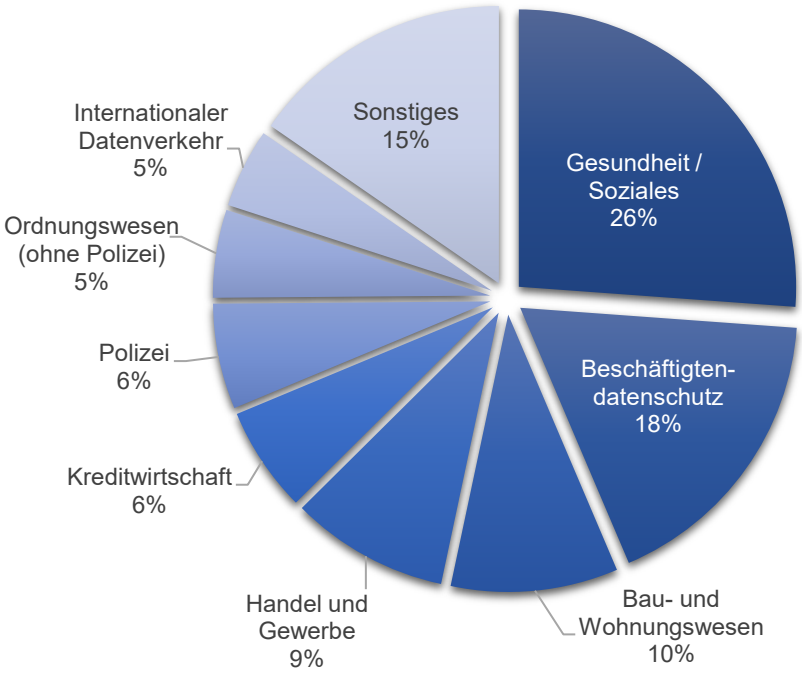


Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2021 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen. Daneben wird danach unterschieden, wer Beratungsanfragen stellt. Dies sind zum einen die Verantwortlichen (Behörden und Unternehmen) 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 der Jahre 2018 bis 2021 dargestellt.



Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2021 nach Themengebieten auf.

2.5 Abhilfemaßnahmen

Warnungen

nach Artikel 58 Absatz 2 a DSGVO: Zwei

Verwarnungen

nach Artikel 58 Absatz 2 b DSGVO: 15

Anweisungen und Anordnungen

nach Artikel 58 Absatz 2 c-g DSGVO und § 85 BremPolG: 24

Geldbußen

nach Artikel 58 Absatz 2 i DSGVO: Fünf

Widerruf von Zertifizierungen

nach Artikel 58 Absatz 2 h DSGVO: Keine

2.6 Europäische Verfahren

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

2.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Folgende Beratungen wurden im Berichtsjahr 2021 durchgeführt:

Gesundheit

- Gesetz über die Berufsvertretung, die Berufsausübung, die Weiterleitung und die Berufsgerichtsbarkeit der Ärzte, Zahnärzte, Psychotherapeuten, Tierärzte und Apotheker (Heilberufsgesetz)

Justiz

- Gesetz zur Umsetzung der Datenübermittlungspflicht von berufsständischen Versorgungseinrichtungen nach dem Gesetz zur Verbesserung des Schutzes von Gerichtsvollzieher:innen vor Gewalt sowie zur Änderung weiterer zwangsvollstreckungsrechtlicher Vorschriften
- Gesetz für die Rechtsanwaltsversorgung in der Freien Hansestadt Bremen (RAVG)

Bau und Wohnen

- Bremisches Wohnraumschutzgesetz (WoSchG)
- Verordnung über das automatisierte Verfahren zum Abruf von personenbezogenen Daten aus dem Liegenschaftskataster (LieDAV)
- Ortsgesetz über vorhabenbezogene Stellplätze, Fahrradabstellplätze und Mobilitätsmanagement in der Stadtgemeinde Bremen (Mobilitätsortsgesetz – MobOG HB)
- Bremisches Gesetz zur Durchführung der Marktüberwachung von Bauprodukten (BremBauPMÜG)

Verkehr, Umweltschutz und Geodaten

- Staatsvertrag zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen im Bereich des Ökologischen Landbaus

- Staatsvertrag 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

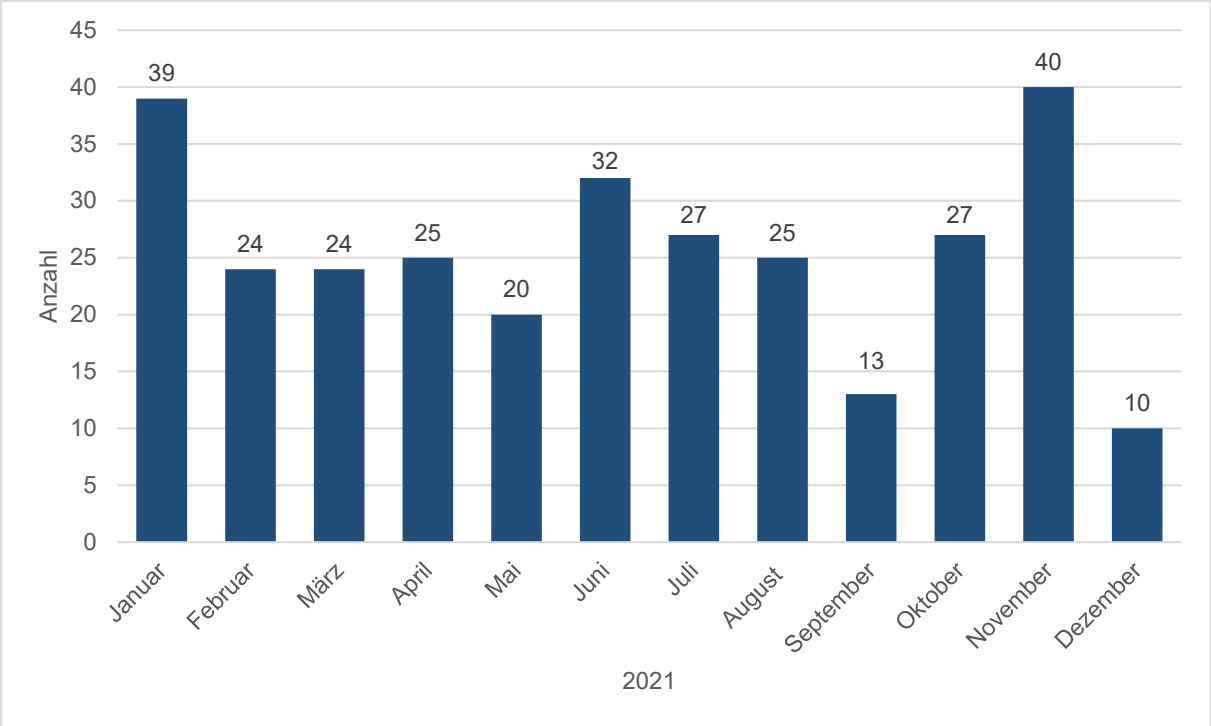
- Mantelgesetz zur Novellierung des Bremischen Wald-, Naturschutz-, Jagd- und Wasserrechts

- Gesetz über die Erhebung einer Wasserentnahmegebühr (BremWEGG)

- Gesetz zur Anpassung von Vorschriften aus dem Bereich Häfen an die Datenschutz-Grundverordnung

- Ortsgesetz zur Änderung ortsrechtlicher Regelungen im Bereich der kommunalen Abfallentsorgung

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

Gemäß Artikel 42 der Datenschutzgrundverordnung (DSGVO) haben die Datenschutzaufsichtsbehörden und damit auch die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit die Aufgabe, die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutzsiegeln und Datenschutzprüfzeichen zu fördern. Im Berichtsjahr erarbeiteten wir in Zusammenarbeit mit den anderen deutschen Aufsichtsbehörden Anforderungen an datenschutzrechtliche Zertifizierungsprogramme[1], um einen deutschlandweit einheitlichen Prüfstandard zu gewährleisten. Als zuständige Datenschutzaufsichtsbehörde prüfte die Landesbeauftragte für Datenschutz und Informationsfreiheit zudem in Zusammenarbeit mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) ein ihr vorgelegtes Konformitätsbewertungsprogramm sowie den dazugehörigen nach Artikel 42 Absatz 5 DSGVO zu genehmigenden Kriterienkatalog (siehe hierzu 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 2.9).

2.10 Europäisches Binnenmarkt-Informationssystem

Die Anzahl der zu sichtenden und zu bewertenden E-Mails, die durch das europäische Binnenmarkt-Informationssystem (Internal Market System, IMI) versandt wurden, blieb 2021 auf dem Niveau des Vorjahres. Für Verfahren nach den Artikeln 56, 60, 61, 62, 64, 65 und 66 Datenschutzgrundverordnung (DSGVO) gingen mehr als 2.500 Benachrichtigungen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit ein. Ein Großteil der Nachrichten betraf die Prüfung der Zuständigkeit. Ressourcenbedingt war es nicht möglich, dieser Aufgabe in vollem Umfang nachzukommen.

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

Der Bericht und Antrag des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit (WMDI-Ausschuss) zum 3. Jahresbericht nach der Europäischen Datenschutzgrundverordnung (DSGVO) der Landesbeauftragten für Datenschutz vom 26. März 2021 (Drucksache 20/891) und zur Stellungnahme des Senats vom 14. September 2021 (Drucksache 20/1103) lag zum Redaktionsschluss noch nicht vor.

[1] https://www.datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf

4. Datenschutzbeauftragte

4.1 in Vereinen

Bei der Bearbeitung eines Vorgangs, der einen Sportverein in Bremen betraf, erfuhren wir, dass dessen Geschäftsführerin auch als Datenschutzbeauftragte tätig war. Hieraus ergab sich eine Inkompatibilität, die mit den Bestimmungen der Datenschutzgrundverordnung (DSGVO) nicht zu vereinbaren war. Nachdem wir den Verein auf die einzuhaltenden Anforderungen aufmerksam gemacht hatten, benannte dieser einen neuen Datenschutzbeauftragten, bei dem eine Inkompatibilität nicht festzustellen war.

Auch in Vereinen erfüllen Datenschutzbeauftragte wichtige Funktionen für die Gewährleistung von korrekten, den datenschutzrechtlichen Anforderungen entsprechenden Verarbeitungen personenbezogener Daten. Auch in Fällen, in denen verantwortliche Stellen nicht zur Benennung einer oder eines Datenschutzbeauftragten verpflichtet sind, sondern die Beauftragte oder den Beauftragten freiwillig benennen, gelten im Wesentlichen die an die Funktion geknüpften Anforderungen der DSGVO. Insbesondere dürfen Personen, bei denen ein Interessenkonflikt zwischen den Aufgaben und Pflichten, die sie sonst wahrzunehmen haben, und der Beauftragtenfunktion besteht, nicht mit der Funktion der oder des Datenschutzbeauftragten betraut werden. Dies betrifft insbesondere Personen in leitender Funktion, unter anderem in der Leitung einer Abteilung, der Geschäftsführung oder im Vorsitz eines Vereins Tätige, unabhängig davon, ob diese hautberuflich oder ehrenamtlich agieren.

4.2 in Arztpraxen

Mehrfach erhielten wir im Berichtszeitraum von Arztpraxen Mitteilungen über die Funktionsbeendigung von ihnen benannter Datenschutzbeauftragter. Begründet wurde dies jeweils damit, dass Beauftragte nach § 38 Bundesdatenschutzgesetz nur zu benennen seien, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt seien. Dieses treffe bei ihnen nicht zu. Wir machten die betreffenden Arztpraxen darauf aufmerksam, dass die Rechtsgrundlage für die Benennung von Datenschutzbeauftragten die der dem mitgliedstaatlichen Recht vorgehende Europäische Datenschutzgrundverordnung (DSGVO) ist (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 4.3). Nach Artikel 37 Absatz 1 Buchstabe c, 1. Halbsatz DSGVO sind auf jeden Fall Datenschutzbeauftragte zu bestellen, wenn die Kerntätigkeit der oder des für die Datenverarbeitung Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht. Nach Artikel 9 Absatz 1 DSGVO zählen hierzu auch Gesundheitsdaten. Mit ihrem Beschluss vom 28. April 2018 zur Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Absatz 1 Buchstabe c DSGVO bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufes hatte die Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einen Katalog von Kriterien veröffentlicht, der für die Benennung von Datenschutzbeauftragten durch Arztpraxen auch weiterhin maßgeblich ist. Da die Arztpraxen, von denen wir die betreffenden Mitteilungen erhalten hatten, nach diesen Kriterien auch weiterhin eine Datenschutzbeauftragte beziehungsweise einen Datenschutzbeauftragten zu benennen haben, forderten wir diese zu einer erneuten Benennung auf. Die Arztpraxen kamen unserer Aufforderung bislang nur teilweise nach und verhielten sich insofern rechtswidrig. Wir informierten die Ärztekammer Bremen erneut über den Beschluss der DSK. Die Kammer sagte zu, unseren Hinweis auf die einzuhaltenden gesetzlichen Anforderungen und die zu beachtenden Kriterien aufzugreifen und für ihre Kammermitglieder zu veröffentlichen.

4.3 Stichprobenprüfungen von Meldungen

Im Berichtszeitraum erhielten wir auf der Grundlage von Artikel 37 Absatz 7 Datenschutzgrundverordnung (DSGVO) von öffentlichen und nicht öffentlichen Stellen ungefähr 300 Meldungen hinsichtlich der Neubenennung, der Änderung und der Funktionsbeendigung der oder des jeweiligen Datenschutzbeauftragten. Wir überprüften diese Mitteilungen stichprobenartig. Mängel ergaben sich insbesondere hinsichtlich der bei der Benennung anzuwendenden Rechtsgrundlage, bei der Zahl der zu berücksichtigenden Mitarbeitenden, die mit Aufgaben der Verarbeitung personenbezogener Daten betraut sind, bei der Vereinbarkeit der Beauftragtenfunktion mit anderen von den Beauftragten bei den meldenden Stellen wahrzunehmenden Aufgaben und bei der Wiederbesetzung des Amtes. Wir machten die meldenden Stellen auf die festgestellten Mängel aufmerksam und forderten sie auf, diese zu beheben. Die betreffenden Stellen kamen unserer Aufforderung weitgehend nach. Sofern dies nicht geschah, liegen Verstöße gegen die DSGVO vor.

4.4 Meldungen durch Unternehmen mit Sitz außerhalb Bremens

Die beziehungsweise der Verantwortliche oder die Auftragsverarbeiterin beziehungsweise der Auftragsverarbeiter sind nach Artikel 37 Absatz 7 Datenschutzgrundverordnung (DSGVO) verpflichtet, der Aufsichtsbehörde die Kontaktdaten der oder des Datenschutzbeauftragten mitzuteilen. Durch diese Verpflichtung soll der örtlich zuständigen Aufsichtsbehörde bekannt werden, wer bei der beziehungsweise dem Verantwortlichen oder bei der Auftragsverarbeiterin beziehungsweise dem Auftragsverarbeiter die oder der Datenschutzbeauftragte als Anlaufstelle in mit der Verarbeitung personenbezogener Daten zusammenhängenden Fragen ist. Gleichzeitig kann die Aufsichtsbehörde kontrollieren, ob die gesetzliche Pflicht zur Benennung einer oder eines Datenschutzbeauftragten erfüllt wurde. Mehrfach erhielten wir im Berichtszeitraum Meldungen nach Artikel 37 Absatz 7 DSGVO von Unternehmen, die ihren Sitz nicht im Land Bremen haben oder dort nur eine Filiale oder Zweigstelle betreiben. Gab es in Bremen eine Filiale oder Zweigstelle, so war von uns auch zu prüfen, ob es sich hierbei um

eine Verantwortliche beziehungsweise einen Verantwortlichen im Sinne der DSGVO handelte. War die Frage zu bejahen, nahmen wir die Meldung zu unseren Registervorgängen. Traf dies nicht zu, wiesen wir die meldende Stelle darauf hin, dass sie ihre Meldung an die für sie zuständige Aufsichtsbehörde zu richten habe.

5. Inneres

5.1 Gemeldete Datenschutzverletzungen

Aus dem Bereich Inneres erreichten uns im Berichtsjahr insgesamt sieben Meldungen der Verletzung des Schutzes personenbezogener Daten. Vier der sieben Meldungen erfolgten durch die Polizeien Bremen und Bremerhaven. Zwei dieser Meldungen bezogen sich auf mehrere Verarbeitungssysteme (insgesamt 32). In einer Meldung ging es erneut um den Verlust von Online-Anzeigen und Online-Bewerbungen (siehe hierzu 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.1), ausgelöst durch Wartungsarbeiten. Zudem erfolgten zwei Meldungen durch Bürger- und Ordnungsämter.

5.2 Polizeiliche Informationssysteme

Im Juli 2021 berichtete unter anderem das Fernsehmagazin "buten un binnen" darüber, dass die Polizei Bremen im digitalen Vorgangsbearbeitungssystem @rtus seit dessen Inbetriebnahme im Jahr 2014 lediglich diejenigen personenbezogenen Datensätze gelöscht hatte, deren Löschung im Einzelfall durch betroffene Personen oder uns erwirkt worden war. Zahlreiche personenbezogene Daten waren somit trotz bestehender Löschpflicht nicht gelöscht worden. Später stellte sich heraus, dass ähnliches für das Vorgängersystem ISA-Web und für die Ortspolizeibehörde Bremerhaven galt.

Aufgrund der den Bericht bestätigenden Aussage einer Sprecherin der Polizei Bremen im Fernsehbeitrag sprachen wir zunächst eine Beanstandung nach § 85 Absatz 1 des neuen Bremischen Polizeigesetzes aus und ordneten nach Auswertung der Stellungnahme der Polizei nach § 85 Absatz 2 des Bremischen Polizeigesetzes gegenüber der Polizei Bremen sowie der Ortspolizeibehörde Bremerhaven unter anderem an, alle rechtswidrig gespeicherten Daten unverzüglich zu löschen, Empfänger:innen, denen Daten übermittelt worden waren, über die Löschung zu benachrichtigen und ein Löschkonzept für @rtus zu erstellen, das den Vorgaben des neuen Bremischen Polizeigesetzes genügt.

Bis Mitte September wurden von der Polizei laut ihren eigenen Angaben alle löschpflichten Vorgänge gelöscht (rund 950.000 durch die Polizei Bremen). Die Löschung erfolge nun tagesaktuell nach festgelegten Fristen. Bei einem Vor-Ort-Termin überprüften wir die Datenlöschung. Wir stellen aktuell fest, dass dieser Themenkomplex noch nicht als abgeschlossen betrachtet werden kann.

Die Erfüllung der Benachrichtigungspflicht, die sich unmittelbar aus dem neuen Bremischen Polizeigesetz ergibt, erwies sich als problematisch, da die Polizei vortrug, aufgrund der Datenlöschung nicht mehr nachvollziehen zu können, wem sie welche Daten übermittelt habe. Wir beharren nach wie vor darauf, dass alle potenziellen Empfänger:innen zumindest allgemein darüber benachrichtigt werden, dass sie Daten von der Polizei erhalten haben könnten, deren Löschfrist vor der Übermittlung abgelaufen war und daher nicht übermittelt werden durften. Nur so kann sichergestellt werden, dass die Empfänger:innen ihren eigenen Datenbestand überprüfen und löschpflichtige Daten ebenfalls löschen können.

Die Erstellung eines Löschkonzepts wird zukünftig davon abhängig sein, dass Überprüfungs- und Speicherfristen durch Rechtsverordnungen geregelt werden. Zumindest die bislang fehlende umfassende Regelung der Prüffristen stellt nicht nur eine mangelhafte Umsetzung europäischer Vorgaben dar, sondern erschwert auch die Erstellung und Überprüfung von Datenverarbeitungskonzepten. Wir haben uns diesbezüglich bereits an den Senator für Inneres gewandt. Eine entsprechende Verordnung soll nunmehr in Arbeit sein. Das neue Löschkonzept wird sich an deren Vorgaben orientieren müssen.

In den beschriebenen Bereichen zeigt sich, dass die Anwendung und Umsetzung des seit 8. Dezember 2020 geltenden neuen Bremischen Polizeigesetzes geeignet ist, den Grundrechtsschutz betroffener Personen im Land Bremen zu stärken. Wir drängen daher in unserer Aufsichtspraxis darauf, dass die neuen Vorgaben schnell umgesetzt werden, und blicken zuversichtlich auf die zukünftige kooperative Zusammenarbeit mit der Polizei.

5.3 Umfang des Auskunftsanspruchs nach § 73 Bremisches Polizeigesetz gegenüber der Polizei

Anlässlich mehrerer Beschwerden prüften wir die Praxis der Auskunftserteilung bei der Polizei Bremen. Die betroffenen Personen hatten bei der Polizei Auskunft über die Verarbeitung personenbezogener Daten beantragt und beschwerten sich anschließend wegen unvollständig erteilter Auskunft.

Bei unseren Prüfungen stellten wir fest, dass die Polizei Bremen in allen Beschwerdefällen den betroffenen Personen keine den gesetzlichen Vorgaben des § 73 Bremisches Polizeigesetz (BremPolG) genügende Auskunft erteilt hatte. Die von der Polizei erteilte schriftliche Auskunft beschränkte sich jeweils auf ein oder zwei von ihr genutzten Vorgangsbearbeitungssysteme; dabei handelte es sich in der Regel um das Vorgangsbearbeitungssystem @rtus und die elektronische Kriminalakte. Personenbezogene Daten werden durch die Polizei indes auch in anderen (IT-)Systemen verarbeitet. Wir machten gegenüber der Polizei deutlich, dass die Auskunft nach § 73 BremPolG sich auf alle von der Polizei zur Datenverarbeitung genutzten Systeme beziehen müsse. Außerdem wiesen wir die

Polizei darauf hin, dass sich das Recht der betroffenen Personen auf Auskunft nach § 73 BremPolG auf alle in dieser Vorschrift genannten Informationen erstreckt. Betroffene haben auf Antrag das Recht, unter anderem zu erfahren, zu welchen Zwecken und wie lange ihre personenbezogenen Daten verarbeitet werden. Außerdem muss die Polizei betroffenen Personen im Rahmen einer Auskunft mitteilen, an welche Stellen sie ihre personenbezogenen Daten übermittelt hat.

In einem Beschwerdefall sprachen wir gegenüber der Polizei Bremen eine Beanstandung nach § 85 BremPolG wegen unvollständig erteilter Auskunft aus.

In beratender Funktion nahmen wir Ende 2021 an einem Austausch mit der Polizei Bremen zum Umfang der nach § 73 BremPolG zu erteilenden Auskünfte teil.

5.4 Polizeiliche Videoüberwachungen

5.4.1 Maritime Tage

Im August des Berichtsjahres nutzte die Ortspolizeibehörde Bremerhaven erstmalig die neue Rechtsgrundlage des § 32 Absatz 3 Satz 1 Nummer 2 Bremisches Polizeigesetz (BremPolG) für eine fünftägige Videoüberwachungsmaßnahme im Zusammenhang mit den Maritimen Tagen. Für die gesetzmäßige Videoüberwachung der in § 32 Absatz 3 Satz 1 Nummer 2 BremPolG genannten Orte ist keine konkrete Gefahrenlage erforderlich. Durch den Einsatz eines Videoüberwachungssystems, das über Kameras mit Zoomfunktion, Standbild und Einzelbildschaltungsfunktion sowie über Drehtechnik und Schwenktechnik verfügte, war eine gegenüber einer Überwachung durch das menschliche Auge wesentlich großflächigere und intensivere Beobachtung, etwa die Identifizierung über eine große Entfernung wie 300 Meter, möglich als durch den aufwändigeren Einsatz einer Vielzahl von Polizeibeamt:innen. Es fand damit eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche mittels Bildübertragung und Bildaufzeichnung statt.

Erst nachdem wir gegenüber der Ortspolizeibehörde Bremerhaven eine Warnung gemäß § 85 Absatz 1 Satz 4 BremPolG ausgesprochen hatten, hatte diese eine Datenschutz-Folgenabschätzung erstellt, obwohl eine solche aufgrund des erheblichen Umfangs der anfallenden Videodaten und der großen Anzahl der von der Videoüberwachung erfassten Personen gemäß § 82 BremPolG erforderlich war.

Unsere angekündigte Nachbesprechung im September 2021 ergab, dass keine Videoaufzeichnungen zur Ermittlung und Verfolgung von Straftaten angefertigt worden waren.

5.4.2 Weihnachtsmarkt

Mit einem sich nur im Detail von der Videoüberwachung der Maritimen Tage (siehe hierzu Ziffer 5.4.1 dieses Berichts) unterscheidenden Konzeptes überwachte die Ortspolizeibehörde Bremerhaven auch den dortigen Weihnachtsmarkt. Nach einem Vor-Ort-Termin bei der Ortspolizeibehörde Bremerhaven wurde uns umgehend eine Datenschutz-Folgenabschätzung übermittelt. Zu dieser nahmen wir Stellung. Ebenfalls wohnten wir einmal dem Betrieb der Kameras bei und kontrollierten die Beschilderung vor Ort.

Die Videoüberwachung des Weihnachtsmarktes ist nach der der Maritimen Tage die zweite polizeiliche Überwachungsmaßnahme innerhalb kurzer Zeit. Wir sehen daher Anlass, anhand der konkreten Überwachungen, aber auch auf einer generell-abstrakten Ebene, die Verhältnismäßigkeit von Videoüberwachungen zu hinterfragen und Untersuchungen zu beginnen, mittels derer überprüft werden kann, ob die Zwecke der Überwachung tatsächlich erreicht werden können und ob die Anforderung des Bundesverfassungsgerichts zur Aufstellung einer Überwachungsgesamtrechnung dabei ausreichend beachtet wird. Die Ausdehnung der Videoüberwachung auf weitere Veranstaltungen in Bremen und Bremerhaven darf nicht zur Routine werden. Polizeiliche Videoüberwachungen gehen mit schwerwiegenden Grundrechtseingriffen einher. Stattfindende Videoüberwachungen sind fortwährend zu evaluieren. Wir haben daher von der Ortspolizeibehörde Bremerhaven einen Controlling-Bericht angefordert, der Rückschlüsse auf den Nutzen der Überwachung ermöglichen soll, um ihre Verhältnismäßigkeit bewerten zu können.

5.5 Prüfung des Schengener Informationssystems

Gemäß europäischer Vorgaben wie Artikel 60 Absatz 1 des Beschlusses 2007/533/JI-Rat über die Nutzung des Schengener Informationssystems (im Folgenden SIS II-Ratsbeschluss) müssen die datenschutzrechtlichen Aufsichtsbehörden das System alle vier Jahre für ihren Zuständigkeitsbereich prüfen. Für das Bundesland Bremen waren im Juni 2021 insgesamt 356 SIS-Personenfahndungen gespeichert. Diese stellten wir in den Mittelpunkt unserer Prüfung. Den im SIS II enthaltenen Personenfahndungen liegen sehr unterschiedliche Sachverhalte wie etwa Festnahme, Ingewahrsamnahme vermisster minderjähriger Personen oder Ingewahrsamnahme von Zeug:innen zur Zeugenaussage zu Grunde. Bei den 21 der besonders tief in Grundrechte eingreifenden Systemeinträge zur Ermöglichung gezielter und verdeckter Personenfahndungen nach Artikel 36 SIS II-Ratsbeschluss ergab unsere stichprobenhafte Prüfung, dass die rechtlichen Anforderungen eingehalten worden waren.

5.6 Prüfung des europäischen Visa-Informationssystems

Gemäß europäischer Vorgaben wie Artikel 41 Verordnung (EG) 767/2008 vom 9. Juli 2008 über das Visa-Informationssystem und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (im Folgenden VIS-Verordnung) und Artikel 8 des Ratsbeschlusses 2008/633/JI über den Zugang von Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten ist die Landesbeauftragte für Datenschutz und Informationsfreiheit alle vier Jahre verpflichtet, in ihrem Zuständigkeitsbereich das Visa-Informationssystem zu prüfen. Unsere Prüfung im Juni 2021 ergab, dass das Visa-Informationssystem im Land Bremen wenig genutzt wird. Als Grund wurde uns die äußerst geringe Trefferquote genannt. In den vergangenen sieben Jahren gab es etwa 300 Anfragen an das Visa-Informationssystem. Mangels Dokumentation ergebnisloser Anfragen konnten wir keine weitergehende Prüfung des Akteninhaltes und damit der materiellen Voraussetzungen für die Anfragen durchführen. Wir forderten daher, dass künftig eine recherchierbare Dokumentation erstellt und vorgehalten wird, die uns die Prüfung der materiellen Voraussetzungen der Anfragen ermöglicht.

5.7 Prüfung des Informationssystems Eurodac

Gemäß europäischer Vorgaben wie der Verordnung (EU) 603/2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaates, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrages auf internationalen Schutz zuständig ist, und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts muss die Landesbeauftragte für Datenschutz und Informationsfreiheit jährlich die Abfragen in Eurodac prüfen. Unsere Anfrage bei der Polizei Bremen ergab, dass von dort seit 2016 keine Abfragen im Eurodac-System durchgeführt worden sind, was die Erforderlichkeit dieses Systems in Frage stellt.

5.8 Ausstellung von Kontrollbescheinigungen über durchgeführte Identitätsfeststellungen

Gemäß § 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

(sogenannte Kontrollbescheinigungen) ausstellen. Die Kontrollbescheinigungen müssen den datenschutzrechtlichen Informationspflichten gegenüber den kontrollierten betroffenen Personen genügen und die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten. Hierauf wiesen wir die Polizei Bremen in der Beratung hin.

Im Zusammenhang mit der Einführung der Kontrollbescheinigungen plante die Polizei Bremen den Einsatz von "Optical Character Recognition" (OCR). Mit Hilfe von OCR können Texte, die auf Ausweisen in Normschrift aufgedruckt sind, erkannt und direkt weiterverarbeitet werden. Für den Einsatz von OCR im Zusammenhang mit Kontrollbescheinigungen nach § 27 BremPolG ist keine Rechtsgrundlage ersichtlich. Das Personalausweisgesetz erlaubt in § 14 bestimmten öffentlichen Stellen wie zum Beispiel der Polizei, die dort abschließend aufgeführten technischen Verfahren zu nutzen. Das OCR-Verfahren gehört nicht hierzu. Die Nutzung von OCR zur Texterkennung ist daher wegen des abschließenden und speziellen Charakters der Regelung nicht möglich. Dasselbe gilt für Pässe deutscher Staatsangehöriger und Aufenthaltstitel von Ausländer:innen.

5.9 Anforderung von Unterlagen durch die Standesämter in Bremen

Uns erreichten mehrere Beschwerden und eine Anfrage betreffend die Datenverarbeitung in Verfahren zur Ausstellung von Geburtsurkunden bei den Standesämtern Bremen-Mitte und Bremen-Nord. Uns wurde berichtet, dass die Standesämter von Antragsteller:innen vor der Ausstellung von Geburtsurkunden eine Vielzahl an Unterlagen verlangten, die teilweise für die Ausstellung der begehrten Geburtsurkunden und die vorangestellte Prüfung durch die Standesbeamt:innen nicht erforderlich waren. In mindestens einem Fall wurde durch das Standesamt eine Geburtsurkunde ausgestellt, obwohl nicht alle zuvor von der betroffenen Person geforderten Unterlagen beigebracht worden waren.

5.10 Telekommunikationsüberwachung

Bereits in einigen vorherigen Jahresberichten berichtete die Landesbeauftragte für Datenschutz und Informationsfreiheit über die Probleme bei der Telekommunikationsüberwachung durch die Polizei (siehe hierzu 40. Jahresbericht, Ziffern 5.5 und 5.7; 37. Jahresbericht, Ziffer 5.2.; 36. Jahresbericht, Ziffer 5.1; 35. Jahresbericht, Ziffer 5.11). Die Probleme bestehen grundsätzlich fort. Das Nachfolgesystem zum Betreiben der Telekommunikationsüberwachung ist aktuell und entgegen des im 40. Jahresbericht dargelegten Zeitrahmens noch nicht in Betrieb. Wir beanstandeten die weitere Nutzung des aktuellen Systems entsprechend unserer Pflichten aus dem Bremischen Polizeigesetz.

5.11 Datenverarbeitung durch Sicherheitsfirma beim BürgerServiceCenter

Wir berichteten bereits im 3. Jahresbericht nach der Datenschutzgrundverordnung (DSGVO) unter Ziffer 5.8 über eine Beschwerde über die Datenverarbeitung durch Beschäftigte einer Sicherheitsfirma im Bremer BürgerServiceCenter (BSC). Die Aufgaben der Beschäftigten der Sicherheitsfirma liegen in der Gebäudesicherung und während der Corona-Pandemie vor allem darin, die nötigen Sicherheitsregelungen, insbesondere die Einhaltung von Abstandsregeln zu prüfen und entsprechend zu koordinieren. Hierfür kann es in Einzelfällen erforderlich und damit rechtmäßig sein, dass Besucher:innen des BSC allgemein nach ihren Anliegen befragt werden, um sie entsprechend zu lotsen. Zwischenzeitlich steht fest, dass es sich hierbei um ein Auftragsverarbeitungsverhältnis gemäß Artikel 28 DSGVO zwischen dem Bürgeramt und der Sicherheitsfirma handelt. Das Bürgeramt setzte den Vertrag über die Auftragsverarbeitung mit der Sicherheitsfirma im Berichtsjahr auf.

5.12 Datenschutz beim Schadensmelder der Stadt Bremerhaven

Uns erreichte eine Beschwerde, mit der datenschutzrechtliche Bedenken im Zusammenhang mit dem Onlineportal des sogenannten Schadensmelders der Stadt Bremerhaven geäußert wurden. Insbesondere wurde kritisiert, dass bei diesem Dienst, der es Bremerhavener:innen ermöglicht, Schäden zu melden, derer sie gewahr werden, und darüber informiert zu werden, wie die Verwaltung mit ihrer Meldung verfährt, personenbezogene Daten verarbeitet werden. Wir nahmen dies zum Anlass, den Dienst genauer zu prüfen. Nach einem Vor-Ort-Termin Ende 2020, bei dem wir festgestellt hatten, dass für die Verarbeitung personenbezogener Daten Einwilligungen der Betroffenen eingeholt wurden, obwohl dies nicht erforderlich war, setzte der Magistrat der Stadt Bremerhaven unsere datenschutzrechtlichen Anmerkungen für die Erhebungen und Speicherung personenbezogener Daten um.

5.13 Anfertigen von Ausweiskopien durch das Ordnungsamt

Uns erreichte eine Beschwerde darüber, dass Verkehrsüberwacher:innen des Ordnungsamtes Bremen Kopien von Personalausweisen angefertigt hatten. Im konkreten Fall ging es um die Herausgabe eines polizeirechtlich sichergestellten Fahrzeuges. Der Beschwerdeführer war persönlich anwesend und musste sich für die Herausgabe des Fahrzeuges zwecks Identitätsfeststellung ausweisen. Die Sachbearbeiterin fertigte sodann gegen seinen Willen eine Kopie seines Personalausweises an, nahm die Kopie zum Vorgang und archivierte diese. Diese Datenverarbeitung stützte die Behörde auf eine Vorschrift aus dem Bremischen Polizeigesetz mit der Begründung, nur so die Herausgabe des sichergestellten Fahrzeuges an einen Nichtberechtigten verhüten zu können.

Das Datenschutzrecht sieht demgegenüber den Grundsatz der Datenminimierung vor. Demnach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Deshalb reicht es grundsätzlich aus, sich bei persönlicher Anwesenheit der betroffenen Person den Personalausweis vorlegen zu lassen, die Identität zu prüfen und schließlich einen entsprechenden Vermerk in der Akte, etwa "Ausweis hat vorgelegen", vorzunehmen. Das Anfertigen einer Kopie des Personalausweises darf bei persönlicher Anwesenheit der betroffenen Person nur in Ausnahmefällen und mit einer eindeutigen Rechtsgrundlage erfolgen. Das Ordnungsamt sagte uns zu, dass dieses Verfahren im Sinne des Grundsatzes der Datenminimierung in sämtlichen Fachbereichen der Behörde umgesetzt werden soll und die Mitarbeitenden eine entsprechende Sensibilisierung erhalten sollen. Auch will das Ordnungsamt in Abstimmung mit den anderen bürgernahen Ämtern des Bremer Innenressorts ein einheitliches und standardisiertes Verfahren erarbeiten, um die sachgerechte Aufklärung von Bürger:innen bezüglich des Datenschutzes in geeigneter Weise sicherzustellen.

5.14 Unzulässige Kontaktdatenerhebung auf Anweisung des Ordnungsamtes?

Im Berichtsjahr erhielten wir eine Beschwerde wegen umfangreicher Kontaktdatenerhebung durch einen Friseurbetrieb, der Adressdaten erhoben und Corona-Schnelltests fotografisch dokumentiert hatte. In diesem Zusammenhang teilte uns der Beschwerdeführer mit, dass er auch von anderen Betrieben erfahren habe, die Kontaktdaten erhöben, die den zulässigen Rahmen der Kontaktdatenerhebung gemäß § 6 Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 (Corona-Verordnung) überschritten. Die Betriebe beriefen sich dabei häufig darauf, dass Mitarbeitende des Ordnungsamtes entsprechende Anweisungen machten und bei Nichteinhaltung mit Schließungen drohten. Wir baten daraufhin das Ordnungsamt um Stellungnahme. Dieses teilte uns mit, dass die Außendienstkräfte des Ordnungsamtes keine Maßnahmen anwiesen, die über die jeweils geltenden gesetzlichen Vorgaben der Corona-Verordnung hinausgingen. Bei Bedarf komme es vor, dass die Mitarbeitenden des Ordnungsdienstes hinsichtlich der praktischen Umsetzung geltender Regelungen verschiedene Betriebe berieten, dabei würden sie jedoch ausdrücklich auf den geltenden Rahmen hinweisen. Es habe sich herausgestellt, dass sich Betriebe bei den Maßnahmen gegenüber Kund:innen häufig auf "Anweisungen des Ordnungsamtes" beriefen, um bestimmte Verhaltensweisen zu erwirken. Demzufolge konnten wir keinen datenschutzrechtlichen Verstoß beim Ordnungsamt feststellen. Demgegenüber war die beschriebene Kontaktdatenerhebung durch den Friseurbetrieb rechtswidrig.

5.15 Veröffentlichungen von Mitschnitten aus Beiratssitzungen

Uns erreichten über den Berichtzeitraum zwölf Beschwerden über die Veröffentlichung von Mitschnitten aus Beiratssitzungen dreier unterschiedlicher Ortsämter. Personen, die an den öffentlich zugänglichen digitalen Beiratssitzungen als Zuschauer:innen teilgenommen hatten, hatten die Sitzungen mitgeschnitten und über Medienplattformen und soziale Netze einer Vielzahl anderer Nutzer:innen zugänglich gemacht. Beiratsmitglieder sind ehrenamtliche Kommunalpolitiker:innen und damit sowohl Personen des öffentlichen Lebens als auch Träger:innen des Grundrechts auf informationelle Selbstbestimmung, sodass auch sie dem Schutz der Datenschutzgrundverordnung unterliegen. Der Mitschnitt von Beiratssitzungen stellt daher eine Verarbeitung personenbezogener Daten dar und bedarf einer Rechtsgrundlage. Anlässlich der pandemischen Lage erließ der bremische Ortsgesetzgeber deshalb § 14 Absatz 2a Satz 2 des Ortsgesetzes über Beiräte und Ortsämter, wonach der Beirat unter bestimmten Umständen eine Beteiligung der Öffentlichkeit mittels Übertragung der öffentlichen Sitzung durch geeignete digitale Verfahren sicherstellen kann. Die Veröffentlichung der Mittschnitte stellt eine erneute Verarbeitung personenbezogener Daten dar und bedarf ebenfalls einer Rechtsgrundlage. In den Beschwerden zugrundeliegenden Fällen war eine solche nicht gegeben. Deshalb erließen wir Anordnungen mit dem Ziel der Löschung der betreffenden Beiträge. Die Beiträge wurden daraufhin ausnahmslos gelöscht. In einigen Fällen wurde die Anordnung gerichtlich angefochten.

5.16 Einführung eines VIS-Einheitsmandanten

Der Senator für Finanzen arbeitet unter Mitarbeit verschiedener Ressorts an der Umsetzung eines sogenannten Einheitsmandanten für das elektronische Dokumentenmanagementsystem (VISkompakt) 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 auf nur einem einzigen Mandanten gebündelt werden. Ein Mandant ist eine eigenständige und abgeschlossene digitale Instanz. Bislang galt der Grundsatz, dass für jede verantwortliche Stelle ein einzelner Mandant einzurichten ist. Damit sind die unterschiedlichen organisatorischen Bereiche der bremischen Verwaltung gegenwärtig in digitaler Hinsicht selbstständig.

Wir begleiten das Projekt, das trotz der von uns anfangs geäußerten prinzipiellen Bedenken grundsätzlich die Chance bietet, einen hohen Datenschutzstandard zu erreichen, und warfen einige rechtliche und technische Fragestellungen auf, die geprüft und umgesetzt werden müssen, damit die Datenschutzkonformität sichergestellt ist. Die von uns geforderten Maßnahmen betreffen vor allem die Zugriffsrechte auf Dokumente und Vorgänge/Akten sowie die Protokollierung von erfolgten Zugriffen. Außerdem forderten wir notwendige Maßnahmen

zum Schutz von besonders schutzbedürftigen Daten. Je höher der Schutzbedarf und je gravierender die Risiken für die Rechte und Freiheiten natürlicher Personen (zum Beispiel bei Steuer- oder Gesundheitsdaten) sind, desto strengere Anforderungen sind an die Berechtigungsvergabe zu stellen.

5.17 Datenschutzcockpit

Durch das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz, OZG) sind Bund und Länder verpflichtet, bis spätestens Ende 2022 ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten. Damit Bürger:innen nachvollziehen können, welche Stellen Daten über sie gespeichert haben, um welche Daten es sich im Einzelfall handelt und wann, von wem und zu welchem Zweck auf die personenbezogenen Daten zugegriffen worden ist, wurde im Registermodernisierungsgesetz vom 28. März 2021 die Notwendigkeit eines "Datenschutzcockpits" gesetzlich verankert. Pilotiert wird dieses Projekt durch die Freie Hansestadt Bremen und das Bundesministerium des Innern und für Heimat. Die Landesbeauftragte für Datenschutz und Informationsfreiheit begleitet dieses Projekt gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

6. Justiz

6.1 Gemeldete Datenschutzverletzungen

Im Jahr 2021 wurden von Rechtsanwält:innen und Notar:innen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit zehn 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 2021 keine Verletzungen des Schutzes personenbezogener Daten.

6.2 Übersendung von Datenkopien durch Rechtsanwaltskanzlei

Wir erhielten eine Beschwerde über eine Rechtsanwaltskanzlei, die anlässlich eines Auskunftsersuchens eines ehemaligen Mandanten die Übersendung von Datenkopien verweigert hatte. Dies hatte sie mit ihrem aus der Bundesrechtsanwaltsordnung resultierenden Recht begründet, Dokumente, die Rechtsanwält:innen aus Anlass ihrer beruflichen Tätigkeit von ihren Mandant:innen oder für sie erhalten haben, bis zur Begleichung der geschuldeten Gebühren und Auslagen zurückbehalten zu dürfen. Dieses Zurückbehaltungsrecht stehe dem Recht auf Erhalt von Kopien als entgegenstehendes Recht im Sinne des Artikel 15 Absatz 4 Datenschutzgrundverordnung (DSGVO) entgegen.

Wir konnten die Rechtsanwaltskanzlei, die die begehrten Datenkopien schließlich übermittelte, davon überzeugen, dass das anwaltlich Zurückbehaltungsrecht hier nicht beeinträchtigt war, da nicht die Herausgabe der Originalakte, sondern lediglich die Übersendung von Kopien der personenbezogenen Daten beantragt war. Erwägungsgrund 63 Satz 6 der DSGVO weist im Übrigen ausdrücklich darauf hin, dass die Berücksichtigung der der Übersendung von Kopien entgegenstehenden Rechte und Freiheiten Dritter, nicht dazu führen darf, dass der betroffenen Person jegliche Auskunft verweigert wird.

6.3 Fehlversand anwaltlicher Schreiben

Wir erhielten mehrere Beschwerden über Rechtsanwaltskanzleien, die anwaltliche Schreiben an falsche Empfänger:innen versendet hatten. Rechtsanwaltskanzleien unterliegen aufgrund ihrer berufsrechtlichen Verpflichtungen beim Versand von Schreiben besonderen Sorgfaltspflichten. Daher sind weitreichende technische und organisatorische Maßnahmen notwendig, um die Versendung von anwaltlichen Schreiben datenschutzkonform zu gestalten. Es empfiehlt sich beispielsweise die Einführung des Vieraugenprinzips bei der Freigabe von Schreiben sowie die Etablierung eines ausführlichen, verbindlichen und dokumentierten Verfahrens zur datenschutzkonformen Versendung von Schreiben.

6.4 Weitergabe der Daten gegnerischer Mandant:innen

Zunehmend erreichen uns Beschwerden über Rechtsanwaltskanzleien im Zusammenhang mit der Verarbeitung personenbezogener Daten bei der Geltendmachung zivilrechtlicher Ansprüche. Die Beschwerdeführenden sind Anspruchsgegner:innen der jeweiligen Mandant:innen und haben den Eindruck, dass ihre personenbezogenen Daten ohne Rechtsgrund an die Kanzleien weitergegeben wurden und dort nicht verarbeitet werden dürfen.

Diese Beschwerdeführenden weisen wir darauf hin, dass es allen Menschen freisteht, Rechtsanwaltskanzleien oder Inkassounternehmen zur Geltendmachung zivilrechtlicher Ansprüche einzuschalten. Die für die Durchführung des betreffenden Mandats erforderlichen personenbezogenen Daten der Anspruchsgegner:innen dürfen an Rechtsanwaltskanzleien und Inkassounternehmen übermittelt und dort verarbeitet werden, da sonst die Geltendmachung von Ansprüchen nicht möglich wäre. Solange über das Bestehen eines solchen Anspruchs gestritten wird, ist es rechtmäßig, dass die betreffenden Daten bei der Kanzlei oder dem Inkassounternehmen verarbeitet werden. Die Daten sind erst zu löschen, wenn ihre Verarbeitung für die Durchführung des konkreten Mandats nicht mehr erforderlich ist.

6.5 Fehlende Protokollierung lesender Zugriffe in der Anwendung web.sta bei der Staatsanwaltschaft Bremen

Das Fachverfahren web.sta wird von der Bremer Staatsanwaltschaft für alle Geschäftsabläufe genutzt. Es wird unter anderem zur Registrierung, Anlage und Verwaltung der Akten verwendet. Darüber hinaus bietet web.sta die Möglichkeit, Auskünfte aus dem Bundeszentralregister (BZR), dem Fahreignungsregister (FAER) und dem Europäischen Strafregisterinformationssystem (ECRIS) elektronisch anzufordern. Insgesamt haben bei der Staatsanwaltschaft und bei der Generalstaatsanwaltschaft Bremen etwa 200 Beschäftigte eine Zugriffsberechtigung auf web.sta. Schreibende Zugriffe wie das Erfassen, Ändern oder Löschen von Daten werden vom System protokolliert.

Auf Nachfrage bei der Staatsanwaltschaft Bremen im September 2021 erfuhr die Landesbeauftragte für Datenschutz und Informationsfreiheit, dass die von uns bereits im 40. Jahresbericht unter Ziffer 6.3 sowie im 38. Jahresbericht unter Ziffer 6.2 geforderte Protokollierung lesender Zugriffe (Abfragen) in web.sta immer noch nicht eingeführt worden ist.

Protokolldaten geben darüber Auskunft, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Der Zweck der Protokollierung ist, die Verarbeitung personenbezogener Daten insoweit transparent zu machen als die Ordnungsmäßigkeit beziehungsweise ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar werden. Um missbräuchliche Abrufe und somit die Kenntnisnahme personenbezogener Daten zu verhindern und zu erkennen, ist eine Protokollierung lesender Zugriffe zwingend erforderlich. So kann verhindert werden, dass Recherche- und Auswertungsmöglichkeiten in web.sta für Abfragen genutzt werden, bei denen das Vorliegen eines sachlichen Grundes fehlt.

Ende 2021 teilte uns die Staatsanwaltschaft mit, dass sie die Einführung der Protokollierung lesender Zugriffe in web.sta plane. Ein genauer Zeitplan für die Umsetzung wurde uns nicht genannt. Wir erwarten, dass die Staatsanwaltschaft Bremen unverzüglich die Protokollierung lesender Zugriffe in web.sta einführt.

6.6 Personenverwechslung bei der Staatsanwaltschaft Bremen

Uns erreichte eine Beschwerde im Zusammenhang mit einer Personenverwechslung bei der Staatsanwaltschaft Bremen. Die Staatsanwaltschaft hatte per Post zwei Schreiben, die sich auf zwei verschiedene von ihr geführte Ermittlungsverfahren bezogen, an die Beschwerdeführerin versendet. Die Beschwerdeführerin stand in keinerlei Verbindung zu diesen Ermittlungsverfahren, die eigentlich eine andere Person betrafen. Die miteinander

verwechselten Personen wohnen an unterschiedlichen Adressen, haben jedoch den selben Nachnamen und nahezu identische Vornamen. Die Staatsanwaltschaft Bremen bestritt zunächst das Vorliegen einer Personenverwechslung. Uns liegen die Schreiben an die Beschwerdeführerin vor und wir sind zusammen mit der Staatsanwaltschaft noch in Klärung, wie es zu einer solchen Fehlsendungen kommen konnte.

7. Gesundheit

7.1 Gemeldete Datenschutzverletzungen

Im Bereich Gesundheit wurden uns im Berichtsjahr insgesamt 39 Datenschutzverletzungen gemeldet. Neben zahlreichen Fehlversendungen und Fällen, in denen personenbezogene Daten bei einem Diebstahl entwendet worden waren, wurden wir auch über einige Vorfälle informiert, bei denen Beschäftigte Patientendaten ohne dienstlichen Anlass zu eigenen Zwecken verwendet hatten. In einem Fall hatte ein Beschäftigter eines Krankenhauses eine Patientin sechs Monate nach ihrem Krankenhausaufenthalt zu privaten Zwecken über einen Messengerdienst kontaktiert. Ein anderer Fall betraf die Notaufnahme eines Krankenhauses. Dort hatte mutmaßlich ein Mitarbeiter eines Sanitätsdienstes Fotos von Computerbildschirmen angefertigt und zu privaten Zwecken an eine andere Person weitergeleitet.

Sofern seitens des Verantwortlichen im Vorfeld geeignete Maßnahmen getroffen wurden, um solchen Vorfällen vorzubeugen, sind die Beschäftigten für die Rechtsverletzungen datenschutzrechtlich selbst verantwortlich und müssen die Konsequenzen für ihre Handlungen tragen (sogenannter Beschäftigtenexzess).

7.2 Datenschutz im Impfzentrum

Im zweiten Jahr der Corona-Pandemie stand vor allem das Impfen im Fokus der Öffentlichkeit. Die Stadt Bremen baute in den Messehallen auf der Bürgerweide eines der größten Impfzentren Deutschlands auf, in dem der Großteil der über 500.000 in der Stadt Bremen geimpften Bremer:innen die Schutzimpfung erhielt. Schon früh lag das Land Bremen bundesweit mit der Anzahl verabreichter Impfdosen auf dem Spitzenplatz. Ein solch groß angelegtes Impfprojekt führt auch zu einer umfangreichen Verarbeitung höchst sensibler Daten. Neben der Impfdokumentation werden im Rahmen der vorherigen Anamnese unter anderem Allergien, Vorerkrankungen und Risikofaktoren erhoben und gespeichert. Umso wichtiger ist es, die datenschutzrechtlichen Rahmenbedingungen und Prozesse sicher zu gestalten, auch um das Vertrauen in die staatlichen Institutionen nicht zu erschüttern.

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz legte uns für die Impfzentren Bremen und Bremerhaven im März ein Datenschutzkonzept und eine Datenschutz-Folgenabschätzung vor. Darin fehlten noch wesentliche Informationen. Zum einen bezogen

sich die Abläufe lediglich auf die Personen der Priorisierungsstufe I. Da bereits im Frühjahr auch den Personen der anderen Priorisierungsstufen ein Impfangebot gemacht werden konnte, war es für eine Prüfung der Unterlagen genauso entscheidend, wie die Prozesse in dieser Hinsicht ausgestaltet waren. Zum anderen war das Konzept hinsichtlich der Risikobewertung sowie der beschriebenen technischen und organisatorischen Maßnahmen der Datensicherheit nicht detailliert genug, was uns letztendlich eine Prüfung unmöglich machte. Daher baten wir um Überarbeitung der Datenschutz-Dokumentation. Bis zur Schließung des zentralen Impfzentrums Bremen Ende Oktober wurde uns jedoch trotz mehrfacher Aufforderung keine neue, prüffähige Version vorgelegt. Auch zum Redaktionsschluss lag uns diese noch nicht vor.

Ähnlich schwierig gestaltete sich die Zusammenarbeit mit der Senatorin für Gesundheit, Frauen und Verbraucherschutz bei der Bearbeitung von Beschwerden und Hinweisen, welche die Datenverarbeitung im Impfzentrum Bremen betrafen. Auskünfte, die wir zur Sachverhaltsermittlung zwingend benötigen, wurden monatelang nicht erteilt. Bis auf einige wenige Ausnahmen konnten wir aufgrund dessen bis zum Redaktionsschluss keine der eingegangen Beschwerden oder Hinweise abschließend prüfen. Dieser Missstand spiegelte sich auch in der Kommunikation der senatorischen Dienststelle mit den betroffenen Personen wider. So wurden Auskunftsersuchen nicht zuverlässig bearbeitet und Hinweise zu möglichen Datenschutzmängeln nicht weitergeleitet. Für die betroffenen Personen bedeutet dies eine erhebliche Verzögerung der Verfahren, während derer sie sich bezüglich des Umgangs mit ihren Daten im Dunkeln gelassen fühlen.

Die Bereitstellung der angeforderten Informationen wurde uns bis Ende Januar 2022 zugesagt.

7.3 Kontaktnachverfolgung im Krankenhaus

Um eine Ausbreitung des Coronavirus zu verhindern, setzte der öffentliche Gesundheitsdienst auch im Berichtsjahr auf die Nachverfolgung von Kontakten infizierter Personen (siehe hierzu 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffern 1.3 und 12.4). Viele Einrichtungen des öffentlichen Lebens wurden daher durch die jeweiligen Corona-Verordnungen verpflichtet, Kontaktdaten von Kund:innen und Besucher:innen zu erheben.

In einem uns bekannt gewordenen Fall führte eine Auseinandersetzung über den zulässigen Umfang der Kontakterhebung dazu, dass ein Bremer Krankenhaus einem Patienten den Zutritt zu einer Einrichtung innerhalb des Krankenhauses verweigerte. Der Patient war bereit, seinen Namen und seine Telefonnummer zu Zwecken der Kontaktnachverfolgung zu hinterlassen. Für die Angabe seines Geburtsdatums und seiner Wohnadresse sah er jedoch keine rechtliche Grundlage. In der Folge durfte er den vereinbarten Untersuchungstermin nicht wahrnehmen.

Nach Prüfung der bei uns eingereichten Beschwerde kamen wir ebenfalls zu dem Ergebnis, dass die Angabe weiterer Kontaktdaten für die Nachverfolgung möglicher Kontaktpersonen nicht erforderlich und somit unzulässig war. Der Landesverordnungsgeber verpflichtet die jeweiligen für Einrichtungen, Betriebe oder Veranstaltungen verantwortlichen Personen in § 6 Absatz 1 Satz 1 der zum Beispiel 29. Corona-Verordnung, "zumindest den Namen und die zugehörige Telefonnummer oder E-Mail-Adresse sowie den Zeitpunkt des Betretens und Verlassens je einer Vertreterin oder eines Vertreters der anwesenden Personen aus einem Haushalt zu erheben". Im vorliegenden Fall war eine über die Basisdaten Name und Telefonnummer oder E-Mail-Adresse sowie Zeitpunkt des Betretens und Verlassens der Einrichtung hinausgehende Datenerhebung nicht erforderlich und durfte daher von den betroffenen Personen nicht erzwungen werden. Hier war zusätzlich zu beachten, dass es in keinem angemessenen Verhältnis zu dem verfolgten Zweck der Kontaktnachverfolgung stand, eine medizinische Behandlung von der Angabe solcher zusätzlichen Daten abhängig zu machen. Das Krankenhaus verzichtet zukünftig darauf, die Datenerhebung zur Kontaktnachverfolgung zentral für alle auf dem Krankenhausgelände ansässigen Institutionen vorzunehmen und überlässt diese Aufgabe den Einrichtungen selbst.

7.4 Verlust von Untersuchungsdaten durch Einbruchdiebstahl

Über die Meldung einer Datenschutzverletzung erhielten wir bereits im Berichtsjahr 2020 Kenntnis über einen Einbruchdiebstahl, bei welchem aus einem Bremer Klinikum ein Laptop mit Patient:innendaten entwendet worden war. Auf dem Gerät waren Ergebnisse von psychiatrisch-psychologischen Tests gespeichert. Zwar war das Laptop zumindest passwortgeschützt, diese Maßnahme stellte sich jedoch als ineffektiv heraus, da sich ein Zettel mit dem Passwort auf dem Gerät befand. Seitens des Krankenhauses konnte nicht ausgeschlossen werden, dass Klarnamen von Patient:innen auf dem Gerät gespeichert worden waren, zumindest wurden dort aber Namenskürzel und somit Pseudonyme verwendet, die als personenbeziehbare Daten dem Datenschutzrecht unterliegen. Das Krankenhaus vertrat die Auffassung, es bestünde kein hohes Risiko für die betroffenen Personen und benachrichtigte die betroffenen Personen trotz unserer mitgeteilten gegenteiligen Auffassung nicht. Von einer förmlichen Anweisung der Benachrichtigung sahen wir vor dem Hintergrund ab, dass nach Auskunft des Krankenhauses eine Identifizierung der betroffenen Personen mithilfe der entwendeten Daten für Dritte so gut wie unmöglich sei.

7.5 Unsichere Datenerhebung in Bremer Kliniken zu Infektionsschutzzwecken

Im Rahmen eines aufsichtsbehördlichen Verfahrens erfuhren wir von einem bremischen Krankenhaus, dass das Gesundheitsamt Bremen von den Krankenhäusern im Land Bremen

seit Beginn der Pandemie täglich Daten zu Coronafällen bei Patient:innen und Mitarbeiter:innen anfordert. Für die Übermittlung der Daten stellte das Gesundheitsamt Bremen lediglich eine E-Mail-Adresse zur Verfügung; andere Übermittlungswege standen nicht bereit. Auf Nachfrage teilte uns das Gesundheitsamt Bremen mit, dass die Listen erforderlich seien, um Ausbruchsgeschehen im stationären Bereich nachvollziehen und eingrenzen zu können. Bei diesen durchaus nachvollziehbaren Zielen geriet die Datensicherheit offenbar aus dem Blick. Es ist nicht nur diejenige Person, die personenbezogene Daten übermittelt, sondern auch diejenige, die personenbezogene Daten gezielt erhebt, für die Sicherheit dieser Daten verantwortlich. Bei der Datenerhebung muss zumindest ein sicherer Übertragungsweg bereitgestellt werden. Die Übermittlung von Gesundheitsdaten darf nur dann per E-Mail erfolgen, wenn die Daten durch geeignete Maßnahmen, etwa eine ausreichende Verschlüsselung, vor unbefugten Zugriffen durch Dritte geschützt werden. Wir forderten das Gesundheitsamt Bremen daher auf, den Krankenhäusern einen sicheren Übertragungsweg zur Verfügung zu stellen. Seit Juli des aktuellen Berichtsjahres steht den Krankenhäusern nun eine vom Gesundheitsamt Bremen bereitgestellte verschlüsselte Tabelle für die Datenübermittlung zur Verfügung.

7.6 Einsatz eines externen Call-Centers für die Kontaktnachverfolgung

Insbesondere die Nachverfolgung von Kontaktpersonen brachte die Gesundheitsämter im Laufe der Corona-Pandemie immer wieder an ihre personellen Grenzen. Abhilfe konnten in Bremen und Bremerhaven vor allem die sogenannten Containment Scouts schaffen, die zu diesem Zweck kurzfristig eingestellt wurden. Um noch flexibler auf den Anstieg von Infektionszahlen reagieren zu können, traf Bremen die Entscheidung, ein externes Call-Center als Auftragsverarbeiter in die Kontaktverfolgung einzubeziehen. Nach Prüfung der uns dazu vorgelegten Dokumente wiesen wir das Gesundheitsamt darauf hin, dass die Einbeziehung Externer zwar grundsätzlich möglich ist, aber zusätzliche Risiken für die Sicherheit der verarbeiteten personenbezogenen Daten birgt. Der Mehrzahl dieser Risiken konnte das Gesundheitsamt durch entsprechende technische und organisatorische Maßnahmen entgegenwirken. Einige der von uns vorgeschlagenen Maßnahmen ließen sich jedoch nicht in der verwendeten Software umsetzen, da diese bundesweit für die Kontaktnachverfolgung eingesetzt wird und nur eingeschränkte Möglichkeiten für individuelle Anpassungen vorsieht. Damit diese und weitere datenschutzrechtliche Themen aufgegriffen und möglichst zeitnah in der Software umgesetzt werden, hat sich eine Arbeitsgruppe aus einigen Datenschutzaufsichtsbehörden der Länder und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gebildet, die den Prozess begleitet und im regelmäßigen Austausch mit dem Hersteller der Software steht.

7.7 Rezept einer Bremer Arztpraxis bei niederländischer Versandapotheke ohne Kenntnis der Patientin

Wir erhielten die Beschwerde einer Patientin, die uns mitteilte, ihr sei von einer niederländischen Versandapotheke ein Paket mit einem Medikament zugesandt worden. Auf Nachfrage habe die von ihr kontaktierte niederländische Apotheke mitgeteilt, dass dort ein entsprechendes Rezept vorliege. Die Beschwerdeführerin gab an, sie könne sich diesen Umstand nicht erklären, da sie das Rezept selbst in einer Bremer Apotheke eingelöst und das Medikament somit bereits erhalten habe. Bei unseren Ermittlungen stellte sich heraus, dass das Rezept offenbar zweimal von der Arztpraxis ausgestellt worden war. Eines der Rezepte war an die Patientin ausgehändigt worden, die dieses sodann in einer Bremer Apotheke einlöste. Wie das andere Rezept an die niederländische Versandapotheke gelangte, konnte von der Praxis nicht mehr nachvollzogen werden. Unabhängig von dem konkreten Geschehenshergang handelt es sich bei diesem Fall um eine Datenübermittlung innerhalb der Europäischen Union (EU) und somit innerhalb des Geltungsbereichs der Datenschutzgrundverordnung (DSGVO). Wir kontaktierten daher auch die niederländische Datenschutzaufsichtsbehörde und informierten sie über den Vorfall. Vielleicht kann mit ihrer Unterstützung der Sachverhalt noch aufgeklärt werden.

Die Beschwerde führt einmal mehr vor Augen, wie schnell betroffene Personen die Kontrolle über sie betreffende Daten verlieren können und wie wichtig es aus diesem Grund für die Verantwortlichen ist, die Verarbeitung personenbezogener Daten sicher und nachvollziehbar zu gestalten.

7.8 Beschwerden über Corona-Testzentren

Im Berichtsjahr erreichten uns zahlreiche Beschwerden und Hinweise über die Datenverarbeitung in privat betriebenen Corona-Testzentren, insbesondere im Zusammenhang mit der Durchführung der kostenlosen Testungen. Sowohl bei den Testpersonen als auch bei den Testzentren herrschte zu Beginn Unsicherheit darüber, welche personenbezogenen Daten in diesem Zusammenhang erhoben werden dürfen und wie lange diese aufzubewahren sind. Im Sommer des Berichtsjahres schaffte der Bundesgesetzgeber mit der Änderung der Corona-Testverordnung Klarheit. Danach sind zu Zwecken der Auftrags- und Leistungsdokumentation insbesondere der Name, das Geburtsdatum, die Anschrift, die Art der Leistung, Datum und Uhrzeit der Testung sowie das Testergebnis zu erheben und zu speichern (§ 7 Absatz 5 Coronavirus-Testverordnung). Hinsichtlich der Aufbewahrung ist zu beachten, dass die Betreiber privater Testzentren auch nach Schließung der Zentren verpflichtet sind, die Daten sicher zu speichern und die Testergebnisse fristgerecht zum 1. Januar 2023 und die übrigen Daten zum 1. Januar 2025 zu löschen.

8. Soziales

8.1 Gemeldete Datenschutzverletzungen

Im Bereich Soziales wurden uns im Berichtsjahr insgesamt acht Datenschutzverletzungen gemeldet. Die Mehrheit der Meldungen betraf Fälle, in denen personenbezogene Daten bei einem Einbruch entwendet worden oder aufgrund unzureichender Vorsichtsmaßnahmen auf dem Transportweg verloren gegangen waren. Bei der Verwendung elektronischer Geräte wie Laptops oder Digitalkameras ist noch immer festzustellen, dass diese oftmals unzureichend vor einem Zugriff durch Unbefugte gesichert sind.

8.2 Offenlegung von personenbezogenen Daten durch Integrationsamt

Durch die Meldung einer Datenschutzverletzung erfuhren wir vom Amt für Menschen mit Behinderung Bremerhaven, dass es im Rahmen der Beteiligung bei einem Kündigungsverfahren zu einer unbefugten Offenlegung von personenbezogenen Daten der zu kündigenden Beschäftigten gekommen war.

Für eine Kündigung des Arbeitsverhältnisses mit einem schwerbehinderten Menschen sieht das Sozialgesetzbuch vor, dass das zuständige Integrationsamt der Kündigung zustimmen muss. In diesem Zusammenhang hört das Integrationsamt unter anderem die von der Kündigung betroffene schwerbehinderte Person an. In dem uns gemeldeten Fall hatte das Amt den schwerbehinderten Personen aus Unachtsamkeit zusammen mit den erforderlichen Unterlagen auch eine namentliche Liste aller Beschäftigten des Unternehmens, denen gekündigt werden sollte, geschickt. Auf diese Weise gab das Amt den Empfänger:innen ohne gesetzliche Befugnis neben anderen sensiblen Daten aus dem Arbeitsverhältnis auch Informationen über Schwerbehinderungen sowie über die familiären Verhältnisse anderer Beschäftigter preis. Aufgrund der hohen Risiken persönlicher oder finanzieller Art, die dieser Vorfall birgt, war das Amt für Menschen mit Behinderung verpflichtet, die betroffenen Personen über den Vorfall zu informieren. Darüber hinaus wurden die unberechtigten Empfänger:innen aufgefordert, die Daten zu vernichten. Da wir durch die Meldung Kenntnis von dem Vorfall hatten, konnten wir die betroffenen Personen, die sich zwecks Aufklärung an uns wandten, zeitnah über die getroffenen Maßnahmen informieren und sie hinsichtlich ihrer rechtlichen Möglichkeiten zur Durchsetzung ihrer Persönlichkeitsrechte beraten.

8.3 Unzureichende Datenschutzinformation beim Amt für Soziale Dienste

Uns erreichte eine Beschwerde, die eine Datenerhebung durch das Amt für Soziale Dienste (AfSD) betraf. Im Rahmen der Unterstützung einer unterhaltsberechtigten Person bei der Geltendmachung ihrer Unterhaltsansprüche hatte das AfSD die Einkommensverhältnisse

einer unterhaltspflichtigen Person abgefragt. Das von der betroffenen Person dazu auszufüllende Formular enthielt keine Informationen zur Rechtsgrundlage und zum Zweck der Datenerhebung. Eine allgemeine Datenschutzinformation nach Artikel 13 Datenschutzgrundverordnung (DSGVO) lag dem Formular nicht bei und wurde der betroffenen Person erst auf ihren Hinweis hin nachträglich zur Verfügung gestellt. Auch darin wurden weder die konkreten Verarbeitungszwecke noch die Rechtsgrundlagen benannt. Eine differenzierte Darstellung dieser Angaben muss auch dann erfolgen, wenn die oder der Verantwortliche eine Datenschutzinformation wie in diesem Fall für verschiedene Zwecke einsetzt. Das AfSD war insofern seiner Informationspflicht nach Artikel 13 DSGVO gegenüber der betroffenen Person nicht vollumfänglich nachgekommen.

Wir wiesen das AfSD darauf hin, dass es die betroffene Person zum Zeitpunkt der Erhebung der Daten in präziser und verständlicher Weise über den Zweck und die Rechtsgrundlage dieser Datenverarbeitung hätte informieren müssen und forderten das Amt auf, dies nachzuholen.

Trotz mehrmaliger Aufforderung kam das AfSD bis zum Redaktionsschluss seiner Informationsverpflichtung gegenüber der unterhaltsverpflichteten Person nicht nach. Auch die Überarbeitung der allgemeinen, vom AfSD für verschiedene Datenerhebungen genutzten Datenschutzinformation steht noch aus.

8.4 Datenschutz bei Vermittlung von Nachbarschaftshilfe

Uns erreichte die Beratungsanfrage einer Bürgerin, deren Mutter in einer Unterkunft im Rahmen des betreuten Wohnens lebt. Ihrer Mutter war dort ein Einwilligungsformular für die Verarbeitung personenbezogener Daten zu Zwecken der Vermittlung von Nachbarschaftshilfe vorgelegt worden. Die Tochter wunderte sich hierüber, weil ihre Mutter keine Vereinbarung über Nachbarschaftshilfe abgeschlossen hatte und dies auch nicht beabsichtigte.

Bei unserer Prüfung stellten wir zudem fest, dass das Einwilligungsformular einige Mängel aufwies.

Wir wandten uns an den Dienstleister des betreuten Wohnens, um den Sachverhalt aufzuklären und die Überarbeitung des Formulars zu fordern. Im Zuge dessen wurde uns erklärt, dass in dem Ausgangsfall versehentlich zu einem falschen Formular gegriffen worden sei. Außerdem sei festgestellt worden, dass die abgefragten vermeintlichen Einwilligungen lediglich die Datenverarbeitungen abdeckten, die zur Erfüllung der Dienstleistung erforderlich seien. Da in diesem Umfang personenbezogene Daten bereits auf gesetzlicher Grundlage verarbeitet werden dürften und eine Einwilligung daher ohne Wirkung sei, verzichte der Dienstleister künftig hierauf. Er nahm den Vorfall zudem zum Anlass, sämtliche Einwilligungsformulare unter Berücksichtigung unserer Anmerkungen zu überarbeiten. Die

Zwecke der Verarbeitung werden nun wesentlich differenzierter dargestellt. Dies gilt auch für die Datenarten, die nicht mehr mit pauschalen Begriffen wie "Bankdaten" und "Gesundheitsdaten" bezeichnet werden.

8.5 Bewohner- und Quartiersmanagementsoftware

Zuerst berichteten wir im 40. Jahresbericht unter Ziffer 8.9 über die Software zum Management der Flüchtlingsunterkünfte. In den folgenden Jahresberichten (1. Jahresbericht nach der Datenschutzgrundverordnung (DSGVO), Ziffer 8.1; 2. Jahresbericht nach der DSGVO, Ziffer 9.5; 3. Jahresbericht nach der DSGVO, Ziffer 8.4) erläuterten wir jeweils die noch offenen Punkte. Dabei handelte es sich um datenschutzrechtliche Fragestellungen im Zusammenhang mit der Speicherung von Essensausgabedaten für jede einzelne Person, mit Freitexteingaben und mit der Löschung nicht mehr erforderlicher Daten.

Hinsichtlich der Nutzung der Software als Fachverfahren für die Zentrale Aufnahmestelle für Asylbewerber und Flüchtlinge im Lande Bremen wurde uns inzwischen ein überarbeitetes Datenschutzkonzept vorgelegt. Bezüglich der Klärung einzelner Unklarheiten befinden wir uns aktuell noch im Gespräch mit der Senatorin für Soziales, Jugend, Integration und Sport. Datenschutzrechtliche Verbesserungen konnten vor allem in Bezug auf die Speicherung der Daten über die Essensausgabe erzielt werden. Die Speicherdauer wurde von 14 Tagen auf vier Tage reduziert. Zudem ist das Freitextfeld für die Angabe von gesundheitlichen Einschränkungen inzwischen durch weitere Ankreuzfelder ersetzt worden, sodass dort keine für die Unterbringungen irrelevanten Gesundheitsdaten mehr hinterlegt werden können.

Im Berichtsjahr erhielten wir außerdem den Hinweis, die Gemeinschaftsunterkünfte seien aus Gründen des Infektionsschutzes durch die Senatorin für Soziales, Jugend, Integration und Sport aufgefordert worden, die Anwesenheit und Abwesenheit der Bewohner:innen täglich zu kontrollieren und das Ergebnis der Kontrolle in der Bewohner- und Quartiersmanagementsoftware einzutragen. Die Senatorin für Soziales, Jugend, Integration und Sport teilte uns mit, diese Anweisung an die Gemeinschaftsunterkünfte sei zwar ergangen, in der Praxis aber nicht umgesetzt worden. Dies sei seitens der Senatorischen Behörde sichergestellt worden, sodass unsere datenschutzrechtlichen Bedenken insoweit gegenstandslos geworden waren.

9. Bildung

9.1 Gemeldete Datenschutzverletzungen

Im Bereich Schulen und schulische Bildung gab es im Berichtsjahr keine Meldungen von Verantwortlichen nach Artikel 33 der Datenschutzgrundverordnung. Es erreichten uns jedoch erneut, insbesondere in der ersten Jahreshälfte, diverse Anfragen von Betroffenen und von

Lehrkräften. Der weit überwiegende Anteil der Anfragen bezog sich wie im Vorjahr auf Datenschutzthemen im Zusammenhang mit der fortbestehenden pandemischen Lage, hier kam der Umgang mit Impfdaten als neues Thema hinzu.

9.2 Videokonferenzsysteme im Schulkontext

Die Verwendung von Videokonferenzsystemen zu Unterrichts- oder ähnlichen Zwecken im häuslichen Kontext stellt sich datenschutzrechtlich weiterhin als hoch problematisch dar. Die bereits im letzten Jahresbericht unter Ziffer 9.6 aufgeworfenen Fragen wurden bislang nicht oder nur unzureichend gelöst, insbesondere im Hinblick auf die erforderliche Aufklärung und Einwilligung. Für die bremischen Schulen fehlt es trotz diverser Nachfragen bei der zuständigen Behörde zudem an der erforderlichen Datenschutz-Folgenabschätzung im Hinblick auf das nach unseren Informationen aktuell für den schulischen Einsatz vorgesehene Videokonferenzsystem Webex von Cisco. Diesbezüglich wird auf die von uns gemäß Artikel 35 Absatz 4 der Datenschutzgrundverordnung (DSGVO) erstellte und an den Europäischen Datenschutzausschuss übermittelte Liste von Verarbeitungsvorgängen[2], für die von Verantwortlichen im öffentlichen Bereich eine Datenschutz-Folgenabschätzung durchzuführen ist, insbesondere auf Ziffer 8 der Liste ("Umfangreiche Verarbeitung von Daten über Kinder") Bezug genommen.

9.3 Interessensabfrage für Impfangebote über itslearning

Uns erreichte eine Eingabe, dass in einer weiterführenden öffentlichen Schule in Bremen über die Lernplattform itslearning eine Nachricht an die Schüler:innen versandt wurde, dass ihnen kurzfristig Termine für Impfungen gegen COVID-19 Erkrankungen über das Klinikum Bremen-Mitte angeboten werden könnten. Die Koordinierung sollte über die Schulleitung des Hauses erfolgen. Die Schüler:innen sollten sich bei Interesse an der Vergabe eines Impftermins über itslearning oder persönlich direkt bei der Schulleitung melden. Eine Einbindung der Sorgeberechtigten erfolgte nicht. Diese Abfrage war datenschutzrechtlich unter diversen Aspekten unzulässig. Die Aktion wurde nach Intervention durch uns abgebrochen und die bereits erhobenen Daten wurden gelöscht.

9.4 Befragung zum Stellenwert von sexuellen Orientierungen und geschlechtlichen Identitäten

Uns erreichte eine Eingabe, dass die Senatorin für Kinder und Bildung eine Befragung der Schüler:innen zum Thema "Stellenwert von sexueller und geschlechtlicher Vielfalt" in Planung

---

2 https://www.datenschutz.bremen.de/sixcms/media.php/13/Liste%20von%20Verarbeitungsvorg%C3%A4ngen%20nach%20Artikel%2035.pdf

habe. Zur Vorbereitung dieser Befragung ließ die Behörde über die Schulen ein Schreiben mit der Bezeichnung "Elterninformation über eine Befragung, hier: Einverständniserklärung" an die Schüler:innen verteilen, in dem die "Eltern und Erziehungsberechtigten" aufgefordert wurden, durch Ankreuzen anzugeben, ob sie mit der Teilnahme des Kindes an der Befragung einverstanden oder nicht einverstanden seien. Die begleitende Angabe, die geplante Befragung sei "anonym", war datenschutzrechtlich unzutreffend. Gegenstand der Befragung waren zudem personenbezogene Daten besonderer Kategorien für die nach Artikel 9 der Datenschutzgrundverordnung ein besonders hohes Schutzniveau besteht. Sowohl die Abfrage bei den Sorgeberechtigten als auch die geplante Befragung der Schüler:innen waren datenschutzrechtlich unter mehreren Gesichtspunkten unzulässig, sodass der Abbruch der Erhebung in der bestehenden Form sowie die Vernichtung bereits erhobener Daten angeordnet wurden.

10. Beschäftigtendatenschutz

10.1 Gemeldete Datenschutzverletzungen

Im Bereich Beschäftigtendatenschutz wurden im Jahr 2021 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit insgesamt 33 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. Darüber hinaus erreichten uns viele telefonische Anfragen, welche häufig im Zusammenhang mit der andauernden Pandemielage standen. Diese betrafen unter anderem die Möglichkeiten der Kontaktnachverfolgung, die Abfrage des Impfstatus sowie die Nutzung von Videokonferenzsystemen.

10.2 Weitergabe von privaten Kontaktdaten der Beschäftigten an einen Auftraggeber

Uns erreichte die Information, dass ein Dienstleister im Veranstaltungsgewerbe im Rahmen der Organisation einer größeren Veranstaltung eine Liste mit privaten Festnetz- und Handynummern der Beschäftigten, die bei der Veranstaltung im Einsatz waren, an den Veranstalter herausgegeben hatte. Dies sollte der Kontaktnachverfolgung im Rahmen der Corona-Pandemie dienen. Wir wiesen den Verantwortlichen darauf hin, dass aufgrund der 17. Corona-Verordnung zwar eine Erfassung der bei einer Veranstaltung anwesenden Personen durch den Veranstalter erfolgen musste, die Herausgabe der privaten Daten der Beschäftigten durch den Arbeitgeber jedoch nicht zulässig war. Wie der bremische Verordnungsgeber (beispielsweise in § 6 Absatz 1 Satz 3 der 29. Corona-Verordnung) inzwischen ausdrücklich klargestellt hat, wird bei dienstlichen Tätigkeiten auch die Angabe der dienstlichen Kontaktdaten als ausreichend erachtet. Auch müssen die Kontaktdaten direkt bei den Beschäftigten erhoben werden.

Aufgrund unseres Hinweises auf die Unzulässigkeit der erfolgten Verarbeitung versicherte uns das Dienstleistungsunternehmen, dass das Verfahren angepasst worden sei und die Namen der anwesenden Beschäftigten nur noch auf Aufforderung des Gesundheitsamtes Bremen an dieses herausgegeben würden. Eine Herausgabe an Dritte, wie zum Beispiel Veranstalter, erfolge hingegen nicht mehr.

10.3 Impflisten beziehungsweise Abfrage des Impfstatus

Wie schon im Vorjahr erreichten uns diverse Anfragen und Beschwerden im Pandemiekontext. Diese betrafen häufig die Abfrage des Impfstatus durch Arbeitgeber:innen. Neben Anfragen von öffentlichen sowie nicht öffentlichen Arbeitgeber:innen hinsichtlich der Zulässigkeit der Abfrage waren auch mehrere Beschwerden Beschäftigter über die Forderung nach Offenlegung des Impfstatus zu verzeichnen. In allen Fällen wiesen wir darauf hin, dass die Abfrage des Impfstatus regelmäßig unzulässig sei, da es sich bei dem Impfstatus sowie dem Genesungsstatus um ein Gesundheitsdatum handele, dessen Verarbeitung grundsätzlich verboten und nur ausnahmsweise erlaubt sei. Eine Abfrage ist nur auf Grundlage gesetzlicher Regelungen möglich, welche sich aus dem Infektionsschutzgesetz (IfSG) oder aus Rechtsverordnungen zur Pandemiebekämpfung auf Basis des IfSG ergeben können.

Dies wird auch aus dem Beschluss der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 19. Oktober 2021 deutlich. Danach dürfen Arbeitgeber:innen das Datum Impfstatus ihrer Beschäftigten ohne eine ausdrückliche gesetzliche Ermächtigung grundsätzlich nicht verarbeiten. Lediglich in Einzelfällen ist die Verarbeitung auf Grundlage gesetzlicher Regelungen möglich. So dürfen bestimmte – im Gesetz genannte – Arbeitgeber:innen aus dem Gesundheitsbereich unter den im Infektionsschutzgesetz genannten gesetzlichen Voraussetzungen den Impfstatus ihrer Beschäftigten verarbeiten. Auch weitere im Gesetz genannte Arbeitgeber:innen, wie zum Beispiel Träger:innen von Kindertageseinrichtungen, ambulanten Pflegediensten et cetera, dürfen unter den in § 36 Absatz 3 IfSG genannten Voraussetzungen den Impfstatus ihrer Beschäftigten im Zusammenhang mit COVID-19 verarbeiten. Eine weitere Rechtsgrundlage stellt § 56 Absatz 1 Infektionsschutzgesetz dar. Danach dürfen Arbeitgeber:innen den Impfstatus derjenigen Beschäftigten verarbeiten, die ihnen gegenüber aufgrund einer möglichen Infektion mit dem Coronavirus SARS-CoV-2 sowie einer sich anschließenden Quarantäne einen Anspruch auf Lohnersatz geltend machen. Eine Verarbeitung ist ebenfalls zulässig, soweit dies durch Rechtsverordnungen zur Pandemiebekämpfung auf Basis des IfSG vorgegeben ist. Die Verarbeitung aufgrund einer Einwilligung der Beschäftigten scheidet hingegen regelmäßig aus, da aufgrund des im Beschäftigtenverhältnisses bestehenden Über- und Unterordnungsverhältnisses Zweifel an der Freiwilligkeit der Einwilligung bestehen.

Auch nach der Neufassung des § 28 b IfSG im November 2021 dürfen Arbeitgeber:innen weiterhin den Impfstatus ihrer Beschäftigten nicht direkt abfragen, sondern lediglich im Rahmen der Zutrittskontrolle einen 3G-Nachweis verlangen. § 28 b IfSG regelt, dass Arbeitgeber:innen und Beschäftigte Arbeitsstätten nur betreten dürfen, wenn sie geimpft, genesen oder getestet sind und einen Nachweis mit sich führen, der den 3G-Status belegt. Bei der Umsetzung der 3G-Regelung handelt es sich um eine Verarbeitung von Gesundheitsdaten von Beschäftigten. Es sind daher zwingend die Grundsätze der Datenminimierung, der Speicherbegrenzung sowie der Vertraulichkeit und Integrität zu beachten. So ist unter anderem zu prüfen, ob eine reine Abfrage der Gesundheitsdaten zur Zweckerreichung bereits ausreichend ist. Auch müssen die Daten unverzüglich gelöscht werden, sobald der Zweck für die Speicherung der Gesundheitsdaten entfallen ist. Das Gesetz sieht für die 3G-Daten derzeit eine maximale Speicherdauer von sechs Monaten vor. Auch müssen für die Zutritts- beziehungsweise Nachweiskontrollen geeignete Beschäftigte oder Dritte eingesetzt werden, welche auf die Verschwiegenheit zu verpflichten sind. Der Kreis der Personen, die Zugang zu den 3G-Daten der Beschäftigten haben, ist dabei so klein wie möglich zu halten. Arbeitgeber:innen sind darüber hinaus dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zur Datensicherheit zu ergreifen, bei denen auch berücksichtigt werden muss, dass es sich bei den erfassten Daten um eine besondere Kategorie personenbezogener Daten im Sinne des Artikel 9 Datenschutzgrundverordnung handelt. Dies verdeutlicht auch die DSK in ihrer Anwendungshilfe[3] vom 20. Dezember 2021. Diese enthält häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie und soll die Rechtsanwendung bei der Pandemiebekämpfung im Bereich des Beschäftigtendatenschutzes erleichtern.

10.4 Mitteilung der Coronatest-Ergebnisse per WhatsApp

Arbeitgeber:innen sind aufgrund von § 4 der SARS-CoV-2-Arbeitsschutzverordnung verpflichtet, Beschäftigten, die nicht ausschließlich in ihrer Wohnung arbeiten, zweimal pro Kalenderwoche einen Test in Bezug auf einen direkten Erregernachweis des Coronavirus anzubieten. Im Land Bremen sind die Beschäftigten aufgrund der hier geltenden Corona-Verordnung verpflichtet dieses Testangebot anzunehmen, wobei für Geimpfte und Genesene Ausnahmen gelten. Eine Nachweispflicht hinsichtlich der erfolgten Durchführung der Tests durch die Beschäftigten ist hingegen nicht geregelt. Viele Arbeitgeber:innen ließen sich dennoch, ohne rechtliche Grundlage, die Testergebnisse ihrer Beschäftigten vorlegen und übertrugen diese sogar teilweise in Listen.

[3] https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf

In einem Fall wurden Beschäftigte sogar angehalten, ihre Testergebnisse abzufotografieren und in eine betriebliche WhatsApp-Gruppe hochzuladen, sodass nicht nur ihre Vorgesetzten, sondern auch alle anderen Mitglieder der WhatsApp-Gruppe Kenntnis über das Testergebnis erhielten. Nicht nur deshalb, weil dadurch Kontaktdaten ohne ausreichende Rechtsgrundlage auf Server außerhalb der Europäischen Union übermittelt werden, ist die Nutzung von WhatsApp für die Übermittlung von Beschäftigtendaten in jedem Fall unzulässig. Vorliegend wurden darüber hinaus mit den Testergebnissen Gesundheitsdaten der Beschäftigten übermittelt, welche zu den besonderen Kategorien personenbezogener Daten gehören. Deren Verarbeitung ist nach Artikel 9 Datenschutzgrundverordnung grundsätzlich verboten und nur ausnahmsweise erlaubt. Ein entsprechender Ausnahmetatbestand war hier nicht gegeben. Nachdem wir den betreffenden Verantwortlichen auf die Unzulässigkeit der Verarbeitung hingewiesen hatten, stellte dieser das bemängelte Vorgehen ein. Auch wurde unser Schreiben zum Anlass genommen, den Umgang mit Telekommunikationsmitteln im Betrieb zu überdenken und zukünftig gänzlich auf die Nutzung von WhatsApp im betrieblichen Kontext zu verzichten.

10.5 Unzulässigkeit dauerhafter Videokonferenzen

Einige Anfragen von Beschäftigten betrafen die Frage der Zulässigkeit von dauerhaften Videokonferenzen. Die Aufforderung an Beschäftigte, im Homeoffice dauerhaft die Kamera einzuschalten, um so eine schnellere Kommunikation ähnlich wie im normalen Büroalltag zu ermöglichen, ist aus Gründen des Beschäftigtendatenschutzes unzulässig. Eine solche dauerhafte Videokonferenz führt zu einem immensen nicht hinnehmbaren ständigen Überwachungsdruck der Beschäftigten und stellt einen schwerwiegenden Eingriff in die Privatsphäre dar, für den es keine gesetzliche Rechtsgrundlage gibt.

10.6 Einsehbar gespeicherte Personaldaten

In einem Teil des Netzwerkes der Polizei Bremen, in welchem Daten abgelegt werden können, um einem größeren Kreis von zugriffsberechtigten Nutzer:innen die Möglichkeit zu geben, gemeinsam Daten zu verarbeiten, wurden durch einen Mitarbeiter unter anderem auch Personaldaten abgelegt. Auch wenn kein Zugriff auf die Ordnerinhalte möglich war, so waren doch die Überschriften der Ordnerstrukturen für sämtliche Personen mit einer Zugriffsberechtigung für den betreffenden Teil des Netzwerkes sichtbar. Einsehbar waren neben den Namen einzelner Beschäftigter auch weitere Überschriften wie zum Beispiel "Auflistung von Krankheitstagen", "Beurteilung", "Schwerbehinderung". Nachdem die Polizei Bremen von der Fehlspeicherung Kenntnis erlangt hatte, wurde der entsprechende Ordner umgehend gesperrt und kurz darauf komplett gelöscht. Außerdem meldete uns die Polizei Bremen den Datenschutzvorfall und berichtete auf unsere Nachfrage hin darüber, dass vor Inkrafttreten des novellierten Bremischen Polizeigesetzes (BremPolG) im November 2020

sämtliche Mitarbeiter:innen mittels Multiplikatoren-Schulungen über die neuen datenschutzrechtlichen Regelungen des BremPolG geschult worden seien. Aufgrund des genannten Vorfalls seien zusätzliche Sensibilisierungsmaßnahmen durchgeführt worden. Auch wurde angekündigt, zukünftig häufiger Schulungen zum Thema Datenschutz durchzuführen. Darüber hinaus werde eine Anpassung der Führungskräftequalifizierung geprüft, um auch hier für eine Sensibilisierung bezüglich des Schutzes personenbezogener Daten zu sorgen.

10.7 Personaldaten für einen unberechtigten Personenkreis einsehbar gespeichert

Durch mehrere Beschwerden erhielten wir davon Kenntnis, dass bei einem Verkehrsunternehmen Personaldaten (unter anderem Protokolle von Gesprächen mit Beschäftigten, Einschätzungen über Mitarbeitende, Abwesenheitslisten, Dokumente zur Pandemiebekämpfung) in einem digitalen Ordner abgelegt worden waren, auf den mehr als 20 Führungskräfte aus unterschiedlichen Abteilungen Zugriff hatten. Dies hatte zur Folge, dass verschiedene Vorgesetzte auf Daten von Beschäftigten außerhalb des eigenen Zuständigkeitsbereichs zugreifen konnten. Nachdem das Unternehmen in einem Rundschreiben die Beschäftigten über den Datenschutzverstoß informiert hatte und den Vorfall auch gemäß Artikel 33 Datenschutzgrundverordnung (DSGVO) an die Landesbeauftragten für Datenschutz und Informationsfreiheit gemeldet hatte, gingen auch mehrere Beschwerden von Beschäftigten bei uns ein. Personenbezogene Daten von Beschäftigten dürfen nach § 26 Bundesdatenschutzgesetz im Beschäftigungsverhältnis nur verarbeitet werden, wenn dies für die Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Erforderlich sind regelmäßig Daten, die der Arbeitgeber zur Erfüllung gesetzlicher oder vertraglicher Pflichten benötigt. Zur Durchführung des Arbeitsverhältnisses ist die Kontrolle der Arbeitsleistung grundsätzlich in engen Grenzen zulässig, unzulässig hingegen ist die dauerhafte Überwachung der Beschäftigten. Auch im Rahmen der Kontrolle der Arbeitsleistung ist stets der Grundsatz der Datenminimierung zu beachten. Die Verarbeitung der personenbezogenen Daten muss also dem Zweck angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Der Kreis der zugriffsberechtigten Personen muss daher insbesondere bei Personaldaten auf die jeweils zuständigen Mitarbeiter:innen begrenzt werden. Eine Erweiterung der Zugriffsrechte, die zwar der Arbeitserleichterung dienen mag, jedoch nicht erforderlich ist, ist dementsprechend unzulässig. Daher wurde durch den Verantwortlichen nach Bekanntwerden des Datenschutzvorfalls der Zugriff auf die entsprechenden Ordner gesperrt und eine Umstrukturierung der Benutzerberechtigungssteuerung vorgenommen. Gemäß dem Prinzip der minimalen Berechtigung haben nun alle Beschäftigten ausschließlich Zugriff auf die Daten, die sie im Rahmen ihrer Tätigkeit benötigen.

10.8 Versendung eines nicht anonymisierten Sozialplans an Beschäftigte

Uns erreichte die Information, dass ein Hersteller von Computer Hard- und Software im Rahmen einer betriebsbedingten Kündigung einen nicht anonymisierten Sozialplan an die Beschäftigten versendet hatte. Dieser enthielt unter anderem neben einer Namensliste Angaben zu Familienstand, Unterhaltspflichten, Geburtsdatum, Beschäftigungsdauer, Betriebsratszugehörigkeit und Schwerbehinderung der betroffenen Beschäftigten. Nachdem wir das Technologieunternehmen darauf hingewiesen hatten, dass dieses Vorgehen datenschutzrechtlich unzulässig war, erfolgte ein erneutes Anschreiben an die Beschäftigten durch die verantwortliche Stelle. Dieser war die entsprechende Liste erneut beigefügt, die Namen waren jedoch geschwärzt worden. Anders als die verantwortliche Stelle dachte, handelt es sich bei einem solchen Vorgehen nicht um eine Anonymisierung, sondern lediglich um eine Pseudonymisierung, da aufgrund der übrigen Daten weiterhin Rückschlüsse auf die betroffenen Personen möglich waren. Nach unserem erneuten Hinweis auf die datenschutzrechtliche Unzulässigkeit auch dieser Versendung des Sozialplanes teilte die verantwortliche Stelle mit, dass die Beschäftigten nun zur Vernichtung der fälschlicherweise erhaltenen Daten aufgefordert worden seien. Darüber hinaus seien Sensibilisierungsmaßnahmen durchgeführt und eine Anpassung der Arbeitsabläufe initiiert worden, um derartige Datenschutzverstöße zukünftig zu vermeiden.

11. Videoüberwachung

11.1 Gemeldete Datenschutzverletzungen

Im Bereich Videoüberwachung gab es im Berichtsjahr keine Meldungen der Verletzung des Schutzes personenbezogener Daten nach Artikel 33 der Datenschutzgrundverordnung (DSGVO). Hingegen erhielten wir im Berichtszeitraum 43 Beschwerden, die sich auf Videoüberwachungen durch private Stellen bezogen.

11.2 Fahrassistenzsysteme in hochmodernen Fahrzeugen

Uns erreichen immer wieder Beschwerden von Bürger:innen, die sich durch Videoaufnahmen aus geparkten Fahrzeugen in ihren Rechten verletzt fühlen. Ursache ist die zunehmende Ausrüstung der Fahrzeuge der neuesten Generation mit hochmodernen Fahrassistenzsystemen, die auf kleine Kameras zurückgreifen. Diese fest mit der Karosserie verbauten Geräte sollen laut Hersteller dem Schutz vor Diebstahl und Vandalismus dienen. Bei einem parkenden Fahrzeug wird hierbei die Umgebung rund um das Fahrzeug aufgenommen, die Videobilder vorläufig abgespeichert und nach festgelegter Zeit wieder überschrieben. Kommt es in der Nähe des parkenden Fahrzeuges zu einer verdächtigen Bewegung, werden die Videobilder für einen festgelegten Zeitraum vor und nach dem Ereignis

gespeichert. Da es sich bei diesen gespeicherten Videodaten häufig um personenbezogene Daten handelt, dürfen diese nicht verarbeitet werden, es sei denn, es gibt eine gesetzliche Grundlage hierfür oder die abgebildete Person hat eingewilligt. Eine solche Einwilligung ist bei Videodaten aus dem Auto heraus nicht einholbar. Aus diesem Grund sind derartige Videokameras nicht rechtskonform einsetzbar. Wir fordern daher regelmäßig die Halter:innen der Fahrzeuge auf, die Funktionen der Videodatenspeicherung zu deaktivieren und das Speichermedium zu entfernen. Es bleibt zu hoffen, dass die Hersteller in ihren Fahrzeugen künftig durch den Verzicht auf diese Kameras datenschutzgerechte Funktionalitäten ab Werk gewährleisten, denn für die von ihnen verbauten Kameras liegt die datenschutzrechtliche Verantwortung bei den Fahrzeughalter:innen.

11.3 Videoüberwachung von Großbaustellen

Auch in diesem Berichtszeitraum erreichten uns Beschwerden zur Videoüberwachung von Großbaustellen. Vorwiegend wurde von den Beschwerdeführenden eine Überwachung unmittelbar angrenzender öffentlicher Fußwege, Straßen sowie Parkplätze befürchtet, da die Ausrichtung der Kameras aufgrund einer dunklen Abdeckung nicht zu erkennen war. Da sich die Baustellen häufig in bereits stark bebauten Gebieten befanden, es sich zumeist um Lückenbebauungen handelte oder eine vorhandene alte Bausubstanz neu erstellt wurde, waren auch die sich in unmittelbarer Nachbarschaft befindlichen Privatgrundstücke und Gebäude von der Kameraüberwachung betroffen. Bauunternehmen beauftragen zunehmend spezielle Überwachungsfirmen mit der Videoüberwachung der Baustellen, um Diebstähle von Baumaterialien zu verhindern. Bei den von den Spezialfirmen eingesetzten Kameras handelt es sich zumeist um Domekameras, die an mobilen Beleuchtungsmasten installiert sind. Auf unsere schriftlichen Anfragen hin teilten uns die verantwortlichen Stellen mit, dass keine öffentlichen Bereiche miterfasst würden, da diese ausgeblendet würden und auch bei einer Einsicht in die aufgezeichneten Daten im Nachgang nicht wieder sichtbar gemacht werden könnten. Anhand der uns übersandten Screenshots der einzelnen Kameras konnten wir feststellen, dass tatsächlich keine öffentlich zugänglichen Bereiche sowie angrenzende Grundstücke von den Kameras erfasst wurden und somit kein Verstoß gegen datenschutzrechtliche Vorschriften festzustellen war.

12. Wirtschaft und Gewerbe

12.1 Gemeldete Datenschutzverletzungen

Wie bereits im Vorjahr waren es auch in diesem Berichtszeitraum leider wieder etliche erfolgreiche Schadware-Attacken auf die IT-Infrastruktur, auf die Meldungen verantwortlicher Stellen verschiedenster Branchen über Verletzungen des Schutzes personenbezogener Daten zurückgingen. Mitunter erfolgten Meldungen auch rein vorsorglich im Hinblick auf

entdeckte Sicherheitslücken bei Software-Produkten, die potenziell einen Zugriff Unbefugter auf personenbezogene Daten möglich erscheinen ließen. Weitere Fälle betrafen den Versand elektronischer Nachrichten über die offenen Empfänger-Adressfelder "An" beziehungsweise "Cc" an eine Vielzahl von Kund:innen oder Mitgliedern unter Nutzung deren personenbezogener beziehungsweise personenbeziehbarer E-Mail-Adressen (siehe hierzu Ziffer 12.7 dieses Berichts) und den Diebstahl mobiler Endgeräte mit gespeicherten personenbezogenen Daten.

12.2 Fehlende Betroffenenauskünfte

Ein nicht unerheblicher Anteil der Beschwerdefälle im Bereich Wirtschaft und Gewerbe entfiel auch in diesem Berichtszeitraum wieder auf tatsächliche oder mutmaßliche Verletzungen des Betroffenenselbstauskunftsrechts aus Artikel 15 Datenschutzgrundverordnung. Die Ursachen für ein Unterbleiben der Erteilung einer geforderten Selbstauskunft sind mannigfaltig. Eine häufigere Fehlerquelle ist dabei schlicht eine unzureichende Ablauforganisation. In einem Fall ging der Verantwortliche irrigerweise davon aus, dass er die Auskunftserteilung nicht schriftlich gegenüber dem Betroffenen erteilen könne, da dieser nicht eingewilligt habe. Wir konnten diesen Irrtum aufklären und für eine zeitnahe Auskunftserteilung sorgen. In einem anderen Fall verweigerte die Verantwortliche die Auskünfte aufgrund eines ihrer Ansicht nach rechtsmissbräuchlichen Verhaltens des Betroffenen. Dieser hatte nach der Darstellung der Verantwortlichen zeitgleich zum Auskunftsbegehren diverse öffentliche Stellen mit dem Ziel angeschrieben, die Verantwortliche und ihre Mitarbeiter in Misskredit zu bringen und zu schädigen. Wir beanstandeten die Auskunftsverweigerung. Etwaige Konflikte mit Betroffenen können nicht dazu führen, den datenschutzrechtlichen Auskunftsanspruch einzuschränken. Verantwortliche haben die Möglichkeit, gegen etwaige unwahre Behauptungen zivilrechtlich oder strafrechtlich vorzugehen. Im beschriebenen Fall erteilte die Verantwortliche nach unserer Intervention die gewünschte Auskunft.

12.3 Kontaktdatenerhebung im Gastronomiebereich

Ein Teil unserer Aufsichtstätigkeit im Bereich Wirtschaft und Gewerbe entfiel erneut auf Sachverhalte im Zusammenhang mit der Bewältigung der Corona-Pandemie (siehe für den Krankenhausbereich Ziffer 8.3 dieses Berichts und 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffern 1.3 und 12.4). Exemplarisch erreichten uns im Rahmen der Kontaktdatenerhebung im Bereich der Gastronomie im Berichtsjahr vier Beschwerden. In zwei Fällen erhielten wir den Hinweis, dass die Corona-Kontaktdatenerhebung auf fortlaufenden Listen erfolgt sei, sodass Gäste die Daten anderer Gäste einsehen konnten. In einem anderen Fall wurde ein Kontaktformular sogar an einen anderen Gast herausgegeben, in einem weiteren Fall war das Kontaktformular abhandengekommen. Wir forderten die jeweiligen Verantwortlichen umgehend zur Stellungnahme auf. In zwei Fällen sprachen wir

Verwarnungen im Sinne von Artikel 58 Absatz 2 Buchstabe b Datenschutzgrundverordnung (DSGVO) aus, in einem Fall beließen wir es bei einer formlosen Ermahnung und in einem Fall konnten wir keinen Verstoß feststellen.

Aufgrund der Vielzahl der gastronomischen Betriebe im Land Bremen gehen wir davon aus, dass uns nur Informationen über einen kleinen Teil der Verstöße gegen die DSGVO hinsichtlich der Verarbeitung von personenbezogenen Daten im Rahmen der Kontaktdatenerhebung erreicht haben. Wir gehen von einer hohen Dunkelziffer aus. Deshalb weisen wir nochmals (siehe hierzu unsere Pressemitteilung "Offene Listen von Gästedaten in Gaststätten: Verletzung des Rechts, selbst zu entscheiden, an welche Privatpersonen Handynummern und Mailadressen weitergeben werden" vom 2. Juni 2020[4]) darauf hin, dass die nicht digitale Corona-Kontaktdatenerhebung (zur digitalen Kontaktnachverfolgung siehe Ziffer 17.3 dieses Berichts) auf separaten Kontaktverfolgungsformularen erfolgen muss. Nach § 6 Absatz 2 der 29. Corona-Verordnung müssen die Verantwortlichen geeignete Vorkehrungen dafür treffen, dass diese Formulare keinem unberechtigten Dritten zugänglich gemacht werden. Die entsprechenden personenbezogenen Daten dürfen ausschließlich dem zuständigen Gesundheitsamt herausgegeben werden. Nach Ablauf von vier Wochen müssen die Kontaktformulare datenschutzkonform vernichtet werden. Auch müssen Gastwirt:innen ihren Informationspflichten nach Artikel 13 DSGVO nachkommen. Dazu gehört auch, ihren Gästen genau zu erklären, was mit ihren Daten passieren wird, wie die Daten sicher aufbewahrt und wie sie vernichten werden. Auch müssen die Gäste über ihr Recht auf Auskunft, ihr Recht auf Berichtigung, ihr Recht auf Löschung und darüber informiert werden, dass sie sich bei der Landesbeauftragten für Datenschutz und Informationsfreiheit darüber beschweren können, wenn sie den Eindruck haben, dass die Gastwirt:innen sich nicht an die Regeln halten.

12.4 Datenerhebung durch Kaufhausdetektiv

Im Bereich des Einzelhandels erreichte uns ein besonders gravierender Fall einer unbefugten Weitergabe personenbezogener Daten. Ein Kaufhausdetektiv hatte einem mutmaßlichen Ladendieb bereits gestellte Strafanzeigen gegen andere mutmaßliche Ladendieb:innen gezeigt. Zudem fertigte der Kaufhausdetektiv mit seinem Mobiltelefon ein Foto des mutmaßlich auf frischer Tat Erwischten an und lud dies in einen WhatsApp-Gruppe mit anderen Kolleg:innen des Einzelhandelsgeschäftes hoch.

Dieses Vorgehen wurde von uns umgehend beanstandet. Der Inhaber des Einzelhandelsgeschäftes als Verantwortlicher zeigte sich einsichtig und ergriff Gegenmaßnahmen. Das Foto wurde sofort gelöscht. Die bei dem Verantwortlichen tätigen

[4] https://www.datenschutz.bremen.de/sixcms/media.php/13/Pressemitteilung_02Juni2020.pdf

Beschäftigten, insbesondere der betreffende Kaufhausdetektiv, wurden im Bereich Datenschutz nachgeschult. Zudem wurde ein Datenschutzkonzept erstellt; darin war angegeben, dass keine Fotos von mutmaßlichen Ladendieben angefertigt werden dürfen. Zudem dürfe keine Weiterleitung und Verbreitung von Anzeigen über Messenger-Dienste wie WhatsApp oder Social Media erfolgen.

12.5 Anspruch auf Protokollierung von Grundbucheinsichtnahmen

Im Berichtszeitraum erbat ein Miteigentümer eines Grundstücks, das als Standort von Windkraftanlagen in Betracht kommt, unseren Rat. Er sei von einem ihm völlig unbekannten Unternehmen aus der Windkraftbranche zur Abklärung seiner etwaigen Verkaufsbereitschaft angeschrieben worden. Woher dieses Unternehmen um sein Miteigentum und seine Kontaktdaten wisse, sei ihm unverständlich.

In der Sache hatte das Unternehmen vermutlich zunächst einmal Einsicht in das öffentliche Grundstücksregister, das Grundbuch, genommen. Jedem, der ein "berechtigtes Interesse" darlegt, ist die Einsichtnahme gestattet. Freilich hat das Grundbuchamt über die Einsichtnahmen Protokoll zu führen. Eine Grundbuch-Einsichtnahme durch einen Dritten lässt sich also seitens der (Mit-) Eigentümer:innen überprüfen, da sie einen Anspruch auf Auskunft aus diesem Protokoll besitzen. Neben diesem Anspruch gegenüber dem Grundbuchamt stand dem von der Verarbeitung seiner Daten Betroffenen auch ein Recht auf Auskunft nach Artikel 15 Datenschutzgrundverordnung (DSGVO) gegenüber dem Unternehmen zu. Mittels dieser beiden Ansprüche hatte der Betroffene also die Möglichkeit, die Verarbeitung seiner Daten zu kontrollieren.

12.6 Kein Energiekunden-Auskunftspool

Im Herbst/Winter des Jahres 2020 waren Gedankenspiele zweier Wirtschaftsauskunfteien zum Aufbau von Branchendatenbanken für Energieversorgungsunternehmen in der Öffentlichkeit bekannt geworden. In diesen "Datenpools" sollten wohl insbesondere auch Informationen über störungsfrei verlaufende Energieversorgungsvertragsverhältnisse mit privaten Haushaltskunden gesammelt und dann im Kreis der Energieversorger bei Bedarf ausgetauscht werden können. Die Überlegungen sorgten für erhebliche Verunsicherung in der Öffentlichkeit und lösten eine Diskussion zur Frage der Vereinbarkeit beziehungsweise Unvereinbarkeit entsprechender Datenverarbeitungsvorgänge mit der europäischen Datenschutzgrundverordnung aus. Auch der Deutsche Bundestag befasste sich mit der Thematik (siehe hierzu die Kleine Anfrage, Bundestags-Drucksache[5] 19/23338 vom 13. Oktober 2020).

[5] https://dip21.bundestag.de/dip21/btd/19/233/1923338.pdf

Wir hatten bereits früh den Standpunkt vertreten, dass eine derartige Sammlung von Vertragsinformationen abgesehen von einer praktisch eher nicht realistischen Einwilligung der privaten Energieversorgungskunden keine datenschutzrechtliche Grundlage fände. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder nahm sich der Frage an und bekundeten ihre einvernehmliche Rechtsauffassung in einer öffentlichen Mitteilung Mitte März des Berichtsjahres (siehe hierzu im Anschluss dieser Ziffer den vollständigen Text des Beschlusses). Kurz zusammengefasst kann nach einheitlicher Rechtsansicht eine Übermittlung von Informationen zu einem störungsfrei verlaufenden Energieversorgungsvertrag eines Haushaltskunden in einen Branchendatenpool der Energieversorgungsunternehmen rechtlich nicht auf der praktisch einzig denkbaren Grundlage einer Interessenabwägung erfolgen.

"Energieversorgerpool" darf nicht zu gläsernen Verbraucher:innen führen

(Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 15. März 2021)

Bei Auskunfteien und Energieversorgern gibt es Überlegungen, einen sogenannten Energieversorgerpool zu schaffen. In diesem zentralen Datenpool sollen auch Positivdaten der Kund:innen gespeichert und an andere Energieversorger übermittelt werden. Positivdaten sind Daten über Verträge, bei denen die Belieferten keinen Anlass zu Beanstandungen geben, sich also vertragskonform verhalten. Informationen über die Anzahl abgeschlossener Verträge und die jeweilige Vertragsdauer können Hinweise darauf geben, ob Verbraucher:innen eine längere Vertragsbeziehung zu einem Stromversorger beabsichtigen oder etwa regelmäßig Angebote für Neukund:innen nutzen. Verbraucher:innen, die regelmäßig das für Sie kostengünstigste Angebot am Markt wählen und dazu den Anbieter wechseln möchten, könnten dann von Versorgungsunternehmen bei preislich attraktiven Angeboten ausgeschlossen werden. Jede Bürgerin und jeder Bürger hat jedoch das Recht, den Wettbewerb zwischen den Energieversorgern zu nutzen und am Markt nach günstigen Angeboten zu suchen. Der Wunsch, vermeintliche "Schnäppchenjäger" in einem zentralen Datenpool zu erfassen, um sie bei Vertragsanbahnung als solche identifizieren und gegebenenfalls von Angeboten ausschließen zu können, stellt kein berechtigtes Interesse im Sinne des Artikel 6 Absatz 1 Satz 1 Buchstabe f) Datenschutzgrundverordnung (DSGVO) dar. Es war gerade das Ziel des Gesetzgebers, durch die Liberalisierung des Energiemarktes einen wirksamen und unverfälschten Wettbewerb bei der Versorgung mit Elektrizität und Gas zu ermöglichen. Der Versuch, preisbewusste und wechselfreudige Verbraucher:innen zu identifizieren und sie gegebenenfalls von bestimmten Angeboten auszuschließen, liefe dieser Zielsetzung zuwider. Selbst wenn die Interessen der Unternehmen als berechtigt angesehen würden, überwiegen in derartigen Fällen die schutzwürdigen Interessen und Grundrechte der Kund:innen. Vertragstreue Verbraucher:innen dürfen zu Recht erwarten, dass keine über den

Vertragszweck hinausgehende Verarbeitung ihrer Daten erfolgt, die gegebenenfalls ihre Möglichkeiten einschränkt, frei am Markt agieren zu können. Die Speicherung und Übermittlung von Positivdaten durch einen Energieversorgerpool würde erheblich zu gläsernen Verbraucher:innen beitragen und wäre nach Artikel 6 Absatz 1 Satz 1 Buchstabe f) DSGVO rechtswidrig.

12.7 Offener E-Mail-Verteiler

Zu unserem Aufsichtsalltag gehören in jedem Berichtszeitraum Beschwerden über die – fast immer allein aus Gründen der Unachtsamkeit erfolgende – Weitergabe von personifizierten E-Mail-Adressen durch elektronischen Nachrichtenversand über die für alle Empfänger:innen einsehbaren E-Mail-Adressfelder "An" und "Cc". Exemplarisch hierfür ist folgender Fall: Ein Unternehmen aus der Logistikbranche versandte an über einhundert seiner auch privaten Kund:innen seine neuen Geschäftsbedingungen. Sämtliche Nachrichtenempfänger:innen waren in das Adressfeld "An" eingetragen. Damit erhielten alle Empfänger:innen nicht nur die neuen Geschäftsbedingungen, sondern zusätzlich auch noch im Nachrichtenkopf die zu einem guten Teil personifizierten E-Mail-Adressen ihrer Mitkund:innen. Da mittlerweile bei Unternehmen insoweit ein entsprechendes Datenschutzbewusstsein vorhanden sein muss, ahnden wir derartige Verstöße regelmäßig.

12.8 Keine private Impfdatenverarbeitung ohne Gesetz

Im Februar des Berichtsjahres äußerte sich der Vorstandsvorsitzende eines bundesweit tätigen Unternehmens presseöffentlich zur Impfstatusdatenerhebung durch Veranstalter im Freizeit- und Kulturbereich. Er wurde mit einer Äußerung zitiert, in der er sich dafür aussprach, es privatrechtlichen Veranstaltern zu ermöglichen, eine Impfung zur Zugangsvoraussetzung für Veranstaltungen zu machen, sobald genügend Impfstoff gegen das Coronavirus SARS-CoV-2 vorhanden sei. Das Unternehmen habe seine Systeme technisch in der Weise eingerichtet, dass auch Impfausweise "gelesen" werden könnten.

Ungeachtet der verständlichen wirtschaftlichen Beweggründe nahmen wir dies im Rahmen unseres gesetzlichen Auftrages zur Sensibilisierung verantwortlicher Stellen zum Anlass, darauf hinzuweisen, dass die Verarbeitung von Informationen über den Impfstatus einer Person, also eines Gesundheitsdatums, das unter Umständen weitere Rückschlüsse auf die individuelle körperliche Verfassung zulässt (etwa auf die Zugehörigkeit zu einer Risikogruppe), als besondere Kategorie personenbezogener Daten nach der Datenschutzgrundverordnung (DSGVO) unter hohen Anforderungen steht. Wir wiesen dabei darauf hin, dass ein Gesetz, das nach Maßgabe dieser hohen rechtlichen Anforderungen die Verarbeitung von Impfdaten zu den genannten privatwirtschaftlichen Zwecken erlauben würde, zu diesem Zeitpunkt nicht vorhanden war. Das Partikularinteresse eines privaten Wirtschaftsakteurs am Absatz

beziehungsweise an der Gewinnerzielung im Rahmen von Veranstaltungen genüge nicht, um das gesetzlich notwendige erhebliche öffentliche Interesse an der Verarbeitung zu begründen.

Da es zu diesem Zeitpunkt in der Öffentlichkeit Irritationen über die Zulässigkeit der privaten Impfdatenverarbeitung gab und die Fehlinformation im Raum stand, die Vertragsfreiheit vermöge eine solche Zulässigkeit zu begründen, veröffentlichte die Landesbeauftragte für Datenschutz und Informationsfreiheit am 9. Februar 2021 unter der Überschrift "**Keine private Impfdatenverarbeitung ohne Gesetz**" eine Pressemitteilung mit folgendem Wortlaut:

> Der Presse war zu entnehmen, dass ein bremisches Onlineticketunternehmen bereits technische Voraussetzungen dafür geschaffen hat, es Konzertveranstaltern perspektivisch zu ermöglichen, den Nachweis einer Impfung zur Zugangsvoraussetzung für Veranstaltungen zu machen. Die Landesbeauftragte für Datenschutz und Informationsfreiheit hat das betroffene Unternehmen darauf hingewiesen, dass eine solche Verarbeitung von Impfdaten als "Eintrittskarte" für Veranstaltungen zu privatwirtschaftlichen Zwecken nur mit ausdrücklicher gesetzlicher Erlaubnis möglich wäre und dass es ein entsprechendes Gesetz zum gegenwärtigen Zeitpunkt nicht gibt.
>
> Die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit, Dr. Imke Sommer, hierzu: "Impfdaten sind als Gesundheitsdaten besonders geschützt und dürfen nur in besonderen Ausnahmefällen von Privaten verarbeitet werden. Es ist ein Irrtum zu glauben, dass die Vertragsfreiheit zu den Ausnahmetatbeständen gehört. Auch eine rechtswirksame Einwilligung der Geimpften kann es nicht geben, weil sie nach den Maßstäben der Europäischen Datenschutzgrundverordnung nicht als freiwillig angesehen würde. Wenn nur diejenigen eine Veranstaltung besuchen dürfen, die einen Scan ihres Impfausweises hochladen, liegt ein Verstoß gegen das Koppelungsverbot vor. Die Verarbeitung von Impfdaten durch private Stellen könnte allenfalls in einem Gesetz erlaubt werden, das den hohen Anforderungen der Datenschutzgrundverordnung genügt."

In ihrer Entschließung vom 29. März 2021 (siehe hierzu Ziffer 21.1 dieses Berichts) schloss sich die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder dieser Auffassung an. In der begleitenden Pressemitteilung heißt es: "Im Rahmen der derzeitigen Diskussion über mögliche Öffnungsschritte ist die Frage, ob die Nutzung verschiedenster privatwirtschaftlicher Angebote an den Nachweis einer erfolgten Impfung, einer überstandenen Infektion oder eines negativen Testergebnisses geknüpft werden darf, von zentraler Bedeutung. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hält es für unerlässlich, dass die Voraussetzungen einer solchen Datenverarbeitung, beispielsweise im Kontext von Veranstaltungs- und

Restaurantbesuchen oder im Rahmen von Beschäftigungsverhältnissen, durch den Gesetzgeber geregelt werden. (…) Die DSK fordert den Gesetzgeber mit ihrer heutigen Entschließung daher auf, schnellstmöglich zu handeln und eine gesetzliche Grundlage zu schaffen, die den strengen Vorgaben des Artikels 9 Absatz 2 DSGVO bei der Verarbeitung von Gesundheitsdaten genügt."

Mittlerweile wurden gesetzliche Grundlagen für die Impf-, Genesenen- und Testdatenerhebung durch private Stellen geschaffen. Hierbei handelte es sich zunächst um die Einfügung der Nummer 2a in § 28 a Absatz Infektionsschutzgesetz (IfSG), die notwendige Schutzmaßnahmen zur Verhinderung der Verbreitung von COVID-19 für die Dauer der Feststellung einer epidemischen Lage von nationaler Tragweite durch den Deutschen Bundestag bestimmt. Der bremische Verordnungsgeber machte von der entsprechenden Verordnungsermächtigung durch entsprechende Regelungen in § 3 der jeweiligen Corona-Verordnungen Gebrauch. Seit Auslaufen der epidemischen Lage von nationaler Tragweite ist hierfür § 28 a Absatz 7 Nummer 4 IfSG einschlägig. Hiernach können unabhängig von einer durch den Deutschen Bundestag festgestellten epidemischen Lage von nationaler Tragweite "die Verpflichtung zur Vorlage von Impf-, Genesenen- oder Testnachweisen sowie an die Vorlage solcher Nachweise anknüpfende Beschränkungen des Zugangs in den oder bei (…) Betrieben, Gewerben, Einrichtungen, Angeboten, Veranstaltungen, Reisen und Ausübungen" notwendige Schutzmaßnahmen sein, soweit sie zur Verhinderung der Verbreitung von COVID-19 erforderlich sind.

13. Kreditwirtschaft

13.1 Gemeldete Datenschutzverletzungen

Im Berichtszeitraum erhielten wir neun Meldungen über Datenschutzverletzungen im Kreditwesenssektor. Gegenstand der Meldungen waren etwa die Übermittlung von Kontoinformationen an falsche Empfänger:innen, die fehlerhafte Übermittlung von Unterlagen, in einem Fall die Mitteilung der Privatadresse einer Notarin anstelle ihrer Geschäftsadresse an einen Bankkunden oder technische Defekte an Selbstbedienungs-Terminals (siehe hierzu Ziffer 13.2 dieses Berichts). Auffällig war in diesem Zusammenhang, dass bis auf eine Meldung sämtliche Meldungen von Seiten eines einzigen Kreditinstituts im Land Bremen erfolgten. Die Meldepraxis und Zusammenarbeit gestaltete sich hier in der von der Datenschutzgrundverordnung vorgesehenen Weise. Andere Kreditinstitute, von deren Seite uns keine entsprechenden Meldungen erreichten, sollten sich dies zum Vorbild nehmen. Wir halten es für kaum vorstellbar, dass es lediglich in dem Tätigkeitsbereich eines Kreditinstituts im Land Bremen zu "Datenschutzvorfällen" gekommen ist und werden diesen Befund bei künftigen Aufsichtsverfahren im Fokus behalten.

13.2 Datenschutzvorfälle an Selbstbedienungs-Terminals

Uns erreichten Informationen über mehrere Fälle, in denen die Bildschirme der Selbstbedienungs-Terminals (SB-Terminals) eines Kreditinstituts im Rahmen von Überweisungsvorgängen "einfroren". Dies hatte jeweils zur Folge, dass die Internationale Bankkontonummer (IBAN) der Betroffenen dauerhaft erkennbar war. In einem Fall kam es sogar dazu, dass das SB-Terminal die EC-Karte des Betroffenen einbehielt und diese anschließend nicht mehr auffindbar war.

Auf unseren Hinweis hin passte das Kreditinstitut die Software der SB-Terminals umgehend an, um den Systemfehler, der zum Einfrieren der Bildschirme führte, zu beseitigen. Zudem wurde ein Prozess etabliert, um bei einem erneuten Auftreten eines Systemfehlers für eine sofortige Abschaltung der SB-Terminals zu sorgen. Eine solche sofortige Abhilfe ist von der Datenschutzgrundverordnung gefordert.

13.3 Missbräuchlicher Zugriff auf Kund:innendaten

Ein Kunde eines Kreditinstituts wandte sich im Berichtszeitraum an uns und äußerte die Vermutung, dass in diesem Kreditinstitut unbefugt auf seine Daten zugegriffen worden sei. Mit einer Person, die dort beschäftigt sei, sei der private Kontakt abgebrochen worden. Im Zuge dieses Kontaktabbruchs seien die privaten Kontaktdaten vollständig geändert worden. Gleichwohl habe sich die beim Kreditinstitut beschäftigte Person nun über die neuen Kontaktdaten bei ihm gemeldet. Bei dem Kreditinstitut seien die neuen Kontaktdaten hinterlegt, eine andere Datenquelle könne ausgeschlossen werden. Im Zuge einer Auswertung von Zugriffsprotokolldaten bei dem Kreditinstitut bewahrheitete sich die Vermutung des Kunden. Das Kreditinstitut reagierte umgehend, entzog intern die Zugriffsberechtigungen, traf weitere zusätzliche Absicherungsmaßnahmen und zog ferner arbeitsrechtliche Konsequenzen. Aufsichtsbehördliche Maßnahmen gegenüber dem Kreditinstitut waren in diesem Fall eines sogenannten Beschäftigtenexzesses nicht veranlasst. Zu prüfen bleibt eine Ahndung gegenüber der beschäftigten Person des Kreditinstituts, die missbräuchlich zu Privatzwecken unter Hinwegsetzung über interne organisatorische Vorgaben die Daten des Kunden erhoben und genutzt hatte.

13.4 Keine Betroffenenselbstauskunft an Angehörige Verstorbener

Ein Erbe fragte bei uns an, ob ein Kreditinstitut, das für eine zwischenzeitlich verstorbene Angehörige das Konto führte, ihm Auskunft erteilen müsse, wenn er das datenschutzrechtliche Betroffenenselbstauskunftsrecht der Verstorbenen geltend mache. Wir erläuterten, dass das Betroffenenselbstauskunftsrecht nach der gesetzlichen Konzeption ein höchstpersönliches Recht der von der Datenverarbeitung Betroffenen ist, hier also der verstorbenen

Angehörigen, und allein deren informationelle Selbstbestimmung absichern soll. Der Betroffenenselbstauskunftsanspruch gehört daher nicht zu der an Erb:innen übergehenden Erbschaftsmasse, sondern fällt mit dem Tod der Betroffenen weg.

14. Werbung

14.1 Gemeldete Datenschutzverletzungen

Im Bereich der Werbung wurden der Landesbeauftragen für Datenschutz und Informationsfreiheit keine Meldungen von Verletzungen des Schutzes personenbezogener Daten zugesandt.

14.2 Betroffenenrechte

Im Bereich Werbung und Adresshandel erreichten uns zahlreiche Beratungsanfragen Betroffener. Dabei ging es insbesondere um die Abbestellung von Newslettern und die Betroffenenrechte nach der Datenschutzgrundverordnung (DSGVO), wie zum Beispiel Auskunftsrechte der betroffenen Personen oder das Recht auf Löschung von personenbezogenen Daten.

Wir machten die Betroffenen in diesem Zusammenhang darauf aufmerksam, 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.

Im Zusammenhang mit Direktwerbung, also der Kontaktaufnahme von Unternehmen, Parteien, Verbänden oder Vereinen, die dazu dienen, ihren Absatz zu steigern oder ihre Ziele 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 vom Verantwortlichen nicht mehr hierfür verarbeitet werden.

14.3 Direktwerbung ohne Einwilligung

Wir erhielten 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.

Die verantwortlichen Unternehmen vertraten uns gegenüber die Auffassung, dass diese Kontaktaufnahmen ohne Einwilligung nach Artikel 6 Absatz 1 Buchstabe f

Datenschutzgrundverordnung (DSGVO) aufgrund eines berechtigten Interesses gerechtfertigt seien. Demgegenüber bezweifelt eine Entscheidung des Oberverwaltungsgerichts Saarlouis vom 16. Februar 2021, dass Direktwerbung beispielsweise per Telefon oder E-Mail ohne Einwilligung aufgrund eines berechtigten Interesses im Sinne von Artikel 6 Absatz 1 Buchstabe f DSGVO überhaupt möglich ist. Es sei zwar zutreffend, dass auch die Verarbeitung personenbezogener Daten für Direktwerbung ein berechtigtes Interesse nach dem Erwägungsgrund Nummer 47 zur DSGVO darstellen könne. Allerdings sei in diesem Zusammenhang zu berücksichtigen, dass die Ziele, die mit der Verarbeitung verfolgt würden, unionsrechtskonform sein müssten. Daher gelte auch in diesem Zusammenhang die Wertung des Gesetzes gegen den unlauteren Wettbewerb, wonach Werbung mit einem Telefonanruf bei Verbraucher:innen ohne deren vorherige ausdrückliche Einwilligungen oder bei sonstigen Marktteilnehmer:innen ohne deren zumindest mutmaßliche Einwilligung stets eine unzumutbare Belästigung darstellten. In diesen Fällen könnten sich werbende Verantwortliche daher nicht auf ein "berechtigtes" Interesse berufen.

Vor dem Hintergrund dieser Rechtsprechung ist Werbenden dringender denn je zu raten, die vorherige Einwilligung der jeweiligen Betroffenen einzuholen.

15. Bauen und Wohnen

15.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr 2021 erreichten uns 20 Meldungen bezüglich der Verletzung des Schutzes personenbezogener Daten im Bereich Bauen und Wohnen.

Dabei handelte es sich in mehreren Fällen um den Fehlversand von Unterlagen zum jeweiligen Mietverhältnis. So waren zum Beispiel Mietverträge, Übergabeprotokolle, Kündigungsschreiben und weitere, den Mietvertrag betreffende Dokumente falsch adressiert worden. In einem Vorgang wurde uns ein Cyberangriff auf eine Ingenieursgesellschaft angezeigt.

15.2 Verarbeitung besonderer personenbezogener Daten durch bremische Wohnungsbaugesellschaften

Aufgrund eines Berichts des Fernsehmagazins "buten un binnen" über diskriminierende Vorgehensweisen einer bremischen Wohnungsbaugesellschaft, stand im Berichtsjahr auch die rechtswidrige Verarbeitung besonderer personenbezogener Daten im Raum. Unter anderem sollten sensible personenbezogene Daten von Mietinteressent:innen wie deren Hautfarbe, Religion und sexuelle Orientierung teilweise verklausuliert erfasst und gespeichert

worden sein. Anlässlich dieser Berichte leitete die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) ein datenschutzrechtliches Aufsichtsverfahren ein.

Auch meldete sich eine weitere bremische Wohnungsbaugesellschaft bei der LfDI und teilte mit, dass im Rahmen von internen Ermittlungen auch dort bekannt geworden war, dass sensible personenbezogene Daten, wie unter anderem zu Religion, Hautfarbe und Herkunft ohne datenschutzrechtliche Legitimation erfasst worden waren. Auch hier leitete die LfDI ein Aufsichtsverfahren ein.

Beim Vermietungs- und Mietverwaltungsprozess ist zu beachten, dass für die Verarbeitung besonderer Kategorien personenbezogener Daten, zu denen auch solche gehören, aus denen die "rassische oder ethnische Herkunft" im Sinne des Artikel 9 Absatz 1 Datenschutzgrundverordnung (DSGVO), religiöse Überzeugungen oder die sexuelle Orientierung der betroffenen Personen hervorgehen, nach Artikel 9 DSGVO ein Verarbeitungsverbot gilt, von dem es nur enge Ausnahmemöglichkeiten gibt. Auch müssen betroffene Personen nach der DSGVO im Zeitpunkt der Erhebung ihrer Daten wahrheitsgemäß, vollständig und unaufgefordert über die Zwecke und Rechtsgrundlagen der Verarbeitung hinsichtlich aller sie betreffenden personenbezogenen Daten informiert werden. Hingewiesen sei in diesem Zusammenhang auf die Orientierungshilfe zur "Einholung von Selbstauskünften bei Mietinteressentinnen" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder[6].

15.3 Datenschutzkonformität von digitalen Wasserzählern mit Fernauslesemöglichkeit (Funkwasserzähler)

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) befasste sich im Berichtsjahr mit der Frage der Datenschutzkonformität von digitalen Wasserzählern mit Fernauslesemöglichkeit (sogenannte Funkwasserzähler). Die entscheidende datenschutzrechtliche Problematik bei Funkwasserzählern liegt darin, dass diese digitalen Geräte im Gegensatz zu den bisherigen analogen Wasserzählern in der Lage sind, personenbezogene Daten in einem viel intensiveren und ausführlichen Umfang zu erfassen, zu speichern und weiterzuleiten. Dies ermöglicht sehr detaillierte Informationen zum einzelnen (Verbrauchs-)Verhalten der jeweiligen Nutzer:innen. Daher erfordert die Datenverarbeitung im Rahmen der Nutzung digitaler Wasserzähler ab einer Gebäudedimension, bei der Personenbeziehbarkeit angenommen werden kann, eine Rechtsgrundlage. Die LfDI hält die Generalklausel aus dem Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) nicht für eine ausreichende Rechtsgrundlage und fordert

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

eine spezielle, landesrechtliche Rechtsgrundlage, die allein geeignet ist, einen ausreichenden Schutz für das Grundrecht auf die informationelle Selbstbestimmung der Kund:innen des Wasserversorgers zu gewährleisten. Wir wiesen den hiesigen Wasserversorger im Rahmen unserer Beratungsfunktion auf unsere Rechtsauffassung hin, insbesondere unter Hinweis auf das Messstellenbetriebsgesetz, das für sogenannte Smart Meter eine bundesweit geltende Gesetzesgrundlage darstellt. Eine entsprechende landesrechtliche Rechtsgrundlage für den Bereich der Funkwasserzähler schüfe Rechtssicherheit einerseits für die Kund:innen und andererseits für den Wasserversorger.

Aktueller Sachstand ist, dass der Wasserversorger mit der Beschreibung seines Projektes und seinem Anliegen an die senatorische Behörde herangetreten ist. Den Prozess zur Formulierung einer entsprechenden landesrechtlichen Rechtsgrundlage werden wir gern begleiten.

15.4 Datenweitergabe innerhalb von Wohnungseigentümer-gemeinschaften

Wie bereits in den Vorjahren erreichten die Landesbeauftragte für Datenschutz und Informationsfreiheit auch in diesem Jahr zahlreiche Anfragen zum Umgang mit personenbezogenen Daten innerhalb von Wohnungseigentümergemeinschaften (WEG). Im letzten Jahresbericht wurde das Thema Datenverarbeitung durch die Hausverwaltung und insbesondere die Klärung der Verantwortlichkeit behandelt (siehe hierzu 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 16.2).

Auch eine bereits im 2. Jahresbericht nach der Datenschutzgrundverordnung (siehe hierzu Ziffer 16.2) aufgeworfene Frage, stellte sich erneut. Hierbei ging es darum, ob den einzelnen Eigentümer:innen einer WEG aus Datenschutzgründen die Namen, Anschriften und Telefonnummern der Miteigentümer:innen durch die eingesetzte Wohnungsverwaltungsfirma bekanntgegeben werden dürften. Es ist eine klare Differenzierung zwischen den Namen und Anschriften der Eigentümer:innen einerseits und ihren sonstigen Kontaktdaten, wie beispielsweise Telefonnummern und E-Mail-Adressen vorzunehmen. Grundsätzlich haben die Mitglieder der WEG das Recht zu erfahren, wer außer ihnen selbst deren Mitglied ist. Das Recht der einzelnen Wohnungseigentümer:innen, dies zu erfahren, ergibt sich aus ihrer Zugehörigkeit zur WEG. Dieses Recht umfasst jedoch lediglich den vollständigen Namen und die ladungsfähige Anschrift. Demzufolge sind Verwalter:innen verpflichtet, auf Verlangen der einzelnen Eigentümer:innen die Liste der Miteigentümer:innen (inklusive Name und Anschrift) zur Verfügung zu stellen.

Weitere personenbezogene Daten der Miteigentümer:innen, wie zum Beispiel die Telefonnummer oder die E-Mail-Adresse sind jedoch nicht von diesem Anspruch umfasst. Für

die Weitergabe dieser Daten bedarf es deshalb einer Einwilligung durch die jeweiligen Eigentümer:innen oder einer anderen Legitimationsgrundlage aus Artikel 6 Absatz 1 der Datenschutzgrundverordnung.

16. Verkehr und Umwelt

16.1 Gemeldete Datenschutzverletzungen

Im Bereich Verkehr und Umwelt wurden uns im Berichtsjahr 2021 neun Datenschutzverletzungen gemeldet. In mehreren Fällen handelte es sich um von einer öffentlichen Stelle falsch versandte Unterlagen und vertauschte Poststücke. Auch wurden uns Hackerangriffe auf private Unternehmen im Bereich Verkehr gemeldet.

16.2 Beratung zahlreicher Rechtsetzungsvorhaben

Auch in den Bereichen Umwelt und Verkehr wurde der Landesbeauftragten für Datenschutz und Informationsfreiheit im Berichtsjahr im Rahmen ihrer gesetzlichen Befugnisse Gelegenheit zur Stellungnahme zu zahlreichen Gesetzesentwürfen und Novellierungsverfahren gegeben: Der Entwurf eines Gesetzes zur Anpassung von Vorschriften aus dem Bereich Häfen an die Datenschutzgrundverordnung, die Anhörung zum Entwurf eines Mobilitätsortsgesetzes für die Stadtgemeinde Bremen, das Ortsgesetz zur Änderung ortsrechtlicher Regelungen im Bereich der kommunalen Abfallentsorgung, die Änderung des Gesetzes zur Erhebung einer Wasserentnahmegebühr und der Entwurf eines Mantelgesetzes zur Novellierung des Bremischen Wald-, Naturschutz-, Jagd- und Wasserrechts waren nur einige der zahlreichen Regelungsentwürfe, die uns vorgelegt wurden (siehe hierzu Ziffer 2.7 dieses Berichts).

In diesem Zusammenhang weisen wir auf die Anforderung des § 21 Absatz 3 Nummer 2 aus dem Bremischen Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDSGVOAG) hin, wonach die Unterrichtung der Landesbeauftragten für Datenschutz und Informationsfreiheit über entsprechende Entwürfe "rechtzeitig" erfolgen muss.

16.3 Digitaler Kennzeichenscan auf Parkplätzen

Eine der zahlreichen Presseanfragen an unser Haus betraf ebenso wie mehrere Beschwerden und Anfragen Betroffener die Frage zum automatischen Kennzeichenscan auf dem Parkplatz einer Supermarktkette, die mehrfach in Bremen vertreten ist. Die Parkdauer wird dort nicht durch einen Parkschein oder eine Parkscheibe, sondern durch eine digitale Kennzeichenerfassung ermittelt.

Neben der Frage, ob es für entsprechende Verarbeitungen personenbezogener Daten im Einzelfall eine ausreichende Rechtsgrundlage gibt, ist hier ist aus datenschutzrechtlicher Sicht

entscheidend, ob die durch die Datenschutzgrundverordnung auferlegten Informationspflichten des Verantwortlichen gegenüber den parkenden Personen erfüllt werden. Hier ist es keineswegs ausreichend, nur kleine Schilder an der Parkplatzeinfahrt zu platzieren. Erforderlich ist ein auffälliger Hinweis auf den Scanvorgang auf dem Parkplatz selbst, etwa durch Piktogramme auf dem Boden und eine auffällige Gestaltung des Scangerätes. Wichtig ist es auch, unnötig lange Speicherdauern zu vermeiden. Daten derjenigen Kund:innen, die entsprechend den Bedingungen des Parkhausbetreibers die angegebene zulässige Parkdauer nicht überschritten und somit keine Strafgebühr zu erwarten haben, müssen unverzüglich wieder gelöscht werden.

16.4 Neues Projekt des Verkehrsverbundes Bremen/Niedersachsen

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) erhielt Kenntnis von einem neuen Projekt des Verkehrsverbundes Bremen/Niedersachsen (VBN): Anstatt wie bisher vor Fahrantritt das obligatorische Erwerben eines Fahrtickets zur Pflicht zu machen, wird anhand einer zuvor heruntergeladenen App die gefahrene Strecke ermittelt und daraufhin der Fahrpreis (unter Umständen auch mit Vergünstigungen wie beispielsweise bei häufigeren Fahrten per Tagesticket) abgerechnet. Im VBN sind 30 kommunale und private Verkehrsunternehmen zum öffentlichen Personennahverkehr der Städte Bremen, Bremerhaven, Delmenhorst, Oldenburg sowie der Landkreise Ammerland, Oldenburg, Wesermarsch, Cuxhaven, Nienburg, Osterholz, Rotenburg (Wümme), Verden und Diepholz zusammengeschlossen.

Der Einsatz einer App zur Berechnung des Fahrpreises anhand der gefahrenen Strecken der jeweiligen Person bedeutet unausweichlich eine intensive Preisgabe von personenbezogenen Daten, denn bereits bei Installation der App sind Name, Adresse, Geburtsdatum und Kreditkartendaten oder alternative Zahlungsmethoden anzugeben. Außerdem muss der GPS-Zugriff ermöglicht werden, denn über ein Bewegungsprofil erkennt die App, wo die Nutzer:innen gerade mit welchem Verkehrsmittel unterwegs sind. Die LfDI wird sich daher auch im folgenden Jahr noch datenschutzrechtlich intensiv mit diesem Projekt befassen.

17. Telemedien

17.1 Gemeldete Datenschutzverletzungen

Im Bereich Telemedien wurden im Berichtsjahr fünf Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet.

17.2 Koordinierte Prüfung der Webseiten von Medienunternehmen

Im letzten Jahresbericht berichteten wir unter Ziffer 18.2 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. Um einen länderübergreifenden einheitlichen Maßstab zur Prüfung im Online-Bereich zu gewährleisten, wurden im Berichtsjahr gemeinsame Prüfkriterien, vor allem zum Thema Tracking, entwickelt und verschiedene Dienste, die auf vielzähligen Webseiten eingebunden werden, gemeinsam geprüft. In Bremen laufen noch mehrere Aufsichtsverfahren. Die gemeinsam erarbeiteten Prüfkriterien werden wir in Zukunft auch für Webseiten anwenden, die nicht von Medienunternehmen betrieben werden.

17.3 Kontaktnachverfolgung via App

Im Berichtsjahr ging eine Vielzahl von Anfragen und Hinweisen von Unternehmen und Betroffenen zur Kontaktnachverfolgung via App im Pandemiekontext ein. Allgemein empfehlen wir allen verantwortlichen Stellen der Freien Hansestadt Bremen, Kontaktnachverfolgungs-Apps gewissenhaft und sorgfältig auszuwählen. Dies gilt nicht nur deshalb, weil mit dem Einsatz einer solchen App auch die datenschutzrechtliche (Mit-) Verantwortlichkeit begründet wird. Sofern Unternehmen die Kontaktnachverfolgung ausschließlich digital per App anbieten und keine papierne Kontaktdatenerfassung zur Verfügung stellen, verstoßen sie gegen die Pflicht, eine analoge Alternative anzubieten. Die meisten Kontaktnachverfolgungs-Apps bergen für Verantwortliche im Land Bremen das Problem, dass diese Adressdaten erheben, obwohl § 6 Absatz 1 der bremischen Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 (Corona-Verordnung) gemäß dem Grundsatz der Datenminimierung ausdrücklich nur die Erhebung von Namen und Telefonnummer oder E-Mail-Adresse vorsieht und gerade keine Erhebung der Adressdaten zulässt. Die auch im Land Bremen eingesetzte Luca-App zeigte bereits von Anfang an Sicherheitslücken und zahlreiche Systemschwächen, deren Schließung und Behebung dem Betreiber des Systems, trotz intensiven Austausches mit der zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht vollständig gelang. Da nach wie vor Sicherheitsdefizite der Luca-App bestehen und die App nicht allen Datenschutzstandards gerecht wird, können wir deshalb verantwortlichen Stellen in der Freien Hansestadt Bremen den Einsatz dieser Kontaktnachverfolgungs-App nicht empfehlen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) nahm in diesem Sinne zur Luca-App Stellung und veröffentlichte eine Orientierungshilfe zu Kontaktnachverfolgungssystemen im Allgemeinen. Mit den Betreibern der Gast-Bremen-App befinden wir uns noch im Austausch. Derzeit prüfen wir, ob die App die technischen und

rechtlichen Anforderungen der Datenschutzgrundverordnung erfüllt. Das Ergebnis der Prüfung steht noch aus.

Erneut weisen wir Verantwortliche im Land Bremen darauf hin, dass die Corona-Warn-App eine datensparsame und effektive Alternative für die Unterbrechung von Infektionsketten ist. Die Corona-Warn-App alarmiert direkt alle Kontaktpersonen, sobald ein positiver Testnachweis gemeldet wird. Dies macht die Kontaktnachverfolgung über die Gesundheitsämter obsolet und die Kontaktpersonen werden schneller und effektiver erreicht. Insofern begrüßen wir es, dass der bremische Verordnungsgeber § 6 Absatz 1 Satz 4 der bremischen Corona-Verordnung mit der am 23. Dezember 2021 verkündeten sechsten Verordnung zur Änderung der 29. Verordnung zum Schutz vor Neuinfektionen mit dem Coronavirus SARS-CoV-2 wie folgt gefasst hat: "Die Kontaktdatenerfassung nach Satz 1 und 2 ist nicht erforderlich, wenn die Person, deren Daten zu erfassen sind, die in der Corona-Warn-App des Robert Koch-Instituts enthaltene QR-Code-Registrierung nutzt." Damit macht auch der bremische Verordnungsgeber von der Möglichkeit Gebrauch, die die Änderung des Infektionsschutzgesetzes, die am 18. November 2021 vom Deutschen Bundestag verabschiedet wurde, den Bundesländern einräumt.

17.4 Nutzung von Facebook Fanpages durch Behörden

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wies die Bundesregierung sowie die Bundesbehörden im Jahr 2021 erneut auf seine Bedenken hinsichtlich der Nutzung von Facebook Fanpages hin und forderte sie auf, ihre Facebook Fanpages bis Ende des Jahres 2021 zu deaktivieren. In diesem Zusammenhang wies er auf die aufsichtsbehördlichen Befugnisse nach Artikel 58 Datenschutzgrundverordnung (DSGVO) hin.

Auch wir haben insbesondere die bremischen Behörden in der Vergangenheit wiederholt darauf hingewiesen, dass das Betreiben einer Facebook Fanpage nicht mit den Vorschriften der DSGVO zu vereinbaren ist, solange Facebook die Verarbeitung personenbezogener Daten nicht transparent macht. Fanpagebetreiber sind gemäß Artikel 26 DSGVO gemeinsam mit Facebook verantwortlich für die Datenverarbeitung durch Facebook. Dies hatte der Europäische Gerichtshof am 5. Juni 2018 bereits so entschieden. Gemeinsam mit den anderen deutschen Aufsichtsbehörden werden wir in dieser Angelegenheit unsere aufsichtsbehördlichen Befugnisse nutzen.

17.5 Nutzung sozialer Medien durch Polizeivollzugsbehörden

Weil wir es begrüßen, dass der Senator für Inneres nach datenschutzkonformen Wegen für die Präsenz der Polizeivollzugsbehörden in sozialen Medien sucht, beteiligen wir uns an einer

entsprechenden Arbeitsgruppe, in der unter anderem auch die Polizei Bremen und die Ortspolizeibehörde Bremerhaven selbst vertreten sind. Bislang gab es eine Telefonkonferenz Ende 2020, in der die Ziele der Arbeitsgruppe sowie Impulse aus anderen Bundesländern besprochen wurden. Eine Einladung für ein persönliches Treffen, das zunächst für das erste Quartal 2021 geplant war, hat uns bis Ende des Berichtszeitraums nicht erreicht.

17.6 Unerwünschte Anrufe durch Anlageportal

Uns erreichte eine Beschwerde wegen unerwünschter Kontaktaufnahme durch ein Anlageportal auf den British Virgin Islands. Wir versuchten, über das Binnenmarkt Informationssystem (siehe Ziffer 2.10 dieses Berichts) eine federführende Aufsichtsbehörde in der Europäischen Union ausfindig zu machen, hatten damit aber keinen Erfolg. Wir kontaktierten das Anlageportal daraufhin selbst. In der Stellungnahme des Anlageportals wurde uns glaubhaft dargestellt, dass das Unternehmen weltweit ausschließlich über das Portal tätig ist und über keine Mitarbeiter:innen verfügt, die Bürger:innen direkt kontaktieren.

17.7 Datenschutzverstöße durch Datingportale

Seit dem Inkrafttreten der Datenschutzgrundverordnung gingen bei uns immer wieder Beschwerden gegen Betreiber von Online-Datingportalen ein. In den letzten Jahren nahmen wir besonders zwei Bremer Unternehmen in den Fokus, die eine größere Anzahl solcher Portale betreiben. In regelmäßigen Abständen gehen bei uns Beschwerden vor allem darüber ein, dass die von den betreffenden Datingportalen erhobenen personenbezogenen Daten nicht beziehungsweise nicht im erforderlichen Umfang gelöscht werden.

18. Vereine

18.1 Gemeldete Datenschutzverletzungen

Im Bereich Vereine erreichte uns im Berichtsjahr eine Meldung einer Datenschutzverletzung nach Artikel 33 Datenschutzgrundverordnung. Darüber hinaus gab es diverse telefonische Anfragen, die häufig die Pandemielage zum Hintergrund hatten. Beratungsbedarf bestand unter anderem hinsichtlich des Umgangs mit der Kontaktnachverfolgung sowie hinsichtlich der Umsetzung der 3G-Regel.

18.2 Herausgabe von Mitgliederlisten an Vereinsmitglieder

Immer wieder erreichen uns Anfragen von Vereinen sowie Beschwerden von Vereinsmitgliedern hinsichtlich der Zulässigkeit der Herausgabe von Mitgliederlisten der Vereine. So baten uns Mitglieder von zwei Vereinen um Auskunft, ob ein Anspruch auf die Herausgabe der Mitgliederliste bestehe, um mit anderen Mitgliedern Kontakt aufzunehmen. In

diesem Zusammenhang weisen wir darauf hin, dass eine Herausgabe der Daten der Mitglieder nur bei berechtigtem Interesse der anfragenden Mitglieder erfolgen darf und kein überwiegendes Interesse der Vereine oder berechtigte Belange der anderen Vereinsmitglieder der Herausgabe entgegensehen dürfen. Hält ein Verein im Einzelfall die Herausgabe an ein Mitglied für zulässig, so sollte er dabei stets darauf hinweisen, dass Daten lediglich für den angegebenen Zweck verwendet werden dürfen und nach Erreichung des Zwecks zu löschen sind. Diese Information sowie weitere wichtige Hinweise zum Datenschutz im Verein finden sich auch in unserer Orientierungshilfe "Datenschutz im Verein nach der Datenschutzgrundverordnung"[7].

18.3 Herausgabe von Mitgliederdaten an Externe

Eine weitere Beratungsbitte betraf die Anfrage eines Kleingartenvereins, ob die Herausgabe der Mitgliedsdaten auch an Externe, wie zum Beispiel Versicherungsmakler zulässig sei. Dies wird als datenschutzrechtlich sehr problematisch erachtet. Wir wiesen daher darauf hin, dass Vereine die Daten ihrer Mitglieder nur im Rahmen ihres Vereinszwecks verwenden dürfen, sodass eine Übermittlung der Daten an Externe regelmäßig unzulässig ist. Sollte dennoch im Einzelfall eine Übermittlung von Mitgliedsdaten geplant sein, so ist dies ausschließlich mit Einwilligung der Betroffenen zulässig.

19. Internationales und Europa

19.1 Neue Standarddatenschutzklauseln

Nachdem der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der Europäischen Kommission für die Vereinigten Staaten von Amerika (USA) für ungültig erklärt hatte, mussten Datenexporteure die Übermittlung personenbezogener Daten in die USA aussetzen oder beenden, sofern sie keine zusätzlichen Maßnahmen ergriffen hatten, um den Schutz personenbezogener Daten zu gewährleisten (siehe hierzu 3. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 19.1). Die Europäische Kommission erließ im Juni 2021 neue Standarddatenschutzklauseln, welche seit dem 27. September 2021 zwingend für Neuverträge verwendet werden müssen. Die bestehenden Altverträge müssen bis spätestens 27. Dezember 2022 auf die neuen Standarddatenschutzklauseln umgestellt werden. Der modulare Aufbau der Klauseln ermöglicht den Einsatz bei Datenübertragungen von verantwortlichen Stellen an weitere verantwortliche Stellen, von verantwortlichen Stellen an Auftragsverarbeiter, von Auftragsverarbeitern an (Unter-) Auftragsverarbeiter und von Auftragsverarbeitern an verantwortliche Stellen (wenn sich der Auftragsverarbeiter in der Europäischen Union und die verantwortliche Stelle in einem Drittland befindet). Ein Beitritt

[7] https://www.datenschutz.bremen.de/sixcms/media.php/13/LfDI%20HB_2018_OH%20Datenschutz%20im%20Verein.pdf

weiterer Parteien zu den Standarddatenschutzklauseln wird durch die Koppelungsklausel (Klausel 7 der neuen Standarddatenschutzklauseln) ermöglicht. Die neuen, aus dem EuGH-Urteil entstandenen Pflichten werden insbesondere durch die Klauseln 14 ("Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken") und 15 ("Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten") abgedeckt. Die Landesbeauftrage für Datenschutz und Informationsfreiheit wird die Entwicklung bei Unternehmen im Land Bremen weiter beobachten und die Gestaltung, Einhaltung und Umsetzung der Standarddatenschutzklauseln verstärkt in den Blick nehmen.

19.2 Länderübergreifende Kontrolle von Unternehmen zur Schrems-II-Entscheidung

Die Landesbeauftrage für Datenschutz und Informationsfreiheit beteiligte sich im Berichtsjahr an der länderübergreifenden Kontrolle von Unternehmen zur Umsetzung des Schrems-II-Urteils des Europäischen Gerichtshofs (EuGH). Dabei wurden 37 Unternehmen mit Sitz im Land Bremen angeschrieben und aufgefordert, Fragen zum internationalen Datentransfer, konkret zu Bewerbungsportalen, zum konzerninternen Datenverkehr, zum Tracking sowie zu Mail- und Webhostern zu beantworten. Nach gegebenenfalls beantragten und genehmigten Fristverlängerungen beantworteten 29 Unternehmen die Fragen; die anderen Unternehmen wurden entsprechend angemahnt. Die Auswertung der Umfrage ergab, dass bei den Fragen zu Mail- und Webhostern noch viele Defizite insbesondere bei kleineren Unternehmen bestehen. Aufgrund der zum Teil sehr späten Eingänge der angemahnten Unternehmen ist eine präzise Auswertung der Antwortbögen zum Redaktionsschluss noch nicht abgeschlossen. Ein vorläufiges Fazit ist die Erkenntnis, dass die durch das EuGH-Urteil entstandenen Schwierigkeiten zum internationalen Datentransfer zwar in der Breite wahrgenommen, aber oftmals nicht gelöst worden sind. Die Landesbeauftragte für Datenschutz und Informationsfreiheit wird hier weiterhin beratend und auch sanktionierend auftreten.

20. 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[8] und trifft verbindliche Beschlüsse in Einzelfällen.

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

21. Die Entschließungen der Datenschutzkonferenzen im Jahr 2021

21.1 Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. März 2021)

Darf die Teilnahme an privatwirtschaftlichen Angeboten wie Restaurant- oder Konzertbesuche davon abhängig gemacht werden, dass die Besucher und Besucherinnen eine erfolgte Anti-Corona-Impfung oder eine überstandene Infektion nachweisen beziehungsweise ein negatives Testergebnis vorlegen? Neben dieser etwa im Zusammenhang mit dem auf EU-Ebene geplanten "digitalen grünen Zertifikat" vieldiskutierten Frage erreichen die Datenschutzaufsichtsbehörden fortlaufend Beratungsanfragen von Arbeitgeber, die Gesundheitsdaten wie die Körpertemperatur oder den Impfstatus von Beschäftigten erheben und verarbeiten wollen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) weist darauf hin, dass die Verarbeitung von Gesundheitsdaten zu privatwirtschaftlichen Zwecken (sei es im allgemeinen Wirtschaftsbereich oder im Beschäftigungsbereich) den Anforderungen der europäischen Datenschutzgrundverordnung (DSGVO) genügen muss. Informationen über den Impfstatus einer Person sind ebenso Gesundheitsdaten wie das Ergebnis eines Coronatests oder der Nachweis einer überstandenen Infektion. Gesundheitsdaten stehen unter dem besonders strengen Schutz der DSGVO und dürfen nur unter eng zu verstehenden Ausnahmen verarbeitet werden.

In aller Regel geboten sind konkrete gesetzliche Regelungen, die eine Verarbeitung solcher Gesundheitsdaten ausdrücklich zulassen, wie es etwa nach § 20 Infektionsschutzgesetz bei der Masernschutzimpfung im Bereich von Kindertageseinrichtungen der Fall ist. Derartige Regelungen zur Nachweispflicht einer Impfung, einer Genesung beziehungsweise eines negativen Tests, um den Zugang zu privatwirtschaftlichen Veranstaltungen oder Einrichtungen zu ermöglichen, fehlen bislang im Zusammenhang mit der Corona-Pandemie weitestgehend.

In Ermangelung einer gesetzlichen Grundlage bedarf es somit in der Regel einer Einwilligung der Restaurant- oder Konzertbesucher, Arbeitnehmer et cetera in die Erhebung und Verarbeitung ihrer Gesundheitsdaten, wobei vor allem im Beschäftigungsbereich die Freiwilligkeit der Einwilligung regelmäßig problematisch ist.

Ohne eine gesetzliche Regelung muss stets im Einzelfall geprüft werden, inwieweit die Verarbeitung von Daten über den Impfstatus oder im Rahmen einer Testung datenschutzrechtlich zulässig ist. Diese Einzelfallbetrachtung ist aufgrund der anzustellenden komplexen juristischen Abwägungen für alle Beteiligten mit großem Aufwand und rechtlichen Unsicherheiten verbunden. Ein uneinheitliches Vorgehen, etwa durch unterschiedliche Regelungen in den Kommunen, könnte zudem zu einer für die Bürgerinnen und Bürger schwer überblickbaren Praxis führen.

Um dies zu vermeiden und für die Datenerhebung und -verarbeitung im privatwirtschaftlichen Bereich Rechtsklarheit, Rechtssicherheit und eine einheitliche Lösung zu erreichen, bedarf es nach Ansicht der DSK einer auf die konkrete pandemische Lage bezogenen, zeitlich befristeten gesetzlichen Regelung. Hierin ist klar und transparent zu regeln, wer, von wem und unter welchen Voraussetzungen Impfdaten, Testergebnisse, Nachweise zu einer überstandenen Infektion und andere Gesundheitsdaten im privatwirtschaftlichen Kontext nutzen darf. Dabei muss das Gesetz den strengen Vorgaben des Artikels 9 Absatz 2 DSGVO genügen.

Die DSK fordert den Gesetzgeber auf, kurzfristig ein entsprechendes Gesetzgebungsverfahren in die Wege zu leiten.

21.2 Chancen der Corona-Warn-App 2.0 nutzen

(Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2021)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) erinnert angesichts der bereits seit mehr als einem Jahr andauernden Pandemie und der damit auch im Bereich des Datenschutzes einhergehenden Grundrechtseingriffe an das grundlegende rechtsstaatliche Erfordernis, diese Eingriffe fortlaufend kritisch zu bewerten und zu evaluieren. Die DSK bittet im Zuge einer solchen Evaluation und Anpassung infektionsschutzrechtlicher Instrumente durch Bund und Länder die mit der Version 2.0 der Corona-Warn-App (CWA) eröffneten datensparsameren Möglichkeiten der pseudonymisierten Clustererkennung und Kontaktbenachrichtigung eingehend und zeitnah zu prüfen.

Die DSK empfiehlt den Ländern, die Nutzung der CWA jedenfalls als ergänzende Möglichkeit zur Benachrichtigung potenziell infizierter Personen und zur Clustererkennung in ihren Konzepten zur Pandemiebekämpfung zu berücksichtigen.

Seit dem Update auf die Version 2.0 verfügt die CWA über eine entsprechende Funktion, die genutzt werden kann, um sich an Orten oder Veranstaltungen, wo viele Menschen zusammenkommen, zu registrieren. Auch wenn hierbei – anders als bei anderen Apps – keine

personenbezogenen Daten erhoben und später an ein Gesundheitsamt übermittelt werden können, kann die pseudonymisierte Clustererkennung der CWA einen erheblichen Beitrag zur Unterbrechung von Infektionsketten leisten.

Durch die unmittelbare Vernetzung der CWA-Nutzenden werden Personen, die einem potenziellen Infektionsrisiko ausgesetzt waren, unmittelbar und somit schneller als über die Gesundheitsämter informiert. Zudem ist aufgrund der hohen Akzeptanz der CWA mit mittlerweile über 27 Millionen Downloads die Wahrscheinlichkeit hoch, dass Personen auf diese Möglichkeit der aus datenschutzrechtlicher Sicht zu bevorzugenden pseudonymen digitalen Registrierung zurückgreifen.

Die Förderung der Nutzung der CWA zur Clustererkennung könnte dazu führen, dass die App von noch mehr Personen genutzt werden würde. Dies wiederum würde auch die Chance der Erkennung und Warnung vor Risikobegegnungen außerhalb der Nutzung der Clustererkennung weiter erhöhen und damit aktiv zur Pandemiebekämpfung beitragen.