3. 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 2020. Redaktionsschluss war der 31. Dezember 2020.

Dr. Imke Sommer

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen

Inhaltsverzeichnis

1. Die Vermessung der Pandemie – oder: Verhältnismäßigkeit ist kein Gefühl

Verhältnismäßigkeitsprüfungen gehören zum täglichen Brot der Landesbeauftragten für Datenschutz. Auch im vergangenen Jahr haben sie unsere Arbeit, über die ich hier berichte, geprägt. Im Pandemiejahr war jedoch eines anders: Verhältnismäßigkeit wurde Gegenstand öffentlicher Debatten. Dies geschah auch, aber nicht nur im datenschutzrechtlichen Kontext. Der Begriff Verhältnismäßigkeit war geradezu omnipräsent. In der Diskussion über den richtigen Umgang mit der COVID-19-Pandemie war und ist allenthalben zu vernehmen: "Maßnahme X ist unverhältnismäßig; Maßnahme Y erst Recht. Maßnahme Z kann unter keinen Umständen verhältnismäßig sein."

Der Begriff der Verhältnismäßigkeit entwickelte dabei ein Eigenleben. Es entstand zuweilen der Eindruck, dass er keinen Sachverhalt feststellt, sondern eine subjektive und gefühlsabhängige Situation beschreibt: Die einen halten eine Maßnahme für verhältnismäßig, die anderen nicht. Aber so funktioniert das Vermessen nicht. Ein "gefühlter" Meter ist eben kein Meter, sondern bezeichnet eine Länge von möglicherweise 95 cm oder 127 cm. Die "gefühlte" Temperatur ist eben nicht die exakt gemessene, sondern wird individuell unterschiedlich wahrgenommen: Die Stockholmerin geht bei 0 Grad in der Mittagspause schnell mal im T-Shirt ins benachbarte Geschäft, während der Römer bei derselben Temperatur eher die dickste Winterjacke wählt. Auch die Verhältnismäßigkeit, also das Maß des Verhältnisses, kann nicht "gefühlt" werden, sondern muss mit einer festgelegten Methode ermittelt, also "gemessen" werden.

1.1 Zweck-Mittel-Relation – Vom Nageln des Puddings

Die Verselbständigung des Begriffs lässt leider die eigentliche Bedeutung aus dem Blickfeld geraten, obwohl der Begriff so schön sprechend ist: Bei der Verhältnismäßigkeit geht es um ein Verhältnis, und damit um das "In-Beziehung-Setzen" zweier Faktoren. Genauer gesagt geht es um die Beziehung zwischen dem angestrebten Ziel, dem "Zweck", und dem "Mittel", mit dessen Hilfe der Zweck erreicht werden soll. Es geht um die **Zweck-Mittel-Relation**. Beantwortet werden Fragen wie die der Beziehung zwischen dem Befestigen von Pudding an der Wand und dem Nageln und die der Beziehung zwischen dem Türenöffnen und dem Holzhammer.

Die Verhältnismäßigkeitsprüfung folgt der Logik jedes "Ins-Verhältnis-Setzens" und "vermisst" nach feststehenden Kriterien und Methoden, wie sich das gewählte Mittel zur Erreichung des angestrebten Ziels verhält. Sie geschieht in vier Phasen. Der erste Schritt ist die **Vermessung der Legalität des Ziels**, der zweite die **Vermessung der Eignung** der Maßnahme zur Erreichung des Ziels, der dritte die **Vermessung der Erforderlichkeit** des Mittels zur

Erreichung des Ziels, also die Feststellung der Nichtverfügbarkeit anderer Maßnahmen, die bei geringeren Nebenfolgen ebenfalls geeignet sind, das Ziel zu erreichen. **Die ersten drei Prüfungsschritte** müssen damit unter **purer Anwendung der Logik** durchlaufen werden. Die Unverhältnismäßigkeit der geprüften Maßnahme ist schon dann belegt, wenn im ersten (Legitimität des Ziels), zweiten (Eignung des Mittels) oder dritten (Erforderlichkeit des Mittels) Prüfungsschritt das Ergebnis negativ ist. Das Nageln ist nicht geeignet, den Pudding an der Wand zu befestigen und der Holzhammer ist nicht erforderlich zur Öffnung der Tür, weil der passende Schlüssel keine zerstörerische Kraft entfaltet. Weil die Schritte logisch aufeinander aufbauen, kann die Prüfung sofort abgebrochen werden, wenn der Zweck nicht legal, oder das Mittel nicht geeignet oder nicht erforderlich ist. Die Vermessung hat dann die Unverhältnismäßigkeit bewiesen.

1.2 Es ist kein Abwiegen, wenn der Apfel immer gewinnt

Der vierte Prüfungsschritt befasst sich mit der Frage, ob ein **verbotenes Übermaß** besteht, ob das Mittel also zwar erforderlich, aber **nicht angemessen** ist, weil es ein verfassungsmäßiges, aber weniger bedeutsames Ziel herbeiführt und dabei sehr einschneidende Wirkungen hat, die "außer Verhältnis" zum Erfolg der Erreichung des konkreten Ziels stehen. Erst auf dieser vierten Prüfungsebene kommen Argumente in Betracht, die etwas mit der Abwägung zwischen unterschiedlichen Prinzipien, wie etwa unterschiedlichen Grundrechten zu tun haben können. Abwägungen, bei denen es durchaus möglich ist, dass beispielsweise die Relevanz unterschiedlicher Grundrechte aus unterschiedlichen Perspektiven unterschiedlich beurteilt wird, kommen also erst ins Spiel, wenn Legalität des Ziels und Eignung und Erforderlichkeit des Mittels zur Erreichung des Ziels mit Hilfe von Methoden der Logik festgestellt wurden.

Auf der vierten Prüfungsstufe muss eine Entscheidung getroffen werden, die den kollidierenden Rechtsgütern jeweils zu optimaler Wirksamkeit verhilft, also "praktische Konkordanz" zwischen den unterschiedlichen Zielen, etwa den verschiedenen Grundrechtspositionen herstellt. In einem demokratischen Rechtsstaat sind dabei Argumentationen ausgeschlossen, die darauf abzielen, ein bestimmtes Grundrecht sei komplett verzichtbar, während ein anderes ausnahmslos den anderen vorgehe. Es kann bezweifelt werden, dass Frank Plasberg dies wirklich verstanden hatte, als in seiner Sendung "hart aber fair" am 14. Dezember 2020 die "Ikone Datenschutz" für verzichtbar hielt ("Sch… [*hier nicht ausgeschrieben*] auf Datenschutz") und deutlich machte, für die Religionsfreiheit gelte ein besonderer Grundrechtsschutz, der in jedem Fall vorrangig sei. Im Übrigen hatten die Zuschauerinnen und Zuschauer bis dahin den Eindruck gewinnen können, dass Gegenstand der Diskussion nicht die Abwägung zwischen unterschiedlichen Grundrechtspositionen, sondern die Erforderlichkeit des harten Lockdowns war, also darüber diskutiert wurde, ob es mildere, ebenso geeignete Maßnahmen gibt, die Infektionszahlen so

zurückzuführen, dass in den Krankenhäusern keine Triagesituationen entstehen. Auch bei der Abwägung hilft also der sprechende Wortsinn: Für das Abwägen, das Abwiegen benötige ich definitionsgemäß zwei Dinge. Wenn ich die Birnen komplett von der Balkenwaage nehme, kann ich die Äpfel nicht mehr gegen sie abwiegen. Dann ist es keine Kunst für die Äpfel, zu gewinnen.

1.3 Kulinarische Pandemiebekämpfung

Es überrascht nicht, dass unsere aufsichtsbehördliche Prüfung der Verhältnismäßigkeit der Verarbeitung personenbezogener Daten im Berichtsjahr von Fragestellungen im Zusammenhang mit der Pandemiebekämpfung geprägt war. Dies soll hier am Beispiel der Maßnahme der Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte zum Ziel des Lebens- und Gesundheitsschutzes nachvollzogen werden, die uns in vielerlei Hinsicht beschäftigte (siehe Ziffer 12.4 dieses Berichts). Was den ersten Prüfungsschritt anbelangt, steht es im demokratischen Rechtsstaat außer Frage, dass der Zweck, der mit dem Einsatz des Mittels erreicht werden soll, ein gesetz- und verfassungsmäßiger sein muss. Artikel 2 Absatz 2 Grundgesetz verbürgt das Grundrecht auf Leben und körperliche Unversehrtheit. Maßnahmen, die der Rettung von Menschenleben und der Verhinderung von Krankheiten, im Jahr 2020 beispielsweise der Bekämpfung des Coronavirus SARS-CoV-2 dienen, verfolgen also ein **verfassungsmäßiges Ziel**. Die erste Prüfungsstufe ist damit durchlaufen.

Im zweiten Schritt muss die Frage beantwortet werden, ob die Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte überhaupt **geeignet** ist, **das verfassungsmäßige Ziel zu erreichen**, also geeignet ist, die Gesundheit und das Leben zu schützen. Die Gesundheit der Menschen und ihr Leben werden geschützt, wenn sich möglichst wenige Menschen infizieren. Das Coronavirus SARS-CoV-2 verbreitet sich durch Aerosole, die infizierte Menschen ausatmen. Deshalb müssen die Gesundheitsämter, also diejenigen Stellen, die gemeinsam mit den infizierten Menschen dazu beitragen können, dass diese keine weiteren Menschen anstecken, darüber informiert werden, dass eine bestimmte Person beispielsweise bei Gelegenheit eines Restaurantbesuchs möglicherweise Luft eingeatmet hat, die von einem Menschen ausgeatmet wurde, der ansteckend war. In diesem Fall kann überprüft werden, ob tatsächlich eine Ansteckung erfolgte, und es kann gelingen, sicher zu stellen, dass die nun selbst infizierte Person nicht noch weitere Menschen ansteckt. Die Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte ist also geeignet, die Gesundheit und das Leben derjenigen zu schützen, die mit einem unerkannt infizierten Menschen in Kontakt gekommen sind. Damit ist sie gleichzeitig geeignet, die Infektionskette zu unterbrechen und so die Gesundheit und das Leben einer Vielzahl von Menschen zu schützen.

Gegenstand des nächsten Prüfungsschrittes, der **Erforderlichkeitsprüfung,** ist die Frage, ob es möglicherweise neben der Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte

andere Mittel gibt, die das verfolgte Ziel mit weniger einschneiden Maßnahmen erreichen können. Hier ist Phantasie gefragt. Wie könnten die Gesundheitsämter auf ebenso geeignete Weise wie mit Hilfe der von Gastwirtinnen und Gastwirten erhobenen und weitergegebenen Kontaktdaten davon erfahren, welche Personen, die sich mittelweile als infiziert herausgestellt haben, sich möglicherweise im Restaurant angesteckt haben könnten? Und welche dieser anderen Maßnahmen ist milder als die Maßnahme der Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte? Eine mildere Maßnahme als die digitale oder schriftliche Erfassung von personenbezogenen Daten wäre es, sich auf das Gedächtnis der Gastwirtinnen und Gastwirte zu verlassen. Weil es aber nicht unwahrscheinlich ist, dass Gastwirtinnen und Gastwirte sich nicht an alle ihre Gäste erinnern können, ist diese Maßnahme zwar milder, aber nicht ebenso geeignet wie die Kontaktdatenverarbeitung. Eine in ähnlicher Weise wie die Kontaktdatenverarbeitung durch die Gastwirtinnen und Gastwirte geeignete Maßnahme wäre die Videoüberwachung der Gasträume kombiniert mit einer Gesichtserkennungssoftware. Dass diese Maßnahme deutlich stärker in die Grundrechte der Gäste einschneidet, also nicht "milder" als die Kontaktdatenverarbeitung ist, liegt auf der Hand.

Wenn es keine anderen, ebenso geeigneten, aber milderen Mittel zur Erreichung des Ziels gibt, zu wissen, wer anlässlich eines Restaurantbesuchs von einer infizierten Person angesteckt worden sein könnte, heißt dies aber noch nicht, dass jede Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte erforderlich ist. Deshalb muss die **Art und Weise der Kontaktdatenverarbeitung unter Erforderlichkeitskriterien** genauer unter die Lupe genommen werden. Es muss beispielsweise geprüft werden, welche personenbezogenen Daten die Gesundheitsämter unbedingt kennen müssen, um das Ziel zu erreichen. Nur sie sind erforderlich und damit verhältnismäßig. Auch muss geprüft werden, wie lange diese Daten gespeichert werden müssen, um das Ziel zu erreichen.

Was die Einschränkung der Verarbeitung der Kontaktdaten nach Erforderlichkeitsgesichtspunkten anbelangt, hat sich der bremische Verordnungsgeber durch die Präzisierung des Verordnungstextes gesteigert. So hat er mit der Definition des Begriffs der Kontaktdaten verdeutlicht, dass lediglich Name und die Telefonnummer oder die E-Mail-Adresse verarbeitet werden dürfen. Hiermit wurde klargestellt, dass nur die für eine schnelle Kontaktverfolgung durch die Gesundheitsämter erforderlichen Daten erhoben und gespeichert werden dürfen. Jede darüber hinaus gehende Verarbeitung ist nicht erforderlich und daher unverhältnismäßig und rechtswidrig. In § 8 der zu Redaktionsschluss geltenden Dreiundzwanzigsten Coronaverordnung, die in stärkerem Maße als die frühen Verordnungen an die Willensbildung in der Bremischen Bürgerschaft gekoppelt ist, ist der Rahmen der Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte im Vergleich zu den Formulierungen in den frühen Coronaverordnungen sehr genau beschrieben. Es wird bestimmt, dass nur die Kontaktdaten je einer Vertreterin oder eines Vertreters der anwesenden Haushalte erhoben werden dürfen, dass bei dienstlichen Tätigkeiten die dienstlichen

Kontaktdaten genügen, dass die Gastwirtinnen und Gastwirte geeignete Vorkehrungen treffen müssen, damit Dritte keine Kenntnis von den erhobenen Daten erlangen können, dass die Kontaktdaten sicher aufzubewahren, auf begründeten Antrag dem zuständigen Gesundheitsamt zwecks Identifizierung und Benachrichtigung ansteckungsverdächtiger Personen mit Coronavirus SARS-CoV-2 herausgegeben werden müssen, worüber dieses die betroffenen Personen unterrichten muss, und dass die Kontaktdaten nach vier Wochen zu löschen sind.

Mit dieser Festlegung in der Coronaverordnung ist gleichzeitig festgelegt, dass jede über diesen Rahmen hinausgehende Verarbeitung nicht erforderlich und damit nicht verhältnismäßig und rechtswidrig ist (siehe hierzu die Pressemitteilung vom 2. Juni 2020 "Offene Listen von Gästedaten in Gaststätten"[1]). Deshalb waren datenschutzrechtliche Beschwerden darüber, dass offene Gästelisten von Tisch zu Tisch gingen, Gästelisten für nachfolgende Gäste einsehbar auf dem Tisch liegen blieben und nicht erforderliche Daten erhoben wurden, ebenso begründet wie die Beschwerde darüber, dass ein Kellner eine eingetragene Mobiltelefonnummer zur Kontaktaufnahme genutzt hatte. Im letztgenannten Fall war es richtig, dass die Beschwerdeführerin parallel Strafanzeige bei der Polizei erstattet hatte.

1.4 What´s next?

Das Beispiel der Verhältnismäßigkeitsprüfung der Kontaktdatenerhebung durch Gastwirtinnen und Gastwirte zum Schutz des Lebens und der Gesundheit derjenigen, die von unerkannt Infizierten angesteckt worden sein könnten, und damit der gesamten Bevölkerung zeigt, dass auf den drei "logischen" Prüfungsstufen Legalität des Ziels und Eignung und Erforderlichkeit des Mittels zur Erreichung des Ziels der überwiegende Großteil der Argumente abgebildet werden kann, die im Zusammenhang mit der Vermessung der Verhältnismäßigkeit der Pandemiebekämpfungsmaßnahmen diskutiert werden. Es wird ebenfalls deutlich, dass neue wissenschaftliche Erkenntnisse dazu führen, dass sich die Beurteilung der Verhältnismäßigkeit der ergriffenen Maßnahmen verändert. Wenn wissenschaftlich erwiesen wäre, dass eine Infektion doch nur durch direkten Kontakt mit den Schleimhäuten Infizierter möglich wäre oder die Aerosole erst nach zehn Stunden gemeinsamen Daueraufenthalts in einem Raum übertragen würden, wäre die gegenwärtig normierte Kontaktdatenerhebung zum Schutz der Gesundheit und des Lebens nicht geeignet, jedenfalls aber nicht erforderlich und damit unverhältnismäßig.

Auf der vierten Prüfungsstufe der Verhältnismäßigkeit der Kontaktdatenverarbeitung durch Gastwirtinnen und Gastwirte hätte eine Diskussion geführt werden können, die die Kontaktdatenverarbeitung zur Erreichung des Schutzes von Leben und Gesundheit auf einen

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

Verstoß gegen das Übermaßverbot geprüft hätte. Um zu dem Ergebnis zu kommen, dass die Kontaktdatenverarbeitung wegen Verstoßes gegen das Übermaßverbot unverhältnismäßig war, hätte argumentiert werden müssen, dass das Ziel des Gesundheits- und Lebensschutzes ein zwar verfassungsmäßiges, aber weniger bedeutsames Ziel ist, dessen Erreichung "außer Verhältnis" zu den Wirkungen der Kontaktdatenerhebung durch Gastwirtinnen und Gastwirte gestanden hätte, die nach dieser Auffassung als sehr einschneidend hätten angesehen werden müssen. Auch aus datenschutzrechtlicher Sicht bestand hierzu aufgrund der Eindeutigkeit der grundgesetzlichen Wertung kein Anlass. Nach dem Grundgesetz muss der Schutz jedes einzelnen Lebens und der Gesundheit jedes einzelnen Menschen ungleich höher gewichtet werden, als der Grad des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung, den eine rechtmäßige, in den Grenzen der Coronaverordnung erfolgende Kontaktdatennachverfolgung verursacht.

Eine solche grundrechtliche Beurteilung bezieht sich auf eine bestimmte Situation und kann nicht statisch sein. Ob das Grundrecht auf Schutz der informationellen Selbstbestimmung und alle anderen Verfassungspositionen ausreichend beachtet werden, muss permanent überprüft und auf die neuesten Entwicklungen hin beurteilt werden. Diese Einsicht ist auch Gegenstand der Entschließung "Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. April 2020 (siehe Ziffer 21.1 dieses Berichts). Ausgehend von der Erkenntnis, dass die zur Pandemiebekämpfung getroffenen Maßnahmen den Wert der Freiheitsrechte und damit auch den Wert des Grundrechts auf informationelle Selbstbestimmung erlebbar machen, heißt es dort: "Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden."

Diese Grundsätze müssen auch bei allen noch folgenden Diskussionen im Pandemiekontext beachtet werden. Schon jetzt sei dringlich daran erinnert, dass die Tatsache, ob eine Person geimpft ist oder nicht, ein personenbezogenes Datum ist, das als Gesundheitsdatum in besonderer Weise geschützt ist: Nach Artikel 9 Datenschutzgrundverordnung (DSGVO) unterliegen Gesundheitsdaten einem grundsätzlichen Verarbeitungsverbot und dürfen nur ausnahmsweise und unter sehr engen Voraussetzungen verarbeitet werden. Damit verbannt die DSGVO Visionen vom Impfpass als Eintrittskarte in die Gesellschaft ins Reich der Albträume.

Dr. Imke Sommer

2. Zahlen und Fakten

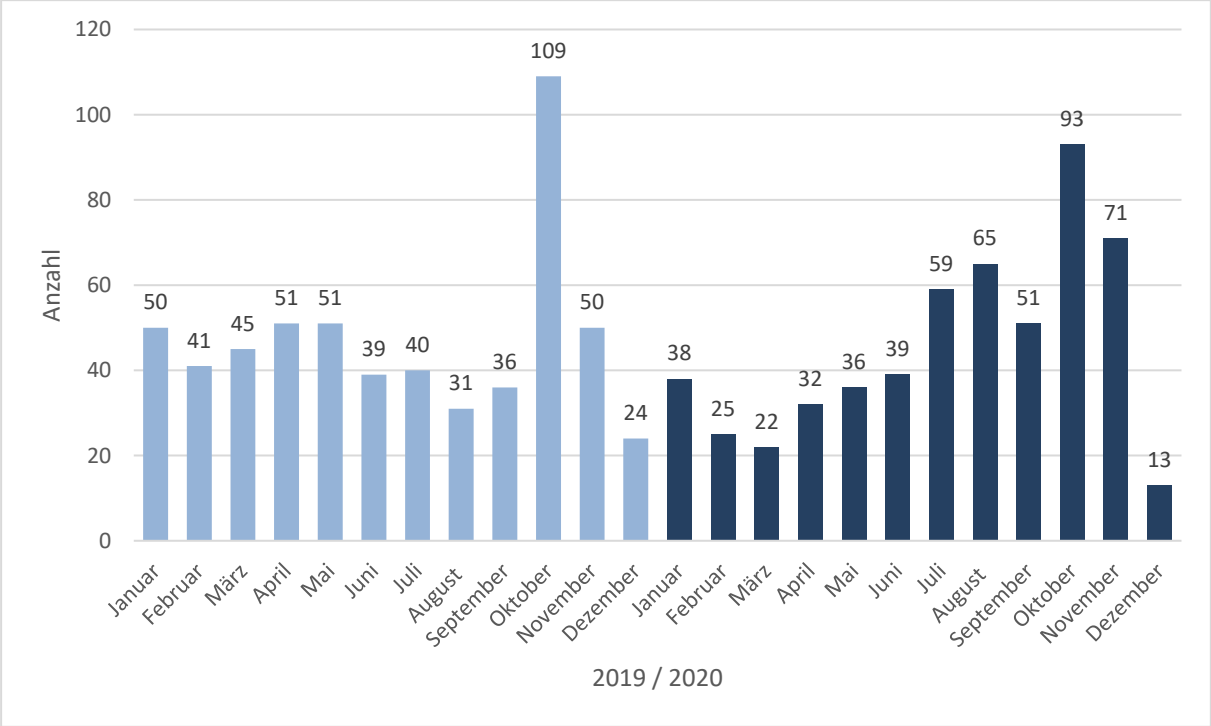
Die Datenschutzgrundverordnung macht es den Aufsichtsbehörden in Artikel 59 zur Pflicht, jährlich über ihre Tätigkeit zu berichten. Um die Transparenz und Vergleichbarkeit innerhalb der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) und für die Öffentlichkeit zu erhöhen, hat die DSK beschlossen, künftig 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 2020 an die Landesbeauftragte für Datenschutz und Informationsfreiheit herangetragen wurden

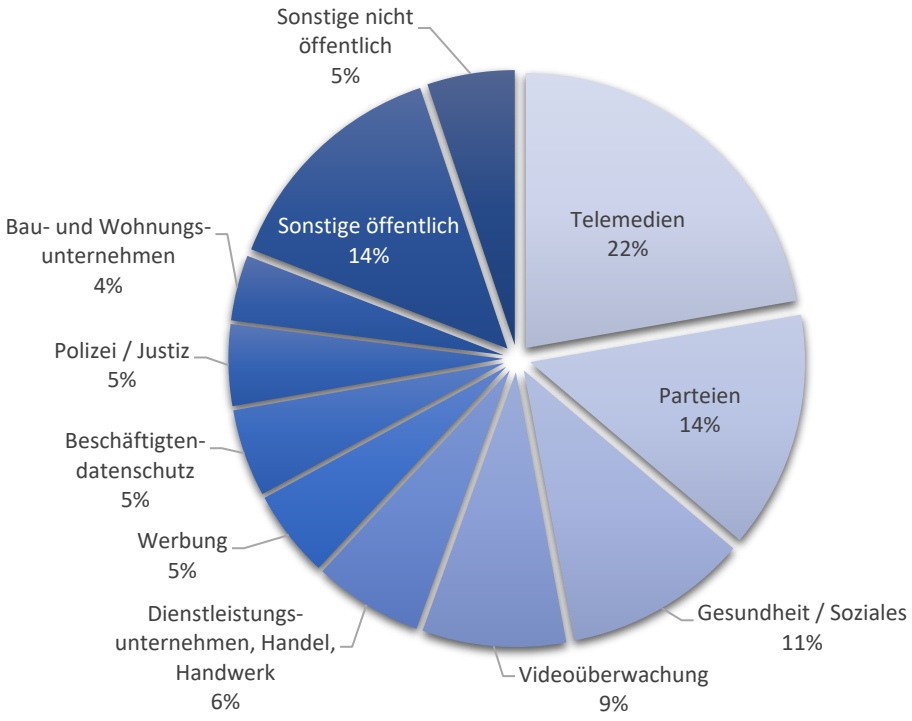
Monat	Beschwerden	Beratungs-anfragen	Meldungen Datenschutz-verletzungen	Meldungen Datenschutz-beauftragte
Januar	38	47	8	37
Februar	25	46	5	26
März	22	43	8	22
April	32	41	4	25
Mai	36	60	9	35
Juni	39	45	5	17
Juli	59	47	16	15
August	65	29	11	20
September	51	42	7	45
Oktober	93	39	12	27
November	71	27	3	33
Dezember	13	28	6	14
Gesamt	**544**	**494**	**94**	**316**

Nähere Angaben hierzu finden sich in den nachfolgenden Ziffern.

2.2 Beschwerden



In diesem Diagramm sind die monatlichen Beschwerdezahlen seit dem Jahr 2019 dargestellt. Die Beschwerden bewegten sich trotz der Besonderheiten des "Pandemiejahres" 2020 mit durchschnittlich 47,3 im Jahr 2019 und 45,3 im Jahr 2020 auf etwa gleichem Niveau.



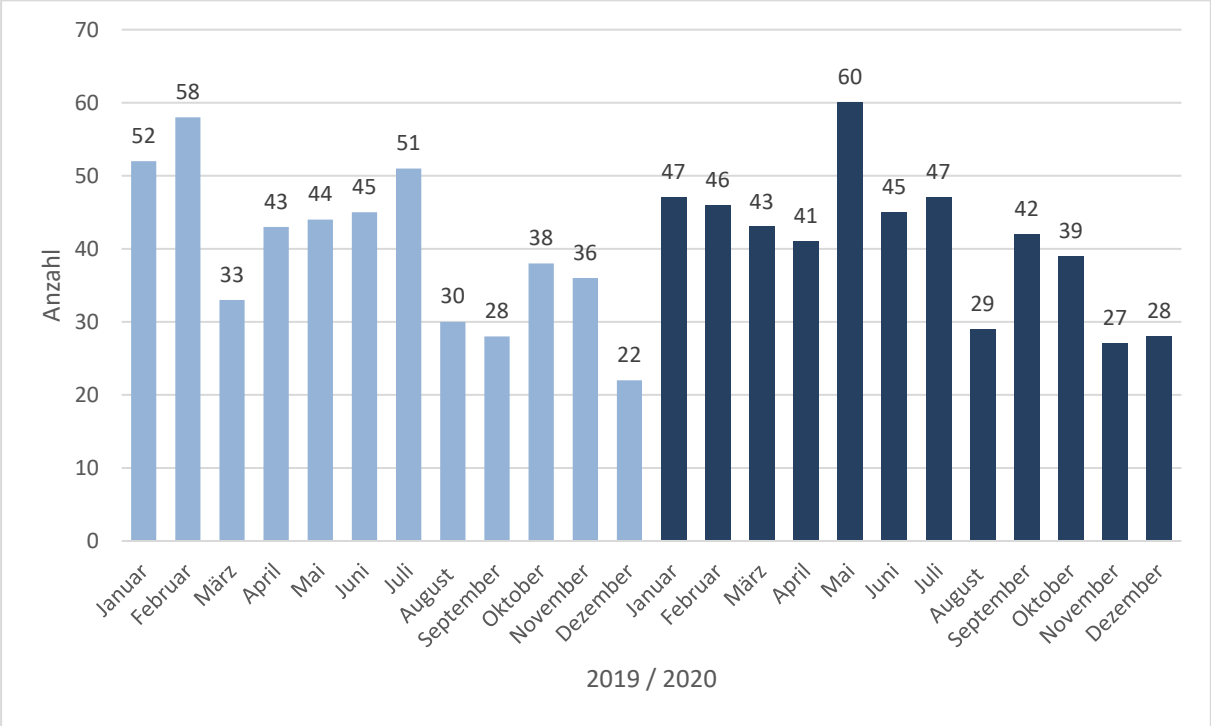
Das Diagramm zeigt die bei der Landesbeauftragten für Datenschutz und Informationsfreiheit eingegangenen Beschwerden im gesamten Jahr 2020 nach Themengebieten aufgeschlüsselt.

Themengebiet	AW	RW
Dienstleistungsunternehmen, Handel, Handwerk	35	6 %
Beschäftigtendatenschutz	28	5 %
Werbung	28	5 %
Telemedien	121	22 %
Gesundheit und Soziales	59	11 %
Parteien	76	14 %

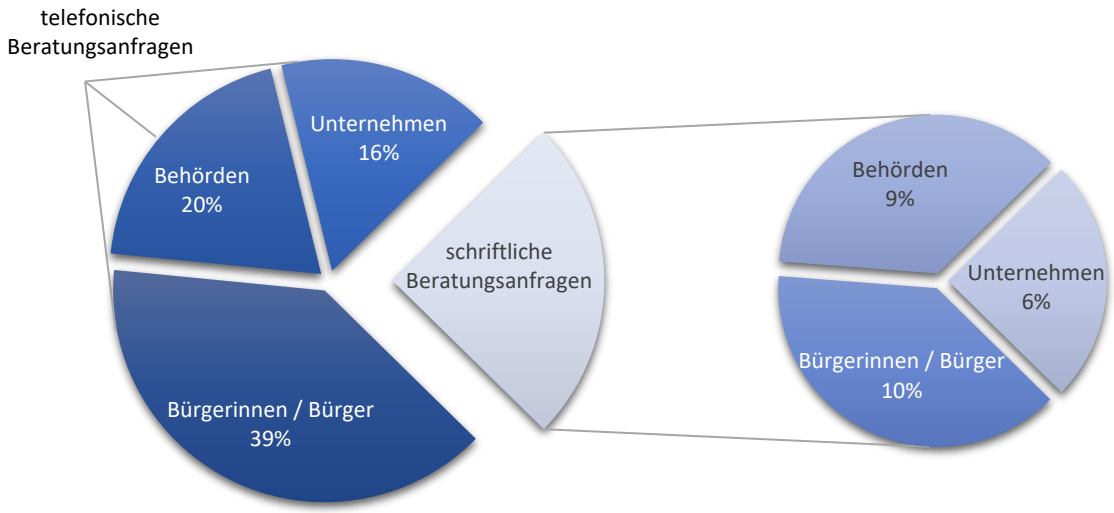
Themengebiet	AW	RW
Bau- und Wohnungsunternehmen	21	4 %
Sonstiges (nicht öffentlich)	28	5 %
Sonstiges (öffentlich)	76	14 %
Polizei / Justiz	26	5 %
Videoüberwachung	46	9 %

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

2.3 Beratungen

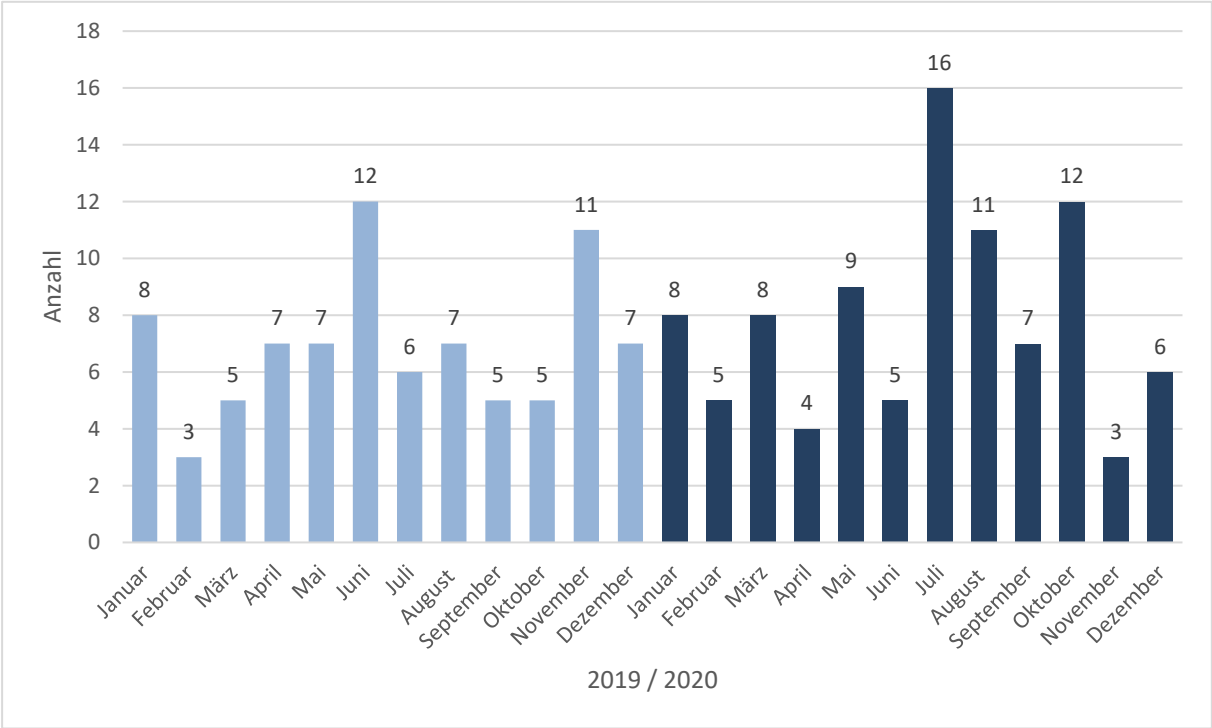


Diese Grafik gibt eine Übersicht über die Anzahl von schriftlichen und telefonischen Beratungen von Verantwortlichen und betroffenen Personen.

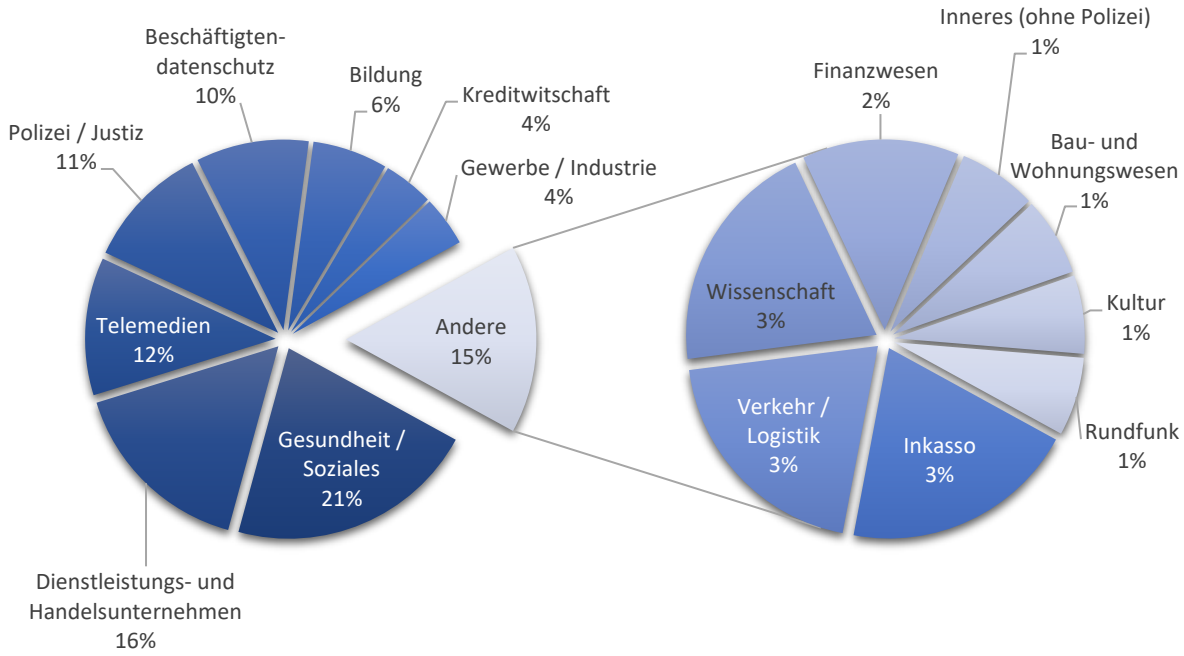


Dieses Tortendiagramm stellt die telefonischen und schriftlichen Beratungen im Jahr 2020 dar. Differenziert wird dabei zwischen telefonischen und schriftlichen Beratungsanfragen. Daneben wird danach unterschieden, wer Beratungsanfragen stellt. Dies sind zum einen die Verantwortlichen (Behörden und Unternehmen) und andererseits die von der Verarbeitung personenbezogener Daten betroffenen Grundrechtsträgerinnen und Grundrechtsträger.

2.4 Meldungen von Datenschutzverletzungen



Diese Grafik vermittelt eine Übersicht über die Anzahl schriftlicher Meldungen über Datenschutzverletzungen durch Verantwortliche oder Auftragsverarbeiter nach Artikel 33 Datenschutzgrundverordnung.



Diese Darstellung schlüsselt die gemeldeten Datenschutzverletzungen für das Jahr 2020 nach Themengebieten auf.

2.5 Abhilfemaßnahmen

Warnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 a DSGVO: Eine

Verwarnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 b DSGVO: Drei

Anweisungen und Anordnungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 c-g DSGVO: Eine

Geldbußen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 i DSGVO: Eine

Widerruf von Zertifizierungen

Abhilfemaßnahmen nach Artikel 58 Absatz 2 h DSGVO: Keine

2.6 Europäische Verfahren

Anzahl der Verfahren mit Betroffenheit nach Artikel 56 DSGVO

Fünf Fälle.

Anzahl der Verfahren mit Federführung nach Artikel 56 DSGVO

Kein Fall.

Anzahl der Verfahren gemäß Kapitel VII nach den Artikeln 60ff. DSGVO

Ein Fall nach Artikel 61 DSGVO.

2.7 Förmliche Begleitung bei Rechtsetzungsvorhaben

Folgende Beratungen wurden im Berichtsjahr 2020 durchgeführt:

Gesundheit

- Bremisches Krankenhausgesetz (BremKrhG)
- Gesetz über den Öffentlichen Gesundheitsdienst im Lande Bremen (Gesundheitsdienstgesetz - ÖGDG)
- Bremische Verordnung über die Erteilung einer Erlaubnis für den Betrieb eines Drogenkonsumraums

Inneres

- Änderung des Bremischen Polizeigesetzes (zur Umsetzung der JI-Richtlinie)

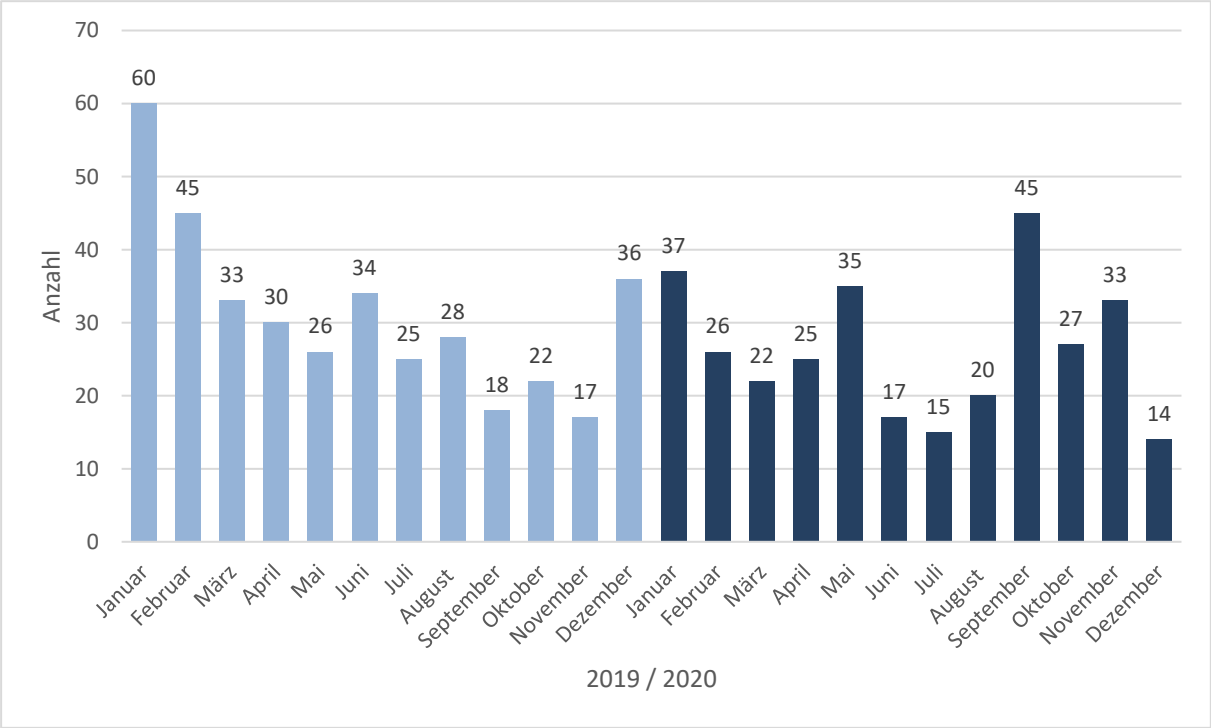
Justiz

- Bremisches Justizvollzugsdatenschutzgesetz (BremJVollzDSG)
- Gesetz zur Ausführung der EU-Datenschutz-Richtlinie im Bereich der Strafjustiz und zur Änderung des Bremischen Sicherheitsüberprüfungsgesetzes

Wissenschaft

- Bremisches Hochschulgesetz (BremHG)

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 Akkreditierung von Zertifizierungsverfahren und Zertifizierungsstellen

Nach der Datenschutzgrundverordnung hat die Landesbeauftrage für Datenschutz auch die Aufgabe, die Einführung von datenschutzspezifischen Zertifizierungsverfahren und Datenschutzsiegeln zu fördern. In diesem Zusammenhang prüfen wir derzeit als eine der ersten Datenschutzaufsichtsbehörden in Deutschland ein zur Genehmigung vorgelegtes Konformitätsbewertungsprogramm. Gleichzeitig arbeiten wir im Rahmen der Zusammenarbeit mit den anderen deutschen Aufsichtsbehörden an der Entwicklung allgemeiner Prüfkriterien für datenschutzspezifische Zertifizierungen mit.

2.10 Europäisches Binnenmarkt-Informationssystem

Das europäische Binnenmarkt-Informationssystem (Internal Market Information System, IMI) konnte im Berichtsjahr nur sehr selten genutzt werden. Nach wie vor übersteigt die Anzahl der zu bearbeitenden E-Mails (alleine mehr als 2.500 sogenannte Benachrichtigungen des IMI-Systems im Jahr 2020) die Kapazitäten der Landesbeauftragten für Datenschutz und

Informationsfreiheit. Auch die Aufsichtsbehörden anderer europäischer Mitgliedstaaten konnten ressourcenbedingt in nur vier Fällen über das System angefragt werden. In einem zwischenzeitlich erledigten Fall, der durch die Beschwerde einer Bürgerin über die Veröffentlichung personenbezogener Daten auf einer aus Frankreich betriebenen Webseite aufgenommen wurde, übernahm die französische Aufsichtsbehörde (CNIL) die Federführung. In einem anderen Fall, dem eine Beschwerde über die Veröffentlichung personenbezogener Daten in "Telefonbuchverzeichnissen" zugrunde liegt, besteht noch Kontakt zu der polnischen Aufsichtsbehörde. Die Aufsichtsbehörden anderer Bundesländer befassen sich zudem zeitgleich mit vermeintlichen "Telefonbuchverzeichnissen", die im europäischen Ausland betrieben werden. In den übrigen beiden Fällen – einmal ein Werbeanruf aus dem Ausland, einmal eine Veröffentlichung von Videomaterial auf einer niederländischen Erotikplattform – ist die Zuständigkeit hingegen sowohl auf europäischer als auf nationaler Ebene noch ungeklärt.

3. Bremische Bürgerschaft – Ergebnisse der Beratungen des 2. Jahresberichts nach Inkrafttreten der DSGVO

Bericht Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit.

2. Jahresbericht der Landesbeauftragten für Datenschutz nach der Europäischen Datenschutzgrundverordnung und Stellungnahme des Senats.

Bericht:

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 13. Mai 2020 den 2. Jahresbericht der Landesbeauftragten für Datenschutz vom 24. März 2020 (Drucksache 20/330) und in ihrer Sitzung am 16. September 2020 die dazu erfolgte Stellungnahme des Senats vom 8. September 2020 (Drucksache 20/597) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 2. Jahresberichts Beratungsbedarf fest:

Ziffer 5 Übergreifende IT-Verfahren

Ziffer 6 Inneres

Ziffer 7 Justiz

Ziffer 8 Gesundheit

Ziffer 9 Soziales

Ziffer 10 Bildung

Ziffer 11 Beschäftigtendatenschutz

Ziffer 13 Wirtschaft und Gewerbe

In seiner Sitzung am 20. Januar 2021 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und Informationsfreiheit sowie mit den Vertreterinnen und Vertretern der betroffenen Ressorts.

Der Ausschuss begrüßt, dass es in vielen Fällen, die Anlass zur Kritik gegeben haben, bereits zu einer Klärung mit den zuständigen Ressorts und Dienststellen gekommen ist beziehungsweise im Rahmen von Gesprächen zwischen den Beteiligten konstruktiv an Lösungsmöglichkeiten gearbeitet wird.

Aus dem Bereich "Übergreifende IT-Verfahren" hat sich der Ausschuss erneut mit der Problematik der Gewährleistung der Sicherheit der Verarbeitung bei der Übertragung personenbezogener Daten per Fax (Ziffer 5.1) befasst. Der Ausschuss hat zur Kenntnis genommen, dass es immer noch vereinzelt alte Faxgeräte in der Verwaltung gibt, diese Technologie aber nach und nach bis Ende 2022 abgeschafft werden soll. Die Mitarbeiterinnen und Mitarbeiter sind jedoch gehalten, diese Technik nicht mehr für die Übermittlung personenbezogener Daten zu verwenden, da der Sicherheitsstandard lediglich dem einer unverschlüsselten E-Mail entspricht und damit nicht ausreichend ist.

Zum Themenbereich "Inneres" begrüßt der Ausschuss, dass sich die Bearbeitungsdauer (Ziffer 6.4.1) durch eine Konkretisierung der Zuständigkeiten innerhalb der Polizei sowie durch die Einführung eines Controllings erheblich verringert hat. Dem Ausschuss wurde versichert, dass aktuell keine Beschwerden über die Bearbeitungsdauer mehr anhängig sind.

Eine zufriedenstellende Lösung ist ebenfalls bei der Erteilung von Auskünften (Ziffer 6.4.2) gefunden worden. Durch eine Neuorganisation der Prozesse sollte es nun nicht mehr vorkommen, dass Auskünfte nicht oder erst mit großer zeitlicher Verzögerung erteilt werden.

Der Ausschuss sieht es hingegen kritisch, dass die Umsetzung der Richtlinie (EU) 2016/680 ("JI-Richtlinie") durch die Ressorts Justiz und Inneres trotz Fristsetzung bis zum Mai 2018 erst mit großer zeitlicher Verzögerung erfolgt ist (Ziffer 6.5 und Ziffer 7.4). So ist das neue Polizeigesetz, das Teile der Richtlinie umsetzt, erst vor kurzem in Kraft getreten. Im Bereich des Justizvollzugs ist die Umsetzung ebenfalls erst mit Verspätung im Juli 2020 erfolgt, bei den Strafgerichten steht sie nach wie vor aus. Allerdings liegt der Gesetzesentwurf zu einem Bremischen Strafjustizdatenschutzgesetz bereits vor und befindet sich in der Abstimmung. Im Ergebnis sind die Vorgaben der Richtlinie trotz der zeitlichen Verzögerung rechtskonform

umgesetzt worden, auch wenn zwischen Ressort und Datenschutzbeauftragter teilweise unterschiedliche Auffassungen hinsichtlich des zu wählenden Umsetzungsniveaus bestehen.

Zu den Fällen der Nichterteilung von Auskunftssperren (Ziffer 6.6.2) hat sich der Ausschuss berichten lassen, dass sich die Bundesarbeitsgruppe zum Bundesmeldegesetz dieser Thematik angenommen und Leitlinien für die Meldebehörden erarbeitet hat. Nach diesen Leitlinien kann eine Auskunftssperre auch bei einer abstrakten Gefahr eingetragen werden. Eine Änderung des Bundesmeldegesetzes ist im Rahmen des "Gesetzes zur besseren Bekämpfung des Rechtsextremismus und der Hasskriminalität" geplant. Dort ist eine Regelung aufgenommen, die dem Bremer Entschließungsantrag entspricht, wonach es Möglichkeiten für die Eintragung von Auskunftssperren im Bereich von Berufsgruppen geben soll, die aufgrund ihrer Berufsausübung Gefährdungslagen ausgesetzt, oder von Privatpersonen, die durch ihr grundrechtskonformes Verhalten zur Zielscheibe gewaltbereiter Gruppen geworden sind. Der Ausschuss begrüßt es, dass die entsprechende Gesetzesänderung unmittelbar bevorsteht.

Bei der Übermittlung von Patientendaten an externe Abrechnungsunternehmen (Ziffer 8.4) nimmt der Ausschuss zur Kenntnis, dass für die Datenübermittlung grundsätzlich eine Einwilligungserklärung des Patienten beziehungsweise der Patientin erforderlich ist. Ob sich dieses Erfordernis auch auf andere Bereiche im Rahmen der freiberuflichen Tätigkeiten übertragen lässt, muss in jedem Einzelfall geprüft werden. Vergleichbare Beschwerden sind jedoch bisher nicht zu verzeichnen.

Zu der Problematik im Zusammenhang mit der Anforderung eines vollständigen MDK-Gutachtens (Ziffer 9.4) begrüßt der Ausschuss, dass die Anforderungen hinsichtlich der Übermittlungen von Gesundheits- und Sozialdaten durch den MDK inzwischen entsprechend den Vorgaben der Landesbeauftragten für Datenschutz geändert worden sind, um den Grundsatz der Datenminimierung einzuhalten.

Das Thema "Datenbank Haaranalysen" (Ziffer 9.6) war bereits Gegenstand zahlreicher Jahresberichte und hat den Ausschuss im Hinblick auf die datenschutzrechtliche Problematik auch im vorliegenden Berichtsjahr wieder beschäftigt. Die Datenbank ist inzwischen konzeptionell überarbeitet worden, ein Löschkonzept liegt vor. Allerdings fehlt es laut Auskunft des Ressorts noch an einer Auswertungsroutine. Ferner besteht bei einzelnen Punkten noch Klärungsbedarf, über die das Ressort mit der Datenschutzbeauftragten aber im Gespräch ist.

Im Bereich Bildung nimmt der Ausschuss zur Kenntnis, dass das Verfahren zum Beschwerdeportal (Ziffer 10.2) noch nicht vollständig abgeschlossen ist.

Die Veröffentlichung von privaten Fotos und Videos auf Social-Media-Seiten (Ziffer 10.5), insbesondere im Rahmen von Schulveranstaltungen, ist immer wieder Gegenstand von

datenschutzrechtlichen Beschwerden. Hier muss im Zweifel in jedem Einzelfall geprüft werden, ob eine Veröffentlichung zulässig gewesen ist oder nicht. Neben dem Datenschutz ist in bestimmten Konstellationen auch das Kunsturhebergesetz zu berücksichtigen.

Die Verwendung von Microsoft 365 und des Programms "Teams" in Schulen (Ziffer 10.6) wird von der Landesdatenschutzbeauftragten grundsätzlich kritisch gesehen, auch wenn es Verständnis dafür gibt, dass zu Beginn der Pandemie erst einmal schnell Lösungen für den digitalen Unterricht gefunden werden mussten. Der Ausschuss teilt die Auffassung der Landesdatenschutzbeauftragten, dass es wünschenswert wäre, wenn einheitliche und datenschutzkonforme Videokonferenzlösungen für alle Schulen, private und öffentliche, gefunden werden könnten.

Im Bereich des Beschäftigtendatenschutzes (Ziffer 11) stellten sich immer wieder datenschutzrechtliche Fragen im Zusammenhang mit der Zulässigkeit von Überwachungen und Kontrollen der Beschäftigten. Bei der Aufzeichnung von Anrufen durch ein Callcenter (Ziffer 11.2) kommt es bei der Frage der Zulässigkeit neben der konkreten Ausgestaltung der Tätigkeit und des Arbeitsverhältnisses auch auf die Frage des Vorliegens einer Einwilligungserklärung der Mitarbeiterin beziehungsweise des Mitarbeiters an.

Die Aufforderung an Bedienstete in der Verwaltung, für eventuelle Vertretungsfälle die Möglichkeit eines Vertretungszugriffs auf die personalisierten dienstlichen E-Mail-Postfächer einzurichten, ist grundsätzlich unzulässig (Ziffer 11.5). Diese Auffassung wird vom Senat uneingeschränkt geteilt. Für unvorhersehbare Vertretungsfälle sind deshalb auch andere, datenschutzkonforme Verfahren vorgesehen. Der Ausschuss geht daher davon aus, dass es sich bei der Beschwerde um einen Einzelfall gehandelt hat.

Im Bereich Wirtschaft und Gewerbe sieht es der Ausschuss sehr kritisch, dass in Kopiergeschäften tagtäglich eine Unmenge an persönlichen Daten auf den Speichermedien der Kopier- beziehungsweise Multifunktionsgeräte landet (Ziffer 13.2). Da die Geräte in der Regel eine automatische Speicherung vorsehen, müsste diese aktiv ausgeschaltet werden, was in der Praxis eher selten der Fall sein dürfte. Die Landesdatenschutzbeauftragte stellt jedoch in Aussicht, aufgrund des aufgestockten Personals künftig mehr stichprobenartige Kontrollen durchführen zu können.

Beschlussempfehlung:

Die Bürgerschaft (Landtag) nimmt den Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Kenntnis.

Dr. Solveig Eschen

4. Datenschutzbeauftragte

4.1 Rechtsanwalt als Datenschutzbeauftragter

Wiederholt erreichte uns im Berichtsjahr die Frage, ob Unternehmen der Privatwirtschaft die Funktion der oder des Datenschutzbeauftragten auch an ihre Rechtsanwältin beziehungsweise ihren Rechtsanwalt übertragen dürften oder im Hinblick auf die Verarbeitung personenbezogener Daten eine Unvereinbarkeit bestünde, die eine solche Übertragung nicht zulässt. Letzteres ist der Fall.

Zwar können Datenschutzbeauftragte nach Artikel 38 Absatz 6 Datenschutzgrundverordnung (DSGVO) beim Verantwortlichen auch andere Aufgaben wahrnehmen. Das jeweilige Unternehmen hat hinsichtlich seiner personenbezogenen Datenverarbeitung aber sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen, weil sie die Datenschutzbeauftragten etwa in eine Situation bringen, die ihre ordnungsgemäße und unabhängige Aufgabenerfüllung in Frage stellen kann. Bei der Beurteilung datenschutzrechtlicher Sachverhalte im Hinblick auf die Umsetzung und Einhaltung datenschutzrechtlicher Vorgaben müssen die Beauftragten in ihren Positionen und Entscheidungen unabhängig und frei von Weisungen der Unternehmensleitung sein. Darüber hinaus gehört es zu den Aufgaben der Datenschutzbeauftragten nach Artikel 39 Absatz 1 Buchstabe d DSGVO, mit der Datenschutzaufsichtsbehörde im Hinblick auf die Umsetzung und Einhaltung der Verordnung in ihren Unternehmen zusammen zu arbeiten und dort den Datenschutzbestimmungen gemeinsam mit der Datenschutzaufsichtsbehörde wie vom Gesetzgeber gewollt Geltung zu verschaffen. Datenschutzbeauftragte dürfen daher in Angelegenheiten der personenbezogenen Datenverarbeitung nicht anwaltlich für das von ihnen vertretene Unternehmen tätig werden, weil sie anderenfalls möglicherweise bei der Prüfung der rechtlichen Zulässigkeit einer Datenverarbeitung von ihnen selbst vorgenommene Beurteilungen überprüfen müssten. Auch könnte ihre anwaltliche Verpflichtung zur Vertretung der Interessen ihrer Mandantschaft mit der Zusammenarbeitsverpflichtung mit der Aufsichtsbehörde kollidieren.

4.2 Befristung der Benennung von Datenschutzbeauftragten

Uns erreichten mehrere Anfragen zur zeitlich begrenzten Benennung von Datenschutzbeauftragten. In einem Fall wies ein Datenschutzbeauftragter einer öffentlichen Einrichtung in Bremerhaven darauf hin, dass sein Nachfolger zunächst nur für ein Jahr bestellt werden solle. Bei anderen Anfragen sollte die befristete Benennung immer nur um ein Jahr verlängert werden. Derart kurze Benennungszeiträume sind in der Regel unzulässig. Die Datenschutzgrundverordnung (DSGVO) sieht eine Befristung für die Benennung der oder des Datenschutzbeauftragten nicht vor. Eine kurze Amtszeit gefährdet die unabhängige Stellung

der oder des Beauftragten, was zur Folge haben könnte, dass die Aufgaben nach Artikel 39 DSGVO nicht mehr effektiv erfüllt würden. Datenschutzbeauftragte stehen in einem besonderen Spannungsverhältnis, da sie den Verantwortlichen zwar einerseits auf Datenschutzrechtsverstöße aufmerksam machen und ihn zur Einhaltung der datenschutzrechtlichen Vorgaben anhalten sollen, andererseits aber im Hinblick auf den Fortbestand des der Benennung zugrundeliegenden Vertrags oder arbeitsrechtlichen oder dienstrechtlichen Bewertungen Anreizen unterliegen, Kontroversen mit den Verantwortlichen zu meiden. Eine Befristung kann dazu führen, dass das Verbot umgangen wird, Datenschutzbeauftragte wegen der Erfüllung ihrer Aufgaben abzuberufen. Eine Befristung der Benennung darf daher nur ausnahmsweise und mit stichhaltiger und mit den Wertungen der Datenschutzgrundverordnung konformer Begründung erfolgen.

4.3 Kündigungsschutz des Datenschutzbeauftragten bei bremischen öffentlichen Stellen

Der Datenschutzbeauftragte einer bremischen Kammer beklagte sich bei uns, dass er anders als die Datenschutzbeauftragten nicht öffentlicher Stellen als Datenschutzbeauftragter einer bremischen öffentlichen Stelle "keinen Kündigungsschutz" genieße. Nach Artikel 38 Absatz 3 Satz 2 Datenschutzgrundverordnung (DSGVO) dürfen Datenschutzbeauftragte von der oder dem Verantwortlichen oder Auftragsverarbeiter wegen der Erfüllung ihrer Aufgaben nicht abberufen werden. Für Datenschutzbeauftragte, die dem Bundesdatenschutzgesetz (BDSG) unterliegen, konkretisieren § 6 Absatz 4 BDSG (für Datenschutzbeauftragte öffentlicher Stellen des Bundes) und § 38 Absatz 2 BDSG (für Datenschutzbeauftragte nicht öffentlicher Stellen, deren Benennung verpflichtend ist) Artikel 38 DSGVO dahingehend, dass die Abberufung der oder des Datenschutzbeauftragten nur in entsprechender Anwendung des § 626 Bürgerlichen Gesetzbuches (BGB), also bei Vorliegen außerordentlicher Kündigungsgründe zulässig ist. Nach Auffassung des Bundesarbeitsgerichts hatte die gleichlautende Vorgängerregelung zur Folge, dass der Abberufungsschutz auf den Bestandsschutz des Beschäftigungsverhältnisses übertragen wurde.

Zwar gilt diese Bundesregelung nicht für die dem Bremischen Ausführungsgesetz zur EU-Datenschutzgrundverordnung unterliegenden Stellen und damit auch nicht für Datenschutzbeauftragte der öffentlichen Stellen des Landes Bremen. Ein der Rechtsprechung zugrundeliegender Gedanke, dass der Bestand der Bestellung als Datenschutzbeauftragte oder Datenschutzbeauftragter mit dem Bestand des Beschäftigungsverhältnisses verknüpft werden muss, um gewährleisten zu können, dass Datenschutzbeauftragte von der oder dem Verantwortlichen oder Auftragsverarbeiter wegen der Erfüllung ihrer Aufgaben nicht abberufen werden, kann jedoch bereits Artikel 38 Absatz 3 DSGVO entnommen werden. Insofern stellt § 6 Absatz 4 BDSG im Vergleich zur Regelung der DSGVO keine Erweiterung, sondern

lediglich eine Konkretisierung des Abberufungsschutzes dar. Es spricht jedoch nichts dagegen, bei einer Novellierung des Bremischen Ausführungsgesetzes zur EU-Datenschutzgrundverordnung klarstellend aus dem § 6 Absatz 4 BDSG entsprechende Regelung einzufügen.

4.4 Haftung der Datenschutzbeauftragten

Wiederholt baten Datenschutzbeauftragte um Auskunft darüber, inwieweit sie im Sinn des § 823 Bürgerlichen Gesetzbuches (BGB) haften müssen, wenn sie falsch beraten und aufgrund dieser Beratung ein Datenschutzmangel oder Datenschutzverstoß bestehen bleibt oder entsteht, der zum Beispiel zur Verhängung eines Bußgeldes führt. Nach § 823 BGB ist derjenige dem anderen zum Ersatz des daraus entstandenen Schadens verpflichtet, der vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt (deliktische Haftung).

Die Haftung der oder des Datenschutzbeauftragten ist möglich, kommt aber nur selten vor, weil für die Haftung die Ursächlichkeit des Verhaltens der oder des Beauftragten maßgeblich ist. Der entstandene Schaden muss kausal unmittelbar darauf zurückzuführen sein, dass die oder der Datenschutzbeauftragte ihren beziehungsweise seinen Aufgaben nicht wie von ihr oder ihm verlangt und wahrnehmbar entsprochen hat. Auch hätte die oder der Beauftragte nachweislich eine Vermeidung des Datenschutzmangels oder Datenschutzverstoßes erreichen können müssen. Der Mangel oder der Verstoß hätte mit an Sicherheit grenzender Wahrscheinlichkeit ausgeblieben sein müssen.

Bei vorsätzlicher oder grob fahrlässiger Falschberatung ist demgegenüber eine Haftung auch gegenüber Dritten denkbar, wenn es erst diese Falschberatung ist, die den Verantwortlichen zu einem gesetzeswidrigen Verhalten veranlasste.

5. Inneres

5.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr 2020 meldeten uns die Polizeien in Bremen in fünf Fällen eigene Verstöße gegen datenschutzrechtliche Vorschriften. Unter anderem war beziehungsweise ist es circa 50 Bediensteten der Polizeien in Bremen technisch möglich, Datenabfragen in einem polizeilichen Informationssystem durchzuführen, ohne protokolliert zu werden und ohne fachlich dazu befugt zu sein. Weitere Beispiele von Datenschutzverstößen wurden in Zusammenhang mit der Online-Wache gemeldet. Es kam beispielsweise im Januar 2020 aufgrund einer technischen Störung zu einem Verlust von 22 Online-Strafanzeigen, von denen nur eine Strafanzeige wiederhergestellt werden konnte. Die restlichen 21 Strafanzeigen

konnten nicht rekonstruiert werden. Zu diesen 21 Anzeigen konnten aber zumindest alle Anzeigenden erfolgreich kontaktiert werden.

5.2 Mobile Datenverarbeitung bei der Polizei

Aufgrund einer frühzeitigen Beteiligungsbitte berieten wir sowohl die Polizei Bremen als auch die Ortspolizeibehörde Bremerhaven bei der Einführung eines sogenannten "digitalen Notizbuchs". Die dort erfassten Daten werden in das Vorgangsbearbeitungssystem der jeweiligen Polizeien übertragen. Die technisch erforderlichen Maßnahmen zur Einführung eines solchen digitalen Notizbuchs wurden im Berichtsjahr weitestgehend abgeschlossen. Wegen der sehr komplexen Möglichkeiten zur differenzierten Berechtigungssteuerung mussten vor dem Echtbetrieb insbesondere das vorliegende Rechtekonzept und Rollenkonzept überarbeitet werden. Von der Nutzung eines Ausweis-Scans im Testbetrieb rieten wir ab. Der Testbetrieb hatte im dritten Quartal 2020 mit 20 mobilen Endgeräten begonnen.

5.3 Das neue Polizeirecht

Am 19. November 2020 verabschiedete die Bremische Bürgerschaft die lange diskutierte Änderung des Bremischen Polizeigesetzes (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 6.5 und 40. Jahresbericht, Ziffer 5.7). Zuvor waren die Ergebnisse der öffentlichen Anhörung der Deputation für Inneres am 8. September 2020 (siehe die 14 Stellungnahmen[2], zu denen auch diejenige der bremischen Landesbeauftragten für Datenschutz und Informationsfreiheit gehört), eingearbeitet worden. Die Novelle des Bremischen Polizeigesetzes (BremPolG) verfolgt zum einen das Ziel, die europäische Richtlinie 2016/680 (JI-Richtlinie) umzusetzen. Andererseits werden präventiv-polizeiliche Befugnisse erstmals begründet oder ausgeweitet.

Die Ausstattung der Polizeien im Land Bremen mit neuen präventiven Eingriffsbefugnissen, die bislang nur für den Strafverfolgungsbereich existierten, bleibt auch nach den Anpassungen des Gesetzentwurfs im Anschluss an die Anhörung verfassungsrechtlich bedenklich. Insbesondere fällt auf, dass die gegenwärtig in Schleswig-Holstein und in Berlin diskutierten Gesetzentwürfe im Gegensatz zur bremischen Novellierung im Hinblick auf die Verfassungsrechtsprechung auf die Möglichkeit zur Verarbeitung von Verkehrsdaten verzichten. Das Bremische Polizeigesetz orientiert sich am Bundeskriminalamtsgesetz und der hierzu ergangenen Rechtsprechung des Bundesverfassungsgerichts, obwohl sich die Aufgaben des Bundeskriminalamts von denen der Polizeien im Land Bremen unterscheiden: Während das Bundeskriminalamtsgesetz auf die Strafverfolgung nach terroristischen Anschlägen zielt, also sehr hohe Schutzgüter nach deren Verletzung verteidigt, kommt das

[2] https://sd.bremische-buergerschaft.de/tops/?__=UGhVM0hpd2NXNFdFcExjZbJksZprkAU2OPwF0ipT5Vs

Bremische Polizeigesetz schon zur Anwendung, wenn einfache Körperverletzungen oder die Beschädigung von Sachgütern bevorstehen. Umso wichtiger ist es, dass entscheidende Regelungen des Gesetzes bis zum 30. Juni 2024 befristet sind und wissenschaftlich evaluiert werden müssen.

Die neu geschaffenen Regelungen zur Überwachung von Telekommunikation zu präventiven Zwecken greifen stark in die Grundrechte von Bürgerinnen und Bürgern ein. Dies ist besonders bedenklich, weil die gegenwärtig von Bremen gemeinsam mit Niedersachsen genutzte Telekommunikationsüberwachungsanlage aus datenschutzrechtlicher Sicht mit vielen Mängeln behaftet ist (siehe hierzu 40. Jahresbericht, Ziffern 5.5 und 5.7.1, 39. Jahresbericht, Ziffer 6.1, 38. Jahresbericht, Ziffer 6.1 und 37. Jahresbericht, Ziffer 5.2). Solange keine Lösung gefunden wird, die diese Mängel behebt, ist den Polizeien im Land Bremen von der Nutzung der neuen Befugnisse im Rahmen des Betriebs der Telekommunikationsüberwachung mit dem Landeskriminalamt Niedersachsen dringend abzuraten.

Auch den neuen Regelungen zur Videoüberwachung mittels am Körper getragener Kamera (sogenannte Bodycam) begegnen verfassungsrechtlichen Bedenken: Ermöglicht wird mit der Videoüberwachung in Wohnungen die Überwachung in einem Privatbereich, der durch das Grundrecht der Unverletzlichkeit der Wohnung nach Artikel 13 Grundgesetz besonders stark geschützt ist. Auch handelt es sich bei dem nach der gesetzlichen Regelung erlaubten Pre-Recording, (also der permanenten Aufzeichnung im Normalmodus, die nach 60 Sekunden wieder überschrieben wird), anders als dies die Gesetzesformulierung nahelegt, de facto um eine verdeckte Überwachung. Deshalb ist es unabdingbar, dass die von Bodycams Erfassten in der Praxis bereits zu Einsatzbeginn über das Pre-Recording von 60 Sekunden informiert werden, um die permanente Aufzeichnung offen zu legen.

Aus datenschutzrechtlicher Sicht gut gelungen ist dagegen die Verpflichtung zur "Überwachungsgesamtrechnung" in § 34 Absatz 5 Satz 1 und 2 BremPolG. Dort heißt es: "Mehrere besondere Mittel und Methoden der Datenerhebung gemäß Absatz 1 dürfen nebeneinander angeordnet werden, sofern sie auch in der Gesamtwirkung nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht, und es hierdurch insbesondere nicht zu einer lückenlosen Registrierung der Bewegungen und Lebensäußerungen der betroffenen Person kommt. Der Polizeivollzugsdienst hat dabei auch Maßnahmen zu berücksichtigen, die von anderen Stellen durchgeführt werden, soweit er hiervon Kenntnis erlangt." Gleiches gilt für die neu geschaffenen Berichtspflichten gegenüber dem für Datenschutz zuständigen Ausschuss der Bremischen Bürgerschaft, die Benachrichtigungspflichten gegenüber den Betroffenen und die Dokumentationspflichten der Polizeien zur Nachvollziehbarkeit der Rechtmäßigkeit ihres Handelns. Wir bedauern, dass die Unterrichtungspflichten gegenüber gesetzlichen Vertretern gemäß § 26 Absatz 6 und gegenüber Betroffenen in § 50 Absatz 4, § 51 Absatz 4, § 55 Absatz 1, § 58 Absatz 8 und § 62

Absatz 1 BremPolG und die Dokumentationspflicht des § 50 Absatz 4 BremPolG erst am 1. September 2021 in Kraft treten werden.

5.4 Mobile Datenverarbeitung im Rettungswagen bei der Feuerwehr

Im Berichtsjahr berieten wir die Feuerwehr Bremen bei der Einführung der mobilen Datenerfassung im Rettungsdienst. Mit diesem Projekt soll im Wesentlichen die bisher manuelle Erfassung der Einsatzprotokolle abgelöst und ein vereinfachter, schnellerer und medienbruchfreier Austausch medizinischer und abrechnungsrelevanter personenbezogener Daten mit den entsprechenden Stellen (beispielsweise Krankenhäuser, Rechnungsstellen und Krankenkassen) realisiert werden. Gerade die Ausgestaltung einer datenschutzkonformen Weitergabe der medizinischen Daten an die Krankenhäuser bedarf besonderer Aufmerksamkeit, da diese sensiblen Daten als besondere Kategorien von personenbezogenen Daten durch das europäische Recht besonders geschützt werden. Unseren Empfehlungen wurde bisher entsprochen.

5.5 Projekt Deradikalisierung und Extremismusprävention mit Schwerpunkt Islamismus/Salafismus

Wir berieten das Projekt zur Deradikalisierung und Extremismusprävention mit Schwerpunkt Islamismus/Salafismus im Land Bremen. In diesem Zusammenhang wiesen wir darauf hin, dass als rechtliche Grundlage für die Verarbeitung der personenbezogenen Daten zusätzlich zu einer Einwilligungserklärung eine Schweigepflichtentbindungserklärung erforderlich ist. Dies ist nur dann nicht der Fall, wenn sich die Rechtsvorschriften, die die Datenverarbeitung erlauben, ausdrücklich an Berufsgeheimnisträgerinnen und Berufsgeheimnisträger richten.

5.6 Beschwerden im Melderecht

Wir erhielten sechs Beschwerden im Melderecht. Die Themen reichten von versagter Auskunftssperre bis hin zum Antrag auf Berichtigung alter Adressen. Das Bürgeramt Bremen half erfreulicher Weise zeitnah jeder Beschwerde ab.

5.7 Vertraulichkeit der Corona-Quarantänekontrolle

Uns erreichten zwei Beschwerden, nach denen im Rahmen von Corona-Quarantänekontrollen durch das Ordnungsamt gegenüber Nachbarinnen und Nachbarn Gesundheitsdaten der kontrollierten Personen offenbart worden seien. Die Beschäftigten des Ordnungsamtes hätten mit den Nachbarinnen und Nachbarn kommuniziert oder aber sich gegenüber den kontrollierten Personen so laut geäußert, dass die Nachbarschaft Kenntnis von der Infektion der Betroffenen erlangte. Das Ordnungsamt teilte in beiden Fällen mit, dass eine Offenbarung

von Daten gegenüber Nachbarinnen oder Nachbarn nicht erfolgt sei. Es gelang uns nicht, die Sachverhalte aufzuklären. Die Fälle zeigen zum einen, dass die Wahrung der Vertraulichkeit im Rahmen der Corona-Quarantänekontrollen für die Betroffenen besondere Relevanz hat und datenschutzrechtlich unabdingbar ist. Andererseits wird deutlich, wie schwierig die Wahrung der Vertraulichkeit bei gleichzeitiger Einhaltung von Abstandsregeln sein kann. Eine Sensibilisierung der Beschäftigten des Ordnungsamtes ist deshalb unerlässlich. Dies gilt auch für die umfassende Dokumentation des Datenumgangs im Rahmen von Quarantäne-Kontrollen.

5.8 Einsatz von Security-Unternehmen in BürgerServiceCentern

Uns erreichte eine Beschwerde über eine Datenerhebung durch Beschäftigte eines Security-Unternehmens im Bremer BürgerServiceCenter (BSC). Danach hätten die Beschäftigten es als ihre Aufgabe betrachtet, Besucherinnen und Besucher des BSC nach ihren Anliegen zu befragen. Ungeklärt ist bislang, wer für die darin liegende Datenerhebung durch die Beschäftigten des Security-Unternehmens im Sinne der Datenschutzgrundverordnung (DSGVO) verantwortlich ist. Die datenschutzrechtliche Verantwortung könnte beim BSC selbst und/oder dem Senator für Inneres und/oder Immobilien Bremen und/oder beim Security-Unternehmen liegen. Es könnte also alleinige Verantwortung einer der Stellen (gegebenenfalls als Auftraggeberin einer Auftragsverarbeitung) oder gemeinsame Verantwortung mehrerer Stellen vorliegen. Die Einstufung als Verantwortlicher nach der DSGVO hat nicht nur Auswirkungen auf die Frage, ob und welche Datenverarbeitungsvorgänge zulässig sind. Daneben ermöglicht eine geklärte und gegenüber den Besucherinnen und Besuchern des BSC transparent kommunizierte Verantwortlichkeit auch, dass diese eine Anlaufstelle für an den Verantwortlichen gerichteten datenschutzrechtlichen Fragestellungen haben und so ihr Recht auf Datenschutz effektiv durchsetzen können. Dass die Verantwortlichkeit zwischen den genannten Stellen nicht beziehungsweise nicht in nach außen sichtbarer Weise geklärt wurde, verdeutlicht, dass hier insbesondere seitens der öffentlichen Stellen noch Handlungsbedarf besteht (siehe hierzu Ziffer 17.2 dieses Berichts).

5.9 Alternierende Telearbeit bei der Polizei Bremen

Die COVID-19-Pandemie führte auch im Bereich der Polizei zu dem Wunsch, vermehrt aus den eigenen vier Wänden arbeiten zu können. Voraussetzung dafür ist, dass neben der Dienstvereinbarung "alternierende Telearbeit" der Freien Hansestadt Bremen auch weitere, mit der Landesbeauftragen für Datenschutz und Informationsfreiheit (LfDI) vereinbarte Grundsätze eingehalten werden. Dazu zählt unter anderem, dass die Mitarbeiterinnen und Mitarbeiter der Polizei digital arbeiten und die Verarbeitung der Daten ausschließlich auf den Servern der Polizei und nicht auf den Endgeräten stattfindet. Die klassische Papierakte darf

zur Bearbeitung nicht an den heimischen Arbeitsplatz genommen werden (weitere Anforderungen finden sich im 40. Jahresbericht, Ziffer 5.6).

Die ursprüngliche Zusage der Polizei, wonach die Anzahl der alternierenden Telearbeitsplätze auf 20 begrenzt sein sollte, wurde in Absprache mit der LfDI temporär (für die Dauer der Pandemie) außer Kraft gesetzt. Der an die LfDI herangetragene Wunsch, auch anschließend vermehrt alternierende Telearbeit anbieten zu können, ist bisher noch nicht endgültig abgestimmt worden. Für die Entscheidung hierüber ist aus unserer Sicht entscheidend, wie die alternierende Telearbeit bei der Polizei zukünftig ausgestaltet sein soll und welche Lehren aus den bisherigen Erfahrungen zu ziehen sind. Dafür müssen spätestens nach der Pandemie unter anderem auch die entsprechenden Protokolldateien angesehen und bewertet werden. Die LfDI steht dazu mit dem behördlichen Datenschutzbeauftragten der Polizei Bremen in Kontakt.

5.10 Vorbereitung ZENSUS

Die Landesbeauftragte für Datenschutz und Informationsfreiheit wird vom Statistischen Landesamt regelmäßig über den aktuellen Stand der Vorbereitung zur Volkszählung (ZENSUS) informiert und – zum Beispiel bei der Erstellung einer Datenschutz-Folgenabschätzung nach Artikel 35 Datenschutzgrundverordnung – beratend mit einbezogen.

6. Justiz

6.1 Verstöße gegen das das Bremische Justizvollzugsdatenschutzgesetz

Für den Berichtszeitraum ab 24. Juli 2020 ist dies gleichzeitig der Bericht nach § 72 Absatz 1 Nummer 4 Bremisches Gesetz zum Schutz personenbezogener Daten im Justizvollzug (Bremisches Justizvollzugsdatenschutzgesetz - BremJVollzDSG) in Verbindung mit § 15 Bundesdatenschutzgesetz. Im gesamten Jahr 2020 erreichten uns keine Informationen über Verstöße gegen das Bremische Justizvollzugsdatenschutzgesetz.

6.2 Gemeldete Datenschutzverletzungen

Im Jahr 2020 wurden von Rechtsanwälten und Notaren bei der Landesbeauftragten für Datenschutz und Informationsfreiheit nur eine Verletzung des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung (DSGVO) gemeldet. Im Vorjahr waren es vier gemeldete Fälle. Es entspricht nicht der Lebenserfahrung, dass bei der erheblichen Anzahl von Schriftstücken und Akten, die von diesen Verantwortlichen versendet werden, keine Fehler passieren, sodass wir davon ausgehen müssen, dass gesetzlich vorgeschriebene Datenpannenmeldungen nicht erfolgten. Wir rechnen mit einer hohen Dunkelziffer und gehen

davon aus, dass die Zahl meldepflichtiger Verletzungen des Schutzes personenbezogener Daten weitaus größer sein wird, als es sich im Berichtsjahr darstellt.

Im Bereich der Staatsanwaltschaft Bremen und der verschiedenen Gerichte wurden von der verantwortlichen Stelle ebenfalls keine Verletzungen des Schutzes personenbezogener Daten gemeldet. Es gab lediglich einen Fall, in dem sich ein Betroffener an uns wandte und uns von einem Fehlversand eines an eine andere Person gerichteten Schriftstücks durch das Amtsgericht Bremen an ihn berichtete. Nach Zustimmung des Bürgers leiteten wir diesen Vorgang an das zuständige Gericht weiter.

6.3 Nennung eines Mandantennamens durch einen Anwalt auf einem Bewertungsportal

Ein Mandant einer Anwaltskanzlei meldete sich bei uns und berichtete, dass er auf einem anwaltlichen Bewertungsportal einen Kommentar zu einem Anwalt geschrieben habe. Dieser Anwalt habe diesen Kommentar wiederum kommentiert und dabei den Nachnamen seines Mandanten angegeben. Nicht nur, weil der Nachname des Mandanten sehr selten ist, konnte dabei ein Personenbezug zu ihm hergestellt werden. Für eine Reidentifikationsmöglichkeit, die zur Personenbeziehbarkeit und damit zur Anwendbarkeit der Datenschutzgrundverordnung (DSGVO) führt, reicht es aus, dass der Personenbezug durch beliebige Dritte hergestellt werden kann. Da die Nennung des Mandantennamens zur Kommentierung nicht erforderlich war, verstieß der Anwalt mit seinem Verhalten gegen die DSGVO. Im ersten Schritt wurde er von uns aufgefordert, den Nachnamen umgehend aus dem Kommentar zu löschen. Dem kam der Anwalt unverzüglich nach.

6.4 Auskunftsanspruch bei der Staatsanwaltschaft

Erfreulicherweise ging im Berichtsjahr 2020 nur eine Beschwerde auf fehlende Auskunft nach Artikel 15 Datenschutzgrundverordnung durch die Staatsanwaltschaft Bremen bei uns ein. Sowohl zu dieser Beschwerde als auch zu einer weiteren ähnlich lautenden Beschwerde aus dem Jahr 2018 erhielten wir trotz mehrmaliger Mahnung von der Staatsanwaltschaft Bremen jedoch bislang weder eine Rückmeldung noch eine Stellungnahme.

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

Im Jahr 2016 verabschiedete der europäische Gesetzgeber die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (JI-Richtlinie). Als Richtlinie ist

diese anders als die Datenschutzgrundverordnung in den meisten Teilen nicht direkt anwendbar und hätte vom bremischen Gesetzgeber bis zum 6. Mai 2018 in Landesrecht umgesetzt werden müssen. Die Senatorin für Justiz und Verfassung legte uns im November 2019 einen Entwurf für ein Bremisches Justizvollzugsdatenschutzgesetz zur Stellungnahme vor. Dazu gaben wir eine ausführliche Stellungnahme ab, in der wir zahlreiche datenschutzrechtlichen Bedenken formulierten. Diese bezogen sich unter anderem auf den Anonymisierungsbegriff, die Einwilligungen Betroffener als Rechtsgrundlage und die Verarbeitung besonderer Kategorien personenbezogener Daten. Mit dem unzutreffenden Hinweis, dieser sei mit uns abgestimmt, wurde der unsere Stellungnahme nicht berücksichtigende Gesetzentwurf am 7. April 2020 in die Bürgerschaft eingebracht. Seit 24. Juli 2020 ist das Gesetz in Kraft. Im gesamten Berichtsjahr erhielten wir keine Informationen über Datenschutzverstöße in den Justizvollzugsanstalten.

Im Februar 2020 leitete uns die Senatorin für Justiz und Verfassung den Entwurf eines Gesetzes zur Einführung eines neuen Bremischen Strafjustizdatenschutzgesetzes mit der Gelegenheit zur Stellungnahme zu. Auch hierzu gaben wir im März 2020 eine ausführliche Stellungnahme mit datenschutzrechtlichen Erwägungen und Änderungsvorschlägen ab, die sich auf ähnliche Thematiken bezog. Das Justizressort teilte uns im Dezember 2020 mit, dass über diesen Gesetzentwurf Gespräche zwischen den Ressorts und den Regierungskoalitionen geführt würden. Bis zur Verabschiedung des Bremischen Strafjustizdatenschutzgesetz besteht im Land Bremen eine Regelungslücke bezügliche der Strafgerichte und der Staatsanwaltschaft.

6.6 Unverschlüsselte E-Mail-Versendung durch Rechtsanwaltskanzleien

Bei uns gehen zunehmend Beschwerden gegen Rechtsanwaltskanzleien ein, die Schreiben per unverschlüsselter E-Mail versenden. Rechtsanwältinnen und Rechtsanwälte dürfen im Auftrag ihrer Mandantinnen und Mandanten nach unterschiedlichen Normen (unter anderem Artikel 6 Absatz 1 Buchstaben b und f DSGVO) Daten erheben und verarbeiten. Die Datenschutzgrundverordnung (DSGVO) macht es aber ebenfalls zur Voraussetzung, beim Versand personenbezogener Daten sichere und damit geeignete Verfahren, wie zum Beispiel die Post oder Ende-zu-Ende verschlüsselte E-Mails zu nutzen.

In diesem Zusammenhang erinnern wir erneut daran (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 5.1), dass die Versendung per Fax hinsichtlich der Vertraulichkeit das gleiche (geringe) Sicherheitsniveau hat wie eine unverschlüsselte E-Mail. Fax-Dienste enthalten keinerlei Sicherungsmaßnahmen, um die Vertraulichkeit der personenbezogenen Daten zu gewährleisten. Unverschlüsselte E-Mails und Fax-Dienste sind daher nicht für die Übertragung personenbezogener Daten geeignet.

7. Gesundheit

7.1 Gemeldete Datenschutzverletzungen

Im Bereich Gesundheit wurden uns im Berichtsjahr insgesamt neun Datenschutzverletzungen gemeldet. Die Mehrzahl der Meldungen betraf Vorfälle, bei denen kriminelle Handlungen zum Verlust oder zu der unbefugten Offenlegung von Gesundheitsdaten führten.

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

Es ist eine der wesentlichen Aufgaben des öffentlichen Gesundheitsschutzes, die Weiterverbreitung übertragbarer Krankheiten zu verhindern und im Zuge dessen vor allem Kontaktpersonen zu ermitteln. Der Umgang mit den Daten solcher Personen, bei denen eine übertragbare Krankheit nachgewiesen wurde, gehörte deshalb auch in der Vergangenheit zu den Aufgaben der Gesundheitsämter. Allerdings veränderte die COVID-19-Pandemie im Berichtsjahr das Ausmaß dieser Tätigkeit erheblich. Die Zusammenarbeit der Gesundheitsämter mit anderen öffentlichen Stellen musste auch im Hinblick auf die damit einhergehenden Datenflüsse überdacht und teilweise neu eingeübt werden. Aufgrund fehlender Übermittlungsbefugnisse war beispielsweise die Übermittlung von personenbezogenen Daten Infizierter durch das Gesundheitsamt Bremen an die Polizei Bremen unzulässig, die zu Beginn der Pandemie erfolgt war. Die Polizei ist in Bremen nicht die für die Maßnahmen nach dem Infektionsschutzgesetz zuständige Behörde. Bis auf wenige Ausnahmen liegt diese Zuständigkeit bei den Gesundheitsämtern und dem Ordnungsamt Bremen beziehungsweise dem Magistrat der Stadt Bremerhaven. Dass im Einzelfall der Polizeivollzugsdienst die Möglichkeit hat, Befragungen durchzuführen und Untersuchungen nach dem Infektionsschutzgesetz anzuordnen, steht dem nicht entgegen. Diese besondere Befugnis ergibt sich aus dem Gesetz zur Behandlungseinleitung bei Infektionen mit übertragbaren Krankheiten durch Dritte und kommt nur dann zum Tragen, wenn bei einem konkreten Vorfall Tatsachen die Annahme rechtfertigen, dass eine Übertragung eines gefährlichen Krankheitserregers stattgefunden hat. Selbst in diesen Fallkonstellationen darf das Gesundheitsamt die Daten lediglich an die möglicherweise infizierte Person, also etwa eine möglicherweise infizierte Polizistin übermitteln. Nachdem sich die Unzulässigkeit der beschriebenen Übermittlungen herausgestellt hatte, wurden diese vom Gesundheitsamt nicht fortgesetzt.

7.3 Veröffentlichung von Corona-Fallzahlen

Im Rahmen der Öffentlichkeitsarbeit des Gesundheitsressorts kam wiederholt die Frage auf, wie klein die geographischen Einheiten sein dürfen, für die die Zahl der dort lebenden Corona-

Infizierten ausgewiesen werden darf. Grundsätzlich ist eine Weitergabe an Dritte (zum Beispiel die Presse) dann möglich, wenn sich ein Personenbezug nicht herstellen lässt. Bei Infektionszahlen, die pro Postleitzahlbezirk ausgewiesen werden, ist dies erst dann gegeben, wenn die Einwohnerzahl in den Postleitzahlbezirken entsprechend hoch ist, was zum Beispiel bei Industriegebieten problematisch sein kann. Die Angabe der Infiziertenzahl pro Postleitzahlbezirk halten wir deshalb für möglich, wenn sichergestellt ist, dass die durchschnittliche Einwohnerzahl pro Postleitzahlbezirk, die derzeit bei circa 16.700 liegt, nicht wesentlich unterschritten wird. Um zu verhindern, dass bei geringen Infiziertenzahlen eine Identifikation möglich ist, müssen in diesem Fall die Zahlen nach Kategorien (zum Beispiel 1 bis 5 Infizierte; 5 bis 10 Infizierte) ausgewiesen werden.

In einem ähnlich gelagerten Fall scheint das Oberverwaltungsgericht Rheinland-Pfalz (Beschluss vom 23. November 2020, Aktenzeichen 2 B 11397/20, Randnummer 14) nicht von einer Personenbeziehbarkeit im Sinne der Datenschutzgrundverordnung (DSGVO) auszugehen, wenn ohne Zusatzwissen keinen Rückschluss auf die konkret betroffene Person möglich ist. Dem steht Artikel 4 Nummer 1 DSGVO entgegen, der besagt, die Identifizierbarkeit bestehe, wenn die natürliche Person "direkt oder indirekt (…) identifiziert werden kann." Das Verwaltungsgericht Neustadt an der Weinstraße hatte in seinem nun aufgehobenen Beschluss vom 29. Oktober 2020 (Aktenzeichen: 5 L 930/20.NW) in einem Landkreis mit kleinteiliger Gemeinde "eine beachtliche Gefahr, dass die Veröffentlichung der Infektionszahlen auf Ortsgemeindeebene zu einer Bestimmbarkeit der betroffenen Personen führen wird", gesehen. Es sei "nicht nur wahrscheinlich, dass infizierte Personen in den kleinteiligen Gemeinden insbesondere über den Austausch in sozialen Netzwerken bestimmbar [seien], sondern dass von dieser Möglichkeit auch tatsächlich Gebrauch gemacht [werde]." (Randnummer 24).

7.4 Nutzung von Corona-Daten zu Forschungszwecken

Das Gesundheitsressort wandte sich mit Beratungsanfragen zu unterschiedlichen Forschungsvorhaben an uns. Geplant ist zum einen ein Projekt zur Erforschung des Krankheitsverlaufs nach einer Ansteckung mit dem Coronavirus SARS-CoV-2 und zum anderen ein Projekt zur wissenschaftlichen Begleitung von Ausbruchsgeschehen an Bildungseinrichtungen. In beiden Projekten wurde das Leibniz-Institut für Präventionsforschung und Epidemiologie (BIPS) mit der Durchführung beauftragt. Die Konzepte sahen jeweils eine Übermittlung von personenbezogenen Daten der mit dem Coronavirus SARS-CoV-2 infizierten Personen durch das Gesundheitsamt Bremen an das BIPS vor. Die Grundlagen der Datenverarbeitung unterschieden sich dabei deutlich: Während bei der Studie zum Krankheitsverlauf allein die Adressen der beim Gesundheitsamt registrierten Fälle verwendet werden sollten, um die betroffenen Personen um freiwillige Teilnahme an der Studie bitten zu können, sah die Studie zum Ausbruchsgeschehen an

Bildungseinrichtungen eine Verarbeitung gruppierter, allerdings gleichwohl noch personenbezogener Daten vor.

Im Rahmen der datenschutzrechtlichen Beratung forderten wir insbesondere eine personelle Trennung hinsichtlich der Verarbeitung der noch personenbezogenen Daten und der anschließenden Verarbeitung der anonymisierten Daten sowie ausreichende Transparenz gegenüber den Betroffenen. Daneben mahnten wir einen sparsamen Umgang mit personenbezogenen Daten an und verwiesen auf die Pflicht, zu prüfen, ob der Forschungszweck nicht auch mit von vornherein bereits anonymisierten Daten erreicht werden könnte. Unsere Forderungen wurden weitestgehend umgesetzt. Eine Übermittlung personenbezogener Daten an das BIPS ist in der Studie zum Krankheitsverlauf nun nicht mehr vorgesehen. Hinsichtlich der Umsetzung unserer Forderungen bei der Studie zu Ausbruchsgeschehen an Bildungseinrichtungen wurden wir nicht weiter beteiligt.

7.5 Meldung von negativen Corona-Testergebnissen

Die Meldepflicht für Labore und andere nach dem Infektionsschutzgesetz meldepflichtige Untersuchungsstellen nach dem Bundesinfektionsschutzgesetz wurde im Rahmen der COVID-19-Pandemie ausgeweitet. Nun sind diese meldepflichtigen Stellen nicht mehr nur verpflichtet, dem Gesundheitsamt den direkten oder indirekten Nachweis des SARS-CoV-2-Virus zu melden, sondern müssen das Untersuchungsergebnis auch dann weitergeben, wenn dies negativ ausfällt. Zwar sind Negativmeldungen in Bremen zum Redaktionsschluss aufgrund mangelnder technischer Voraussetzungen zur Verarbeitung der zu erwartenden hohen Zahl an Meldungen noch nicht vorgesehen. Es ist jedoch zu erwarten, dass die Meldewege in absehbarer Zeit vollständig digitalisiert sind und die gesetzlich vorgesehene Meldepflicht dann umgesetzt wird. Da die Erweiterung der Meldepflicht auf Negativergebnisse keinen erkennbaren Nutzen für den Infektionsschutz birgt und eine personenbezogene Verarbeitung von negativen Testergebnissen zu diesem Zweck insofern nicht geeignet und auch nicht erforderlich ist, ist es höchst zweifelhaft, ob die Meldepflicht für Negativergebnisse mit der Datenschutzgrundverordnung vereinbar ist. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der die Aufgabe hat, die Stellen des Bundes im Zusammenhang mit dem Erlass von Bundesgesetzen zu beraten, hat diesbezüglich bereits Gespräche mit dem Bundesministerium für Gesundheit aufgenommen.

7.6 Fund des Belegungsplanes einer psychiatrischen Station auf offener Straße

Eine aufmerksame Bürgerin meldete sich bei uns, nachdem sie beim Spazierengehen den Belegungsplan einer Krankenhausstation gefunden hatte. Der Plan stammte von der psychiatrischen Station des Krankenhauses und enthielt nicht nur eine Auflistung der dort

untergebrachten Patientinnen und Patienten, sondern auch die jeweils gestellte Diagnose sowie handschriftliche Kommentare zu einzelnen Personen. Auf Nachfrage teilte uns das betroffenen Krankenhaus mit, dass die Mitnahme solcher Belegungspläne unter keinen Umständen gestattet sei. Der Vorfall werde zum Anlass genommen, die Beschäftigten erneut im Umgang mit Belegungsplänen zu schulen und zu sensibilisieren. Außerdem werde diesbezüglich eine neue Prozessanweisung erarbeitet.

7.7 Mehrere Phishing-Angriffe auf E-Mail-Postfächer in Arztpraxen

Uns erreichten in diesem Berichtsjahr mehrere Fälle, die sich auf Phishing-Angriffe auf E-Mail-Postfächer in Arztpraxen bezogen. Bei einem Phishing-Angriff erhält der Angreifer durch gefälschte E-Mails schädliche Anhänge oder präparierte Links zum Beispiel die Möglichkeit, von dem angegriffenen E-Mail-Postfach aus E-Mails zu senden. In den uns vorgetragenen Fällen führte dies dazu, dass von den betroffenen Postfächern aus E-Mails an Patientinnen und Patienten gesandt wurden, indem auf frühere E-Mails dieser Personen im Postfach der Arztpraxis geantwortet wurde und auf diese Weise Anhänge mit schädlichem Inhalt verbreitet wurden. Eine andere Variante dieser Art von Angriff ist es, die E-Mails des betroffenen Postfachs herunterzuladen, um diese mit maskierten E-Mails zu beantworten, um so schädlichen Inhalt zu verbreiten. Die E-Mails in den angegriffenen Postfächern waren teilweise schon mehrere Jahre alt. Diese Vorfälle verdeutlichen noch einmal mehr die Notwendigkeit, auch bei elektronischem Postverkehr angemessene Löschroutinen einzubinden. Sollte ein Angriff trotz regelmäßiger Sensibilisierung aller Beschäftigten und geeigneter Sicherheitsmaßnahmen doch einmal erfolgreich sein, kann hierdurch zumindest der Abfluss personenbezogener Daten und ein damit einhergehender Schaden begrenzt werden.

7.8 Auskunftsrecht in Arztpraxen

Des Öfteren erhalten wir Beschwerden von betroffenen Personen, denen eine kostenfreie Kopie ihrer personenbezogenen Daten durch Arztpraxen mit dem Hinweis verweigert wird, die Patientin oder der Patient habe gemäß § 630 g Absatz 2 Bürgerliches Gesetzbuch (BGB) die für die Erstellung elektronischer Abschriften der Patientenakte entstehenden Kosten zu erstatten. Diese Auffassung wurde bislang offenbar auch von der Ärztekammer Bremen vertreten. Dies nahmen wir zum Anlass, um in einer Stellungnahme das Verhältnis zwischen dem datenschutzrechtlichen Auskunftsrecht (Artikel 15 Datenschutzgrundverordnung) und dem patientenrechtlichen Einsichtsrecht (§ 630 g BGB) zu erläutern: Sofern eine Patientin oder ein Patient von ihrem beziehungsweise seinem Auskunftsrecht nach Artikel 15 Datenschutzgrundverordnung (DSGVO) Gebrauch macht und die Auskunft nicht auf bestimmte Daten beschränkt, ist ihr beziehungsweise ihm vollumfänglich Auskunft zu erteilen. Dies beinhaltet auch die Erstellung einer kostenfreien Kopie der verarbeiteten personenbezogenen Daten. Regelmäßig bestehen Patientenakten ausschließlich aus

personenbezogenen Daten. Dann ist eine vollständige Kopie der "Rohdaten" zu erstellen und der Patientin beziehungsweise dem Patienten zur Verfügung zu stellen. Das Einsichtsrecht in die Patientenakte mit dem Recht auf Erstellung von elektronischen Abschriften besteht grundsätzlich neben dem datenschutzrechtlichen Auskunftsrecht, geht diesem aber keinesfalls vor.

Das Landgericht Dresden unterstützt in seinem Urteil vom 29. Mai 2020 (Aktenzeichen 6 O 76/20) unsere Position: "Soweit die Klägerin sich auf Artikel 15 Absatz 3 DSGVO zur Begründung ihres Auskunftsanspruchs beruft, ist eine Inanspruchnahme für Kosten der Zusammenstellung und Übersendung der Daten nicht vorgesehen. Die Erstauskunft ist vielmehr kostenfrei. Dem steht nicht entgegen, dass bei einer Anforderung nach § 360 g BGB auch für die Erstauskunft eine Kostentragung statuiert ist."

8. Soziales

8.1 Gemeldete Datenschutzverletzungen

Im Bereich Soziales wurden uns im Berichtsjahr insgesamt drei Datenschutzverletzungen gemeldet. Diese Zahl erscheint angesichts der Vielzahl an öffentlichen und nicht öffentlichen Akteuren im Sozialbereich sehr klein. So passt es ins Bild, dass wir in einigen Verfahren durch Hinweise auf Datenschutzverletzungen aufmerksam gemacht wurden, bei denen wir unter anderem auch Verstöße gegen die Meldepflicht nach Artikel 33 Datenschutzgrundverordnung feststellten.

8.2 Unsichere Datenübermittlung durch Unternehmen im Bereich Seniorenassistenz und Seniorenbetreuung

Ein Unternehmen, dessen Dienstleistung darin besteht, pflegebedürftigen Personen eine ganztägige Betreuungskraft aus Osteuropa zu vermitteln, übermittelte personenbezogene Daten von Kundinnen und Kunden sowie von Beschäftigten über unsichere Kommunikationswege wie zum Beispiel unverschlüsselte E-Mails. Zudem war zum Zeitpunkt unseres Tätigwerdens eine rechtliche Grundlage für die Datenübermittlung an die osteuropäischen Vermittlungsagenturen nicht immer geschaffen. Aber das Unternehmen arbeitete nach. Vereinbarungen zur Auftragsverarbeitung wurden geschlossen und die Datenübermittlung erfolgt nunmehr auf sicherem Wege.

8.3 Unzulässige Erhebung des Beschäftigungszeitraums der Erziehungsberechtigten zur Prüfung des Betreuungsbedarfs

Wir erhielten den zutreffenden Hinweis, dass das für die Beantragung eines erhöhten Kinderbetreuungsbedarfs bereitgestellte Formular eines öffentlichen Trägers personenbezogene Daten der Erziehungsberechtigten abfragte, die über das gesetzlich Erforderliche hinausgingen. So musste der Arbeitgeber in dem Formular angeben, seit wann er die jeweilige Antragstellerin oder den jeweiligen Antragsteller beschäftigt. Dies führte regelmäßig dazu, dass nicht nur der Beginn, sondern auch das Ende der Beschäftigung eingetragen wurde und befristet Beschäftigte dadurch Nachteile erfuhren. Nachdem wir den öffentlichen Träger auf unsere datenschutzrechtlichen Bedenken aufmerksam gemacht hatten, passte dieser die Formulare an. Angaben in Bezug auf den Beginn der Beschäftigung müssen fortan nicht mehr vorgelegt werden.

8.4 Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte

Zuerst berichteten wir im 40. Jahresbericht unter Ziffer 8.9 über die Software zum Management der Flüchtlingsunterkünfte. In den folgenden Jahresberichten (2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 9.5 und 1. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 8.1) 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.

Anfang Januar 2021 erfuhren wir von der Senatorin für Soziales, Integration, Jugend und Sport, dass nun geplant sei, das Freitextfeld in Abstimmung mit dem Landesbehindertenbeauftragten durch Ankreuzfelder zu ersetzen. Informationen über die Essensausgabe würden weiterhin für 14 Tage gespeichert. Dadurch solle ermittelt werden, ob Personen, die einen Platz in der Unterkunft belegten, tatsächlich dort äßen und schliefen. Personen, die selten oder unregelmäßig zu den Essensausgaben erschienen, würden abgemeldet, um die Plätze neu vergeben zu können. Die Löschung der übrigen Daten (abgesehen von An- und Abwesenheiten und der Essensausgabe) erfolge nach zehn Jahren. Dabei orientiere man sich an den Aufbewahrungsfristen des Bundesamtes für Migration und Flüchtlinge und der Zentralen Aufnahmestelle für Asylbewerber und Flüchtlinge im Lande Bremen (ZASt).

Die angeführten Aufbewahrungsfristen sind mit dem uns vorliegenden Datenschutzkonzept und den darin aufgeführten Rechtsgrundlagen der Datenverarbeitung nicht vereinbar. Nach der nun eingegangenen Auskunft der senatorischen Behörde wird die Bewohner- und

Quartiersmanagementsoftware bereits seit Februar 2019 als Fachverfahren bei der ZASt genutzt. Diese Nutzungsänderung wurde uns bislang trotz mehrfacher Hinweise auf die Unvereinbarkeit mit den uns vorliegenden Dokumenten weder durch eine Überarbeitung des Datenschutzkonzepts noch im Rahmen der nach diesem Zeitpunkt erfolgten Ortsbesichtigung erläutert, was angesichts des nunmehr seit über drei Jahren bestehenden Kontakts in dieser Angelegenheit durchaus überrascht. Auch eine Rechtsgrundlage, welche die Verarbeitung der in der Software gespeicherten personenbezogenen Daten zu einem anderen Zweck, als demjenigen, zu dem sie ursprünglich erhoben wurden, erlaubt, wurde uns bislang nicht genannt.

9. Bildung

9.1 Gemeldete Datenschutzverletzungen

Im Bereich Schulen und Bildung gab es im Jahr fünf Meldungen von Verantwortlichen nach Artikel 33 der Datenschutzgrundverordnung. Es erreichten uns zudem diverse schriftliche und telefonische Anfragen von Betroffenen. Ein Großteil der Anfragen bezog sich auf Fragestellungen im Zusammenhang mit der besonderen Situation angesichts der seit März bestehenden Pandemielage, zum Beispiel im Hinblick auf die Pflicht zur Vorlage von Attesten, die Teilnahme an digitalem Fernunterricht und die Verwendung digitaler Lehrangebote als Bestandteil des Fernunterrichts.

9.2 Digitale Lernplattform

Uns erreichten verschiedene Anfragen zur Nutzung von itslearning. Dabei handelt es sich um eine bereits seit 2015 in Bremen genutzte webbasierte Lernplattform, die in vielen Schulen im Zusammenhang mit dem pandemiebedingten Distanzunterricht erstmals intensiver genutzt wurde. Vielfach stellte sich heraus, dass sich datenschutzrechtliche Probleme in erster Linie daraus ergaben, dass die Nutzerinnen und Nutzer in der Anwendung unerfahren waren. Dabei fiel auf, dass die programmierten Voreinstellungen der Plattform derartige Fehler zu begünstigen scheinen. Zudem stammt das bestehende Datenschutzkonzept aus dem Jahr 2015 und entspricht bereits seit längerem nicht mehr der aktuellen Rechtslage.

9.3 YouTube-Inhalt als verpflichtender Hausaufgabenbestandteil

Verschiedentlich wurde uns berichtet, dass auf dem US-amerikanischen Videoportal YouTube bereitgestellte Inhalte von Lehrkräften im Rahmen des Distanzunterrichts genutzt wurden. So wurde Schülerinnen und Schülern zum Beispiel ein Link zu einem dort veröffentlichten Video übersandt und ihnen aufgegeben, diesen im Rahmen der häuslichen Aufgabenbearbeitung (von einem privaten Gerät) aufzurufen und im Anschluss schriftlich Fragen zu dem Video zu

beantworten. Dies ist datenschutzrechtlich selbst dann unzulässig, wenn es sich nicht um Pflichtaufgaben handelt und die Nutzung über die im Land Bremen eingesetzte webbasierte Lernplattform itslearning geschieht. Bei Nutzung der Plattform YouTube werden von dieser diverse personenbezogene Daten der Nutzerinnen und Nutzer verarbeitet. Eine Erforderlichkeit der Nutzung in der geschilderten Form ist nicht ersichtlich. Ein zusätzliches Problem in diesem Zusammenhang ist die Übermittlung der erfassten Daten in die Vereinigten Staaten von Amerika.

9.4 Digitales Klassenbuch

Nach einer Pilotphase ist seitens der Senatorin für Kinder und Bildung geplant, allen bremischen Schulen anzubieten, Klassenbücher zukünftig digital zu führen. Genutzt werden soll ein Angebot einer österreichischen Firma. Die zugehörige Verfahrensbeschreibung wurde uns übersandt. Ein weiterer Austausch mit der zuständigen Behörde zu diesem Thema ist geplant.

9.5 Datenschutzwidriger Umgang mit Klassenbüchern in Papierform

Uns erreichte eine Eingabe bezüglich des Umgangs mit in Papierform geführten Klassenbüchern. Diese wurden in einem unverschlossenen und nur unregelmäßig beaufsichtigten Regal im Eingangsbereich einer Schule verwahrt, wenn sie nicht in Benutzung waren. Nach Beanstandung durch uns wurde das Regal zunächst nur mit einer Verschlussmöglichkeit versehen, die jedoch regelmäßig nicht genutzt wurde, auch wenn sich in dem Regal Klassenbücher befanden und das Regal unbeaufsichtigt war.

9.6 Videokonferenzsysteme im Schulkontext

Uns erreichten diverse Anfragen von Seiten aller betroffenen Parteien zur Nutzung von Videokonferenzsystemen im Rahmen des Distanzunterrichts. Die Verwendung von Videokonferenzsystemen zu Unterrichts- oder ähnlichen Zwecken im häuslichen Kontext ist datenschutzrechtlich hoch problematisch. Eine datenschutzkonforme Nutzung ist nur mit wirksamer Einwilligung möglich. Hierfür müssen insbesondere die Schülerinnen und Schüler und gegebenenfalls deren Sorgeberechtigte vor der erstmaligen Nutzung ausreichend über die Risiken aufgeklärt werden. Die Nutzung von Systemen, die personenbezogene Daten in die Vereinigten Staaten von Amerika übermitteln, birgt zusätzliche Probleme. Die von der Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder erarbeitete

Orientierungshilfe Videokonferenzsysteme[3] sowie die dazugehörige Checkliste[4] gilt auch in diesem Zusammenhang.

9.7 Unzulässiges schulisch organisiertes "Freundebuch" der Klasse

Uns erreichte eine Beschwerde darüber, dass an einer Grundschule von einer Lehrkraft als Teil des Unterrichts ein Buch geführt wurde, das den Schülerinnen und Schülern im wöchentlichen Wechsel mit nach Hause gegeben wurde. Die Kinder sollten in dem Buch eine Art Tagebucheintrag über ihr Wochenende erstellen und konnten auch Fotos oder ähnliches beifügen. Dies ist datenschutzrechtlich unzulässig. Durch die Weitergabe des Buches erhalten auch die Familien der Schülerinnen und Schüler, denen das Buch in der Folge mitgegeben wird, Zugriff auf die enthaltenen personenbezogenen Daten. Dabei besteht gerade bei Kindern im Grundschulalter die Gefahr, dass auch besonders sensible personenbezogene Daten Eingang in das Buch finden, wie etwa die Religionszugehörigkeit der Familie eines Kindes, wenn zum Beispiel ein sonntäglicher Kirchenbesuch geschildert würde. Zudem besteht die Gefahr, dass das Buch beim Transport abhandenkommt.

9.8 iPads für Schülerinnen und Schüler

Alle bremischen Schülerinnen und Schüler sollen sukzessive mit iPads ausgestattet werden. Die damit verbundenen datenschutzrechtlichen Fragestellungen und Risiken wurden mit Vertreterinnen und Vertretern des Landesinstituts für Schule und der Senatorin für Kinder und Bildung erörtert.

9.9 Nutzung eigener privater Endgeräte für schulische Zwecke

Die Nutzung privater Endgeräte wie Laptops, Tablets, Mobiltelefone für schulische Zwecke ("bring your own device") sollte im Zusammenhang mit der Verarbeitung personenbezogener Daten nach Möglichkeit vermieden werden. Die Bereitstellung dienstlicher beziehungsweise schulischer Geräte ist vorzuziehen. Eine Verpflichtung zur Nutzung privater Endgeräte ist unzulässig. Dabei ist angesichts der bestehenden Überordnungsverhältnisse und Unterordnungsverhältnisse sowohl im Beschäftigungskontext als auch im schulischen Bereich besondere Sorge dafür zu tragen, dass die für die Nutzung erforderlichen Einwilligungen nicht aufgrund einer bestehenden oder empfundenen Drucksituation für die Betroffenen unwirksam sind.

[3] https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf
[4] https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.docx

9.10 Online-Portal zur Leseförderung

Das Online-Portal Antolin wird von Lehrkräften häufig insbesondere im Grundschulbereich zum Zweck der Leseförderung eingesetzt. Dafür müssen die Kinder durch die Lehrkraft mit einem individuellen Benutzerkonto angemeldet werden. Es werden personenbezogene Daten der Schülerinnen und Schüler zum Leseverhalten sowie zum Nutzungsverhalten der Plattform erhoben. Dies ist zumindest ohne eine ausreichende Information der Schülerinnen und Schüler sowie deren Sorgeberechtigter und ohne eine hierauf basierende und vor der ersten Nutzung erteilte Einwilligung datenschutzrechtlich unzulässig.

9.11 Datenweitergabe für schulische Wettbewerbe an die Veranstalter

In einem uns berichteten Fall nahmen Schülerinnen und Schüler in der Unterrichtszeit an einem mathematischen Wettbewerb teil, für dessen Auswertung die Ergebnisse an den Veranstalter weitergegeben wurden. Dies ist ohne vorherige Einwilligung unzulässig, auch wenn nicht die Klarnamen der Schülerinnen und Schüler, sondern lediglich eine individuelle Kennziffer weitergegeben wird.

10. Beschäftigtendatenschutz

10.1 Gemeldete Datenschutzverletzungen

Insgesamt wurden im Bereich Beschäftigtendatenschutz im Jahr 2020 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit 15 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. Vielfach erreichten uns zudem zusätzlich telefonische Anfragen, insbesondere von Betroffenen, Personalvertretungen und Datenschutzbeauftragten. Diese hatten 2020 häufig ihren Hintergrund in mit der Pandemielage zusammenhängenden Fragen wie zum Beispiel der Nutzung von Videokonferenzsystem, der Nutzung privater Endgeräte und der Arbeitszeiterfassung im Homeoffice.

10.2 Microsoft 365

Angesichts fehlender Transparenz und einer Vielzahl von verschiedenen Modulen wie Microsoft Delve, MyAnalytics und Office Graph, die zumindest bei Beibehaltung der Ausgangskonfiguration diverse Nutzungsdaten erfassen und zumindest teilweise auch in die Vereinigten Staaten von Amerika übermitteln, erscheint ein datenschutzkonformer Einsatz von Microsoft 365 im Hinblick auf den Beschäftigtendatenschutz nur schwer möglich. Verantwortliche, die Microsoft 365 einsetzen, sind in der Pflicht, eine zu umfangreiche Verarbeitung personenbezogener Daten ihrer Beschäftigten durch konkrete Maßnahmen zu verhindern und dies im Zweifelsfall nachzuweisen.

10.3 Nutzung privater Endgeräte im Beschäftigungskontext

Die Nutzung privater Endgeräte durch Beschäftigte zur Erfüllung ihrer Arbeitspflichten oder Dienstpflichten (bring your own device) birgt nicht nur Datenschutzrisiken für die Betroffenen, deren personenbezogene Daten möglicherweise durch die Beschäftigten auf den privaten Geräten verarbeitet werden, sondern auch für die Beschäftigten selbst. Damit die Arbeitgeberin oder der Arbeitgeber seinerseits seinen datenschutzrechtlichen Kontrollpflichten nachkommen kann, muss er sich von den Beschäftigten Zugriffsrechte auf die privaten Endgeräte einräumen lassen. Zum Zweck der Installation von für die Tätigkeit benötigter Programme müssen die Beschäftigten zudem gegebenenfalls sogar Administratorenrechte für die Arbeitgeberin beziehungsweise den Arbeitgeber einräumen. Bei Zuschaltung in Netzwerke der Arbeitgeberin oder des Arbeitgebers können gegebenenfalls Daten über die Nutzung des privaten Geräts erhoben werden oder sogar Zugriffe auf die dort gespeicherten Inhalte erfolgen. Auch im Interesse des Beschäftigungsdatenschutzes sollte daher von der Nutzung privater Geräte zum Zweck der Erfüllung von Arbeitspflichten oder Dienstpflichten abgesehen werden.

10.4 Nutzung privater Telefonnummern im Rahmen von Heimarbeit und Telearbeit

Uns erreichten verschiedene Anfragen dazu, ob und inwieweit die Bekanntgabe privater Telefonnummern von Beschäftigten verlangt werden darf, wenn diese sich im Homeoffice befinden oder mobil arbeiten. Die Herausgabe der privaten Telefonnummer darf von Beschäftigten allenfalls dann gefordert werden, wenn sie alternativ auch an einem Ort arbeiten könnten, an dem sie mit einem dienstlichen Telefonanschluss ausgestattet sind, und wenn die Bekanntgabe gleichzeitig zur Erfüllung ihrer Pflichten aus dem Arbeitsverhältnis beziehungsweise Dienstverhältnis erforderlich ist. Letzteres wird regelmäßig nicht der Fall sein. Ein milderes Mittel ist in vielen Fällen die Zusendung einer Rückrufbitte über E-Mail.

10.5 OpenTouch Conversation in Behörden

Für die Behörden der Freien Hansestadt Bremen wurde im Berichtsjahr im Rahmen der Telefonieunterstützung das Rollout einer CTI-Software (OTC = OpenTouch Conversation) angestoßen. Diese Software bietet unter anderem neben der Telefoniefunktion auch eine Chatfunktion und die Möglichkeit der Bildschirmübertragung und des Teilens von Dokumenten. Zudem wird bei Beibehaltung der Voreinstellungen der Status der Beschäftigten als "Verfügbar", "Besetzt" oder "Abwesend" angezeigt. Ein diesbezügliches Datenschutzkonzept oder eine Dienstvereinbarung existieren unseres Wissens nicht.

10.6 Anfragen im Pandemiekontext

Uns erreichten diverse Anfragen von Beschäftigten und Personalvertretungen zum Umgang mit Kenntnissen zu Vorerkrankungen, mit Attesten und mit Krankmeldungen im Pandemiekontext. In einem Fall wurden beispielsweise Informationen aus einem Attest hinsichtlich gesundheitlicher Einschränkungen des Betroffenen an diejenigen weitergegeben, bei denen der Betroffenen eingesetzt wurde. In einem anderen Fall wurden aus einem anderen Kontext erlangte Kenntnisse des Arbeitgebers zu Vorerkrankungen des Beschäftigten dazu genutzt, diesen aufgrund von Vorerkrankungen gegen seinen Willen (vorgeblich zu seinem eigenen Schutz im Hinblick auf die Pandemiesituation) zu versetzen. Dies war jeweils datenschutzwidrig. Generell dürfen insbesondere Gesundheitsdaten nur aufgrund einer gesetzlichen Grundlage erhoben und weiterverarbeitet werden, wobei grundsätzlich eine strenge Zweckbindung zu beachten ist.

10.7 Digitale Aktivitätserfassung oder Statuserfassung

Die datenschutzrechtlich unzulässige vollständige Überwachung von Beschäftigten darf auch nicht durch Nutzung von digitalen Werkzeugen wie zum Beispiel automatischen Statusanzeigen oder die Verwendung von Programmen, die die Nutzung der Maus oder der Tastatur protokollieren, erfolgen. Auch hierzu erreichten uns insbesondere während der Pandemielage diverse Anfragen. Der Umstand, dass Beschäftigte von zu Hause aus oder mobil arbeiten, rechtfertigt kein höheres Maß an Überwachung.

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. Hingegen erhielten wir im Berichtszeitraum 45 Beschwerden, die sich auf Videoüberwachungen bezogen.

11.2 Schwerpunkte im Bereich Videoüberwachung

In über 50 Prozent der bei uns eingegangenen Beschwerden ging es um Überwachungskameras, die an Fassaden von Privathäusern, Geschäftshäusern und Eigentumswohnanlagen installiert waren, die sich unmittelbar an öffentlichen Straßen, Fußwegen und Radwegen befanden oder es ging um Fälle, in denen die Videoüberwachung direkt aus Fenstern erfolgte.

Die Verantwortlichen verfolgten in der Regel den Zweck durch die Installation der fraglichen Kameras ihr vor dem Gebäude geparktes Privatfahrzeug, Fahrrad oder Motorroller vor Vandalismus oder Diebstahl zu schützen und hatten die Kameras entsprechend auf diese Objekte ausgerichtet. Bei einem solchen Vorgehen wird übersehen, dass die betreffenden Verantwortlichen ihr Eigentum auf Zuwegungen, Fußwegen oder am Straßenrand abgestellt haben und mit ihren Kameras somit Bereiche überwachen, die allgemein zugänglich sind. Auch wenn den Überwachenden möglicherweise nicht bewusst ist, dass bereits eine einfache Überwachungsanlage im erheblichem Umfang personenbezogene Daten verarbeitet, ist die Installation dieser Anlagen rechtswidrig.

11.3 Veröffentlichung der Orientierungshilfe "Videoüberwachung durch nicht öffentliche Stellen"

In diesem Berichtszeitraum wurde die Orientierungshilfe "Videoüberwachung durch nicht öffentliche Stellen" grundlegend überarbeitet und an die neuen rechtlichen Rahmenbedingungen der seit dem 25. Mai 2018 geltenden Datenschutzgrundverordnung (DSGVO) angepasst. In der Orientierungshilfe[5] werden Betroffene und Verantwortliche darüber informiert, welche Rechtsgrundlagen anzuwenden sind und welche datenschutzrechtlichen Voraussetzungen für Videobeobachtungen oder Videoüberwachungen in unterschiedlichen Lebensbereichen jeweils gelten. Ebenso werden Formvorschriften und Dokumentationspflichten erläutert. Neu hinzugekommen sind die Abschnitte zur Überwachung in der Nachbarschaft und zur datenschutzrechtlichen Bewertung von Türkameras und Klingelkameras, Drohnen und Wildkameras sowie Dashcams. Im Anhang der Orientierungshilfe finden sich Musterhinweisschilder, die es den Verantwortlichen erleichtern, den Transparenzpflichten gemäß Artikel 12 fortfolgende DSGVO nachzukommen. Darüber hinaus wird hier eine Checkliste mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung bereitgestellt.

12. Wirtschaft und Gewerbe

12.1 Gemeldete Datenschutzverletzungen

Wie schon im Vorjahr erhielten wir von verantwortlichen Stellen aus den unterschiedlichsten Branchen insbesondere Meldungen aufgrund erfolgreicher Schadsoftware-Angriffe auf ihre IT-Infrastruktur mit (möglichem) Zugang zu und Abfluss von personenbezogenen Daten. Eindrücklich zeigt sich hieran, dass die immer weiter vorangetriebene Digitalisierung eben nicht nur Chancen bietet, sondern auch erhebliche Risiken mit sich bringt. Gegenstand weiterer Meldungen waren etwa ein Konfigurationsfehler eines Servers mit Zugriffsmöglichkeit

[5] https://www.datenschutz.bremen.de/sixcms/media.php/13/OH-V%DC_DSK-final.pdf

auf personenbezogene Daten und ein Fehlversand von Unterlagen aufgrund Adressverwechselung.

12.2 Datenumgang bei Postdienstleistern

Auch in diesem Berichtszeitraum erreichten uns wieder einige Beratungsbitten beziehungsweise Beschwerden zum Datenumgang bei Postdienstleistern. So wollte ein Paketzusteller den Personalausweis des Entgegennehmenden vollständig abfotografieren (unzulässig nach § 41 b Postgesetz), ein anderer wollte bei Paketaushändigung gar ein Foto des Empfängers anfertigen (nicht erforderlich), in einem weiteren Fall fror der Bedienungsbildschirm einer Selbstbedienungs-Paketstation nach Eingabe des Namens und der Unterschrift des Kunden aufgrund eines Fehlers der elektronischen Systemsteuerung ein, sodass diese Daten in der Folge über viele Stunden für Dritte einsehbar waren. Da Postdienstleister bei der Verarbeitung personenbezogener Daten kraft besonderer gesetzlicher Zuständigkeitsregelung im Postgesetz ausschließlich der Kontrolle und Aufsicht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterliegen, leiteten wir die entsprechenden Beschwerden zuständigkeitshalber dorthin weiter.

12.3 Fehlende Betroffenenauskünfte

Ein nicht unerheblicher Anteil der Beschwerdefälle entfiel auch in diesem Berichtszeitraum wieder auf tatsächliche oder auch nur 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: Eingehende Selbstauskunftsersuchen Betroffener werden nicht an die intern zuständige Stelle des verantwortlichen Unternehmens et cetera weitergeleitet.

In manchen Fällen wird das Auskunftsrecht ersichtlich auch als Mittel in einer privaten Auseinandersetzung genutzt, um dem Kontrahenten jedenfalls Aufwand und Mühe zu bereiten. Das Motiv der Geltendmachung des Auskunftsanspruchs ist jedoch rechtlich irrelevant. Das heißt, dass auch einem aus Verärgerung handelnden Selbstauskunftsersuchenden selbstverständlich die begehrte Auskunft erteilt werden muss. Etwas anderes gilt nur im rechtlichen Ausnahmefall eines offenkundigen Missbrauchs der Auskunftsrechtsposition.

12.4 Kontaktdatenerhebung zwecks Verfolgung von Corona-Infektionsketten

Die in Bremen zum Teil im Wochenrhythmus erlassenen Coronaverordnungen begründeten die Rechtspflicht zur flächendeckenden Erhebung von Personenkontaktdaten bei der Wahrnehmung von "Angeboten in geschlossenen Räumen". Auch die Klarstellungen in den Verordnungen, wonach die entsprechenden Datenerhebungen sich allein auf den Namen, eine Telefonnummer oder eine E-Mail-Adresse und den Zeitpunkt des Betretens und Verlassens der Einrichtung oder des Veranstaltungsortes beziehen, allein das zuständige Gesundheitsamt zum Abruf dieser Daten befugt ist, sofern es zur Infektionskettenverfolgung erforderlich ist, die Datenerhebung so erfolgen muss, dass Dritte keine Kenntnis von den Daten erlangen können, und die Daten nach drei Wochen (seit der Zweiundzwanzigsten Coronaverordnung vom 30. November 2020 sind es vier Wochen) gelöscht werden müssen, konnten die vielfachen Unsicherheiten hinsichtlich des Umfangs der zu erhebenden Informationen zu den Gästen, Kundinnen oder Kunden bei den Betreiberinnen und Betreibern der durch die Verordnung adressierten Einrichtungen nicht verhindern. Auch vermögen diese Konkretisierungen durch die Landesregierung die mittlerweile breit diskutierte Problematik der Ermöglichung weitreichender Einschritte per Verordnungen durch das Bundesinfektionsschutzgesetz nicht zu lösen. Auch aus datenschutzrechtlicher Sicht bedürfen wesentliche Eingriffe in das Recht auf Schutz personenbezogener Daten einer parlamentarischen Grundlage (siehe hierzu die Entschließung der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 3. April 2020 unter Ziffer 21.1 "Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie" sowie den Beschluss[6] vom 28. August 2020 [Lv 15/20] des Verfassungsgerichtshofs des Saarlandes).

In Reaktion auf diese öffentliche Diskussion über die mangelnde parlamentarische Einbindung verabschiedete der Bundesgesetzgeber am 18. November 2020 unter anderem § 28 a Bundesinfektionsschutzgesetz (BInfSchG) (siehe hierzu Ziffer 1. dieses Berichts), der deutlich bestimmter ist als § 28 BInfSchG, der "die zuständige Behörde" schlicht ermächtigt, "die besonderen Schutzmaßnahmen" zu treffen. § 28 a Absatz 1 BInfSchG zählt 17 Beispiele für "besondere Schutzmaßnahmen" auf, die "zur Verhinderung der Verbreitung der Coronavirus-Krankheit-2019 (COVID-19) für die Dauer der Feststellung einer epidemischen Lage von nationaler Tragweite nach § 5 Absatz 1 Satz 1 durch den Deutschen Bundestag" von den zuständigen Behörden getroffen werden können. Maßnahme Nummer 17 lautet: "Anordnung der Verarbeitung der Kontaktdaten von Kunden, Gästen oder Veranstaltungsteilnehmern, um nach Auftreten einer Infektion mit dem Coronavirus SARS-CoV-2 mögliche Infektionsketten nachverfolgen und unterbrechen zu können." Was den Umgang der Verantwortlichen mit den

[6] https://verfassungsgerichtshof-saarland.de/verfghsaar/dboutput.php?id=359&download=1

Kontaktdaten anbelangt, trifft § 28 a BInfSchG in Absatz 4 eine Regelung, die der der bremischen Verordnungen sehr ähnelt. Ob dies auch nach Auffassung der Rechtsprechung den Vorgaben von Parlamentsvorbehalt und Bestimmtheitsgrundsatz genügt, wird sich zeigen.

Im Land Bremen waren die Regelungen zur Kontaktdatenerhebung Quelle zahlreicher aufsichtsrechtlicher Prüfungen. Uns erreichten in diesem Zusammenhang allein 21 Beschwerden. Dabei erfuhren wir vor allem von Nachlässigkeiten im Hinblick auf den Schutz der erhobenen Kontaktdaten vor einer Kenntnisnahme durch unbefugte Dritte. In einem Fall meldete sich eine Beschwerdeführerin, deren in einem Restaurant hinterlassene Kontaktdaten von einem Angestellten zweckwidrig zur privaten Kontaktaufnahme verwendet worden waren. Richtiger Weise hatte sie in dieser Sache parallel bei der Polizei Strafanzeige erstattet. Mitunter wurde auch eine eigenhändige Unterzeichnung des Kontaktdatenformulars verlangt, obwohl dies rechtlich nicht vorgesehen ist und mit erheblichem Missbrauchspotenzial einhergeht.

12.5 Vermeintlich unbefugte Herausgabe des Kundenschriftverkehrs

Im Rahmen des Kaufs eines gebrauchten Personenkraftwagens kam es zu Unstimmigkeiten zwischen Käufer und verkaufendem Autohaus. Die Auseinandersetzung zwischen beiden Parteien erfolgte maßgeblich elektronisch. Schließlich wandte sich der Käufer an uns und beschwerte sich darüber, dass seine gesamte Kommunikation durch das Autohaus an eine ihm nicht näher bekannte dritte Person herausgegeben worden sei. Im Zuge unserer Nachforschungen stellte sich jedoch alsbald heraus, dass der angeblich nicht näher bekannte Dritte ein Freund oder jedenfalls guter Bekannter des Käufers war, der sich in dem Kaufvertragsstreit als Schlichter beziehungsweise Vermittler eingeschaltet und insoweit in die Auseinandersetzung involviert war. Ein Datenschutzverstoß war daher nicht festzustellen. Offensichtlich ging es vielmehr allein darum, uns in einer privaten Auseinandersetzung zum Nachteil des Autohauses zu instrumentalisieren. Leider haben wir in diesen Fällen mangels eigener Gebührenordnung keine rechtssichere Möglichkeit, eine abschreckende Missbrauchsgebühr zu verhängen.

12.6 Reinigungsdienstleistungen sind keine Auftragsverarbeitung

Ein Unternehmen aus der Reinigungsdienstleistungsbranche wandte sich im Berichtszeitraum an uns und bat um unsere Beratungshilfe: ein Auftraggeber habe verlangt, dass man einen Auftragsverarbeitungsvertrag unterzeichne; Begründung hierfür: möglicherweise würden bei der Reinigung von Büroräumen personenbezogene Daten zur Kenntnis genommen. Dies könne doch nicht richtig sein.

Auftragsverarbeiter wickeln für eine datenverantwortliche Stelle bestimmte, festgelegte Schritte oder Prozesse der Verarbeitung personenbezogener Daten ab. Ein Beispiel ist die Bereitstellung eines IT-Systems. Ein Reinigungsdienstleistungsunternehmen soll aber offenkundig gerade nur reinigen, nicht aber für die Auftraggeberin beziehungsweise für den Auftraggeber personenbezogene Daten verarbeiten. Das heißt, das auftraggebende Unternehmen hat durch entsprechende technische und organisatorische Vorkehrungen sicherzustellen, dass Beschäftigte seines Reinigungsdienstleisters gerade keine personenbezogenen Daten einsehen können. Nicht aber kann die unbefugte Einsichtnahme durch Reinigungspersonal hingegen durch einen Vertrag zur Auftragsverarbeitung quasi legalisiert werden

13. Kreditwirtschaft

13.1 Gemeldete Datenschutzverletzungen

Die Anzahl der Meldungen über Datenschutzverletzungen im Kreditwesenssektor lag auch in diesem Berichtszeitraum lediglich im niedrigen einstelligen Bereich. Gegenstand der Meldungen waren der Fehlversand von Kontoinformationen mittels einer elektronischen Nachricht an eine dritte Person, der Fehllauf eines postalischen Schreibens mit Kreditinformationen aufgrund eines Adressierungsfehlers, der Verlust eines mobilen Datenverarbeitungssystems und die Erteilung einer Betroffenenselbstauskunft mit Informationen zu einer dritten Person.

Mit der Kenntnisnahme von Betroffenendaten ist der Schaden für das Selbstbestimmungsrecht der Betroffenen regelmäßig bereits eingetreten und – mangels Löschbarkeit der Erinnerung des dritten Datenempfängers – in irreparabler Weise. Deshalb gilt es, möglichen Fehlerquellen bereits im Vorfeld durch effektive technische und organisatorische Schutzmaßnahmen soweit wie möglich zu begegnen.

13.2 Erhebung der Steueridentifikationsnummer des Mieters durch die Vermieterin

Eine Vermieterin wandte sich an uns, weil sie seitens ihres Kreditinstituts bei der Eröffnung eines Treuhandkontos zur Anlage der Mietkaution ihres Neumieters gebeten worden war, dessen Steueridentifikationsnummer mitzuteilen. Diese Abfrage, die nachvollziehbarerweise irritieren kann, war jedoch datenschutzrechtlich zulässig, denn die Abgabenordnung schreibt Kreditinstituten die Erhebung der Steueridentifikationsnummer auch in Bezug auf wirtschaftliche Berechtigte wie vorliegend den Mieter vor. Erhält das Kreditinstitut die Steueridentifikationsnummer nicht, ist es gesetzlich sogar verpflichtet, diese beim Bundeszentralamt für Steuern zu erfragen.

14. Versicherungswirtschaft

14.1 Gemeldete Datenschutzverletzungen

Im Bereich der Versicherungswirtschaft wurden auch im Jahr 2020 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit keine Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 Datenschutzgrundverordnung gemeldet. Wir müssen auch in diesem Bereich mit einer großen Zahl uns nicht gemeldeter Datenschutzverletzungen ausgehen.

14.2 Vertrauliche Kundengespräche einer Versicherungsagentur trotz mithörender Dritter

Ein Versicherungskunde beschwerte sich darüber, dass in einem Büro einer Versicherungsagentur unter Namensnennung sowohl persönlich als auch telefonisch vertrauliche Kundengespräche geführt wurden, obwohl dabei alle anderen wartenden Kundinnen und Kunden mithören konnten. Dabei wurden zum Teil auch Krankheitsfragen ausführlich erläutert.

Für die Durchführung von Kundengesprächen muss darauf geachtet werden, dass Kundinnen und Kunden für persönliche Gespräche ein separater Raum oder, wenn weitere Kundinnen beziehungsweise Kunden die Geschäftsstelle betreten, das laufende Gespräch mit der jeweiligen Kundin oder dem jeweiligen Kunden unterbrochen und ein Termin angeboten wird. Auch muss bei der Annahme von Telefonaten verhindert werden, dass andere Kundinnen und Kunden mithören können und Namen auf keinen Fall genannt werden. Verstöße gegen diese Grundsätze sind im Fall von Versicherungsagenturen besonders schwerwiegend, da hier sehr häufig besondere Kategorien personenbezogener Daten, wie zum Beispiel Gesundheitsdaten, verarbeitet werden.

15. Werbung und Adresshandel

15.1 Gemeldete Datenschutzverletzungen

In den Bereichen Werbung und Adresshandel wurden uns auch im Jahr 2020 von den in Frage kommenden Unternehmen keine Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. Aufgrund der hohen Anzahl an Werbeschreiben und der großen Datenmengen in entsprechenden Datenbanken halten wir es für sehr unwahrscheinlich, dass es im Berichtsjahr beispielsweise bei dem Versand nicht zu Falschkuvertierungen oder anderen Datenpannen kam, sodass wir davon ausgehen müssen,

dass es hier gleichwohl Verletzungen des Schutzes personenbezogener Daten gab, die uns hätten gemeldet werden müssen.

15.2 Unerwünschte Werbe-E-Mails trotz Abmeldung vom Newsletter

Kundinnen und Kunden eines Unternehmens beschwerten sich bei uns darüber, dass sie trotz Abmeldung vom Newsletter des Unternehmens und der eingegangenen Bestätigung der Deaktivierung weiterhin Werbung erhielten. Nach mehrmaligen Aufforderungen unsererseits erhielten wir die Stellungnahme, dass die Deaktivierung fälschlicherweise nicht richtig abgespeichert worden sei. Das Unternehmen änderte aufgrund der Beschwerde den entsprechenden Arbeitsprozess und führte ein Vier-Augen-Prinzip bei der Löschung aus dem E-Mail-Verteiler ein, sodass sich dieser Fehler bei diesem Unternehmen hoffentlich nicht wiederholen wird.

16. Bauen und Wohnen

16.1 Gemeldete Datenschutzverletzungen

Im Berichtsjahr 2020 erreichten uns drei Meldungen über die Verletzung des Schutzes personenbezogener Daten im Bereich Bauen und Wohnen. Dabei handelte es sich in zwei Fällen um Angriffe auf IT-Systeme in Büros von Maklerinnen und Maklern, in einem Fall um den Diebstahl eines Mitarbeiterlaptops.

16.2 Datenweitergabe durch die Hausverwaltung

Im letzten Jahresbericht berichteten wir über Beschwerden von Miteigentümerinnen und Miteigentümern darüber, dass Hausverwaltungen ihre über Namen und Wohnadressen hinausgehenden Kontaktdaten wie Telefonnummern und E-Mail-Adressen an die Wohnungseigentümergemeinschaft (WEG) und damit an allen übrigen Miteigentümerinnen und Miteigentümer weitergegebenen hatten, indem diese von ihnen verfasste an die Hausverwaltung adressierte Schreiben weiterleiteten (siehe hierzu 2. Jahresbericht nach der Datenschutzgrundverordnung, Ziffer 16.2). Aus unserer Sicht kann eine derartige Weitergabe dann zulässig sein, wenn sie im Rahmen der Einberufung einer Versammlung der Wohnungseigentümergemeinschaft und der Aufstellung der Tagesordnung erfolgt. Nach einer zwischenzeitlich veröffentlichten, allerdings nicht unumstrittenen Entscheidung des Amtsgerichts Mannheim[7], kann die Verwalterin beziehungsweise der Verwalter zwar auch verantwortliche Stelle im Sinne des Artikel 4 Nummer 7 Datenschutzgrundverordnung (DSGVO) sein – gegebenenfalls auch gemeinsam verantwortlich mit der Eigentümergemeinschaft (Artikel 26 DSGVO). Im genannten Rahmen betrachten wir die

[7] Amtsgericht Mannheim, Urteil vom 11. September 2019 – 5 C 1733/19 WEG.

Verwalterin beziehungsweise den Verwalter jedoch nicht als verantwortliche Stelle im Sinne der DSGVO. Verantwortlich und eigentlicher Empfänger der Schreiben ist vielmehr die Eigentümergemeinschaft selbst. Die Verwalterin beziehungsweise der Verwalter ist lediglich berechtigt, die Zustellungen für die Versammlung entgegenzunehmen. Diejenige Person, die Schriftsätze, Anträge oder ähnliches für die Versammlung einreicht, ist daher so zu stellen, als hätte sie ihre Schreiben direkt an die Gemeinschaft der Eigentümerinnen und Eigentümer adressiert.

16.3 Datenschutz im Maklergeschäft

Uns erreichten mehrere Beschwerden, Hinweise sowie die Meldung einer Datenschutzverletzung nach Artikel 33 Datenschutzgrundverordnung (DSGVO), die das Maklerwesen zum Gegenstand hatten. So beschwerte sich beispielsweise Bürgerinnen und Bürger über unerwünschte Kontaktaufnahmen durch Maklerinnen und Makler nach Bekundung von Interesse an einem inserierten Objekt, an den "Verkauf" ihrer Daten an andere "Maklerbüros" und über erfolgte Datenweitergaben im Allgemeineren. Als Vermittlerinnen und Vermittlern zwischen Verkäuferinnen und Verkäufern auf der einen und Käuferinnen und Käufern auf der anderen Seite nehmen Maklerinnen und Makler naturgemäß eine Verteilerfunktion ein – sie übermitteln Daten zwischen den beiden Gruppen sowie an weitere an der Abwicklung des Kaufgeschäfts Beteiligte (Notarinnen und Notare, Banken und so weiter). Die Daten, die Maklerinnen und Maklern vorliegen, können zudem besonders sensibel sein, auch wenn diese nicht zwangsläufig unter den besonderen Schutz des Artikel 9 DSGVO fallen. Dies ist etwa bei Informationen zur finanziellen Situation einer Kaufinteressentin oder eines Kaufinteressenten der Fall. Maklerinnen und Makler müssen auf dem Gebiet des Datenschutzes einschließlich der Datensicherheit daher besonders sensibilisiert sein. Diese Sensibilisierung scheint nach den gegenüber uns vorgetragenen Sachverhalten noch nicht bei allen im Maklergeschäft Tätigen erfolgt zu sein.

16.4 Luftbildaufnahmen

Anlässlich einer Beschwerde eines Bürgers und einer Beratungsanfrage des Landesamt GeoInformation Bremen haben wir uns mit den Fragen beschäftigt, ob und gegebenenfalls unter welchen Voraussetzungen die Erstellung von Luftbildaufnahmen durch Vermessungs- und Katasterämter zulässig ist und ob die erstellten Aufnahmen Dritten zur Verfügung gestellt werden dürfen. Die Erstellung von Luftbildaufnahmen stellt dabei regelmäßig eine Verarbeitung personenbezogener Daten dar, genau wie auch die Speicherung der Aufnahmen und deren Übermittlung an Dritte. Die bremische Rechtslage (insbesondere das Vermessungs- und Katastergesetz sowie das Geodatenzugangsgesetz) lassen die Erstellung, Speicherung und Übermittlung von Luftbildaufnahmen unter Beachtung der normierten Voraussetzungen grundsätzlich zu. Von den verantwortlichen Stellen muss vor der

Durchführung von "Bildflügen" oder ähnlichen Aktionen jedoch ein Weg gefunden werden, alle potenziellen Betroffenen in geeigneter Weise im Sinne des Artikel 13 Datenschutzgrundverordnung über die beabsichtigten Verarbeitungsvorgänge zu informieren. In Betracht kommen dafür etwa Schreiben an alle Haushalte. Angesichts der hohen Anzahl Betroffener kann dies unter Umständen schwierig sein, weshalb Mitteilungen in Regionalzeitungen das adäquate Mittel sein können.

Die Zulässigkeit der Erstellung von Luftbildaufnahmen ergibt sich aus der bremischen Rechtslage, insbesondere den speziellen Regelungen im bremischen Vermessungs- und Katastergesetz. Ohne diese speziellen Regelungen wäre die Erstellung unzulässig, sie kann vor allem nicht auf die sogenannte "Generalklausel" des Bremischen Ausführungsgesetzes zur EU-Datenschutzgrundverordnung gestützt werden, wenngleich fälschlicherweise und für uns nicht mehr nachvollziehbar – inzwischen aber richtiggestellt – unsere Stellungnahme derart interpretiert ihren Weg nach Hamburg gefunden haben soll.

17. Verkehr und Umwelt

17.1 Gemeldete Datenschutzverletzungen

Im Bereich Verkehr und Umwelt wurde zwei Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet. Es handelte sich dabei um einmal um eine Meldung falsch adressierter Schreiben durch ein Logistikunternehmen, bei der anderen Meldung um einen Fall des Phishings (Mailserver), ebenfalls bei einem Logistikunternehmen.

17.2 Ausbau A 281 – Datenweitergabe durch Projektverantwortliche

Im Rahmen der Bearbeitung einer Beschwerde über eine Weitergabe personenbezogener Daten im Zuge des Ausbaus der Autobahn 281 (A 281) durch einen privaten Projektverantwortlichen zeigte sich, dass die datenschutzrechtliche Verantwortlichkeit zwischen den Beteiligten öffentlichen wie privaten Stellen augenscheinlich ungeklärt ist. Unabhängig von der Frage, ob die Datenweitergabe in rechtmäßiger Weise erfolgte, besteht nach unserer Einschätzung hier insbesondere seitens der betroffenen öffentlichen Stellen großer Handlungsbedarf. Es muss sichergestellt sein, dass die Verantwortlichkeit zwischen den beteiligten öffentlichen Stellen untereinander, vor allem aber zwischen öffentlichen und privaten Stellen geklärt ist und durch gegebenenfalls erforderliche vertragliche Vereinbarungen (einen Vertrag zur gemeinsamen Verantwortlichkeit nach Artikel 26 Datenschutzgrundverordnung [DSGVO] oder einen Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO) auch rechtlich abgesichert und festgehalten sowie gegenüber den Betroffenen im Rahmen der Informationspflichten offengelegt wird. Eine ungeklärte und ungeregelte datenschutzrechtliche Verantwortlichkeit kann nicht nur zur Unzulässigkeit einzelner

Verarbeitungsvorgänge führen, sondern insgesamt die (Grund-)Rechtspositionen der Betroffenen und deren Durchsetzbarkeit schwächen (siehe hierzu Ziffer 5.8 dieses Berichts).

17.3 Kennzeichenerfassung in Parkhäusern

Vermehrt wird in Parkhäusern mit Kennzeichenerfassungssystemen gearbeitet. Hierauf bezogen sich bei uns eingegangene Beratungsanfragen verschiedener Unternehmen, die zum Teil die Einführung derartiger Systeme auch im Bundesland Bremen beabsichtigten. Diese Systeme ermöglichen ein schrankenloses Parken oder aber zumindest eine schnellere Abwicklung von Parkvorgängen und eine Verhinderung von missbräuchlicher Inanspruchnahme etwaiger günstigerer Regeln im Falle eines vermeintlichen Parkticketverlustes. Der Einsatz von Kennzeichenerfassungssystemen ist unter Beachtung datenschutzrechtlicher Anforderungen zulässig. Zu diesen Anforderungen gehören etwa die Festlegung und strikte Beachtung kurzer Speicherfristen, eine möglichst hohe Datensicherheit, etwa durch die Datenspeicherung auf eigenen Servern, sowie die Herstellung von Transparenz.

18. Telemedien

18.1 Gemeldete Datenschutzverletzungen

Im Bereich Telemedien wurden im Berichtsjahr 14 Datenschutzverletzungen nach Artikel 33 Datenschutzgrundverordnung gemeldet.

18.2 Koordinierte Prüfung der Webseiten von Medienunternehmen

Zu Beginn des Berichtsjahres beschlossen zehn Datenschutzaufsichtsbehörden der Länder, zu denen auch die bremische Landesbeauftragte für Datenschutz und Informationsfreiheit gehörte, die Webseiten von Medienunternehmen in einer koordinierten Prüfung zu untersuchen. Die für diese Prüfung genutzten Kriterien und Methoden wurden gemeinsam erarbeitet. Kurz nach Versand der Anschreiben durch die beteiligten Aufsichtsbehörden schloss sich eine weitere Aufsichtsbehörde der Prüfung an. Bezüglich der angeschriebenen bremischen Medienanbieter befinden wir uns derzeit in der Auswertungsphase.

18.3 Überprüfung des Einsatzes von Analyse-Tools

Seit dem Inkrafttreten der Datenschutzgrundverordnung erreichten uns zunehmend Beschwerden, die den Einsatz von Analyse-Tools auf Webseiten bremischer Stellen kritisieren. Wir sammelten diese zahlreichen Beschwerden zunächst und nahmen sie im Berichtsjahr zum Anlass, die jeweiligen Webseitenbetreiber zu kontaktieren und uns die Verarbeitung personenbezogener Daten durch ein weit verbreitetes Analyse-Tool zu schildern.

Nach Eingang der Antworten prüfen wir diese und werden erforderlichenfalls Maßnahmen ergreifen, um anhaltende datenschutzrechtliche Verstöße zu unterbinden. Gegenwärtig befinden wir uns noch in der Phase der Auswertung der Antworten. Aufgrund neuer Beschwerden steigt die Anzahl der angeschriebenen Webseitenbetreiber kontinuierlich.

18.4 Anordnung gegen facebook-Fanpage-Betreiber

Uns erreichte eine Beschwerde über einen in Bremen ansässigen facebook-Fanpage-Betreiber, der sich als "Person des öffentlichen Lebens" sieht, und auf seiner Fanpage über seine Aktivitäten und Angebote informiert und seinen "Fans" die Möglichkeit des Austausches bietet. Ein Besucher der Fanpage, der auch auf dieser kommuniziert hatte, begehrte vom Fanpage-Betreiber die Löschung seiner personenbezogenen Daten. Spätestens seit dem 2018 ergangenen Urteil des Europäischen Gerichtshofs zu facebook-Fanpages steht fest, dass Betreiberinnen und Betreiber von Fanpages gemeinsam mit facebook für die Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher der Seiten verantwortlich sind. Da der Fanpage-Betreiber dem Begehren des Beschwerdeführers nur unzureichend nachgekommen war, erließen wir unsere erste Anordnung gegen einen Fanpage-Betreiber. Wir verpflichteten ihn zum einen, dem Löschungsbegehren nachzugehen, indem er dieses zumindest mittels der dazu von facebook zur Verfügung gestellten Infrastruktur an facebook weiterleitet. Weiterhin verpflichteten wir ihn, künftig ausreichende Datenschutzinformationen zur Verfügung zu stellen, damit alle Nutzerinnen und Nutzer, welche die Fanpage aufrufen, sich über ihre Rechte informieren können und wissen, an wen sie sich zur Geltendmachung ihrer Rechte wenden müssen. Betreiberinnen und Betreiber einer Fanpage müssen sich der gemeinsamen Verantwortlichkeit bewusst sein, die besteht, obwohl sie nicht alle Datenverarbeitungsvorgänge bei facebook nachvollziehen und erkennen können.

18.5 Hackerangriff gegen Cloud-Software-Anbieter für Gastronomie

Anfang August gelang es Mitgliedern des Chaos Computer Clubs, über eine Sicherheitslücke Zugriff auf das Cloud-System eines Bremer Dienstleisters für gastronomische Betriebe zu erhalten. Dort lagen Millionen von Datensätzen, unter denen sich auch Reservierungsdaten und Corona-Kontaktdaten aus dem Gastronomiebereich befanden. Um gegenüber dem Betreiber den Zugang nachweisen zu können, sicherte der Chaos Computer Club einige dieser Datensätze und setzte sich mit diesem in Kontakt. Nachdem die Sicherheitslücke behoben worden war, informierte uns der Dienstleister über den Angriff. Im Zuge der Prüfung stellten wir fest, dass die Kundinnen und Kunden einen Auftragsverarbeitungsvertrag mit dem Dienstleister geschlossen hatten und die gastronomischen Betriebe datenschutzrechtlich Verantwortliche nach der Datenschutzgrundverordnung (DSGVO) sind. Die Pflicht, den Hackerangriff zu melden liegt demnach in der Verantwortung der Kundinnen und Kunden des

Dienstleisters. Unsere Behörde übermittelte die Listen der betroffenen Kundinnen und Kunden an die zuständigen Aufsichtsbehörden und begann, diejenigen im Land Bremen ansässigen Kundinnen beziehungsweise Kunden des Dienstleisters zu kontaktieren, die uns keine Datenschutzverletzung nach Artikel 33 DSGVO gemeldet hatten. Der Vorgang ist aktuell noch in Bearbeitung.

18.6 Datenschutz auf Erotikportalen

Kontinuierlich gehen bei uns Beschwerden und Hinweise ein, die sich auf die Datenverarbeitung durch Betreiberinnen und Betreiber von Erotikportalen beziehen. Dabei geht es etwa um die ungewollte Zusendung von Werbung, die unzureichende Beantwortung von Auskunftsbegehren, die überlange Speicherung von Vertragsdaten und die Veröffentlichung von vermeintlich gelöschtem Videomaterial. So unterschiedlich der Sitz der Betreiberinnen und Betreiber der Erotikportale im geografischen Sinne ist, so unterschiedlich ist auch die geografische Herkunft derjenigen, die sich bezogen auf die Betreiberinnen un Betreiber im Land Bremen an uns wenden. Sie kommen aus Bremen, anderen Bundesländern und dem deutschsprachigen Ausland. Allen Betroffenen ist gemeinsam, dass sie in den meisten Fällen berechtigte Zweifel an der Rechtmäßigkeit des Umgangs mit personenbezogenen Daten durch Betreiberinnen und Betreiber von Erotikportalen haben. Hierbei ist wichtig, dass es sich bei Daten zum Sexualleben um besondere personenbezogene Daten nach Artikel 9 Datenschutzgrundverordnung handelt und die Betroffenen häufig in der Hoffnung, eine Partnerin oder einen Partner zu finden, höchst intime Daten preisgegeben. Betreiberinnen und Betreiber von Erotikportalen müssen die Nutzerinnen und Nutzer in transparenter Form über die Verarbeitung dieser Daten informieren und sich strikt an die Vorgaben des Datenschutzrechts halten. Unsere Erfahrung zeigt, dass sie dabei in vielerlei Hinsicht Nachholbedarf haben.

19. Internationales und Europa

19.1 EU-U.S. Privacy Shield – Urteil des Europäischen Gerichtshofs

Am 16. Juli 2020 erklärte der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der Kommission für die Vereinigten Staaten von Amerika (USA) für ungültig[8]. Ab diesem Zeitpunkt durften keine Übermittlungen personenbezogener Daten in die USA auf Artikel 45 Absatz 1 Datenschutzgrundverordnung (DSGVO) gestützt werden.

[8] Das Urteil ist abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst

Der EU-U.S. Privacy Shield war am 12. Juli 2016 in Kraft getreten, nachdem die Vorgängerregelung, das Safe-Harbor-Abkommen, am 6. Oktober 2015 vom EuGH für ungültig erklärt worden war (siehe hierzu 38. Jahresbericht, Ziffer 15.2). Grundlegende Kritikpunkte am Safe-Harbor-Abkommen konnte aber auch der EU-U.S. Privacy Shield nicht ausräumen (siehe hierzu 40. Jahresbericht, Ziffer 14.3). Der bereits damals an Bremer Unternehmen gegebene Hinweis, sich über andere Möglichkeiten des Datentransfers in die USA Gedanken zu machen und entsprechende technische Vorkehrungen zu treffen, ist durch das Urteil des EuGH wichtiger denn je geworden.

Eine Möglichkeit, personenbezogene Daten in Länder außerhalb der Europäischen Union zu übermitteln, können Standarddatenschutzklauseln bieten, sofern diese aus geeigneten Garantien bestehen (siehe Artikel 46 Absatz 2 Buchstabe c DSGVO). Der EuGH hat in seinem Urteil jedoch verdeutlicht, dass Datenexporteure die Übermittlung personenbezogener Daten aussetzen oder beenden müssen, wenn sie keine hinreichenden zusätzlichen Maßnahmen ergreifen können, um den notwendigen Schutz personenbezogener Daten zu gewährleisten.

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[9] und trifft verbindliche Beschlüsse in Einzelfällen.

21. Die Entschließungen der Datenschutzkonferenzen im Jahr 2020

21.1 Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 3. April 2020)

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht

[9] online unter https://edpb.europa.eu/our-work-tools/consistency-findings_de

auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutzgrundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

- Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.

- Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.

- Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder – wie eine vorherige Anonymisierung – sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung – **außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

- Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.

- Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können. Das europäische Datenschutzrecht verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. **Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten** sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

21.2 Polizei 2020 – Risiken sehen, Chancen nutzen!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16. April 2020)

Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 besteht die Chance, bisherige datenschutzrechtliche Defizite zu beseitigen und den Datenschutz nachhaltig zu verbessern. Die Polizeibehörden in Bund und Ländern haben einen ersten "fachlichen Bebauungsplan" für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßt dies ausdrücklich. Sie vermisst aber ausreichende Vorschläge, wie das Projekt den Datenschutz stärken will. Die Konferenz fordert deshalb, die Ziele und Meilensteine des Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.

Aus Sicht der Datenschutzbehörden sind vorrangig folgende Ziele in den Blick zu nehmen:

1. Umfassende Bestandsaufnahme

Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Sie hat insbesondere nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

2. Rechtliche Leitplanken

Mit dem neuen "Datenhaus" in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

3. Zwecktrennung

Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Dies ist der Kern des Datenschutzrechts. Deshalb muss das neue System präzise zwischen den verschiedenen Verarbeitungszwecken Aufgabenerfüllung, Dokumentation und Vorsorge trennen. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden oder als Auswerteplattform und Rechercheplattform genutzt werden.

4. Verbesserung der Datenqualität

Wenn die Polizeibehörden die IT-Struktur neu aufstellen, müssen sie alle Chancen nutzen: Sie müssen vorhandene Datenbestände bereinigen, unnötige Daten aussondern und die Qualität der Daten sichern. Dies gilt auch, wenn alte Daten in die neuen Systeme übertragen werden. Datenschutzkontrollen haben aufgezeigt, dass dies erforderlich ist. Beispiel ist die Falldatei Rauschgift.

5. Datenschutzspezifische Basisdienste

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als "Basisdienste" zu implementieren. Notwendig sind zum Beispiel ein "Basisdienst Zwecktrennung", ein "Basisdienst Datenqualität" und ein "Basisdienst Aufsicht und Kontrolle".

21.3 Registermodernisierung verfassungskonform umsetzen!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26. August 2020)

Mit dem Gesetz zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung (enthalten im Registermodernisierungsgesetz – RegMoG) plant die Bundesregierung eine Modernisierung der in der Verwaltung geführten Register. Hierzu soll unter anderem eine Identifikationsnummer (ID-Nr.) für natürliche Personen als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern eingeführt werden.

Als übergreifendes Ordnungsmerkmal soll die Steuer-Identifikationsnummer (Steuer-ID) dienen, vor deren fortschreitend ausgedehnter Nutzung die Datenschutzbeauftragten des Bundes und der Länder mehrfach deutlich gewarnt hatten. Die nun geplante ausgedehnte Verwendung der Steuer-ID als einheitliches Personenkennzeichen löst sich vollständig von ihrer ursprünglichen Zweckbestimmung für rein steuerliche Sachverhalte, obwohl sie nur deswegen bislang als verfassungskonform angesehen werden kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies bereits in ihrer Entschließung vom 12. September 2019 darauf hin, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennzeichen beziehungsweise Identifikatoren (auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch) die Gefahr birgt, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können.

Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen seit jeher enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang der geplanten Regelung zeigt das Potential der möglichen missbräuchlichen Verwendung.

So verknüpft der Gesetzentwurf bei mehr als 50 Registern die Steuer-ID als zusätzliches Ordnungsmerkmal. Auf diese Weise könnten Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden. Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern. Diese stellen zwar sicher, dass nur autorisierte Behörden die erforderlichen Daten Ende-zu-Ende verschlüsselt übermitteln. Sie bieten aber keinen ausreichenden Schutz gegen die missbräuchliche Zusammenführung der Daten zu einer Person, die aus unterschiedlichen Registern stammen, übrigens auch nicht bei Datenlecks.

Zudem ist damit zu rechnen, dass die neue ID-Nr. auch im Wirtschaftsleben weite Verbreitung finden wird, was das Missbrauchsrisiko weiter erhöht.

Die Datenschutzkonferenz hatte demgegenüber "sektorspezifische" Personenkennziffern gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren.

Obwohl ein solches Modell in der Republik Österreich seit vielen Jahren erfolgreich praktiziert wird, hat die Bundesregierung dies nie ernsthaft erwogen und ohne überzeugende Begründung mit dem pauschalen Verweis auf "rechtliche, technische und organisatorische Komplexität" abgelehnt.

Auch wenn die Corona-Pandemie zeigt, wie notwendig eine Beschleunigung der Digitalisierung ist, darf dies nicht als Argument dafür benutzt werden, verfassungsrechtlich notwendige Nachbesserungen unter Hinweis auf den "Eilbedarf" unter den Tisch fallen zu lassen.

Die Datenschutzkonferenz weist daher nochmals darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie fordert deshalb die Bundesregierung dazu auf, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.

21.4 Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 1. September 2020)

Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (EPA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen.

Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden.

Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutzgrundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der EPA am 1. Januar 2021 die volle Hoheit

über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten EPA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der EPA für alle Versicherten datenschutzgerecht auszugestalten.

Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der EPA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten et cetera) in der elektronischen Patientenakte gespeicherten Daten zu einem "alles oder nichts" gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.

Erst ein Jahr nach dem Start der EPA, das heißt ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre EPA geeignete Endgeräte (Smartphone, Tablet et cetera) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (das heißt sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die EPA und die "Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus". Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektronischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (Bundesrat-Drucksache 164/1/20, siehe Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 fortfolgende SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der EPA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der

Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der EPA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

21.5 Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 22. September 2020)

Der Begriff "Digitale Souveränität" wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[10] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Artikel 1 Datenschutzgrundverordnung (DSGVO) formulierten Ziele im Einklang mit den in Artikel 5 DSGVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten "Strategischen Marktanalyse"[11] beeinträchtigt, "da die Geschäftsbeziehungen der öffentlichen Verwaltung mit

[10] Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t

[11] PwC Strategy& (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter

externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Danach resultieren diese Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten." Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.

Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der "Strategischen Marktanalyse" empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sichergestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,

- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und

- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen — sowohl bei der Auswahl als auch im laufenden Betrieb:

---

https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

- Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.

- Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.

- Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.

2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:

    - Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.

3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:

    - Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft Systemsoftware und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.

4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:

    - Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.

- Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).

5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:

   - Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Artikel 25 DSGVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten "Verwaltungscloud", ist es eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

21.6 Datenschutz braucht Landgerichte auch erstinstanzlich

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 22. September 2020)

Mit dem *"Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens"* (Bundesrats-Drucksache 107/20 (B)) will der Bundesrat die erstinstanzliche Zuständigkeit der Landgerichte für Geldbußen nach der Datenschutzgrundverordnung (DSGVO) über 100.000 Euro streichen. Selbst über Geldbußen in dieser Höhe sollen künftig die Amtsgerichte entscheiden.

Das Ziel der Effektivierung des Bußgeldverfahrens wird mit dem geplanten Gesetz jedoch nicht erreicht werden. Der Gesetzentwurf verkennt in eklatanter Weise die besondere

wirtschaftliche, technische und rechtliche Komplexität von DSGVO-Geldbußen. Eine Streichung der landgerichtlichen Zuständigkeit würde die Amtsgerichte zudem nicht etwa entlasten, sondern noch stärker als bisher belasten.

Das Sanktionsrecht der DSGVO ist — anders als der Bundesrat unterstellt — mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten wie etwa Geldbußen im Straßenverkehr in keiner Weise vergleichbar. Es geht hierbei nicht etwa um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können teils Millionen von Kundendaten betroffen sein. Datenschutz-Ordnungswidrigkeiten mit Geldbußen über 100.000 Euro weisen wirtschaftlich und technisch eine besondere Komplexität auf und bedürfen daher einer Würdigung durch den Spruchkörper eines Kollegialgerichts. Sie sind viel eher mit Wirtschaftsstrafsachen vergleichbar, die ohnehin den Landgerichten zugewiesen sind. Nicht ohne Grund hat sich der europäische Gesetzgeber bei den Bußgeldvorschriften der DSGVO am Kartellrecht orientiert. Für ähnlich komplexe Ordnungswidrigkeiten in Kartellangelegenheiten ist in Deutschland sogar eine Zuständigkeit der Oberlandesgerichte gegeben. Diese Wertung kommt auch in dem insoweit eindeutigen Wortlaut von § 41 Absatz 2 Satz 1 Bundesdatenschutzgesetzes (BDSG) zum Ausdruck, der eine entsprechende Anwendung der Vorschriften über das Strafverfahren und damit auch eine Besetzung der Strafkammern als sogenannte große Bußgeldkammern entsprechend § 76 Gerichtsverfassungsgesetz (GVG) vorsieht.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert daher die Beibehaltung der landgerichtlichen Zuständigkeit für DSGVO-Geldbußen über 100.000 Euro und warnt vor einer Streichung der Vorschrift und deren Folgen.

21.7 Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. November 2020)

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) tritt Forderungen der Regierungen der Mitgliedstaaten der Europäischen Union entgegen, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Als Reaktion auf jüngste Terroranschläge soll diesen Behörden und Diensten der Zugriff auf die verschlüsselte Kommunikation ermöglicht werden. Dies umfasst insbesondere auch Messenger-Dienste wie

WhatsApp, Threema oder Signal. Nach dem Resolutionsentwurf "Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" des Rates der Europäischen Union (Nummer 12143/1/20 vom 6. November 2020) sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.

Eine sichere und vertrauenswürdige Verschlüsselung ist essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Eine Schwächung der Verschlüsselungsverfahren könnte jedoch europäische Unternehmen im globalen Markt benachteiligen. Bürgerinnen und Bürger müssen auf eine sichere und integre Nutzung digitaler Verwaltungsleistungen vertrauen können und benötigen hierbei Schutz vor umfassender Überwachung und Datenmissbrauch. Auch die Ziele des Onlinezugangsgesetzes, Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.

Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in Drittländer gemäß den Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des Europäischen Datenschutzausschusses als Reaktion auf das "Schrems II"-Urteil des Europäischen Gerichtshofs.

Würden die Vorschläge des Rates der Europäischen Union umgesetzt, würde eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört, ohne dass das angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden zu verbessern, nachhaltig und effektiv erreicht wird. Hintertüren in Verschlüsselungsverfahren stellen die Sicherheit und Wirksamkeit dieser gänzlich in Frage. Die Aushöhlung von Verschlüsselungslösungen würde zudem unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten.

Gleichzeitig würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.

Aus gutem Grund hat sich die Bundesregierung bereits im Jahr 1999 in den Leitlinien deutscher Kryptopolitik zum Einsatz kryptographischer Verfahren bekannt. In Europa wird die Vertraulichkeit der Kommunikation durch das individuelle Recht auf Achtung der Kommunikation in Artikel 7 Charta der Grundrechte der Europäischen Union (GRCh) geschützt. Ergänzend greift für gespeicherte Kommunikationsinhalte das in Artikel 8 GRCh garantierte Recht auf Schutz personenbezogener Daten. In Deutschland wird der Grundrechtsschutz beim Einsatz von Kommunikationsdiensten durch das Fernmeldegeheimnis in Artikel 10 Grundgesetz und ergänzend durch das Recht auf

informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation.

Die Datenschutzkonferenz sieht keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.

Die Datenschutzkonferenz hat sich wiederholt für den Einsatz sicherer und integrer Verschlüsselung eingesetzt und auf die Unverzichtbarkeit vertrauenswürdiger und integrer Kommunikationsmöglichkeiten hingewiesen. Sie fordert erneut die Bundesregierung und die deutsche EU-Ratspräsidentschaft auf, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten. Sichere Ende-zu-Ende-Verschlüsselung muss die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integre Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

21.8 Betreiber von Webseiten benötigen Rechtssicherheit – Bundesgesetzgeber muss europarechtliche Verpflichtungen der "ePrivacy-Richtlinie" endlich erfüllen

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. November 2020)

Der Gesetzgeber ist verpflichtet, die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 (RL 2018/1972/EU) bis zum 20. Dezember 2020 umzusetzen.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Gesetzgeber auf, endlich Regelungen zu erlassen, um die ePrivacy-Richtlinie[12] vollständig und im Einklang mit der Datenschutzgrundverordnung (DSGVO) umzusetzen.

Die DSK hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Artikel 5 Absatz 3 ePrivacy-Richtlinie nicht oder nicht ordnungsgemäß umgesetzt

[12] Richtlinie 2002/58/EG in der letzten Änderung durch die Richtlinie 2009/136/EU

hat.[13] Das Urteil des Bundesgerichtshofs (BGH) vom 28. Mai 2020 (I ZR 7/16 – "Planet49") verstärkt nach Auffassung der DSK den seit langem bestehenden, dringenden Handlungsbedarf.

Die DSK hat bereits im April 2018 in der Positionsbestimmung "Zur Anwendbarkeit des TMG für nicht öffentliche Stellen ab dem 25. Mai 2018" den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes (TMG) neben der Datenschutzgrundverordnung (DSGVO) nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht.[14]

Der BGH hatte im Planet49-Verfahren einen Streit zu entscheiden, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbrauchern mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Nach dem Wortlaut des § 15 Absatz 3 TMG wäre ein solches Vorgehen dann zulässig, wenn die betroffenen Personen entsprechend informiert wurden und nicht widersprochen haben (sogenannte Widerspruchslösung). Mit Blick auf Artikel 5 Absatz 3 ePrivacy-Richtlinie legt der BGH § 15 Absatz 3 TMG dahingehend aus, schon in dem Fehlen einer wirksamen Einwilligung könne ein solcher Widerspruch gesehen werden, weshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung von § 15 Absatz 3 TMG wendet er diese Vorschrift neben der DSGVO an. Letztlich ist der BGH der Vorabentscheidung des Europäischen Gerichtshofs gefolgt und bestätigt das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies.

Schon die Tatsache, dass die DSK und der BGH bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.

Mit der Entscheidung wird die Abgrenzung der Regelungsbereiche zwischen ePrivacy-Richtlinie, DSGVO und den Datenschutzvorschriften des TMG deutlich erschwert. Der BGH stellt ausdrücklich heraus, dass ePrivacy-Richtlinie und DSGVO unterschiedliche Schutzrichtungen verfolgen. Die Vorschriften in den §§ 12 bis 15 TMG knüpfen ausdrücklich

---

[13] Siehe Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 5. Februar 2015, abrufbar unter:
https://www.datenschutzkonferenz-online.de/media/en/20150205_en_Entschliessung_Cookies.pdf

[14] Positionsbestimmung der DSK vom 26. April 2018 "Zur Anwendbarkeit des TMG für nicht öffentliche Stellen ab dem 25. Mai 2018", abrufbar unter:
https://www.datenschutzkonferenz-online.de/anwendungshinweise.html,
Orientierungshilfe für Anbieter von Telemedien, abrufbar unter:
https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

an den Begriff der Verarbeitung personenbezogener Daten an. Diese Materie ist auf europäischer Ebene weitgehend abschließend durch die Datenschutzgrundverordnung geregelt. Artikel 5 Absatz 3 ePrivacy-Richtlinie hat hingegen auch Informationen ohne Personenbezug zum Regelungsgegenstand. Es bleibt daher offen, ob § 15 Absatz 3 TMG – entgegen des Wortlautes – auch dann eine Umsetzung des Artikel 5 Absatz 3 ePrivacy-Richtlinie darstellen soll, wenn die Informationen, die im Endgerät eines Teilnehmers gespeichert werden oder auf die zugegriffen wird, keinen Personenbezug haben.

§ 15 Absatz 3 TMG bezieht sich ausdrücklich und ausschließlich auf die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien. Die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, kann jedoch auch zu anderen Zwecken erfolgen und ist nicht auf die in § 15 Absatz 3 TMG genannten Zwecke beschränkt.

Schließlich fordert Artikel 5 Absatz 3 ePrivacy-Richtlinie grundsätzlich ohne Berücksichtigung konkreter Zwecke eine Einwilligung. Lediglich in Artikel 5 Absatz 3 Satz 2 ePrivacy-Richtlinie finden sich Ausnahmen von diesem Grundsatz. Dieses Regel-Ausnahme-Prinzip findet sich im TMG nicht wieder.

Webseitenbetreiber und andere Akteure, die ihre Dienste unter anderem in Bezug auf "Cookies" rechtskonform gestalten müssen, brauchen Rechtsklarheit. Der Gesetzgeber ist deshalb aufgefordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung zu beseitigen.

21.9 Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten

(Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25. November 2020)

Bei der Einrichtung des manuellen Auskunftsverfahrens von Bestandsdaten von Telekommunikationskunden hat der Gesetzgeber wichtige verfassungsrechtliche Vorgaben außer Acht gelassen. Die bisherigen Zugriffsbefugnisse der Sicherheitsbehörden sind zu weitreichend. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben bereits seit Jahren auf die Unverhältnismäßigkeit entsprechender Regelungen hingewiesen.

Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – ("Bestandsdatenauskunft II") hat das Bundesverfassungsgericht (BVerfG) erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Gericht bekräftigte, dass sowohl die

Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungsregelungen und Abrufregelungen müssen – so das Gericht – die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden (1. Leitsatz). Hierzu gehört, dass für den Einsatz zur Gefahrabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen (4. Leitsatz). Die Übermittlungsvorschrift des §113 Telekommunikationsgesetz sowie eine Reihe mit ihm korrespondierender fachgesetzlicher Abrufregelungen wurden im Hinblick hierauf für mit dem Grundgesetz unvereinbar erklärt.

Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) jedoch an die politisch Verantwortlichen, diese Frist nicht auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.

Die DSK hält es zudem für geboten, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung nicht nur die unmittelbar von der Entscheidung betroffenen Vorschriften anpassen, sondern alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts überprüfen und gegebenenfalls verfassungskonform ausgestalten. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften über Daten lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Solche Regelungen sind mit der Gefahr unbegrenzter Verwendungen von Daten verbunden und damit unverhältnismäßig (vergleiche BVerfG, oben genannter Beschluss vom 27. Mai 2020, Randnummern 154, 197). Datenabfragen dürfen nicht länger aufgrund derart unbestimmter Rechtsgrundlagen erfolgen.